Taylor & Francis
Taylor & Francis Group

The separating variety for 2 × 2 matrix invariants

Jonathan Elmer

Published online: 16 Jan 2023.

Submit your article to this journal ⅾ

Article views: 485

View related articles ⅾ

View Crossmark data ⅾ

Taylor & Francis
Taylor & Francis Group

The separating variety for 2 × 2 matrix invariants

Jonathan Elmer 📵

Middlesex University, London, UK

ABSTRACT

Let G be a linear algebraic group acting linearly on a vector space (or more generally, an affine variety) $\mathcal{V}$, and let $\Bbbk[\mathcal{V}]^G$ be the corresponding algebra of invariant polynomial functions. A separating set $S \subseteq \Bbbk[\mathcal{V}]^G$ is a set of polynomials with the property that for all $v, w \in \mathcal{V}$, if there exists $f \in \Bbbk[\mathcal{V}]^G$ separating v and w, then there exists $f \in S$ separating v and w. In this article, we consider the action of $G = \mathrm{GL}_2(\mathbb{C})$ on the $\mathbb{C}$-vector space $\mathcal{M}_2^n$ of n-tuples of 2×2 matrices by simultaneous conjugation. Minimal generating sets S_n of $\mathbb{C}[\mathcal{M}_2^n]^G$ are well known and $|S_n| = \frac{1}{6}(n^3 + 11n)$. In recent work, Kaygorodov et al. [Kaygorodov I, Lopatin A, Popov Y. Separating invariants for 2×2 matrices. Linear Algebra Appl. 2018;559:114-124.] showed that for all $n \geq 1$, S_n is a minimal separating set by inclusion, i.e. that no proper subset of S_n is a separating set. This does not necessarily mean that S_n has minimum cardinality among all separating sets for $\mathbb{C}[\mathcal{M}_2^n]^G$. Our main result shows that any separating set for $\mathbb{C}[\mathcal{M}_2^n]^G$ has cardinality $\geq 5n - 5$. In particular, there is no separating set of size $\dim(\mathbb{C}[\mathcal{M}_2^n]^G) = 4n - 3$ for $n \geq 3$. Further, S_3 has indeed minimum cardinality as a separating set, but for $n \geq 4$ there may exist a smaller separating set than S_n. We show that a smaller separating set does in fact exist for all $n \geq 5$. We also prove similar results for the left–right action of $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})$ on $\mathcal{M}_2^n$.

1. Introduction

1.1. Matrix invariants

Let $\Bbbk$ be an infinite field and let $\mathcal{M}_d$ denote the space of $d \times d$ matrices with coefficients in $\Bbbk$. The linear algebraic group $G := \mathrm{GL}_d(\Bbbk)$ acts on $\mathcal{M}_d$ by conjugation. More generally we can consider the action of G on $\mathcal{M}_d^n$ by simultaneous conjugation.

The elements of $\mathcal{M}_d^n$ can be viewed as n-tuples $\mathbf{A} = (A_1, A_2, \dots, A_n)$, or as $d \times d$ matrices with entries in $\Bbbk^n$. We call these n-matrices for short. For $g \in G$ we write the conjugation action as

$$g \cdot \mathbf{A} := (gA_1 g^{-1}, \dots, gA_n g^{-1}).$$

The question of determining whether a pair of matrices lie in the same G-orbit is a staple of undergraduate linear algebra. On the other hand, the question of determining whether

a pair of n-matrices lie in the same G-orbit for $n \geq 2$ is the archetypal 'wild' problem, see, for example [1].

There is an action of $\mathrm{GL}_n(\Bbbk)$ on $\mathcal{M}_d^n$ which commutes with the conjugation action: namely, for $h \in \mathrm{GL}_n(\Bbbk)$ and an n-matrix $\mathbf{A} = (\mathbf{a}_{ij}) \in \mathcal{M}_d(\Bbbk^n)$ we write $h \star \mathbf{A}$ for the n-matrix whose i, j entry is

$$(h \star \mathbf{A})_{ij} = h(\mathbf{a}_{ij}) \tag{1}$$

Now for $1 \leq i, j \leq d$ and $1 \leq k \leq n$, let $x_{ij}^{(k)}$ denote the linear functional $\mathcal{M}_d^n \to \Bbbk$ which picks out the i, jth entry of A_k, and introduce generic matrices

$$X_k := \begin{pmatrix} x_{11}^{(k)} & x_{12}^{(k)} & \cdots & x_{1d}^{(k)} \\ x_{21}^{(k)} & x_{22}^{(k)} & \cdots & x_{2d}^{(k)} \\ \vdots & \vdots & & \vdots \\ x_{d1}^{(k)} & x_{d2}^{(k)} & \cdots & x_{dd}^{(k)} \end{pmatrix}.$$

Then we have

$$\Bbbk[\mathcal{M}_d^n] = \Bbbk[x_{ij}^{(k)} : i, j = 1, \ldots, d, k = 1, \ldots, n].$$

The action of G on $\mathcal{M}_d^n$ induces an action of G on $\Bbbk[\mathcal{M}_d^n]$ by algebra automorphisms: we define

$$(g \cdot f)(\mathbf{A}) = f(g^{-1} \cdot \mathbf{A})$$

for all $g \in G, f \in \Bbbk[\mathcal{M}_d^n]$ and $\mathbf{A} \in \mathcal{M}_d^n$. The set $\Bbbk[\mathcal{M}_d^n]^G$ of fixed points of this action forms a $\Bbbk$-subalgebra. Elements of $\Bbbk[\mathcal{M}_d^n]^G$ are called matrix invariants. The algebra $\mathbb{C}[\mathcal{M}_d^n]^G$ has been intensely studied over the years. A minimal generating set is known for arbitrary n only in the case $d \leq 2$. We ignore $d = 1$ as in this case G acts trivially. For $d = 2$ we have the following result [2]:

Proposition 1.1 (LeBruyn–Procesi): *The following set S_n of invariants minimally generates* $\mathbb{C}[\mathcal{M}_2^n]^G$ *as an algebra:*

- $\mathrm{Tr}(X_i), i = 1, \ldots, n.$
- $\det(X_i), i = 1, \ldots n.$
- $\mathrm{Tr}(X_i X_j), 1 \leq i < j \leq n.$
- $\mathrm{Tr}(X_i X_j X_k), 1 \leq i < j < k \leq n.$

1.2. Separating invariants

Now consider a more general situation in which a linear algebraic group G defined over $\Bbbk$ acts linearly on an affine $\Bbbk$-variety $\mathcal{V}$. Let $\Bbbk[\mathcal{V}]$ denote the algebra of polynomial functions on $\mathcal{V}$. Then G acts on $\Bbbk[\mathcal{V}]^G$ according to the formula

$$(g \cdot f)(v) = f(g^{-1}v). \tag{2}$$

We denote by $\Bbbk[\mathcal{V}]^G$ the subalgebra of $\Bbbk[\mathcal{V}]$ fixed by this action. For $v, w \in \mathcal{V}$ and any $f \in \Bbbk[\mathcal{V}]^G$ we have $f(v) = f(w)$ if $v \in Gw$, but the converse is not true in general.

Example 1.2: Let $G = \mathrm{GL}_2(\mathbb{C})$ as in Section 1.1. It's well known that

$$\mathbb{C}[\mathcal{M}_2^1]^G = \mathbb{C}[\mathrm{Tr}(X_1), \det(X_1)].$$

However, the matrices

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, A' = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

do not lie in the same orbit (G fixes A') and we have $\mathrm{Tr}(A) = \mathrm{Tr}(A') = 0$ and $\det(A) = \det(A') = 0$.

If $f \in \mathbb{k}[\mathcal{V}]^G$ and $f(v) \neq f(w)$, we say that f *separates* v and w. We say that v and w are *separated by invariants* if there exists an invariant separating v and w. In case G is reductive, we have that $f(v) = f(w)$ for all $f \in \mathbb{k}[\mathcal{V}]^G$ if and only if $\overline{Gv} \cap \overline{Gw} \neq \emptyset$ where the bar denotes closure in the Zariski topology, see [3, Corollary 6.1] (note that in Example 1.2 we have $A' \in \overline{GA}$ and G is reductive). In particular, the invariants separate the orbits if G is a finite group.

One can in principle separate orbits whenever one can find an explicit generating set for $\mathbb{k}[\mathcal{V}]^G$, but this is an extremely difficult problem in general. For this reason, Derksen and Kemper introduced the following in 2002 [4, Definition 2.3.8]:

Definition 1.3: Let $S \subseteq \mathbb{k}[\mathcal{V}]^G$. We say S is a *separating set* for $\mathbb{k}[\mathcal{V}]^G$ if the following holds for all $v, w \in \mathcal{V}$:

$$s(v) = s(w) \text{ for all } s \in S \Leftrightarrow f(v) = f(w) \text{ for all } f \in \mathbb{k}[\mathcal{V}]^G.$$

Separating sets of invariants have been an area of much recent interest. In general they have nicer properties and are easier to construct than generating sets. For example, if G is a finite group acting on a vector space V, then the set of invariants of degree $\leq |G|$ is a separating set [4, Theorem 3.9.14]. This is also true for generating invariants if $\mathrm{char}(\mathbb{k}) = 0$ [5], [6] but fails for generating invariants in the modular case. Separating sets for the rings of invariants $\mathbb{k}[V]^{C_p}$, where $\mathbb{k}$ is a field of characteristic p and C_p the cyclic group of order p and V is indecomposable were constructed in [7]. Corresponding sets of generating invariants are known only when $\dim(V) \leq 10$ [8]. For the (non-reductive) linear algebraic group $\mathbb{G}_a$ of a field of characteristic zero, separating sets for $\mathbb{k}[V]^{\mathbb{G}_a}$ for arbitary indecomposable linear representations V were constructed in [9]. These results were extended to decomposable representations in [10]. Even for indecomposable representations, generating sets are known only where $\dim(V) \leq 8$ [11]. Finally, for an arbitrary (i.e. non-linear) $\mathbb{G}_a$-variety $\mathcal{V}$, the algebra of invariants $\mathbb{k}[\mathcal{V}]^{\mathbb{G}_a}$ may not be finitely generated, but it is known that there must exist a finite separating set [12] and finite separating sets have been constructed for many examples where $\mathbb{k}[\mathcal{V}]^{\mathbb{G}_a}$ is infinitely generated [13, 14].

Let S be a separating set for $\mathbb{k}[\mathcal{V}]^G$ consisting of homogeneous polynomials. The subalgebra $\mathbb{k}[S]$ of $\mathbb{k}[\mathcal{V}]^G$ generated by S is called a *separating algebra*. By [15, Proposition 3.2.3], the quotient fields of $\mathbb{k}[S]$ and $\mathbb{k}[\mathcal{V}]^G$ have the same transcendence degree over $\mathbb{k}$. Then by [16, Proposition 2.3(b)], we get that $\dim(\mathbb{k}[S]) = \dim(\mathbb{k}[\mathcal{V}]^G)$. Consequently, the size of a separating set is bounded below by the dimension of $\mathbb{k}[\mathcal{V}]^G$. A separating set whose size equals the dimension of $\mathbb{k}[\mathcal{V}]^G$ is sometimes called a *polynomial separating set*,

n	$\dim(\mathbb{C}[\mathcal{M}_2^n]^G)$	$|S_n'|$	$|S_n|$	Lower bound	Upper bound
2	5	5	5	5	11
3	9	10	10	10	19
4	13	18	18	15	27
5	17	27	30	20	35
6	21	37	47	25	43
7	25	48	70	30	51
8	29	60	100	35	59

because it necessarily generates a polynomial subalgebra of $\mathbb{k}[\mathcal{V}]^G$. On the other hand, there always exists a separating set of size $\leq 2\dim(\mathbb{k}[\mathcal{V}]^G) + 1$, albeit such a separating set may necessarily contain non-homogeneous polynomials; see [17, Theorem 5.3] for a proof.

1.3. Statement of results

We return to the notation of Section 1.1. Recently, Kaygorodov et al. [18] showed that S_n is a minimal separating set for $\mathbb{C}[\mathcal{M}_2^n]^G$ by inclusion , i.e. no proper subset of S_n is a separating set. (The authors also considered the problem over fields of finite characteristic, but we will not). Note that this does not necessarily mean that S_n has minimal cardinality as a separating set. Our main results are as follows:

Theorem 1.4: *Let $n \geq 2$ and suppose that $S \subseteq \mathbb{C}[\mathcal{M}_2^n]^G$ is a separating set. Then $|S| \geq 5n - 5$.*

We will see in Section 2 that $\dim(\mathbb{C}[\mathcal{M}_2^n]^G) = 4n - 3$ for $n \geq 2$, and that $\dim(\mathbb{C}[\mathcal{M}_2]^G = 1)$. Thus the previous theorem implies

Corollary 1.5: *Let $n \geq 3$. Then there does not exist a polynomial separating set for $\mathbb{C}[\mathcal{M}_2^n]^G$.*

The cardinality of S_n is $\frac{1}{6}(n^3 + 11n)$. For $n \geq 7$ this exceeds the upper bound $2\dim(\mathbb{C}[\mathcal{M}_2^n]^G) + 1 = 8n - 5$. So S_n does not have minimal cardinality for $n \geq 7$. We also prove

Theorem 1.6: *Let $n \geq 3$. Then there exists a separating set, S_n' for $\mathbb{C}[\mathcal{M}_2^n]^G$ with cardinality $\frac{1}{2}(n^2 + 9n - 16)$. S_n' consists of homogeneous polynomials.*

The following table compares our lower bound $5n-5$ with the dimension of $\mathbb{C}[\mathcal{M}_2^n]^G$ and the sizes of S_n' and S_n and the known upper bound $8n-5$ for small values of n:

In particular, our results imply that S_3 is indeed a separating set of minimal cardinality, but that S_4 may not be so, and S_n for $n \geq 5$ is not. Note, however, that our separating set S_n' may not have minimum cardinality for $n \geq 4$ either and certainly does not have minimum cardinality for $n \geq 8$.

1.4. Structure of the paper

This paper is organized as follows. In Section 2, we define the separating variety for the action of a linear algebraic group on an affine variety. We explain how the geometry of the

separating variety places obstructions on the existence of small separating sets, using ideas found primarily in the work of Dufresne and others [14, 19, 20]. In Section 3, we gather the results we need on matrix invariants and compute a decomposition of the separating variety for 2×2 matrix invariants into irreducible components. We then compute the dimension of these components and prove our main results on lower bounds. In Section 4, we show how to construct the smaller separating sets S_n'. In Section 5, we prove similar results for the algebra of matrix semi-invariants.

2. Invariants of algebraic groups and the separating variety

In this section, we return to the situation and notation of Section 1.2. We note that G also acts (by the same formula (2)) on the field $\Bbbk(\mathcal{V})$ of rational functions $\mathcal{V} \to \Bbbk$. We denote the field of rational functions invariant under this action by $\Bbbk(\mathcal{V})^G$.

The following is a well-known consequence of a theorem of Rosenlicht: see [21, Corollary of Lemma 2.4] for a modern proof.

Proposition 2.1: *In the above setting, we have*

$$\operatorname{trdeg}_{\Bbbk}(\Bbbk(\mathcal{V})^G) = \dim(\mathcal{V}) - \dim(G) + \min_{v \in \mathcal{V}} \dim(G_v),$$

where G_v denotes the stabilizer of a point $v \in \mathcal{V}$.

The following is also well known. For lack of a reference, we provide a proof:

Proposition 2.2: *Suppose there exists no non-trivial character $G \to \Bbbk^*$. Then*

$$\operatorname{Quot}(\Bbbk[\mathcal{V}]^G) = \Bbbk(\mathcal{V})^G.$$

Proof: It is clear that the right-hand side contains the left. So let $\frac{f_1}{f_2} \in \Bbbk(\mathcal{V})^G$. We may assume f_1 and f_2 are coprime in $\Bbbk[\mathcal{V}]$. Now for any $g \in G$ we have

$$\frac{f_1}{f_2} = \frac{g \cdot f_1}{g \cdot f_2}.$$

Then since f_1 and f_2 are coprime and the action of G preserves degree, we must have

$$g \cdot f_1 = \lambda_g f_1, g \cdot f_2 = \lambda_g f_2$$

for some constant $\lambda_g \in \Bbbk$. Moreover, one sees easily that the assignment $g \to \lambda_g$ is a homomorphism $G \to \Bbbk^*$. Since there exists no non-trivial character $G \to \Bbbk^*$ we get that $f_1, f_2 \in \Bbbk[\mathcal{V}]^G$ as required. ∎

Corollary 2.3: *Suppose there exists no non-trivial character $G \to \Bbbk^*$. Then*

$$\dim(\Bbbk[\mathcal{V}]^G) = \dim(\mathcal{V}) - \dim(G) + \min_{v \in \mathcal{V}} \dim(G_v).$$

We note that this applies in particular when $G = \mathrm{SL}_2(\mathbb{C})$.

The main tool in our proofs will be the separating variety. This was introduced by Kemper in [22]:

Definition 2.4:

$$\mathcal{S}_{G,\mathcal{V}} = \{(v,w) \in \mathcal{V}^2 : f(v) = f(w) \text{ for all } f \in \Bbbk[\mathcal{V}]^G\}.$$

In other words, the separating variety is the subvariety of $\mathcal{V}^2$ consisting of pairs of points which are not separated by any invariant.

We define $I_{G,\mathcal{V}}$ to be the ideal of $\Bbbk[\mathcal{V}^2]$ consisting of the polynomial functions which vanish on $\mathcal{S}_{G,\mathcal{V}}$. Clearly this is a radical ideal. Then a separating set can be characterized as a subset $S \subseteq \Bbbk[\mathcal{V}]^G$ which cuts out the separating variety in $\mathcal{V}^2$, in other words (see [19, Theorem 2.1])

Proposition 2.5: $S \subseteq \Bbbk[\mathcal{V}]^G$ *is a separating set if and only if*

$$V_{\mathcal{V}^2}(\delta(S)) = \mathcal{S}_{G,\mathcal{V}}.$$

where $\delta : \Bbbk[\mathcal{V}] \to \Bbbk[\mathcal{V}^2] = \Bbbk[\mathcal{V}] \otimes \Bbbk[\mathcal{V}]$ is defined by

$$\delta(f) = 1 \otimes f - f \otimes 1.$$

Equivalently, via the Nullstellensatz, S is a separating set if and only if

$$\sqrt{(\delta(f) : f \in S)} = I_{G,\mathcal{V}}.$$

Consequently the size of a separating set for $\mathcal{V}$ is bounded below by the minimum number of generators of $I_{G,\mathcal{V}}$ up to radical, that is, the minimum number of elements generating any ideal whose radical is $I_{G,\mathcal{V}}$ (this is sometimes called the *arithmetic rank* of $I_{G,\mathcal{V}}$). We then find, using Krull's height theorem (see, e.g. [23, Theorem 10.2]) that :

Proposition 2.6: *Let* $S \subseteq \Bbbk[\mathcal{V}]^G$ *by a separating set. Then* $|S| \geq \mathrm{codim}_{\mathcal{V}^2}(\mathcal{C})$ *for all irreducible components* $\mathcal{C}$ *of* $\mathcal{S}_{G,\mathcal{V}}$.

Therefore, to use Proposition 2.6 to find lower bounds for separating sets, we must decompose $\mathcal{S}_{G,\mathcal{V}}$ into irreducible components. As a first step, we observe that the separating variety contains the following subvariety, which we call the *graph* of the action:

Definition 2.7:

$$\Gamma_{G,\mathcal{V}} = \{(v, gv) : v \in \mathcal{V}, g \in G\}.$$

If G is connected and reductive, then $\overline{\Gamma_{G,\mathcal{V}}}$ is an irreducible component of $\mathcal{S}_{G,\mathcal{V}}$. Its dimension is easily seen to equal $\dim(\mathcal{V}) + \dim(G) - \min\{\dim(G_v) : v \in \mathcal{V}\}$, and we note that in case there is no nontrivial character $G \to \mathbb{C}^*$ that

$$\dim \overline{(\Gamma_{G,\mathcal{V}})} = 2\dim(\mathcal{V}) - \dim(\Bbbk[\mathcal{V}]^G). \tag{3}$$

However, the separating variety may have extra components and some of these may have smaller dimension. These components are an obstruction to the existence of small separating sets.

Stronger obstructions may be obtained by taking a closer look at the geometry of $\mathcal{S}_{G,\mathcal{V}}$. Recall that a Noetherian topological space $\mathcal{V}$ is said to be *connected in dimension k* if the following holds: for each closed subvariety $Z \subseteq \mathcal{V}$ with dimension $< k$, the complement $\mathcal{V} \setminus Z$ is connected. If the same holds for all $Z \subseteq \mathcal{V}$ with $\text{codim}_{\mathcal{V}}(Z) > k$, we say that $\mathcal{V}$ is *connected in codimension k*. Note that if $\mathcal{V}$ is equidimensional, or all irreducible components of $\mathcal{V}$ intersect nontrivially then we have $\dim(Z) = \dim(\mathcal{V}) - \text{codim}_{\mathcal{V}}(Z)$; consequently $\mathcal{V}$ is connected in dimension k if and only if it is connected in codimension $\dim(\mathcal{V}) - k$.

Now we recall Grothendieck's connectedness theorem (see [24, Exposé XIII, Theorem 2.1]): suppose $(R, \mathfrak{m})$ is a complete local ring of dimension n such that $\text{Spec}(R)$ is connected in dimension $k < n$, and let $f_1, f_2, \ldots, f_r \in \mathfrak{m}$. Then $\text{Spec}(R/(f_1, f_2, \ldots, f_r))$ is connected in dimension $k-r$.

The idea is to apply this to $\mathcal{V}^2 = \text{Spec}(\mathbb{k}[\mathcal{V}^2])$. Of course, $\mathbb{k}[\mathcal{V}^2]$ is graded-local but not a complete ring, but we can bring the connectedness back from that of the completion $\text{Spec}(\widehat{\mathbb{k}[\mathcal{V}^2]})$ using some ideas of Reimers [25] to obtain the following:

Proposition 2.8: *Suppose $\mathcal{S}_{G,\mathcal{V}}$ is not connected in codimension k, and let $S \subseteq \mathbb{k}[\mathcal{V}]^G$ be a separating set. Suppose further that all irreducible components of $\mathcal{S}_{G,\mathcal{V}}$ intersect nontrivially, and that there does not exist a non-trivial character $G \to \mathbb{k}^*$. Then $|S| \geq \dim(\mathbb{k}[\mathcal{V}]^G) + k$.*

Proof: Set $R = \mathbb{k}[\mathcal{V}^2]$. Let $S \subset \mathbb{k}[\mathcal{V}]^G$ be a separating set of size r and let $J = (\delta(f) : f \in S)R$. By Proposition 2.5, $\mathcal{S}_{G,\mathcal{V}} = \text{Spec}(R/J)$.

Now let $\mathfrak{m}$ be the maximal ideal of R and let $\widehat{R}$ denote the $\mathfrak{m}$-adic completion of R. As $\mathcal{V}^2$ is normal, we have that $\text{Spec}(\widehat{R})$ is irreducible, and hence connected in dimension d for all $d \leq \dim(\text{Spec}(\widehat{R})) = 2n$. Applying the connectedness theorem with $d = 2n-1$ shows that $\text{Spec}(\widehat{R}/J\widehat{R})$ is connected in dimension $2n-1-r$.

Since $\widehat{R}/J\widehat{R}$ is also the completion of R/J at the maximal ideal $\mathfrak{m}/J$, it follows from the proof of [25, Lemma 4.3] that $\text{Spec}((R/J)_{\mathfrak{m}/J})$ is connected in dimension $2n-1-r$, and from [25, Proposition 4.4] that $\text{Spec}(R/J) = \mathcal{S}_{G,\mathcal{V}}$ is connected in dimension $2n-1-r$ too. Further since

$$\dim(\mathcal{S}_{G,\mathcal{V}}) \geq \dim(\overline{\Gamma_{G,\mathcal{V}}}) = 2n - \dim(\mathbb{k}[\mathcal{V}]^G)$$

and all irreducible components intersect nontrivially we get that $\mathcal{S}_{G,V}$ is connected in codimension $1 + r - \dim(\mathbb{k}[\mathcal{V}]^G)$. Since $\mathcal{S}_{G,\mathcal{V}}$ is not connected in codimension k we must have that

$$k < 1 + r - \dim(\mathbb{k}[\mathcal{V}]^G),$$

i.e. that $r \geq \dim(\mathbb{k}[\mathcal{V}]^G) + k$ as required. ∎

3. Invariants of 2×2 matrices

We begin this section by fixing some notation and simplifying our problem as much as possible. As we will be considering only 2×2 matrices, we drop some subscripts, writing $\mathcal{M} = \mathcal{M}_2$, etc. Observe that the action of $\text{GL}_2(\mathbb{C})$ on $\mathcal{M}^n$ is not faithful – the kernel is the subgroup of scalar matrices. Therefore we have a faithful action of $\text{SL}_2(\mathbb{C})$ on $\mathcal{M}^n$ and $\mathbb{C}[\mathcal{M}^n]^{\text{GL}_2(\mathbb{C})} = \mathbb{C}[\mathcal{M}^n]^{\text{SL}_2(\mathbb{C})}$. Since it is enough to study this action, we write $G := \text{SL}_2(\mathbb{C})$ from now on.

We fix the notation for some subgroups of G: the torus

$$T := \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} : t \in \mathbb{C}^* \right\},$$

the unipotent subgroup

$$U := \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} : u \in \mathbb{C} \right\},$$

and the Borel subgroup

$$B := \left\{ \begin{pmatrix} t & u \\ 0 & t^{-1} \end{pmatrix} : t \in \mathbb{C}^*, u \in \mathbb{C} \right\}.$$

Next observe that $\mathcal{M}$ is not an indecomposable representation of G, we have

$$\mathcal{M} \cong \mathcal{V} \oplus \mathbb{C}I$$

where $\mathcal{V}$ denotes the set of trace-zero matrices in $\mathcal{M}$, I the 2×2 identity matrix and G acts trivially on $\mathbb{C}I$. It is now easy to see that

$$\mathbb{C}[\mathcal{M}^n]^G = \mathbb{C}[\mathcal{V}^n]^G \otimes \mathbb{C}[\text{Tr}(X_i) : i = 1, \ldots, n].$$

Note also that $\mathcal{V}$ is fixed by the commuting action of GL_n on $\mathcal{M}$ as defined in (1).

A generic element $\mathbf{A} \in \mathcal{V}^n$ will be written as $(A_1, A_2, \ldots, A_n)$ where

$$A_i = \begin{pmatrix} b_i & c_i \\ a_i & -b_i \end{pmatrix}.$$

A generic element $(\mathbf{A}, \mathbf{A}') \in \mathcal{V}^n \times \mathcal{V}^n$ will be written with $\mathbf{A}$ as above and $\mathbf{A}' = (A_1', A_2', \ldots, A_n')$ where

$$A_i' = \begin{pmatrix} b_i' & c_i' \\ a_i' & -b_i' \end{pmatrix}.$$

Throughout we write $g \cdot \mathbf{A}$ for the conjugation action of $g \in \text{SL}_2$ on $\mathbf{A} \in \mathcal{M}$. We use the notation $h \star \mathbf{A}$ for the commuting action of $h \in \text{GL}_n$.

From this point onwards, X_i etc. represent generic trace-zero matrices of coordinate functions on $\mathcal{V}$. It is now easy to see that $\text{Tr}(X_i^2) = -2 \det(X_i)$. Consequently, Proposition 1.1 implies:

Proposition 3.1: *The following set E_n of invariants minimally generates $\mathbb{C}[\mathcal{V}^n]^G$ as an algebra:*

- $t_{ij} := \text{Tr}(X_i X_j), 1 \leq i \leq j \leq n.$
- $t_{ijk} := \text{Tr}(X_i X_j X_k), 1 \leq i < j < k \leq n.$

We note for future reference that

$$t_{ijk} = \begin{vmatrix} c_i & c_j & c_k \\ b_i & b_j & b_k \\ a_i & a_j & a_k \end{vmatrix}. \tag{4}$$

This implies that $t_{ijk} = \text{sgn}(\sigma) t_{\sigma(i)\sigma(j)\sigma(k)}$ for any permutation σ of i, j, k, and that $t_{iij} = 0$ for all i, j, etc.

The dimension of $\mathbb{C}[\mathcal{V}^n]^G$ is $3n-3$ for $n \geq 2$. To see this note that there exists a trace-free n-matrix $\mathbf{A}$ whose stabilizer is the finite group $\pm I$: take

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, A_i = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

for $i \geq 2$. The result now follows from Corollary 2.3. Note that this also implies that $\dim(\mathbb{C}[\mathcal{M}^n]^G) = 4n - 3$ for $n \geq 2$ as stated in the introduction.

The discussion above shows that our main results for $\mathbb{C}[\mathcal{M}^n]^G$ are equivalent to the following:

Proposition 3.2: *Let $n \geq 2$ and suppose that $S \subseteq \mathbb{C}[\mathcal{V}^n]^G$ is a separating set. Then $|S| \geq 4n - 5$.*

Proposition 3.3: *Let $n \geq 3$. Then there exists a separating set $S' \subseteq \mathbb{C}[\mathcal{V}^n]^G$ with cardinality $\frac{1}{2}(n^2 + 7n - 16)$.*

We will need to consider certain subspaces of $\mathcal{V}$: let $\mathcal{W}$ denote the B-subspace of upper triangular matrices in $\mathcal{V}$. Further, define

$$\mathcal{C} := \{(\mathbf{A}, \mathbf{A}') \in \mathcal{W}^n \times \mathcal{W}^n : b_i = b_i' \text{ for all } i = 1, \ldots, n\},$$
$$\mathcal{C}' := \{(\mathbf{A}, \mathbf{A}') \in \mathcal{W}^n \times \mathcal{W}^n : b_i = -b_i' \text{ for all } i = 1, \ldots, n\},$$
$$\mathcal{C}_0 := \{(\mathbf{A}, \mathbf{A}') \in \mathcal{W}^n \times \mathcal{W}^n : b_i = b_i' = 0 \text{ for all } i = 1, \ldots, n\}.$$

The above are subspaces of $\mathcal{V}^n \times \mathcal{V}^n$, which are fixed under the diagonal action of GL_n. Since the action commutes with the conjugation action of G, the same is true of the orbit subsets $(G \times G) \cdot \mathcal{C}$, $(G \times G) \cdot \mathcal{C}'$ and $(G \times G) \cdot \mathcal{C}_0$.

Note that $U \cong \mathbb{G}_a(\mathbb{C})$, the additive group of $\mathbb{C}$. The linear representation theory of this group is well known: each indecomposable module is isomorphic to $S^n(V)$, where V is the restriction of the natural two-dimensional $\mathbb{C}G$-module, and S^n represents symmetric powers. One usually studies the so-called 'basic' $\mathbb{G}_a$-actions: these are the $\mathbb{G}_a(\mathbb{C})$-modules

$$V_i := \langle v_0, v_1, \ldots, v_i \rangle : i \in \mathbb{N}$$

on which $u \in \mathbb{C}$ acts via the formula

$$u \bullet v_i = \sum_{j=0}^{i} \frac{u^j}{j!} v_{i-j}$$

and it can be shown that $V_i \cong S^i(V)$. In our case, a direct calculation shows that $\mathcal{V} \cong V_2$ as a U-module.

The separating variety for arbitrary linear representations of $\mathbb{G}_a(\mathbb{C})$ was considered by Dufresne and Kraft: in our case we have $\mathcal{V}^n \cong V_2^{\oplus n}$ as U-modules, and from a careful reading of [26, Theorem 7.5, Lemma 7.6] we obtain:

Proposition 3.4: *(i) We have $\mathcal{S}_{U,\mathcal{V}^n} = \overline{\Gamma_{U,\mathcal{V}^n}} \cup \mathcal{C}$.*
(ii) $\overline{\Gamma_{U,\mathcal{V}^n}} = \Gamma_{U,\mathcal{V}^n} \cup \mathcal{C}'$.

In particular, $\mathcal{C}_0 \subset \overline{\Gamma_{U,\mathcal{V}^n}}$.

Note also that $T \cong \mathbb{G}_m(\mathbb{C})$, the multiplicative group of $\mathbb{C}$. The representation theory of this group is very straightforward; the indecomposable modules are all one-dimensional, isomorphic to W_z for some $z \in \mathbb{Z}$ where $W_z = \langle v \rangle$ and the action of $t \in T$ is given by

$$t \bullet v = t^z v.$$

Now it's easy to see that $\mathcal{V} \cong V_0 \oplus V_0 \oplus V_2 \oplus V_{-2}$. Moreover, $\mathcal{W}$ is a direct summand of $\mathcal{V}$ isomorphic to $V_0 \oplus V_0 \oplus V_2$.

The separating variety for arbitary linear actions of algebraic tori $\mathbb{G}_m^k$ was considered by Dufresne and Jeffries. In our case, the action is particularly simple, and from careful reading of [27, Lemma 3.5], we obtain:

Proposition 3.5: *(i) We have $\mathcal{S}_{T,\mathcal{W}^n} = \mathcal{C}$.*
(ii) $(\mathbf{A}, \mathbf{A}') \in \overline{\Gamma_{T,\mathcal{W}^n}}$ if and only if $(\mathbf{A}, \mathbf{A}') \in \mathcal{C}$ and in addition $c_i c_j' = c_j c_i'$ for all $1 \leq i, j \leq n$.

Our goal in this section is to describe the separating variety $\mathcal{S}_{G,\mathcal{V}^n}$. As observed in the previous section, one irreducible component is given by the Zariski closure of the graph

$$\Gamma_{G,\mathcal{V}^n} = \{(\mathbf{A}, g \cdot \mathbf{A}) : \mathbf{A} \in \mathcal{V}^n, g \in G\}$$

but there may be more. The description of $\mathcal{S}_{G,\mathcal{V}^n}$ as the set of pairs of n-matrices whose orbit closures intersect makes it clear that the separating variety is fixed by the action of $G \times G$. It is also clear that $\Gamma_{G,\mathcal{V}^n}$ is fixed by the action of $G \times G$. The commuting action of GL_n on $\mathcal{V}^n$ induces a diagonal action on $\mathcal{V}^n \times \mathcal{V}^n$ which commutes with the action of $G \times G$. The following simple observations are crucial:

Lemma 3.6: *Suppose $(\mathbf{A}, \mathbf{A}') \in \overline{\Gamma_{G,\mathcal{V}^n}}$. Then $(h \star \mathbf{A}, h \star \mathbf{A}') \in \overline{\Gamma_{\mathcal{V}^n}}$ for all $h \in \mathrm{GL}_n$.*

Proof: Let $(\mathbf{A}, \mathbf{A}') \in \overline{\Gamma_{G,\mathcal{V}^n}}$. Then there exist morphisms $\mathbf{A} : \mathbb{C}^* \to \mathcal{V}^n, g : \mathbb{C}^* \to G$ such that

$$\mathbf{A} = \lim_{t \to 0} \mathbf{A}(t), \mathbf{A}' = \lim_{t \to 0} g(t) \cdot \mathbf{A}(t).$$

Let $h \in \mathrm{GL}_n$, then

$$h \star \mathbf{A} = \lim_{t \to 0}(h \star \mathbf{A}(t)), h \star \mathbf{A}' = \lim_{t \to 0} h \star (g(t) \cdot \mathbf{A}(t)) = . \lim_{t \to 0} g(t) \cdot (h \star \mathbf{A}(t))).$$

■

Lemma 3.7: *Let $(\mathbf{A}, \mathbf{A}') \in \mathcal{S}_{G,\mathcal{V}^n}$ and let $h \in \mathrm{GL}_n$. Then $(h \star \mathbf{A}, h \star \mathbf{A}') \in \mathcal{S}_{G,\mathcal{V}^n}$.*

Proof: The action of GL_n on $\mathcal{V}^n$ induces an action on $\mathbb{C}[\mathcal{V}^n]$: we define

$$(h \star f)(\mathbf{A}) = f(h^{-1} \star \mathbf{A})$$

for $h \in \mathrm{GL}_n, f \in \mathbb{C}[\mathcal{V}^n]$ and $\mathbf{A} \in \mathcal{V}^n$. If $f \in \mathbb{C}[\mathcal{V}^n]^G$, then so is $h \star f$ for all $h \in \mathrm{GL}_n$. Now suppose $(\mathbf{A}, \mathbf{A}') \in \mathcal{S}_{G,\mathcal{V}^n}$. Let $h \in \mathrm{GL}_n$ and $f \in \mathbb{C}[\mathcal{V}^n]^G$. Then we have

$$f(h \star \mathbf{A}) = (h^{-1} \star f)(\mathbf{A}) = (h^{-1} \star f)(\mathbf{A}') = f(h \star \mathbf{A}')$$

which shows that $(h \star \mathbf{A}, h \star \mathbf{A}') \in \mathcal{S}_{G,\mathcal{V}^n}$ as required.

■

These observations allow us to apply a sort of simultaneous column-reduction to elements of $\mathcal{C}$ and $\mathcal{C}'$. In more detail, to every pair $(\mathbf{A}, \mathbf{A}') \in \mathcal{C}$ or $\mathcal{C}'$ we assign a $3 \times n$ matrix

$$m_{\mathbf{A},\mathbf{A}'} := \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \\ c_1' & c_2' & \cdots & c_n' \end{pmatrix}. \tag{5}$$

Denote the minor of $m_{\mathbf{A},\mathbf{A}'}$ obtained by taking only the ith, jth and kth columns by $\Delta_{ijk}(\mathbf{A}, \mathbf{A}')$. Finally we define

$$\widehat{\mathcal{C}} := \{(\mathbf{A}, \mathbf{A}') \in \mathcal{C} : \mathrm{rk}(m_{\mathbf{A},\mathbf{A}'}) \leq 2\}$$

and

$$\widehat{\mathcal{C}'} := \{(\mathbf{A}, \mathbf{A}') \in \mathcal{C}' : \mathrm{rk}(m_{\mathbf{A},\mathbf{A}'}) \leq 2\}.$$

Then we have:

Lemma 3.8: *The following are equivalent:*

  (i) $\mathrm{rk}(m_{\mathbf{A},\mathbf{A}'}) \leq 2$;
  (ii) $\Delta_{ijk}(\mathbf{A}, \mathbf{A}') = 0$ *for all* $1 \leq i < j < k \leq n$;
  (iii) *There exists* $h \in \mathrm{GL}_n$ *such that* $(h \star A_i) = (h \star A_i') = 0$ *for all* $i \geq 3$.

Proof: The equivalence of (i) and (ii) is well known. Let $E_{ij}(\lambda)$ denote the elementary matrix with λ in position i, j, 1's on the diagonal and 0's elsewhere. The action of $E_{ij}(\lambda)$ on $(\mathbf{A}, \mathbf{A}')$ is to replace A_i and A_i' by $A_i + \lambda A_j$ and $A_i' + \lambda A_j'$ respectively. The effect on $m_{\mathbf{A},\mathbf{A}'}$ is to replace the ith column with the ith column plus λ times the jth column. The sequence of column operations which place $m_{\mathbf{A},\mathbf{A}'}$ in column echelon form produce $(h \star \mathbf{A}, h \star \mathbf{A}')$ of the form claimed. ∎

Now we consider the G-orbit structure of $\mathcal{V}$. The following result is key to obtaining a decomposition of the separating variety $\mathcal{S}_{G,\mathcal{V}^n}$:

Lemma 3.9: *Suppose* $\mathbf{A} \in \mathcal{V}^n \setminus G \cdot \mathcal{W}^n$. *Then* $G \cdot \mathbf{A}$ *is closed*

Proof: We use the Hilbert–Mumford criterion [28]. Let $\lambda : \mathbb{C}^* \to G$ be a one-parameter subgroup. The Hilbert–Mumford weight of $\mathbf{A}$ with respect to λ is the unique smallest integer $\mu(\mathbf{A}, \lambda)$ such that

$$\lim_{t \to 0} t^{\mu(\mathbf{A},\lambda)}(\lambda(t) \cdot \mathbf{A})$$

exists. $\mathbf{A}$ is stable (i.e. has closed orbit and finite stabilizer) if and only if $\mu(\mathbf{A}, \lambda) > 0$ for all one-parameter subgroups λ of G. Now each one-parameter subgroup of G is of the form

$$\lambda_g(t) = g \cdot \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$$

for some $g \in G$. Letting $e \in G$ denote the identity, it follows that $\mathbf{A}$ is stable if and only if $\mu(g \cdot \mathbf{A}, \lambda_e) > 0$ for all $g \in G$.

Let $g \in G$ and suppose $g \cdot \mathbf{A} \notin \mathcal{W}^n$. Writing $g \cdot \mathbf{A} = \mathbf{A}'$, we see that $a_i' \neq 0$ for some $i = 1, \ldots, n$. Therefore $\mu(g \cdot \mathbf{A}, \lambda_e) = 2 > 0$. Since g was arbitrary we conclude that $\mathbf{A}$ is stable, and in particular $G \cdot \mathbf{A}$ is closed. ∎

Remark 3.10: One can complete the analysis of orbit closures in $\mathcal{V}^n$: it turns out that $G \cdot \mathbf{A}$ is not closed if and only if $\mathbf{A} \in G \cdot \mathcal{W}^n \setminus \{\mathbf{0}\}$ where $\mathbf{0}$ represents the n-matrix consisting entirely of zero matrices. See [29, Proposition 8.9] for a proof in a more general case.

An n-matrix with all traces equal to zero belongs to $G \cdot \mathcal{W}^n$ if and only if there exists $g \in G$ such that $g \cdot A_i$ is upper triangular for all i. Such matrices may be called *simultaneously (upper) -triangularizable*. Since an matrix is upper triangularizable if and only if it is lower triangularizable via the action of

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

we usually speak simply of simultaneously triangularizable matrices.

Simultaneous triangularization of 2×2 matrices was studied by Florentino [30]. He showed that arbitrary (i.e. not trace-free) n-matrices are upper triangularizable if and only if

$$\mathrm{Tr}(A_i A_j A_k) = \mathrm{Tr}(A_k A_j A_i)$$

for all $i < j < k$ and

$$\det(A_i A_j - A_j A_i) = 0$$

for all $i < j$. But for tracefree matrices, Equation (4) implies that

$$\mathrm{Tr}(A_i A_j A_k) = -\mathrm{Tr}(A_k A_j A_i).$$

Further, for tracefree matrices we can show

$$\det(A_i A_j - A_j A_i) = 4 \det(A_i) \det(A_j) - \mathrm{Tr}(A_i A_j)^2.$$

It follows that $G \cdot \mathcal{W}^n$ is the subvariety of $\mathcal{V}^n$ cut out by the set of polynomials

$$\{t_{ijk} : 1 \leq i < j < k \leq n\} \cup \{t_{ii} t_{jj} - t_{ij}^2 : 1 \leq i < j \leq n\}.$$

In particular, this shows that $G \cdot \mathcal{W}^n$ is closed. It is also irreducible, being the orbit of a connected algebraic group on a vector space. As a first step towards a decomposition of $\mathcal{S}_{G,\mathcal{V}^n}$ we have the following.

Lemma 3.11: $\mathcal{S}_{G,\mathcal{V}} = \overline{\Gamma_{G,\mathcal{V}}} \cup ((G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,\mathcal{V}^n})$. *Moreover,* $\overline{\Gamma_{G,\mathcal{V}^n}}$ *and* $(G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,\mathcal{V}^n}$ *are closed and* $\overline{\Gamma_{G,\mathcal{V}^n}}$ *is irreducible.*

Proof: Let $(\mathbf{A}, \mathbf{A}') \in \mathcal{S}_{G,\mathcal{V}^n}$. Then $\overline{G \cdot \mathbf{A}} \cap \overline{G \cdot \mathbf{A}'} \neq \emptyset$. Unless $\mathbf{A} \in G \cdot \mathcal{W}^n$ and $\mathbf{A}' \in G \cdot \mathcal{W}^n$, then by Lemma 3.9, the orbit of either $\mathbf{A}$ or $\mathbf{A}'$ is closed and $(\mathbf{A}, \mathbf{A}') \in \overline{\Gamma_{G,\mathcal{V}^n}}$ (if both orbits are closed, $(\mathbf{A}, \mathbf{A}') \in \Gamma_{G,\mathcal{V}^n}$). This shows that $\mathcal{S}_{G,\mathcal{V}^n} \subseteq \overline{\Gamma_{G,\mathcal{V}^n}} \cup ((G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,\mathcal{V}^n})$. Clearly $\overline{\Gamma_{G,\mathcal{V}^n}}$ is closed and irreducible. $(G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,\mathcal{V}^n}$ is closed as it is the intersection of two closed sets. ∎

The following Lemma describes $(G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,\mathcal{V}^n}$ as a union of sets. Note that at this stage we do not know whether $(G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,\mathcal{V}^n}$ is irreducible, as the sets on the right hand side may not themselves be closed.

Lemma 3.12: *We have*

$$(G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,\mathcal{V}^n} = (G \times G) \cdot \mathcal{C} \cup (G \times G) \cdot \mathcal{C}'.$$

Proof: Suppose $(\mathbf{A}, \mathbf{A}') \in (\mathcal{W}^n \times \mathcal{W}^n)$. Then since $\det(A_i) = \det(A_i')$ for all i we get $b_i = \pm b_i'$. Further, since for each $i \neq j$

$$2b_i b_j = \mathrm{Tr}(A_i A_j) = \mathrm{Tr}(A_i' A_j') = 2b_i' b_j' \tag{6}$$

we have that $b_i = b_i'$ for each i or $b_i = -b_i'$ for each i. This shows that $(\mathbf{A}, \mathbf{A}') \in \mathcal{C} \cup \mathcal{C}'$. Since $(\mathbf{A}, \mathbf{A}') \in \mathcal{S}_{G,\mathcal{V}^n}$ if and only $(g \cdot \mathbf{A}, g' \cdot \mathbf{A}') \in \mathcal{S}_{G,\mathcal{V}^n}$ for all $g, g' \in G$ we get that

$$(G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,V} = (G \times G) \cdot \mathcal{C} \cup (G \times G) \cdot \mathcal{C}'$$

as required. ∎

Lemma 3.13: *For all $n \geq 2$ we have $(G \times G) \cdot \mathcal{C}' \subseteq \overline{\Gamma_{G,\mathcal{V}^n}}$.*

Proof: As $\overline{\Gamma_{G,\mathcal{V}^n}}$ is stabilized by the action of $G \times G$, it is enough to show that $\mathcal{C}' \subseteq \overline{\Gamma_{G,\mathcal{V}^n}}$, and this follows from Proposition 3.4 (ii): we have

$$\mathcal{C}' \subseteq \overline{\Gamma_{U,\mathcal{V}^n}} \subseteq \overline{\Gamma_{G,\mathcal{V}^n}}$$

as required. ∎

Combining Lemmas 3.11–3.13 we obtain a decomposition

$$\mathcal{S}_{G,\mathcal{V}^n} = \overline{\Gamma_{G,\mathcal{V}^n}} \cup \overline{(G \times G) \cdot \mathcal{C}}. \tag{7}$$

Note that the stabilizer of the action of $G \times G$ on $\mathcal{C}$ is $B \times B$, so the dimension of $\overline{(G \times G) \cdot \mathcal{C}}$ is

$$\dim(\mathcal{C}) + 2\dim(G) - 2\dim(B) = 3n + 2.$$

By Equation (3), the dimension of $\overline{\Gamma_{G,\mathcal{V}^n}}$ is

$$\dim(\mathcal{V}^n) + \dim(G) = 3n + 3.$$

So there are two possibilities: either $\overline{(G \times G) \cdot \mathcal{C}} \subseteq \overline{\Gamma_{G,\mathcal{V}^n}}$ and hence $\mathcal{S}_{G,\mathcal{V}^n}$ has a single irreducible component, or else $\mathcal{S}_{G,\mathcal{V}^n}$ has two irreducible components of different dimensions.

The following result is key in our proof of Proposition 3.2.

Proposition 3.14: *For $n \geq 2$ we have $(G \times G) \cdot \mathcal{C} \cap \overline{\Gamma_{G,\mathcal{V}^n}} = (G \times G) \cdot \widehat{\mathcal{C}}$.*

Note that for $n = 2$ this implies that $(G \times G) \cdot \mathcal{C} \subseteq \overline{\Gamma_{G,\mathcal{V}^n}}$ and hence $\overline{(G \times G) \cdot \mathcal{C}} \subseteq \overline{\Gamma_{G,\mathcal{V}^n}}$, since $\widehat{\mathcal{C}} = \mathcal{C}$. Therefore it follows that $\mathcal{S}_{G,\mathcal{V}^2}$ is irreducible.

Proof: We begin by showing that $(G \times G) \cdot \widehat{\mathcal{C}} \subseteq (G \times G) \cdot \mathcal{C} \cap \overline{\Gamma_{G,\mathcal{V}^n}}$. It is clear that $(G \times G) \cdot \widehat{\mathcal{C}} \subseteq (G \times G) \cdot \mathcal{C}$ and since $\overline{\Gamma_{G,\mathcal{V}^n}}$ is fixed by the action of $G \times G$ it is enough to show that $\widehat{\mathcal{C}} \subseteq \overline{\Gamma_{G,\mathcal{V}^n}}$.

Let $(\mathbf{A}, \mathbf{A}') \in \widehat{\mathcal{C}}$. By Lemma 3.6, it is enough to show that there exists $h \in \mathrm{GL}_n$ with $(h \star \mathbf{A}, h \star \mathbf{A}') \in \overline{\Gamma_{G,\mathcal{V}^n}}$. Therefore by Lemma 3.8 we may assume $A_i = A'_i = 0$ for $i \geq 3$.

Suppose that there exists i such that $b_i = b'_i \neq 0$, without loss of generality $i = 1$. Set

$$g := \begin{pmatrix} 1 & \frac{-c_1}{2b_1} \\ 0 & 1 \end{pmatrix}, g' := \begin{pmatrix} 1 & \frac{-c'_1}{2b_1} \\ 0 & 1 \end{pmatrix}. \tag{8}$$

Then

$$g \cdot A_1 = g' \cdot A'_1 = \begin{pmatrix} b_1 & 0 \\ 0 & -b_1 \end{pmatrix},$$

and $(g \cdot A_2, g' \cdot A'_2)$ are upper triangular with equal diagonal entries. By Proposition 3.5,

$$(g \cdot \mathbf{A}, g \cdot \mathbf{A}') \in \overline{\Gamma_{T,\mathcal{W}^n}} \subseteq \overline{\Gamma_{G,\mathcal{V}^n}}.$$

Therefore $(\mathbf{A}, \mathbf{A}') \in \overline{\Gamma_{G,\mathcal{V}^n}}$ as required.

Hence we may assume $b_i = b'_i = 0$ for $i = 1, 2$. But in that case

$$(\mathbf{A}, \mathbf{A}') \in \mathcal{C}_0 \subseteq \overline{\Gamma_{U,\mathcal{V}^n}} \subseteq \overline{\Gamma_{G,\mathcal{V}^n}}$$

where the first inclusion comes from Proposition 3.4.

To prove the converse it is enough to show that $\mathcal{C} \cap \overline{\Gamma_{G,\mathcal{V}^n}} \subseteq \widehat{\mathcal{C}}$. So, let $(\mathbf{A}, \mathbf{A}') \in \mathcal{C} \cap \overline{\Gamma_{G,\mathcal{V}^n}}$. Thus there exist morphisms $g : \mathbb{C}^* \to G$, and $\mathbf{A} : \mathbb{C}^* \to \mathcal{V}^n$ such that

$$\lim_{t \to 0} \mathbf{A}(t) = \mathbf{A}, \lim_{t \to 0}(g(t) \cdot \mathbf{A}(t)) = \mathbf{A}',$$

where we abuse notation by using $\mathbf{A}$ for a function and its limit. Also let $\mathbf{A}'(t) := (g(t) \cdot \mathbf{A}(t))$ for all $t \in \mathbb{C}^*$. Note that although $a_i = a'_i = 0$ for all i and $b_i = b'_i$ we do not have $a_i(t) = a'_i(t) = 0$ or $b_i(t) = b'_i(t)$ for all t in general. Write

$$g(t) = \begin{pmatrix} w(t) & x(t) \\ y(t) & z(t) \end{pmatrix}.$$

Let $1 \leq i < j < k \leq n$. Write $\mathbf{a}(t), \mathbf{b}(t), \mathbf{c}(t)$ and $\mathbf{c}'(t)$ for the row vectors $(a_i(t), a_j(t), a_k(t)), (b_i(t), b_j(t), b_k(t)), (c_i(t), c_j(t), c_k(t))$ and $(c'_i(t), c'_j(t), c'_k(t))$ respectively with analogous notation for their limits, and consider

$$\Delta_{ijk}(\mathbf{A}, \mathbf{A}') = \begin{vmatrix} \mathbf{b} \\ \mathbf{c} \\ \mathbf{c}' \end{vmatrix}.$$

On the one hand this is

$$\lim_{t \to 0} \begin{vmatrix} \mathbf{b}(t) \\ \mathbf{c}(t) \\ \mathbf{c}'(t) \end{vmatrix}$$

$$= \lim_{t \to 0} \begin{vmatrix} \mathbf{b}(t) \\ \mathbf{c}(t) \\ 2x(t)z(t)\mathbf{b}(t) - x(t)^2\mathbf{a}(t) + z(t)^2\mathbf{c}(t) \end{vmatrix}$$

$$= -\lim_{t \to 0} x(t)^2 \begin{vmatrix} \mathbf{b}(t) \\ \mathbf{c}(t) \\ \mathbf{a}(t) \end{vmatrix}.$$

using row operations and the facts that $\mathbf{b}(t) \to \mathbf{b}$, $\mathbf{c}(t) \to \mathbf{c}$, $\mathbf{c}'(t) \to \mathbf{c}'$ as $t \to 0$. But we also have $\mathbf{b}'(t) \to \mathbf{b}$, so that

$$\Delta_{ijk}(\mathbf{A}, \mathbf{A}') = \lim_{t \to 0} \begin{vmatrix} \mathbf{b}'(t) \\ \mathbf{c}(t) \\ \mathbf{c}'(t) \end{vmatrix}$$

$$= \lim_{t \to 0} \begin{vmatrix} 2x(t)y(t)\mathbf{b}(t) - w(t)x(t)\mathbf{a}(t) + y(t)z(t)\mathbf{c}(t) \\ \mathbf{c}(t) \\ 2x(t)z(t)\mathbf{b}(t) - x(t)^2\mathbf{a}(t) + z(t)^2\mathbf{c}(t) \end{vmatrix}$$

$$= \lim_{t \to 0} \begin{vmatrix} 2x(t)y(t)\mathbf{b}(t) - w(t)x(t)\mathbf{a}(t) \\ \mathbf{c}(t) \\ 2z(t)\mathbf{b}(t)x(t) - x(t)^2\mathbf{a}(t) \end{vmatrix}.$$

Noting that $w(t)z(t) - x(t)y(t) = 1$ for all $t \in \mathbb{C}^*$, this is equal to

$$\lim_{t \to 0} \begin{vmatrix} 2(w(t)z(t) - 1)\mathbf{b}(t) - w(t)x(t)\mathbf{a}(t) \\ \mathbf{c}(t) \\ 2z(t)\mathbf{b}(t)x(t) - x(t)^2\mathbf{a}(t) \end{vmatrix}$$

$$= \lim_{t \to 0} x(t) \begin{vmatrix} 2(w(t)z(t) - 1)\mathbf{b}(t) - w(t)x(t)\mathbf{a}(t) \\ \mathbf{c}(t) \\ 2z(t)\mathbf{b}(t) - x(t)\mathbf{a}(t) \end{vmatrix}$$

$$= \lim_{t \to 0} x(t) \begin{vmatrix} w(t)(2z(t)\mathbf{b}(t) - x(t)\mathbf{a}(t)) - 2\mathbf{b}(t) \\ \mathbf{c}(t) \\ 2z(t)\mathbf{b}(t) - x(t)\mathbf{a}(t) \end{vmatrix}$$

$$= \lim_{t \to 0} x(t) \begin{vmatrix} -2\mathbf{b}(t) \\ \mathbf{c}(t) \\ 2z(t)\mathbf{b}(t) - x(t)\mathbf{a}(t) \end{vmatrix}$$

$$= \lim_{t \to 0} 2x(t)^2 \begin{vmatrix} \mathbf{b}(t) \\ \mathbf{c}(t) \\ \mathbf{a}(t) \end{vmatrix}$$

This shows that $\Delta_{ijk}(\mathbf{A}, \mathbf{A}') = 0$ as required, and therefore $(\mathbf{A}, \mathbf{A}') \in \widehat{\mathcal{C}}$. ∎

Example 3.15: Let $n \geq 3$ and define a pair of n-matrices:

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

and

$$A_1' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, A_2' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, A_3' = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

with $A_i = A_i' = 0$ for all $i > 3$. Then $\mathrm{rk}(m_{\mathbf{A},\mathbf{A}'}) = 3$, and so Proposition 3.14 above shows that $(\mathbf{A}, \mathbf{A}') \in \overline{(G \times G) \cdot \mathcal{C}} \setminus \overline{\Gamma_{G,\mathcal{V}^n}}$. Thus, for $n \geq 3$, $\mathcal{S}_{G,\mathcal{V}^n}$ has two irreducible components.

We obtain the following immediate Corollary, from which Corollary 1.5 also follows:

Corollary 3.16: *Let $n \geq 3$ and suppose $S \subseteq \mathbb{C}[\mathcal{V}^n]^G$ is a separating set. Then $|S| \geq 3n - 2$.*

Proof: For $n \geq 3$ we have shown that $\mathcal{S}_{G,\mathcal{V}^n}$ has two irreducible components. The component $\overline{\Gamma_{G,\mathcal{V}^n}}$ has dimension $3n + 3$, i.e. codimension $3n-3$ in $\mathcal{V}^n \times \mathcal{V}^n$, while $(G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,\mathcal{V}^n}$ has dimension $3n + 2$, i.e. codimension $3n-2$ in $\mathcal{V}^n \times \mathcal{V}^n$. The result now follows from Proposition 2.6. ∎

To obtain the stronger bound in Proposition 3.2, we need to compute the dimension of $\overline{(G \times G) \cdot \mathcal{C}} \cap \overline{\Gamma_{G,\mathcal{V}^n}}$. We are not able to find a complete description of $\overline{(G \times G) \cdot \mathcal{C}}$; but for our purposes the following is enough.

Lemma 3.17:

$$\overline{(G \times G) \cdot \mathcal{C}} \subseteq (G \times G) \cdot \mathcal{C} \cup (G \times G) \cdot \widehat{\mathcal{C}'}.$$

Proof: Suppose $(\mathbf{A}, \mathbf{A}') \in \overline{(G \times G) \cdot \mathcal{C}} \setminus (G \times G) \cdot \mathcal{C}$. As $(G \times G) \cdot \mathcal{C} \subseteq (G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,\mathcal{V}^n}$ and the latter is closed, we have

$$(\mathbf{A}, \mathbf{A}') \in \overline{(G \times G) \cdot \mathcal{C}} \subseteq (G \cdot \mathcal{W}^n \times G \cdot \mathcal{W}^n) \cap \mathcal{S}_{G,\mathcal{V}^n} = (G \times G) \cdot \mathcal{C} \cup (G \times G) \cdot \mathcal{C}',$$

with the final equality coming from Lemma 3.12. Therefore $(\mathbf{A}, \mathbf{A}') \in (G \times G) \cdot \mathcal{C}'$. Since $(G \times G) \cdot \mathcal{C}, \overline{(G \times G) \cdot \mathcal{C}}$ and $(G \times G) \cdot \mathcal{C}'$ are all fixed by the action of $(G \times G)$, it is enough to show that

$$\mathcal{C}' \cap \overline{(G \times G) \cdot \mathcal{C}} \subseteq \widehat{\mathcal{C}'}.$$

So, suppose $(\mathbf{A}, \mathbf{A}') \in \overline{(G \times G) \cdot \mathcal{C}} \cap \mathcal{C}'$; we aim to show that $\mathrm{rk}(m_{\mathbf{A},\mathbf{A}'}) \leq 2$.

Let $1 \leq i < j < k \leq n$, and write $\mathbf{b}, \mathbf{c}$ and $\mathbf{c}'$ for the row vectors (b_i, b_j, b_k), (c_i, c_j, c_k) and (c_i', c_j', c_k') respectively. Since $(\mathbf{A}, \mathbf{A}') \in \overline{(G \times G) \cdot \mathcal{C}}$, there exist morphisms $g, g' : \mathbb{C}^* \to G$, and $\mathbf{Z}, \mathbf{Z}' : \mathbb{C}^* \to \mathcal{C}$ such that

$$\lim_{t \to 0} g(t) \cdot \mathbf{Z}(t) = \mathbf{A}, \lim_{t \to 0} g'(t) \cdot \mathbf{Z}'(t) = \mathbf{A}'.$$

Write

$$g(t) = \begin{pmatrix} w(t) & x(t) \\ y(t) & z(t) \end{pmatrix}, g'(t) = \begin{pmatrix} w'(t) & x'(t) \\ y'(t) & z'(t) \end{pmatrix},$$

and

$$Z_l(t) = \begin{pmatrix} \beta_l(t) & \gamma_l(t) \\ 0 & -\beta_l(t) \end{pmatrix}, Z_l'(t) = \begin{pmatrix} \beta_l(t) & \gamma_l'(t) \\ 0 & -\beta_l(t) \end{pmatrix}$$

for $l = 1, \ldots, n$, where $\mathbf{Z} = (Z_1, Z_2, \ldots, Z_n)$ and $\mathbf{Z}'$ is similar.

Now writing $\boldsymbol{\beta}$, $\boldsymbol{\gamma}$ and $\boldsymbol{\gamma}'$ for the row vectors $(\beta_i, \beta_j, \beta_k)$, $(\gamma_i, \gamma_j, \gamma_k)$ and $(\gamma_i', \gamma_j', \gamma_k')$ respectively and evaluating $g(t) \cdot \mathbf{Z}(t)$ shows that

$$\mathbf{b} = \lim_{t \to 0}(w(t)z(t)\boldsymbol{\beta}(t) - w(t)y(t)\boldsymbol{\gamma}(t) + x(t)y(t)\boldsymbol{\beta}(t)) \tag{9}$$

and

$$\mathbf{c} = \lim_{t \to 0}(-2x(t)w(t)\boldsymbol{\beta}(t) + w(t)^2 \boldsymbol{\gamma}(t)). \tag{10}$$

Meanwhile, evaluating $g'(t) \cdot \mathbf{Z}'(t)$ shows that

$$\mathbf{b} = \lim_{t \to 0}(-w'(t)z'(t)\boldsymbol{\beta}(t) + w'(t)y'(t)\boldsymbol{\gamma}'(t) - x(t)y(t)\boldsymbol{\beta}(t)) \tag{11}$$

and

$$\mathbf{c}' = \lim_{t \to 0}(-2x'(t)w'(t)\boldsymbol{\beta}(t) + w'(t)^2 \boldsymbol{\gamma}'(t)). \tag{12}$$

Now using (9), (10) and (12) we have

$$\Delta_{ijk}(\mathbf{A}, \mathbf{A}') = \lim_{t \to 0} \begin{vmatrix} w(t)z(t)\boldsymbol{\beta}(t) - w(t)y(t)\boldsymbol{\gamma}(t) + x(t)y(t)\boldsymbol{\beta}(t) \\ -2w(t)x(t)\boldsymbol{\beta}(t) + w(t)^2 \boldsymbol{\gamma}(t) \\ -2w'(t)x'(t)\boldsymbol{\beta}(t) + w'(t)^2 \boldsymbol{\gamma}(t) \end{vmatrix}$$

$$= \lim_{t \to 0} w(t)w'(t) \begin{vmatrix} \boldsymbol{\beta}(t) + 2x(t)y(t)\boldsymbol{\beta}(t) - w(t)y(t)\boldsymbol{\gamma}(t) \\ -2x(t)\boldsymbol{\beta}(t) + w(t)\boldsymbol{\gamma}(t) \\ -2x'(t)\boldsymbol{\beta}(t) + w'(t)\boldsymbol{\gamma}(t) \end{vmatrix}$$

where we use the fact that $w(t)z(t) - x(t)y(t) = 1$ for all $t \in \mathbb{C}^*$ in the first row. Now using row operations to simplify the determinant we get

$$\Delta_{ijk}(\mathbf{A}, \mathbf{A}') = \lim_{t \to 0} w(t)w'(t) \begin{vmatrix} \boldsymbol{\beta}(t) \\ -2x(t)\boldsymbol{\beta}(t) + w(t)\boldsymbol{\gamma}(t) \\ -2x'(t)\boldsymbol{\beta}(t) + w'(t)\boldsymbol{\gamma}'(t) \end{vmatrix}$$

$$= \lim_{t \to 0} w(t)^2 w'(t)^2 \begin{vmatrix} \boldsymbol{\beta}(t) \\ \boldsymbol{\gamma}(t) \\ \boldsymbol{\gamma}'(t) \end{vmatrix}.$$

On the other hand, using (10)–(12) gives us

$$\Delta_{ijk}(\mathbf{A}, \mathbf{A}') = \lim_{t \to 0} \begin{vmatrix} -w'(t)z'(t)\boldsymbol{\beta}(t) + w'(t)y'(t)\boldsymbol{\gamma}'(t) - x'(t)y'(t)\boldsymbol{\beta}(t) \\ -2w(t)x(t)\boldsymbol{\beta}(t) + w(t)^2 \boldsymbol{\gamma}(t) \\ -2w'(t)x'(t)\boldsymbol{\beta}(t) + w'(t)^2 \boldsymbol{\gamma}(t) \end{vmatrix}$$

$$= \lim_{t \to 0} w(t)w'(t) \begin{vmatrix} -\boldsymbol{\beta}(t) - 2x'(t)y'(t)\boldsymbol{\beta}(t) + w'(t)y'(t)\boldsymbol{\gamma}'(t) \\ -2x(t)\boldsymbol{\beta}(t) + w(t)\boldsymbol{\gamma}(t) \\ -2x'(t)\boldsymbol{\beta}(t) + w'(t)\boldsymbol{\gamma}(t) \end{vmatrix}$$

where we use the fact that $w'(t)z'(t) - x'(t)y'(t) = 1$ for all $t \in \mathbb{C}^*$ in the first row. Now using row operations to simplify the determinant we get

$$\Delta_{ijk}(\mathbf{A}, \mathbf{A}') = \lim_{t \to 0} w(t)w'(t) \begin{vmatrix} -\boldsymbol{\beta}(t) \\ -2x(t)\boldsymbol{\beta}(t) + w(t)\boldsymbol{\gamma}(t) \\ -2x'(t)\boldsymbol{\beta}(t) + w'(t)\boldsymbol{\gamma}'(t) \end{vmatrix}$$

$$= \lim_{t \to 0} w(t)^2 w'(t)^2 \begin{vmatrix} -\boldsymbol{\beta}(t) \\ \boldsymbol{\gamma}(t) \\ \boldsymbol{\gamma}'(t) \end{vmatrix}.$$

This shows that $\Delta_{ijk}(\mathbf{A}, \mathbf{A}') = 0$. Since this applies to all $1 \le i < j < k \le n$ we get $\mathrm{rk}(m_{\mathbf{A}, \mathbf{A}'}) \le 2$ as required, i.e. $(\mathbf{A}, \mathbf{A}') \in \widehat{\mathcal{C}'}$. ∎

Corollary 3.18: *We have*

$$\overline{(G \times G) \cdot \widehat{\mathcal{C}}} \subseteq \overline{(G \times G) \cdot \mathcal{C}} \cap \overline{\Gamma_{G, \mathcal{V}^n}} \subseteq \overline{(G \times G) \cdot \widehat{\mathcal{C}}} \cup \overline{(G \times G) \cdot \widehat{\mathcal{C}'}}.$$

Proof: The first inclusion follows from Proposition 3.14 and the fact that the middle term is closed. For the second we have

$$\overline{(G \times G) \cdot \mathcal{C}} \cap \overline{\Gamma_{G, \mathcal{V}^n}} \subseteq ((G \times G) \cdot \mathcal{C} \cup (G \times G) \cdot \widehat{\mathcal{C}'}) \cap \overline{\Gamma_{G, \mathcal{V}^n}}$$

by Lemma 3.17,

$$= (G \times G) \cdot \widehat{\mathcal{C}} \cup (\overline{\Gamma_{G, \mathcal{V}^n}} \cap (G \times G) \cdot \widehat{\mathcal{C}'})$$

by Proposition 3.14,

$$= (G \times G) \cdot \widehat{\mathcal{C}} \cup (G \times G) \cdot \widehat{\mathcal{C}'}$$

since

$$(G \times G) \cdot \widehat{\mathcal{C}'} \subseteq (G \times G) \cdot \mathcal{C}' \subseteq \overline{\Gamma_{G, \mathcal{V}^n}}$$

by Lemma 3.13. ∎

Notice that $\widehat{\mathcal{C}}$ and $\widehat{\mathcal{C}'}$ are both fixed by $B \times B$, since Δ_{ijk} is $B \times B$ semi-invariant for all i, j, k on both $\mathcal{C}$ and $\mathcal{C}'$, and both $\mathcal{C}$ and $\mathcal{C}'$ are $B \times B$-modules. Therefore we have

$$\dim(\overline{(G \times G) \cdot \widehat{\mathcal{C}}}) = \dim(\widehat{\mathcal{C}}) + 2 \dim(G) - 2 \dim(B) = \dim(\widehat{\mathcal{C}}) + 2.$$

Now it's easy to see that $\widehat{\mathcal{C}}$ is isomorphic to the variety of $3 \times n$ matrices with rank at most 2, which is well known to have dimension $2n + 2$. Therefore we have $\dim(\overline{(G \times G) \cdot \widehat{\mathcal{C}}}) = 2n + 4$. Exactly the same argument also shows $\dim(\overline{(G \times G) \cdot \widehat{\mathcal{C}'}}) = 2n + 4$. Now Corollary 3.18 above shows that

$$\dim(\overline{(G \times G) \cdot \mathcal{C}} \cap \overline{\Gamma_{G, \mathcal{V}^n}}) = 2n + 4.$$

Consequently, since $\dim(\mathcal{S}_{G, \mathcal{V}^n}) = 6n - (3n - 3) = 3n + 3$, we get that $\mathcal{S}_{G, \mathcal{V}^n}$ is connected in codimension $n-1$ but not in codimension $n-2$. We also note that $\mathcal{S}_{G, \mathcal{V}^n}$ contains just two components and these have non-trivial intersection. By Proposition 2.8, for any separating set $S \subseteq \mathbb{C}[\mathcal{V}^n]^G$ we have

$$|S| \ge \dim(\mathbb{C}[\mathcal{V}^n])^G + n - 2 = 3n - 3 + n - 2 = 4n - 5.$$

This completes the proof of Proposition 3.2 and Theorem 1.4 follows immediately.

4. Smaller separating sets

In this section, we will show that for $n \geq 5$ there exist smaller separating sets for $\mathbb{C}[\mathcal{V}^n]^G$ than S_n. The aim is to prove Proposition 3.3; Theorem 1.6 will follow immediately.

We begin by noting that, for $n \geq 4$, $\mathbb{C}[\mathcal{V}^n]^G$ is not a polynomial ring; for $n \geq 2$ its dimension is $4n-3$ and the minimum number of algebra generators is $\frac{1}{6}(n^3 + 5n)$. Relations between the generators of $\mathbb{C}[\mathcal{M}^n]^G$ were completely described by Drensky [31], but we do not need a complete description here. The following is a translation of one kind of relation from [31] to the trace-zero setting:

$$t_{ijk}t_{pqr} = -\frac{1}{8} \begin{vmatrix} t_{ip} & t_{iq} & t_{ir} \\ t_{jp} & t_{jq} & t_{jr} \\ t_{kp} & t_{kq} & t_{kr} \end{vmatrix} \tag{13}$$

for $1 \leq i < j < k \leq n, 1 \leq p < q < r \leq n, n \geq 4$. This can also be shown directly using (4) and standard properties of determinants.

For the rest of this section, assume $n \geq 3$. Now suppose that $\mathbf{A}, \mathbf{A}'$ are trace-zero n-matrices and that $\text{Tr}(A_iA_j) = \text{Tr}(A_i'A_j')$ for all $1 \leq i \leq j \leq n$. The relation (13) above with $i = p, j = q, r = k$ tells us immediately that $\text{Tr}(A_iA_jA_k) = \pm \text{Tr}(A_i'A_j'A_k')$ for all $1 \leq i < j < k \leq n$. Applying the same relation with arbitrary i, j, k, p, q, r shows that either $\text{Tr}(A_iA_jA_k) = \text{Tr}(A_i'A_j'A_k')$ for all $1 \leq i < j < k \leq n$ or $\text{Tr}(A_iA_jA_k) = - \text{Tr}(A_i'A_j'A_k')$ for all $1 \leq i < j < k \leq n$.

Further, suppose $f \in \bigoplus_{1 \leq i < j < k \leq n} \mathbb{C}t_{ijk}$. Then $f(\mathbf{A}) = \pm f(\mathbf{A}')$. If $f(\mathbf{A}) = f(\mathbf{A}') \neq 0$ then for $1 \leq i < j < k \leq n$ we have

$$t_{ijk}(\mathbf{A}) = \frac{t_{ijk}f(\mathbf{A})}{f(\mathbf{A})} = \frac{t_{ijk}f(\mathbf{A}')}{f(\mathbf{A}')} = t_{ijk}(\mathbf{A}')$$

since $t_{ijk}f \in \mathbb{C}[t_{ij} : 1 \leq i \leq j \leq n]$.

From the above discussion we deduce:

Lemma 4.1: *Let* $S' = \{t_{ij} : 1 \leq i \leq j \leq n\} \cup F$ *where* $F \subset \bigoplus_{1 \leq i < j < k \leq n} \mathbb{C}t_{ijk}$. *Then* S' *is a separating set for* $\mathbb{C}[\mathcal{V}^n]^G$ *if and only if for all* $\mathbf{A} \in \mathcal{V}^n$ *we have*

$$f(\mathbf{A}) = 0 \text{ for all } f \in F \Rightarrow t_{ijk}(\mathbf{A}) = 0 \text{ for all } 1 \leq i < j < k \leq n.$$

Given $\mathbf{A} \in \mathcal{V}^n$ we may form a $3 \times n$ matrix $M_{\mathbf{A}}$ as follows:

$$M_{\mathbf{A}} = \begin{pmatrix} c_1 & c_2 & \cdots & c_n \\ b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

The values of $t_{ijk}(\mathbf{A})$ are the maximal minors of this matrix. Let Y be a generic $3 \times n$ matrix and let I be the ideal of $\mathbb{C}[Y]$ generated by its 3×3 minors. Choosing a set F as in Lemma 4.1 is equivalent to choosing a set of linear combinations of 3×3 minors generating an ideal of $\mathbb{C}[Y]$ whose radical is the same as the radical of I (in fact, I is a radical ideal). [32, Lemma 5.9] describes how to do this, and Proposition 5.20, Corollary 5.21 and

Proposition 5.22 [loc. cit.] show that $3n-8$ linear combinations suffice. Concretely, let $[ijk]$ denote the minor corresponding to columns i, j, k in Y; choose $e_1, \ldots, e_r, r = 3n-8$ where

$$e_l = \sum_{1 \le i < j < k \le n} \lambda_{ijk}[ijk]$$

for $l = 1, \ldots, r$. Set

$$f_l = \sum_{1 \le i < j < k \le n} \lambda_{ijk} t_{ijk}$$

for $l = 1, \ldots, r$. Then

$$S' = \{t_{ij} : 1 \le i \le j \le n\} \cup \{f_l : l = 1, \ldots, r\}$$

is a separating set for $\mathbb{C}[\mathcal{V}^n]^G$. The cardinality of this set is

$$n + \binom{n}{2} + 3n - 8 = \frac{1}{2}(n^2 + 7n - 16).$$

This completes the proof of Proposition 3.3; Theorem 1.6 now follows immediately from the remarks at the beginning of Section 3.

5. Matrix semi-invariants

In this section, we consider the action of a different but related group on $\mathcal{M}_2^n$: let $H := \mathrm{SL}_2 \times \mathrm{SL}_2$. This acts on an n-matrix $\mathbf{A}$ according to the formula

$$(h_1, h_2) \cdot \mathbf{A} = (h_1 A_1 h_2^{-1}, h_1 A_2 h_2^{-1}, \ldots, h_1 A_n h_2^{-1}).$$

Generating sets for the algebras of invariants $\mathbb{C}[\mathcal{M}_2^n]^H$ are known, see [33]. More recently, Domokos [34] showed that the following set S_n of invariants are a separating set for $\mathbb{C}[\mathcal{M}_2^n]^H$ which is minimal by inclusion (we retain the notation of Section 1):

- $\det(X_i) : 1 \le i \le n$;
- $\langle X_i | X_j \rangle := \mathrm{Tr}(X_i)\,\mathrm{Tr}(X_j) - \mathrm{Tr}(X_i X_j) : 1 \le i < j \le n$;
- $\xi(X_i X_j X_k X_l) : 1 \le i < j < k < l \le n$.

Here $\xi(X_i X_j X_k X_l)$ is the coefficient of $a_i a_j a_k a_l$ in the determinant

$$\begin{vmatrix} a_i X_i & a_j X_j \\ a_k X_k & a_l X_l \end{vmatrix} \in \mathbb{C}[\mathcal{M}_2^n][a_i, a_j, a_k, a_l].$$

The size of this separating set is $n + \binom{n}{2} + \binom{n}{4}$. We note once again that the fact that this separating set is minimal by inclusion does not mean that it has minimal cardinality.

In this section, we prove the following:

Theorem 5.1: *Let $S \subseteq \mathbb{C}[\mathcal{M}_2^n]^H$ be a separating set. Then $|S| \ge 5n - 10$.*

n	$\dim(\mathbb{C}[\mathcal{M}_2^n]^H)$	$|S_n|$	Lower bound
2	3	3	3
3	6	6	6
4	10	11	10
5	14	20	15
6	18	36	20

The dimension of $\mathbb{C}[\mathcal{M}_2^n]^H$ for $n \geq 3$ is $\dim(\mathcal{M}_2^n) - \dim(H) = 4n - 6$. This follows from Proposition 2.3 because there exist 3-matrices whose stabilizer in H is the finite group $\{(\pm I, \pm I)\}$. Contrastingly, $\dim(\mathbb{C}[\mathcal{M}_2^n]^H) = 8 - 6 + 1 = 3$, since every 2-matrix has at least a one-dimensional stabilizer, and $\dim(\mathbb{C}[\mathcal{M}_2]^H) = 4 - 6 + 3 = 1$ since the stabilizer of any matrix has dimension at least 3. So, our result implies that for $n \geq 5$ there does not exist a polynomial separating set for the action of H on $\mathcal{M}_2^n$.

The proof is a straightforward application of a result of Domokos: for $n \geq 1$ consider the morphism $\sigma : \mathcal{M}_2^n \to \mathcal{M}_2^{n+1}$ given by

$$\sigma(A_1, A_2, \ldots, A_n) = (A_1, A_2, \ldots, A_n, I)$$

where I is the 2×2 identity matrix. By [35, Proposition 4.1], the induced morphism

$$\sigma^* : \mathbb{C}[\mathcal{M}_2^{n+1}]^H \to \mathbb{C}[\mathcal{M}_2^n]^G$$

is surjective (the reference has $G = \mathrm{GL}_2$ but the algebras of invariants are the same). This can be used to show that for any separating set $S \subseteq \mathbb{C}[\mathcal{M}_2^{n+1}]^H$, $\sigma^*(S) \subseteq \mathbb{C}[\mathcal{M}_2^n]^G$ is a separating set, see [34, Corollary 6.3]. Now Theorem 5.1 follows immediately from this observation and Theorem 1.4.

The table below compares this lower bound with the size of the separating set given in this section.

Note that in the case $n = 4$ we cannot rule out the existence of a polynomial separating set with these methods. In a forthcoming paper, we plan to compute the separating variety for this action directly and thereby sharpen these lower bounds.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Data Access Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Jonathan Elmer 🔟 http://orcid.org/0000-0001-5296-1987

References

[1] Belitskii GR, Sergeichuk VV. Complexity of matrix problems. 2003;361:203–222. Ninth Conference of the International Linear Algebra Society (Haifa, 2001)..

[2] Le Bruyn L, Procesi C. Semisimple representations of quivers. Trans Amer Math Soc. 1990;317(2):585–598.

[3] Dolgachev I. Lectures on invariant theory. Cambridge: Cambridge University Press; 2003. (London Mathematical Society Lecture Note Series; vol. 296).

[4] Derksen H, Kemper G. Computational invariant theory. Berlin: Springer-Verlag; 2002. (Invariant Theory and Algebraic Transformation Groups, I; Encyclopaedia of Mathematical Sciences; vol. 130).

[5] Fleischmann P. The Noether bound in invariant theory of finite groups. Adv Math. 2000;156(1):23–32.

[6] Fogarty J. On Noether's bound for polynomial invariants of a finite group. Electron Res Announc Amer Math Soc. 2001;7(2):5–7. (electronic).

[7] Sezer Müfit. Explicit separating invariants for cyclic *P*-groups. J Comb Theory Ser A. 2011;118(2):681–689.

[8] Wehlau DL. Invariants for the modular cyclic group of prime order via classical invariant theory. J Eur Math Soc (JEMS). 2013;15(3):775–803.

[9] Elmer J, Kohls M. Separating invariants for the basic $\mathbb{G}_a$-actions. Proc Amer Math Soc. 2012;140(1):135–146.

[10] Dufresne E, Elmer J, Sezer Müfit. Separating invariants for arbitrary linear actions of the additive group. Manuscr Math. 2014;143(1-2):207–219.

[11] Bedratyuk L. A complete minimal system of covariants for the binary form of degree 7. J Symb Comput. 2009;44(2):211–220.

[12] Kemper G. Separating invariants. J Symb Comput. 2009;44(9):1212–1222. Effective Methods in Algebraic Geometry.

[13] Dufresne E, Kohls M. A finite separating set for Daigle and Freudenburg's counterexample to Hilbert's fourteenth problem. Comm Algebra. 2010;38(11):3987–3992.

[14] Dufresne E, Kohls M. The separating variety for the basic representations of the additive group. J Algebra. 2013;377:269–280.

[15] Dufresne E. Separating invariants. [Ph. D. thesis] Kingston Ontario: 2008.

[16] Giral JéM. Krull dimension, transcendence degree and subalgebras of finitely generated algebras. Arch Math. 1981;36(1):305–312.

[17] Kamke T, Kemper G. Algorithmic invariant theory of nonreductive groups. Qual Theory Dyn Syst. 2012;11(1):79–110.

[18] Kaygorodov I, Lopatin A, Popov Y. Separating invariants for 2×2 matrices. Linear Algebra Appl. 2018;559:114–124.

[19] Dufresne E. Separating invariants and finite reflection groups. Adv Math. 2009;221(6):1979–1989.

[20] Dufresne E, Jeffries J. Separating invariants and local cohomology. Adv Math. 2015;270:565–581.

[21] Vinberg ÈB, Popov VL. Invariant theory. In: Algebraic geometry, 4 (Russian). Itogi Nauki i Tekhniki, 315. Moscow: Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform; 1989. p. 137–314.

[22] Kemper G. Computing invariants of reductive groups in positive characteristic. Transform Groups. 2003;8(2):159–176.

[23] Eisenbud D. Commutative algebra with a view toward algebraic geometry. New York: Springer-Verlag; 1995. (Graduate Texts in Mathematics; vol. 150).

[24] Grothendieck A. Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux (SGA 2). Amsterdam: North-Holland Publishing Co; 1962. (Séminaire de Géométrie Algébrique du Bois-Marie). Augmenté d'un exposé par Michèle Raynaud, Advanced Studies in Pure Mathematics, Vol. 2. Masson & Cie, Éditeur, Paris, 1968.

[25] Reimers F. Separating invariants of finite groups. J Algebra. 2018;507:19–46.

[26] Dufresne E, Kraft H. Invariants and separating morphisms for algebraic group actions. Math Z. 2015;280(1-2):231–255.

[27] Dufresne E, Jeffries J. Mapping toric varieties into low dimensional spaces. *Trans. Amer. Math. Soc.*, to appear.

[28] Mumford D, Fogarty J, Kirwan F. Geometric invariant theory. 3rd ed. Berlin: Springer-Verlag; 1994. (Ergebnisse der Mathematik und ihrer Grenzgebiete (2); vol. 34).

[29] Drézet J-M. Luna's slice theorem and applications. In: Algebraic group actions and quotients. Cairo: Hindawi Publ. Corp; 2004. p. 39–89.

[30] Florentino CAA. Simultaneous similarity and triangularization of sets of 2 by 2 matrices. Linear Algebra Appl. 2009;431(9):1652–1674.

[31] Drensky V. Defining relations for the algebra of invariants of 2×2 matrices. Algebr Rep Theory. 2003;6(2):193–214.

[32] Bruns W, Vetter U. Determinantal rings. Rio de Janeiro: Instituto de Matemática Pura e Aplicada (IMPA); 1988. (Monografías de Matemática [Mathematical Monographs]; vol. 45).

[33] Domokos Mátyás. Poincaré series of semi-invariants of 2×2 matrices. Linear Algebra Appl. 2000;310(1-3):183–194.

[34] Domokos M. Characteristic free description of semi-invariants of 2×2 matrices. J Pure Appl Algebra. 2020;224(5):106220. 13.

[35] Domokos Mátyás. Relative invariants of 3×3 matrix triples. Linear Multilinear Algebra. 2000;47(2):175–190.