Symbolic determinant identity testing (SDIT) is not a null cone problem; and the symmetries of algebraic varieties

Visu Makam
School of Mathematics
Institute for Advanced Study
Princeton, USA
visu@umich.edu

Avi Wigderson
School of Mathematics
Institute for Advanced Study
Princeton, USA
Email: avi@ias.edu

***Abstract*—The object of study of this paper is the following multi-determinantal algebraic variety, $\mathrm{SING}_{n,m}$, which captures the symbolic determinant identity testing (SDIT) problem (a canonical version of the polynomial identity testing (PIT) problem), and plays a central role in algebra, algebraic geometry and computational complexity theory. $\mathrm{SING}_{n,m}$ is the set of all m-tuples of $n \times n$ complex matrices which span *only* singular matrices. In other words, the determinant of any linear combination of the matrices in such a tuple vanishes.**

The algorithmic complexity of testing membership in $\mathrm{SING}_{n,m}$ is a central question in computational complexity. Having almost a trivial probabilistic algorithm, finding an efficient deterministic algorithm is a holy grail of derandomization, and to top it, will imply super-polynomial circuit lower bounds!

A sequence of recent works suggests efficient deterministic "geodesic descent" algorithms for memberships in a general class of algebraic varieties, namely the *null cones* of (reductive) linear group actions. Can such algorithms be used for the problem above? Our main result is *negative*: $\mathrm{SING}_{n,m}$ is *not* the null cone of any such group action! This stands in stark contrast to a non-commutative analog of this variety (for which such algorithms work), and points to an inherent structural difficulty of $\mathrm{SING}_{n,m}$. In other words, we provide a barrier for the attempts of derandomizing SDIT via these algorithms.

To prove this result we identify precisely the group of symmetries of $\mathrm{SING}_{n,m}$. We find this characterization, and the tools we introduce to prove it, of independent interest. Our characterization significantly generalizes a result of Frobenius for the special case $m = 1$ (namely, computing the symmetries of the determinant). Our proof suggests a general method for determining the symmetries of general algebraic varieties, an algorithmic problem that was hardly studied and we believe is central to algebraic complexity.

***Keywords*-polynomial identity testing; null cone membership; symmetries of algebraic varieties;**

We begin with a general discussion of the main problems and their motivations. Next we turn to describe our main object of study - singular spaces of matrices. We then state our main results. Finally, we end by discussing some open problems and future directions. While a few technical terms here may be unfamiliar to some readers, we will have a simple running example to demonstrate all essential notions. Throughout, the underlying field is the complex numbers $\mathbb{C}$.

I. Motivation and main problems

Consider a (reductive[1]) group G acting (algebraically) on a vector space V by linear transformations. Understanding this very general setting is the purview of *invariant theory*. As a simple, and very relevant running example, consider the following.

Example 1.1 (Running example): Consider $G = \mathrm{SL}_n$ acting on $n \times n$ matrices (namely $V = \mathbb{C}^{n^2}$) by left multiplication, i.e, the action of $P \in \mathrm{SL}_n$ sends the matrix X to PX.

A group action partitions V into *orbits*: the orbit of v is the set of all points in V it can be moved to by an element $g \in G$. An even more natural object in our setting is the *orbit closure*: all limit points of an orbit[2].

The *null cone* of a group action is the set of points $v \in V$ whose orbit closure contains the origin, namely the point 0. Null cones of group actions are central to invariant theory, and are interesting algebraic objects to study in mathematics and physics. More recently, connections to fundamental problems in computational complexity have surfaced. Diverse problems (see [GGOW16], [BGO$^+$18]) such as bipartite matching, equivalence of non-commutative rational expressions, tensor scaling and quantum distillation, can each be formulated (for specific choices of G, V and an action) as a *null cone membership problem* – given a point $v \in V$, decide if it is in the null cone. Note that in our running example, i.e., Example 1.1, the null cone is precisely the set of singular matrices.

A closely related problem is the *orbit closure intersection problem* – given $v, w \in V$, decide if the orbit closures of v and w intersect. The orbit closure intersection problem is a generalization of the null cone membership problem, and this too has many connections with arithmetic complexity. For example, the graph isomorphism problem can be phrased as an orbit closure intersection problem! We refer to [Mul17] for more details on the aforementioned problems and their

[1] A technical term that includes all classical groups.

[2] where limits can be equivalently taken in the Euclidean or Zariski topology

2575-8454/20/$31.00 ©2020 IEEE
DOI 10.1109/FOCS46700.2020.00086

relevance in the Geometric Complexity Theory (GCT) program, which is an algebro-geometric approach to the VP vs VNP problem (Valiant's algebraic analog of P vs NP), a starting point of which is that the determinant and permanent polynomials are determined by their symmetries. Note that in Example 1.1, the orbit closure of two matrices X and Y intersect precisely when $\det(X) = \det(Y)$.

In an exciting series of recent works, efficient algorithms for the null cone membership and orbit closure intersection problems in various cases have been discovered, and moreover techniques have developed that may allow significant generalization of their applicability [GGOW16], [IQS18], [FS13], [DM17b], [DM18a], [GGOW18], [AZGL$^+$18], [BGO$^+$18], [BFG$^+$18], [Fra18], [DM17a], [DM18b]. Curiously, Geometric Complexity Theory (morally) predicts efficient algorithms for null cone membership problems in great generality (see [Mul17] for precise formulations), although establishing this remains an elusive goal.

What is remarkable is the possibility that such efficient algorithms, through the work of [KI04], enable proving non-trivial *lower bounds* on computation, the major challenge of computational complexity. Specifically, what is needed is a deterministic polynomial time algorithm for a problem called Symbolic Determinant Identity Testing (SDIT)[3] that is central to this work, and will be defined soon. SDIT happens to be a membership problem in an *algebraic variety*, a context generalizing null cones.

A subset $S \subseteq V$ is called an algebraic variety[4] (or simply a *variety*) if it is the zero locus of a collection of polynomial functions on V.[5] Many algorithmic problems can be phrased as "membership in a variety", and is non-trivial when the underlying set of polynomials is given implicitly or are difficult to compute. It is a fundamental result of invariant theory that *every null cone is an algebraic variety*, a connection which goes through *invariant polynomials* of group actions. A polynomial function f on V is called invariant if it is constant along orbits, i.e., $f(gv) = f(v)$ for all $g \in G, v \in V$. Invariant polynomials form a graded subring of $\mathbb{C}[V]$, the ring of polynomial functions on V. Mumford proved that the orbit closures of any two points $v, w \in V$ intersect, if and only if $f(v) = f(w)$ for all invariant polynomials[6], see [MFK94]. As a consequence, the null cone can also be described as the zero locus of all (non-constant) homogenous invariant polynomials. Indeed, this analytic-algebraic connection provides the path to structural and algorithmic understanding of the null cone membership and orbit closure intersection problems via invariant theory.

Summarizing, if a variety $S \subseteq V$ happens to be a null cone for some group action, then the aforementioned algorithms can be used to decide "membership in S", with the exciting possibility that they could very well be efficient. Of course, not every variety is a null cone, which leads to the following interesting problem:

Problem 1.2: Given a variety $S \subseteq V$, is it the null cone for the (algebraic) action of a (reductive) group G on V?

We now make an important observation. If S is to be the null cone for the action of a group G, then the group must "preserve" S, i.e., for all $g \in G$, we must have $gS = S$. We define the *group of symmetries* to be the (largest) subgroup of $\mathrm{GL}(V)$ consisting of all linear transformations that preserve S. With reference to Example 1.1, one might ask which is the largest group of symmetries in GL_{n^2} which preserves the set of $n \times n$ the singular matrices (which is defined by the zeros of the single determinant polynomial). This question was resolved by Frobenius [Fro97] as we will later see, and is a very special case of our main technical result.

So, the (hypothetical) acting group G must be a subgroup[7] of the group of symmetries of S. Roughly speaking, this provides an important "upper bound" to the groups that one must consider while resolving Problem 1.2.

Problem 1.3: Given a variety $S \subseteq V$, compute its group of symmetries.

Needless to say, the important role of symmetries in mathematics is present in just about every branch, and exploiting symmetries is an immensely powerful tool. Specifically, the fact that the determinant and permanent polynomials are *defined* by their symmetries form the starting point to the GCT program of Mulmuley and Sohoni [MS01], [MS08] mentioned earlier towards the VP $\neq$ VNP conjecture. Computing the group of symmetries of an algebraic variety is an extremely natural problem (even in the absence of Problem 1.2!), and may be useful for other purposes. We now elaborate informally on the path we take to solve Problem 1.3, and another natural problem it raises.

The group of symmetries of an algebraic variety $S \subseteq V$ is always an algebraic subgroup of $\mathrm{GL}(V)$ (and hence a Lie subgroup). Suppose that H is an algebraic group that acts linearly on a vector space V. It is a fact that the null cone for the action of its identity component[8] (denoted H°) is the same as the null cone for the action of H. Thus, for Problem 1.2, one might as well study the *connected group of symmetries*, i.e., the identity component of the group of symmetries. Indeed, if S is the null cone for the action of a reductive group G, then it is the null cone for the action of its identity component G°, which must be a subgroup of

[3]A canonical version of the Polynomial Identity Testing (PIT) problem.

[4]We do not require irreducibility in our definition of varieties.

[5]All our varieties are explicitly described with coordinates in Euclidean space. In the literature, they are sometimes called (affine) embedded varieties.

[6]Reductivity is essential for this.

[7]Any group G acting on V gives a map $\rho : G \to \mathrm{GL}(V)$. The null cone for G is the same as the null cone for $\rho(G)$, so we can always restrict ourselves to subgroups of $\mathrm{GL}(V)$ when concerned about Problem 1.2. Moreover, note that if G is reductive, so is $\rho(G)$.

[8]The identity component is the connected component of H that contains the identity element. It is always an algebraic subgroup.

the connected group of symmetries. Thus, we are led to the problem below.

Problem 1.4: Given a variety $S \subseteq V$, compute its connected group of symmetries.

Problem 1.4 turns out to be much easier than Problem 1.3. Indeed, while both are non-linear, Problem 1.4 can be "linearized". The reason is that the connected group of symmetries is a connected algebraic subgroup of $\mathrm{GL}(V)$, and so in particular is determined by its Lie algebra (which is a Lie subalgebra of the Lie algebra of $\mathrm{GL}(V)$). The benefit of the Lie algebra perspective is that computations tend to be linear algebraic in nature.

To do such a computation, we will however need a sufficient understanding of the ideal of *all* polynomials vanishing on S. For $S = \mathrm{SING}_{n,m}$, the ideal of polynomials is quite complicated and we do not know how to determine the ideal (we list this as an open problem, i.e., Problem 4.6). Nevertheless, we are able to extract sufficient information about the ideal to proceed with the computation using techniques from representation theory, see [MW19] for details.

Perhaps the most important point to note is that the computation is algorithmically efficient if one is given the ideal generators explicitly (say in the monomial representation). It is interesting to further study the algorithmic issues in computing symmetries when the ideal generators are given in a more implicit or concise form (as in the case of $\mathrm{SING}_{n,m}$ that we solve). We state this also as an open problem, see Problem 4.3.

Algebraic varieties are defined as the zero locus of a collection of polynomials. Suppose we have a collection of homogeneous polynomials $\{f_i : i \in I\}$, and let S be its zero locus. If the ring of invariants for the action of some group G is precisely $\mathbb{C}[f_i : i \in I]$, then S would be the null cone (recall that the null cone can be seen as the zero locus of non-constant homogeneous invariant polynomials). This brings us to another interesting problem, which can be seen as a scheme-theoretic version of Problem 1.2.

Problem 1.5: Given a collection of polynomials $\{f_i : i \in I\}$ on V, is there a group G acting on V by linear transformations such that the ring of invariants is $\mathbb{C}[\{f_i : i \in I\}]$.

Curiously, the above problem is in some sense is an inverse problem to the classical one in invariant theory: there, given a group action on V, we seek its invariant polynomials, whereas here we are given the polynomials, and seek the group which makes them all invariant.

Remark 1.6: Both Problem 1.3 and Problem 1.5 belong to a general class of problems called *linear preserver problems*. We refer the reader to the survey [LP01] which contains in particular some general techniques for approaching linear preserver problems. These techniques do not seem to be sufficient for us.

All the aforementioned problems are very natural structural and algorithmic problems at the interface of computational complexity (especially algebraic complexity) and algebra (mainly representation theory, invariant theory and algebraic geometry). To the best of our knowledge, very little work on them was done so far, and we expect that further progress will be fruitful for both sides of this collaboration.

II. The algebraic variety SING and the computational problem SDIT

Having introduced the problems of interest, let us introduce the variety which we will be the main focus of this paper. Let Mat_n denote $n \times n$ matrices with entries in $\mathbb{C}$. Let $t_1, \ldots, t_m$ be indeterminates, and let $\mathbb{C}(t_1, \ldots, t_m)$ denote the function field in m indeterminates. Define

$$\mathrm{SING}_{n,m} \triangleq \left\{ \begin{array}{c} X = (X_1, \ldots, X_m) \in \mathrm{Mat}_n^m : \\ \sum_{i=1}^m t_i X_i \text{ singular (over } \mathbb{C}(t_1, \ldots, t_m)) \end{array} \right\}. \tag{1}$$

Note that $\mathrm{SING}_{n,m} \subseteq V = \mathrm{Mat}_n^m = \mathbb{C}^{mn^2}$, given by the zero locus of all polynomials $\{\det(c_1 X_1 + c_2 X_2 + \cdots + c_m X_m) : c_i \in \mathbb{C}\}$. While this is an uncountable set, one can easily replace it with a finite set whose zero locus is still $\mathrm{SING}_{n,m}$. Another important note is that the case $m = 1$ is the null cone for our simple running example (Example 1.1) of the previous subsection!

The variety $\mathrm{SING}_{n,m}$ is of central importance in computational complexity. The membership problem for $\mathrm{SING}_{n,m}$ (i.e., given $X \in \mathrm{Mat}_n^m$, decide if $X \in \mathrm{SING}_{n,m}$) is often called Symbolic Determinant Identity Testing (SDIT). This problem is also sometimes referred to as the *Edmonds' problem*, as Edmonds' paper [Edm67] first explicitly defined it and asked if it has a polynomial time algorithm. Note that any *fixed* tuple $X = (X_1, \ldots, X_m) \in \mathrm{SING}_{n,m}$ if and only if the *symbolic* determinant $\det(t_1 X_1 + t_2 X_2 + \ldots t_m X_m)$ vanishes identically when viewed now as a polynomial in the new variables $t_1, \ldots, t_m$. This viewpoint immediately provides an efficient *probabilistic* algorithm for the SDIT [Lov79]: given X, simply pick (appropriately) at random values for the variables t_i and evaluate the resulting *numeric* determinant.

The importance of determining the complexity of SDIT stems from several central results in arithmetic complexity and beyond. First, Valiant's completeness theorem for VP [Val79] implies that SDIT captures the general problem of Polynomial Identity Testing (PIT) (see the survey [SY09], for background and status of this problem, and more generally on arithmetic complexity).[9] An equivalent way of phrasing Valiant's result is that SDIT *is* the *word problem* for $\mathbb{C}(t_1, \ldots, t_m)$, namely testing if a rational expression in $\mathbb{C}(t_1, \ldots, t_m)$ is identically zero. A second, and far more surprising result of Kabanets and Impagliazzo [KI04] shows that efficient *deterministic* algorithms for PIT would imply

[9]Derandomizing special cases of PIT has been (and continues to be) the subject of attention for many complexity theorists (although most often with techniques that don't seem to generalize to SDIT).

circuit lower bounds, a holy grail of complexity theory. SDIT also plays an important role in the GCT program, see [Mul17]. Finally, the structural study of the variety $\mathrm{SING}_{n,m}$, namely of singular spaces of matrices is a rich subject in linear algebra and geometry (see e.g. [FR07], [EH88], [RW19], [Mes85], [Mes90], [GM02] and references therein).

It is illustrative to compare with the non-commutative version of the above story, and we will do so. Let $t_1, \ldots, t_m$ be now *non-commuting* indeterminates, and let $\mathbb{C}\langle\langle t_1, \ldots, t_m \rangle\rangle$ denote the free skew field[10]. Consider

$$\mathrm{NSING}_{n,m} \triangleq \left\{ \begin{array}{c} X = (X_1, \ldots, X_m) \in \mathrm{Mat}_n^m : \\ \sum_i t_i X_i \text{ singular (over } \mathbb{C}\langle\langle t_1, \ldots, t_m \rangle\rangle) \end{array} \right\},$$

which is clearly a non-commutative analog of $\mathrm{SING}_{n,m}$. Moreover, membership in $\mathrm{NSING}_{n,m}$ captures the word problem over the free skew field $\mathbb{C}\langle\langle t_1, \ldots, t_m \rangle\rangle$ (often called non-commutative rational identity testing (RIT)) in precisely the same manner as membership in $\mathrm{SING}_{n,m}$ captures the word problem over the function field $\mathbb{C}(t_1, \ldots, t_m)$.

The surprising fact is that membership in $\mathrm{NSING}_{n,m}$ *does* have polynomial time deterministic algorithms, see [GGOW16], [IQS18]. The main point to note is that the algorithms use crucially the fact that $\mathrm{NSING}_{n,m}$ is a null cone! Indeed, it is the null cone for the so called left-right action of $\mathrm{SL}_n \times \mathrm{SL}_n$ on Mat_n^m which is defined by:

$$(P, Q) \cdot (X_1, \ldots, X_m) = (PX_1Q^t, PX_2Q^t, \ldots, PX_mQ^t),$$

where Q^t denotes the transpose of the matrix Q. In view of this, it is only natural to ask whether a similar approach can be used to give an efficient algorithm for membership in $\mathrm{SING}_{n,m}$. This provides the principal motivation for studying Problem 1.2.

III. Main results

In this paper, we will answer Problem 1.2 and Problem 1.3 (and hence also Problem 1.4) for $S = \mathrm{SING}_{n,m}$. Moreover, recall that $\mathrm{SING}_{n,m}$ is the zero locus of a natural collection of polynomials, namely $\{\det(\sum_i c_i X_i) : c_i \in \mathbb{C}\}$. We also give a negative answer to Problem 1.5 for this collection of polynomials. We will now proceed to give precise statements.

We first state our main result, which is a negative answer to Problem 1.2 for $\mathrm{SING}_{n,m}$.

Theorem 3.1: Let $n, m \geq 3$. Let G be any reductive group acting algebraically on Mat_n^m by linear transformations. Then the null cone for the action of G is not equal to $\mathrm{SING}_{n,m}$.

[10]The free skew field is intuitively the natural non-commutative analog of $\mathbb{C}(t_1, \ldots, t_m)$, namely may be viewed as the field of fractions completing non-commutative polynomials. However, we note that its very existence, let alone its construction is highly non-trivial, and was first established by Amitsur [Ami66] (see also [Coh95]). For one illustration of the complexity of this field, it is easy to see that unlike in the commutative case, its elements cannot be represented as ratios of polynomials (or any finite number of inversions - an important result of [Reu96]).

First, and foremost, let us observe that the condition $n, m \geq 3$ cannot be removed or even improved. Indeed, if $n \leq 2$ or $m \leq 2$, we have $\mathrm{SING}_{n,m} = \mathrm{NSING}_{n,m}$ and hence it is a null cone! Thus, the above theorem gives the strongest possible statement of this nature. The above theorem follows from the following one, which has no restrictions on n and m.

Theorem 3.2: Let G be any reductive group acting algebraically on $V = \mathrm{Mat}_n^m$ by linear transformations which preserve $\mathrm{SING}_{n,m}$ (i.e., $g \cdot \mathrm{SING}_{n,m} = \mathrm{SING}_{n,m}$ for all $g \in G$). Let $\mathcal{N} = \mathcal{N}_G(V)$ denote the null cone for this action. If the null cone $\mathcal{N} \subseteq \mathrm{SING}_{n,m}$, then the null cone $\mathcal{N} \subseteq \mathrm{NSING}_{n,m}$.

Indeed, Theorem 3.1 follows from the above theorem as $n, m \geq 3$ is precisely the condition needed to ensure that $\mathrm{NSING}_{n,m}$ is a proper subset of $\mathrm{SING}_{n,m}$.

A crucial component in the proof of the above theorem is the computation of the group of symmetries for $\mathrm{SING}_{n,m}$. The importance of this computation is well beyond the context of this paper. For example, it should serve as the starting point for any approach to SDIT that aims at utilizing symmetry. Let us formally define the group of symmetries for a variety.

Definition 3.3 (Group of symmetries): For a variety $S \subseteq V$, we define its group of symmetries

$$\mathcal{G}_S = \{g \in \mathrm{GL}(V) \mid gS = S\}.$$

The group of symmetries $\mathcal{G}_S$ is always an algebraic subgroup of $\mathrm{GL}(V)$. We call its identity component (denoted $\mathcal{G}_S^\circ$) the connected group of symmetries.

In order to compute the group of symmetries for $\mathrm{SING}_{n,m}$, we first compute the connected group of symmetries. Viewing Mat_n^m as $\mathbb{C}^m \otimes \mathbb{C}^n \otimes \mathbb{C}^n$ elucidates a natural linear action of $\mathrm{GL}_m \times \mathrm{GL}_n \times \mathrm{GL}_n$ on Mat_n^m. Concretely, the action is given by the formula:

$$(P, Q, R) \cdot (X_1, \ldots, X_m) = \left(\sum_{j=1}^m p_{1j} Q X_j R^{-1}, \sum_{j=1}^m p_{2j} Q X_j R^{-1}, \ldots, \sum_{j=1}^m p_{nj} Q X_j R^{-1} \right),$$

where p_{ij} denotes the $(i,j)^{th}$ entry of P. A linear action is simply a representation, so we have a map $\mathrm{GL}_m \times \mathrm{GL}_n \times \mathrm{GL}_n \to \mathrm{GL}(\mathrm{Mat}_n^m)$. We will call the image of this map $G_{n,m}$.

Theorem 3.4: Let $S = \mathrm{SING}_{n,m} \subseteq V = \mathrm{Mat}_n^m$. Then the connected group of symmetries $\mathcal{G}_S^\circ$ is the subgroup $G_{n,m}$.

For more details regarding the strategy of proof for the above theorem, see [MW19] . However, it is worth mentioning that it is essentially a linear algebraic computation on the level of Lie algebras, and is applicable in more generality. At this juncture, we note a classical result of Frobenius that addresses the special case of $m = 1$ (see [Fro97], [Die49]),

which deals with our simple running example earlier. This result is essential for our proof of the above theorem for any value of m. We will also give our own proof of this result as it allows us to illustrate our proof strategy in the simple case.

Theorem 3.5 (Frobenius): Let $S = \mathrm{SING}_{n,1} \subseteq V = \mathrm{Mat}_n$. The group of symmetries $\mathcal{G}_S$ consists of linear transformations of the form $X \mapsto PXQ$ or of the form $X \mapsto PX^tQ$ where $P, Q \in \mathrm{SL}_n$.

First, note that the above result computes the entire group of symmetries! In the general case, let us first note that apriori there could be an incredible number of groups whose identity component is $G_{n,m}$. However, it turns out that they are actually manageable, and with some fairly elementary results on semisimple Lie algebras, we can determine the entire group of symmetries for any m.

Theorem 3.6: Let $S = \mathrm{SING}_{n,m} \subseteq V = \mathrm{Mat}_n^m$. Let τ denote the linear transformation that sends $X = (X_1, \ldots, X_m) \mapsto (X_1^t, \ldots, X_m^t)$. Then the group of symmetries $\mathcal{G}_S = G_{n,m} \cup G_{n,m} \cdot \tau = G_{n,m} \rtimes \mathbb{Z}/2$.

The key idea here is that the entire group of symmetries must normalize the connected group of symmetries, i.e., $G_{n,m}$. So, we compute the normalizer of $G_{n,m}$. To do so, we utilize heavily that the group $G_{n,m}$ is reductive, and use ad-hoc arguments that are particularly suited to this special case. A slightly more abstract approach via automorphisms of Dynkin diagrams such as the one in [Gur94] would work in this case (see also [Lan17]). We do not quite know a general strategy to bridge the gap between the connected group of symmetries and the entire group of symmetries. We also note that the same strategy yields the group of symmetries for $\mathrm{NSING}_{n,m}$

Theorem 3.7: Let $S = \mathrm{NSING}_{n,m} \subseteq \mathrm{Mat}_n$. Then the group of symmetries $\mathcal{G}_S = G_{n,m} \rtimes \mathbb{Z}/2$ (as defined in the above theorem).

Once we compute the group of symmetries, the rest of the argument relies on an understanding of the Hilbert–Mumford criterion which tells us that the null cone is a union of G-orbits of coordinate subspaces (linear subspaces that are defined by the vanishing of a subset of coordinates). In particular, we will show that the union of all the coordinate subspaces contained in $\mathrm{SING}_{n,m}$ moved around by the action of its group of symmetries does not cover all of $\mathrm{SING}_{n,m}$, which will give the contradiction, see [MW19] for details.

Remark 3.8 (Positive characteristic): Our choice in working with $\mathbb{C}$ as a ground field is essentially for simplicity of the exposition and proofs. All our results above (specifically Theorems 3.1, 3.2, 3.4, 3.5, 3.6 and 3.7) hold for every algebraically closed fields of every characteristic. The issues that arise in positive characteristic and the appropriate modifications needed to deal with them are discussed in [MW19, Appendix C].

The variety $\mathrm{SING}_{n,m}$ is the zero locus of some very structured polynomials. Observe that for any $c_i \in \mathbb{C}$, the polynomial $\det(\sum_i c_i X_i)$ vanishes on $\mathrm{SING}_{n,m}$. It is easy to see that the zero locus of the collection of all $\det(\sum_i c_i X_i)$ (for all choices of c_i) is precisely $\mathrm{SING}_{n,m}$.[11] We prove a negative result for Problem 1.5 for this collection of polynomials.

Theorem 3.9: Suppose $n, m \geq 3$. Then the subring $R = \mathbb{C}[\{\det(\sum_i c_i X_i) : c_i \in \mathbb{C}\}] \subseteq \mathbb{C}[\mathrm{Mat}_n^m]$ is not the invariant ring for any linear action of any group G on Mat_n^m.

If we restrict to reductive groups, then the above theorem is a simple consequence of Theorem 3.1 and the alternate definition of null cone as the zero locus of non-constant homogenous invariants. However, we use a different argument that works for *any* group, irrespective of reductivity.

In recent years, problems that look very similar to SDIT have been solved by new invariant theoretic algorithms. Our main result, i.e., Theorem 3.1 can be interpreted as a *barrier* to utilizing such algorithms for SDIT. A variety of barrier results have the subject of several investigations in complexity, see [BGS75], [RR94], [AW09], [Raz89], [Pot16], [FSV17], [GKSS17], [BIJL18], [EGdOW18], [GMdOW19]. Our result, however, has a slightly different flavor from the aforementioned works and provides a *structural barrier* by exhibiting a structural feature (or rather a non-feature) that hinders our ability to approach SDIT through a collection of new and powerful algorithms.

IV. Discussion and open questions

This paper demonstrates another collaboration of different fields in mathematics. Expanding on ongoing work cited in the introduction, here too fundamental problems in computational complexity have given rise to a new flavor of problems that are purely algebraic in nature, some of which arise from analyzing analytic (rather than symbolic) algorithms. We feel that it is important to introduce these problems to representation theorists, algebraic geometers and commutative algebraists. The results of this paper open the door for several further avenues of research, inviting a further collaboration between theoretical computer scientists and mathematicians to resolve them.

Let us begin with the stating that $\mathrm{SING}_{n,m}$ is a very important variety to study due to its connection to circuit lower bounds ([KI04]) that we mentioned earlier. Insights from any field of mathematics may be helpful! The major open problem is of course:

Problem 4.1: Is there a deterministic polynomial time algorithm for SDIT?

[11] It seems plausible that these polynomials generate the ideal of polynomials that vanish on $\mathrm{SING}_{n,m}$, but it is well known in the commutative algebra community such plausible statements can be quite subtle, difficult to prove, and may not always be true. For example, it is a famous long standing open problem to determine the ideal of polynomials that vanish on the variety of commuting matrices, i.e., $\{(X, Y) \in \mathrm{Mat}_n^2 \mid XY = YX\}$, for $n > 3$.

Various subclasses of SDIT (and PIT) have polynomial time algorithms. For example, we say an m-tuple of $n \times n$ matrices $X = (X_1, \ldots, X_m)$ satisfies the property $(R1)$ if the linear subspace in Mat_n^m spanned by $X_1, \ldots, X_m$ has a basis consisting of rank 1 matrices. It turns out that if X satisfies $(R1)$, then $X \in \mathrm{SING}_{n,m}$ if and only if $X \in \mathrm{NSING}_{n,m}$. Thus, SDIT restricted to tuples with the $(R1)$ property can be solved via a null cone membership algorithm! (this is implicit in [Gur04]). One direction of future research is to consider the following natural generalization of the $(R1)$ property.

For fixed $k \in \mathbb{Z}_{\geq 1}$ We say $X = (X_1, \ldots, X_m)$ satisfies the property (Rk) if the linear subspace in Mat_n^m spanned by $X_1, \ldots, X_m$ has a basis consisting of rank $\leq k$ matrices.

Problem 4.2: Is there a deterministic polynomial time algorithm for SDIT for tuples satisfying (Rk)? How about $(R2)$?

Next, we turn to the symmetry group of an algebraic variety.

Problem 4.3: What algorithms can one use to determine the group of symmetries of a variety? How efficient are these algorithms?

In this paper, we explicitly determined the group of symmetries of one family of varieties. It is however very clear that most steps are algorithmic. Roughly speaking, if the generators for the ideal of polynomials vanishing on the variety are given as an input, then determining the Lie algebra of symmetries reduces to solving a system of linear equations. So, in terms of the input size of such generating polynomials given by their coefficients, this Lie algebra part is efficient. It is not entirely clear to us how to obtain the group itself efficiently from the Lie algebra. Moreover, if we are given the generating polynomials that describes the variety (set-theoretically) in an implicit, concise way (as in SING) it seems that more work is needed even to define the computational task. It is possible that when the generators themselves have some symmetries, or rich relations (as in SING), one can do more.

Another general problem to be pursued is to get a better understanding of null cones (and orbit closure equivalence classes)

Problem 4.4: Can one classify null cones? What features must a variety satisfy in order to possibly be a null cone?

In this paper, we used mainly the fact that the null cone must be the translation (by a group element) of a union of coordinate subspaces (i.e., the Hilbert–Mumford criterion). It will be interesting to find other properties of null cones which distinguish them from arbitrary varieties.

A different direction to pursue is the following. The main result of this paper is that $\mathrm{SING}_{n,m}$ is not a null cone for any *reductive* group action. Natural as this condition is mathematically (and we use it and consequences of it here), it is not important algorithmically, and one can potentially implement and analyze null cone membership algorithms using non-reductive groups.[12] So, what if we drop the reductivity assumption?

Problem 4.5: Can $\mathrm{SING}_{n,m}$ be the null cone for the action of a non-reductive group?

Now, we mention a few more problems which are a little bit more technical, and of interest to commutative algebraists and algebraic geometers.

Problem 4.6: Let I be the ideal of polynomials vanishing on $\mathrm{SING}_{n,m}$. Determine the ideal generators of I. Do the determinantal polynomials $\det(\sum_i c_i X_i)$ generate the ideal?

Problem 4.7: Consider the ring $\mathbb{C}[\{\det(\sum_i c_i X_i) : c_i \in \mathbb{C}\}] \subseteq \mathbb{C}[\mathrm{Mat}_{n,n}^m]$. Is it Cohen–Macaulay? What is its regularity, etc?

ACKNOWLEDGMENT

We would like to especially thank J. M. Landsberg for suggesting that we compute the group of symmetries, and Gurbir Dhillon for helping us with the Lie theoretic statements needed for the computation. In addition, we also thank Ronno Das, Harm Derksen, Ankit Garg, Robert Guralnick, Alexander Kleschev, Thomas Lam, Daniel Litt, Rafael Oliveira, Gopal Prasad, Akash Sengupta, Rahul Singh, Yuval Wigderson, John Wiltshire-Gordon and Jakub Witaszek for helpful discussions.

REFERENCES

[Ami66] S. A. Amitsur. Rational identities and applications to algebra and geometry. *J. Algebra*, 3:304–359, 1966.

[AW09] Scott Aaronson and Avi Wigderson. Algebrization: A new barrier in complexity theory. *TOCT*, 1(1):2:1–2:54, 2009.

[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 *STOC'18—Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 172–181. ACM, New York, 2018.

[BFG+18] Peter Bürgisser, Cole Franks, Ankit Garg, Rafael Oliveira, Michael Walter, and Avi Wigderson. Efficient algorithms for tensor scaling, quantum marginals, and moment polytopes. In *59th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2018*, pages 883–897. IEEE Computer Soc., Los Alamitos, CA, 2018.

[BGO+18] Peter Bürgisser, Ankit Garg, Rafael Oliveira, Michael Walter, and Avi Wigderson. Alternating minimization, scaling algorithms, and the null-cone problem from invariant theory. In *9th Innovations in Theoretical Computer Science*, volume 94 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 24, 20. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2018.

[12]Clearly, for such groups the definition of a null cone must be taken to be the analytic one.

[BGS75] Theodore P. Baker, John Gill, and Robert Solovay. Relativizations of the P =? NP question. *SIAM J. Comput.*, 4(4):431–442, 1975.

[BIJL18] Markus Bläser, Christian Ikenmeyer, Gorav Jindal, and Vladimir Lysikov. Generalized matrix completion and algebraic natural proofs. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 1193–1206. ACM, 2018.

[Coh95] P. M. Cohn. *Skew fields*, volume 57 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995. Theory of general division rings.

[Die49] Jean Dieudonné. Sur une généralisation du groupe orthogonal à quatre variables. *Arch. Math.*, 1:282–287, 1949.

[DM17a] Harm Derksen and Visu Makam. Generating invariant rings of quivers in arbitrary characteristic. *J. Algebra*, 489:435–445, 2017.

[DM17b] Harm Derksen and Visu Makam. Polynomial degree bounds for matrix semi-invariants. *Adv. Math.*, 310:44–63, 2017.

[DM18a] Harm Derksen and Visu Makam. Algorithms for orbit closure separation for invariants and semi-invariants of matrices. *arXiv e-prints*, page arXiv:1801.02043, January 2018.

[DM18b] Harm Derksen and Visu Makam. Degree bounds for semi-invariant rings of quivers. *J. Pure Appl. Algebra*, 222(10):3282–3292, 2018.

[Edm67] Jack Edmonds. Systems of distinct representatives and linear algebra. *J. Res. Nat. Bur. Standards Sect. B*, 71(4):241–245, 1967.

[EGdOW18] Klim Efremenko, Ankit Garg, Rafael Mendes de Oliveira, and Avi Wigderson. Barriers for rank methods in arithmetic complexity. 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 1:1–1:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.

[EH88] David Eisenbud and Joe Harris. Vector spaces of matrices of low rank. *Adv. in Math.*, 70(2):135–155, 1988.

[FR07] Marc Fortin and Christophe Reutenauer. Commutative/noncommutative rank of linear matrices and subspaces of matrices of low rank. *Sém. Lothar. Combin.*, 52:Art. B52f, 12, 2004/07.

[Fra18] Cole Franks. Operator scaling with specified marginals. In *STOC'18—Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 190–203. ACM, New York, 2018.

[Fro97] G. Frobenius. Uber die darstellung der endlichen gruppen durch linear substitutionen. *Akad. Wiss. Berlin*, pages 994–1015, 1897.

[FS13] Michael A. Forbes and Amir Shpilka. Explicit Noether normalization for simultaneous conjugation via polynomial identity testing. In *Approximation, randomization, and combinatorial optimization*, volume 8096 of *Lecture Notes in Comput. Sci.*, pages 527–542. Springer, Heidelberg, 2013.

[FSV17] Michael A. Forbes, Amir Shpilka, and Ben Lee Volk. Succinct hitting sets and barriers to proving algebraic circuits lower bounds. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 653–664. ACM, 2017.

[GGOW16] Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. A deterministic polynomial time algorithm for non-commutative rational identity testing. In *57th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2016*, pages 109–117. IEEE Computer Soc., Los Alamitos, CA, 2016.

[GGOW18] Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. Algorithmic and optimization aspects of Brascamp-Lieb inequalities, via operator scaling. *Geom. Funct. Anal.*, 28(1):100–145, 2018.

[GKSS17] Joshua A. Grochow, Mrinal Kumar, Michael Saks, and Shubhangi Saraf. Towards an algebraic natural proofs barrier via polynomial identity testing. *arXiv e-prints*, page arXiv:1701.01717, January 2017.

[GM02] Boaz Gelbord and Roy Meshulam. Spaces of singular matrices and matroid parity. *European J. Combin.*, 23(4):389–397, 2002.

[GMdOW19] Ankit Garg, Visu Makam, Rafael Mendes de Oliveira, and Avi Wigderson. More barriers for rank methods, via a "numeric to symbolic" transfer. In David Zuckerman, editor, *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019, Baltimore, Maryland, USA, November 9-12, 2019*, pages 824–844. IEEE Computer Society, 2019.

[Gur94] Robert M. Guralnick. Invertible preservers and algebraic groups. In *Proceedings of the 3rd ILAS Conference (Pensacola, FL, 1993)*, volume 212/213, pages 249–257, 1994.

[Gur04] Leonid Gurvits. Classical complexity and quantum entanglement. *Journal of Computer and System Sciences*, 69(3):448–484, 2004.

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

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Comput. Complexity*, 13(1-2):1–46, 2004.

[Lan17] J. M. Landsberg. *Geometry and complexity theory*, volume 169 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017.

[Lov79] L. Lovász. On determinants, matchings, and random algorithms. In *Fundamentals of computation theory (Proc. Conf. Algebraic, Arith. and Categorical Methods in Comput. Theory, Berlin/Wendisch-Rietz, 1979)*, volume 2 of *Math. Res.*, pages 565–574. Akademie-Verlag, Berlin, 1979.

[LP01] Chi-Kwong Li and Stephen Pierce. Linear preserver problems. *Amer. Math. Monthly*, 108(7):591–605, 2001.

[Mes85] Roy Meshulam. On the maximal rank in a subspace of matrices. *Quart. J. Math. Oxford Ser. (2)*, 36(142):225–229, 1985.

[Mes90] Roy Meshulam. On k-spaces of real matrices. *Linear and Multilinear Algebra*, 26(1-2):39–41, 1990.

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)]*. Springer-Verlag, Berlin, third edition, 1994.

[MS01] Ketan D. Mulmuley and Milind Sohoni. Geometric complexity theory. I. An approach to the P vs. NP and related problems. *SIAM J. Comput.*, 31(2):496–526, 2001.

[MS08] Ketan D. Mulmuley and Milind Sohoni. Geometric complexity theory. II. Towards explicit obstructions for embeddings among class varieties. *SIAM J. Comput.*, 38(3):1175–1206, 2008.

[Mul17] Ketan D. Mulmuley. Geometric complexity theory V: Efficient algorithms for Noether normalization. *J. Amer. Math. Soc.*, 30(1):225–309, 2017.

[MW19] Visu Makam and Avi Wigderson. Symbolic determinant identity testing (SDIT) is not a null cone problem; and, the symmetries of algebraic varieties. *arXiv e-prints*, page arXiv:1909.00857, September 2019.

[Pot16] Aaron Potechin. A note on amortized space complexity. *CoRR*, abs/1611.06632, 2016.

[Raz89] Alexander A. Razborov. On the method of approximations. In David S. Johnson, editor, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washigton, USA*, pages 167–176. ACM, 1989.

[Reu96] C. Reutenauer. Inversion height in free fields. *Selecta Math. (N.S.)*, 2(1):93–109, 1996.

[RR94] Alexander A. Razborov and Steven Rudich. Natural proofs. In Frank Thomson Leighton and Michael T. Goodrich, editors, *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, 23-25 May 1994, Montréal, Québec, Canada*, pages 204–213. ACM, 1994.

[RW19] Orit E. Raz and Avi Wigderson. Subspace arrangements, graph rigidity and derandomization through submodular optimization. *arXiv e-prints*, page arXiv:1901.09423, January 2019.

[SY09] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: a survey of recent results and open questions. *Found. Trends Theor. Comput. Sci.*, 5(3-4):207–388 (2010), 2009.

[Val79] L. G. Valiant. The complexity of computing the permanent. *Theoret. Comput. Sci.*, 8(2):189–201, 1979.