On the orbit closure intersection problems for matrix tuples under conjugation and left-right actions

Gábor Ivanyos* Youming Qiao†

Abstract

Let G be a linear algebraic group acting on the vector space V. Given $v, v' \in V$, the orbit closure intersection problem asks to decide if the orbit closures of v and v' under G intersect. Due to connections with polynomial identity testing, the orbit closure intersection problems for the conjugation and left-right actions on matrix tuples received considerable attention in computational complexity and computational invariant theory, as seen in the works of Forbes–Shpilka (*RANDOM* 2013), Allen-Zhu–Garg–Li–Oliveira–Wigderson (*STOC* 2018), and Derksen–Makam (*Algebra & Number Theory* 2020). In this paper, we present new algorithms for the orbit closure problem for the conjugation and left-right actions on matrix tuples. The main novel feature is that in the case of intersecting orbit closures, our algorithm outputs cosets of one-parameter subgroups that drive the matrix tuples to a tuple in the intersection of the orbit closures.

1 Introduction

Background and motivations. In this paper we study the orbit closure intersection problems for the conjugation and left-right actions on matrix tuples. Such problems naturally arise from invariant theory, and they can be formulated as special cases of the polynomial identity testing (PIT) problem [Mul17, AZGL+18]. To devise a deterministic efficient algorithm for PIT is a significant problem in computational complexity due to its implications to circuit lower bounds [KI04]. In the past few years, invariant-theoretic problems, such as nullcone membership and orbit closure intersection, for the conjugation, left-right, and other actions, received considerable attention [FS13, IQS17, GGdOW16, AZGL+18, IQS18, BGdO+18, BFG+19, GIM+20, BIL+21, MW21]. This paper is yet another addition to this research line.

Matrix tuples and two group actions. Let $\mathbb{F}$ be a field. Let $\mathrm{M}(\ell \times n, \mathbb{F})$ be the linear space of $\ell \times n$ matrices over $\mathbb{F}$, and $\mathrm{M}(n, \mathbb{F}) := \mathrm{M}(n \times n, \mathbb{F})$. Let $\mathbf{A} = (A_1, \ldots, A_m) \in \mathrm{M}(\ell \times n, \mathbb{F})^m$ be a tuple of matrices, also called a matrix tuple.

Two natural group actions on matrix tuples are the *conjugation action* and the *left-right action*. Let $\mathrm{GL}(n, \mathbb{F})$ (resp. $\mathrm{SL}(n, \mathbb{F})$) be the general (resp. special) linear group of degree n over $\mathbb{F}$. Given $\mathbf{A} \in \mathrm{M}(n, \mathbb{F})^m$, the conjugation action of $C \in \mathrm{GL}(n, \mathbb{F})$ sends $\mathbf{A}$ to $C^{-1}\mathbf{A}C := (C^{-1}A_1C, \ldots, C^{-1}A_mC)$. The orbit of $\mathbf{A}$ under the conjugation action is $\mathrm{O}_{\mathrm{conj}}(\mathbf{A}) := \{C^{-1}\mathbf{A}C \mid C \in \mathrm{GL}(n, \mathbb{F})\}$. Given $\mathbf{A} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$, the left-right action of $(C, D) \in \mathrm{SL}(\ell, \mathbb{F}) \times \mathrm{SL}(n, \mathbb{F})$ sends $\mathbf{A} \in \mathrm{M}(\ell \times n, \mathbb{F})$ to $C^{-1}\mathbf{A}D := (C^{-1}A_1D, \ldots, C^{-1}A_mD)$. The orbit of $\mathbf{A}$ under the left-right action is $\mathrm{O}_{\mathrm{lr}}(\mathbf{A}) := \{C^{-1}\mathbf{A}D \mid C \in \mathrm{SL}(\ell, \mathbb{F}), D \in \mathrm{SL}(n, \mathbb{F})\}$.

Orbit closures under the two group actions. Suppose $\mathbb{F}$ is algebraically closed. The vector space $\mathrm{M}(\ell \times n, \mathbb{F})^m$ is naturally endowed with the Zariski topology. The orbit closure of $\mathbf{A} \in \mathrm{M}(n, \mathbb{F})^m$ under the conjugation action, denoted as $\overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{A})$, is the smallest Zariski-closed set containing $\mathrm{O}_{\mathrm{conj}}(\mathbf{A})$. The orbit closure of $\mathbf{A} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$ under the left-right action, denoted as $\overline{\mathrm{O}_{\mathrm{lr}}}(\mathbf{A})$, is the smallest Zariski-closed set containing $\mathrm{O}_{\mathrm{lr}}(\mathbf{A})$.

We also recall the following notions from invariant theory. Let G be an algebraic group. A *one-parameter subgroup* of G is an algebraic group morphism $\lambda : \mathbb{F}^\times \to G$. More specifically, a one-parameter subgroup of $\mathrm{GL}(n, \mathbb{F})$ is a map of the form $t \mapsto C^{-1}\,\mathrm{diag}(t^{a_1}, \ldots, t^{a_n})C$, $C \in \mathrm{GL}(n, \mathbb{F})$, $a_i \in \mathbb{Z}$, a_i's are called the weights of this one-parameter subgroup. The ring of *matrix invariants* $\mathrm{MI}(n, m, \mathbb{F})$ consists of those polynomial functions on $\mathrm{M}(n, \mathbb{F})^m$ that are invariant under the induced action of the conjugation action. The ring of *matrix semi-invariants* $\mathrm{MSI}(\ell \times n, m, \mathbb{F})$ consists of those polynomial functions on $\mathrm{M}(\ell \times n, \mathbb{F})^m$ that are invariant under the induced action of the left-right action.

Let $\mathbf{A}, \mathbf{B} \in \mathrm{M}(n, \mathbb{F})^m$. By classical invariant theory [Hil90, MFK94], we have the following.

*Institute for Computer Science and Control, Eótvös Loránd Reserch Network, Budapest, Hungary (Gabor.Ivanyos@sztaki.hu).
†Centre for Quantum Software and Information, University of Technology Sydney, Australia (Youming.Qiao@uts.edu.au).

- Suppose $\overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{A}) \cap \overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{B}) = \emptyset$. Then there exists a matrix invariant $f \in \mathrm{MI}(n, m, \mathbb{F})$ such that $f(\mathbf{A}) \neq f(\mathbf{B})$.
- Suppose $\overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{A}) \cap \overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{B}) \neq \emptyset$. Then by the Hilbert–Mumford criterion, for $\mathbf{C} \in \overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{A}) \cap \overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{B})$, there exist two one-parameter subgroups λ_1, λ_2, such that $\lim_{t\to 0} \lambda_1(t) \cdot \mathbf{A}$ and $\lim_{t\to 0} \lambda_2(t) \cdot \mathbf{B}$ are in $\overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{C})$, where $\lambda_i(t) \cdot \mathbf{A}$ denotes the conjugation action of $\lambda_i(t)$ on $\mathbf{A}$.

Analogous results for the left-right action also hold.

Orbit closure intersection problems and previous algorithms. The notion of orbit closure leads to the following algorithmic problem.

PROBLEM 1. (ORBIT CLOSURE PROBLEMS UNDER CONJUGATION AND LEFT-RIGHT ACTIONS) *Let $\mathbb{F}$ be an algebraically closed field. Given $\mathbf{A}, \mathbf{B} \in \mathrm{M}(n, \mathbb{F})^m$, decide whether $\overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{A}) \cap \overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{B}) = \emptyset$. Given $\mathbf{A}, \mathbf{B} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$, decide whether $\overline{\mathrm{O}_{\mathrm{lr}}}(\mathbf{A}) \cap \overline{\mathrm{O}_{\mathrm{lr}}}(\mathbf{B}) = \emptyset$.*

For the orbit closure problem of the conjugation action, the following results are known. Forbes and Shpilka presented a deterministic polynomial-time algorithm over characteristic-0 fields [FS13]. Derksen and Makam presented a deterministic polynomial-time algorithm over fields of arbitrary characteristics [DM20], which, in the case when $\overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{A})$ and $\overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{B})$ do not intersect, outputs a matrix semi-invariant that separates $\mathbf{A}$ and $\mathbf{B}$.

For the orbit closure problem of the left-right action, the following results are known. Allen-Zhu, Garg, Li, Oliveira and Wigderson presented a deterministic polynomial-time algorithm over characteristic-0 fields [AZGL+18]. Derksen and Makam presented a deterministic polynomial-time algorithm over fields of arbitrary characteristics [DM20], which, in the case when $\overline{\mathrm{O}_{\mathrm{lr}}}(\mathbf{A})$ and $\overline{\mathrm{O}_{\mathrm{lr}}}(\mathbf{B})$ do not intersect, outputs a matrix semi-invariant that separates $\mathbf{A}$ and $\mathbf{B}$.

Main results. When the orbit closures do intersect, the above algorithms do not output a matrix tuple in the intersection, and the corresponding cosets of one-parameter subgroups driving the input matrix tuples to it. In this paper, we present new algorithms addressing this issue. Rather than computing separating invariants, our approach is based on a reduction to the orbit problem via finding two tuples in the closures of the orbits such that their orbits are the same if and only if the original orbit closures intersect.

THEOREM 1.1. *There exist deterministic polynomial-time algorithms for the orbit closure intersection problems for the conjugation and left-right actions. In the case when the orbit closures intersect, these algorithms output a matrix tuple in the intersection, together with the cosets of the one-parameter subgroups driving the input matrix tuples to it.*

Here, by a polynomial time algorithm we mean an arithmetic circuit of size polynomial in mn or $m\ell n$, that is, a procedure that uses polynomially many standard field operations, except for the cosets in the case of the left-right action, where we may need to take ℓth and nth roots of certain determinants. When the input tuples are given over a number field or over a finite field the procedures result in algorithms of polynomial bit complexity.

Algorithm outline for the conjugation action. Given $\mathbf{A} = (A_1, \ldots, A_m), \mathbf{B} = (B_1, \ldots, B_m) \in \mathrm{M}(n, \mathbb{F})^m$, there is a well-known algebraic criterion to determine whether $\overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{A}) \cap \overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{B}) = \emptyset$ by Artin [Art69] as follows: there exists a matrix tuple $\mathbf{A}'$ (resp. $\mathbf{B}'$) associated with $\mathbf{A}$ (resp. $\mathbf{B}$), which, roughly speaking, consists of the simple factors of $\mathbf{A}$ (resp. $\mathbf{B}$) as an algebra representation. Then the orbit closure problem of $\mathbf{A}$ and $\mathbf{B}$ reduces to the orbit problem for $\mathbf{A}'$ and $\mathbf{B}'$.

Since the orbit problem for the conjugation action, known as the module isomorphism problem, is solvable in polynomial time [CIK97, BL08, IKS10], a natural strategy is to compute $\mathbf{A}'$ from $\mathbf{A}$. Computing the simple factors is a fundamental task in computational module theory which has efficient solutions over various base fields. The methods require factoring (univariate) polynomials so merely standard field operations do not suffice. Also, if the tuples are given over a number field or a finite field it is desirable to have an algorithm of time polynomial in the size of the input. However, the simple factors over the algebraic closure are defined over extensions which may generate a common extension field of exponential dimension. This issue can be circumvented by allowing an output of a rather complicated form like in [IQS18]. Fortunately, there is a rational method that gives a partial factorization which is sufficient for our purposes. This is based on computing the radical (a special ideal) of matrix algebras and can be efficiently done in the characteristic zero case or when the input over a finite base field and in certain other cases. However, in characteristic $p > 0$ the radical over the algebraic closure of the field defining the input may be defined on over an extension field and hence there is no rational method computing it.

The main technical contribution of this article is a completely rational algorithm which gets around the above issues by using $\mathbf{A}'$ in an implicit way. The basic technical idea is to maintain a suitable lower approximation of the radical, and if this approximation fails to work, replace it with a more appropriate one. This idea originates from the work of Ciocănea-Teodorescu [CT15].

Algorithm outline for the left-right action. For the left-right action, first we use a square blow-up (as [DM17] in the study of semi-invariants of quiver representations), and then the nullcone membership algorithm from [IQS17, IQS18] to decide if the input matrix tuples are in the nullcone, that is, whether their orbit closures contain 0. This allows us to focus on the case when neither of the input matrix tuples are in the nullcone. When this holds, we can use the non-vanishing semi-invariant constructed by the algorithm in [IQS17, IQS18] to reduce to the conjugation setting. While this idea was also used by Derksen and Makam [DM20], some new ingredients are required in order to construct the desired cosets of one-parameter subgroups, such as correspondences between invariant subspaces pairs (Lemma 4.3), and"conjugating matrix pairs" (Lemma 4.4), between matrix tuples and their blow-ups.

More previous works. Given an algebraic group G acting on a vector space V, there are several algorithmic questions that can be asked regarding orbit closures of $v, v' \in V$, such as the nullcone problem (whether the orbit closure of v contains 0), the orbit closure intersection problem, and the orbit closure containment problem (whether v is contained in the closure of v). We mentioned some works on the orbit closure intersection problem in the above, and we briefly introduce some other related works here.

The nullcone problem for the left-right action on matrix tuples turns out to have connections to several areas including non-commutative algebra, combinatorics, linear algebra, and quantum information [GGdOW16, IQS17]. This problem was recently shown to be in P via three solutions: over $\mathbb{Q}$ by [GGdOW16], and over any field first by [IQS17, IQS18] and then by [HH21].

In [BIL$^+$21], it was shown that the orbit closure containment problem is NP-hard in general. In [GIM$^+$20], it was shown that there exist invariant rings which do not have polynomial-size "encodings" under standard complexity-theoretic assumptions, and several interesting problems at the surface between invariant theory and complexity were proposed.

We mentioned the connection between the orbit closure intersection problem and the polynomial identity testing problem at the beginning of this introduction. After settling the nullcone membership and orbit closure intersection problems for the left-right action, there have been several works studying its implications to the general polynomial identity testing problem [IQ19, MW21, IMQ22]. The messages of these papers seem to be that algebraic varieties beyond invariant-theoretic examples need to be studied, and one such algebraic variety can be found in [LQW$^+$22].

Paper outline. In Section 2, some preliminary material will be presented. In Section 3, we present the algorithm for the orbit closure intersection problem under the conjugation action. In Section 4, we present the algorithm for the orbit closure intersection problem under the left-right action.

2 Preliminaries

Notation. For $n \in \mathbb{N}$, $[n] := \{1, 2, \ldots, n\}$. We use $\mathbb{F}^n$ to denote the linear space of length-n column vectors. We use $\leq$ to denote containment of subspaces.

Matrix algebras. A *matrix algebra* is a subalgebra of $\mathrm{M}(n, \mathbb{F})$. Let $\mathbf{A} = (A_1, \ldots, A_m) \in \mathrm{M}(n, \mathbb{F})^m$. The *enveloping algebra* of $\mathbf{A}$, $\mathrm{Env}(\mathbf{A})$, is the smallest matrix algebra containing the A_i's. A linear basis of $\mathrm{Env}(\mathbf{A})$ can be computed in a straightforward way analogous to the breadth first search on graphs, i.e., by maintaining a list of longer and longer products of elements from $\mathbf{A}$, and adding a new product if it is linearly independent of the already collected elements.

Module isomorphism problem. The module isomorphism problem asks the following. Given $\mathbf{A} = (A_1, \ldots, A_m), \mathbf{B} = (B_1, \ldots, B_m) \in \mathrm{M}(n, \mathbb{F})^m$, decide if $\mathbf{A}$ and $\mathbf{B}$ are *conjugate*, that is there exists $T \in \mathrm{GL}(n, \mathbb{F})$, such that $\forall i \in [m]$, $TA_iT^{-1} = B_i$. This problem admits deterministic efficient algorithms by [CIK97, IKS10] and [BL08]. See also [CT15] for a method for modules over finite rings.

THEOREM 2.1. ([CIK97, BL08, IKS10]) *Let $\mathbf{A}$ and $\mathbf{B}$ be from $\mathrm{M}(n, \mathbb{F})^m$. There exists a deterministic algorithm that decides whether $\mathbf{A}$ and $\mathbf{B}$ are conjugate. The algorithm uses polynomially many arithmetic operations. Over number fields the bit complexity of the algorithm is also polynomial.*

Algebras and modules. We shall use some standard terminologies about algebras and modules, which are collected here for convenience of the reader. Classical references on these include [Pie82], and a concise introduction can be found in [AB95, Sec. 5]. All the algebras we consider in this paper are finite dimensional associative algebras over some field $\mathbb{F}$, possibly without identity. An *ideal* is a linear subspace of $\mathcal{A}$ closed under multiplication by elements of $\mathcal{A}$, both from the left and from the right. Left ideals are subspaces closed under multiplication by elements of $\mathcal{A}$ from the left, and right ideals are defined analogously.

Let V be a vector space, and $\mathrm{End}(V)$ be the algebra of homomorphisms on V. Let $\mathcal{A}$ be an algebra. Then V is an $\mathcal{A}$-module if there exists an algebra homomorphism $\phi : \mathcal{A} \to \mathrm{End}(V)$, which defines an action of $a \in \mathcal{A}$ on V by $\phi(a)$. If $\phi(a) = 0$ for every $a \in \mathcal{A}$, then V is a trivial $\mathcal{A}$-module. The (left or right) multiplication of $\mathcal{A}$ on itself makes $\mathcal{A}$ a (left or right) module. A subspace W of V is a submodule if the action of any $a \in \mathcal{A}$ preserves W. In this case, the quotient space V/W is also an $\mathcal{A}$- module, called the factor module. We say that a submodule W is a direct summand of V if V is the direct sum of W and another submodule U. *Free* (left or right) $\mathcal{A}$ modules are isomorphic to direct sums of copies of the (left or right) $\mathcal{A}$-module $\mathcal{A}$ itself. A module P is called *projective* if every homomorphisms ϕ from P to a factor module U/V can be lifted to a homomorphism ψ to U such that $\phi = \pi \circ \psi$ where π is the projection map $U \to U/V$. Projective modules are characterized as those isomorphic to direct summands of free modules.

An *idempotent* in $\mathcal{A}$ is a nonzero element e with $e^2 = e$. Left ideals that are projective modules are just the direct summands of $\mathcal{A}$. A left ideal P is projective if it is generated by an idempotent: $P = \mathcal{A}e$ for some idempotent $e \in \mathcal{A}$. (This is equivalent to saying that e is a right identity element of P.) Therefore, in algorithms we can use idempotents to represent projective left ideals.

3 The algorithm for the conjugation action

3.1 Artin's algebraic criterion The purpose of this subsection is to present Artin's algebraic criterion for the orbit closures of two matrix tuples to intersect under the conjugation action.

Invariant subspaces. Given $\mathbf{A} = (A_1, \ldots, A_m) \in \mathrm{M}(n, \mathbb{F})^m$, we say that $U \leq \mathbb{F}^n$ is an *invariant subspace* of $\mathbf{A}$, if for any $i \in [m]$, $A_i(U) \leq U$. If the only invariant subspaces of $\mathbf{A}$ are the zero space and the full space, then $\mathbf{A}$ is called *irreducible*. Note that $\mathbf{A}$ is not irreducible, if and only if there exists $C \in \mathrm{GL}(n, \mathbb{F})$, such that $C^{-1}\mathbf{A}C = (\tilde{A}_1, \ldots, \tilde{A}_m)$, and every $\tilde{A}_i = \begin{bmatrix} A_{i,1} & A_{i,2} \\ 0 & A_{i,3} \end{bmatrix}$, where $A_{i,1}$ is of size $d \times d$ for some $d \in [n-1]$.

Invariant subspace flags. Let $U_0 = 0 < U_1 < \cdots < U_b = \mathbb{F}^n$ be a flag of invariant subspaces of $\mathbf{A}$. Suppose for $i \in [b]$, $\dim(U_i) - \dim(U_{i-1}) = d_i$. Then there exists $C \in \mathrm{GL}(n, \mathbb{F})$, such that $C^{-1}\mathbf{A}C = (\tilde{A}_1, \ldots, \tilde{A}_m)$, and every $\tilde{A}_i = \begin{bmatrix} A_{1,i} & * & * & \ldots & * \\ 0 & A_{2,i} & * & \ldots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & A_{b,i} \end{bmatrix}$, where $A_{j,i}$ is of size $d_j \times d_j$. Let $\mathbf{A}_j = (A_{j,1}, \ldots, A_{j,m}) \in \mathrm{M}(d_j, \mathbb{F})^m$. If every $\mathbf{A}_j$, $j \in [b]$, is irreducible, then the flag $U_0 = 0 < U_1 < \cdots < U_b = \mathbb{F}^n$ is called a *fully-refined invariant subspace flag*.

Suppose $U_0 = 0 < U_1 < \cdots < U_b = \mathbb{F}^n$ is an invariant subspace flag. Let $\tilde{A}_i$ be defined as above. Set $\hat{A}_i = \begin{bmatrix} A_{1,i} & 0 & 0 & \ldots & 0 \\ 0 & A_{2,i} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & A_{b,i} \end{bmatrix}$, where $A_{j,i}$ is of size $d_j \times d_j$. Let $\hat{\mathbf{A}} = (\hat{A}_1, \ldots, \hat{A}_m) \in \mathrm{M}(n, \mathbb{F})^m$. In the special case when the flag is fully-refined $\hat{\mathbf{A}}$ is called a *semisimple matrix tuple* associated with $\mathbf{A}$. It is easy to verify that for a given fully-refined invariant subspace flag, two different semisimple matrix tuples associated with $\mathbf{A}$ are in the same orbit under the conjugation action. It is a basic fact from representation theory that semisimple matrix tuples arising from different fully-refined invariant subspace flags are also in the same orbit under the conjugation action.

The following result will be useful.

LEMMA 3.1. *Let $\mathbf{A} \in \mathrm{M}(n, \mathbb{F})^m$, $U_0 = 0 < U_1 < \cdots < U_b = \mathbb{F}^n$ be a flag of invariant subspaces of $\mathbf{A}$ and $\hat{\mathbf{A}} \in \mathrm{M}(n, \mathbb{F})^m$ be as above. Let $\lambda : \mathbb{F}^\times \to \mathrm{GL}(n, \mathbb{F})$ be the one-parameter subgroup defined by sending t to*

$\begin{bmatrix} D_1 & 0 & \dots & 0 \\ 0 & D_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & D_b \end{bmatrix}$, *where* $D_j = \operatorname{diag}(t^{e_j}, \dots, t^{e_j})$ *is of size* $d_j \times d_j$, *and* $e_j = \sum_{i>j} d_i - \sum_{i<j} d_i$. *Then* $\hat{\mathbf{A}} = \lim_{t\to 0} \lambda(t)^{-1}\mathbf{A}\lambda(t)$.

Artin's criterion. We are now ready to state Artin's criterion.

THEOREM 3.1. ([ART69]) *Let* $\mathbf{A}, \mathbf{B} \in \mathrm{M}(n, \mathbb{F})^m$, *and let* $\hat{\mathbf{A}}$ *and* $\hat{\mathbf{B}}$ *be semisimple matrix tuples associated with* $\mathbf{A}$ *and* $\mathbf{B}$, *respectively. Then* $\overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{A})$ *intersects* $\overline{\mathrm{O}_{\mathrm{conj}}}(\mathbf{B})$ *if and only if* $\hat{\mathbf{A}}$ *and* $\hat{\mathbf{B}}$ *are in the same orbit under the conjugation action.*

In light of Lemma 3.1, the main content of Theorem 3.1 is that the orbit of a semisimple matrix tuple is closed. An "effective" proof of this fact can be found in [CIW97, Section 3, in particular Corollary 12]. There, invariants that separate non-isomorphic semisimple modules are devised, and essentially the same invariants are used in [DM20].

3.2 The orbit closure algorithm We assume that the entries of our input tuples are from a subfield $\mathbb{K}$ of $\mathbb{F}$ and that $\mathbb{F}$ is the algebraic closure of $\mathbb{K}$ or possibly an even larger algebraically closed field.

3.2.1 Solutions based on classical module factorization techniques Suppose we are given $\mathbf{A}, \mathbf{B} \in \mathrm{M}(n, \mathbb{K})^m$. By Theorem 3.1, the orbit closure intersection problem for conjugation action naturally admits the following algorithm.

First, compute semisimple matrix tuples associated with them. Second, decide whether the two semisimple matrix tuples are in the same orbit under the conjugation action by Theorem 2.1. By Lemma 3.1, this would also yield a matrix tuple in the orbit closure intersection, and the one-parameter subgroups.

The main issue with this approach is that a fully-refined invariant subspace flag over $\mathbb{F}$ is not necessarily defined over $\mathbb{K}$. To see this, consider the following simple example. Assume that $m = 1$ and that A_1 is the companion matrix $\begin{bmatrix} & & & -a_0 \\ 1 & & & -a_1 \\ & 1 & & -a_2 \\ & & \ddots & \vdots \\ & & 1 & -a_{n-1} \end{bmatrix}$ of the monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{K}[x]^n$. Then the entries of a basis corresponding to a fully refined associated subspace flag, i.e., the entries of a matrix C such that $C^{-1}A_1C$ is diagonal must generate the splitting field of $f(x)$. This may be an extension of huge degree even when $\mathbb{K}$ is a finite field, e.g., when f is a product of many irreducible polynomials having different prime degrees. Fortunately, if $\mathbb{K}$ is a perfect field, it is sufficient to find a subspace flag of $\mathbb{K}^n$ that has no refinement over $\mathbb{K}$ and take the associated block diagonal tuple $\hat{\mathbf{A}}$. This is because if a diagonal block of $\hat{\mathbf{A}}$ is irreducible over $\mathbb{K}$ then this block is similar to a refinement over $\mathbb{F}$ which is semisimple. This observation would offer a method based on finding composition series over $\mathbb{K}$. In the example above, this would require factoring the polynomial $f(x)$ over $\mathbb{K}$.

One can save even more efforts. It is actually sufficient to ensure that the diagonal blocks of $\hat{\mathbf{A}}$ are similar to semisimple tuples over $\mathbb{F}$. (In other words, the module $\mathbb{F}^n$ is semisimple.) If $\mathbb{K}$ is a perfect field then the module $\mathbb{K}^n$ is semisimple if and only if $\mathbb{F}^n = \mathbb{F}\mathbb{K}^n$ is semisimple. This offers the following solution based on the enveloping algebra $\mathrm{Env}(\mathbf{A})$ in $\mathrm{M}(n, \mathbb{K})$.

Suppose $\mathrm{Env}(\mathbf{A})$ acts on a vector space V. Recall that the *radical* of V is the smallest submodule W such that V/W is semisimple, or more precisely, V/W is the direct sum of a trivial module and a semisimple one, if the identity matrix is not contained in $\mathrm{Env}(\mathbf{A})$. This coincides with $\mathrm{rad}(\mathrm{Env}(\mathbf{A}))V$, where $\mathrm{rad}(\mathrm{Env}(\mathbf{A}))$, the Jacobson radical of $\mathrm{rad}(\mathrm{Env}(\mathbf{A}))$, is the largest nilpotent ideal of $\mathrm{Env}(\mathbf{A})$. The *radical series* of V is the descending chain starting with V, continuing with the radical of V and the radical thereof, and so on, ending at the trivial vector space 0. When $\mathbb{F}$ is of characteristic zero or $\mathbb{F}$ is the algebraic closure of a finite field, $\mathrm{rad}(\mathrm{Env}(\mathbf{A}))$ can be computed in polynomial time by the methods of Rónyai [Rón90]. See also [CIW97] for a method over more general fields of positive characteristic p, based on taking pth roots. We therefore have the following over finite fields and algebraic number fields.

THEOREM 3.2. *Let $\mathbb{K}$ be an algebraic number field or a finite field and let $\mathbb{F}$ be an algebraically closed extension field of $\mathbb{K}$. Given a matrix tuple $\mathbf{A} \in \mathrm{M}(n,\mathbb{K})^m$, a tuple $\hat{\mathbf{A}}$ over $\mathbb{K}$ that is similar to a semisimple matrix tuple associated with $\mathbf{A}$ over $\mathbb{F}$ can be computed in deterministic polynomial time. The algorithm also returns a one-parameter subgroup of $\mathrm{GL}(n,\mathbb{F})$ defined over $\mathbb{K}$ driving $\mathbf{A}$ to $\hat{\mathbf{A}}$.*

For an algebraic number field the method uses only standard field operations only and can be turned into an algebraic circuit that works in general fields of characteristic zero. On the other hand, for general $\mathbb{K}$ of positive characteristic $p \leq n$, computing radicals involve taking pth roots, which again cannot be be done using the standard field operations; see [CIW97]. As an illuminating example, consider the companion matrix A_1 of the polynomial $x^p - a$ where p is a prime and a is an element of the characteristic p field $\mathbb{K}$ that is not a pth power. Then $\mathbf{A}$ consisting of the singleton A_1 is irreducible over $\mathbb{K}$. However, it is not diagonalizable over $\mathbb{F}$ as its Jordan normal form over the algebraic closure consists of just one p by p block with $\sqrt[p]{a}$ in the diagonal.

3.2.2 A completely rational algorithm We now present our algorithm, which avoids using polynomial factorisation or pth root computation. Therefore, this algorithm works over any field. The basic idea is to maintain a suitable lower approximation of the radical, and replace it with a better one if it fails to work. This idea was originally used in the work of Ciocănea-Teodorescu [CT15].

Restricting to unital modules. An initial phase ensures that we may restrict ourselves to unital modules. These are modules V over algebras with identity where the identity element of $\mathcal{A}$ act as the identity on V.

Let us indicate how to reduce to the setting of unital modules if $\mathcal{A}$ does not contain the identity matrix. Assume that the matrix algebra $\mathcal{A} \leq \mathrm{M}(n,\mathbb{F})$ does not contain the identity matrix. Then we take $\mathcal{A}' = \mathcal{A} \oplus \mathbb{F}I_n$. In $\mathcal{A}'$, $\mathcal{A}$ is an ideal of codimension one. The $\mathcal{A}'$-submodules of $V = \mathbb{F}^n$ are exactly the $\mathcal{A}$-submodules. Also, suppose $V_1 < V_2 \leq V$ and $V_3 < V_4 \leq V$ are submodules. Then the factor modules V_2/V_1 and V_4/V_3 are isomorphic as $\mathcal{A}'$-modules if and only if they are isomorphic as $\mathcal{A}$-modules. It follows that composition factors of V as $\mathcal{A}'$ modules are in one-to one correspondence with composition factors of V as $\mathcal{A}$ modules. One-dimensional factors that are trivial as $\mathcal{A}$-modules correspond to $\mathcal{A}'$-modules on which $\mathcal{A}$ acts as zero.

On partial decompositions. We now have the following key proposition.

PROPOSITION 3.1. *Let $\mathcal{A}$ be a finite dimensional $\mathbb{F}$-algebra with identity, and J be a nilpotent ideal of $\mathcal{A}$. Suppose $\mathcal{A} = L_1 \oplus \ldots \oplus L_r$ is a decomposition of $\mathcal{A}$ into a direct sum of left ideals. Suppose V and V' are (unital) left $\mathcal{A}$-modules, with flags of submodules of V and V' as $0 = V_0 < V_1 < \ldots V_s = V$ and $0 = V'_0 < V'_1 < \ldots V_t = V'$, such that*

(a) $\forall i \in [s]$, $JV_i \leq V_{i-1}$,

(b) $\forall i \in [t]$, $JV'_i \leq V'_{i-1}$,

(c) $\forall i \in [r]$ and $j \in [s]$, either $\mathrm{Hom}(L_i/JL_i, V_j/V_{j-1}) = 0$ or $V_j/V_{j-1} \cong L_i/JL_i$, and

(d) $\forall i \in [r]$ and $j \in [t]$, either $\mathrm{Hom}(L_i/JL_i, V'_j/V'_{j-1}) = 0$ or $V'_j/V'_{j-1} \cong L_i/JL_i$.

Then the direct sum of the composition factors of V is isomorphic to that for V' if and only if

$$\bigoplus_{j=1}^{s} V_j/V_{j-1} \cong \bigoplus_{j=1}^{t} V'_j/V'_{j-1}.$$

Proof. Let W be simple $\mathcal{A}$-module. Assume that W appears in V_j/V_{j-1}, that is, there exist submodules T and U of V such that $V_{j-1} \leq T < U \leq V_j$ and that $W \cong U/T$. As W is a factor module of $\mathcal{A}$, there exists at least one index i such that W is a factor module of L_i. By the projective property of L_i, applied to the projection $L_i \to W$ and to the projection $U/V_{j-1} \to U/T \cong W$, there is a nonzero homomorphism $\phi : L_i \to U/V_{j-1} \leq V_j/V_{j-1}$. As $JV_j \leq V_{j-1}$, JL_i is in the kernel of ϕ whence ϕ induces a nonzero element of $\mathrm{Hom}(L_i/JL_i, V_j/V_{j-1})$. It follows that $V_j/V_{j-1} \cong L_i/JL_i$. For every simple module W we pick and index i_W such that W is a factor of L_{i_W} and denote by I_W the set of indices j such that W appears in V_j/V_{j-1}. We have that $V_j/V_{j-1} \cong L_{i_W}$ if and only if $j \in I_W$. Thus the multiplicity of W in V is the cardinality of I_W times the multiplicity of W in L_{i_W}. We have an analogous statement for the flag in V'. Therefore the multiplicities of W are the same in the two modules $\oplus_{j=1}^{s} V_j/V_{j-1}$ and $\oplus_{j=1}^{t} V'_j/V'_{j-1}$ if and only if the factor modules in the flags can be matched. ∎

Proposition 3.1 is the key to our algorithm, because it allows us to decide the isomorphism between direct sums of composition factors without computing them explicitly – instead, it is enough to compute flags of submodules satisfying those properties in Proposition 3.1. This applies in particular if we use radicals and possibly further decompositions that are available over the subfield $\mathbb{K}$. In the following we present an algorithm to do so.

The algorithm. Let $\mathbf{A} = (A_1, \ldots, A_m), \mathbf{A}' = (A'_1, \ldots, A'_m) \in \mathrm{M}(n, \mathbb{F})^m$. The direct sum $\mathbf{A} \oplus \mathbf{A}' = (\widetilde{A_1}, \ldots, \widetilde{A_m}) \in \mathrm{M}(2n, \mathbb{F})^m$, where $\widetilde{A_i} := \mathrm{diag}(A_i, A'_i)$.

Let $\mathcal{A}$ be the enveloping algebra $\mathrm{Env}(\mathbf{A} \oplus \mathbf{A}')$. Let V (resp. V') be the two n-dimensional $\mathcal{A}$-modules on which the generators of $\mathcal{A}$ act as $A_1, \ldots, A_m$ (resp. $A'_1, \ldots, A'_m$). If $\mathcal{A}$ does not contain the identity matrix then we replace $\mathcal{A}$ by $\mathcal{A} \oplus \mathbb{F}I_{2n}$. Then V and V' are unital $\mathcal{A}$-modules.

Our goal is to find flags of submodules $0 = V_0 < V_1 < \ldots < V_s = V$ and $0 = V'_0 < V'_1 < \ldots < V'_t = V'$, a nilpotent ideal J of $\mathcal{A}$, as well as left ideals $L_1, \ldots, L_r$, such that they satisfy the conditions of Proposition 3.1. We maintain the two flags, the ideal J, and a decomposition $\mathcal{A}$ as the direct sum of left ideals L_i. We represent the decomposition of $\mathcal{A}$ into a direct sum of left ideals by a decomposition of the identity element into a sum of pairwise orthogonal idempotents generating the left ideals.

The algorithm is of a recursive structure. In each iteration, we check the conditions of Proposition 3.1, and update these lists if some of them is violated. We now describe the algorithm.

Initially $J = 0$, $s = t = r = 1$. Then the following conditions will be checked.

1. If JV_i is not contained in V_{i-1}, then insert $JV_i + V_{i-1}$ between V_{i-1} and V_i. The corresponding procedure will be performed, if JV'_i is not contained in JV'_{i-1}.

   Update s to be the length of the subspace flag consisting of V_i's, and t to be that of V'_i's. After this step, in the following we have $\forall i \in [s]$, $JV_i \subseteq V_{i-1}$, and $\forall i \in [t]$, $JV'_i \subseteq V'_{i-1}$.

2. Compute $\mathrm{Hom}(L_i/JL_i, V_j/V_{j-1})$. If it is nonzero, take a nontrivial homomorphism ϕ.

   (a) If ϕ is not surjective, then insert a submodule $V_{j-1} < W < V_j$ such that W/V_{j-1} is the image of ϕ.

   (b) If ϕ is not injective, then its kernel corresponds to a left ideal L which sits properly between L_i and JL_i.

      i. If L is nilpotent, then we replace J with the two-sided ideal generated by $L + J$.

      ii. If L is not nilpotent, then we find a nonzero idempotent e in L as follows.
      Any basis for L contains a non-nilpotent element a (see [IQ19, Fact 2.2]). Take such an a. Then for sufficiently large $\ell \leq 2n$, the minimal polynomial $g(X)$ of $b = a^\ell$ has zero constant term (as a is a zero divisor in $\mathcal{A}$) but nonzero linear term αX. Let $e(X) = (\alpha X)^{-1}(g(X) - \alpha X)$. Then $e(b)b = b$ and hence $f = e(b)$ is a nonzero idempotent. Now we refine the decomposition of $\mathcal{A}$ as follows.
      Assume that L_i is generated by the idempotent e, i.e., $L_i = \mathcal{A}e$. Then $fe = f$. Also, $(ef)^2 = efef = eff = ef$, thus ef is also an idempotent from L. It is nonzero as $fef = ff = f$. We also have $efe = ef$ and $eef = ef$, thus is we replace f with ef (if not already equal) we achieve $ef = f = fe$. Then $(e - f)^2 = ee - ef - fe + ff = e - f - f + f = e - f$, thus $e - f$ is also an idempotent. It is nonzero as f is in a left ideal strictly smaller than $L_i = \mathcal{A}e$. We have $f(e - f) = fe - ff = f - f = 0$ and $(e - f)f = ef - ff = f - f = 0$. Therefore, we can refine the the decomposition of the identity element by replacing e with $f + (e - f)$ and L_i with $\mathcal{A}f$ and $\mathcal{A}(e - f)$.

   We also compute $\mathrm{Hom}(L_i/JL_i, V'_j/V'_{j-1})$ and perform the above operations.

3. If the list of J, L_i, and the two submodule flags is not updated after steps 1 and 2, then terminate. Otherwise, go back to step 1.

Note that the above procedure uses only basic arithmetic operations over $\mathbb{F}$. To bound the running time of this procedure, first note that the number of iterations is bounded by the product of the number of left ideals, the numbers of subspaces in the flags, and the dimension of the nilpotent ideal J. These numbers are upper bounded by $\dim(\mathcal{A})$, $\dim(V)$, and $\dim(V')$. In each iteration, the number of arithmetic operations is also seen to be bounded by $\mathrm{poly}(\dim(\mathcal{A}), \dim(V), \dim(V'))$.

After the above operations, Proposition 3.1 becomes applicable. It remains to construct the one-parameter subgroups that replace V with the direct sum of the factors V_i/V_{i-1} and V' with the direct sum of the factors V'_i/V'_{i-1}, and finally check isomorphism of these sums (and compute one between them) by Theorem 2.1. We remark that in the case of isomorphism, it is necessary that $s = t$ and the isomorphisms between the L_i/JL_i and the factors in the two flags can be used to build up an isomorphism between the two sums.

4 The algorithm for the left-right action

4.1 An algebraic criterion As in the conjugation case, for the left-right action on matrix tuples, we also need an algebraic criterion for two matrix tuples to be in the same orbit closure.

Nullcones of the left-right action. Consider the left-right action of $\mathrm{SL}(\ell,\mathbb{F}) \times \mathrm{SL}(n,\mathbb{F})$ on $\mathrm{M}(\ell \times n,\mathbb{F})^m$, and suppose $\ell \geq n$. Recall that $\mathbf{A} \in \mathrm{M}(\ell \times n,\mathbb{F})^m$ is in the nullcone if its orbit closure contains the zero matrix tuple. By [BD06, Theorem 1], $\mathbf{A}$ is in the nullcone if and only if there exists an invariant subspace pair (U, V) such that $\dim(U)/\dim(V) < \ell/n$. In this case, a one-parameter subgroup λ that drives $\mathbf{A}$ to $\mathbf{0}$ can be devised as follows. Let $\dim(U) = t$ and $\dim(V) = s$. Let U' be a complement of U in $\mathbb{F}^\ell$, and V' a complement of V in $\mathbb{F}^n$. Then set $a_1 = \ell(n-s)$, $a_2 = -\ell s$, $b_1 = n(\ell - t)$, and $b_2 = -nt$. Let A be the one parameter subgroup of $\mathrm{SL}(n,\mathbb{F})$ with weights a_1 on V and a_2 on V'. Let B be the one parameter subgroup of $\mathrm{SL}(\ell,\mathbb{F})$ with weights b_1 on U and b_2 on U'. As shown in [BD06], it can be verified that (A, B) drives $\mathbf{A}$ to 0.

Invariant subspace pairs. Suppose $\mathbf{A} = (A_1, \ldots, A_m) \in \mathrm{M}(\ell \times n,\mathbb{F})^m$ is not in the nullcone of the left-right action. Then we say that (U, V), $U \leq \mathbb{F}^\ell, V \leq \mathbb{F}^n$, is an *invariant subspace pair* of $\mathbf{A}$, if (1) $\dim(U)/\dim(V) = \ell/n$, and (2) for any $i \in [m]$, $A_i(V) \leq U$. If the only invariant subspace pairs of $\mathbf{A}$ are $(\mathbb{F}^\ell, \mathbb{F}^n)$ and $(0, 0)$, then $\mathbf{A}$ is called *stable*. Clearly, $\mathbf{A}$ is not stable if and only if there exist $C \in \mathrm{GL}(\ell,\mathbb{F})$ and $D \in \mathrm{GL}(n,\mathbb{F})$, such that $C^{-1}\mathbf{A}D = (\tilde{A}_1, \ldots, \tilde{A}_m)$, and every $\tilde{A}_i = \begin{bmatrix} A_{i,1} & A_{i,2} \\ 0 & A_{i,3} \end{bmatrix}$, where $A_{i,1}$ is of size $j \times k$ for $j \in [\ell - 1]$ and $k \in [n - 1]$, and $j/k = \ell/n$.

Invariant subspace flag pairs. Suppose $\mathbf{A} = (A_1, \ldots, A_m) \in \mathrm{M}(\ell \times n,\mathbb{F})^m$ is not in the nullcone of the left-right action. An *invariant subspace flag pair* consists of flags $0 = U_0 < U_1 < \cdots < U_b = \mathbb{F}^\ell$ and $0 = V_0 < V_1 < \cdots < V_b = \mathbb{F}^n$, such that for any $i \in [b]$, (U_i, V_i) is a invariant subspace pair. Suppose for $i \in [b]$, $\dim(U_i) - \dim(U_{i-1}) = d_i$, and $\dim(V_i) - \dim(V_{i-1}) = e_i$. Then there exists $C, D \in \mathrm{GL}(n,\mathbb{F})$, such that $C^{-1}\mathbf{A}D = (\tilde{A}_1, \ldots, \tilde{A}_m)$, and every $\tilde{A}_i = \begin{bmatrix} A_{1,i} & * & * & \ldots & * \\ 0 & A_{2,i} & * & \ldots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & A_{b,i} \end{bmatrix}$, where $A_{j,i}$ is of size $d_j \times e_j$. Let $\mathbf{A}_j = (A_{j,1}, \ldots, A_{j,m}) \in \mathrm{M}(d_j,\mathbb{F})^m$. Set $\hat{A}_i = \begin{bmatrix} A_{1,i} & 0 & 0 & \ldots & 0 \\ 0 & A_{2,i} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & A_{b,i} \end{bmatrix}$. Let $\hat{\mathbf{A}} = (\hat{A}_1, \ldots, \hat{A}_m) \in \mathrm{M}(n,\mathbb{F})^m$. The following result is the analogue of Lemma 3.1 in the left-right action setting.

LEMMA 4.1. *Let $\mathbf{A} \in \mathrm{M}(\ell \times n,\mathbb{F})^m$ and let $\hat{\mathbf{A}}$ be the block diagonal part constructed as above for an invariant subspace pair flag. Let $\lambda : \mathbb{F}^\times \to \mathrm{GL}(\ell,\mathbb{F}) \times \mathrm{GL}(n,\mathbb{F})$ be the one-parameter subgroup defined by sending t to*

$$(D(t), E(t)) := \left(\begin{bmatrix} D_1 & 0 & 0 & \ldots & 0 \\ 0 & D_2 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & D_b \end{bmatrix}, \begin{bmatrix} E_1 & 0 & 0 & \ldots & 0 \\ 0 & E_2 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & E_b \end{bmatrix} \right),$$

where $D_j = \mathrm{diag}(t^{a_j}, \ldots, t^{a_j})$ is of size $d_j \times d_j$ and $a_j = \sum_{i>j} d_i - \sum_{i<j} d_i$, and $E_j = \mathrm{diag}(t^{b_j}, \ldots, t^{b_j})$ and $b_j = \sum_{i>j} e_i - \sum_{i<j} e_i$. Then $\hat{\mathbf{A}} = \lim_{t\to 0} D(t)^{-1}\mathbf{A}E(t)$.

If every $\mathbf{A}_j$, $j \in [b]$, is stable, then the pair of flags $(U_0 = 0 < U_1 < \cdots < U_b = \mathbb{F}^n, 0 = V_0 < V_1 < \cdots < V_b = \mathbb{F}^n)$ is called a *fully-refined invariant subspace flag pair*. Then $\hat{\mathbf{A}}$ is called a *closed matrix tuple* associated with $\mathbf{A}$. The term closed is justified by Theorem 4.1.

It is easy to verify that for a given fully-refined invariant subspace flag pair, two different closed matrix tuples associated with $\mathbf{A}$ are in the same orbit under the left-right action. Furthermore, closed matrix tuples arising from different fully-refined invariant subspace flags are also in the same orbit under the left-right action.

The algebraic criterion for the left-right action. The following analogue of Artin's criterion for the left-right action is classical and can be found in e.g. [Shm07].

THEOREM 4.1. ([SHM07]) *Suppose $\mathbf{A}, \mathbf{B} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$ are not in the nullcone of the left-right action, and let $\hat{\mathbf{A}}$ and $\hat{\mathbf{B}}$ be closed matrix tuples associated with $\mathbf{A}$ and $\mathbf{B}$, respectively. Then $\overline{\mathrm{O_{lr}}}(\mathbf{A})$ intersects $\overline{\mathrm{O_{lr}}}(\mathbf{B})$ if and only if $\hat{\mathbf{A}}$ and $\hat{\mathbf{B}}$ are in the same orbit under the left-right action.*

4.2 The orbit closure algorithm In this section we present the orbit closure algorithm for the left-right action.

Blow-ups. Let $\mathbf{A} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$ be a matrix tuple. For $r, s \in \mathbb{N}$, and $j \in [r], k \in [s]$, $E_{j,k} \in \mathrm{M}(r \times s, \mathbb{F})$ is the elementary matrix with the (j,k)th entry being 1, and other entries being 0. The $r \times s$-blowup $\mathbf{A}^{(r\times s)}$ of $\mathbf{A}$ is the matrix tuple $(A_i \otimes E_{j,k})_{i\in[m],j\in[r],k\in[s]} \in \mathrm{M}(\ell r \times ns, \mathbb{F})^{mrs}$, where (i,j,k) is arranged in the lexicographic order. Note that each $A_i \otimes E_{j,k}$ is a $r \times s$ block matrix, where each block is of size $\ell \times n$, there exists exactly one block being A_i, and the other blocks are all 0.

LEMMA 4.2. *Let $\mathbf{A}$ and $\mathbf{A}^{(r\times s)}$ be as above. For $U \leq \mathbb{F}^\ell$,$V \leq \mathbb{F}^n$, if $\mathbf{A}V \leq U$ then $\mathbf{A}^{(r\times s)}V \otimes \mathbb{F}^s \leq U \otimes \mathbb{F}^r$. Conversely, if for $U \leq \mathbb{F}^\ell \otimes \mathbb{F}^r$, $V \leq \mathbb{F}^n \otimes \mathbb{F}^s$ we have $\mathbf{A}^{(r\times s)}V \leq U$ there exist subspaces $\hat{U} \leq \mathbb{F}^\ell$, $\hat{V} \leq \mathbb{F}^n$ such that $\mathbf{A}\hat{V} \leq \hat{U}$ and that $\hat{U} \otimes F^r \leq U$ and $V \leq \hat{V} \otimes F^s$.*

In words, common zero blocks for $\mathbf{A}$ are "blown up" to common zero blocks of $\mathbf{A}^{(r\times s)}$ and maximal common zero blocks of $\mathbf{A}^{(r\times s)}$ arise from maximal common zero blocks of $\mathbf{A}$.

Proof. The first statement is obvious. The second statement follows from the fact that the linear span of $\mathbf{A}^{(r\times s)}$ is closed under the left-right action of $(C, D) \in \mathrm{GL}(r, \mathbb{F}) \times \mathrm{GL}(s, \mathbb{F})$ by $(I_\ell \otimes C, I_n \otimes D)$. ∎

We remark that $\hat{U}$ and $\hat{V}$ as int the second statement of the lemma can be efficiently computed given U and V.

A consequence of Lemma 4.2 is the following.

LEMMA 4.3. *Let $\mathbf{A} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$. Then $\mathbf{A}$ is in the nullcone of the left-right action of $\mathrm{SL}(\ell, \mathbb{F}) \times \mathrm{SL}(n, \mathbb{F})$ if and only if $\mathbf{A}^{(r\times s)}$ is in the nullcone of the left-right action of $\mathrm{SL}(\ell r, \mathbb{F}) \times \mathrm{SL}(ns, \mathbb{F})$. If $\mathbf{A}$ is not in the nullcone then $(U, V) \mapsto (U \otimes \mathbb{F}^s, V^{\otimes}\mathbb{F}^r)$ gives a bijection of invariant subspace pairs of $\mathbf{A}$ and those of $\mathbf{A}^{(r\times s)}$. This map induces a one-to-one correspondence between fully refined subspace pairs.*

For "non-singular" square blowups we have the following counterpart for the orbits.

LEMMA 4.4. *Let q be a common multiple of n and ℓ. Assume that the span of $\mathbf{A}^{(q/\ell\times q/n)}$ contains an invertible q by q matrix and that $(X_1, X_2) \in \mathrm{GL}(q, \mathbb{F}) \times \mathrm{GL}(q, \mathbb{F})$ satisfies $\mathbf{B}^{(q/\ell\times q/n)} = X_1\mathbf{A}^{(q/\ell\times q/n)}X_2^{-1}$ for some $\mathbf{B} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$. Then there exists $(Y_1, Y_2) \in \mathrm{GL}(\ell, \mathbb{F}) \times \mathrm{GL}(n, \mathbb{F})$ such that $X_1 = Y_1 \otimes I_{q/\ell}$ and $X_2 = Y_2 \otimes I_{q/n}$.*

Proof. Choose a nonsingular linear combination C of the entires of $\mathbf{A}^{(q/\ell\times q/n)}$ and let C' be combination of the entries of $\mathbf{B}^{(q/\ell\times q/n)}$ with the same coefficients. Then $C' = X_1CX_2^{-1}$ is also invertible with $C'^{-1} = X_2C^{-1}X_1^{-1}$. We have $C'^{-1}\mathbf{B}^{(q/\ell\times q/n)} = X_2C^{-1}\mathbf{A}^{(q/\ell\times q/n)}X_2^{-1}$. The linear span of $\mathbf{A}^{(q/\ell\times q/n)}$ is closed under multiplication by matrices from $I_n \otimes \mathrm{M}(q/n, \mathbb{F})$ from the right, therefore for any matrix $Z \in \mathrm{M}(q/n, \mathbb{F})$ we can express $I_n \otimes Z$ as a linear combination of the entries of the tuple $C^{-1}\mathbf{A}^{(q/\ell\times q/n)}$ with coefficients depending on Z. But in the same vein, $I_n \otimes Z$ appears as a linear combination of the tuple $C'^{-1}\mathbf{B}^{(q/\ell\times q/n)}$ with the same coefficients, and hence $X_2I_n \otimes ZX_2^{-1} = I_n \otimes Z$. It readily follows that X_2 must be of the form $Y_2 \otimes I_{q/n}$. The analogous argument, applied to $\hat{\mathbf{B}}^{(q/\ell\times q/n)}C'^{-1} = X_1\hat{\mathbf{A}}^{(q/\ell\times q/n)}C^{-1}X_1^{-1}$, shows that X_1 is of the form $Y_1 \otimes I_{q/\ell}$. ∎

LEMMA 4.5. *Let $\mathbf{A}, \mathbf{B} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$ outside the nullcone of the left-right action. Then $\overline{\mathrm{O_{lr}}}(\mathbf{A}) \cap \overline{\mathrm{O_{lr}}}(\mathbf{B}) \neq \emptyset$ if and only if $\overline{\mathrm{O_{lr}}}(\mathbf{A}^{(r\times s)}) \cap \overline{\mathrm{O_{lr}}}(\mathbf{B}^{(r\times s)}) \neq \emptyset$.*

Proof. Assume they are not in the nullcone. Let q be a common multiple of ℓr and ns such that the span of $\mathbf{A}^{(q/\ell,q/n)}$ contains a nonsingular matrix. Apply Theorem 4.1 and Lemmas 4.3 and 4.4 to show the statement between the pairs $(\mathbf{A}, \mathbf{B})$ and $(\mathbf{A}^{(q/\ell,\times q/n)}, \mathbf{B}^{(q/\ell\times q/n)})$ and similarly show the statement between $(\mathbf{A}^{(r\times s)}, \mathbf{B}^{(r\times s)})$ and $(\mathbf{A}^{(q/\ell\times q/n)}, \mathbf{B}^{(q/\ell\times q/n)})$. ∎

The algorithm: the starting point. Given $\mathbf{A}, \mathbf{B} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$, we wish to determine if their orbit closures under the left-right action intersect. Let p be the least common multiple of ℓ and n.

The starting point of the algorithm is to use the algorithm in [IQS17, IQS18] which decides the nullcone memberships of $\mathbf{A}$ and $\mathbf{B}$. More specifically, we apply the algorithm to $\mathbf{A}^{(p/\ell \times p/n)}$ and $\mathbf{B}^{(p/\ell \times p/n)}$.

For $\mathbf{A}^{(p/\ell \times p/n)}$, the algorithm has two possible outputs.

- Either it returns an invertible matrix in the linear span of $\mathbf{A}^{(q/\ell \times q/n)}$ for some common multiple q of ℓ and n, and $q \leq p^2$.
- Or it returns $U, V \leq \mathbb{F}^p$, $\dim(U) < \dim(V)$, such that every $A \in \mathbf{A}^{(p/\ell \times p/n)}$ sends V to U. This pair (U, V) can then be used to construct $(\hat{U}, \hat{V})$ where $\hat{U} \leq \mathbb{F}^\ell, \hat{V} \leq \mathbb{F}^n$, $\dim(\hat{U})/\dim(\hat{V}) < \ell/n$, such that every $\hat{A} \in \mathbf{A}$ sends V to U. Note that in this case $\mathbf{A}$ is in the nullcone of the left-right action.

Similarly this holds for $\mathbf{B}^{(p/\ell \times p/n)}$.

If one of $\mathbf{A}$ and $\mathbf{B}$ is in the nullcone while the other is not, then we report that their orbit closures do not intersect.

If both of them are in the nullcone, then we can make use of the subspace pairs output by the algorithm, and Lemma 4.1, to get the desired one-parameter subgroups driving them to the 0 matrix tuple.

The more difficult case is when neither of them is in the nullcone, which will be dealt with in the following part.

Neither of the input matrix tuples is in the nullcone. Recall that we have $\mathbf{A}, \mathbf{B} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$, $p = \mathrm{lcm}(\ell, n)$, and $q \leq p^2$ which is also a common multiple of ℓ and n. The algorithm in [IQS17, IQS18] also gives us an invertible matrix $S \in \mathrm{span}(\mathbf{A}^{(q/\ell \times q/n)})$. To be more specific, put $r = mq^2/(\ell n)$ and assume that $\mathbf{A}^{(q/\ell \times q/n)} = (A'_i)_{i=1,\ldots,r}$ and $\mathbf{B}^{(q/\ell \times q/n)} = (B'_i)_{i=1,\ldots,r}$. Then we obtain an array $(\alpha_1, \ldots, \alpha_r) \in \mathbb{F}^r$ such that $S = \sum_{i=1}^r \alpha_i A'_i$ is an r by r matrix of determinant $\Delta \neq 0$. Put $T = \sum_{i=1}^r \alpha_i B'_i$. If $\det T \neq \Delta$ then we have separated $\mathbf{A}$ and $\mathbf{B}$ by a semi-invariant and can conclude their orbit closures are disjoint.

Assume that $\det T = \Delta = \det S$. We adopt an idea from [DM20] to make use of S and T to reduce to the conjugation case.

A combination of Lemma 4.5 with Corollary 3.3 of [DM20] gives that the closure of the orbits of $\mathbf{A}$ and $\mathbf{B}$ under the left-right action intersect if and only if the orbits of $S^{-1}\mathbf{A}^{(q/\ell \times q/n)})$ and $T^{-1}\mathbf{B}^{(q/\ell \times q/n)})$ under the conjugation action of $\mathrm{SL}(r, \mathbb{F})$ intersect. We remark that we need here the (easy) "only if" part and for the "if" part we give below a sort of contructive proof that computes one-parameter subgroups driving from the tuples to the intersection of the orbit closures.

We apply the algorithm in Section 3 for the conjugation action to $S^{-1}\mathbf{A}^{(q/\ell \times q/n)}$ and $T^{-1}\mathbf{B}^{(q/\ell \times q/n)}$. This produces flags $0 = U_0 < U_1 < \cdots < U_b = \mathbb{F}^q$ and $0 = V_0 < V_1 < \cdots < V_b = \mathbb{F}^q$, such that the factors add up to isomorphic modules for the common enveloping algebra. Note that the two modules V and V' are already unital so there is no need to add the identity matrix artificially as $S^{-1}S = T^{-1}T = I_q$. Now (U_i, SU_i) and (V_i, TV_i) are invariant subspace pairs for $\mathbf{A}^{(q/\ell \times q/n)}$ and $\mathbf{B}^{(q/\ell \times q/n)}$, respectively. We obtain invariant subspace pairs for the original $\mathbf{A}$ and using Lemma 4.3 to form $\mathbb{F}^{q/n} \otimes \hat{U}_i$ and $\mathbb{F}^{q/n} \otimes \hat{V}_i$, where $\hat{U}_i, \hat{V}_i \leq \mathbb{F}^n$. Let $\tilde{U}_i = \mathbf{A}(\hat{U}_i)$ and $\tilde{V}_i = \mathbf{B}(\hat{V}_i)$. Lemma 4.1 can be used for computing $\hat{\mathbf{A}}$ (resp. $\hat{\mathbf{B}}$) in the orbit closure of $\mathbf{A}$ (resp. $\mathbf{B}$).

Now $\hat{\mathbf{A}}^{(q/\ell \times q/n)}$ lies in the orbit of $\hat{\mathbf{B}}^{(q/\ell \times q/n)}$. We then compute pair $(X_1, X_2) \in \mathrm{GL}(q, \mathbb{F}) \times \mathrm{GL}(q, \mathbb{F})$ such that $\hat{\mathbf{B}}^{(q/\ell \times q/n)} = X_1 \hat{\mathbf{A}}^{(q/\ell \times q/n)} X_2^{-1}$ and apply Lemma 4.4 to get $(Y_1, Y_2) \in \mathrm{GL}(\ell, \mathbb{F}) \times \mathrm{GL}(n, \mathbb{F})$ such that $\hat{\mathbf{B}} = Y_1 \hat{\mathbf{A}} Y_2^{-1}$.

Note that to be fully constructive over $\mathrm{SL}(n, \mathbb{F}) \times \mathrm{SL}(n, \mathbb{F})$, one may need to take ℓth and nth roots of elements of $\mathbb{F}$.

Finally, we remark that the above reduction, combined with Theorem 3.2, gives the following.

THEOREM 4.2. *Let $\mathbb{K}$ be an algebraic number field or a finite field and let $\mathbb{F}$ be an algebraically closed extension field of $\mathbb{K}$. Given a matrix tuple $\mathbf{A} \in \mathrm{M}(\ell \times n, \mathbb{K})^m$, a tuple $\hat{\mathbf{A}} \in \mathrm{M}(\ell \times n, \mathbb{K})^m$ that is in the orbit of $\mathrm{SL}(\ell, \mathbb{F}) \times \mathrm{SL}(n, \mathbb{F})$ of a closed matrix tuple associated with $\mathbf{A}$ over $\mathbb{F}$ can be computed in deterministic polynomial time. The algorithm also returns a one-parameter subgroup of $\mathrm{SL}(\ell, \mathbb{F}) \times \mathrm{SL}(n, \mathbb{F})$ defined over $\mathbb{K}$ driving $\mathbf{A}$ to $\hat{\mathbf{A}}$.*

Acknowledgments. The research of the first author was supported by the Hungarian Ministry of Innovation and Technology NRDI Office within the framework of the Artificial Intelligence National Laboratory Program. The research of the second author was partly supported by the Australian Research Council DP200100950.

References

[AB95] J.L. Alperin and R.B. Bell. *Groups and representations*. Graduate texts in mathematics. Springer, 1995.

[Art69] Michael Artin. On azumaya algebras and finite dimensional representations of rings. *Journal of Algebra*, 11(4):532–563, 1969.

[AZGL+18] Zeyuan Allen-Zhu, Ankit Garg, Yuanzhi Li, Rafael Oliveira, and Avi Wigderson. Operator scaling via geodesically convex optimization, invariant theory and polynomial identity testing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 172–181, 2018.

[BD06] M. Bürgin and J. Draisma. The Hilbert null-cone on tuples of matrices and bilinear forms. *Mathematische Zeitschrift*, 254(4):785–809, 2006.

[BFG+19] Peter Bürgisser, Cole Franks, Ankit Garg, Rafael Mendes de Oliveira, Michael Walter, and Avi Wigderson. Towards a theory of non-commutative optimization: Geodesic 1st and 2nd order methods for moment maps and polytopes. In David Zuckerman, editor, *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019, Baltimore, Maryland, USA, November 9-12, 2019*, pages 845–861. IEEE Computer Society, 2019.

[BGdO+18] Peter Bürgisser, Ankit Garg, Rafael Mendes de Oliveira, Michael Walter, and Avi Wigderson. Alternating minimization, scaling algorithms, and the null-cone problem from invariant theory. In Anna R. Karlin, editor, *9th Innovations in Theoretical Computer Science Conference, ITCS 2018, January 11-14, 2018, Cambridge, MA, USA*, volume 94 of *LIPIcs*, pages 24:1–24:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.

[BIL+21] Markus Bläser, Christian Ikenmeyer, Vladimir Lysikov, Anurag Pandey, and Frank-Olaf Schreyer. On the orbit closure containment problem and slice rank of tensors. In Dániel Marx, editor, *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms, SODA 2021, Virtual Conference, January 10 - 13, 2021*, pages 2565–2584. SIAM, 2021.

[BL08] Peter A. Brooksbank and Eugene M. Luks. Testing isomorphism of modules. *Journal of Algebra*, 320(11):4020 – 4029, 2008.

[CIK97] Alexander Chistov, Gábor Ivanyos, and Marek Karpinski. Polynomial time algorithms for modules over finite dimensional algebras. In *Proceedings of the 1997 international symposium on Symbolic and algebraic computation*, ISSAC '97, pages 68–74, New York, NY, USA, 1997. ACM.

[CIW97] Ajeh M Cohen, Gábor Ivanyos, and David B Wales. Finding the radical of an algebra of linear transformations. *Journal of Pure and Applied Algebra*, 117:177–193, 1997.

[CT15] Iuliana Ciocănea-Teodorescu. The module isomorphism problem for finite rings and related results. *ACM Commun. Comput. Algebra*, 49(1):14, 2015.

[DM17] Harm Derksen and Visu Makam. Polynomial degree bounds for matrix semi-invariants. *Advances in Mathematics*, 310:44–63, 2017.

[DM20] Harm Derksen and Visu Makam. Algorithms for orbit closure separation for invariants and semi-invariants of matrices. *Algebra & Number Theory*, 14(10):2791–2813, 2020.

[FS13] Michael A Forbes and Amir Shpilka. Explicit noether normalization for simultaneous conjugation via polynomial identity testing. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 527–542. Springer, 2013.

[GGdOW16] Ankit Garg, Leonid Gurvits, Rafael Mendes de Oliveira, and Avi Wigderson. A deterministic polynomial time algorithm for non-commutative rational identity testing. In *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA*, pages 109–117, 2016.

[GIM+20] Ankit Garg, Christian Ikenmeyer, Visu Makam, Rafael Mendes de Oliveira, Michael Walter, and Avi Wigderson. Search problems in algebraic complexity, gct, and hardness of generators for invariant rings. In Shubhangi Saraf, editor, *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*, volume 169 of *LIPIcs*, pages 12:1–12:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[HH21] Masaki Hamada and Hiroshi Hirai. Computing the nc-rank via discrete convex optimization on CAT (0) spaces. *SIAM J. Appl. Algebra Geom.*, 5(3):455–478, 2021.

[Hil90] David Hilbert. Ueber die theorie der algebraischen formen. *Mathematische annalen*, 36(4):473–534, 1890.

[IKS10] Gábor Ivanyos, Marek Karpinski, and Nitin Saxena. Deterministic polynomial time algorithms for matrix completion problems. *SIAM J. Comput.*, 39(8):3736–3751, 2010.

[IMQ22] Gábor Ivanyos, Tushant Mittal, and Youming Qiao. Symbolic determinant identity testing and non-commutative ranks of matrix lie algebras. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 87:1–87:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[IQ19] Gábor Ivanyos and Youming Qiao. Algorithms based on *-algebras, and their applications to isomorphism of polynomials with one secret, group isomorphism, and polynomial identity testing. *SIAM Journal on Computing*, 48(3):926–963, 2019.

[IQS17] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Non-commutative edmonds' problem and matrix semi-invariants. *computational complexity*, 26(3):717–763, Sep 2017.

[IQS18] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *computational complexity*, 27(4):561–593, Dec 2018.

[KI04] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1/2):1–46, 2004.

[LQW+22] Yinan Li, Youming Qiao, Avi Wigderson, Yuval Wigderson, and Chuanqi Zhang. Connections between graphs and matrix spaces. *CoRR*, abs/2206.04815, 2022.

[MFK94] David Mumford, John Fogarty, and Frances Kirwan. *Geometric invariant theory*. Springer-Verlag, 1994.

[Mul17] Ketan Mulmuley. Geometric complexity theory V: Efficient algorithms for Noether normalization. *Journal of the American Mathematical Society*, 30(1):225–309, 2017.

[MW21] Visu Makam and Avi Wigderson. Singular tuples of matrices is not a null cone (and the symmetries of algebraic varieties). *J. Reine Angew. Math.*, 780:79–131, 2021.

[Pie82] Richard S. Pierce. *Associative algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982. Studies in the History of Modern Science, 9.

[Rón90] Lajos Rónyai. Computing the structure of finite algebras. *J. Symb. Comput.*, 9(3):355–373, 1990.

[Shm07] D. Shmelkin. Locally semi-simple representations of quivers. *Transformation Groups*, 12(1):153–173, 2007.