Fixed-Parameter Degree Bounds and Complexity of the Orbit Closure Intersection Problem for Tensors

M. Levent Doğan
LMU Munich, Germany

John Maar
Technical University Berlin, Germany

Rafael Oliveira
University of Waterloo, Canada

Youming Qiao
University of Technology Sydney, Australia

Abstract

The orbit closure intersection problem for a reductive group action is a geometric relaxation of the orbit equality problem. These problems capture a range of isomorphism, degeneration and identity-testing problems in computational complexity. We study this problem for the tensor action of $G = \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_m(\mathbb{K})$ on $\mathcal{V} = \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$ (equivalently, on m-tuples of $n \times n$-matrices) where the base field is algebraically closed with characteristic zero.

We focus on the fixed-parameter regime where m is constant and n is allowed to grow. The case of $m = 3$ is already interesting in the context of tensor rank and matrix multiplication. Prior to our work, only a special case of this problem, namely when one of the input tensors is the zero-tensor (this corresponds to the null cone problem for the tensor action), was known to be solvable in polynomial time (Bürgisser–Franks–Garg–Oliveira–Walter–Wigderson, *FOCS*'19).

Our main result is to show that the orbit closure intersection problem for the above action can be solved in randomized polynomial time. This is achieved by the following new ingredients:

1. We prove an explicit fixed-parameter bound on the degrees needed to generate the invariant ring for the tensor action: for every fixed m, these bounds are polynomial in n.
2. We prove that there is a succinct encoding of the invariants: we construct a uniform, polynomial-sized arithmetic circuit generating all invariants up to the required degree.

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory; Computing methodologies → Algebraic algorithms

Keywords and phrases computational invariant theory, geometric complexity theory, orbit closure intersection problem

Digital Object Identifier 10.4230/LIPIcs.CCC.2026.32

Funding *M. Levent Doğan*: The author was funded by European Union (ERC Grant SYMOPTIC, 101040907) and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, 556164098).
John Maar: The author was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, 556164098).
Youming Qiao: Youming's research is partly supported by ARC LP220100332.

Acknowledgements The authors are grateful to Peter Bürgisser for valuable discussions during the Simons Program. This work started while the authors were supported by the Simons Institute for the Theory of Computing, and conducted when the authors were visiting the Institute. The authors would like to thank the generosity, hospitality, and excellent research environment provided by the Simons Institute.

1 Introduction

Several decision problems in complexity theory ask whether two given objects are equivalent up to a given set of transformations. For many of these problems, these transformations are captured by the action of a group G on a set $\mathcal{V}$, and the equivalence question becomes the orbit problem for this action, which asks whether $u, v \in \mathcal{V}$ are *equivalent* under the action of the group G, that is, whether u and v are in the same orbit. For instance, a flagship problem in this family is the graph isomorphism problem, which asks whether two graphs are the same up to permuting the vertices. Other examples of orbit problems are the equivalence of quiver representations [16, 17], classification of quantum states under LOCC and SLOCC operations [3, 4, 13], ring/algebra/module isomorphism [38, 6, 25], tensor isomorphism [27, 28, 29], linear code equivalence [47] and group isomorphism [26].

When the group G and the set $\mathcal{V}$ admit a natural geometric structure, a geometric version of the orbit problem is the orbit closure intersection problem, which asks whether the topological (Zariski) closures of the orbits of $u, v \in \mathcal{V}$ intersect. Orbit closure intersection, together with its important special case – the null cone problem with one of the vectors is taken to be the zero vector – has its origins in invariant theory, tracing back to the celebrated work of Hilbert on the finite generation of invariant rings for reductive groups [31, 32], and Mumford's development of geometric invariant theory [43].

In computational complexity, the algorithmic study of orbit closure intersection problems was largely motivated by algebraic complexity theory. In [33], Hrubeš and Wigderson discovered a close relation between non-commutative rational identity testing and the null cone problem for the left-right action on matrix tuples. This connection has led to the development and rigorous analysis of polynomial time algorithms, via invariant theory, for the rational identity testing problem [23, 36]. Another connection comes from a closely related problem, the orbit closure containment problem, which asks whether the orbit closure of u is contained in the orbit closure of v. Orbit closure containment problems encompass (geometric strengthenings of) major problems in algebraic complexity theory, including the algebraic complexity of matrix multiplication [12] and the VP vs VNP problem [42]. In [41], Mulmuley proposed the succinct encoding framework for invariant rings and presented a general methodology for using polynomial identity testing to devise algorithms for orbit closure intersection problems.

Before proceeding further, we formally introduce the orbit closure intersection problem.

▶ **Problem 1** (Orbit Closure Intersection). *The **Orbit Closure Intersection (OCI)** problem is defined as follows: given as input an action of a linearly reductive group G on the vector space $\mathcal{V}$[1] and two vectors $u, v \in \mathcal{V}$, decide whether $\overline{G \cdot u} \cap \overline{G \cdot v} \neq \emptyset$.*

▶ Remark 2. When $v = 0$ in Problem 1, the Orbit Closure Intersection problem is known as the **null cone** problem: decide if $0 \in \overline{G \cdot u}$.

In the past decade, progress was made on the various instances of the orbit closure intersection problem. Notable examples where a polynomial time algorithm is available are the orbit closure intersection problem for matrix tuples under simultaneous conjugation [21, 17], under the left-right action [2, 17, 34], as well as the action of a product of general linear groups on quiver representations, the actions of tori [9, 10], and when the group G is fixed [41].

[1] We will assume in this paper that the group action belongs to a parameterized family of group actions, such as the left-right action of $\mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K})$ on $\mathrm{Mat}(n, \mathbb{K})^{\oplus m}$, with the action is specified by the input parameter, e.g. by the pair (n, m) for the left-right action.

Since they play an important role in this work, we recall that the left-right action of $(g, h) \in \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K})$ sends a matrix tuple $(A_1, \ldots, A_m) \in \mathrm{Mat}(n, \mathbb{K})^m$ to $(gA_1h^T, \ldots, gA_mh^T)$. Here, and in the rest of the paper, $\mathbb{K}$ denotes an algebraically closed field with characteristic zero. The orbit closure intersection problem for this action has intriguing applications in areas such as identity testing non-commutative rational formulas [33] and geometric complexity theory [41], and it naturally generalizes classical combinatorial problems such as the bipartite perfect matching problem and the linear matroid intersection problem [23, 35]. The null cone problem for the left-right action admits three deterministic polynomial-time solutions [23, 36, 30], and so does its orbit closure intersection problem [2, 17, 34]. These results and the algorithmic techniques developed for solving them demonstrate connections between different areas including invariant theory, analysis, optimization, and non-commutative algebra, as seen in the surveys by Bürgisser [7] and Wigderson [49].

After these positive results for various group actions, the next natural and important target is to study tensors with the natural action by direct products of reductive algebraic groups. For example, we consider the action of $\mathrm{SL}_a(\mathbb{K}) \times \mathrm{SL}_b(\mathbb{K}) \times \mathrm{SL}_c(\mathbb{K})$ on the space of tensors $\mathbb{K}^a \otimes \mathbb{K}^b \otimes \mathbb{K}^c$, with its action on the standard basis given by

$$(g, h, k) \cdot e_i \otimes e_j \otimes e_l = (ge_i) \otimes (he_j) \otimes (ke_l), \quad (g, h, k) \in \mathrm{SL}_a(\mathbb{K}) \times \mathrm{SL}_b(\mathbb{K}) \times \mathrm{SL}_c(\mathbb{K}),$$

or the action of $\mathrm{GL}_n(\mathbb{K})$ on a space $\bigoplus_{i=1}^{a} (\mathbb{K}^n)^{\otimes c_i} \oplus \bigoplus_{i=1}^{b} ((\mathbb{K}^n)^*)^{\otimes d_i}$ of tensors.[2] Such actions are important due to their connections and applications to other areas, such as tensor networks in quantum information [1], tensor rank and matrix multiplication [48, 5, 8], cryptography [37], and isomorphism problems for groups and polynomials [27]. Interestingly, the orbit closure intersection problem for these actions appears to be much harder, with evidence from invariant theory [18], algebraic complexity [24], and optimization [22]. The recent result [40, Theorem 1.5] gives a partial explanation, namely the orbit closure intersection problem for the natural $\mathrm{GL}_n(\mathbb{K})$ action on $(\mathbb{K}^n)^{\otimes 2} \oplus (\mathbb{K}^n)^{\otimes 3} \oplus ((\mathbb{K}^n)^*)^{\otimes 2}$, as well as for certain other natural tensor actions, is graph isomorphism hard.

Given these difficulties, it is intriguing to see that the null cone problem for $\mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$ where $m \in O(1)$ is a constant can be solved in deterministic polynomial time [11, Corollary 6.24]. This case is also of great interest in tensor rank and matrix multiplication even for $m = 3$: Strassen proved that certain invariants in $\mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^3$ can be elevated via the substitution method to prove lower bounds for the border rank of the matrix multiplication [48, 5], see also [11, Section 1.7.1]. However, before this work, the orbit closure intersection problem was only known to be in exponential time. Recently, Bürgisser asked if the orbit closure intersection problem admits a deterministic polynomial-time algorithm; see Problem 2.4 in the open problems list from the recent Workshop on Randomness, Invariants, and Complexity at the Simons Institute in 2025. Note that the distinction between null cone and orbit closure intersection could be significant, as already seen in the case of the left-right action on matrix tuples: while the scaling algorithm for the null cone problem does not require invariant-theoretic degree bounds [23], a polynomial degree bound for matrix semi-invariants [16] is necessary for the scaling algorithm for orbit closure intersection [2].

In this paper, our main result is to put the orbit closure intersection problem for the action of $\mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_m(\mathbb{K})$ on $\mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$ where $m = O(1)$ in coRP.

[2] It is important to restrict to unit determinant matrices for the first action, as the orbit closures of two tensors will always intersect at zero under the action of the product of general linear groups.

▶ **Theorem 3.** *The orbit closure intersection problem for the tensor action of* $G := \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_m(\mathbb{K})$ *on* $\mathcal{V} := \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$ *with* $m = O(1)$ *is in* coRP. *More explicitly, given* n *and two vectors* $u, v \in \mathbb{Q}[i]^n \otimes \mathbb{Q}[i]^n \otimes \mathbb{Q}[i]^m$*, there exists a randomized algorithm with one-sided bounded error that decides whether the orbit closures of* u *and* v *intersect in time polynomial in* n *and the bit-lengths of* u *and* v*.*

The above theorem is the main application of our two technical theorems, which we present in Section 1.2, along with a technical overview.

▶ Remark 4. In fact, our results and techniques apply to more general settings, which include the important setting of higher dimensional *rectangular* tensors – i.e., tensors of constantly many sides where all but two dimensions of the tensor factors are constant. However, for ease of exposition, we have decided to present only the above theorem as the main application of our technical results. We provide a more detailed discussion on the generality of our results at the end of Section 1.2.

We now review the literature and previous works.

1.1 Related Work

The orbit closure intersection problem has been studied in certain algorithmically tractable group actions, but the tensor action has so far remained the main frontier for this problem. A key positive case is the left-right action of $\mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K})$ on matrix tuples (equivalently, on $\mathcal{V} = \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$ where the third factor is not acted upon). In this setting, polynomial degree bounds for the generators of the invariant ring are known [16], and they are critical for obtaining efficient algorithms for the orbit closure intersection problem [2, 36, 17].

Another positive regime is when the group $\mathrm{SL}_m(\mathbb{K})$, with constant m, acts on a vector space. In geometric complexity theory, Mulmuley [41] developed the idea of "succinct encoding" framework for invariant rings, and constructed explicit generating invariants for $\mathrm{SL}_m(\mathbb{K})$-actions that enable randomized polynomial time algorithms for the orbit closure intersection problem.

In contrast, the complexity of OCI seems to drastically change when we consider the action of $\mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K})$ on $\mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^n$, where n varies. While no explicit hardness result for OCI is known, several lines of work show limitations of the current techniques. An indication of hardness from invariant theory comes from [18], where the authors proved exponential lower bounds for the degrees of the generators for the action of $\mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K})$ on $(\mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^n)^{\oplus 9}$. This result highlights that the generation in low degree may fail once all dimensions are allowed to vary.

Even in the setting where degree bounds are not the main obstacle, succinct encoding of the invariants may fail: [24] showed (under standard complexity theoretic assumptions) that for certain (torus) actions on $\mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$, no polynomial-sized encoding of the invariants exists, placing a further limitation in this setting.

The optimization approach also seems to have important barriers, as we now explain. The non-commutative optimization framework of Bürgisser et al. [11] provides a natural gradient descent algorithm for the null cone problem. The iteration complexity of their algorithm depends inversely on a parameter known as the *weight margin* of the action. For the 3-tensor action where all dimensions are allowed to vary, this parameter can be exponentially small as shown by Franks and Reichenbach [22], and the resulting algorithm is only guaranteed to run in exponential-time.

Our work studies the intermediate fixed-parameter regime for the action of $G = \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_m(\mathbb{K})$ on $\mathcal{V} = \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$ where m is constant and n is allowed to grow. On the one hand, the group $\mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K})$ acts by the left-right action on $\mathcal{V}$ but on the other

hand the $\mathrm{SL}_m(\mathbb{K})$ factor is constant and acts only by shuffling the m slices. Conceptually, our approach exploits this decomposition of the group, albeit in a very different way than the work [11] exploits this product structure in their polynomial-time algorithm for the null cone problem. The null cone algorithm for [11, Corollary 6.24] is based on the scaling technique, and the key there is to bound the weight margins of the representation, and they use the product structure of the group to obtain such a bound. On the other hand, we manage to first obtain a degree bound for generating the invariant ring, and then utilize an effective version of the Cayley's Omega process to obtain a succinct encoding of the invariant ring. Combining these with the polynomial identity lemma (also known as Schwartz-Zippel lemma), the randomized polynomial-time algorithm follows.

1.2 Technical Overview

In this subsection we provide a proof overview of Theorem 3.

1.2.1 Geometric invariant theory

Consider the natural action of $G := \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_m(\mathbb{K})$ on the space of tensors $\mathcal{V} := \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$. We are given two tensors $u, v \in \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$, each given to us by n^2m many entries in $\mathbb{K}$. Our goal is to decide if their orbit closures intersect (OCI).

We consider the ring $\mathbb{K}[\mathcal{V}]$ of polynomial functions on $\mathcal{V}$. This ring is isomorphic to the polynomial ring with n^2m variables with coefficients in $\mathbb{K}$. A polynomial $f \in \mathbb{K}[\mathcal{V}]$ is called an *invariant* if $f(g \cdot v) = f(v)$ for every $g \in G$ and $v \in \mathcal{V}$. The set of invariants forms a $\mathbb{K}$-subalgebra of $\mathbb{K}[\mathcal{V}]$ that we denote by $\mathbb{K}[\mathcal{V}]^G$.

The conceptual bridge between invariant theory and OCI is Mumford's theorem: For linearly reductive groups, orbit closures are disjoint if and only if there is an invariant polynomial that separates them.

▶ **Theorem 5** (Mumford's Theorem [43]). *Let $\mathbb{K}$ be an algebraically closed field and let G be a reductive group acting linearly on a vector space $\mathcal{V}$. Given two elements $u, v \in \mathcal{V}$, we have $\overline{G \cdot u} \cap \overline{G \cdot v} \neq \emptyset \iff p(u) = p(v)$ for all $p \in \mathbb{K}[\mathcal{V}]^G$.*

In an ideal world, Mumford's theorem reduces OCI to computing and evaluating invariants. In practice, however, this approach fails due to two phenomena: first, even when invariants are generated in low degree for some special actions, the general upper bounds are exponential and there are instances where they must be exponential [18]. Second, even if a generating set exists in low degrees, it may be algorithmically infeasible to evaluate them all. We shall now discuss how we address these two issues.

1.2.2 Degree bounds for the invariant ring

As the invariant ring is usually infinite, we can only hope to capture it by a finite generating set. Indeed, the finite generation of this ring is ensured by Hilbert's celebrated results [31, 32]. The first difficulty that one needs to overcome is to bound the degrees of generators. Our first main contribution is a polynomial degree bound for the generators of the invariant ring.

▶ **Theorem 6** (Theorem 21 – informal). *Consider the action of $G := \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_m(\mathbb{K})$ on $\mathcal{V} := \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$. When $m = O(1)$, $\mathbb{K}[\mathcal{V}]^G$ is generated by homogeneous invariants of degree* $\mathrm{poly}(n)$.

To the best of our knowledge, only an upper bound of the form $O(\exp(n^2))$ was known for the degrees of the generators in this regime, see [15, Prop. 4.7.16] or [11, Prop. 7.2].

1.2.3 Succinct encoding of invariant rings

Even though the invariant ring is finitely generated, the number of generators can be exponential in size and they may be infeasible to evaluate.

To overcome this issue, Mulmuley proposed the notion of succinct encodings of invariant rings [41]. The basic idea is to introduce auxiliary variables so a set of generators can be obtained by interpolating over these auxiliary variables. This leads to the following definition from [41], which we state in adapted form from [24, Definition 1.3].

▶ **Definition 7.** *Let a group G act on a vector space $\mathcal{V} \cong \mathbb{K}^N$. We say that an arithmetic circuit $C = C(x_1, \ldots, x_N, y_1, \ldots, y_r)$* succinctly encodes *$\mathbb{K}[\mathcal{V}]^G$, if the set*

$$\{\, C(x_1, \ldots, x_N, a_1, \ldots, a_r) \mid (a_1, \ldots, a_r) \in \mathbb{K}^r \,\}$$

generates $\mathbb{K}[\mathcal{V}]^G$ as a $\mathbb{K}$-algebra. The size *of a succinct encoding is defined to be the size of the circuit C, measured by the number of gates and the bit-lengths of the constants used in the computation of C. In particular, we require that the constants are rational numbers.*

A succinct encoding for the action of G on $\mathcal{V}$ allows one to obtain a randomized algorithm for the orbit closure problem of this action as follows. By Theorem 5, the orbit closures of $u, v \in V$ intersect if and only if for any $f \in \mathbb{K}[V]^G$, $f(u) = f(v)$. Therefore, once a succinct encoding $C(x_1, \ldots, x_N, y_1, \ldots, y_r)$ of $\mathbb{K}[\mathcal{V}]^G$ is given, testing whether the orbit closures of u and v intersect reduces to testing if the two circuits in y-variables, $C(u_1, \ldots, u_N, y_1, \ldots, y_r)$ and $C(v_1, \ldots, v_N, y_1, \ldots, y_r)$, compute the same polynomial. This is an instance of the polynomial identity testing problem, which, by the polynomial identity testing lemma, admits a randomized polynomial-time algorithm by specializing $y_1, y_2, \ldots, y_r$ randomly to integers of bit-length $\mathrm{poly}(\mathrm{size}(C))$.

Thus, to reduce the OCI problem to an instance of PIT, we need to prove that we can efficiently compute a succinct generator for $\mathbb{K}[\mathcal{V}]^G$. This is our second main contribution: an efficient succinct encoding of the invariant ring $\mathbb{K}[\mathcal{V}]^G$.

▶ **Theorem 8.** *Assume $m = O(1)$. Then, there is a uniform family of $\mathrm{poly}(n)$-sized arithmetic circuit C that succinctly encodes $\mathbb{K}[\mathcal{V}]^G$.*

We prove Theorem 8 in Section 4. We now give an overview of how we prove degree bounds and also on how we efficiently construct such a succinct generator.

1.2.4 The basic strategy to prove Theorems 6 and 8

Our basic strategy is to "split" the action of $G = \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_m(\mathbb{K})$ into two steps as $G = H \times K$, where $H = \mathrm{SL}_n \times \mathrm{SL}_n$ and $K = \mathrm{SL}_m$. This decomposition encodes the invariant ring $R = \mathbb{K}[\mathcal{V}]^G$ as $R = (\mathbb{K}[\mathcal{V}]^H)^K$. Note that $\mathbb{K}[\mathcal{V}]^H$ is the invariant ring for the left-right action on matrix tuples, for which closed forms of invariant polynomials are known (Theorem 14), and polynomial degree upper bounds are also known [16]. In particular, these yield a succinct encoding of the invariant ring $\mathbb{K}[\mathcal{V}]^H$.

Given these, going from $\mathbb{K}[\mathcal{V}]^H$ to $(\mathbb{K}[\mathcal{V}]^H)^K$ still requires some work. Note that by the polynomial degree bound of the H-action, we can focus on K acting only on those invariants of polynomially bounded degrees, but the issue that we need to be careful about is that those invariants span a vector space of exponential dimension. This creates obstacles for proving a degree bound of the form $\mathrm{poly}(n, m)^{f(m)}$ where a function just depending on m stands on the exponent, as the generation degree bounds such as in [14] always depend polynomially in the dimension of the base vector space. And on the succinct generation question, even from

the succinct generation for the left-right action, we still need to obtain generators for the tensor action, thus we cannot naively construct the succinct generator based on the vector space of generators of the left-right action.

1.2.5 Addressing the technical difficulties

We overcome the above issues by (1) presenting a generation degree upper bound for the invariant ring R in the form of $\mathrm{poly}(n,m)^{f(m)}$, and (2) making an effective use of the Cayley Omega process to produce a succinct encoding.

For the degree upper bounds, we mentioned the problem of K acting on an exponential-dimension vector space. To get around this problem, the main idea is to resort to the nullcone defining bound as much as possible rather than on the generation bound. Indeed, in [14, Proposition 1.2], the nullcone defining bound has the intriguing property that it *does not depend on the ambient vector space dimension*. This allows us to get around the issue of working over a vector space of an exponentially large dimension by showing a suitable nullcone defining bound first, and then using the relation between generation and nullcone bounds [14, Theorem 1.1] to obtain the generation bound for the full invariant ring $\mathbb{K}[\mathcal{V}]^G$. Details on how we execute this approach are in Section 3.

Given the degree generation bound, we resort to the Cayley Omega process to obtain a succinct generator of $(\mathbb{K}[\mathcal{V}]^H)^K$ from the succinct generator of $\mathbb{K}[\mathcal{V}]^H$. The Cayley Omega process is a generic procedure to obtain a generating set, and we need to apply this process to the succinct encoding setting where sequences of partial derivatives need to be computed efficiently. At first sight, efficiently computing the partial derivative operator arising from the Omega process seems to be an impossible task, due to the complexity of the Omega process. However, the key here is to note that we are only applying the Omega process in constantly many variables (when $m \in O(1)$), which allows us to be inefficient in terms of m, while still preserving the efficiency of the succinct generator for the left-right action, as we operate on it to transform it into a succinct generator for the tensor action. This is analogous to how Mulmuley was able to compute his succinct generator [41]. Our efficient construction of the succinct generator appears in Section 4.

1.2.6 Generality of Our Techniques

While the above results are only stated in terms of the natural 3-tensor action, a quick look into our techniques and our proofs show that our results apply in much more generality. In particular, our degree bounds and efficient generation results need only the following general assumptions on G and $\mathcal{V}$: that the group G factors as a product of two groups $G = H \times K$, for which K is a product of special linear groups of constant total dimension – that is, $K = \prod_{i=1}^{k} \mathrm{SL}_{m_i}$ where $\prod_{i=1}^{k} m_i \in O(1)$ – and H is any group such that the corresponding action of H on $\mathcal{V}$ has polynomial degree bounds and an efficiently computable succinct generator. For instance, this setup also captures more general tensor actions where we have constantly many tensor factors where all but 2 of the factors have bounded dimension.

2 Preliminaries

Throughout this paper, we write $[\ell] := \{1, 2, \ldots, \ell\}$ for $\ell \in \mathbb{N}$. We take $\mathbb{K}$ to be an algebraically closed field of characteristic zero. For a $\mathbb{K}$-vector space $\mathcal{V}$, we denote by $\mathbb{K}[\mathcal{V}]$ the ring of polynomial functions on $\mathcal{V}$. If $\dim \mathcal{V} = N$, then we have an isomorphism $\mathbb{K}[\mathcal{V}] \cong \mathbb{K}[x_1, x_2, \ldots, x_N]$ with the latter denoting the polynomial ring with N variables over $\mathbb{K}$.

The zero locus of a set of polynomials $h_1, h_2, \ldots, h_\ell \in \mathbb{K}[\mathcal{V}]$, denoted $\mathcal{Z} = \mathcal{Z}(h_1, h_2, \ldots, h_\ell) := \{v \in \mathcal{V} \mid h_1(v) = \ldots = h_\ell(v) = 0\}$, is called an *affine algebraic set*. The ring of regular functions on $\mathcal{Z}$ is denoted by $\mathbb{K}[\mathcal{Z}] := \mathbb{K}[\mathcal{V}]/I$ where I is the radical of the ideal generated by $h_1, h_2, \ldots, h_\ell$. If $S \subset \mathcal{V}$ is an arbitrary set, we denote by $\overline{S}$ its *Zariski closure*, the smallest affine algebraic set that contains S.

2.1 Groups, Representations, and Invariant Theory

We will briefly introduce the main results in invariant theory that are relevant for the next sections. We refer to [15, 39, 43] for a more detailed treatment of the subject.

For a natural number $s \in \mathbb{N}$, we denote by $\mathrm{GL}_s(\mathbb{K})$ (resp. $\mathrm{SL}_s(\mathbb{K})$) the set of invertible (resp. with unit determinant) $s \times s$-matrices with entries in $\mathbb{K}$. A Zariski closed subgroup $G \leq \mathrm{GL}_s(\mathbb{K})$ is called an *algebraic group*. For simplicity of the presentation, we will assume that $G \leq \mathrm{SL}_s(\mathbb{K})$, since this is true for the groups that we will consider throughout the paper. In this case, G is an affine algebraic set in $\mathrm{Mat}(s, \mathbb{K})$, the vector space of $s \times s$ matrices over $\mathbb{K}$, and it is the zero locus of some polynomials $h_1, h_2, \ldots, h_\ell \in \mathbb{K}[g_{1,1}, \ldots, g_{s,s}]$.

Suppose $\mathcal{V}$ is an N-dimensional vector space over $\mathbb{K}$. A group homomorphism $\pi : G \to \mathrm{GL}(\mathcal{V})$ is called a *rational representation* if matrix entries of $\pi(g)$ are regular functions on G. That is,

$$\pi(g) = \begin{pmatrix} a_{1,1}(g) & a_{1,2}(g) & \ldots & a_{1,N}(g) \\ a_{2,1}(g) & \ddots & & \\ \vdots & & \ddots & \\ a_{N,1}(g) & & & a_{N,N}(g) \end{pmatrix}, \quad g \in G \tag{1}$$

for some polynomials $a_{1,1}, \ldots, a_{N,N} \in \mathbb{K}[g_{1,1}, \ldots, g_{s,s}]$.

Let $\pi : G \to \mathrm{GL}(\mathcal{V})$ be a rational representation. A subspace $\mathcal{U} \subset \mathcal{V}$ is called *G-stable* if $\pi(g)u \in \mathcal{U}$ for every $g \in G$ and $u \in \mathcal{U}$. In this case, the map $\gamma : G \to \mathrm{GL}(\mathcal{U})$ defined by $\gamma(g) = \pi(g)|_{\mathcal{U}}$ is also a rational representation of G. We call $\mathcal{V}$ *irreducible* if the only G-stable subspaces are $\{0\}$ and $\mathcal{V}$. An algebraic subgroup $G \leq \mathrm{GL}_s(\mathbb{K})$ is called *reductive* if $\mathcal{V}$ is a direct sum of its irreducible G-stable subspaces for every rational representation $\pi : G \to \mathrm{GL}(\mathcal{V})$. Important examples of reductive algebraic groups are $\mathrm{GL}_s(\mathbb{K}), \mathrm{SL}_s(\mathbb{K}), \mathrm{O}_s(\mathbb{K})$ (the group of orthogonal matrices), $\mathrm{Sp}_s(\mathbb{K})$ (the group of symplectic matrices), the tori $(\mathbb{K}^\times)^s$, all finite groups and their direct products.

A rational representation $\pi : G \to \mathrm{GL}(\mathcal{V})$ naturally defines a group action of G on $\mathcal{V}$ via

$$g \cdot v = \pi(g)v, \quad g \in G, v \in \mathcal{V}.$$

The action of G on $\mathcal{V}$ also induces an action on $\mathbb{K}[\mathcal{V}]$ by defining

$$(g \cdot f)(v) = f(g^{-1} \cdot v), \quad g \in G, v \in \mathcal{V}, f \in \mathbb{K}[\mathcal{V}].$$

A polynomial f is called an *invariant* if $g \cdot f = f$ for every $g \in G$. We denote by $\mathbb{K}[\mathcal{V}]^G$ the ring of invariants, which is a $\mathbb{K}$-subalgebra of $\mathbb{K}[\mathcal{V}]$. A celebrated result due to Hilbert [31, 32] states that the invariant ring $\mathbb{K}[\mathcal{V}]^G$ is finitely generated as a $\mathbb{K}$-algebra for every rational representation $\pi : G \to \mathrm{GL}(\mathcal{V})$ of a reductive group G. We note that since polynomials are continuous functions, invariant polynomials must take the same value on an orbit closure $\overline{G \cdot u}$. In particular, the invariant polynomials cannot distinguish two orbit closures that intersect. Mumford's Theorem 5 provides a converse statement, namely, two orbit closures $\overline{G \cdot u}$ and $\overline{G \cdot v}$ do not intersect if and only if there exists an invariant polynomial that distinguishes them.

Two important numerical invariants of a rational representation are: the minimum degree of polynomials that generate the invariant ring, that we denote by $\beta_\pi(\mathcal{V})$, and the minimum degree $\sigma_\pi(\mathcal{V})$ of invariants $f_1, f_2, \ldots, f_\ell$ such that the invariant ring $\mathbb{K}[\mathcal{V}]^G$ is integral over the $\mathbb{K}$-algebra $\mathbb{K}[f_1, f_2, \ldots, f_\ell]$. Namely,

$$\beta_\pi(\mathcal{V}) := \min\left\{d \in \mathbb{N} \mid \mathbb{K}[\mathcal{V}]^G \text{ is generated by invariants of degree } \leq d\right\} \tag{2}$$

and

$$\sigma_\pi(\mathcal{V}) := \min\left\{d \in \mathbb{N} \mid \mathbb{K}[\mathcal{V}]^G \text{ is integral over } \mathbb{K}[\mathcal{V}]^G_{\leq d}\right\}. \tag{3}$$

The *null cone* $\mathcal{N}(\mathcal{V}) \subset \mathcal{V}$ of π is defined as the zero locus of all homogeneous, non-constant invariants. By [15, Remark 1.7.2], $\sigma_\pi(\mathcal{V})$ is also equal to the minimum degree of *null cone definers*, i.e.,

$$\sigma_\pi(\mathcal{V}) = \min\left\{d \mid \mathcal{N}(\mathcal{V}) = \mathcal{Z}(f_1, f_2, \ldots, f_\ell) \text{ for some } f_1, f_2, \ldots, f_\ell \in \mathbb{K}[\mathcal{V}]^G_{\leq d}\right\}.$$

We note that by definition, $\beta_\pi(\mathcal{V})$ and $\sigma_\pi(\mathcal{V})$ only depend on the invariant ring $\mathbb{K}[\mathcal{V}]^G$, i.e., if $\mathbb{K}[\mathcal{V}]^G \cong \mathbb{K}[\mathcal{W}]^H$ as filtered $\mathbb{K}$-algebras for two rational representations $\pi : G \to \mathrm{GL}(\mathcal{V})$ and $\gamma : H \to \mathrm{GL}(\mathcal{W})$, then $\beta_\pi(\mathcal{V}) = \beta_\gamma(\mathcal{W})$ and $\sigma_\pi(\mathcal{V}) = \sigma_\gamma(\mathcal{W})$.

The following important result appears in [14, Proposition 1.2]. An important consequence of it is that $\sigma_\pi(\mathcal{V})$ admits an upper bound independent of the dimension of $\mathcal{V}$.

▶ **Proposition 9** ([14, Proposition 1.2]). *In the setting above, define $m := \dim(G)$. Recall that $G \leq \mathrm{GL}_s(\mathbb{K})$ is an algebraic group. Additionally, let $H := \max\{\deg(h_i) \mid i \in [\ell]\}$ and $A := \max\{\deg(a_{j,k}) \mid 1 \leq j, k \leq \dim(\mathcal{V})\}$ where $a_{i,j}$ are the defining polynomials of π, see Equation (1). Then*

$$\sigma_\pi(\mathcal{V}) \leq H^{s^2-m} \cdot A^m.$$

Let's consider the case $G = \mathrm{SL}_s(\mathbb{K})$. The special linear group is cut out by the polynomial $\det(g) - 1$, which has degree $H = s$, and the dimension of $\mathrm{SL}_s(\mathbb{K})$ is $m = s^2 - 1$.

▶ **Corollary 10.** *Let $\pi : \mathrm{SL}_s(\mathbb{K}) \to \mathrm{GL}(\mathcal{V})$ be a rational representation with $\pi(g) = (a_{i,j}(g))_{i,j\in[N]}$. Set $A := \max\limits_{1\leq i,j\leq N} \deg(a_{i,j})$. Then,*

$$\sigma_\pi(\mathcal{V}) \leq s\, A^{s^2-1}.$$

The above degree bounds on the null cone can be used to derive degree bounds for the generators of the invariant ring, as the following remarkable result shows.

▶ **Theorem 11** (Degree bounds for generators, [14, Theorem 1.1]). *In the setting of Proposition 9,*

$$\beta_\pi(\mathcal{V}) \leq \max\left\{2,\ \frac{3}{8} \cdot \dim(\mathbb{K}[\mathcal{V}]^G) \cdot \sigma_\pi(\mathcal{V})^2\right\},$$

where $\dim \mathbb{K}[\mathcal{V}]^G$ is the Krull dimension *of $\mathbb{K}[\mathcal{V}]^G$, and thus $\dim \mathbb{K}[\mathcal{V}]^G \leq \dim \mathcal{V}$.*

Suppose $\mathcal{X} \subset \mathcal{V}$ and $\mathcal{Z} \subset \mathcal{W}$ are two G-stable affine algebraic sets. A morphism $f : \mathcal{X} \to \mathcal{Z}$ that satisfies $f(g \cdot x) = g \cdot f(x)$ is called a G-equivariant map. There is an induced ring homomorphism $f^\sharp : \mathbb{K}[\mathcal{Z}] \to \mathbb{K}[\mathcal{X}]$ defined by $f^\sharp(F)(x) = F(f(x))$. We say that f has degree at most D if

$$\deg(f^\sharp(F)) \leq D \cdot \deg(F), \quad \text{for every } F \in \mathbb{K}[\mathcal{Z}].$$

If $f^\sharp$ is surjective, then we say that f is an *embedding*.

▶ **Proposition 12** ([15, Corollary 2.2.9]). *Let $f : \mathcal{X} \to \mathcal{Z}$ be a G-equivariant embedding. Then*

$$f^\sharp(\mathbb{K}[\mathcal{Z}]^G) = \mathbb{K}[\mathcal{X}]^G.$$

Proposition 12 allows us to pull-back the degree bounds for $\mathbb{K}[\mathcal{Z}]^G$ to $\mathbb{K}[\mathcal{X}]^G$.

▶ **Corollary 13.** *Let $\pi : G \to \mathrm{GL}(\mathcal{V})$, $\gamma : G \to \mathrm{GL}(\mathcal{W})$ be rational representations, $\mathcal{X} \subseteq \mathcal{V}, \mathcal{Z} \subseteq \mathcal{W}$ be G-stable algebraic sets and $f : \mathcal{X} \to \mathcal{Z}$ be a G-equivariant embedding of degree D. Then,*

$$\beta_\pi(\mathcal{X}) \leq D \cdot \beta_\gamma(\mathcal{Z}) \quad \textit{and} \quad \sigma_\pi(\mathcal{X}) \leq D \cdot \sigma_\gamma(\mathcal{Z}).$$

2.2 The Left-Right Action on Matrix Tuples

For certain families of actions, we have more structure on the set of generators for the invariant ring, as well as a better control on the degree bounds for the null cone and for the generators of the invariant ring. An important example is the left-right action, which we now define.

Let $m, n \in \mathbb{N}$, $H := \mathrm{SL}_n \times \mathrm{SL}_n$ and $\mathcal{V} := \mathrm{Mat}(n, \mathbb{K})^m$ where $\mathrm{Mat}(n, \mathbb{K})$ denotes the space of $n \times n$-matrices over $\mathbb{K}$. The left-right action of H on $\mathcal{V}$ is given by

$$\pi_H(X, Y) \cdot (A_1, \ldots, A_m) := (XA_1Y^t, \ldots, XA_mY^t).$$

The following theorem on the generators of the ring of invariants for the left-right action appears in [19, Corollary 3], [20] and [46].

▶ **Theorem 14.** *The space $\mathbb{K}[\mathcal{V}]^H$ is spanned as a vector space by all the forms*

$$f_T(A) := \det\left(\sum_{i=1}^{m} T_i \otimes A_i\right) \tag{4}$$

where $T = (T_1, \ldots, T_m) \in \mathrm{Mat}(d, \mathbb{K})^m$ and $d \in \mathbb{N}$.

If we apply the general bounds in Proposition 9 and Theorem 11 from [14], we would get a degree bound for $\mathbb{K}[\mathcal{V}]^H$ that is exponential in n, see also [11, Prop. 7.2]. The result [16, Theorem 1.8] (see also [36, Theorem 1]), which we now state, gives much sharper degree bounds for equations defining the null cone of the left-right action.

▶ **Theorem 15** ([16, Theorem 1.8]). *The following bound holds: $\sigma_{\pi_H}(\mathcal{V}) \leq n(n-1)$.*

We note that since $f_T(X)$ has degree dn, Theorem 15 implies that the null cone is cut out by the polynomials $f_T(X)$ for $T = (T_1, \ldots, T_m) \in \mathrm{Mat}(d, \mathbb{K})^m$ with $d \leq n - 1$. This bound, when combined with Popov's theorem [44, 45] yields the following generating degree bounds for the left-right action, obtained in [16, Theorem 1.2].

▶ **Theorem 16** ([16, Theorem 1.2]). *The following bound holds: $\beta_{\pi_H}(\mathcal{V}) \leq m \cdot n^4$.*

2.3 Reynolds Operator & Cayley's Omega Process

In the general setting of a rational representation $\pi : G \to \mathrm{GL}(\mathcal{V})$ of a reductive group G, there exists a linear operator $\mathcal{R} : \mathbb{K}[\mathcal{V}] \to \mathbb{K}[\mathcal{V}]^G$ with the following properties

1. $\mathcal{R}(f) = f$ for all invariants $f \in \mathbb{K}[\mathcal{V}]^G$.
2. $\mathcal{R}(g \cdot h) = \mathcal{R}(h)$ for all $h \in \mathbb{K}[\mathcal{V}]$ and $g \in G$.

This operator is uniquely determined by the properties above and is called the Reynolds operator [15, Theorem 2.2.5]. The following lemma gives an important factoring property of the Reynolds operator, and appears in [15, Lemma 4.5.4].

▶ **Lemma 17.** *Consider a rational representation $\pi : G \to \mathrm{GL}(\mathcal{V})$ and suppose that G has a normal subgroup H. Let $\mathcal{R}_G : \mathbb{K}[\mathcal{V}] \to \mathbb{K}[\mathcal{V}]^G$ be the Reynolds operator with respect to G, $\mathcal{R}_H : \mathbb{K}[\mathcal{V}] \to \mathbb{K}[\mathcal{V}]^H$ the Reynolds operator with respect to H and $\mathcal{R}_{G/H} : \mathbb{K}[\mathcal{V}]^H \to \mathbb{K}[\mathcal{V}]^G$ be the Reynolds operator with respect to G/H. Then $\mathcal{R}_G = \mathcal{R}_{G/H} \circ \mathcal{R}_H$.*

For homogeneous actions of $G = \mathrm{SL}_m(\mathbb{K})$, there is an explicit algebraic construction of the Reynolds operator, given by Cayley's Omega process, which we now briefly present. We will use this construction in Section 4 together with other results from algebraic complexity theory to give uniform succinct circuits that compute generators for the invariant ring of the tensor action. For more background and proofs of the results that we invoke in this subsection, we refer the reader to [15, 11] and references therein.

Consider a homogeneous degree D representation $\pi : \mathrm{SL}_m(\mathbb{K}) \to \mathrm{GL}(\mathcal{W})$, along with its induced action on the polynomials in $\mathbb{K}[\mathcal{W}]$, denoted by $\tilde{\pi}$. That is, $(\tilde{\pi}(g)f)(x) := f(\pi^{-1}(g)x)$. After fixing a basis (e_i) of $\mathcal{W}$, the entries of $\pi(Z)$ are homogeneous degree D polynomials in the variables $Z := (Z_{i,j})_{i,j\in[m]}$ and the entries of $\tilde{\pi}$, when acting on the space $\mathbb{K}[\mathcal{W}]_r$ of degree r forms, are homogeneous polynomials of degree $\tilde{D}_r := rD(m-1)$.[3] Our goal is to describe the invariant ring $\mathbb{K}[\mathcal{W}]^{\mathrm{SL}_m}$ corresponding to the above action.

Define $\partial := (\partial_{Z_{i,j}})_{i,j\in[m]}$ to be the $m \times m$ matrix of partial derivatives of Z. Let $\mathbb{K}[\partial]$ be the ring of differential operators on $\mathbb{K}[Z]$. For any $p \in \mathbb{K}[Z]$, let $\partial_p := p(\partial)$. Cayley's Ω-operator is defined as follows

$$\Omega : \mathbb{K}[Z] \to \mathbb{K}[Z], \qquad \Omega := \partial_{\det} = \sum_{\sigma\in S_m} \mathrm{sgn}(\sigma) \prod_{k=1}^{m} \partial_{Z_{k,\sigma(k)}}. \tag{5}$$

Applying Ω to a homogeneous polynomial q reduces its degree by m, thus if q has degree rm, $\Omega^r(q)$ is a constant. In order to state the invariance properties of the Ω-operator we introduce the left and right multiplication maps for $A \in \mathrm{Mat}(m, \mathbb{K})$.

$$R_A : \mathrm{Mat}(m,\mathbb{K}) \to \mathrm{Mat}(m,\mathbb{K}), \quad X \mapsto XA$$
$$L_A : \mathrm{Mat}(m,\mathbb{K}) \to \mathrm{Mat}(m,\mathbb{K}), \quad X \mapsto AX.$$

With the above definitions, we have the following properties:

▶ **Lemma 18** ([11, Proposition 7.8])**.** *In the setting above, the following properties hold:*

1. *For any $q \in \mathbb{K}[Z]$ and $A \in \mathrm{Mat}(m,\mathbb{K})$ we have*

$$\Omega(q \circ L_A) = \det(A) \cdot (\Omega(q) \circ L_A), \qquad \Omega(q \circ R_A) = \det(A) \cdot (\Omega(q) \circ R_A).$$

2. *If $q \in \mathbb{K}[Z]_{rm}$ and $A \in \mathrm{SL}_m$, then $\Omega^r(q) \in \mathbb{K}$ and $\Omega^r(q) = \Omega^r(q \circ L_A) = \Omega^r(q \circ R_A)$.*
3. *$c_{r,m} := \Omega^r(\det(Z)^r) \in \mathbb{K}^\times$, that is, $c_{r,m}$ is a nonzero element of $\mathbb{K}$.*

[3] We note that for $g \in \mathrm{SL}_m(\mathbb{K})$ we have $g^{-1} = \mathrm{Adj}(g)$ where $\mathrm{Adj}(g)$ denotes the *adjugate matrix*, which has degree $m-1$ as a polynomial function of g.

We are now ready to define the Reynolds operator $\mathcal{R} : \mathbb{K}[\mathcal{W}] \to \mathbb{K}[\mathcal{W}]$ for the representation $\pi : \mathrm{SL}_m(\mathbb{K}) \to \mathrm{GL}(\mathcal{W})$. For $f \in \mathbb{K}[\mathcal{W}]_r$, we have:

$$\mathcal{R}(f) := \begin{cases} \dfrac{\Omega^{\tilde{D}_r/m} \circ \tilde{\pi}(Z) \cdot f}{c_{\tilde{D}_r/m,m}} & \text{if } m \mid \tilde{D}_r, \\ 0 & \text{otherwise,} \end{cases} \tag{6}$$

where $\tilde{D}_r = rD(m-1)$, $c_{\tilde{D}_r/m,m}$ is defined in Lemma 18 (3), and $\Omega^{\tilde{D}_r/m} \circ \tilde{\pi}(Z) \cdot f$ means applying $\Omega^{\tilde{D}_r/m}$ to the Z coefficients of $\tilde{\pi}(Z) \cdot f$.

The following implies that $\mathcal{R}$ indeed has the properties characterizing the Reynolds operator.

▶ **Proposition 19** ([11, Proposition 7.9 and Corollary 7.10]). *The map $\mathcal{R} : \mathbb{K}[\mathcal{W}] \to \mathbb{K}[\mathcal{W}]$ defined in Equation (6) satisfies the following conditions.*

1. *If $f \in \mathbb{K}[\mathcal{W}]^G$, then $\mathcal{R}(f) = f$.*
2. *If $f \in \mathbb{K}[\mathcal{W}]$ and $g \in G$, then $\mathcal{R}(g \cdot f) = \mathcal{R}(f)$.*
3. *$\mathcal{R}(\mathbb{K}[\mathcal{W}]) = \mathbb{K}[\mathcal{W}]^G$.*

3 Fixed-Parameter Polynomial Degree Bounds

In this section we prove our first main technical theorem: Theorem 21, which is the formal statement of Theorem 6.

3.1 Setup

Let $n, m \in \mathbb{N}$ be natural numbers and consider the natural action of the product group $G := \mathrm{SL}_n \times \mathrm{SL}_n \times \mathrm{SL}_m$ on the tensor space $\mathcal{V} := \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$, when m is fixed and n becomes large. In the following, we will identify a tensor $T \in \mathcal{V}$ with the matrix tuple $(A_1, A_2, \ldots, A_m)$, where $A_i \in \mathrm{Mat}(n, \mathbb{K})$ is the i^{th} 3-*slice* of T.

The action of G on $\mathcal{V}$ is given by the rational representation $\pi_G : G \to \mathrm{GL}(\mathcal{V})$, which defines the action of G on $\mathcal{V}$ as

$$(X, Y, Z) \cdot (A_1, \ldots, A_m) = \left(X \left(\sum_{j=1}^{m} Z_{1j} A_j \right) Y^t,\ X \left(\sum_{j=1}^{m} Z_{2j} A_j \right) Y^t,\ \ldots,\ X \left(\sum_{j=1}^{m} Z_{mj} A_j \right) Y^t \right).$$

In other words, $\mathrm{SL}_n \times \mathrm{SL}_n$ acts on $\mathcal{V}$ by the *left-right action* and SL_m acts by *shuffling* the 3-slices. In representation theoretic terms, we have

$$\pi_G(X, Y, Z) = X \otimes Y \otimes Z \in \mathrm{GL}(\mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m).$$

The group G is a direct product of its subgroups $H := \mathrm{SL}_n \times \mathrm{SL}_n$ and $K := \mathrm{SL}_m$. We denote the restriction of π_G to H (resp. K) by π_H (resp. π_K). Then, the induced action of H and K on $\mathcal{V}$ are given by

$$(X, Y) \cdot (A_1, \ldots, A_m) = (XA_1Y^t, \ldots, XA_mY^t),$$

$$Z \cdot (A_1, \ldots, A_m) = \left(\sum_{j=1}^{m} Z_{1j} A_j, \ldots, \sum_{j=1}^{m} Z_{mj} A_j \right),$$

and we have $\pi_H(X, Y) = X \otimes Y \otimes I_m$ and $\pi_K(Z) = I_n \otimes I_n \otimes Z$.

Since H and K commute, we have the following identification of the invariant rings:

$$\mathbb{K}[\mathcal{V}]^G = \left(\mathbb{K}[\mathcal{V}]^H\right)^K \tag{7}$$

In the following, we will obtain degree bounds on $\mathbb{K}$-algebra generators of $\mathbb{K}[\mathcal{V}]^G$ by making use of this identification. As π_H is simply the left-right action, by Theorem 16, the invariant ring $\mathbb{K}[\mathcal{V}]^H$ is generated by invariants of degree $\beta_H \leq mn^4$, where we denote $\beta_H := \beta_{\pi_H}(\mathcal{V})$ from now on and similarly for β_G and β_K.

3.2 Using the left-right action

Consider the vector space $\mathcal{W} := \bigoplus_{d=1}^{\beta_H} \mathbb{K}[\mathcal{V}]_d^H \subset \mathbb{K}[\mathcal{V}]^H$. In plain English, $\mathcal{W}$ is the space of non-constant H-invariants up to degree β_H. We denote the dimension of $\mathcal{W}$ by $N := \dim \mathcal{W}$ and we choose a linear basis $\{f_1, \ldots, f_N\}$ of $\mathcal{W}$ consisting of homogeneous invariants. Note that f_i's may be of different degrees.

We now show that there is a polynomial ring $\mathbb{K}[y_1, y_2, \ldots, y_N]$, on which K acts, such that $\mathbb{K}[y_1, \ldots, y_N]^K$ surjects onto $\mathbb{K}[\mathcal{V}]^G$. We define the *categorical quotient* $\mathcal{V} /\!\!/ H$ of $\mathcal{V}$ by the action of H as the affine variety $\operatorname{maxSpec}(\mathbb{K}[\mathcal{V}]^H)$, corresponding to the ring $\mathbb{K}[\mathcal{V}]^H$. Explicitly, we may assume that $\mathcal{V} /\!\!/ H$ is the image of the polynomial map $\mathcal{V} \to \mathbb{K}^N$, $v \mapsto (f_1(v), f_2(v), \ldots, f_N(v))$. We denote the image of a vector $v \in \mathcal{V}$ under this map by $[v]$. Since the actions of K and H commute, there is a natural K-action on $\mathcal{V} /\!\!/ H$ via

$$k \cdot [v] = [k \cdot v].$$

Note that this is well-defined since K sends H-invariants to H-invariants.

There is a map from the categorical quotient $\mathcal{V} /\!\!/ H$ to the dual vector space $\mathcal{W}^*$, defined by

$$\Phi : \mathcal{V} /\!\!/ H \to \mathcal{W}^*, \qquad \Phi([v]) = \mathrm{ev}_v \text{ where } \mathrm{ev}_v(f) := f(v).$$

The corresponding ring map is the $\mathbb{K}$-algebra homomorphism $\Phi^\sharp : \mathbb{K}[\mathcal{W}^*] \to \mathbb{K}[\mathcal{V}]^H$, defined by $F \mapsto F \circ \Phi$. Since $\mathcal{W}$ is N-dimensional, we can identify $\mathbb{K}[\mathcal{W}^*] = \mathbb{K}[y_1, y_2, \ldots, y_N]$ and $\Phi^\sharp$ becomes

$$\Phi^\sharp : \mathbb{K}[y_1, y_2, \ldots, y_N] \to \mathbb{K}[\mathcal{V}]^H, \quad \Phi^\sharp(y_i) = f_i \text{ for } i = 1, 2, \ldots, N.$$

We note that if $F(y_1, \ldots, y_N) \in \mathbb{K}[y_1, \ldots, y_N]$ is a polynomial of degree D, then $\Phi^\sharp(F)$ has degree at most $D \cdot \max_i \deg(f_i) = D \cdot \beta_H$.

Since the subgroups H and K commute, K acts on $\mathcal{W}$ by a restriction of its action on $\mathbb{K}[\mathcal{V}]$. More concretely, $k \in K$ acts by $(k \cdot f)(v) = f(k^{-1} \cdot v) = (f \circ \pi_K(k^{-1}))(v)$ for $f \in \mathcal{W}$ and $v \in \mathcal{V}$. This action induces an action of K on $\mathcal{W}^*$ by $(k \cdot \varphi)(f) = \varphi(k^{-1} \cdot f) = \varphi(f \circ \pi_K(k))$. More concretely $\mathcal{W}^* \cong \bigoplus_{d=1}^{\beta_H} S^d(\mathcal{V})^H$ as representations of K, where $S^d(\cdot)$ denotes the d-th symmetric power. Hence, for $v \in \mathcal{V}$ we have $(k \cdot \mathrm{ev}_v)(f) = \mathrm{ev}_v(k^{-1} \cdot f) = f(k \cdot v) = \mathrm{ev}_{k \cdot v}(f)$. This implies that

$$k \cdot \mathrm{ev}_v = \mathrm{ev}_{k \cdot v} \tag{8}$$

▶ **Lemma 20.** *The map Φ is a K-equivariant embedding and we have $\Phi^\sharp(\mathbb{K}[y_1, \ldots, y_N]^K) = \mathbb{K}[\mathcal{V}]^G$.*

Proof. For $[v] \in \mathcal{V} /\!\!/ H$ and $k \in K$ we have

$$\Phi(k \cdot [v]) = \Phi([k \cdot v]) = \mathrm{ev}_{k \cdot v} = k \cdot \mathrm{ev}_v = k \cdot \Phi([v]),$$

where we use Equation (8) in the third equality. This shows that Φ is K-equivariant.

The ring map $\Phi^\sharp : \mathbb{K}[\mathcal{W}^*] \to \mathbb{K}[\mathcal{V} /\!\!/ H] = \mathbb{K}[\mathcal{V}]^H$ is surjective since $\Phi^\sharp(y_i) = f_i$ and $f_1, f_2, \ldots, f_N$ generate the invariant ring $\mathbb{K}[\mathcal{V}]^H$. Thus, Φ is an embedding, and the second claims follows from Proposition 12. ◀

We are now ready to prove our main technical theorem: a fixed-parameter degree bound for $\beta_G(\mathcal{V})$.

▶ **Theorem 21** (Fixed-parameter degree bounds). *In the setup of this section, we have*

$$\sigma_G(\mathcal{V}) \leq m \cdot (\beta_H)^{m^2} \quad \text{and} \quad \beta_G(\mathcal{V}) \leq \frac{3}{8} \cdot m^3 n^2 \cdot (\beta_H)^{2m^2}.$$

In particular, $\beta_G(\mathcal{V}) = \mathrm{poly}(n)$ when m is a constant.

Proof. Note that the ring map $\Phi^\sharp$ has degree $\max_i \deg(f_i) = \beta_H$ since $\Phi^\sharp(y_i) = f_i$ and $\mathbb{K}[\mathcal{W}^*] = \mathbb{K}[y_1, \ldots, y_N]$. Hence, Lemma 20 and Corollary 13 imply that

$$\sigma_G(\mathcal{V}) \leq \beta_H \cdot \sigma_K(\mathcal{W}^*).$$

We now claim that $\sigma_K(\mathcal{W}^*) \leq m \cdot (\beta_H)^{m^2-1}$. Let $\rho : K \to \mathrm{GL}(\mathcal{W}^*)$ denote the representation of $K = \mathrm{SL}_m$ that is induced from its action on $\mathcal{W}^*$. The action of K on $\mathcal{W}$ is a restriction of its action on $\mathbb{K}[\mathcal{V}] = \bigoplus_{\ell \geq 0} S^\ell(\mathcal{V}^*)$. Since $\mathcal{W}$ consists of polynomials of degree at most β_H, $\mathcal{W}^*$ is a K-stable subspace of $\bigoplus_{\ell=1}^{\beta_H} S^\ell(\mathcal{V})$. In particular, as matrices we have for $k \in K = \mathrm{SL}_m$

$$\rho(k) = \left(\bigoplus_{\ell=1}^{\beta_H} S^\ell(\pi_K(k)) \right) \Bigg|_{\mathcal{W}^*}, \tag{9}$$

where $S^\ell(\pi_K(k))$ denotes the ℓ-th symmetric matrix power. By the definition of π_K, the degrees of the matrix coefficients $\pi_K(k)$ have degree 1. Hence, the degrees of the matrix coefficients of $\bigoplus_{\ell=1}^{\beta_H} S^\ell(\pi_K(k))$ are bounded by β_H. Since restriction does not increase the degree, we deduce that the degrees of the matrix coefficients of $\rho(k)$ are bounded by β_H.

Now, by Corollary 10 we have

$$\sigma_K(\mathcal{W}^*) \leq m \cdot (\beta_H)^{m^2-1}.$$

Here a key property of Corollary 10 is that $\dim(\mathcal{W}^*)$, which is exponential in n, does not play a role in this bound. This finishes the proof of the first claim. The second claim simply follows from Theorem 11 using the upper bound for $\sigma_G(\mathcal{V})$. ◀

▶ Remark 22. In the above theorem, it is important to upper bound $\sigma_K(\mathcal{W})$ first and use it to upper bound $\sigma_G(\mathcal{V})$ and then deduce an upper bound for $\beta_G(\mathcal{V})$ using Theorem 11. If we instead upper bound $\beta_K(\mathcal{W})$ first and then pull-back the bound along $\Phi^\sharp$ to get an upper bound for $\beta_G(\mathcal{V})$, we get the worse upper bound $\beta_G(\mathcal{V}) \leq \frac{3}{8} N \cdot m^2 \cdot (\beta_H)^{2m^2-1}$, which is exponentially large in n.

4 Efficient Succinct Computation of Generating Invariants

In this section we will show that, in the setting where $m = O(1)$, we can efficiently compute a succinct circuit that computes the generating invariants for the tensor action of $G := \mathrm{SL}_n \times \mathrm{SL}_n \times \mathrm{SL}_m$ on $\mathcal{V} := \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$. Once we have this succinct circuit, we will be able to give a randomized algorithm for the Orbit Closure Intersection problem. Before we show this, we will need some elementary results which are folklore in the literature, and thus we present them here with full proofs. For a vector $\mathbf{u} \in \mathbb{K}^t$, let $V(\mathbf{u}) \in \mathrm{Mat}(t, \mathbb{K})$ be the (square) Vandermonde matrix given by $V(\mathbf{u})_{i,j} := \mathbf{u}_i^j$, where $j \in \{0, \ldots, t-1\}$. The Vandermonde matrix is invertible whenever the entries of $\mathbf{u}$ are pairwise distinct. In this section, given a tuple of variables $\mathbf{y} := (y_1, \ldots, y_m)$ and $\mathbf{e} \in \mathbb{Z}^m$, we define

$$\mathbf{y}^{\mathbf{e}} := \begin{cases} \prod_{i \in [m]} y_i^{e_i}, & \text{if } \mathbf{e} \in \mathbb{N}^m, \\ 0, & \text{otherwise.} \end{cases}$$

▶ **Proposition 23** (Multivariate Vandermonde). *Let $m, D \in \mathbb{N}$ and $\mathcal{S} := \{0, \dots, D\}$. In the space of square matrices $\mathrm{Mat}((D+1)^m, \mathbb{K})$, index the rows and columns by tuples from $\mathcal{S}^m$. Lastly, let $M_{\mathcal{S}} \in \mathrm{Mat}((D+1)^m, \mathbb{K})$ be the matrix defined as $M_{\mathcal{S}}(\mathbf{a}, \mathbf{b}) := \mathbf{a}^{\mathbf{b}}$ for $\mathbf{a}, \mathbf{b} \in \mathcal{S}^m$. Then, $M_{\mathcal{S}} = V(0, \dots, D)^{\boxtimes m}$, and thus, $M_{\mathcal{S}}$ is invertible.*

Proof. Let $V := V(0, \dots, D)$ and $M := V^{\boxtimes m}$. Since $M \in \mathrm{Mat}((D+1)^m, \mathbb{K})$, let us compute $M(\mathbf{a}, \mathbf{b})$. By definition, we have $M(\mathbf{a}, \mathbf{b}) = \prod_{i \in [m]} V_{\mathbf{a}_i, \mathbf{b}_i} = \prod_{i \in [m]} \mathbf{a}_i^{\mathbf{b}_i} = \mathbf{a}^{\mathbf{b}} = M_{\mathcal{S}}(\mathbf{a}, \mathbf{b})$, as we wanted. ◀

▶ **Proposition 24** (Coefficients and evaluations). *Let $D \in \mathbb{N}$, $\mathcal{S} := \{0, 1, \dots, D\}$, R be a graded $\mathbb{K}$-algebra with $R_0 = \mathbb{K}$, $\mathbf{y} := (y_1, \dots, y_m)$ and $P \in R[\mathbf{y}]$ be such that $\deg_{y_i} P \leq D$ for all $i \in [m]$. Thus, we can write $P = \sum_{\mathbf{a} \in \mathcal{S}^m} P_{\mathbf{a}} \cdot \mathbf{y}^{\mathbf{a}}$ for some $P_{\mathbf{a}} \in R$. Let $\mathbf{v}_P \in R^{\mathcal{S}^m}$ be defined as $(\mathbf{v}_P)_{\mathbf{a}} := P_{\mathbf{a}}$ and $\mathbf{w}_P \in R^{\mathcal{S}^m}$ be defined as $(\mathbf{w}_P)_{\mathbf{a}} := P(\mathbf{a})$. Then, we have that $\mathbf{w}_P = M_{\mathcal{S}} \cdot \mathbf{v}_P$, where $M_{\mathcal{S}}$ is the matrix from Proposition 23.*

Proof. Since $(\mathbf{w}_P)_{\mathbf{a}} = P(\mathbf{a}) = \sum_{\mathbf{b} \in \mathcal{S}^m} P_{\mathbf{b}} \cdot \mathbf{a}^{\mathbf{b}} = \sum_{\mathbf{b} \in \mathcal{S}^m} M_{\mathcal{S}}(\mathbf{a}, \mathbf{b}) \cdot P_{\mathbf{b}}$, which is the $\mathbf{a}^{th}$ entry of the matrix-vector product $M_{\mathcal{S}} \mathbf{v}_P$, this proves the above proposition. ◀

With the above facts, we can give a uniform algorithm to compute any homogeneous partial derivative operator (of a given individual degree) of a given circuit.

▶ **Proposition 25.** *Let $\mathbf{x} := (x_1, \dots, x_r)$ and $\mathbf{z} := (z_1, \dots, z_m)$ be tuples of variables and let $P \in \mathbb{K}[\mathbf{x}, \mathbf{z}]$ be a polynomial with $\deg_{z_i}(P) \leq D$ for all $i \in [m]$. Let $\partial_{\mathbf{z}} := (\partial_{z_1}, \dots, \partial_{z_m})$ and $Q \in \mathbb{K}[\partial_{\mathbf{z}}]$ be a partial differential operator with $\deg_{\partial_{z_i}}(Q) \leq D$ for all $i \in [m]$. If P can be computed by a uniform algebraic circuit Ψ of size $s \geq m$, then $(Q \circ P)\,|_{\mathbf{z}=\mathbf{0}}$ can be computed by a uniform algebraic circuit Φ of size $O((D+1)^{3m+3} \cdot s)$.*

Proof. Take $\mathcal{S} := \{0, \dots, D\}$ and $M := M_{\mathcal{S}}$ as in Proposition 23. Since $\deg_{z_i}(P) \leq D$ for all $i \in [m]$, we can write $P = \sum_{\mathbf{a} \in \mathcal{S}^m} P_{\mathbf{a}}(\mathbf{x}) \cdot \mathbf{z}^{\mathbf{a}}$ where $P_{\mathbf{a}} \in \mathbb{K}[\mathbf{x}]$. Similarly, we can write $Q(\partial_{\mathbf{z}}) = \sum_{\mathbf{b} \in \mathcal{S}^m} Q_{\mathbf{b}} \cdot \partial_{\mathbf{z}}^{\mathbf{b}}$ with $Q_{\mathbf{b}} \in \mathbb{K}$. Thus, we get that

$$(Q \circ P)\,|_{\mathbf{z}=\mathbf{0}} = \sum_{\mathbf{a} \in \mathcal{S}^m} P_{\mathbf{a}}(\mathbf{x}) \cdot (Q(\partial_{\mathbf{z}}) \circ \mathbf{z}^{\mathbf{a}})\,|_{\mathbf{z}=\mathbf{0}} = \sum_{\mathbf{a} \in \mathcal{S}^m} P_{\mathbf{a}}(\mathbf{x}) \cdot (\partial_{\mathbf{z}}^{\mathbf{a}} \circ Q(\mathbf{z}))\,|_{\mathbf{z}=\mathbf{0}}$$

where $Q(\mathbf{z}) := \sum_{\mathbf{b} \in \mathcal{S}^m} Q_{\mathbf{b}} \cdot \mathbf{z}^{\mathbf{b}}$.

Let $\mathbf{v}_Q, \mathbf{w}_Q \in \mathbb{K}^{\mathcal{S}^m}$ and $\mathbf{v}_P, \mathbf{w}_P \in \mathbb{K}[\mathbf{x}]^{\mathcal{S}^m}$ be defined as in Proposition 24. With these definitions, Proposition 24 and the fact that $(\partial_{\mathbf{z}}^{\mathbf{a}} \circ Q(\mathbf{z}))\,|_{\mathbf{z}=\mathbf{0}} = Q_{\mathbf{a}}$ tell us that the above equation can be written in matrix-vector product format as:

$$(Q \circ P)\,|_{\mathbf{z}=\mathbf{0}} = \mathbf{v}_P^T \cdot \mathbf{v}_Q = (M^{-1}\mathbf{w}_P)^T \cdot \mathbf{v}_Q = \mathbf{w}_P \cdot (M^{-1})^T \cdot \mathbf{v}_Q.$$

Since $(\mathbf{w}_P)_{\mathbf{b}} = \Psi(\mathbf{b})$, we can compute $\mathbf{w}_P$ by $(D+1)^m$ distinct evaluations to Ψ. As Q is a $(D+1)^m$-sparse polynomial, we can (uniformly) compute $\mathbf{v}_Q$ simply by writing all coefficients of Q in its sparse representation. By the definition of M we can (uniformly) compute it with $(D+1)^m \cdot D^3 \cdot m$ algebraic operations. In particular, we can (uniformly) compute $(M^{-1})^T$ by the naive algorithm using $O((D+1)^{3m})$ algebraic operations. This implies that $(Q \circ P)|_{\mathbf{z}=\mathbf{0}}$ can be computed by $O((D+1)^{3m+3} \cdot s)$ operations. ◀

We can now construct an efficient succinct circuit for a generating set of invariants for the tensor action. We recall the setting of Section 4, that is, $\mathcal{V} := \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$, with $G := \mathrm{SL}_n \times \mathrm{SL}_n \times \mathrm{SL}_m$ acting on $\mathcal{V}$ via the natural tensor action. We denote $H := \mathrm{SL}_n \times \mathrm{SL}_n$ and $K := \mathrm{SL}_m$ so G is the direct product of its subgroups H and K.

▶ **Theorem 26** (Efficient Succinct Generation of Invariants)**.** *There is a universal constant $c > 0$ such that the following holds. Given any $D \in \mathbb{N}$, there exists a uniform algebraic circuit Φ of size $\leq c \cdot (Dnm^3)^{3m^2+6}$ that computes a succinct generator for the vector space $\mathbb{K}[\mathcal{V}]^G_{\leq D}$. Moreover, the circuit Φ has $1 + m \cdot D^2$ auxiliary variables and computes a polynomial with individual degree upper bounded by D.*

Proof. By Equation (7), we have $\mathbb{K}[\mathcal{V}]^G = (\mathbb{K}[\mathcal{V}]^H)^K$ as graded $\mathbb{K}$-algebras. Thus, we have $\mathbb{K}[\mathcal{V}]^G_{\leq D} = \left(\mathbb{K}[\mathcal{V}]^H_{\leq D}\right)^K$. By Theorem 14, we have that $\mathbb{K}[\mathcal{V}]^H$ is spanned by the homogeneous polynomials

$$f_T(X) := \det\left(\sum_{i=1}^{m} T_i \otimes X_i\right),$$

where $T = (T_1, \ldots, T_m) \in \mathrm{Mat}(d, \mathbb{K})^m$ and $d \in \mathbb{N}$. In particular, if $N := \dim \mathbb{K}[V]^H_{\leq D}$, there are N tuples of matrices $\left\{T^{(e)}\right\}_{e\in[N]}$, where $T^{(e)} \in \mathrm{Mat}(d_e, \mathbb{K})^m$ for some $d_e \leq D$ such that, denoting by $f_e(X) := f_{T^{(e)}}(X)$, we have that $\mathbb{K}[\mathcal{V}]^H_{\leq D} = \mathrm{span}_{\mathbb{K}} \{f_e\}_{e\in[N]}$. Thus, we have

$$\mathbb{K}[\mathcal{V}]^G_{\leq D} = \mathrm{span}_{\mathbb{K}} \{\mathcal{R}_G(f_e)\}_{e\in[N]} = \mathrm{span}_{\mathbb{K}} \{\mathcal{R}_K(f_e)\}_{e\in[N]}, \tag{10}$$

where the last equality above comes from the fact that $\mathcal{R}_G = \mathcal{R}_K \circ \mathcal{R}_H$, by Lemma 17, together with the fact that $\mathcal{R}_H(f_e) = f_e$ since f_e is an H-invariant.

Now, let $Y := (Y_1, \ldots, Y_m)$ be a tuple of symbolic $D \times D$ matrices, and for each $r \in [D]$ and $i \in [m]$, let $Y_i^{(r)} := (Y_i)_{[r]\times[r]}$ be the top-left $r \times r$ principal submatrix of Y_i. Define

$$F_r(Y, X) := f_{Y^{(r)}}(X) = \det\left(\sum_{i=1}^{m} Y_i^{(r)} \otimes X_i\right).$$

Letting u be a formal variable and using the Lagrange interpolation polynomials $L_r(u) := \prod_{\substack{i\in[D]\\ i\neq r}} \frac{u-i}{r-i}$, we have that the following polynomial is a succinct generator for the non-constant polynomials in $\mathbb{K}[V]^H_{\leq D}$

$$F(u, Y, X) := \sum_{r=1}^{D} L_r(u) \cdot F_r(Y, X). \tag{11}$$

To see that the above polynomial is a succinct generator, note that for any $e \in [N]$, if we set $u = d_e$ and $\widehat{Y}_i = T^{(e)} \oplus 0_{D-d_e}$, we have that $F(d_e, \widehat{Y}, X) = L_{d_e}(d_e) \cdot F_{d_e}(\widehat{Y}, X) = f_{T^{(e)}}(X) = f_e$.

The above, together with Equation (10) implies that $\mathcal{R}_K(F(u, Y, X))$ is a succinct generator for $\mathbb{K}[V]^G_{\leq D}$. Using Equation (6) to express $\mathcal{R}_K$ in terms of Ω, we have that the action of $\mathcal{R}_K$ on $F(u, Y, X)$ is given by

$$\begin{aligned}
\mathcal{R}_K(F(u, Y, X)) &= \sum_{r=1}^{D} L_r(u) \cdot \mathcal{R}_K(F_r(Y, X)) = \sum_{r=1}^{D} L_r(u) \cdot \mathcal{R}_K(f_{Y^{(r)}}(X)) \\
&= \sum_{r=1}^{D} L_r(u) \cdot c^{-1}_{rn(m-1)/m,m} \cdot \Omega^{rn(m-1)/m} \left(\widetilde{\pi}_K(Z) \circ f_{Y^{(r)}}(X)\right)) \\
&= \sum_{r=1}^{D} L_r(u) \cdot c^{-1}_{rn(m-1)/m,m} \cdot \Omega^{rn(m-1)/m} \left(f_{Y^{(r)}}(\pi_K(Z)^{-1} \circ X))\right). \qquad (12)
\end{aligned}$$

By definition of the Ω-process (see Equation (5)), we have that $\Omega^{rn(m-1)/m}$ is a polynomial derivative operator over m^2 variables, with integral coefficients, and of individual degree $\leq rn(m-1)/m$. In particular, its sparse representation has $\leq (rn(m-1)/m)^{m^2}$ terms, each monomial having an integral coefficient, and they can all be simultaneously computed uniformly with $(rn(m-1)/m)^{2m^2}$ algebraic operations by the naive algorithm. Note that $f_{Y^{(r)}}(\pi_K(Z)^{-1} \circ X)$ can be computed by a (uniform) circuit Ψ_r of size $O((rn \cdot m^3)^3)$, as $f_{Y^{(r)}}$ is the determinant of size $rn \times rn$ symbolic matrix whose entries involve determinants of size m matrices.[4] By Proposition 25 there is a universal constant $C > 0$ and a (uniform) circuit Φ_r of size $C \cdot (rn)^{3m^2+3} \cdot (rnm^3)^3$ such that Φ_r computes $\Omega^{rn(m-1)/m}\left(f_{Y^{(r)}}(\pi_K(Z)^{-1} \circ X)\right)$.[5] Note that the Ω-process constants can also be computed by a uniform circuit with the same upper bound as above.

Combining the circuits Φ_r with $L_r(u)$ and the Ω-process constants, we obtain a uniform circuit Φ of size $\leq 3 \cdot C \cdot (Dnm^3)^{3m^2+6}$ computing $\mathcal{R}_K(F(u, Y, X))$. Taking $c := 3C$ finishes the proof. It is easy to see from the above construction the bound on the number of auxiliary variables as well as on the individual degree of the succinct generator. ◀

We can now prove our second main result: Theorem 8, which gives a uniform, polynomial-sized succinct generating circuit for the natural tensor action, whenever the third tensor factor is of constant dimension.

▶ **Theorem 8.** *Assume $m = O(1)$. Then, there is a uniform family of $\mathrm{poly}(n)$-sized arithmetic circuit C that succinctly encodes $\mathbb{K}[\mathcal{V}]^G$.*

Proof of Theorem 8. By Theorem 21, the invariant ring $\mathbb{K}[\mathcal{V}]^G$ is generated by invariants of degree at most $D := \frac{3}{8} \cdot m^3 n^2 \cdot (\beta_H)^{2m^2} \leq \frac{3}{8} \cdot m^{2m^2+3} \cdot n^{4m^2+2}$, where the inequality follows from the bound $\beta_H \leq m \cdot n^4$ (Theorem 16).

By Theorem 26, there is an algebraic circuit of size

$$O\left((Dnm^3)^{3m^2+6}\right) = O(m^{6m^4+30m^2+36} \cdot n^{12m^4+33m^2+18}),$$

that succinctly encodes the invariants up to degree D. Since $\mathbb{K}[\mathcal{V}]^G$ is generated by forms of degree at most D, this circuit is a succinct encoding of the invariant ring. When $m = O(1)$, the size of the circuit is $\mathrm{poly}(n)$ and this finishes the proof. ◀

Given the above results, we can now prove our main application: a randomized, polynomial-time algorithm for the Orbit Closure Intersection problem for the natural tensor action, whenever the third factor is of constant dimension.

▶ **Theorem 3.** *The orbit closure intersection problem for the tensor action of $G := \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_n(\mathbb{K}) \times \mathrm{SL}_m(\mathbb{K})$ on $\mathcal{V} := \mathbb{K}^n \otimes \mathbb{K}^n \otimes \mathbb{K}^m$ with $m = O(1)$ is in coRP. More explicitly, given n and two vectors $u, v \in \mathbb{Q}[i]^n \otimes \mathbb{Q}[i]^n \otimes \mathbb{Q}[i]^m$, there exists a randomized algorithm with one-sided bounded error that decides whether the orbit closures of u and v intersect in time polynomial in n and the bit-lengths of u and v.*

[4] As Z is from SL_m, $\pi_K(Z)^{-1}$ can be computed by taking the adjugate matrix.

[5] We can apply Proposition 25, since the derivative operator has the same Z-degree as the polynomial $f_{Y^{(r)}}(\pi_K(Z)^{-1} \circ X))$, and thus

$$\Omega^{rn(m-1)/m}\left(f_{Y^{(r)}}(\pi_K(Z)^{-1} \circ X))\right) = \left(\Omega^{rn(m-1)/m}\left(f_{Y^{(r)}}(\pi_K(Z)^{-1} \circ X))\right)\right)|_{Z=0}.$$

Proof. By Theorem 8, there is a uniform algebraic circuit $C(x_1, x_2, \ldots, x_{n^2m}, y_1, y_2, \ldots, y_r)$ of size $\mathrm{poly}(n)$ that succinctly encodes $\mathbb{K}[\mathcal{V}]^G$. In particular, the number of auxiliary variables r and the bit-lengths of the constants used in C are bounded by $\mathrm{poly}(n)$. By Theorem 26, the degree of C, i.e., the degree of the polynomial that C computes, is also bounded by $\mathrm{poly}(n)$.

Mumford's Theorem 5 implies that

$$\overline{G \cdot u} \cap \overline{G \cdot v} \neq \varnothing \quad \iff \quad C(u_1, \ldots, u_{n^2m}, a_1, \ldots, a_r) = C(v_1, \ldots, v_{n^2m}, a_1, \ldots, a_r)$$

for every $\mathbf{a} \in \mathbb{K}^r$. The latter is an instance of polynomial identity testing. By the Polynomial Identity Lemma, choosing each $a_1, a_2, \ldots, a_r$ uniformly at random from $[3 \deg C]$ and returning the result of the equality check $C(u_1, \ldots, u_{n^2m}, a_1, \ldots, a_r) = C(v_1, \ldots, v_{n^2m}, a_1, \ldots, a_r)$ gives us an algorithm with error probability bounded by $1/3$. Since $\mathrm{size}(C), \deg C \in \mathrm{poly}(n)$, we can compute $C(u, a)$ and $C(v, a)$ and test whether they are equal in $\mathrm{poly}(n, \langle u \rangle, \langle v \rangle)$-time where $\langle \cdot \rangle$ denotes the number of bits in the binary expansion of a vector. This finishes the proof. ◀

References

1. Arturo Acuaviva, Visu Makam, Harold Nieuwboer, David Pérez-Garcia, Friedrich Sittner, Michael Walter, and Freek Witteveen. The minimal canonical form of a tensor network. In *64th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2023*, pages 328–362. IEEE, 2023. doi:10.1109/FOCS57990.2023.00027.
2. Zeyuan Allen-Zhu, Ankit Garg, Yuanzhi Li, Rafael Mendes de 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, STOC 2018*, pages 172–181. ACM, 2018. doi:10.1145/3188745.3188942.
3. Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, March 1993. doi:10.1103/PhysRevLett.70.1895.
4. Charles H. Bennett, Sandu Popescu, Daniel Rohrlich, John A. Smolin, and Ashish V. Thapliyal. Exact and asymptotic measures of multipartite pure-state entanglement. *Physical Review A*, 63:012307, December 2000. doi:10.1103/PhysRevA.63.012307.
5. Markus Bläser. A $5/2n^2$-lower bound for the multiplicative complexity of $n \times n$-matrix multiplication. In *STACS 2001*, pages 99–109. Springer, 2001.
6. Peter A. Brooksbank and Eugene M. Luks. Testing isomorphism of modules. *Journal of Algebra*, 320(11):4020–4029, 2008. Computational Algebra. doi:10.1016/j.jalgebra.2008.07.014.
7. Peter Bürgisser. Optimization, complexity and invariant theory (invited talk). In *38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021*, volume 187, pages 1:1–1:20. Schloss Dagstuhl, 2021. doi:10.4230/LIPIcs.STACS.2021.1.
8. Peter Bürgisser, Michael Clausen, and Mohammad A Shokrollahi. *Algebraic complexity theory*, volume 315. Springer Science & Business Media, 2013.
9. Peter Bürgisser, Mahmut Levent Doğan, Visu Makam, Michael Walter, and Avi Wigderson. Polynomial Time Algorithms in Invariant Theory for Torus Actions. In *36th Computational Complexity Conference (CCC 2021)*, pages 32:1–32:30. Schloss Dagstuhl, 2021. doi:10.4230/LIPIcs.CCC.2021.32.
10. Peter Bürgisser, Mahmut Levent Doğan, Visu Makam, Michael Walter, and Avi Wigderson. Complexity of Robust Orbit Problems for Torus Actions and the abc-Conjecture. In *39th Computational Complexity Conference (CCC 2024)*, volume 300, pages 14:1–14:48. Schloss Dagstuhl, 2024. doi:10.4230/LIPIcs.CCC.2024.14.

11 Peter Bürgisser, Cole Franks, Ankit Garg, Rafael 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 *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 845–861. IEEE, 2019. arXiv:1910.12375, version 3. arXiv:1910.12375.

12 Peter Bürgisser and Christian Ikenmeyer. Explicit lower bounds via geometric complexity theory. In *Symposium on Theory of Computing Conference, STOC 2013*, pages 141–150. ACM, 2013. doi:10.1145/2488608.2488627.

13 Zhili Chen, Joshua A. Grochow, Youming Qiao, Gang Tang, and Chuanqi Zhang. On the complexity of isomorphism problems for tensors, groups, and polynomials III: actions by classical groups. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference, ITCS 2024, Berkeley, CA, USA, January 30 - February 2, 2024*, volume 287 of *LIPIcs*, pages 31:1–31:23. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPIcs.ITCS.2024.31.

14 Harm Derksen. Polynomial bounds for rings of invariants. *Proceedings of the American Mathematical Society*, 129(4):955–963, 2001.

15 Harm Derksen and Gregor Kemper. *Computational Invariant Theory*. Springer, 2015.

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

17 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.

18 Harm Derksen and Visu Makam. An exponential lower bound for the degrees of invariants of cubic forms and tensor actions. *Advances in Mathematics*, 368:107136, 2020.

19 Harm Derksen and Jerzy Weyman. Semi-invariants of quivers and saturation for littlewood-richardson coefficients. *Journal of the American Mathematical Society*, 13(3):467–479, 2000.

20 Mátyás Domokos and Alexander N Zubkov. Semi-invariants of quivers as determinants. *Transformation groups*, 6(1):9–24, 2001.

21 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, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. doi:10.1007/978-3-642-40328-6_37.

22 William Cole Franks and Philipp Reichenbach. Barriers for recent methods in geodesic optimization. In *36th Computational Complexity Conference, CCC 2021*, volume 200, pages 13:1–13:54. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.CCC.2021.13.

23 Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. Operator scaling: theory and applications. *Foundations of Computational Mathematics*, 20(2):223–290, 2020. doi:10.1007/S10208-019-09417-Z.

24 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 *35th Computational Complexity Conference, CCC 2020*, volume 169, pages 12:1–12:17. Schloss Dagstuhl, 2020. doi:10.4230/LIPIcs.CCC.2020.12.

25 Joshua A. Grochow. Matrix Isomorphism of Matrix Lie Algebras. In *2012 IEEE 27th Conference on Computational Complexity*, pages 203–213, 2012. doi:10.1109/CCC.2012.34.

26 Joshua A. Grochow and Youming Qiao. On p-Group Isomorphism: Search-To-Decision, Counting-To-Decision, and Nilpotency Class Reductions via Tensors. In *36th Computational Complexity Conference (CCC 2021)*, volume 200, pages 16:1–16:38. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.CCC.2021.16.

27 Joshua A. Grochow and Youming Qiao. On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials I: Tensor Isomorphism-Completeness. In *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, volume 185, pages 31:1–31:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.ITCS.2021.31.

28 Joshua A. Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials IV: linear-length reductions and their applications. In Michal Koucký and Nikhil Bansal, editors, *Proceedings of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025*, pages 766–776. ACM, 2025. doi:10.1145/3717823.3718282.

29 Joshua A. Grochow, Youming Qiao, Katherine E. Stange, and Xiaorui Sun. On the complexity of isomorphism problems for tensors, groups, and polynomials V: over commutative rings. In Michal Koucký and Nikhil Bansal, editors, *Proceedings of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025*, pages 777–784. ACM, 2025. doi:10.1145/3717823.3718286.

30 Masaki Hamada and Hiroshi Hirai. Computing the nc-rank via discrete convex optimization on cat (0) spaces. *SIAM Journal on Applied Algebra and Geometry*, 5(3):455–478, 2021. doi:10.1137/20M138836X.

31 David Hilbert. Über die Theorie der algebraischen Formen. *Math. Ann.*, 36(4):473–534, 1890. doi:10.1007/BF01208503.

32 David Hilbert. Über die vollen Invariantensysteme. *Math. Ann.*, 42:313–373, 1893. URL: http://eudml.org/doc/157652.

33 Pavel Hrubeš and Avi Wigderson. Non-commutative arithmetic circuits with division. *Theory Comput.*, 11:357–393, 2015. doi:10.4086/TOC.2015.V011A014.

34 Gábor Ivanyos and Youming Qiao. On the orbit closure intersection problems for matrix tuples under conjugation and left-right actions. In *2023 ACM-SIAM Symposium on Discrete Algorithms, SODA 2023*, pages 4115–4126. SIAM, 2023. doi:10.1137/1.9781611977554.CH158.

35 Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Non-commutative edmonds' problem and matrix semi-invariants. *Comput. Complex.*, 26(3):717–763, 2017. doi:10.1007/S00037-016-0143-X.

36 Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *Comput. Complex.*, 27(4):561–593, 2018. doi:10.1007/S00037-018-0165-7.

37 Zhengfeng Ji, Youming Qiao, Fang Song, and Aaram Yun. General linear group action on tensors: A candidate for post-quantum cryptography. In *Theory of Cryptography - 17th International Conference, TCC 2019*, volume 11891 of *Lecture Notes in Computer Science*, pages 251–281. Springer, 2019. doi:10.1007/978-3-030-36030-6_11.

38 Neeraj Kayal and Nitin Saxena. Complexity of Ring Morphism Problems. *computational complexity*, 15(4):342–390, December 2006. doi:10.1007/s00037-007-0219-8.

39 Hanspeter Kraft. *Geometrische Methoden in der Invariantentheorie*. Aspects of Mathematics, D1. Friedr. Vieweg & Sohn, Braunschweig, 1984. doi:10.1007/978-3-322-83813-1.

40 Vladimir Lysikov and Michael Walter. Complexity theory of orbit closure intersection for tensors: reductions, completeness, and graph isomorphism hardness, 2025. doi:10.48550/arXiv.2411.04639.

41 Ketan Mulmuley. Geometric complexity theory v: Efficient algorithms for noether normalization. *Journal of the American Mathematical Society*, 30(1):225–309, 2017.

42 Ketan Mulmuley and Milind A. Sohoni. Geometric complexity theory I: an approach to the P vs. NP and related problems. *SIAM J. Comput.*, 31(2):496–526, 2001. doi:10.1137/S009753970038715X.

43 David Mumford, John Fogarty, and Frances Kirwan. *Geometric invariant theory*, volume 34. Springer Science & Business Media, 1994.

44 Vladimir L Popov. Constructive invariant-theory. *Astérisque*, pages 303–334, 1981.

45 Vladimir L Popov. The constructive theory of invariants. *Mathematics of the USSR-Izvestiya*, 19(2):359, 1982.

46 Aidan Schofield and Michel Van den Bergh. Semi-invariants of quivers for arbitrary dimension vectors. *Indagationes Mathematicae*, 12(1):125–138, 2001.

47 Nicolas Sendrier and Dimitris E. Simos. The Hardness of Code Equivalence over $\mathbb{F}_q$ and Its Application to Code-Based Cryptography. In *Post-Quantum Cryptography*, pages 203–216, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. doi:10.1007/978-3-642-38616-9_14.

48 V Strassen. Relative bilinear complexity and matrix multiplication. *Journal für die reine und angewandte Mathematik*, 374:406–443, 1987.

49 Avi Wigderson. Non-commutative optimization - where algebra, analysis and computational complexity meet. In *ISSAC '22: International Symposium on Symbolic and Algebraic Computation, 2022*, pages 13–19. ACM, 2022. doi:10.1145/3476446.3535489.