International Journal of Algebra, Vol. 6, 2012, no. 6, 291 - 297

A Note on Separating Vector Invariants for Modular Representations

Uğur Madran

Izmir University of Economics
Department of Mathematics
Balçova, 35330 Izmir, Turkey
ugur.madran@ieu.edu.tr
madran@member.ams.org

Abstract. In this note, we present an efficient method of calculating *separating invariants* for vector invariants in the modular case which fills a gap for polynomial invariants over a field of relatively small size.

Mathematics Subject Classification: Primary 13A50

Keywords: Invariant theory, separating invariants, vector invariants

1. Introduction

Let G be a finite group acting on an n-dimensional vector space V over a field $\mathbb{F}$ of characteristic $p > 0$ which is algebraic over prime field. We denote the ring of regular functions on V by $\mathbb{F}[V]$, i.e., if $\{x_1, \ldots, x_n\}$ is a basis for the dual space V^* then $\mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n]$ is the polynomial ring in n variables.

A word of caution is needed here: We regard functions on $V \otimes \overline{\mathbb{F}}$ in order to distinguish, for example x^q and x on $V = \mathbb{F}^n$ where $\mathbb{F}$ is a finite field with $q = p^\nu$ elements and $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$. A simple solution is generally to identify $\mathbb{F}[V]$ with the symmetric algebra $S(V^*)$. After determining a basis for V^*, we can safely work on the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$.

The ring of invariants of G is defined as

$$\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \mid g(f) = f \ \forall g \in G\},$$

where the action of G on $\mathbb{F}[V]$ is induced by the action of G on V, given explicitly as $g(f)(v) = f(g^{-1}(v))$, for $g \in G$. For the sake of simplicity, we will denote the invariant ring by $A = \mathbb{F}[V]^G$ throughout the paper.

It is well-known that A is finitely generated as an algebra and moreover the degree of generators is bounded from above by $|G|$ whenever $\mathrm{char}(\mathbb{F}) \nmid |G|$. This case is known as non-modular case. In the *modular case,* where $|G| = 0$ in $\mathbb{F}$, the generating set is generally not well-behaved. There is no priori upper bound for the degree of generators which only depends on G. Moreover, A is mostly not Cohen-Macaulay in the modular case, providing a strong evidence for the structural complexity of the modular invariant rings.

In 2002, Derksen and Kemper [3] introduced a separating set as an alternative tool to a generating set.

Definition 1 (Separating Set)**.** A subset $S \subset A$ is said to be a *separating set* if for all $u, v \in V$ if there exists $f \in A$ such that $f(u) \neq f(v)$ then there exists $\widetilde{f} \in S$ such that $\widetilde{f}(u) \neq \widetilde{f}(v)$.

Separating sets have been extensively studied after being introduced, and became a popular research topic in the theory of polynomial invariants. Some of articles can be cited as [4, 5, 7, 8, 9, 10, 11, 12, 14, 15] and references cited in these articles.

It is known that separating sets are well-behaved when compared to generating sets. We will summarize some of important known results about separating sets:

- There always exists a finite separating set. [3]
- For finite groups, there exists a separating set consisting of invariants of degree at most $|G|$. [3]
- (Cheap) Polarizations of a separating set of one copy of a representation give a separating set for vector invariants if the ground field has sufficiently many elements, or the original separating set is a generating set (as an algebra). [5]
- The restriction on the field size cannot be removed (even in nonmodular case). [6]
- Trivial polarizations work for any separating set if we start with enough many copies of the representations. [4]

This paper is organized as follows: In the next section, we will introduce the *vector invariants.* Results about vector invariants are generally called as *First Fundamental Theorem* of the given representation. In the third section, we will describe tools to achieve the main result. The following section is devoted to the main result of the paper. Finally, in the last section, we will compare our results with previously known results.

2. Vector Invariants

Let m be a positive integer, and $W = V \oplus \cdots \oplus V$ vector space consisting of m copies of V. The action of G on V can be extended to W diagonally. Explicitly, the action of G on W can be given as $g(v_1, \ldots, v_m) := (g(v_1), \ldots, g(v_m))$. The main problem here is to find invariant ring $\mathbb{F}[W]^G$, and if possible, in terms of $\mathbb{F}[V]^G$.

Vector invariants are generally used as a tool to show how a particular property of an invariant ring is well-behaved or wildly-behaved. As an example, Weyl's theorem [16, Theorem 2.5.A] shows that generating sets are well-behaved vector invariants in characteristic 0 and Richman's theorem [13] shows that beta-number of vector invariants is wildly-behaved in modular case over finite fields.

We are mainly interested in the modular case. The main reason for dealing with the modular case is that, actually, any generating set is also a separating set. Moreover, polarizations of generating sets provide separating sets (see [5]). But finding generating sets in the modular case is mostly infeasible. So, we need an alternative approach to find separating sets for vector invariants.

Remark 2. Draisma et.al. also provide a method for finding separating invariants (see [5]). Namely, if $S \subset \mathbb{F}[V]^G$ is a separating set and $\mathbb{F}$ has at least $(n-1)|G|$ elements, then polarization of S is a separating set for $\mathbb{F}[W]^G$. Although this result is remarkable, it does not give any separating set for the most simple cases. For example, if $\mathbb{F}$ is the prime field with p elements, then G should have at least p elements in the modular case, therefore, the only case that the result can be applied is where $n = \dim V = 2$. But the whole invariant ring $\mathbb{F}_p[V_2^m]^{C_p}$ is completely known, where $G = C_p$ is the cyclic group of order p and V_2^m is the direct sum of m-copies of 2-dimensional vector space $V = V_2 = \mathbb{F}^2$. (See, for example, [2, pp.23-24].)

Remark 3. The restriction on the field size of the above mentioned result cannot be removed. The next example is from [6]. We include it here for the convenience of the reader.

Example 4 (Dufresne's counter example)**.** Consider the action of C_3 on $V_2 = \mathbb{F}_2^2$ afforded by

$$1 \mapsto \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

The invariant ring is generated by 3 polynomials, say f_1, f_2, f_3, 1 of degree 2 and 2 of degree 3. Moreover, each of these generators constitute a set of single element which separates $A = \mathbb{F}_2[V_2]^{C_3}$.

Since we are looking for a simple (and hence of minimal degree) separating set, we consider $S = \{f_1\} = \{x^2 + xy + y^2\}$. But $\mathrm{Pol}(S) = \{x_1^2 + x_1y_1 + y_2^2, x_1y_2 + y_1x_2, x_2^2 + x_2y_2 + y_2^2\}$ is no more a separating set for $\mathbb{F}_2[2V_2]^{C_3}$. (See [6] for details.)

This example is also remarkable for being an example in the non-modular case, showing difficulties of working over positive characteristics.

3. Polarizations and Separating Invariants

Existence of a separating set for any invariant ring (of a finite group) is guaranteed by the following theorem of Derksen and Kemper:

Theorem 5 (c.f. Theorem 3.9.13 in [3])**.** *Let*

$$(1)\qquad F(T, U_1, \ldots, U_n) = \prod_{g \in G} \left(T - \sum_{j=1}^{n} g(x_j)U_j \right) \in \mathbb{F}[V]^G[T, U_1, \ldots, U_n].$$

Then the coefficients of F (as a polynomial in $T, U_1, \dots, U_n$) form a separating set.

Polarization of a function provides a passage from $\mathbb{F}[V]$ to $\mathbb{F}[W]$ (recall that $W = V \oplus \cdots \oplus V$, or in short $W = V^m$). Let $f(x_1, \dots, x_n) \in \mathbb{F}[V]$ be a polynomial. Then define

$$\Phi(f) = f\big(\sum_{i=1}^{m} x_{i,1}\lambda_i, \dots, \sum_{i=1}^{m} x_{i,n}\lambda_i\big) = \sum f_{(d_1,\dots,d_m)}(x_{i,j})\lambda_1^{d_1}\cdots\lambda_m^{d_m},$$

where the last sum if over nonnegative exponent sequence $(d_1, \dots, d_m) \in \mathbb{N}_0^m$. Polarization of f is the set of coefficients of $\Phi(f)$ as a polynomial in λ_i's:

$$\mathrm{Pol}(f) = \{f_{(d_1,\dots,d_m)} \,|\, f_{(d_1,\dots,d_m)} \text{ appears in } \Phi(f)\}.$$

Cheap polarization is defined analogously:

$$\Psi(f) = f\big(\sum_{i=1}^{m} x_{i,1}\lambda^{i-1}, \dots, \sum_{i=1}^{m} x_{i,n}\lambda^{i-1}\big) = \sum_{d\geq 0} f_d(x_{i,j})\lambda^d,$$

and

$$\mathrm{Pol}_{\mathrm{cheap}}(f) = \{f_d \,|\, f_d \text{ appears in } \Psi(f)\}.$$

We will illustrate the above definitions with an example:

Example 6. Let $f(x, y) = xy \in \mathbb{F}[V_2]$ be a symmetric polynomial. If we take $m = 3$, then

$$\mathrm{Pol}(f) = \{x_1y_1, x_2y_2, x_3y_3, x_1y_2 + x_2y_1, x_1y_3 + x_3y_1, x_2y_3 + x_3y_2, \}$$

is the set of multi-symmetric polynomials. Moreover,

$$\mathrm{Pol}_{\mathrm{cheap}}(f) = \{x_1y_1, x_1y_2 + x_2y_1, x_2y_2 + x_1y_3 + x_3y_1, x_2y_3 + x_3y_2, x_3y_3\}.$$

Note that, the polarized polynomials x_2y_2 and $x_1y_3 + x_3y_1$ do not belong to $\mathrm{Pol}_{\mathrm{cheap}}$ but their sum does.

Remark 7. The following modification of the auxiliary function $F(T, U_1, \dots, U_n)$ defined in (1) also gives a separating set (see [5] for details):

$$\widetilde{F}(T, U) = \prod_{g\in G}\left(T - \sum_{j=1}^{n} g(x_j)U^{j-1}\right) \in \mathbb{F}[V]^G[T, U]. \tag{2}$$

Note that the analogy between (1) and (2) is the same analogy between Pol and $\mathrm{Pol}_{\mathrm{cheap}}$.

4. Main Result

As has been mentioned in Remark 2, to our knowledge, no optimized way of finding a separating set for invariant rings over fields of small size in the modular case exists. It is our aim here in this section to fill this gap.

4.1. **Notations:** Throughout the rest of this paper, let $\mathbb{F}[V] = \mathbb{F}[x_1, \dots, x_n]$, and $W = V \oplus \cdots \oplus V$ direct sum of m-copies of V, with polynomial algebra $\mathbb{F}[W] = \mathbb{F}[x_{1,1}, \dots, x_{1,n}, \cdots, x_{m,1}, \dots, x_{m,n}]$. Moreover, let $G \leq \mathrm{GL}(V)$ and the action of G is extended to W diagonally, as defined before. We will consider the modular case where $|G| \notin \mathbb{F}^{\times}$, but the result is also valid for any characteristic.

Let A be an $\mathbb{F}$-algebra (in our paper, A is either $\mathbb{F}[V]^G$ or $\mathbb{F}[W]^G$, depending on the context) and $X_1, \dots, X_k$ be new indeterminates (or equivalently some transcendental elements over A). Then for any $F \in A[X_1, \dots, X_k]$, we will denote the set of coefficients of F (as a polynomial in $X_1, X_2, \dots, X_k$) by $\mathrm{Coeffs}(F)$ (in what follows, X_i's will be either T or U's, or λ's).

Proposition 8. *With the notations defined above, let*

$$\widetilde{F}_m(T, U) = \prod_{g \in G} \Big(T - \sum_{i=1}^{m} \sum_{j=1}^{n} g(x_{i,j}) U^{(i-1)n+j-1} \Big). \tag{3}$$

Then $\mathrm{Coeffs}(\widetilde{F}_m)$ *is a separating set for* $\mathbb{F}[W]^G$.

Proof. The result follows by applying the result mentioned in Remark 7. We direct the reader to [5, c.f. Lemma 2.1] for details. □

Remark 9. The proposition is also valid if we use an alternative form

$$F_m(T, \widetilde{U}_1, \dots, \widetilde{U}_m) = \prod_{g \in G} (T - \sum_{i=1}^{m} \sum_{j=1}^{n} g(x_{i,j}) \widetilde{U}_i^{j-1}). \tag{4}$$

The proof for this alternative form is mostly the same but requires more detailed calculations. For the sake of simplicity, we omit the details here and continue our note only by considering the results obtained through the polynomial introduced in equation (3). One final comment here is necessary: U's have been denoted on purpose by $\widetilde{U}_i$ to distinguish them from their previous usage. Their previous usage (see (1)) reveals a characteristic property of the representation V and hence there were only $n = \dim V$ of them. Here, we have m of $\widetilde{U}_i$'s and we are trying to observe some characteristics of diagonal representation $W = V^m$, where $\dim W = mn \neq m$.

An important observation about these auxiliary polynomials is that the degree of $\widetilde{F}_m$ is $(mn - 1)|G|$ in 2 variables, and the degree of F_m is $(n - 1)|G|$ in $m + 1$ variables. That means, both auxiliary polynomials $\widetilde{F}_m(T, U)$ and $F_m(T, \widetilde{U}_1, \dots, \widetilde{U}_m)$ requires calculating approximately $nm|G|$ terms. This process can be cumbersome, especially when m is large enough even $|G|$ and n are small. ◁

Theorem 10 (Main Result)**.** *With the notations of this section, let* $S = \mathrm{Coeffs}(\widetilde{F}(T, U))$. *Then,* $\mathrm{Pol}(S)$ *is a separating set for* $\mathbb{F}[W]^G$.

In order to prove this result, we need a technical result:

Lemma 11. $\mathrm{Coeffs}(\widetilde{F}_m(T, U)) = \mathrm{Coeffs}(\mathrm{Pol}(\widetilde{F}(T, U)))$.

Proof. Note that

$$\begin{aligned}
\operatorname{Pol}(\widetilde{F}(T,U)) &= \operatorname{Pol}\Big(\prod_{g\in G}\big(T-\sum_{j=1}^{n} g(x_j)U^{j-1}\big)\Big)\\
&= \operatorname{Coeffs}\Big(\prod_{g\in G}\big(T-\sum_{j=1}^{n} g(\sum_{i=1}^{m} x_{i,j}\lambda_i)U^{j-1}\big)\Big)\\
(\star) \qquad &= \operatorname{Coeffs}\Big(\prod_{g\in G}\big(T-\sum_{i=1}^{m}\sum_{j=1}^{n} g(x_{i,j})\lambda_i U^{j-1}\big)\Big)
\end{aligned}$$

Now, lets specialize $(\star)$ at $\lambda_i = U^{(i-1)n}$ which actually provides an injective map between terms of given polynomials. Hence, the proof is completed. □

Proof of Main Theorem. The proof now follows from Proposition 8 by combining with the result of the above Lemma. □

5. Concluding Remarks

It is important to note that Pol$(-)$ always gives a separating set for vector invariants if we begin with a "nice" set.

In the nonmodular case, one may begin with a generating set (for degree considerations) if it is easier to find it first. But especially for the modular case, finding these generators is much more difficult. Separating invariants were mainly introduced to ease this difficulty.

Thus, our result allows to construct a separating set for vector invariants without any priori knowledge. First, we obtain a separating set for $\mathbb{F}[V]^G$ and then extend it to $\mathbb{F}[W]^G$. Though, it might not be the optimum set but it is easier to compute and fills the mentioned gap in [5].

It has been recently announced (see [11]) that for any p-group G, $\beta_{\text{sep}} = |G|$. Thus, any separating set should contain an invariant of degree $|G|$. It is unavoidable. Our separating set also attains this bound, and moreover, the separating has no invariants of larger degree. From this point of view, our separating set for vector invariants is optimal.

Acknowledgements

This result was first presented in the 2010 Summer Meeting of Canadian Mathematical Society in UNB, Fredericton, by the author.

References

[1] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235–265.

[2] H.E.A.E. Campbell, D.L. Wehlau, *Modular invariant theory*, Springer-Verlag, Berlin, (2011).

[3] H. Derksen, G. Kemper, *Computational invariant theory*, Springer-Verlag, Berlin, (2002).

[4] M. Domokos, Typical separating invariants, *Transform. Groups* **12** (2007), no. 1, 49–63.

[5] J. Draisma, G. Kemper, D. Wehlau, Polarization of separating invariants, *Canad. J. Math.* **60** (2008), no. 3, 556–571.

[6] E. Dufresne, *Separating Invariants*, Ph. D. thesis, Queen's University, Kingston, ON, Canada, (2008).

[7] E. Dufresne, Separating invariants and finite reflection groups, *Adv. Math.* **221** (2009), no. 6, 1979–1989.

[8] E. Dufresne, J. Elmer, M. Kohls, The Cohen-Macaulay property of separating invariants of finite groups, *Transform. Groups* **14** (2009), no. 4, 771–785.

[9] E. Dufresne, M. Kohls, A finite separating set for Daigle and Freudenburg's counterexample to Hilbert's fourteenth problem, *Comm. Algebra* **38** (2010), no. 11, 3987–3992.

[10] G. Kemper, Separating invariants, *J. Symbolic Comput.* **44** (2009), no. 9, 1212–1222.

[11] M. Kohls, H. Kraft, Degree bounds for separating invariants, *Math. Res. Lett.* **17** (2010), no. 6, 1171–1182.

[12] M.D. Neusel, M. Sezer, Separating invariants for modular p-groups and groups acting diagonally, *Math. Res. Lett.* **16** (2009), no. 6, 1029–1036.

[13] D.R. Richman, Invariants of finite groups over fields of characteristic p, *Adv. Math.* **124** (1996), no. 1, 25–48.

[14] M. Sezer, Constructing modular separating invariants, *J. Algebra* **322** (2009), no. 11, 4099–4104.

[15] M. Sezer, Explicit separating invariants for cyclic P-groups, *J. Combin. Theory Ser. A* **118** (2011), no. 2, 681–689.

[16] H. Weyl, *The classical groups: Their invariants and representations*, Princeton University Press, Princeton, NJ, (1997).

Received: October, 2011