On separating invariants over prime fields

Uğur Madran

İzmir University of Economics
Dept. of Mathematics

CMS Summer Meeting 2010
June 6 2010, Fredericton

Contents

Main Object.

- Let $\mathbb{F}$ be a finite field of characteristic p, V be an n-dimensional vector space over $\mathbb{F}$, and G be a subgroup of $\mathrm{GL}(V)$. We will consider $A = \mathbb{F}[V]^G$.

Main Object.

- Let $\mathbb{F}$ be a finite field of characteristic p, V be an n-dimensional vector space over $\mathbb{F}$, and G be a subgroup of $\mathrm{GL}(V)$. We will consider $A = \mathbb{F}[V]^G$.

Definition (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 $\widetilde{f}(u) \neq \widetilde{f}(v)$.

Generators.

- There always exists a finite separating set. (Derksen-Kemper, 2002.)

Generators.

- There always exists a finite separating set. (Derksen-Kemper, 2002.)
- For finite groups, there exists a separating set consisting of invariants of degree at most $|G|$. (Derksen-Kemper, 2002.)

Generators.

- There always exists a finite separating set. (Derksen-Kemper, 2002.)
- For finite groups, there exists a separating set consisting of invariants of degree at most $|G|$. (Derksen-Kemper, 2002.)
- (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). (Draisma-Kemper-Wehlau, 2008.)

Generators.

- There always exists a finite separating set. (Derksen-Kemper, 2002.)
- For finite groups, there exists a separating set consisting of invariants of degree at most $|G|$. (Derksen-Kemper, 2002.)
- (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). (Draisma-Kemper-Wehlau, 2008.)
- The restriction on the field size cannot be removed (even in nonmodular case). (Dufresne, 2008.)

Generators.

- There always exists a finite separating set. (Derksen-Kemper, 2002.)
- For finite groups, there exists a separating set consisting of invariants of degree at most $|G|$. (Derksen-Kemper, 2002.)
- (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). (Draisma-Kemper-Wehlau, 2008.)
- The restriction on the field size cannot be removed (even in nonmodular case). (Dufresne, 2008.)
- Trivial polarizations work for any separating set if we start with enough many copies of the representations. (Domokos, 2007.)

Dufresne's counter example.

- Consider the action of $\mathbb{Z}/3$ on $V_2 = \mathbb{F}_2^2$ afforded by

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

Dufresne's counter example.

- Consider the action of $\mathbb{Z}/3$ 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.

Dufresne's counter example.

- Consider the action of $\mathbb{Z}/3$ 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.
- Since we are looking for a simple (and hence of minimal degree) separating set, we consider $S = \{f_1\}$.

Dufresne's counter example.

- Consider the action of $\mathbb{Z}/3$ 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.
- Since we are looking for a simple (and hence of minimal degree) separating set, we consider $S = \{f_1\}$.
- But $\mathrm{Pol}(S)$ is no more a separating set for $\mathbb{F}[2V_2]^{\mathbb{Z}/3}$.

Dufresne's counter example.

- Consider the action of $\mathbb{Z}/3$ 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.
- Since we are looking for a simple (and hence of minimal degree) separating set, we consider $S = \{f_1\}$.
- But $\mathrm{Pol}(S)$ is no more a separating set for $\mathbb{F}[2V_2]^{\mathbb{Z}/3}$.
- Nevertheless, $\mathrm{Pol}(\{f_2\})$ is a separating set for $\mathbb{F}[2V_2]^{\mathbb{Z}/3}$.

Construction.

From now on, we are mainly interested in a separating set for $\mathbb{F}[mV]^G$ based on a representation of G on V, with $\dim V = n$.

Construction.

From now on, we are mainly interested in a separating set for $\mathbb{F}[mV]^G$ based on a representation of G on V, with $\dim V = n$.

- The first idea to find a convenient way of constructing a separating set is of course to modify the original auxiliary $F(T, U)$ polynomial given by Derksen and Kemper.

Construction.

From now on, we are mainly interested in a separating set for $\mathbb{F}[mV]^G$ based on a representation of G on V, with $\dim V = n$.

- The first idea to find a convenient way of constructing a separating set is of course to modify the original auxiliary $F(T, U)$ polynomial given by Derksen and Kemper.
- Define,

$$F_m(T, \mathbf{U}) = \prod_{g \in G} (T - \sum_{i=1}^{m} \sum_{j=1}^{n} g(x_{i,j}) U_i^{j-1}).$$

This polynomial is actually "full polarization" of original polynomial $F(T, U)$, and its coefficients give a separating set.

(Cont.)

- Instead, we can think of the vector invariants as a 1-copy of some decomposable representation:

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

This time, we get the "cheaply polarized" version of $F(T,U)$, and again its coefficients give a separating set.

(Cont.)

- Instead, we can think of the vector invariants as a 1-copy of some decomposable representation:

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

  This time, we get the “cheaply polarized” version of $F(T,U)$, and again its coefficients give a separating set.
- But “trivial polarization” of $F(T,U)$, does not provide a separating set (Dufresne’s example is a counter example for V to $2V$.)

Simplifications.

- Evaluating coefficients of $F(T, U)$ or $F_m(T, \mathbf{U})$ might be cumbersome when m is so large. (Number of monomials in U is $(mn|G|)$.)

Simplifications.

- Evaluating coefficients of $F(T, U)$ or $F_m(T, \mathbf{U})$ might be cumbersome when m is so large. (Number of monomials in U is $(mn|G|)$.)
- Instead, we compute coefficients of $F(T, U)$ for $\mathbb{F}[V]^G$ and then apply "cheap polarization" process to this separating set to get a separating set for $\mathbb{F}[mV]^G$.

Simplifications.

- Evaluating coefficients of $F(T, U)$ or $F_m(T, \mathbf{U})$ might be cumbersome when m is so large. (Number of monomials in U is $(mn|G|)$.)
- Instead, we compute coefficients of $F(T, U)$ for $\mathbb{F}[V]^G$ and then apply "cheap polarization" process to this separating set to get a separating set for $\mathbb{F}[mV]^G$.
- **Remark:** It is important to note that $\mathrm{Pol}(\bullet)$ always gives a separating set for vector invariants if we begin with a "nice" set.

Simplifications.

- Evaluating coefficients of $F(T, U)$ or $F_m(T, \mathbf{U})$ might be cumbersome when m is so large. (Number of monomials in U is $(mn|G|)$.)
- Instead, we compute coefficients of $F(T, U)$ for $\mathbb{F}[V]^G$ and then apply "cheap polarization" process to this separating set to get a separating set for $\mathbb{F}[mV]^G$.
- **Remark:** It is important to note that $\mathrm{Pol}(\bullet)$ always gives a separating set for vector invariants if we begin with a "nice" set.

  In the nonmodular case, we may begin with an algebra 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. Thus, this simplification allows us to construct a separating set for vector invariants. Though, it might not be the optimum set but it is easier to compute.

Thanks.

Thank you.