Monatsh Math (2011) 163:197–209
DOI 10.1007/s00605-009-0182-3

Lexsegment and Gotzmann ideals associated with the diagonal action of $\mathbb{Z}/p$

Müfit Sezer

Received: 6 October 2009 / Accepted: 24 November 2009 / Published online: 13 December 2009

Abstract We consider a diagonal action of a cyclic group of prime order on a polynomial ring $F[x_1, \ldots, x_n]$. We give a description of the actions for which the corresponding Hilbert ideal is Gotzmann when $n = 2$. Nevertheless, we show that there is a separating set of invariant monomials that generates a proper lexsegment ideal in the polynomial ring for all n. As well, we provide an algorithm to compute this set.

Keywords Gotzmann ideals · Lexsegment ideals · Separating invariants

Mathematics Subject Classification (2000) 13P10 · 13F20 · 13A50

1 Introduction

Let V denote a finite dimensional representation of a finite group G over a field F. The induced action on the dual space V^* extends to the symmetric algebra $S(V^*)$. This is a polynomial algebra in a basis of V^* and we denote it by $F[V]$. The subalgebra of invariants $F[V]^G = \{f \in F[V] \mid g(f) = f \; \forall g \in G\}$ is a finitely generated algebra. An important course of study is to find relations between the properties of the representation and the properties of the corresponding invariant ring. Among the most well known results in this direction perhaps is that, when the order of the group

Communicated by J. S. Wilson.

Research supported by a grant from Tübitak 109T384.

M. Sezer (✉)
Department of Mathematics, Bilkent University, 06800 Ankara, Turkey
e-mail: sezer@fen.bilkent.edu.tr

the is invertible in F, the invariant ring is polynomial if and only if G is generated by reflections. But to determine the invariant ring is a difficult problem in general as the invariants become messier if one moves away from the groups generated by reflections and the degrees of the generators may become very large. Another important object is the Hilbert ideal H in $F[V]$ generated by invariants of positive degree. This ideal often plays an important role in constructing the invariant ring. For instance a Gröbner basis for H yields a generating set for $F[V]$ as a module over $F[V]^G$ and using this set one can get a basis for all invariants that can be obtained by the averaging operator over the group. For a good account of these matters and a general reference for invariant theory we recommend [2] and [13].

In this paper we study the lexsegment and the Gotzmann properties of the ideals generated by invariants of a cyclic group of prime order. Lexsegment and Gotzmann ideals have certain nice combinatorial properties and they form an important class of ideals in the study of Hilbert series of homogeneous ideals. We give the definitions and some background on them in the next section but at this point we note that the lexsegment property is defined exclusively for monomial ideals and the Gotzmann property is a weakening that practically concerns monomial ideals again. So while studying these ideals in the context of invariant theory it is natural to consider the situation where invariants are generated by monomials. Therefore for the rest of the paper G acts on V^* by diagonal matrices. In Sect. 1 we aim to establish connections between the Gotzmann property of H and the action of the group. We develop criteria to detect the Gotzmann property for the case $n := \dim V = 2$. We show that this property can be read off from the number of monomials in the minimal generating set for H with certain exponents. This quickly yields a sufficient condition for the Gotzmann property that is easily expressible in terms of the characters that appear in the action. In Sect. 2 we show that it is always possible to obtain even more special ideals using separating invariants. A separating set is a set that has the same separating power as the full ring of invariants and appears to be a useful generalization of a generating set. We give a background on them in the next section. Our main result is that there is a separating set of monomials in $F[V]^G$ that generates a proper lexsegment ideal in $F[V]$ for all n. Furthermore we give an algorithm to compute this set. We also present an invariant ring corresponding to a diagonal action of $\mathbb{Z}/2 \times \mathbb{Z}/2$ that has no graded separating subalgebra whose elements of positive degree generate a Gotzmann ideal in $F[V]$. Hence this result can not be generalized to all abelian groups even when the lexsegment property is relaxed to the Gotzmann property.

2 Preliminaries

For the rest of the paper G denotes the cyclic group $\mathbb{Z}/p$ of prime order p with $p \in F^*$. We also assume that F contains a primitive p-th root of unity λ. Fix a generator σ of G. Let $x_1, \dots, x_n$ denote a basis of V^* and assume that the action of σ on V^* with respect to this basis is given by a diagonal matrix, say $\begin{pmatrix} \lambda^{e_1} & \dots & 0 \\ 0 & \ddots & 0 \\ 0 & \cdots & \lambda^{e_n} \end{pmatrix}$. Let κ_i denote the corresponding character at the i-th coordinate and $\kappa(G) \simeq G$ denote the character group of G. We have $\sigma(x_i) = \lambda^{e_i} x_i$ for $1 \leq i \leq n$. We identify $F[V]$ with $F[x_1, x_2, \ldots, x_n]$ and denote it with R. It follows that $F[V]^G = R^G$ is generated by monomials $x_1^{a_1} \cdots x_n^{a_n}$ with $\prod \lambda^{a_i e_i} = 1 \in F$, or equivalently $\sum a_i \kappa_i = 0 \in \kappa(G)$.

We review some basic facts on lexsegment and Gotzmann ideals and separating invariants. We work with the lexicographic order on R with $x_1 > x_2 > \cdots > x_n$. A set M of monomials in R is called lexsegment if for monomials $m \in M$ and $v \in R$ we have: If $\deg m = \deg v$ and $v > m$, then $v \in M$. A monomial ideal I is called lexsegment if the set of monomials in I form a lexsegment set. Let R_t denote the homogeneous component of degree t of R. For a subspace S of R_t, let $\operatorname{lex}(S)$ denote the vector space spanned by the lexsegment set of $\dim_F S$ monomials in R_t. For two subspaces A and B in R, let $A \cdot B$ denote the vector space spanned by the elements of the form ab, for $a \in A$ and $b \in B$. By a classical theorem of Macaulay [7, C4] we have $\dim_F(R_1 \cdot \operatorname{lex}(S)) \leq \dim_F(R_1 \cdot S)$. This inequality implies that for each graded ideal in R there is a lexsegment ideal with the same Hilbert series, hence lexsegment ideals are very important objects. A subspace S in R_t is called Gotzmann if $\dim_F(R_1 \cdot \operatorname{lex}(S)) = \dim_F(R_1 \cdot S)$ and an ideal I is called Gotzmann if its homogeneous component I_t of degree t is Gotzmann for all $t \geq 0$. Notice that a lexsegment ideal is always Gotzmann. For more background on lexsegment and Gotzmann ideals, see [9] and [11]. But we warn the reader that our definition is slightly more general than the definition in these sources where Gotzmann ideals are also assumed to be generated in one degree.

A subset $A \subseteq F[V]^G$ is said to be separating if for any pairs of vectors $u, w \in V$, we have: If $f(u) = f(w)$ for all $f \in A$, then $f(u) = f(w)$ for all $f \in F[V]^G$. Separating invariants have recently emerged as an object of interest as a better behaved weakening of generating invariants. There have been a number of papers showing that one can find separating subalgebras with nice properties that are not shared by the invariant ring. For instance, separating algebras always satisfy Noether's bound [2, 3.9.14.] and separating sets for vector invariants can obtained through polarization independently of the characteristic [5], see also [4]. For more background and motivation on separating invariants we direct the reader to [2, 2.3.2, 3.9.4] and some recent studies can be found in [3,6,8,12,15,16].

For a set of monomials M, let $\langle M \rangle$ denote the vector space generated by the monomials in M. A set M of monomials in R_t is said to be closed if for all monomials $m_1, m_2 \in M$ and $m_3 \in R_t$ with $m_1 > m_3 > m_2$, we have $m_3 \in M$. For a polynomial $f \in R$, let $\operatorname{LM}(f)$ and $\operatorname{LC}(f)$ denote the leading monomial and the leading coefficient of f, respectively.

3 Gotzmann Hilbert ideals in dimension two

In this section we study the Gotzmann property of the Hilbert ideal H when $n = 2$. The main result is a criterion to detect this and consequently we give a sufficient condition on the characters for this property, see Proposition 5 and Corollary 6. For simplicity we put $x = x_1$ and $y = x_2$. Then we have $R = F[x, y]$. The Gotzmann monomial spaces in small dimension has been studied in [9] and it is pointed out in [9, Sect. 2] that if $\{0\} \neq \langle M \rangle \subseteq R_t$ is a Gotzmann space such that the greatest common divisors of monomials in M is 1, then $\langle M\rangle = R_t$. Our first lemma includes a proof of this remark.

Lemma 1 *Let t be a non-negative integer. Let $S \subseteq R_t$ be a subspace and $M \subseteq R_t$ a set of monomials. Then S is Gotzmann if and only if* $\dim_F(R_1 \cdot S) = \dim_F(S) + 1$. *Moreover, $\langle M\rangle$ is Gotzmann if and only if M is closed.*

Proof Let $M \subseteq R_t$ be a closed set of monomials containing k elements, i.e., $M = \{x^a y^{t-a}, \dots, x^{a-k+1}y^{t+k-1+a}\}$ for some non-negative integer a. Then the subspace $R_1 \cdot \langle M\rangle$ is generated by the closed set $\{x^{a+1}y^{t-a}, \dots, x^{a-k+1}y^{t+k+a}\}$ of $k+1$ monomials. It follows that $\dim_F(R_1 \cdot \langle M\rangle) = \dim_F\langle M\rangle + 1$. Moreover this equation shows that $\dim_F(R_1 \cdot \langle M\rangle)$ depends only on the dimension of $\langle M\rangle$ if M is closed. But $\operatorname{lex}(\langle M\rangle)$ is also a subspace generated by a closed set monomials of the same size, so we get $\dim_F(R_1 \cdot \operatorname{lex}(\langle M\rangle)) = \dim_F(R_1 \cdot \langle M\rangle)$. Therefore $\langle M\rangle$ is Gotzmann. More generally for a subspace S, $\operatorname{lex}(S)$ is a subspace generated by the lexsegment set of monomials of size $\dim_F S$, which is a closed set of monomials. Therefore we have

$$\dim_F(R_1 \cdot \operatorname{lex}(S)) = \dim_F S + 1.$$

Hence the first assertion of the lemma follows immediately. On the other hand, if M is not closed then we can write M as a disjoint union of closed set of monomials, say $M = \cup_{1\le i\le b} M_i$ with $b > 1$, where M_i is closed for $1 \le i \le b$ and $M_i \cup M_j$ is not closed for $i \neq j$ (otherwise replace M_i and M_j with $M_i \cup M_j$ in the union for M). Since $M_i \cup M_j$ is not closed for $i \neq j$, the exponent of x in any monomial in M_i differs from the exponent x in any monomial in M_j by at least two, so that $R_1 \cdot \langle M_i\rangle \bigcap R_1 \cdot \langle M_j\rangle = \{0\}$ for $i \neq j$. It follows that

$$\begin{aligned}\dim_F(R_1 \cdot \langle M\rangle) &= \dim_F\Big(\bigoplus_{1\le i\le b} R_1 \cdot \langle M_i\rangle\Big) = \sum_{1\le i\le b} \dim_F(R_1 \cdot \langle M_i\rangle)\\ &= \sum_{1\le i\le b} (\dim_F\langle M_i\rangle + 1) > \ \dim_F\langle M\rangle + 1,\end{aligned}$$

where the strict inequality follows because $b > 1$. Hence $\langle M\rangle$ is not Gotzmann by the first assertion of the lemma. □

Lemma 2 *Let t be a non-negative integer. Let $S \subseteq R_t$ be a subspace generated as a vector space by $f_1, \dots, f_m$. Assume that* $\mathrm{LM}(f_i) > \mathrm{LM}(f_{i+1})$ *for* $1 \le i \le m-1$, $\mathrm{LC}(f_i) = 1$ *for $1 \le i \le m$ and that no non-zero term in f_i is divisible by* $\mathrm{LM}(f_j)$ *for $j \neq i$. Then the following are equivalent.*

(1) *S is Gotzmann.*
(2) *The set* $\{\mathrm{LM}(f_i) \mid 1 \le i \le m\}$ *of leading monomials of basis vectors in S is closed and $xf_{i+1} \in \langle\{yf_i, yf_m\}\rangle$ for $1 \le i \le m-1$.*

Proof Notice that the condition on the leading coefficients and monomials of f_i for $1 \le i \le m$ is not really a restriction because any vector space basis can be refined to a basis satisfying this condition by eliminating the terms of f_i by the leading monomials of f_j for $j \neq i$ and by normalization.

Let M denote the set $\{\mathrm{LM}(f_i) \mid 1 \leq i \leq m\}$ of monomials and assume that S is Gotzmann. By the previous lemma we have that $\dim_F(R_1 \cdot S) = m + 1$. Since every monomial in $R_1 \cdot \langle M\rangle$ is a leading monomial of some polynomial in $R_1 \cdot S$, the number of monomials in $R_1 \cdot \langle M\rangle$ can not exceed $\dim_F(R_1 \cdot S)$. Therefore we get $\dim_F(R_1 \cdot \langle M\rangle) \leq m + 1$. On the other hand by Macaulay's theorem ([7, C4]) we have $\dim_F(R_1 \cdot \mathrm{lex}(\langle M\rangle) \leq \dim_F(R_1 \cdot \langle M\rangle)$. But $\mathrm{lex}(\langle M\rangle)$ is a subspace generated by a closed set of m monomials, hence from the previous lemma we get $\dim_F(R_1 \cdot \mathrm{lex}(\langle M\rangle)) = m + 1$. Combining all this information, we see that $\dim_F(R_1 \cdot \langle M\rangle) = m + 1$, hence $\langle M\rangle$ is Gotzmann and therefore M is closed by the previous lemma. Moreover, it follows that the set consisting of $m + 1$ monomials in $R_1 \cdot \langle M\rangle$ is precisely the set of leading monomials of polynomials in $R_1 \cdot S$. Therefore the smallest monomial in $R_1 \cdot \langle M\rangle$ which is $y\,\mathrm{LM}(f_m)$, is the smallest possible leading monomial of an element in $R_1 \cdot S$. Notice that for $1 \leq i \leq m - 1$, the leading monomials of xf_{i+1} and yf_i are the same because M is closed. Assume that $xf_{i+1} - yf_i \neq 0$. Since no monomial in f_i and f_{i+1} except $\mathrm{LM}(f_i)$ and $\mathrm{LM}(f_{i+1})$ are in M, it follows that $\mathrm{LM}(xf_{i+1} - yf_i) = w_1z_1$, where w_1 is either x or y and z_1 is strictly smaller than all monomials in M, that is $z_1 < \mathrm{LM}(f_m)$. But since $xf_{i+1} - yf_i \in R_1 \cdot S$, we also have $\mathrm{LM}(xf_{i+1} - yf_i) \geq y\,\mathrm{LM}(f_m)$. But $w_1z_1 \geq y\,\mathrm{LM}(f_m)$ together with $z_1 < \mathrm{LM}(f_m)$ implies that $w_1z_1 = y\,\mathrm{LM}(f_m)$, that is $\mathrm{LM}(xf_{i+1} - yf_i) = y\,\mathrm{LM}(f_m)$. Furthermore, if the polynomial $xf_{i+1} - yf_i - \mathrm{LC}(xf_{i+1} - yf_i)yf_m$ is not equal to zero, then we have $\mathrm{LM}(xf_{i+1} - yf_i - \mathrm{LC}(xf_{i+1} - yf_i)yf_m) < y\,\mathrm{LM}(f_m)$ which is a contradiction since smallest possible leading monomial of an element in $R_1 \cdot S$ is $y\,\mathrm{LM}(f_m)$.

In order to prove the converse, it suffices to show by the previous lemma that $\dim_F(R_1 \cdot S) = m + 1$ because $\dim_F S = m$. Note that since $xf_{i+1} \in \langle\{yf_i, yf_m\}\rangle$ for $1 \leq i \leq m - 1$, the subspace $R_1 \cdot S$ is spanned by $xf_1, yf_1, yf_2, \ldots, yf_m$. Hence $\dim_F(R_1 \cdot S) \leq m + 1$. On the other hand by Macaulay's theorem we have that $\dim_F(R_1 \cdot \mathrm{lex}(S)) \leq \dim_F(R_1 \cdot S)$, ([7, C4]). Also from the previous lemma we get $\dim_F(R_1 \cdot \mathrm{lex}(S)) = m + 1$, since $\mathrm{lex}(S)$ is a subspace generated by a closed set of m monomials. It follows that $\dim_F(R_1 \cdot S) = m + 1$, as desired. □

Remark 3 The proof of the previous lemma in fact shows that the condition

$$xf_{i+1} \in \langle\{yf_i, yf_m\}\rangle \quad \text{for } 1 \leq i \leq m - 1$$

implies that the set $\{\mathrm{LM}(f_i) \mid 1 \leq i \leq m\}$ is closed. We choose to phrase the lemma as it is so that it immediately provides an assertion on the set of leading monomials of a vector space basis of a homogeneous Gotzmann space.

Assume that the action of the generator σ of G on $R = F[x, y]$ is given by the matrix $\begin{pmatrix} \lambda^{e_1} & 0 \\ 0 & \lambda^{e_2} \end{pmatrix}$. Let $\kappa_1, \kappa_2 \in \kappa(G)$ be the characters in the first and the second coordinate. Assume that one of κ_1, κ_2, say κ_1 is the zero element in $\kappa(G)$. Then H is generated by x, y^d, where d is the order of $\kappa_2 \in \kappa(G)$. Hence $H_j = R_j$ for all $j \geq d$. On the other hand for $j < d$, the set of monomials in H_j is the set of all monomials in R_j except y^j which is the smallest monomial in R_j. Hence the set of monomials in H_j is closed for all j and so H is Gotzmann by Lemma 1. Therefore for the rest of the section we assume that $\kappa_1, \kappa_2 \neq 0 \in \kappa(G)$. Since $\kappa(G)$ is a cyclic group of prime order, there exist unique integers $0 < c_1, c_2 < p$ such that $\kappa_2 = c_1\kappa_1$ and $\kappa_1 = c_2\kappa_2$. Let $A = \{m_1, m_2, \ldots, m_t\}$ denote the unique minimal generating set of H that consists of monomials. Assume that $m_i = x^{a_i}y^{b_i}$ for some non-negative integers a_i, b_i for $1 \leq i \leq t$. Since each m_i is an invariant monomial we have $a_i\kappa_1 + b_i\kappa_2 = 0 \in \kappa(G)$. Moreover, since each m_i is a member of the minimal generating set, the equation $a_i\kappa_1 + b_i\kappa_2 = 0 \in \kappa(G)$ is non-shortenable for each $1 \leq i \leq t$ in the following sense: If $a\kappa_1 + b\kappa_2 = 0 \in \kappa(G)$ for some non-negative integers $0 \leq a \leq a_i$ and $0 \leq b \leq b_i$ we have either $a = b = 0$ or $a = a_i$ and $b = b_i$. It is easy to see that a non-shortenable equation $a_i\kappa_1 + b_i\kappa_2 = 0 \in \kappa(G)$ should satisfy $a_i + b_i \leq p$ and that for any pair of non-negative integers a, b with $a + b \geq p$, there exist non-negative integers $a' \leq a$ and $b' \leq b$ not simultaneously zero such that $a'\kappa_1 + b'\kappa_2 = 0$, see for instance [14]. It follows that the maximum degree of a monomial in A is p and that H contains all monomials of degree p in R. Hence $H_j = R_j$ for all $j \geq p$.

Lemma 4 *Let $m_i = x^{a_i}y^{b_i} \in A$ be a monomial in the minimal generating set for H. Then $m_i x/y \in H$ if and only if $c_2 \leq b_i$. Similarly, $m_i y/x \in H$ if and only if $c_1 \leq a_i$.*

Proof Assume that $c_2 \leq b_i$. Since m_i is an invariant monomial we have $a_i\kappa_1 + b_i\kappa_2 = 0$. Then $(a_i + 1)\kappa_1 + (b_i - c_2)\kappa_2 = 0$. It follows that $x^{a_i+1}y^{b_i-c_2}$ is an invariant monomial. Since it also divides $m_i x/y$ we have $m_i x/y \in H$. Conversely assume that $m_i x/y \in H$. Hence there exist non-negative integers $a \leq a_i + 1$ and $b \leq b_i - 1$ (not equal to zero simultaneously) such that $a\kappa_1 + b\kappa_2 = 0$. But since the equation $a_i\kappa_1 + b_i\kappa_2 = 0$ is non-shortenable it follows that $a = a_i + 1$. Taking the difference of these two equations we get $\kappa_1 = (b_i - b)\kappa_2$. Since $b_i - b$ is a non-negative integer which is at most $p - 1$, it follows that $b_i - b = c_2$, and hence $b_i \geq c_2$ as desired. The second assertion of the lemma is proven along the same lines. □

Let c denote the number of monomials in A that are not divisible by x^{c_1} or y^{c_2}. We give a sufficient and necessary condition for H to be Gotzmann.

Proposition 5 *H is Gotzmann if and only if $c < 2$.*

Proof We first consider the case $\kappa_1 = \kappa_2$. Then we have $c_1 = c_2 = 1$ and hence H is generated by the set of all monomials of degree p in R. Clearly, $c = 0$ and $H_j = \{0\}$ for $j < p$. Since we also have $H_j = R_j$ for $j \geq p$ it follows that the set of monomials in H is closed at each degree and so H is Gotzmann as well.

Next assume that $\kappa_1 \neq \kappa_2$. In this case there exists an invariant monomial of degree less or equal to $p - 1$, for example xy^{p-c_2}. We enumerate the monomials in the generating set A such that $\deg m_i \leq \deg m_{i+1}$ for $1 \leq i \leq t - 1$. We just observed that $\deg m_1 < p$. We also have if $\deg m_i = \deg m_{i+1}$, then $\deg m_i = \deg m_{i+1} = p$. To see this assume $\deg m_{i+1} \neq p$ and note that $a_i\kappa_1 + b_i\kappa_2 = 0$, $a_{i+1}\kappa_1 + b_{i+1}\kappa_2 = 0$ and $a_i + b_i = a_{i+1} + b_{i+1}$ would all together imply $(a_{i+1} - a_i)\kappa_1 = (a_{i+1} - a_i)\kappa_2$. But this would mean $\kappa_1 = \kappa_2$ (we need $\deg m_{i+1} \neq p$ for this). We have established that in the minimal generating set A no two monomials are of the same degree unless this degree is p. From this it follows that $b_1 < c_2$ because otherwise by the previous lemma m_1x/y is in H and therefore m_1x/y is divisible by some monomial m_j in the minimal generating set A. But this is not possible because the degree of m_1x/y is equal to the degree of m_1 and all other monomials in A have strictly larger degree. Similarly one sees that $a_1 < c_1$. Thus c is at least one. Assume that $c = 1$. We see that H is Gotzmann as follows. Since H_j is a Gotzmann space, in fact is equal to R_j for $j \geq p$, it suffices to show that H_j is Gotzmann for $\deg m_1 \leq j \leq p - 1$. Note that $H_{\deg m_1}$ is an one dimensional vector space spanned by m_1 and hence is Gotzmann. Assume that H_j is Gotzmann for all $\deg m_1 \leq j < i$ for some $\deg m_1 < i \leq p-1$. Therefore by Lemma 1, H_{i-1} is a subspace in R_{i-1} generated by a closed set of monomials. Let h_1, h_2 be the largest and the smallest monomials in H_{i-1}. Then the set of monomials in $R_1 \cdot H_{i-1}$ is precisely the (closed) set of monomials in R_i that lie between h_1x and h_2y. Hence $R_1 \cdot H_{i-1}$ is Gotzmann as well. Therefore if there is no monomial in A that has degree i, then H_i is easily seen to be Gotzmann because then $H_i = R_1 \cdot H_{i-1}$. Otherwise, if there is an element in A that has degree i, say $m_l = x^{a_l}y^{b_l}$, then H_i is spanned as a vector space by m_l and the closed set of monomials in $R_1 \cdot H_{i-1}$. Since $c = 1$, we have either $c_2 \leq b_l$ or $c_1 \leq a_l$. So by the previous lemma we get $m_ly/x \in H_i$ or $m_lx/y \in H_i$. Since m_l is the only monomial of degree i in A it follows that one of m_ly/x and m_lx/y lies in $R_1 \cdot H_{i-1}$. Hence the set of monomials in $R_1 \cdot H_{i-1}$ together with m_l form a closed set. But this set generates H_i, hence H_i is Gotzmann by Lemma 1. Conversely assume that H is Gotzmann and $c > 1$. Hence there exists a monomial $m_l = x^{a_l}y^{b_l} \in A$ with $l > 1$ such that $a_l < c_1$ and $b_l < c_2$. Since $\kappa_1 \neq \kappa_2$, the only invariant monomials of degree p are x^p and y^p, hence $\deg m_l < p$ because $a_l, b_l < p$. Hence m_l is the only monomial in A that has degree $\deg m_l$. Therefore $H_{\deg m_l}$ is spanned as a vector space by the set of monomials in $R_1 \cdot H_{\deg m_l - 1}$ together with m_l which should be a closed set because $H_{\deg m_l}$ is Gotzmann. Hence either m_lx/y or m_ly/x should lie in $R_1 \cdot H_{\deg m_l - 1}$. This contradicts $a_l < c_1$ and $b_l < c_2$ by the previous lemma. □

Consequently we provide a simple condition that rely only on the characters that imply that H is Gotzmann.

Corollary 6 *If $c_1c_2 = p + 1$, then H is Gotzmann.*

Proof Assume that $c_1c_2 = p + 1$. By the previous proposition it is enough to show that $c = 1$. On the contrary assume that $c > 1$ (note that $c = 0$ only if $c_1 = c_2 = 1$ by the proof of the previous proposition). Without loss of generality we take $a_1, a_2 < c_1$ and $b_1, b_2 < c_2$. Substituting $\kappa_2 = c_1\kappa_1$ into equations $a_i\kappa_1 + b_i\kappa_2 = 0$ for $1 \leq i \leq 2$ yields $a_i + b_ic_1 \equiv 0 \mod p$ for $1 \leq i \leq 2$. But since $c_1c_2 = p + 1$ and $b_1, b_2 < c_2$, we actually have $a_i + b_ic_1 = p$ for $1 \leq i \leq 2$. Then we get $a_1 - a_2 = (b_2 - b_1)c_1 \neq 0$. This yields a contradiction because $a_1, a_2 < c_1$. □

Example 1 Assume that $p > 2$ and consider any action of $G = \mathbb{Z}/p$ on R with $\kappa_2 = 2\kappa_1$. For instance we may assume that the action of σ on R is given by $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^2 \end{pmatrix}$, where λ is a primitive p-th root of unity. Clearly we have $c_1 = 2$, $c_2 = (p + 1)/2$. Therefore H is Gotzmann by the previous corollary. One might wonder if the converse of the previous corollary is correct: If σ acts by $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, then $c_1 = c_2 = p - 1$, but H is minimally generated by $\{xy, x^p, y^p\}$ and hence is Gotzmann.

Example 2 Let $G = \mathbb{Z}/17$ and $\lambda \in \mathbb{C}$ be a primitive 17-th root of unity, where $\mathbb{C}$ denotes the complex numbers. Consider the action of σ on $R = \mathbb{C}[x, y]$ afforded by the matrix $\begin{pmatrix} \lambda^2 & 0 \\ 0 & \lambda^5 \end{pmatrix}$. We have $c_1 = 11, c_2 = 14$ and it is easy to see that H is minimally generated by $\{xy^3, x^6y, x^{17}, y^{17}\}$. It follows that $c = 2$ and so H is not Gotzmann by the previous proposition. Indeed, we see that $H_7 = \langle\{x^6y, x^4y^3, x^3y^4, x^2y^5, xy^6\}\rangle$. But the set $\{x^6y, x^4y^3, x^3y^4, x^2y^5, xy^6\}$ of monomials is not closed.

4 Lexsegment ideals generated by separating sets

In this section we show that there is separating set of monomials in R^G that generates a proper lexsegment ideal in R. Our strategy is that we first provide an algorithm that gives an invariant set of monomials that generates a lexsegment ideal in R. Then we show that if one adds some suitable pure powers of the variables to the output of the algorithm, then one obtains a separating set without hurting the lexsegment property. We remark that our algorithm is motivated by [10, 1.2] where it is shown that the smallest $k \leq n$ monomials with respect to the degree lexicographic order in a minimal generating set in a lexsegment ideal is uniquely determined if one knows the degrees of these generators.

As before let σ denote a fixed generator of G and λ denote a fixed primitive p-th root of unity in F. Let $\begin{pmatrix} \lambda^{e_1} & \dots & 0 \\ 0 & \ddots & 0 \\ 0 & \cdots & \lambda^{e_n} \end{pmatrix}$ be the diagonal matrix that defines the action of σ on R. We assume that the corresponding character at the i-th coordinate κ_i is non-zero, that is $\lambda^{e_i} \neq 1 \in F$ for $1 \leq i \leq n$.

Algorithm 1 Assume the notation of the preceding paragraph.

Input. An $n \times n$ diagonal matrix with the diagonal entries $\lambda^{e_1}, \dots, \lambda^{e_n}$ which gives the action of σ on R with $\lambda^{e_i} \neq 1$ (equivalently $\kappa_i \neq 0$) for $1 \leq i \leq n$.

```
(1) Set $k = 0$, $u_1 = x_1^p$, $U = \{u_1\}$.
(2) Set $k := k + 1$. Assume that $u_k = x_1^{a_1} \cdots x_n^{a_n}$. If $a_i = 0$ for $1 \leq i \leq n - 1$,
    then go to Step 3. Otherwise let $j$ be the largest integer in $\{1, \dots, n - 1\}$ such
    that $a_j > 0$. Pick the smallest positive integer $m$ with $u_k x_{j+1}^m / x_j x_n^{a_n} \in R^G$
    and $\deg u_k \leq \deg(u_k x_{j+1}^m / x_j x_n^{a_n})$. Then set $u_{k+1} := u_k x_{j+1}^m / x_j x_n^{a_n}$ and $U :=$
    $U \cup \{u_{k+1}\}$. Repeat Step 2.
(3) Return $U$.
```

Output. The output U is a set of monomials in R^G satisfying the following properties.

(1) U generates a lexsegment ideal in R.

(2) For each $1 \leq i \leq n$, there exists a unique positive integer a_i (divisible by p) such that $x_i^{a_i} \in U$.
(3) For each couple of integers $1 \leq i < j \leq n$, there exists positive integers a_i, a_j such that p does not divide a_i, a_j and $x_i^{a_i} x_j^{a_j} \in U$.

Proof of correctness of Algorithm 1 Note that since $u_k > u_{k+1}$ for $k \geq 1$, the algorithm terminates because of the well ordering property. In fact, the final element of the algorithm is $x_n^{a_n}$ for some a_n. We start with showing that implementing Step 2 is possible. Since $\kappa_{j+1} \neq 0$ and the character group $\kappa_F(G)$ is also isomorphic to G, the character κ_{j+1} generates $\kappa_F(G)$. Therefore there exists a non-negative integer m such that $\sum_{1 \leq i \leq j-1} a_i \kappa_i + (a_j - 1)\kappa_j + m\kappa_{j+1} = 0 \in \kappa_F(G)$. Hence $x_1^{a-1} \cdots x_{j-1}^{a_{j-1}} x_j^{a_j - 1} x_{j+1}^{m} \in R^G$. Moreover by adding multiples of p, we can make m arbitrarily large. Therefore it is indeed possible to choose an integer m that meets the conditions of Step 2.

We now prove that the monomials in U generate a lexsegment ideal in R. Let I^k denote the ideal in R generated by $u_1, \ldots, u_k$. It suffices to show that I^k is lexsegment for all $k \geq 1$. We prove this by induction and this needs some preparation. Assume that $u_i = x_1^{a_1} \cdots x_n^{a_n}$ and $u_j = x_1^{b_1} \cdots x_n^{b_n}$ with $j > i$. By the construction described in Step 2, there exists $1 \leq s \leq n$ such that $b_s < a_s$ and therefore u_i does not divide u_j for $j > i$. Equivalently $u_k \notin I^{k-1}$.

Assume that I^j is a lexsegment ideal for $j \leq k$. Let t, t' denote the degrees of u_k and u_{k+1}, respectively. Then the set of monomials in I_t^k and I_t^{k-1} are lexsegment. Since u_k is the only monomial in I_t^k that is not in I_t^{k-1}, it is the smallest monomial in I_t^k. Furthermore, since I^k is generated by monomials up to degree t, the smallest monomial in $I_{t'}^k$ is given by the product of that smallest monomial in I_t^k with the smallest monomial of degree $t' - t$ in R. Hence the smallest monomial in $I_{t'}^k$ is $u_k x_n^{t'-t}$. Notice that, by construction u_{k+1} is the biggest monomial among the monomials in $R_{t'}$ that are smaller than $u_k x_n^{t'-t}$. Hence if we add u_{k+1} to the lexsegment set of monomials in $I_{t'}^k$ we still get a lexsegment set, but the set we find is exactly the set of monomials in $I_{t'}^{k+1}$. Moreover the set of monomials in I_j^{k+1} for $j < t'$ is also lexsegment by induction because $I_j^{k+1} = I_j^k$ for $j < t'$. This establishes that the set of monomials in I^{k+1} up to degree t' is lexsegment. But this makes the set all monomials in I^{k+1} lexsegment, because I^{k+1} is generated by monomials of degree at most t', see [1, 4.2.5].

Now we prove that the second property holds. Note that if x_1 does not divide u_j then x_1 does not divide u_i for $i \geq j$. Therefore the property follows by induction on the dimension of the representation if we show that there exists k with $u_k = x_2^{a_2}$ for some integer a_2. We start with $u_1 = x_1^p$ and the construction tells us that the exponent of x_1 decreases by at most one at each step. Since the terminal element is not divisible by x_1, the exponent of x_1 should fall to zero during the course of the algorithm. It follows that there exist output elements that are not divisible by x_1. Let u_{k-1} be the last output element that is divisible by x_1. Then by construction $u_k = x_2^{a_2}$ for some a_2 as desired. Uniqueness follows from the fact that $u_j < u_k$ for $j > k$.

The last property is proven along the same lines. Since x_1 does not divide an output monomial after we reach $x_2^{a_2}$, by induction it suffices to show that for each $2 \leq i \leq n$, there exist integers a_1 and a_i, neither divisible by p, such that $x_1^{a_1} x_i^{a_i} \in U$. We started the algorithm with $u_1 = x_1^p$ and therefore $u_2 = x_1^{p-1}x_2^{a_2}$ for some positive integer a_2 by construction. Since x_1^{p-1} is not an invariant, $x_2^{a_2}$ is not an invariant as well, hence p does not divide a_2. During the course of the algorithm the exponent of x_2 will eventually drop to zero (at most one step at a time) before the degree of x_1 decreases again. Therefore, if u_{j-1} is the last output element that is divisible by both x_1^{p-1} and x_2, then $u_j = x_1^{p-1}x_3^{a_3}$ for some $a_3 > 0$. We also have that a_3 is not divisible by p because $x_3^{a_3}$ is not an invariant. Continuing this way one obtains outputs in the form $x_1^{p-1}x_i^{a_i}$ for all $2 \leq i \leq n$ with p not dividing a_i as desired. □

Now we label some elements in U that will be crucial for the separating property. For $1 \leq i \leq n$, let f_i denote the invariant monomial in U that is promised by the second property of the algorithm, that is $f_i = x_i^{a_i}$ for some positive integer a_i divisible by p. Also for $1 \leq i < j \leq n$, let $u_{i,j}$ denote the smallest ranked monomial in the set $\{x_i^{a_i}x_j^{a_j} \in U \mid p \text{ does not divide } a_i, a_j\}$. Note that this set is non-empty by the last property of the algorithm. Furthermore for $1 \leq i \leq n$ define $g_i = f_i x_i^p$ and set $\overline{U} = U \cup \{g_1, \ldots, g_n\} \subseteq R^G$. It turns out that the addition of the monomials $\{g_1, \ldots, g_n\}$ yields a separating set as we show next. Note that U and $\overline{U}$ generate the same ideal in R, hence we preserve the lexsegment property.

Proposition 7 *Assume the notation and the convention of Algorithm 1 and the previous paragraph. The set $\overline{U}$ is separating.*

Proof We show that in fact that the set $A := \{f_i, g_i \mid 1 \leq i \leq n\} \cup \{u_{i,j} \mid 1 \leq i < j \leq n\}$ is separating. Assume that the set A can not separate two vectors, say $v, w \in V$. We show that $m(v) = m(w)$ for any invariant monomial $m \in R^G$ and we do this by induction on the number of variables that divide m. To this end we call the number of variables that divide a monomial the rank of this monomial. If the rank of m is one, that is if $m = x_i^{a_i}$ for some i and a_i, then there exists a positive integer a such that $m = g_i^a f_i^a$ because a_i is divisible by p. Therefore the value of m at a point is determined by f_i and g_i, if f_i is non-zero at that point. But if f_i is zero at a point so is m. It follows that since f_i, g_i can not separate v, w, neither can m.

More generally let $m = x_1^{a_1} \cdots x_n^{a_n} \in R^G$ be a monomial of rank > 1. Choose $1 \leq i < j \leq n$ such that $a_i, a_j > 0$. Since the degree of x_i in $u_{i,j}$ is not divisible by p, we can find a positive integer a such that the degrees of x_i in m and $u_{i,j}^a$ are equal modulo p. Therefore we can divide and multiply $u_{i,j}^a$ with suitable powers of f_i and g_i to make the degree of x_i match the degree of x_i in m. That is, there exist non-negative integers b, c such that the degree of x_i in m and in $u_{i,j}^a f_i^b / g_i^c$ are the same. Then $m g_i^c / u_{i,j}^a f_i^b$ is an invariant rational function, where the denominator is some non-negative power of x_j. Hence by multiplying this rational function with sufficiently large power of f_j we get an invariant monomial, that is there exists a non-negative integer d such that $m g_i^c f_j^d / u_{i,j}^a f_i^b$ is an invariant monomial. Call this monomial m'. Then we have

$$m = m' u_{i,j}^a f_i^b / g_i^c f_j^d.$$

Since x_i does not divide m', the set of variables that divide m' is a proper subset of the set of variables that divide m, i.e., the rank of m' is strictly smaller than the rank of m and hence by induction we can assume that m' does not separate the points v, w as well. First assume that f_j is zero at one of (hence both) these points. Then it follows that m is zero at both points as well because m is divisible by x_j. Similarly if g_i is zero at these points, so is m. Next assume that neither f_j nor g_i is zero at v or w. Then the value of m at these points is determined by the values of $m', u_{i,j}, f_i, g_i, f_j$ and none of these polynomials separate v and w. Therefore m does not separate v and w as well, as desired. □

We have established the following theorem.

Theorem 8 *Let $G = \mathbb{Z}/p$ be the cyclic group of prime order acting diagonally on $R = F[x_1, \ldots, x_n]$. Then there exists a separating set of monomials in R^G of positive degree that generates a lexsegment ideal in R.*

Proof This is the ingredient of Algorithm 1 and the previous proposition. But in the algorithm we assumed that there is a non-trivial action at each coordinate. More generally assume, after rearranging the indices if necessary, that the action of G is trivial on $\{x_1, \ldots, x_j\}$ and non-trivial at each coordinate on $\{x_{j+1}, \ldots, x_n\}$. First apply Algorithm 1 to get a separating set (for the last $n - j$ coordinates) of invariant monomials $\overline{U}$ in $F[x_j, \ldots, x_n]$ that generates a proper lexsegment ideal in $F[x_j, \ldots, x_n]$. Then the ideal generated by $\overline{U} \cup \{x_1, \ldots, x_j\} \subseteq R^G$ is lexsegment in R. Moreover the set $\overline{U} \cup \{x_1, \ldots, x_j\}$ is also separating because if the first j coordinates of two vectors are the same, then they are in the same G-orbit if and only if the projection vectors onto the last $n - j$ coordinates are in the same G-orbit. □

Consider the group $G' = \mathbb{Z}/2 \times \mathbb{Z}/2$ generated by the matrices $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ over the complex numbers $\mathbb{C}$. The group G' acts on $\mathbb{C}[x, y]$ and clearly $\mathbb{C}[x, y]^{G'} = \mathbb{C}[x^2, y^2]$. We conclude by showing that $\mathbb{C}[x^2, y^2]$ has no graded separating subalgebra whose elements of positive degree generate a Gotzmann ideal in $\mathbb{C}[x, y]$. Therefore the previous theorem can not be generalized to all abelian groups even when the lexsegment property is replaced with the Gotzmann property. We preserve the lexicographic order with $x > y$.

Proposition 9 *The invariant ring $\mathbb{C}[x^2, y^2]$ has no graded separating subalgebra whose elements of positive degree generate a Gotzmann ideal in $\mathbb{C}[x, y]$.*

Proof Assume on the contrary that there exists a graded separating subalgebra $A \subseteq \mathbb{C}[x^2, y^2]$ such that the elements of positive degree which we denote by A_+ generate a Gotzmann ideal in $R = \mathbb{C}[x, y]$. Let d be the smallest positive (necessarily even) integer such that the degree d component A_d of A is non-zero. Let $f_1, f_2, \ldots, f_m$ be a vector space basis for A_d satisfying the conditions of Lemma 2. Since $(A_+ \cdot R)_d = A_d$, it follows that A_d is Gotzmann space and therefore by Lemma 2, the set of monomials $M := \{\mathrm{LM}(f_i) \mid 1 \leq i \leq m\}$ is closed. But since all monomials in M are invariant, only even powers of x and y appear in these monomials. Therefore M would not be closed unless $m = 1$. Next we show that y does not divide $\mathrm{LM}(f_1)$. Note that if y divides all monomials of all polynomials in A_+, then A would not be able to separate vectors with zero y-coordinate. But not all such vectors are in the same orbit, therefore this would contradict that A is separating. Let t denote the smallest degree of a homogeneous polynomial in A_+ whose leading monomial is not divisible by y and M' denote the set of leading monomials of elements in $(A_+ \cdot R)_t$. We claim that $t = d$. Otherwise M' fails to be closed as we see as follows. The size of M' is at least two because x^t is in M' and there is a leading monomial in $(A_+ \cdot R)_t$ which is a multiple of the $\mathrm{LM}(f_1)$ which is divisible by y^2. On the other hand $x^{t-1}y \notin M'$ because y^2 divides all monomials of elements in $A_+ \cdot R$ of degree strictly smaller than t, and $x^{t-1}y$ does not appear in an invariant polynomial of degree t. Hence M' is not closed and therefore $(A_+ \cdot R)_t$ is not Gotzmann by Lemma 2. We have established that $m = 1$ and $\mathrm{LM}(f_1) = x^d$.

By [2, 2.3.12], the extension $A \subseteq R$ is finite hence the height of the ideal $A_+ \cdot R$ is two and therefore it is not a principle ideal. Let r denote the smallest (even) positive integer such that there exists a invariant polynomial of degree r in A that is not in the principal ideal $f_1 \cdot R$. We finish the proof by showing that $(A_+ \cdot R)_r$ is not Gotzmann. Let N denote the set of leading monomials of elements in $(A_+ \cdot R)_r$. Again by Lemma 2, it suffices to show that N is not closed. Clearly, all monomials of degree r that are divisible by x^d are all in N. Hence N contains the closed lex-segment set of monomials $\{x^r, x^{r-1}y, \ldots, x^d y^{r-d}\}$. Notice that this containment is proper because not every polynomial in $(A_+ \cdot R)_r$ is a multiple of f_1. Therefore if we show that $x^{d-1}y^{r-d+1} \notin N$, this establishes that N is not closed. On the contrary assume that there exists an element $h \in (A_+ \cdot R)_r$ such that $\mathrm{LM}(h) = x^{d-1}y^{r-d+1}$. We can write

$$h = gf_1 + a,$$

where $g \in R_{r-d}$ and a is an invariant polynomial in A_r. We can also write $g = g_e + g_o$, where only even powers of x and y appear in monomials in g_e (and hence in $g_e f_1$) and only odd powers of x and y appear in monomials in g_o (and in $g_o f_1$). Since only even powers of x and y appear in a, a monomial in a can not form a "*tête à tête*" with a monomial in $g_o f_1$. Since both $d-1$ and $r-d+1$ are odd and only even powers of x and y appear in a and $g_e f_1$, it follows that $x^{d-1}y^{r-d+1}$ is also the leading monomial of $g_o f_1$. This yields a contradiction because $\mathrm{LM}(f_1) = x^d$. □

References

1. Bruns, W., Herzog, J.: Cohen-Macaulay Rings. Cambridge Studies in Advanced Mathematics, Cambridge (1993)
2. Derksen, H., Kemper, G.: Computational invariant theory. Encyclopaedia of Mathematical Sciences, vol. 130, Springer, Berlin (2002)
3. Derksen, H., Kemper, G.: Computing invariants of algebraic groups in arbitrary characteristic. Adv. Math. **217**(5), 2089–2129 (2008)
4. Domokos, M.: Typical separating invariants. Transform. Groups **12**(1), 49–63 (2007)
5. Draisma, J., Kemper, G., Wehlau, D.: Polarization of separating invariants. Can. J. Math. **130**(3), 556–571 (2008)
6. Dufresne, E.: Separating invariants and finite reflection groups. Adv. Math. **221**(6), 1979–1989 (2009)

7. Iarrobino, A., Kanev, V.: Power Sums, Gorenstein Algebras, and Determinantal Loci. Lecture Notes in Mathematics, vol. 1721. Springer, Berlin (1999)
8. Kemper, G.: Separating invariants. J. Symb. Comput. **44**, 1212–1222 (2009)
9. Murai, S.: Gotzmann monomial ideals. Illinois J. Math. **51**(3), 843–852 (2007)
10. Murai, S., Hibi, T.: Depth of an ideal with a given Hilbert function. Proc. Am. Math. Soc. **136**(5), 1533–1538 (2008)
11. Murai, S., Hibi, T.: Gotzmann ideals of the polynomial ring. Math. Z. **260**(3), 629–646 (2008)
12. Neusel, M.D., Sezer, M.: Separating invariants for modular p-groups and groups acting diagonally. Math. Res. Lett. Available at http://www.fen.bilkent.edu.tr/~sezer (2009, to appear)
13. Neusel, M.D., Smith, L.: Invariant Theory of Finite Groups. Mathematical Surveys and Monographs, vol. 94. American Mathematical Society, Providence (2002)
14. Schmid, B.J.: Finite Groups and Invariant Theory. Topics in Invariant Theory (Paris, 1989/1990). Lecture Notes in Mathmatics, vol. 1478, pp. 35–66. Springer, Berlin (1991)
15. Sezer, M.: Constructing modular separating invariants. J. Algebra **322**(11), 4099–4104 (2009)
16. Smith, L., Stong, R.E.: Invariants of binary bilinear forms modulo two. Proc. Am. Math. Soc. **138**(1), 17–26 (2010)