Geometric Complexity Theory V: Equivalence between blackbox derandomization of polynomial identity testing and derandomization of Noether’s Normalization Lemma

Dedicated to Sri Ramakrishna

Ketan D. Mulmuley *
The University of Chicago
mulmuley@cs.uchicago.edu

May 5, 2014

Abstract

It is shown that the problem of derandomizing Noether’s Normalization Lemma (NNL) for any explicit variety can be brought down from EXPSPACE, where it is currently, to $P$ assuming a strengthened form of the black-box derandomization hypothesis (BDH) for polynomial identity testing (PIT), and to quasi-$P$ assuming that some exponential-time-computable multilinear polynomial cannot be approximated infinitesimally closely by arithmetic circuits of sub-exponential size. The converse also holds for a strict form of NNL. This equivalence between the strengthened BDH for PIT and the problem of derandomizing NNL in a strict form reveals that the fundamental problems of Geometry and Complexity Theory share a common root difficulty, namely, the problem of overcoming the EXPSPACE vs. $P$ gap in the complexity of NNL for explicit varieties. This gap is called the GCT chasm.

On the positive side, it is shown that NNL for the ring of invariants for any finite dimensional representation of the special linear group of fixed dimension can be brought down from EXPSPACE to quasi-$P$ unconditionally in characteristic zero.

On the positive side, it has also been shown recently by Forbes and Shpilka that a variant of a conditional derandomization result in this article in conjunction with the quasi-derandomization of ROABP that was known earlier implies unconditional quasi-derandomization of NNL for the ring of matrix invariants in characteristic zero.

1 Introduction

Noether’s Normalization Lemma (NNL), proved by Hilbert [Hil2], is the basis of a large number of foundational results in algebraic geometry such as Hilbert’s Nullstellensatz. It also lies at the heart of the foundational classification problem of algebraic geometry. For any projective variety $X \subseteq P(K^k)$ of dimension $n$, where $K$ is an algebraically closed field and $P(K^k)$ is the projective
space associated with $K^k$, the lemma says that any homogeneous and random (generic) linear map $\psi : K^k \to K^m$, for any $m \geq n+1$, is regular (well defined) on $X$. Furthermore, for any such $\psi$, $\psi(X) \subseteq P(K^m)$, the image of $X$, is closed in $P(K^m)$, and (2) the fibre $\psi^{-1}(p)$, for any point $p \in \psi(X)$, is a finite set. In the context of the main results of this paper, $k$ will be exponential in $n$ and $m$ will be polynomial in $n$. In this case Noether’s Normalization Lemma expresses the variety $X$, embedded in the ambient space $P(K^k)$ of exponential dimension, as a finite cover of the variety $\psi(X)$, embedded in the ambient space $P(K^m)$ of polynomial dimension. This is its main significance from the complexity-theoretic perspective. By derandomization of Noether’s Normalization Lemma we mean deterministic construction of the normalizing map $\psi$. We also refer to this problem as NNL in short. It turns out to be very difficult in general. First, the number of random bits used by the existing algorithms for general $X$ is polynomial in $k$, the dimension of the ambient space $K^k$ containing $X$. Since $k$ is exponential in $n$ in our context, the number of random bits used is thus exponential in $n$. Second, for a general $X$ as above, the current best algorithms for even deterministic verification of $\psi$, let alone construction, based on a recent fundamental advance [MR2] in Gröbner basis theory, take in the worst case space that is polynomial in $k$ and time that is exponential in $k$. The space bound for deterministic verification as well as construction (and even randomized Las Vegas construction) is thus exponential in $n$ and the time bound is double exponential in $n$. (Before [MR2] the time bound was double exponential in $n$ and hence, triple exponential in $n$.) Nothing better can be expected for general varieties because [MR1] also proves a matching lower bound for the computation of a Gröbner basis in this general setting.

In contrast, it is shown here (Theorem 1.1) that NNL for any explicit variety of dimension $n$ specified succinctly using poly($n$) bits (as in Definition 5.4) can be brought down from EXPSPACE, where it is currently for the reasons above, to $P$ assuming a strengthenend form of the black-box derandomization hypothesis (BDH) [HS, IW, KI, Ag] for polynomial identity testing (PIT), and to quasi-$P$ assuming that some exponential-time-computable multilinear polynomial cannot be approximated infinitesimally closely by arithmetic circuits over $K$ of sub-exponential size (the characteristic is assumed to be zero or large enough). The converse also holds for a strict form of NNL. Thus strengthened BDH for PIT, strict derandomization of NNL for explicit varieties, and (ignoring a quasi prefix) sub-exponential lower bounds for infinitesimally close approximation of exponential-time-computable multilinear polynomials are equivalent. This equivalence reveals that the fundamental problems of Geometry (NNL) and Complexity Theory (lower bounds and derandomization) share a common root difficulty, namely, the problem of overcoming the EXPSPACE vs. $P$ gap in the complexity of NNL for explicit varieties. This gap is called the GCT chasm.

This equivalence and the related results (cf. Theorem 1.3 (b)) may explain in a unified way why the fundamental lower bound and derandomization conjectures of complexity theory and the classification problems of invariant theory and algebraic geometry have turned out to be so hard.

On the positive side, it is shown here (Theorem 1.3 (a)) that Noether’s Normalization Lemma for the ring of invariants for any finite dimensional rational representation of the special linear group of fixed dimension can be quasi-derandomized unconditionally, thereby bringing this problem from EXPSPACE (where it was earlier for the same reasons) to quasi-DET $\subseteq$ quasi-NC in characteristic zero.
This invariant ring was the focus of Hilbert’s paper [Hl2] mentioned above. Noether’s Normalization Lemma was, in fact, proved therein to show constructively that this ring is finitely generated. This constructive proof, the celebrated result of Hilbert, and its various mathematical ingredients such as the Normalization Lemma and the Nullstellensatz changed the course of algebraic geometry and invariant theory in the twentieth century. But Hilbert could only show that his deterministic algorithm for constructing finitely many generators for this invariant ring worked in finite time. He could not prove any explicit upper bound on its running time. Such a bound was proved in Popov [P] a century later, and improved significantly in Derksen [D]. This improved analysis, in conjunction with Gröbner basis theory [MR2], yields an EXPSPACE-algorithm for derandomization of Noether’s normalization lemma for the ring of invariants of any finite dimensional rational representation of the special linear group $SL_m$. This algorithm needs exponential space and double exponential time even when $m$ is constant. Hilbert’s paper focussed mainly on the case when $m$ is four.

The unconditional quasi-derandomization result mentioned above shows that this double exponential time bound can be brought down to quasi-polynomial for any constant $m$. Thus this result does quasi-derandomize unconditionally the original instance of NNL in Hilbert’s paper.

On the positive side, it has also been shown recently by Forbes and Shpilka [FS3] that a variant of a conditional derandomization result (Theorem 1.4 (a)) in this article in conjunction with the quasi-derandomization of ROABP that was proved earlier in [FS2] implies unconditional quasi-derandomization of NNL for the ring of matrix invariants in characteristic zero (cf. Theorem 1.4 (b) and the remark thereafter).

The prefix GCT of the GCT chasm refers to its location at the junction of geometry and complexity theory. It does not mean that either of these two fields is necessary to cross it. Though, given the enormity of the chasm, both fields may turn out to be indispensable in practice. By Geometric complexity theory (GCT) we henceforth mean broadly any approach to cross this chasm based on a synthesis of geometry and complexity theory in some form. One such plausible approach is suggested in the sequel [Mu5].

Preliminary versions of the results in this article were announced in [Mu4]. See [Mu2] for an informal overview of the earlier articles in this series, and [Mu3] for a formal overview.

We now state the main results in more detail.

### 1.1 Black-box derandomization

First we state the black-box derandomization hypothesis that is used in this paper.

Let $K$ be an algebraically closed field of arbitrary characteristic. By black-box derandomization of PIT over $K$, we mean the problem of constructing an explicit hitting set $[IW][HS][KL][Ag]$ against all circuits over $K$ and on $r$ variables with size $\leq s$. By the size of a circuit we mean the total number of edges in it. There is no restriction on the bit-lengths of the constants in the circuit. If $K$ is of characteristic zero, then by an explicit hitting set, we mean a poly($s$)-time-constructible set $S_{r,s} \subseteq \mathbb{N}^r$ of test inputs such that, for every circuit $C$ on $K$ and $r$-variables $x = (x_1, \ldots, x_r)$ with size $\leq s$ and $C(x)$ not identically zero, $S_{r,s}$ contains a test input $b$ such that $C(b) \neq 0$. Here $C(x)$ denotes the polynomial computed by $C$. If $K$ is of positive characteristic $p$, then the hitting set is assumed to be a subset of $F_p^r$ for a large enough $l$, where $F_p^l$ denotes
the finite field with \( p^l \) elements. The fundamental black-box derandomization hypothesis (BDH) in complexity theory \([\text{HS}] [\text{IW}] [\text{KI}] [\text{Ag}]\) is that such explicit hitting sets exist. Black-box derandomization of PIT is important, because by the fundamental hardness vs. randomness principle \([\text{IW}] [\text{HS}] [\text{KI}] [\text{Ag}]\) it is essentially equivalent to proving circuit lower bounds for EXP, which are much easier variants of the nonuniform \( P \) vs. \( NP \) problem.

We also consider in this paper a restricted form of PIT called symbolic trace identity testing (STIT). It is equivalent \([\text{MP}] [\text{Sp}]\), up to polynomial factors, to the PIT for arithmetic branching programs or weakly skew straight-line programs, and also to the symbolic determinant identity testing (SDIT); cf. Section 2.1.

By a symbolic trace over \( K \), we mean a polynomial of the form \( \text{trace}(A(x)^l) \), where \( A(x) \) is an \( m \times m \) symbolic matrix whose each entry is a linear function over \( K \) in the variables \( x = (x_1, \ldots, x_r) \). By black-box derandomization of STIT over \( K \), we mean the problem of constructing an explicit hitting set \( S_{r,m} \) of test inputs in \( N^r \) (or \( F_{p^l}^r \) for a large enough \( l \) if the characteristic \( p \) of \( K \) is positive) such that, for any symbolic trace polynomial \( \text{trace}(A(x)^l) \), \( l \leq m \), that is not identically zero, there exists a test input \( b \in S_{r,m} \) such that \( \text{trace}(A(b)^l) \neq 0 \). By explicit we mean computable in poly(\( m, r \)) time.

1.2 Equivalence between BDH and NNL

Now we state the main equivalence result (Theorem 1.2) in this article.

The following is the first implication in this equivalence.

**Theorem 1.1** Let the base field \( K \) be an algebraically closed field of characteristic zero.

For any explicit variety of dimension \( n \) specified succinctly using poly(\( n \)) bits (as in Definition 5.4), the problem of derandomizing Noether’s Normalization Lemma over \( K \) is (1) in EXPSPACE unconditionally, (2) in REXP\( ^{\text{NP}} \), assuming GRH (Generalized Riemann Hypothesis), if explicit defining or close-to-defining equations (cf. Definition 5.13) for the variety are known, (3) in \( P \) assuming a strengthened form of black-box derandomization of PIT (defined in Section 5.1) and using a succinct specification of the normalizing map using poly(\( n \)) bits as in Definition 5.5, and (4) in quasi-\( P \) assuming that some exponential-time-computable multilinear integral polynomial in \( n \) variables cannot be approximated infinitesimally closely by arithmetic circuits over \( K \) of \( O(2^{n^\epsilon}) \) size for some \( \epsilon > 0 \).

The following result says that the strengthened form of black-box derandomization of PIT assumed in (3) is equivalent to derandomization of Noether’s Normalization Lemma in a strict form for a specific explicit variety.

**Theorem 1.2 (Equivalence)**

(1) A strengthened form (defined in Section 5.1) of black-box derandomization of symbolic determinant or trace identity testing (SDIT or STIT) is equivalent to derandomization of Noether’s Normalization Lemma (in a certain strict form) for the explicit orbit-closure associated with the determinant in \([\text{MS}]\) in the context of the permanent vs. determinant problem. A subexponential lower bound as in Theorem 1.1 (4) is also equivalent, ignoring a quasi-prefix, to strict derandomization of Noether’s Normalization Lemma for this explicit variety.
(2) A strengthened form of black-box derandomization of general PIT over \( K \) is equivalent to derandomization of Noether’s Normalization Lemma (in a strict form) for the explicit variety similarly associated with the complexity class \( P \) in [MS1] in the context of the algebraic \( P \) vs. \( NP \) problem.

(3) A strengthened form of black-box derandomization of PIT for depth three circuits over \( K \) is equivalent to derandomization of Noether’s Normalization Lemma (in a strict form) for the (polynomially high order) secant variety of the Chow variety.

(4) Analogues of the results in (1)-(3) also hold in positive characteristic.

See Section 5.4 for the full statements of Theorems 1.1 and 1.2. Their proof combines the basic ideas in the first article [MS1] of this series with Hilbert [Hi2], Gröbner basis theory [MR2, MR3], efficient factorization of multivariate polynomials [Kl1, Kl2, Kl3], the hardness vs. randomness principle [NW, KI], and the PH-algorithm for Hilbert’s Nullstellensatz [Ko1].

Finding explicit defining or close-to-defining equations as required in Theorem 1.1 (2) is a huge challenge for most explicit varieties. For the explicit varieties in Theorem 1.2 this problem is intimately related to the century-old plethysm and Kronecker problems of invariant theory; cf. [MS2, L1]. For the first order secant variety of the Chow variety, explicit set theoretic equations were given by Brill and Gordon [Go] in 1894. Similar equations for even the second order secant variety of the Chow variety are not known at present; cf. Section 8.6 in [L1] for a survey of the current state.

If explicit defining equations can be found for the varieties in Theorem 1.2 it will follow from Theorem 1.1 (2) that (assuming GRH) NNL for these varieties is in the exponential hierarchy. As such, bringing NNL for these varieties from \( EXPSPACE \) (where it is currently) to even the exponential hierarchy unconditionally seems extremely difficult. Theorem 1.1 says that it can be brought down from \( EXPSPACE \) all the way to \( P \) assuming the strengthened black-box derandomization hypothesis, or equivalently (ignoring a quasi-prefix) a subexponential arithmetic circuit lower bound for infinitesimally close approximation for some exponential-time-computable multilinear polynomial. This may explain why derandomization of NNL for arbitrary explicit varieties, and hence by the equivalence above, blackbox derandomization of PIT, has turned out to be so hard.

1.3 The general ring of invariants

Next, we turn to some exceptional instances of explicit varieties for which NNL can be quasi-derandomized unconditionally.

Let \( K \) be an algebraically closed field of characteristic zero. The following result (Theorem 1.3) quasi-derandomizes NNL unconditionally for the invariant ring associated with any finite dimensional rational representation \( V \) of \( G = SL_m(K) \) when \( m \) is constant. The same result also holds for arbitrary \( m \) assuming the standard black-box derandomization hypothesis for PIT (as in Section 1.1 not strengthened as in Theorem 1.1) and also assuming that the variety associated with this ring is explicit (cf. Conjecture 4.10).

Since \( G \) is reductive [Fu], \( V \) can be decomposed as a direct sum of irreducible representations
of $G$:

$$V = \sum_{\lambda} m(\lambda)V_\lambda(G).$$  \hspace{1cm} (1)

Here $\lambda: \lambda_1 \geq \ldots \geq \lambda_l, l < m$, is a partition, i.e., a sequence of non-negative integers, and $V_\lambda(G)$ is the irreducible representation of $G$ (Weyl module $[F1]$) labelled by $\lambda$. Fix the standard monomial basis $DRS \ LR$ for each $V_\lambda(G)$ and thus a standard monomial basis for $V$. Let $v_1, \ldots, v_n$ be the coordinates of $V$ for this basis. This fixes the action of $G$ on $V$. Let $K[V] = K[v_1, \ldots, v_n]$ denote the coordinate ring of $V$. Let $K[V]^G$ be its subring of $G$-invariants. We call a polynomial $f(v) \in K[V]$ a $G$-invariant if $f(\sigma^{-1}v) = f(v)$ for all $\sigma \in G$. By Hilbert $[H12]$, $K[V]^G$ is finitely generated. Hence one can associate with it a variety $V/G = \text{spec}(K[V]^G)$, called the categorical quotient $[MFK]$. We specify $V/G$ and $K[V]^G$ succinctly by giving $n := \dim(V)$ and $m$ (in unary) and the multiplicities $m(\lambda)$'s (in unary) for all $\lambda$'s that occur with nonzero multiplicity in the decomposition (1). The bit-length of this succinct specification is $O(n + m)$, though the dimension of the ambient space containing $V/G$ is exponential; cf. the remark after Proposition $4.2$.

By Noether's Normalization Lemma (Lemma $2.11$), there exists a set $S \subseteq K[V]^G$ of poly($n$) homogeneous invariants such that $K[V]^G$ is integral over the subring generated by $S$. (This statement of Noether's Normalization Lemma for $V/G$ is equivalent to the one given in the beginning of this introduction. Here a ring $R$ is said to be integral over its subring $T$ if every $r \in R$ satisfies a monic polynomial equation of the form $r^l + b_{l-1}r^{l-1} + \ldots + b_1r + b_0 = 0$, where each $b_i \in T$.) In fact, there even exists such an $S$ of optimal cardinality equal to $\text{dim}(K[V]^G)$. It is known that any suitably randomly chosen $S$ of this cardinality has the required property. Such an $S$ of optimal cardinality is called an h.s.o.p. (homogeneous system of parameters) of $K[V]^G$. We do not require optimality of $|S|$ in what follows. By the problem of derandomizing Noether’s Normalization Lemma for $V/G$ (or $K[V]^G$), or in short NNL, we mean the problem of constructing a homogeneous $S$ of poly($n$) cardinality such that $K[V]^G$ is integral over the subring generated by $S$. We say that NNL for $K[V]^G$ is derandomized if a specification of such an $S$ (as a set of straightline programs over $v_1, \ldots, v_n$) can be constructed in poly($n, m$) time; cf. Definition $4.4$ for details. Quasi-derandomization is defined by replacing polynomials with quasi-polynomials.

**Theorem 1.3** Suppose $K$ is an algebraically closed field of characteristic zero. Let $V$ as in (1) be a rational representation of $G = SL_m(K)$ of dimension $n$.

(a) If $m$ is constant, or more generally, $O(\text{polylog}(n))$ then NNL for $V/G$ can be quasi-derandomized unconditionally.

(b) The same result holds for general $m$, assuming that the black-box derandomization hypothesis (BDH) for PIT holds and also that $V/G$ is explicit (Conjecture $4.10$).

See Section $4$ for a detailed statement of this result. In view of $[GKKS]$, we can also use in (b) the BDH for depth three circuits instead of the BDH for general circuits (allowing a quasi-prefix). Variant of (b) also holds in positive characteristic (Theorem $4.20$). These results also hold for any finite dimensional representation of a classical algebraic group; cf. Theorem $4.22$.

Furthermore, variants of (b) (akin to Theorem 1.2 in $[Mu4]$) also hold assuming, instead of BDH, arithmetic lower bounds, or Boolean lower bounds together with GRH, and a weaker
variant of (b) holds assuming, instead of BDH, GRH. These variants are not discussed in this article since they are straightforward consequences of (b) in conjunction with the standard hardness vs. randomness tradeoffs.

Finite generation of the general invariant ring $K[V]^G$ in Theorem 1.3 is the celebrated result of Hilbert [H12]. This ring is crucial for the study of the moduli (classification) problems [MFK] in invariant theory and algebraic geometry. Before this result it was not even known if a finite $S$, let alone a small $S$, such that $K[V]^G$ is integral over the subring generated by $S$, exists. Hilbert’s first proof of finite generation was nonconstructive. This was severely criticized by Gordan as “theology and not mathematics”. Noether’s Normalization Lemma as well as the Nullstellensatz were proved by Hilbert in the course of his second constructive proof of this result in response to this criticism. But, as already mentioned in Section 1, Hilbert could not prove any explicit upper bound on the running time of his algorithm for constructing finitely many generators for $K[V]^G$. Such a bound was eventually proved in Popov [P], and improved in Derksen [D].

This improved analysis, in conjunction with Gröbner basis theory [MR2], yields an EXPSPACE-algorithm to compute a small $S$ such that $K[V]^G$ is integral over the subring generated by $S$; cf. Proposition 1.2. This algorithm needs exponential space and double exponential time even when $m$ is constant, because the dimension of the ambient space containing $V/G$ is exponential in $n$ even when $m$ is constant; cf. Section 2.4 and the remark after Proposition 4.2.

Theorem 1.3 (a) shows that this double exponential time bound can be brought down to quasi-polynomial, thereby bringing NNL from EXPSPACE to quasi-P (in fact, quasi-DET) unconditionally if $m$ is constant or $O(\text{polylog}(n))$. Classical invariant theory mainly focused on the case when $m$ is constant. For example, Hilbert’s paper [H12] mainly focused on the case when $m = 4$. The problem of constructing a finite set of generators for $K[V]^G$ was not known to be decidable before this paper even in this case. Thus Theorem 1.3 (a) does put NNL in quasi-DET unconditionally in the case that Hilbert’s paper focused on.

A crucial ingredient in the proof of (a) is the result here (Theorem 1.8) that $V/G$ is explicit when $m$ is constant. Theorem 1.3 (b) says that NNL can be brought down from EXPSPACE, where it is currently, to $P$ for any $m$ assuming that the black-box derandomization of PIT holds and that $V/G = \text{spec}(K[V]^G)$ is explicit in a relaxed sense for any $m$ as we conjecture (Conjecture 4.10).

Theorem 1.3 is proved using the fundamental works in geometric invariant theory due to Hilbert [H12], Mumford [MFK], and Derksen and Kemper [D], standard monomial theory [LR], and the fundamental works and techniques in algebraic complexity theory due to Strassen [Str1], Valiant et. al [V2, MP], and others.

1.4 The ring of matrix invariants

Next we turn to a special case of the ring of invariants for general $m$ for which NNL can be quasi-derandomized unconditionally. This is the ring of matrix invariants.

Let $M_m(K)$ be the space of $m \times m$ matrices over $K$, and $V = M_m(K)^r$, the direct sum of $r$ copies of $M_m(K)$, with the adjoint (simultaneous conjugate) action of $G = SL_m(K)$. Let $K[V]^G$ be the ring of matrix invariants, $V/G = \text{spec}(K[V]^G)$. We specify $V/G$ and $K[V]^G$ succinctly by giving $m$ and $r$ in unary.
Theorem 1.4 Let $K$ be an algebraically closed field of characteristic zero. Let $V = M_m(K)^r$ and $G = SL_m(K)$ be as above.

(a) Suppose the black-box derandomization hypothesis for STIT (or equivalently SDIT) holds over $K$. Then NNL for $V/G$ can be derandomized. (One can also assume here instead the BDH for ROABP [FS2]; see the remark below.)

(b) [cf. Forbes and Shpilka [FS3] and the remark below] The NNL for $V/G$ can be quasi-derandomized unconditionally.

This result (as well as Theorem 1.3) also holds for a stronger form of NNL (cf. Definitions 3.3 and 4.4 and Theorems 3.4, 4.5, and 4.17). It can be generalized to the invariant ring associated with any quiver (Theorem 3.11). The statement (b) also implies quasi-explicit parametrization of semi-simple representations of any finitely generated algebra in characteristic zero (cf. Theorem 3.9).

The statement (a), assuming BDH for SDIT, was proved in the preliminary version [Mu4] of this article. Subsequently Forbes and Shpilka [FS3] showed that the step in the proof of this result wherein the black-box derandomization hypothesis (BDH) for SDIT enters can be modified (as explained in Section 3.4) so as to use instead the BDH for ROABP (read-only-oblivious algebraic branching programs) for which a quasi-polynomial-time computable hitting set was already known from their earlier work [FS2]. This implied quasi-derandomization of this instance of NNL unconditionally, and showed that this problem was not beyond the reach of the existing techniques as was suggested in [Mu4].

The heart of Theorem 1.4 is the first fundamental theorem (FFT) for matrix invariants in characteristic zero due to Procesi and Razmyslov [Pr, Rz], which is used to show that this instance of $V/G$ is explicit (Lemma 3.5). In retrospect, the NNL for the ring of matrix invariants could be quasi-derandomized unconditionally because this FFT for matrix invariants was already known. There are some other exceptional classes of invariant rings for which explicit FFT’s akin to the one for matrix invariants are known. The original prototype of such an exceptional ring is the ring of vector invariants for which the first explicit FFT of this kind was proved by Weyl in his classic book [Wy] (NNL can be derandomized for this ring too). Unfortunately, explicit FFT’s can be proved for invariant rings only in exceptional cases. The instance of NNL in Theorem 1.4 is one such exceptional instance. The problem of proving an explicit FFT for a general invariant ring, posed by Weyl [Wy] (without defining what explicit means formally), remains one of the outstanding unsolved problems of invariant theory from the last century. This is why the problem of derandomizing NNL for general invariant rings as in Theorem 1.3 (b) turns out to be much harder.

The categorical quotient $V/G$ associated with the ring of matrix invariants in characteristic zero is also one of the exceptional explicit varieties for which explicit defining equations are known, as given by the Second Fundamental Theorem (SFT) for matrix invariants [Pr, Rz] based on the FFT. In contrast, as already mentioned, construction of explicit defining equations for general explicit varieties is extremely hard, and this is why the problem of derandomizing NNL for general explicit varieties as in Theorem 1.2 turns out to be so hard.

---

1 because of a relationship (which turned out to be a red herring) of this instance of NNL with the well-known wild (“impossible”) problem [Dz] of classifying matrix tuples, though this instance of NNL itself is not wild.
1.5 The GCT chasm

The Equivalence Theorem 1.2 and Theorem 1.3 (b) may thus explain why black-box derandomization or super-polynomial lower bounds for unrestricted arithmetic circuits (of even depth three) have turned out to be so hard. In contrast, derandomization results for several versions of restricted PIT's (eg. ASS FS2 KS2 SV) and quadratic lower bounds (eg. MR LR SW) for arithmetic circuits are known.

Theorem 1.2 thus reveals a chasm, in the terminology of AV GKKS, at arithmetic depth three. The root cause of this chasm common to geometry and complexity theory lies at the junction of these two fields, namely, the problem of overcoming the existing EXPSPACE vs. P gap in the complexity of NNL for explicit varieties. We call this gap the GCT chasm. It may be viewed as the cause and measure of the chasm at depth three observed in AV GKKS.

We conjecture that Noether’s Normalization Lemma can be derandomized for any explicit variety, as suggested by Theorems 1.1 and 1.2 cf. Conjecture 5.16 and the GCT chasm can be crossed. One such approach to cross the chasm is suggested in the sequel [Mu5].

1.6 Organization

The rest of this paper is organized as follows. In Section 2 we recall the results and notions in complexity theory and geometric invariant theory that are needed in this paper. Theorems 1.3 and 1.4 for the concrete instances of explicit varieties in invariant theory are then proved first in Sections 3 and 4 respectively, and Theorems 1.1 and 1.2 requiring the abstract notion of a general explicit variety are proved later in Section 5. This order of presentation from concrete to abstract will hopefully motivate and make the rather abstract treatment of general explicit varieties in Section 5 easier to read.

2 Preliminaries

In this section we recall the results and notions in complexity theory and geometric invariant theory that we need in this paper. We assume familiarity with basic complexity theory [AB], algebraic geometry [Mm], and representation theory [Fu].

2.1 Black-box derandomization hypothesis

We begin by stating in more detail the black-box derandomization hypothesis for polynomial identity testing HS IW KI Ag that we need.

Let $K$ be an algebraically closed field of arbitrary characteristic. The polynomial identity testing (PIT) problem over $K$ is the problem of deciding if a given arithmetic circuit $C(x)$, $x = (x_1, \ldots, x_r)$, over $K$ of size at most $s$ computes an identically zero polynomial. By the size of the circuit we mean the total number of edges in it. There is no restriction on the bit-lengths of the constants in the circuit. By the PIT problem of small degree, we mean the PIT problem wherein the degree of the polynomial computed by the circuit is polynomial in the number of variables. The article IM gives a randomized algorithm to solve the PIT problem in poly$(s)$.
operations over $K$. This is a black-box algorithm in the sense that it does not look inside the circuit. It merely evaluates the circuit at randomly chosen test inputs.

The black-box derandomization problem for PIT \( \text{HS, IW, KI, Ag} \) is to design an efficient deterministic black-box algorithm for solving the PIT problem. Specifically, the problem is to construct efficiently a hitting set against all circuits over $K$ with size $\leq s$ and on $r \leq s$ variables. If $K$ is of characteristic zero, then by a hitting set, we mean a set $S_{r,s} \subseteq \mathbb{N}^r$ (or $\mathbb{Z}^r$) of test inputs such that (1) the bit-length of the specification of each test input is poly($s$), and (2) for every circuit $C$ on $K$ and $r$ variables with size $\leq s$ computing a non-zero polynomial $C(x)$, $S_{r,s}$ contains a test input $b$ such that $C(b) \neq 0$. If $K$ is of positive characteristic $p$, then the hitting set is assumed to be a subset of $F_p^r$ for a large enough $l$. The black-box-derandomization hypothesis \( \text{HS, IW, KI, AG} \) in this context is that there exists a hitting set of poly($s$) total bit-size that is computable in poly($s$) time. More generally, if a hitting set has $O(T(s))$ size and is computable in $O(T(s))$ time, we say that PIT for circuits has $T(s)$-time-computable black-box derandomization. By our definition of a hitting set, it is still required here that the bit-length of each test input in the hitting set be poly($s$).

We have also defined a restricted form of PIT called symbolic trace identity testing (STIT) in Section \[\text{III}\]. It is equivalent \( \text{MP, Sp} \) up to polynomial factors, to symbolic determinant identity testing (SDIT) defined as follows. Let $Y$ be a variable $m \times m$ matrix. Let $Y'$ be any $m \times m$ matrix, whose each entry is a homogeneous linear form over $K$ in the variable entries $y_{ij}$'s of $Y$. We call det($Y'$) a symbolic determinant of size $m$. By SDIT, we mean the problem of deciding, given $Y'$, if the symbolic determinant det($Y'$) is an identically zero polynomial in $y_{ij}$'s. The black-box derandomization hypothesis for SDIT is that, given $m$, one can construct in poly($m$) time a hitting set against all non-zero symbolic determinants over $K$ of size $m$. This is equivalent to the black-box derandomization hypothesis for STIT in Section \[\text{III}\]. The parallel black-box derandomization hypothesis for SDIT is that a hitting set is computable by a uniform $\text{AC}^0$ circuit of poly($m$) bit-size with oracle access to $\text{DET}$ (the determinant function). The equivalent parallel black-box-derandomization hypothesis for STIT is that a hitting set against non-zero symbolic traces (of degree $\leq m$) over $K$ for $m \times m$ matrices and $r$ variables is computable by a uniform $\text{AC}^0$ circuit of poly($m, r$) bit-size with oracle access to $\text{DET}$.

The following result says that a hitting set for PIT exists.

**Theorem 2.1 (Heintz, Schnorr)** (cf. Theorem 4.4 in \[\text{HS}\]) Let $K$ be any field of characteristic zero. There exists a hitting set $B \subseteq \lbrack u \rbrack^r$, $u = 2s(d + 1)^2$, of size $6(s + 1 + r)^2$ against all non-zero arithmetic circuits over $K$ and $r$ variables of size $\leq s$ and degree $\leq d$. If $K$ has positive characteristic $p$, then the hitting set is a subset of $F_p^r$ for a large enough $l$.

The proof of this result in \[\text{HS}\] does not yield any efficient algorithm for constructing $B$.

The following result is a variant of Theorem 7.7 in \[\text{KI}\]. This is why PIT is expected to have efficient black-box derandomization.

**Theorem 2.2 (Kabanets and Impagliazzo)** (cf. Theorem 7.7 in \[\text{KI}\]) Let $K$ be an algebraically closed field of characteristic zero.

(a) Suppose there is an exponential-time computable multilinear polynomial $f(x_1, \ldots, x_m)$ with integral coefficients of poly($m$) bit-length such that $f$ cannot be evaluated by an arithmetic circuit
over $K$ of $O(2^{ma})$ size for some constant $a > 0$. Then PIT for small degree circuits of size $\leq s$ has $O(2^{poly\log(s)})$-time computable black-box derandomization.

(b) Suppose there is an exponential-time computable multilinear polynomial $f(x_1, \ldots, x_m)$ with integral coefficients of $poly(m)$ bit-length such that $f$ cannot be evaluated by an arithmetic circuit over $K$ of $O(m^a)$ size for any constant $a > 0$, $m \to \infty$. Then PIT for small degree circuits of size $\leq s$ has $O(2^{s^{\epsilon}})$-time computable black-box derandomization, for any $\epsilon > 0$.

(c) If $K$ is an algebraically closed field of positive characteristic $p$, then an analogue of (a) holds assuming a stronger lower bound, namely, that $f^{p^l}$, $0 \leq l \leq \frac{m^\delta}{\log_2 p}$, for some $\delta > 0$, cannot be evaluated by an arithmetic circuit over $K$ of $O(2^{ma})$ size for some constant $a > 0$, $m \to \infty$. In particular, if $p > 2^m$, for some $\delta > 0$, then the analogue of (a) holds assuming that $f$ cannot be evaluated by an arithmetic circuit over $K$ of $O(2^{ma})$ size for some constant $a > 0$, $m \to \infty$. The coefficients of $f$ are assumed to be in some extension of $F_p$. Similar analogue of (b) also holds (with $l = O(\log m/\log p)$).

The proof of this result is very similar to that of Theorem 7.7 in [KI] (which works in the black-box model). Since we are going to prove its stronger form (Theorem 5.1) later, we only point out here how to take care of the main difference between the setting in [KI] and the one here. The difference is that in [KI] the size of the circuit is defined to be the total number of edges in it plus the total bit-length of the constants in it, whereas here the size just means the total number of edges. A key ingredient in the proof in [KI] is an efficient algorithm in [Kl1] for factoring multivariate polynomials (cf. Lemma 7.6. in [KI]). In its place we use instead the following result in [Kl1, KT] that does not depend on the bit-lengths of the constants in the circuit.

**Theorem 2.3 (Kaltofen)** (cf. Corollary 6.2. in [KI] and Theorem 1 in [KT] for characteristic zero and [Kl2] for positive characteristic)

Let $K$ be an algebraically closed field of characteristic zero. Suppose $g(x_1, \ldots, x_n)$ is $p$-computable [V2] over $K$. This means $g$ is a polynomial of $poly(n)$ degree that can be computed by a nonuniform circuit over $K$ of $poly(n)$ size. Then each factor of $g$ in $K[x_1, \ldots, x_n]$ is also $p$-computable over $K$.

More generally, given any polynomial $g \in K[x_1, \ldots, x_n]$ and a polynomial $f \in K[x_1, \ldots, x_n]$ dividing $g$, there exists a nonuniform circuit over $K$ of $poly(n, \deg(g))$ size, with oracle gates for $g$, that computes $f$.

If $K$ is an algebraically closed field of positive characteristic $p$, then given any polynomial $g \in K[x_1, \ldots, x_n]$ and a polynomial $f \in K[x_1, \ldots, x_n]$ dividing $g$, there exists a nonuniform circuit over $K$ of $poly(n, \deg(g))$ size, with oracle gates for $g$, that computes the highest power of $f$ of the form $f^{p^l}$ that divides $g$.

For the converse of Theorem 2.2, see [HS, Ag].

For the proof of Theorem 1.3 (a), we will need a restricted form of PIT for diagonal depth three circuits [Sx]. By a diagonal depth three circuit, we mean a circuit $C(x)$, $x = (x_1, \ldots, x_r)$,
that computes a sum of powers of linear functions:

\[ C(x) = \sum_{i=1}^{k} l_i^{e_i}, \]

where each \( l_i \) is a possibly non-homogeneous linear form in \( x_i \)'s with coefficients in \( K \). Here \( k \) is called the top fan-in of the circuit, and \( e = \max\{e_i\} \) its degree. The size of this circuit is \( s = O(\text{rek}) \).

The black-box derandomization hypothesis in this context is that a hitting set against diagonal depth three circuits on \( r \) variables with degree \( \leq e \) and top fan-in \( \leq k \) can be computed in \( \text{poly}(s) \) time. The parallel black-box derandomization hypothesis is that such a hitting set can be computed by a uniform \( \text{AC}^0 \) circuit of \( \text{poly}(s) \) bit-size. This holds unconditionally allowing a quasi-prefix:

**Theorem 2.4** (Shpilka, Volkovich; Agrawal, Saha, Saxena) *(cf. Theorem 6.4 in [SV] and the appendix in [ASS]*) A hitting set against all diagonal depth three circuits over \( K \) of size \( \leq s \) can be constructed by a uniform \( \text{AC}^0 \) circuit of \( O(s^{O(\log s)}) \) bit-size.

This result is a variant of Theorem 6.4 in [SV], with essentially the same proof [Sp]. Specifically, the partial derivative method in [SV] implies that if \( 2^l > ke \) then no diagonal depth three circuit over \( x_1, \ldots, x_r \) with degree \( \leq e \) and top fan-in \( \leq k \) can compute a polynomial of the form \( x_{i_1} \cdots x_{i_l} f(x_1, \ldots, x_r) \), for distinct \( i_j \)'s. This lower bound, in conjunction with the proof technique of Theorem 6.4 in [SV], implies that the set of \( r \)-vectors with entries in \( 0, \ldots, e \) that contain at most \( l \) nonzero entries is a hitting set against diagonal depth three circuits over \( x_1, \ldots, x_r \) with degree \( \leq e \) and top fan-in \( \leq k \).

For the proof of Theorem 1.4 we need the following result for a restricted form of PIT for read once oblivious algebraic branching programs (ROABP). See [FS2] for the definition of an ROABP.

**Theorem 2.5** (Forbes, Shpilka) *(FS2)* There exists a quasi-poly(s)-time computable hitting set for ROABP’s of size \( s \) over any field of characteristic zero or any field \( F \) of positive characteristic with \( |F| \) greater than a large enough polynomial in \( s \).

By the analogue of Theorem 1.2 for diagonal depth three circuits (which can be proved similarly), the strengthened black-box derandomization hypothesis for diagonal depth three circuits is equivalent to derandomization of Noether’s Normalization Lemma (in a strict form) for the secant variety [L2] of the Veronese variety. The proof of Theorem 2.4 in [SV] as well as [ASS] is based implicitly on the determinantal equations for this variety that have been studied intensively since the classical work of Sylvester; cf. [L2] for the survey and further references. In contrast, as already pointed out in Section 1.2, finding explicit equations for the (polynomially high order) secant variety of the Chow variety that arises (cf. Theorem 1.2 (3)) in the context of black-box derandomization of (unrestricted) depth-three circuits is extremely hard.
2.2 Geometric invariant theory

We now state some results from geometric invariant theory that are needed for proving Theorems 1.3 and 1.4.

Let $K$ be an algebraically closed field of characteristic zero, $M_m(K)$ the space of $m \times m$ matrices over $K$, and $V = M_m(K)^r$, the direct sum of $r$ copies of $M_m(K)$. Let $n = \dim(V) = rm^2$. The space $V$ has the adjoint action of $G = SL_m(K)$:

\[(A_1, \ldots, A_r) \rightarrow (PA_1P^{-1}, \ldots, PA_rP^{-1}),\]

where $A_1, \ldots, A_r \in M_m(K)$ and $P \in SL_m(K)$. Let $U_1, \ldots, U_r$ be variable $m \times m$ matrices. Then the coordinate ring $K[V]$ of $V$ can be identified with the ring $K[U_1, \ldots, U_r]$ generated by the variable entries of $U_i$'s. Let $K[V]^G \subseteq K[V]$ be the ring of invariants with respect to the adjoint action.

**Theorem 2.6 (Procesi-Razmyslov-Formanek)** [Fo] (The First Fundamental Theorem (FFT) of matrix invariants; cf. Theorems 6 and 10 in [Fo]) The ring $K[V]^G$ is generated by traces of the form $\text{trace}(U_{i_1} \cdots U_{i_l})$, $l \leq m^2$, $i_1, \ldots, i_l \in [r] = \{1, \ldots, r\}$.

Let $K[S_r]$ be the group algebra of the symmetric group $S_r$ on $r$ letters. Write any $\sigma \in S_r$ as a product of disjoint cycles:

\[\sigma = (a_1 \cdots a_{k_1})(b_1 \cdots b_{k_2})\ldots,\]

where 1-cycles are included, so that each of the numbers $1, \ldots, r$ occurs exactly once. Define

\[T_\sigma(U_1, \ldots, U_r) = T(U_{a_1} \cdots U_{a_{k_1}})T(U_{b_1} \cdots U_{b_{k_2}})\cdots.\]

**Theorem 2.7 (Procesi-Razmyslov)** [Pr, Rz] (The Second Fundamental Theorem (SFT) of matrix invariants; cf. Theorem 1 in [Fo]) Let $J(m, r)$ be the two-sided ideal of $K[S_r]$ which is the sum of all simple factors of $K[S_r]$ corresponding to the Young diagrams with $\geq m + 1$ rows. Define the $K$-linear map $\phi : K[S_r] \rightarrow K[V]^G$ by

\[\phi(\sum a_\sigma \sigma) = \sum a_\sigma T_\sigma(U_1, \ldots, U_r).\]

Then $\text{Ker}(\phi) = J(m, r)$. Furthermore, $J(m, r) = 0$ if $r \leq m$.

Let $X_1, \ldots, X_r$ be $k \times k$ variable matrices. For any word $\alpha = i_1, \ldots, i_l$, $i_j \in [r] = \{1, \ldots, r\}$, let

\[T_\alpha(X) = \text{trace}(X_{i_1} \cdots X_{i_l}),\]

where $X = (X_1, \ldots, X_r)$. We say that two words $\alpha$ and $\alpha'$ are equivalent, if $\alpha'$ can be obtained from $\alpha$ by circular rotation. In this case, $T_\alpha(X) = T_{\alpha'}(X)$. Let $[\alpha]$ denote the equivalence class of words equivalent to $\alpha$. Let $T_{[\alpha]}(X) = T_\alpha(X)$; the choice of $\alpha$ in $[\alpha]$ does not matter.

**Corollary 2.8** The traces $\{T_{[\alpha]}(X)\}$, where $[\alpha]$ ranges over all equivalence classes of words of length $l \leq k$, are linearly independent.
Proof: Suppose to the contrary that there is a linear dependence
\[ \sum_{[\alpha]} b_{[\alpha]} T_{[\alpha]}(X) = 0, \quad b_{[\alpha]} \in K. \] (5)

Without loss of generality, we can assume that this relation is homogeneous in \(X_i\)'s. We can also assume that it is multilinear in \(X_i\)'s. Otherwise, we can multilinearize it by substituting
\[ X_i = \sum_j t^j_i X^j_i, \]
in the l.h.s. of (5) and equating the coefficient of \(\prod_i \prod_{j=1}^{d_i} t^j_i\) to zero, where \(d_i\) is the degree of \(X_i\) in the relation, \(t^j_i\)'s are new variables, and \(X^j_i\)'s are new variable \(k \times k\) matrices.

If the dependence is multilinear and homogeneous, then each \([\alpha] = [i_1, \ldots, i_l]\) corresponds to the permutation in \(S_l\) with just one cycle \((i_1, \ldots, i_l)\). We denote it by \([\alpha]\) again. Applying Theorem 2.7 with \(U = X\), \(r = l\), and \(m = k\), it follows that \(b_{[\alpha]}\)'s are all zero, since \(J(k, l) = 0\) for \(l \leq k\). Q.E.D.

The following is an alternative form of Theorem 2.7.

The Cayley-Hamilton theorem implies [Pr] the fundamental trace identity
\[ F(U_1, \ldots, U_{m+1}) = \sum_{\sigma \in S_{m+1}} \text{sign}(\sigma) T_{\sigma}(U_1, \ldots, U_{m+1}) = 0, \]
where the trace function \(T_{\sigma}\) is defined as in (3).

**Theorem 2.9 (Procesi-Razmyslov) (cf. Theorem 4.5 in [Pr])** The ideal of all relations among the trace monomial generators of \(K[V]^G\) given by Theorem 2.6 is generated by the elements of the form \(F(M_1, \ldots, M_{m+1})\), where \(M_i\)'s range over all possible monomials in \(U_j\)'s so that the total length of \(M_i\)'s is \(\leq m^2\).

This follows from the proof of Theorem 4.5 in [Pr].

Now assume that \(G\) is any reductive algebraic group defined over an algebraically closed field \(K\) and \(V\) its any finite dimensional rational representation. Then the invariant ring \(K[V]^G\) is finitely generated \([\text{HI2}],[\text{MFK}]\). So we can consider the variety \(V/G = \text{spec}(K[V]^G)\), called the categorical quotient \([\text{MFK}]\). It has the following property (Theorem 2.10) that plays a crucial role in this paper.

Fix any set \(F = \{f_1, \ldots, f_t\}\) of non-constant homogeneous generators of \(K[V]^G\). Consider the morphism \(\pi_{V/G}\) from \(V\) to \(K^t\) given by
\[ \pi_{V/G} : \quad v \to (f_1(v), \ldots, f_t(v)). \] (6)

Then \(V/G\) can be identified with the closure of the image of this morphism. Let \(z = (z_1, \ldots, z_t)\) be the coordinates of \(K^t\), \(I\) the ideal of \(V/G\) under this embedding, \(K[V/G]/I\) its coordinate ring. Then \(K[V/G] = K[z]/I\), and we have the comorphism \(\pi^*_{V/G} : K[V/G] \to K[V]\) given by
\[ \pi^*_{V/G}(z_i) = f_i. \] (7)
Since $f_i$ are homogeneous, $K[V/G]$ is a graded ring, with the grading given by $\deg(z_i) = \deg(f_i)$. Furthermore, $\pi^*_{V/G}$ gives the isomorphism between $K[V/G]$ and $K[V]^G$, and we have $\pi^*_{V/G}(K[V/G]) = K[V]^G$.

**Theorem 2.10 (Mumford [MFK])** (cf. Theorem 1.1 in [MFK] and Theorem 4.6 and 4.7 in [PV])

(a) The image of $\pi_{V/G}$ is already closed. Hence the map $\pi_{V/G} : V \to V/G$ is surjective.

(b) For any $x \in V/G$, $\pi^{-1}_{V/G}(x)$ contains a unique closed $G$-orbit.

(c) For any $G$-invariant (closed) subvariety $W \subseteq V$, $\pi_{V/G}(W)$ is a closed subvariety of $V/G$.

(d) Given $v, w \in V$, the closures of the $G$-orbits of $v$ and $w$ intersect iff $r(v) = r(w)$ for all $r \in K[V]^G$.

The following is a graded variant of Noether’s normalization Lemma implicit in its proof; cf. Theorem 13.3. in [E], Corollary 2.29 in [Min], and also the proof of Theorem 1.5.17 in [BrH].

**Lemma 2.11 (Graded Noether Normalization)** Let $R$ be any positively graded affine $K$-algebra. Let $f_1, \ldots, f_t$ be any non-constant homogeneous generators of $R$, and $H \subseteq R$ any set of homogeneous elements such that, letting $I(H)$ denote the ideal generated by $H$, $f_i^{e_i} \in I(H)$ for some positive integer $e_i$ for every $i$. Then $R$ is integral over the subring generated by $H$.

If $d_i$’s are positive integers so that $g_i = f_1^{d_1}, \ldots, g_t = f_t^{d_t}$ have the same degree, then any $H, |H| \geq \dim(R)$, consisting of random (generic) linear combinations of $g_i$’s has the property in Lemma 2.11. A set $H$ of homogeneous invariants of cardinality equal to $\dim(R)$ such that $R$ is integral over the subring generated by $H$ is called an h.s.o.p. (homogeneous system of parameters) of $R$.

Following Derksen and Kemper [DK] (cf. Section 2.3.2 therein), let us call a set $S \subseteq K[V]^G$ separating if for any $v, w \in V$ such that $r(v) \neq r(w)$, for some $r \in K[V]^G$, there exists an $s \in S$ such that $s(v) \neq s(w)$.

**Theorem 2.12 (Derksen, Kemper)** (cf. Theorem 2.3.12 in [DK]) Let $S \subseteq K[V]^G$ be a finite separating set of homogeneous invariants. Then $K[V]^G$ is integral over the subring generated by $S$.

**2.3 Solving polynomial equations**

In this section we state the results for solving polynomial equations that are needed in this paper.

**Theorem 2.13 (Koiran: Hilbert’s Nullstellansatz is in PH assuming GRH) (cf. [Ko1])** Assuming GRH, the problem of deciding if a given system of multivariate integral polynomials, specified as straight-line programs, has a complex solution belongs to $RP^{NP} \subseteq \Pi_2$.

This result is stated in [Ko1] for a sparse representation of polynomials. But it can be seen to hold for a representation of polynomials by straight-line programs as well.
Lemma 2.14 (Noether Normalization is in PH for the long representation assuming GRH)

Let $K$ be an algebraically closed field. Let $Z \subseteq K^t$ be the variety consisting of the common zeroes of a set of homogeneous polynomials $f_1(z), f_2(z), \ldots, z = (z_1, \ldots, z_t)$. We assume that $f_i$’s are specified as straight-line programs and that their coefficients are in $\mathbb{Q}$ if the characteristic of $K$ is zero and in $F_{p^l}$ for a large enough $l$ if the characteristic of $K$ is positive $p$. Let $N$ denote the total bit-length of the specification of $f_i$’s. Let $\dim(Z)$ be the dimension of $Z$.

(a) Consider random linear forms $L_r(z) = \sum_{k} b_{k,r} z_k$, $0 \leq r \leq s$, where $b_{k,r}$’s are random elements in $K$ of large enough poly($N$) bit-length. Let $H_r \subseteq K^r$ be the hyperplane defined by $L_r(z) = 0$. If $s < \dim(Z)$, then $Z \cap \bigcap_r H_r \neq \{0\}$. If $s = \dim(Z)$, then with high probability, $Z \cap \bigcap_r H_r = \{0\}$, which implies (by Hilbert’s Nullstellensatz and Lemma 2.11) that the homogeneous coordinate ring of $Z$ is integral over the subring generated by $L_r(z)$’s.

(b) The problem of computing the linear forms $L_r(z)$’s such that $Z \cap \bigcap_r H_r = \{0\}$ belongs to PSPACE. This means the specifications of such linear forms can be computed in poly($N$) workspace.

(c) In characteristic zero, assuming GRH, this problem is in $RP^{NP} \subseteq \Pi_2$.

Proof:

(a) Let us assume that $s = \dim(Z)$, the other case being easy. Let $d = \max\{\deg(f_i)\}$. Clearly, $d \leq 2^N$. By raising $f_i$’s to appropriate powers, we can assume that all of them have the same degree $D \leq 2^{N^2}$. Consider generic combinations of $f_i$’s, and generic linear forms:

$$\begin{align*}
F_j(z) &= \sum_{i} y_{i,j} f_i(z), \quad 1 \leq j \leq t - \dim(Z), \\
L_r(z) &= \sum_k w_{k,r} z_k, \quad 1 \leq r \leq \dim(Z),
\end{align*}$$

where $y_{i,j}$’s and $w_{k,r}$’s are indeterminates. Let $R$ denote the multivariate resultant of $F_j$’s and $L_r$’s. It is a polynomial in $y_{i,j}$’s and $w_{k,r}$’s of degree $\leq D^t$. By Noether’s Normalization Lemma (cf. Corollary 2.29 in [Mm] and Lemma 2.11), the system of equations (8) has only $\{0\}$ as its solution for some rational values for $y_{i,j}$’s and $w_{k,r}$’s. Hence $R$ is not identically zero as a polynomial in $y_{i,j}$’s and $w_{k,r}$’s. By the Schwarz-Zippel lemma [Sc], we can specialize $y_{i,j}$’s randomly to some values in $K$ of $O(\log(D^t)) = poly(N)$ bit-length so that the resulting specialization $R'$ of $R$ is not identically zero. Then $R'$ is a nonzero polynomial in $w_{k,r}$’s of degree $\leq D^t$. By the Schwarz-Zippel lemma again, $R'$ does not vanish identically if we let $w_{k,r} = b_{k,r}$ for randomly chosen elements in $K$ of bit-length $O(\log(D^t)) = poly(N)$. For such $b_{k,r}$’s, $Z \cap \bigcap_r H_r = \{0\}$.

(b) and (c): First, let us assume that we know $\dim(Z)$. Let $s = \dim(Z)$. Choose $b_{k,r}$’s as above randomly of large enough poly($N$) bit-length and test if $Z \cap \bigcap_r H_r = \{0\}$. The latter test can be done in polynomial space since Hilbert’s Nullstellensatz is in PSPACE [Ko] [Ko1] [Ch] (unconditionally): choose random $y_{i,j}$’s and test if the resultant $R$ above, which can be computed in polynomial space [Ch], is zero. Randomization can be removed since $RPSPACE = NPSPACE = PSPACE$. In characteristic zero, assuming GRH, this test can be done by an $RP^{NP}$-algorithm, since Hilbert’s Nullstellensatz is then in $RP^{NP}$ (Theorem 2.13).

The problem that remains is that we do not really know $\dim(Z)$ a priori. So we start with a guess $s$ for $\dim(Z)$, starting with $s = 0$ and increasing it one by one. At each step we randomly choose large enough $b_{k,r}$’s and test if $Z \cap \bigcap_r H_r = \{0\}$. As long as $s < \dim(Z)$, the
test will fail. We stop as soon as it succeeds. Randomization can be removed if we only want a PSPACE-algorithm. Q.E.D.

2.4 Succinct vs. long representation

Lemma 2.14 shows that the problem of constructing an h.s.o.p. for the coordinate ring of a variety $Z$ is in PSPACE unconditionally and, for characteristic zero, in PH assuming GRH if $Z$ is specified by writing down a set of generators for its ideal—we call this a long representation of $Z$. Lemma 2.14 does not show that this problem is in PSPACE or PH (assuming GRH) for the succinct representation of explicit varieties used in this paper. For example, $V/G$ in Theorem 1.4 is specified by just giving $m$ and $r$ in unary, and $V/G$ in Theorem 1.3 is specified by just giving $n$ and $m$ (in unary) and the multiplicities (in unary) of the various Weyl modules $V\lambda(G)$'s in the decomposition of $V$. The bit-lengths of the long representations of these varieties are exponential in the bit-lengths of their succinct representations. This is because the dimension $t$ of the ambient space $K^t$ containing $V/G$ is exponential in the bit-length of the succinct representation; cf. Sections 3.1 and 4.1.

Hence, Lemma 2.14 can only be used (cf. Theorem 3.1) to show that the problem of constructing an h.s.o.p. for $K[V]^G$ in Theorem 1.4, with $V$ and $G$ specified succinctly, is in EXPSPACE unconditionally and in the exponential hierarchy (not polynomial) assuming GRH in characteristic zero. Similar result also holds for any variety for which explicit defining equations are known akin to the ones provided for $V/G$ in Theorem 1.4 by the second fundamental theorem for matrix invariants [Pr, Rz]; cf. Theorem 5.12 (d).

For the varieties for which such explicit defining equations are not known, e.g. $V/G$ in Theorem 1.3, Lemma 2.14 can only be used to show that the problem of constructing an h.s.o.p. is in EXPSPACE; cf. Proposition 4.2 and Theorem 5.12. This is because for such varieties the conversion of the succinct representation into a long representation itself takes exponential space (in the bit-length of the succinct representation) and double exponential time; cf. Lemma 4.3. In a nutshell, this is why the existing techniques for Noether normalization applied to $V/G$ in Theorem 1.3 take exponential space and double exponential time even when $m$ is constant (cf. Proposition 4.2); the story for general explicit varieties being similar (cf. Theorem 5.12).

3 The ring of matrix invariants

In this section we prove Theorem 1.4.

Let $K$ be an algebraically closed field of characteristic zero. Let $V = M_m(K)^r$, with the adjoint action of $G = SL_m(K)$, be as in Theorem 1.4. Let $n = \dim(V) = rm^2$. Let $U_1, \ldots, U_r$ be variable $m \times m$ matrices. Identify the coordinate ring $K[V]$ of $V$ with the ring $K[U_1, \ldots, U_r]$ generated by the variable entries of $U_i$’s. Let $K[V]^G \subseteq K[V]$ be the ring of invariants with respect to the adjoint action. Let $V/G = \text{spec}(K[V]^G)$. We specify $V/G$ and $K[V]^G$ succinctly by giving the pair $(m, r)$ in unary.

The goal is to derandomize NNL for $V/G$ by constructing in poly$(m, r)$ time a suitable specification of a small set $S \subseteq K[V]^G$ of poly$(m, r)$ homogeneous invariants such that $K[V]^G$ is integral over the subring generated by $S$. 

17
3.1 Construction of an h.s.o.p.

We begin with the problem of constructing an h.s.o.p. (homogeneous system of parameters) for \( K[V]^G \). By this we mean a set \( S \subseteq K[V]^G \) of homogeneous invariants of optimal cardinality (equal to \( \dim(K[V]^G) \)) such that \( K[V]^G \) is integral over the subring generated by \( S \). The following result gives the currently best upper bound for this problem.

**Theorem 3.1** The problem of constructing an h.s.o.p. for \( K[V]^G \) belongs to \( \text{EXPSPACE} \) unconditionally. (The space is exponential in the bit-length \( m + r \) of the succinct specification.) Assuming GRH, it belongs to \( \text{REXPNP} \) (allowing exponentially long oracle queries).

The first statement here can be shown in arbitrary characteristic.

**Proof:** First we construct a finite set \( F = \{f_1, \ldots, f_t\} \) of generators of \( K[V]^G \). We can use the set of generators in Theorem 2.6 whose specification can be computed in exponential time. Here \( t \) is exponential in \( m \).

With \( F \) as above, consider the map \( \pi_{V/G} : V \to K^t \):

\[
\pi_{V/G} : \quad A = (A_1, \ldots, A_r) \to (\ldots, f_j(A), \ldots).
\]

(9)

Then the categorical quotient \( V/G \) is the closure of the image of this map. By Theorem 2.10 this image is already closed. Hence \( V/G = \text{Im}(\pi_{V/G}) = \overline{\text{Im}(\pi_{V/G})} \).

This gives an embedding of \( V/G \) in \( K^t \) as in eq.(9), with the set \( F \) of generators as above. Theorem 2.9 gives us equations of \( V/G \) for this embedding whose specifications can be computed in exponential time.

Applying Lemma 2.14 to these equations of \( V/G \), we compute a set \( S \subseteq K[V]^G \) of homogeneous invariants of optimal cardinality (equal to \( \dim(V/G) \leq n \)) such that \( K[V]^G \) is integral over the subring generated by \( S \). Then \( S \) is an h.s.o.p. This is an EXPSPACE algorithm that works in \( 2^{\text{poly}(n)} \) work-space unconditionally.

It is an \( \text{REXPNP} \)-algorithm assuming GRH. The hierarchy here is again exponential and not polynomial because the dimension \( t \) of the ambient space \( K^t \) containing \( V/G \) is exponential in \( m \). Q.E.D.

The space requirement of this algorithm remains exponential even if we only want to construct an \( S \) of \( \text{poly}(n) \) size (not necessarily optimal) such that \( K[V]^G \) is integral over the subring generated by \( S \).

If we insist on an h.s.o.p. then Theorem 3.1 is the best that we can do at present. But if we only require a small \( S \) of \( \text{poly}(n) \) cardinality such that \( K[V]^G \) is integral over the subring generated by \( S \), and do not insist on optimality of \( |S| \), then Theorem 3.4 below says that the double exponential time bound in Theorem 3.1 can be brought down to quasi-polynomial assuming black-box derandomization of STIT.

3.2 Definition of derandomization of NNL

Before turning to this result, we need to define formally derandomization of NNL for \( K[V]^G \). This is done in the following two definitions.
Definition 3.2  (a) We call a set $S \subseteq K[V]^G$ an s.s.o.p. (small system of parameters) for $K[V]^G$ if (1) $S$ contains poly($n$) homogeneous invariants of poly($n$) degree, (2) $K[V]^G$ is integral over the subring generated by $S$, and (3) each invariant $s = s(U_1, \ldots, U_r)$ in $S$ has a weakly skew straight-line program [MP] over $\mathbb{Q}$ (or $F_p$ in positive characteristic) and the variable entries of $U_i$’s of poly($n$) bit-length.

(b) We say that $S$ is a separating s.s.o.p. if (2) is replaced by the stronger (2)’: $S$ is separating.

By Theorem 2.12 (2)’ implies (2). By [MP] (3) is equivalent to (3)’: every $s \in S$ can be expressed as the determinant of a matrix of poly($n$) size whose entries are (possibly non-homogeneous) linear combinations of the entries of $U_i$’s with coefficients of poly($n$) bit length. By [Cs, MP], it follows that, given such a weakly-skew straight-line program of an invariant $s \in S$ and any matrices $A_1, \ldots, A_r \in M_m(\mathbb{Q})$ (or $M_m(F_p)$ in positive characteristic), the value $s(A_1, \ldots, A_r)$ can be computed in time polynomial in $n$ and the total bit-length of the specifications of $A_i$’s (and even fast in parallel). Thus an s.s.o.p. is an approximation to h.s.o.p. that has a small specification and is easy to evaluate.

Definition 3.3  (a) We call a set $S$ an e.s.o.p. (explicit system of parameters) for $K[V]^G$ if (1) $S$ is an s.s.o.p. for $K[V]^G$, and (2) given $m$ and $r$, the specification of $S$, consisting of a weakly skew straight-line program as above for each $s \in S$, can be computed in poly($n$) time.

(b) We call $S$ a separating e.s.o.p. if (1) is replaced by the stronger (1)’: $S$ is a separating s.s.o.p. A separating quasi-e.s.o.p. is defined similarly using quasi-polynomials instead of polynomials.

(c) We say that Noether’s Normalization Lemma (NNL) for $V/G$ or $K[V]^G$ is derandomized if there exists an explicit system of parameters (e.s.o.p.) for $K[V]^G$. We say that it is derandomized in a strong sense if there exists a separating e.s.o.p. for $K[V]^G$.

3.3 Conditional derandomization

The following result proves Theorem 1.4 (a).

Theorem 3.4 Let $K$ be an algebraically closed field of characteristic zero.

(1) Assume that the black-box derandomization hypothesis for STIT (symbolic trace identity testing) over $K$ holds. Then $K[V]^G$ has a separating e.s.o.p.

(2) Assuming parallel black-box derandomization of STIT over $K$ (cf. Section 2.1), the problem of constructing a separating s.s.o.p. for $K[V]^G$ belongs to $\text{DET} \subseteq \text{NC}^2 \subseteq \text{P}$.

Here $\text{DET}$ denotes the class of functions that can be computed by uniform $\text{AC}^0$ circuits (of poly($n$) bit-size) with oracle access to the determinant function.

Proof: We only prove (1). The proof of (2) is similar using the parallel black-box derandomization hypothesis in place of the sequential hypothesis.

For any word $\alpha = i_1, \ldots, i_l$, $l \leq m^2$, $i_j \in [r]$, let

$$T_\alpha(U) = \text{trace}(U_{i_1} \cdots U_{i_l}),$$

(10)
where \( U = (U_1, \ldots, U_r) \). Let
\[
F = \{ T_{[\alpha]}(U) \},
\]
where \([\alpha]\) ranges over the equivalence classes (for circular rotation) of all words in \( 1, \ldots, r \) of length \( \leq m^2 \). Since we are assuming that the characteristic is zero, \( F \) generates \( K[V]^G \) by Theorem 2.6.

Consider the map
\[
\pi_{V/G} : A = (A_1, \ldots, A_r) \mapsto (\ldots, T_{[\alpha]}(A), \ldots).
\]
By Theorem 2.10, the image is already closed and can be identified with \( V/G \).

For any \( l \leq k := m^2 \), consider the generic invariant
\[
T_l(X, U) = \text{trace}((X_1 \otimes U_1 + \cdots + X_r \otimes U_r)^l),
\]
where \( X_i \)'s are new \( k \times k \) variable matrices, \( X = (X_1, \ldots, X_r) \), \( U = (U_1, \ldots, U_r) \), and \( \otimes \) denotes the Kronecker product of matrices. Thus each \( X_i \otimes U_i \) is an \( m' \times m' \) matrix, where \( m' = km = m^3 \), and for any \( A = (A_1, \ldots, A_r) \in M_m(K)^r \), \( T_l(X, A) \) is a symbolic trace polynomial over an \( m' \times m' \) matrix in the \( rk^2 \) entries of \( X_i \)'s. We have
\[
T_l(X, U) = \sum_\alpha T_{[\alpha]}(X)T_{[\alpha]}(U) = \sum_{[\alpha]} ||[\alpha]|| T_{[\alpha]}(X)T_{[\alpha]}(U),
\]
where \([\alpha] = [\alpha_1 \cdots \alpha_l]\) ranges over the equivalence classes of all words of length \( l \) with each \( \alpha_j \in [r] \), \(|[\alpha]|\) denotes the cardinality of the equivalence class \([\alpha]\) of the word \( \alpha \), and \( T_{[\alpha]}(U) \) and \( T_{[\alpha]}(X) \) are as in (10) and (1).

Let \( U' = (U'_1, \ldots, U'_r) \) be another tuple of variable \( m \times m \) matrices. For each \( l \leq k = m^2 \), define the symbolic trace difference
\[
\tilde{T}_l(X, U, U') = T_l(X, U) - T_l(X, U').
\]
Each \( \tilde{T}_l(X, U, U') \) can be expressed as \( \text{trace}(N_l(X, U, U')^r) \) for some symbolic matrix \( N_l(X, U, U') \) of size \( q = \text{poly}(n) \), \( r_l \leq q \), whose entries are (possibly non-homogeneous) linear functions over \( Q \) of the entries of \( X, U, \) and \( U' \). This is because STIT is equivalent to PIT for algebraic branching programs (cf. [2,10], and Section 2.1), and the difference between two branching programs is again a branching program.

By our black-box derandomization hypothesis for STIT, there exists an explicit (\( \text{poly}(n) \)-time computable) hitting set \( B = B_{s,q} \subseteq \mathbb{N}^s \) for STIT for \( q \times q \) matrices whose entries are linear functions of the \( s = rk^2 \) variable entries of \( X_i \)'s with coefficients in \( K \). Fix such an explicit \( B \). We think of each \( b \in B \) as an \( r \)-tuple \( b = (b_1, \ldots, b_r) \) of \( k \times k \) integral matrices. By the definition of the hitting set and the argument in the preceding paragraph, for any symbolic trace difference \( \tilde{T}_l(X, A, A') = T_l(X, A) - T_l(X, A'), \ l \leq k, \ A = (A_1, \ldots, A_r), \ A' = (A'_1, \ldots, A'_r) \in M_m(K)^r \), that is not identically zero as a polynomial in the \( s \) variable entries of \( X_i \)'s, there exists \( b \in B \) such that \( \tilde{T}_l(b, A, A') \neq 0 \).

Let
\[
S = \{ T_l(b, U) \mid b \in B, 1 \leq l \leq k \} \subseteq K[V]^G.
\]
Suppose $A, A' \in M_m(K)$ are two $r$-tuples such that for some invariant $h \in K[V]^G$, $h(A) \neq h(A')$. By Theorem 2.6 it follows that some generator $T_{[\alpha]}(U)$ assumes different values at $A$ and $A'$. By eq. (14) and Corollary 2.8 this implies that $T_l(X, A, A') = T_l(X, A) - T_l(X, A')$ is not identically zero for some $l \leq m^2$. This means there exists $b \in B$ such that $T_l(b, A, A') \neq 0$; i.e., $T_l(b, A) \neq T_l(b, A')$. It follows that $S$ is separating. By Theorem 2.12 it follows that $K[V]^G$ is integral over the subring generated by $S$. Every element of $S$ is clearly homogeneous of poly($n$) degree. Since the hitting set $B$ is explicit, and matrix powering, Kronecker product, and trace have short and explicit weakly-skew straight-line programs [C, MP], it follows from eq. (13) that the specification of $S$ consisting of a weakly skew straight-line program for its every element can be computed in poly($n$) time. Hence $S$ is a separating e.s.o.p. Q.E.D.

For future reference, we note down the following consequesnces of the proof.

**Lemma 3.5** Let $X = (X_1, \ldots, X_r)$ be $k \times k$ variable matrices, where $k = m^2$. There exist poly($n$)-time computable weakly skew circuits $C_i$’s, $l \leq m^2$, over the variable entries of $X_i$’s and $U_i$’s such that (1) the polynomial functions $C_i(X, U)$’s computed by $C_i$’s are of poly($n$) degree, homogeneous in $X$ and $U$, and can be written as

$$C_i(X, U) = \sum_{[\alpha]} f_{[\alpha],l}(X)g_{[\alpha],l}(U),$$

where $[\alpha] = [\alpha_1 \cdots \alpha_l]$ ranges over the equivalence classes of all words of length $l$ with each $\alpha_j \in [r]$, (2) $f_{[\alpha],l}(X)$’s are linearly independent homogeneous polynomials in the entries of $X$, and (3) $g_{[\alpha],l}(U)$’s are homogeneous invariants that generate $K[V]^G$.

This result, a key ingredient in the proof of Theorem 3.4, says that the variety $V/G$ here is strongly explicit as per the general notion of explicit varieties that we shall formulate later (Definition 4.4) taking $V/G$ as a basic prototype of such varieties.

**Proof:** Let $C_l$ be a weakly skew circuit [MP] computing $T_l(X, U)$, cf. eq. (13), so that $C_l(X, U) = T_l(X, U)$, $f_{[\alpha],l}(X) = [[\alpha]]T_{[\alpha]}(X)$, and $g_{[\alpha],l}(U) = T_{[\alpha]}(U)$; cf. eq. (14). Then $f_{[\alpha],l}(X)$’s are linearly independent by Corollary 2.8 and $g_{[\alpha],l}(U)$’s generate $K[V]^G$ by Theorem 2.6 Q.E.D.

**Theorem 3.6** The problem of deciding if the closures of the $G$-orbits of two rational points in $V$ intersect belongs to co-RNC.

**Proof:** By Theorem 2.10 (d) and the proof of Theorem 3.4, the closures of the $G$-orbits of $A, A' \in V$ intersect iff the symbolic trace difference $\tilde{T}_l(X, A, A') = \tilde{T}_l(X, A) - \tilde{T}_l(X, A')$ is identically zero for every $l \leq k = m^2$. For rational $A$ and $A'$, this can be tested by a co-RNC algorithm [IM]: just substitute large enough random integer values for the entries of $X$ and test if all the differences vanish. Q.E.D.

3.4 Unconditional quasi-derandomization

In this section we describe the recent development in Forbes and Shpilka [FS3] leading to Theorem 1.4 (b).
Lemma 3.7 (Forbes, Shpilka) (cf. Lemmas 2.3 and 3.4 in [FS3]) Let $K$ be any field. For any positive integer $l$, there exists a read only algebraic branching program (ROABP) $P_l(Y, U, U')$ of poly$(l, m, r)$ size over $K$ and the variable entries of $U$, $U'$, and the tuple $Y = (y_1, \ldots, y_l)$ of auxiliary variables such that

$$P_l(Y, U, U') = \sum_\alpha Y_\alpha (T_\alpha(U) - T_\alpha(U')),$$

where $\alpha$ ranges over all words of length $l$ with each $\alpha_j \in [r]$, $Y_\alpha = \prod_j y_\alpha^j$.

Proof: The r.h.s. of (18) equals (trace($\prod_{j=1}^{l} \left( \sum_{i=1}^{r} y_i^j U_i \right)$)) - (trace($\prod_{j=1}^{l} \left( \sum_{i=1}^{r} y_i^j U'_i \right)$)), which can clearly be computed by an ROABP of poly$(l, m, r)$ size. Q.E.D.

Since the monomials $Y_\alpha$'s are linearly independent, we can replace $T_l(X, U, U')$ by $P_l(Y, U, U')$ in the proof of Theorem 3.4. This implies that Theorem 3.4 also holds after replacing STIT by PIT for ROABP in its statement. Theorem 1.4 (b) follows in view of Theorem 2.5. This replacement also derandomizes the co-RNC-algorithm in Theorem 3.6 in view of the NC non-black-box algorithm for PIT for ROABP in [Arv].

3.5 Explicit parametrization of closed orbits

The following result says that a separating e.s.o.p., as constructed in Theorem 3.4, implies explicit parametrization of closed orbits, i.e., a one-to-one and onto explicit (polynomial time computable) regular map from the closed orbits of $V$ to the points of a closed variety embedded in an ambient space of poly$(n)$ dimension.

Theorem 3.8 Let $K$ be an algebraically closed field of arbitrary characteristic. Suppose $S$ is a separating e.s.o.p. for $K[V]^G$. Let $\psi_S : V \to K^k$, $k = |S|$, denote the map

$$\psi_S : \quad v \to (s_1(v), \ldots, s_k(v)),$$

where $s_1, \ldots, s_k$ are the elements of $S$. It can be factored as:

$$V \xrightarrow{\pi_{V/G}} V/G \xrightarrow{\psi'_S} K^k. \quad (19)$$

(1) Given a rational $v \in V$, $\psi_S(v)$ can be computed in time that is polynomial in $n$ and the bit length of the specification of $v$. If $v$ is not rational then $\psi_S(v)$ can be computed in poly$(n)$ operations over $K$.

(2) The image $\psi_S(V) \subseteq K^k$ is a closed subvariety. The map $\psi'_S$ from $V/G$ to $\psi_S(V)$ is one-to-one and onto.

(3) For any $x \in \psi_S(V)$, $\psi_S^{-1}(x)$ contains a unique closed $G$-orbit in $V$.

This result holds for any finite dimensional rational representation $V$ of $G$. The definition of an e.s.o.p. in this general setting is given later (Definition 4.4).

Proof: (1) This follows because $S$ is an e.s.o.p.
By Theorem 2.10 (a), the first map in (19) is surjective. The image of the second map in (19) is closed because $K[V/G] = K[V]^G$ is integral over the subring generated by $S$. The map $\psi'_S$ is one-to-one because $S$ is separating.

(3) This follows from (2) and Theorem 2.10 (b). Q.E.D.

3.6 Explicit parametrization of semi-simple representations of any finitely generated algebra

Next we show (Theorem 3.9) that an explicit separating e.s.o.p. (as constructed in Theorem 3.4) implies explicit parametrization of semi-simple representations of any finitely generated algebra in characteristic zero.

Let $K$ be an algebraically closed field of characteristic zero. Let $R$ be a finitely generated associative algebra over $K$, specified by its generators $f_1, \ldots, f_r$ and the relations among them. Let $\rho : R \to M_m(K)$ be an $m$-dimensional representation of $R$. Let $n = rm^2$. Two representations are isomorphic iff they lie in the same $G$-orbit, $G = SL_m(K)$. The representations with closed $G$-orbits are called stable or semi-simple. Each $m$-dimensional representation $\rho$ of $R$ can be identified with the $r$-tuple $(A_1, \ldots, A_r) \in V = M_m(K)^r$ of $m \times m$ matrices, $A_i = \rho(f_i)$. The set $W_m = W_m(R)$ of $m$-dimensional representations of $R$ is a closed $G$-subvariety of $V$.

Theorem 3.9 Let $K$ be an algebraically closed field of characteristic zero, $R$ a finite-dimensional associative algebra over $K$, and $V = M_m(K)^r$.

(a) Assuming black-box derandomization of STIT (or PIT for ROABP) there exists a separating e.s.o.p. $S = S_m$ for $K[V]^G$. This yields an explicit parametrization of semi-simple representations of $R$. Specifically, it yields a one-to-one and onto explicit (polynomial time computable) map $\psi_S$ from the closed $G$-orbits in $W_m$ to the points of $\psi_S(W_m) \subseteq K^k$, $k = |S| = \text{poly}(n)$. Furthermore, $\psi_S(W_m)$ is a closed subvariety of $K^k$.

(b) There also exists a separating quasi-e.s.o.p. $S = S_m$ for $K[V]^G$ unconditionally. This yields a one-to-one and onto quasi-explicit (quasi-polynomial time computable) map $\psi_S$ from the closed $G$-orbits in $W_m$ to the points of $\psi_S(W_m) \subseteq K^k$, $k = |S| = \text{poly}(n)$. Furthermore, $\psi_S(W_m)$ is a closed subvariety of $K^k$.

This result follows from Theorems 1.4, 3.8 and the following result.

Proposition 3.10 Suppose $S$ is a separating e.s.o.p. of $K[V]^G$. Then:

(a) Given any rational $m$-dimensional representation $\rho$ of $R$, $\psi_S(\rho)$ can be computed in time polynomial in $n$ and the bit-length of the specification of $\rho$. If $\rho$ is not rational, then $\psi_S(\rho)$ can be computed in poly($n$) arithmetic operations over $K$.

(b) The image $W'_m = \psi_S(W_m)$ is a closed subvariety of $K^k$, $k = |S| = \text{poly}(n)$.

(c) For any $x \in W'_m$, $\psi_S^{-1}(x)$ contains a unique closed $G$-orbit in $W_m$.

Proof:

(a) This follows since $S$ is an e.s.o.p.

23
(b) By Theorem 2.10 (c), $Y = \pi_{V/G}(W_m)$ is a closed subvariety of $V/G$. The image $\psi'_S(Y)$, with $\psi'_S$ as in eq. (19), is closed since $K[V/G] = K[V]^G$ is integral over the subring generated by $S$ and hence $\psi'_S$ is a finite morphism.

(c) This follows from Theorem 3.8 (3). Q.E.D.

3.7 Generalization to quivers

We now generalize Theorem 3.4 to arbitrary quivers.

Let $Q$ be a quiver $[BP]$, i.e., a four-tuple $(Q_0, Q_1, t, h)$, where $Q_0 = \{1, \ldots, l\}$ is a set of vertices, $Q_1$ is a finite set of arrows between these vertices, and the two maps $t, h : Q_1 \to Q_0$ assign to each arrow $\phi \in Q_1$ its tail $t(\phi)$ and head $h(\phi)$. Loops and multiple arrows are allowed. A representation $W$ of the quiver $Q$ over a field $K$ is a family $\{W(i) : i \in Q_0\}$ of finite dimensional vector spaces over $K$. The $l$-tuple of integers $\dim(W) = \{\dim(W(i)) : i \in Q_0\}$ is called the dimension vector of $W$. A morphism between two representations $f : W_1 \to W_2$ is a family of linear morphisms $\{f(i) : W_1(i) \to W_2(i) \mid i \in Q_0\}$ such that, for all $\phi \in Q_1$, $W_2(\phi) \circ f(t(\phi)) = f(h(\phi)) \circ W_1(\phi)$. For a fixed dimension vector $m = (m(1), \ldots, m(l)) \in \mathbb{N}^l$, the representation space $V = V(Q, m)$ of the quiver $Q$ is the set of all representations $W$ of $Q$ such that $W(i) = K^{m(i)}$ for all $i \in Q_0$. Clearly,

$$V = V(Q, m) = \oplus_{\phi \in Q_1} \text{Hom}_K(K^{m(t(\phi))}, K^{m(h(\phi))}) = \oplus_{\phi \in Q_1} M_\phi(K),$$

where $M_\phi(K)$ denotes the space of $m(h(\phi)) \times m(t(\phi))$ matrices with entries in $K$. There is a canonical action of

$$G = \prod_{i=1}^l GL_{m(i)}(K)$$
on $V$ defined by

$$(g \cdot W)(\phi) = g(h(\phi))W(\phi)g(t(\phi))^{-1}$$

for any $g = (g(1), \ldots, g(l)) \in G$ and $W \in V(Q, m)$. The $G$-orbits in $V$ are precisely the isomorphism classes of representations of $Q$ with the dimension vector $m$.

Assume that $K$ is an algebraically closed field of characteristic zero. Let $U = (\ldots, U_\phi, \ldots)$ be the tuple of variable matrices, where $U_\phi$ is a $m(h(\phi)) \times m(t(\phi))$ variable matrix. Then the coordinate ring $K[V]$ of $V$ can be identified with the ring $K[U]$ over the variable entries of $U_\phi$'s. Let $K[V]^G \subseteq K[V]$ be the subring of $G$-invariants. When $Q$ consists of a single vertex with $r$ self-loops and dimension $m$, $K[V]^G$ coincides with the invariant ring in Theorem 3.4.

The following result generalizes Theorem 3.4 to arbitrary quivers.

**Theorem 3.11** Let $K$ be an algebraically closed field of characteristic zero, and $n = |Q_0| + |Q_1| + |m|$, where $|m| = \sum_{i \in Q_0} m(i)$. Then the analogue of Theorem 3.4 (and also Theorem 1.4 (b)) holds for $V$ and $G$ as above.

**Proof:** Let $R_Q$ denote the finitely generated path algebra $[Br]$ for $Q$. Semi-simple representations of $Q$ correspond to semi-simple representations of $R_Q$ (cf. Proposition 1.2.2 in $[Br]$). The result follows from Theorem 3.9 applied to $R_Q$ and Theorem 1.4. Q.E.D.
4 The general ring of invariants

In this section we prove Theorem 4.3.

Let $K$ be an algebraically closed field of characteristic zero. Let $V$ be a polynomial representation of $G = SL_n(K)$ of dimension $n$. Since $G$ is reductive, $V$ can be decomposed as a direct sum of irreducibles:

$$V = \oplus \lambda m(\lambda) V_\lambda(G).$$

(21)

Here $\lambda : \lambda_1 \geq \cdots \geq \lambda_r > 0$, $r < m$, is a partition, i.e., a non-increasing sequence of positive integers, $V_\lambda(G)$ is the irreducible Weyl module of $G$ labelled by $\lambda$, and $m(\lambda)$ is its multiplicity. The degree $d$ of $V$ is defined to be the maximum of $|\lambda| = \sum \lambda_i$ for the $\lambda$’s that occur in this decomposition with nonzero multiplicity. It is easy to see that $d \leq n$ (Lemma 4.16). For each copy of $V_\lambda(G)$ that occurs in this decomposition, fix the standard monomial basis of $V$ that occurs in the decomposition (21) with nonzero multiplicity.

Let $K[V]^G \subseteq K[V]$ be the ring of invariants, and $V/G := \text{spec}(K[V]^G)$, the categorical quotient [MPK]. We assume that $V/G$ and $K[V]^G$ are specified succinctly by the tuple

$$\langle V, G \rangle := (n, m, \langle \lambda^1, m(\lambda^1) \rangle, \ldots, \langle \lambda^s, m(\lambda^s) \rangle)$$

(22)

that specifies $V$ and $G$ by giving $n$ and $m$ in unary and the multiplicity $m(\lambda^i)$ (in unary) of each Weyl module $V_{\lambda^i}(G)$ that occurs in the decomposition (21) with nonzero multiplicity.

**Theorem 4.1 (Derksen) (cf. Theorem 1.1, Proposition 1.2 and Example 2.1 in [D])** The ring $K[V]^G$ is generated by homogeneous invariants of degree $\leq \ell = nm^2d^m$.

This bound is poly($n$) when $m$ is constant, since $d \leq n$ (Lemma 4.16).

Let $K[V]^G_\leq \subseteq K[V]^G$ be the subspace of invariants of degree $\leq \ell$, and $K[V]^{G}_{\leq \ell}$ the subspace of non-constant invariants of degree $\leq \ell$. The spaces $K[V]_\ell$ and $K[V]^{G}_{\leq \ell}$ are defined similarly. The dimension $t$ of $K[V]^{G}_{\leq \ell}$ is bounded by \( \dim(K[V]^{G}_{\leq \ell}) = \sum_{c \leq \ell} \binom{c+n-1}{n-1} \). This bound is exponential in $n$, even when $m$ is constant. This worst case upper bound on $t$ is not tight. But we can not expect a significantly better bound since, the singularities of $K[V]^G$ being rational [Bt], the function \( h(\ell) = \dim(K[V]^G) \) is, by [F], a quasi-polynomial of degree $\dim(V/G) \geq \dim(V) - \dim(G) = n - m^2$.

Let $F = \{f_1, \ldots, f_l\}$ be a set of non-constant homogeneous invariants that form a basis of $K[V]^{G}_{\leq \ell}$. By Theorem 4.1 $F$ generates $K[V]^G$. Consider the morphism $\pi_{V/G}$ from $V$ to $K^t$ given by

$$\pi_{V/G} : v \rightarrow (f_1(v), \ldots, f_l(v)).$$

(23)

By Theorem 2.10 the image of this morphism is closed, and $V/G$ can be identified with this closed image. Let $z = (z_1, \ldots, z_t)$ be the coordinates of $K^t$, $I$ the ideal of $V/G$ under this embedding, $K[V/G]$ its coordinate ring. Then $K[V/G] = K[z]/I$, and we have the comorphism $\pi^*_v : K[V/G] \rightarrow K[V]$ given by
\[
\pi_{V/G}^*(z_i) = f_i. \tag{24}
\]

Since \( f_i \)'s are homogeneous, \( K[V/G] \) is a graded ring, with the grading given by \( \deg(z_i) = \deg(f_i) \). Furthermore, \( \pi_{V/G}^* \) gives the isomorphism between \( K[V/G] \) and \( K[V]^G \):

\[
\pi_{V/G}^*(K[V/G]) = K[V]^G.
\]

### 4.1 Construction of an h.s.o.p.

Gröbner basis theory implies the following result.

**Proposition 4.2** The problem of constructing an h.s.o.p. for \( K[V]^G \) belongs to \( \text{EXPSPACE} \).

The algorithm here needs exponential space and double exponential time even when \( m \) is constant because, as already observed, the dimension \( t \) of the ambient space \( K^t \) containing \( V/G \), cf. eq. (23), is exponential in \( n \) even when \( m \) is constant. Furthermore, the time requirement of this algorithm remains double exponential even if we only want to construct an \( S \) of poly(\( n \)) size (not necessarily optimal) such that \( K[V]^G \) is integral over the subring generated by \( S \).

If the second fundamental theorem (SFT) akin to that for matrix invariants (Theorem 2.9) holds for \( K[V]^G \) (cf. Definition 5.13) then the problem of constructing an h.s.o.p. can be put in \( REXP^{NP} \) assuming GRH; cf. Theorem 5.12.

It follows from Sturmfels [Sim2] (cf. Theorems 4.6.1 and 4.7.1. therein) that \( K[V]^G \) is integral over the subring generated by any homogeneous basis \( F' = \{ f'_1, \ldots, f'_t \} \) of \( K[V]_{\leq d}^G \), \( t' = m^2(dm + 1)^m \). We can use \( F' \) instead of \( F \) in the algorithms of this section. If \( V = V(d)(G) \), then \( n = \dim(V) = \left( \frac{d+m-1}{m-1} \right) \), and \( t' \) is still exponential in \( n \) for constant \( m \). So the algorithm in Proposition 4.2 will still need exponential space and double exponential time for constant \( m \).

For the proof of Proposition 4.2 we need the following result.

**Lemma 4.3** Let \( F = \{ f_1, \ldots, f_t \} \) be the set of generators of \( K[V]^G \) as in (23). A generating set of syzygies among the elements of \( F \) can be constructed in work-space exponential in \( n \) and \( m \) and time that is double exponential in \( n \) and \( m \).

**Proof:**

Let \( \pi_{V/G} \) be the morphism from \( V \) to \( K^t \) based on \( F \) as in e.q. (23). Using this embedding of \( V/G \) and the Gröbner basis algorithm in [MR2], we can compute a generating set of syzygies among the elements of \( F \). This algorithm works in space that is exponential in \( \dim(V/G) \leq n \), polynomial in the dimension \( t \) of the ambient space, and poly-logarithmic in the maximum degree of the elements in \( F \); cf. Theorem 1 in [MR2]. This work-space requirement is clearly single exponential in \( n \) and \( m \) (since \( d \leq n \)). Q.E.D.

**Proof of Proposition 4.2:**

This is proved just like the first statement of Theorem 3.1 using the set \( F \) of generators in Lemma 4.3 instead of the set \( F \) there. Q.E.D.
4.2 On derandomization of Noether’s normalization lemma

The following result (Theorem 4.5 (2)) says that the double exponential time bound in Proposition 4.2 can be brought down to quasi-polynomial for constant $m$ requiring $|S|$ to be $O(\text{poly}(n))$ (instead of optimal). Before we can state the result, we need a few definitions.

The following definition is a generalization of the definitions of s.s.o.p. and e.s.o.p. for matrix invariants (cf. Definitions 3.2 and 3.3) in this context. We say that Noether’s normalization lemma for $V/G$ or $K[V]^G$ is derandomized if there exists an explicit system of parameters (e.s.o.p) for $K[V]^G$ as defined below. We say that it is derandomized in a strong sense if there exists a separating e.s.o.p. for $K[V]^G$ as defined below.

Definition 4.4 (a) We say that $S \subseteq K[V]^G$ is an s.s.o.p. (small system of parameters) for $K[V]^G$ if (1) $K[V]^G$ is integral over the subring generated by $S$, (2) the cardinality of $S$ is $\text{poly}(n,m)$, (3) every invariant in $S$ is homogeneous of $\text{poly}(n,m)$ degree, and (4) every $s \in S$ has a small specification in the form of a weakly skew straight-line program $\langle \text{MP} \rangle$ of $\text{poly}(n,m)$ bit-length over $Q$ and the coordinates $v_1, \ldots, v_n$ of $V$ in the standard monomial basis.

(b) We say that a subset $S \subseteq K[V]^G$ is an e.s.o.p. (explicit system of parameters) for $K[V]^G$ if (1) $S$ is an s.s.o.p. for $K[V]^G$, and (2) the specification of $S$, consisting of a weakly skew straight-line program as above for each $s \in S$, can be computed in $\text{poly}(n,m)$ time, given $n,m$, and the nonzero multiplicities $m(\lambda)$’s of $V_{\lambda}(G)$’s as in eq. (21).

(c) Quasi-s.s.o.p. and quasi-e.s.o.p. are defined similarly by replacing the $\text{poly}(n,m)$ bounds by $O(2^\text{polylog}(n,m))$ bounds. Subexponential-s.s.o.p. and subexponential-e.s.o.p. with exponent $\delta > 0$ are defined by replacing the $\text{poly}(n,m)$ bounds by $O(2^{O(\ell(n,m)\delta)})$ bounds.

(d) S.s.o.p., e.s.o.p., and the related notions are defined in a relaxed sense by dropping the weakly skew requirement in (a) (4) and the degree requirement in (a) (3).

Here (4) in (a) is equivalent $\langle \text{MP} \rangle$ to (4)’: every $s \in S$ can be expressed as the determinant of a matrix of $\text{poly}(n,m)$ size whose entries are (possibly non-homogeneous) linear combinations of $v_1, \ldots, v_n$ with rational coefficients of $\text{poly}(n,m)$ bit length. By [Cs], it follows that, given such a weakly skew straight-line program of an invariant $s \in S$ and the coordinates of any rational point $v \in V$, the value $s(v)$ can be computed in time that is polynomial in $n,m$, and the total bit-length $\langle v \rangle$ of the specification of $v$, and even fast in parallel, by a uniform $AC^0$ circuit of $\text{poly}(n,m,\langle v \rangle)$ bit-size with oracle access to $DET$.

The following is the full statement of Theorem 1.3 (a).

Theorem 4.5

(1) Suppose the black-box derandomization hypothesis for PIT for diagonal depth three circuits over $K$ holds (cf. Section 2.1). Then $K[V]^G$ has a separating e.s.o.p., if $m$ is constant.

Specifically, there exists a set $S \subseteq K[V]^G$ of $\text{poly}(N)$ invariants, $N = n^{m^2}d^{m^4}$, such that (1) $S$ is separating, and hence (cf. Theorem 2.13) $K[V]^G$ is integral over its subring generated by $S$, (2) every invariant in $S$ is homogeneous of $\text{poly}(N)$ degree, (3) every $s \in S$ has a weakly skew straight-line program over $Q$ and $v_1, \ldots, v_n$ of $\text{poly}(N)$ bit-length, and (4) the specification of $S$, consisting of such a weakly skew straight-line program for every invariant in $S$, can be computed in $\text{poly}(N)$ time.
Assuming the parallel black-box derandomization hypothesis for PIT for diagonal depth three circuits (cf. Section 2.1), the specification of $S$ can be computed by a uniform $AC^0$ circuit of poly$(N)$ bit-size with oracle access to $DET$.

(2) Suppose $m$ is constant, or more generally, $O(polylog(n))$ (as is the case if $m = O(\sqrt{d})$; cf. Lemma 4.16). Then $K[V]^G$ has a separating quasi-e.s.o.p. (unconditionally). Furthermore, such a separating quasi-e.s.o.p. can be constructed by a uniform $AC^0$ circuit of quasi-poly$(n)$ bit-size with oracle access to $DET$.

Theorem 1.3 (a) follows from (2). The proof of this result given in this section also goes through if the characteristic of $K$ is $\Omega(2^{n^{O(m^2)}})$ (as the reader can easily check).

To prove Theorem 1.5, we first recall some results from standard monomial theory [LR, DRS] and prove some lemmas. In what follows, we let $N = n^{m^2}d^{m^4}$ as above.

4.3 The standard monomial basis of $V$

We now define the standard monomial basis of $V$ mentioned in Definition 4.4 following [LR] and prove some lemmas concerning its complexity-theoretic properties.

Let $\bar{G} = GL_m(K)$. Let $Z$ be an $m \times m$ variable matrix. Let $K[Z]$ be the ring generated by the variable entries of $Z$. Let $K[Z]_d$ denote the degree $d$ part of $K[Z]$. It has commuting left and right actions of $\bar{G}$, where $(\sigma, \sigma') \in \bar{G} \times \bar{G}$ maps $h(Z) \in K[Z]_d$ to $h(\sigma'Z\sigma')$. For each partition $\lambda : \lambda_1 \geq \cdots \geq \lambda_q > 0$, $q \leq m$, the Weyl module $V_\lambda(\bar{G})$ labelled by $\lambda$ can be embedded in $K[Z]_d$, $d = |\lambda| = \sum \lambda_i$, as follows.

Let $(A, B)$ be a bi-tableau of shape $\lambda$. This means both $A$ and $B$ are Young tableau [En] of shape $\lambda$ such that (1) each box of $A$ or $B$ contains a number in $[m] = \{1, \ldots, m\}$, (2) all columns of $A$ and $B$ are strictly increasing, and (2) all rows are non-decreasing. Let $A_i$ and $B_i$ denote the $i$-th column of $A$ and $B$ respectively. With any pair $(A_i, B_i)$ of columns, we associate the minor $Z(A_i, B_i)$ of $Z$ indexed by the row numbers occurring in $A_i$ and the column numbers occurring in $B_i$. With each bi-tableau $(A, B)$ we associate the monomial in the minors of $Z$ defined by $Z(A, B) := Z(A_1, B_1)Z(A_2, B_2)Z(A_3, B_3)\cdots$. We call such a monomial standard of shape $\lambda$ and degree $d = |\lambda|$. We call a monomial in the minors of $Z$ nonstandard if it is not standard. It is known [DRS] that the standard monomials of degree $d$ form a basis of $K[Z]_d$. We call it the DRS-basis of $K[Z]_d$ and denote it by $B(Z)_d$.

A standard monomial $Z(A, B)$ is called canonical if the column $B_i$, for each $i$, just consists of the entries $1, 2, 3, \ldots$ in the increasing order. It is easy to see that, for each partition $\lambda$, the subspace of $K[Z]$ spanned by the canonical monomials of shape $\lambda$ is a representation of $G$ under its left action on $K[Z]$. It is known [LR] that this representation is isomorphic to the Weyl module $V_\lambda(\bar{G})$ of $\bar{G}$, and that the set of canonical monomials of shape $\lambda$ form its basis. We refer to it as the standard monomial basis of $V_\lambda(\bar{G})$, and denote it by $B_\lambda = B_\lambda(\bar{G})$. Each Weyl module $V_\lambda(G)$ of $G = SL_m(K)$ is also a Weyl module of $\bar{G}$ in a natural way. Hence this also specifies the standard monomial basis $B_\lambda$ of $V_\lambda(G)$.

Fix the standard monomial basis $B_\lambda$ in each copy of $V_\lambda(G)$ in the complete decomposition of $V$ as in (21). This yields a basis $B(V)$ of $V$, which we call its standard monomial basis. It depends on the choice of the decomposition of $V$ (if the multiplicities are greater than one). But
this choice does not matter in what follows.

Lemma 4.6 (a) Given any nonstandard monomial \( \mu \) of degree \( d \) in the minors of \( Z \), the coefficients of \( \mu \) in the DRS basis \( B(Z)_d \) can be computed in poly\((d^{m^2})\) time. More strongly, they can be computed by a uniform AC\(^0\) circuit of poly\((d^{m^2})\) bit-size with oracle access to DET.

(b) Consider \( K[Z]_d \) as a left \( G \)-module, where \( g \in G \) maps \( h(Z) \) to \( (g \cdot h)(Z) = h(g'Z) \). Then, given the specifying label (a bi-tableau) of any basis element \( b \in B(Z)_d \) and \( g \in GL_m(\mathbb{Q}) \), the coefficients of \( g \cdot b \) in the DRS-basis \( B(Z)_d \) can be computed in poly\((d^{m^2}, \langle g \rangle)\) time, where \( \langle g \rangle \) denotes the bit-length of the specification of \( g \). More strongly, they can be computed by a uniform AC\(^0\) circuit of poly\((d^{m^2}, \langle g \rangle)\) size with oracle access to DET.

(c) Let \( V_\lambda(\hat{G}) \) be a Weyl module of degree \( d \), and \( B_\lambda \) its standard monomial basis as described above. For any basis element \( b \in B_\lambda \), and \( g \in GL_m(\mathbb{Q}) \), the coefficients of \( g \cdot b \) in the basis \( B_\lambda \) can be computed in poly\((d^{m^2}, \langle g \rangle)\) time. More strongly, they can be computed by a uniform AC\(^0\) circuit of poly\((d^{m^2}, \langle g \rangle)\) bit-size with oracle access to DET.

When \( m \) is constant, the poly\((d^{m^2})\) bound becomes poly\((d) = O(poly(n))\).

Proof:

(a) Let \( B'(Z)_d \) denote the usual monomial basis of \( K[Z]_d \) consisting of the monomials in the entries \( z_{ij} \) of \( Z \) of total degree \( d \). The cardinality of \( B'(Z)_d \) is equal to the number of monomials of degree \( d \) in the \( m^2 \) variables \( z_{ij} \). This number is \( \binom{d+m^2-1}{m^2-1} = poly(d^{m^2}) \). The cardinality of \( B(Z)_d \) is the same. Let \( A_d \) be the matrix for the change of basis so that:

\[
B(Z)_d = A_d B'(Z)_d , \quad \text{and} \quad B'(Z)_d = A_d^{-1} B(Z)_d . \tag{25}
\]

The matrix \( A_d \) can be computed in poly\((d^{m^2})\) time. For this, observe that each row of \( A_d \) corresponds to the expansion of a standard monomial \( b \in B(Z)_d \) in the usual monomial basis \( B'(Z)_d \). Since the number of monomials of degree \( \leq d \) in the \( m^2 \) variable entries of \( Z \) is poly\((d^{m^2})\) and the degree of \( b \) is \( d \), this expansion can be computed by a uniform weakly skew [MP] straight-line program of poly\((d^{m^2})\) bit-size (constructed by induction on \( d \)). It follows [MP] that it can also be computed fast in parallel by a uniform AC\(^0\) circuit of poly\((d^{m^2})\) bit-size with oracle access to DET. This yields the representation of \( b \) in the basis \( B'(Z)_d \). Thus \( A_d \) can be computed by a uniform AC\(^0\) circuit of poly\((d^{m^2})\) bit-size with oracle access to DET.

Once \( A_d \) has been computed, \( A_d^{-1} \) can also be computed fast in parallel by a uniform AC\(^0\) circuit of poly\((d^{m^2})\) bit-size with oracle access to DET.

The standard representation in the basis \( B(Z)_d \) of any nonstandard monomial \( \mu \in K[Z]_d \) in the minors of \( Z \) can now be computed fast in parallel as follows. Let \( b(\mu) \) and \( b'(\mu) \) be the row vectors of the coefficients of \( \mu \) in the bases \( B(Z)_d \) and \( B'(Z)_d \), respectively. Clearly \( b(\mu) = b'(\mu) A_d^{-1} \). Expand \( \mu \) fast in parallel (as we expanded \( b \) above) to get its representation \( b'(\mu) \). Multiply this on the right by \( A_d^{-1} \) fast in parallel to get \( b(\mu) \).

(b) First we expand \( g \cdot b \) fast in parallel (as above) to get its representation in the usual monomial basis \( B'(Z)_d \). The representation in \( B(Z)_d \) can now be computed fast in parallel by multiplication on the right by \( A_d^{-1} \).
(c) This follows from (b) using the concrete realization of \( V_\lambda(G) \) described before Lemma 4.6 as the \( G \)-submodule of \( K[Z]_d \), \( d = |\lambda| \), spanned by the canonical standard monomials of shape \( \lambda \). Q.E.D.

We also note the following for future reference.

**Lemma 4.7** (a) Given any standard monomial \( b \in B(Z)_d \) and a generic (variable) \( u \in \bar{G} \), the coefficients of \( u \cdot b \) in the basis \( B(Z)_d \) can be computed in \( \text{poly}(d^{m^2}) \) time. More strongly, they can be computed by a uniform \( AC^0 \) circuit of \( \text{poly}(d^{m^2}) \) bit-size with oracle access to \( \text{DET} \). These coefficients are polynomials in \( u \) of degree \( d \).

(b) Given any basis element \( b \in B_{\lambda} \) and a generic \( u \in G \), the coefficients of \( u \cdot b \) in the basis \( B_{\lambda} \) can be computed in \( \text{poly}(d^{m^2}) \) time. More strongly, they can be computed by a uniform \( AC^0 \) circuit of \( \text{poly}(d^{m^2}) \) bit-size with oracle access to \( \text{DET} \). These coefficients are polynomials in \( u \) of degree \( d = |\lambda| \).

The proof is similar to that of Lemma 4.6.

### 4.4 Proof of Theorem 4.5 assuming explicitness of \( V/G \)

Let \( v = (v_1, \ldots, v_n) \) be the coordinates of \( V \) in the standard monomial basis \( B(V) \) of \( V \). Let \( x = (x_1, \ldots, x_n) \) be new variables. Let

\[
X = \sum x_i v_i \in K[V; x], \quad (26)
\]

be a generic affine combination of \( v_i \)’s. Here \( K[V; x] \) denotes the ring obtained by adjoining \( x_1, \ldots, x_n \) to \( K[V] = K[v_1, \ldots, v_n] \). Then, for any \( c > 0 \), \( X^c \in K[V; x] \) is a generic linear combination of all monomials in \( v_i \)’s of total degree \( c \):

\[
X^c = \sum_{a_1, \ldots, a_n \geq 0, \sum a_i = c} c \left( a_1, \ldots, a_n \right) \left( \prod_{i \geq 1} x_i^{a_i} \right) \left( \prod_{i \geq 1} v_i^{a_i} \right). \quad (27)
\]

Here \( \left( a_1, \ldots, a_n \right) \) denotes the multinomial coefficient, and the monomials \( \left( \prod_{i \geq 1} v_i^{a_i} \right) \) occurring in this expression form a basis of the subspace \( K[V]_c \subseteq K[V] \) of polynomials on \( V \) of degree \( c \).

Let \( R = R_G : K[V] \to K[V]^G \) denote the Reynolds’ operator for \( G \) (cf. Section 2.2.1 in [DK]). We denote the induced map from \( K[V; x] \) to \( K[V]^G[x] \) by \( R \) as well. Here \( K[V]^G[x] \) denotes the ring obtained by adjoining \( x_1, \ldots, x_n \) to \( K[V]^G \). Now consider a generic invariant

\[
R(X^c)(v, x) = \sum_{a_1, \ldots, a_n \geq 0, \sum a_i = c} c \left( a_1, \ldots, a_n \right) R\left( \prod_{i \geq 1} v_i^{a_i} \right) \left( \prod_{i \geq 1} x_i^{a_i} \right) \in K[V]^G[x]. \quad (28)
\]

Since the monomials \( \left( \prod_{i \geq 1} v_i^{a_i} \right) \) in (27) form a basis of \( K[V]_c \), it follows from the properties of the Reynolds’ operator that the elements \( R\left( \prod_{i \geq 1} v_i^{a_i} \right) \in K[V]^G \) occurring in (28) span the subspace \( K[V]^G[c] \subseteq K[V]^G \) of invariants of degree \( c \). By Theorem 4.1 the invariants of degree \( \leq l := nm^2 d^{m^2} \) generate \( K[V]^G \). Hence the set

\[
F = \{R(\prod_{i \geq 1} v_i^{a_i}) \mid \sum_i a_i = c, 0 < c \leq l\}. \quad (29)
\]
generates $K[V]^G$.

Let $\Delta_3[n,l,k]$ denote the class of diagonal depth three circuits (cf. Section 3.4) over $K$ and the variables $x_1, \ldots, x_n$ with total degree $\leq l$ and top fan-in $\leq k$. The size of any such circuit is $O(knl)$.

The following result is the key to the proof of Theorem 4.5.

**Theorem 4.8** Let $N = n^{m^2}d^m$, and let $l = nm^2d^{2m^2}$ as in Theorem 4.4. Given $n, m, 0 < c \leq l$, and the specification $\langle V, G \rangle$ of $V$ and $G$ as in eq. (22), one can compute in $\text{poly}(N)$ time the specification of an arithmetic constant depth circuit $C = C[V, m, c]$ over $\mathbb{Q}$ such that (1) $C$ computes the polynomial $R(X^c)(v, x)$ in $x = (x_1, \ldots, x_n)$ and $v = (v_1, \ldots, v_n)$, and (2) for any fixed $h \in V$, the circuit $C_h$ obtained by specializing the variables $v_i$’s in $C$ to the coordinates of $h$ in the standard monomial basis $B(V)$ of $V$ is a diagonal depth three circuit in the class $\Delta_3[n, c, k]$, with $k = \text{poly}(N)$.

More strongly, $C$ can be computed by a uniform AC$^0$ circuit of $\text{poly}(N)$ bit-size with oracle access to DET.

This result says that $V/G$ for constant $m$ is an explicit variety in the following sense.

**Definition 4.9** We say that $V/G = \text{spec}(K[V]^G)$ is explicit if, given $n, m$, and the specification $\langle V, G \rangle$ of $V$ and $G$ as in eq. (22), one can compute in $\text{poly}(n, m)$ time a set of arithmetic circuits $C = C[V, m, c]$’s, $1 \leq c \leq q = \text{poly}(n, m)$, over $\mathbb{Q}$ of $\text{poly}(n, m)$ bit size over the variables $x = (x_1, \ldots, x_n)$ and $v = (v_1, \ldots, v_n)$ such that the polynomials $C[V, m, c](x,v)$’s computed by $C[V, m, c]$’s are of $\text{poly}(n, m)$ degree and can be expressed in the form

$$C[V, m, c](x,v) = \sum_j f_{j,c}(x)g_{j,c}(v),$$

with homogeneous $f_{j,c}$’s and $g_{j,c}$’s, so that $K[V]^G$ is generated by $g_{j,c}(v)$’s and $f_{j,c}(x)$’s are linearly independent.

We say that $V/G$ is explicit in a relaxed sense if the degree requirement on $C[V, m, c](x,v)$’s is dropped. We also say in this case that an explicit FFT holds for the invariant ring $K[V]^G$.

We say that $V/G$ is strongly explicit if the circuits $C[V, m, c]$’s are weakly skew of $\text{poly}(n, m)$ degree. We also say in this case that a strongly explicit FFT holds for the invariant ring $K[V]^G$.

This definition is a special case of a general definition of an explicit variety that we shall formulate later; cf. Definition 5.4.

By Theorem 4.8, $V/G$ is strongly explicit if $m$ is constant. By Lemma 3.3, $V/G$ in Theorem 3.4 is strongly explicit. More generally:

**Conjecture 4.10** The categorical quotient $V/G$ for $V$ and $G$ as in eq. (22) is explicit in a relaxed sense in general without any restriction on $m$. Equivalently, an explicit FFT holds for $K[V]^G$ in general. The categorical quotient is strongly explicit if each $V_{\lambda}(G)$ in (21) is a subrepresentation of the tensor product of a constant number of standard representations, or their duals, of $G$. Equivalently, a strongly explicit FFT holds for $K[V]^G$ in this case.
Before proving Theorem 4.5 let us prove Theorem 4.8 using it.

**Proof of Theorem 4.5 (1) assuming Theorem 4.8**

Let $N$, $k = \text{poly}(N)$, and $l$ be as in Theorem 4.8. Consider the class $\Delta_3[n, l, 2k]$ of diagonal depth three circuits.

By our black-box derandomization assumption for diagonal depth three circuits over $K$, there exists a hitting set $T$ against $\Delta_3[n, l, 2k]$ that can be computed in $\text{poly}(n, k, l) = \text{poly}(N)$ time. Assuming the parallel black-box derandomization hypothesis, $T$ can be computed by a uniform $AC^0$ circuit of $\text{poly}(N)$ bit-size with oracle access to $DET$.

Fix such a $T$. By the definition of the hitting set, for any circuit $D \in \Delta_3[n, l, 2k]$ such that $D(x)$ is not an identically zero polynomial, there exists $b \in T$ such that $D(b) \neq 0$.

For any $b \in T$ and $0 < c \leq l$, define the invariant
$$r_{b,c} := R(X^c)(v, b) \in K[V]^G,$$
and let
$$S = \{r_{b,c} \mid b \in T, 0 < c \leq l\} \subseteq K[V]^G.$$ The elements of $S$ are homogeneous polynomials in $v$ of degree $\leq l$, which is $\text{poly}(n)$ if $m$ is constant.

**Claim 4.11** The set $S$ is separating.

**Proof:** Let $w_1, \ldots, w_n$ be auxiliary variables. For every $c \leq l$, define the symbolic difference
$$\tilde{R}^c(x, v, w) = R(X^c)(v, x) - R(X^c)(w, x),$$
where $R(X^c)(w, x)$ is defined just like $R(X^c)(v, x)$ substituting $w$ for $v$. Suppose $e, f \in V$ are two points such that $r(e) \neq r(f)$ for some $r \in K[V]^G$. It follows that some generator in the set $F$ in eq. (29) assumes different values at $e$ and $f$. From eq. (28), it follows that, for some $c \leq l$, $\tilde{R}^c(x, e, f)$ is not an identically zero polynomial in $x$. By Theorem 4.8, $R(X^c)(e, x)$ is computed by a diagonal depth three circuit in the class $\Delta_3[n, l, k]$. Hence $\tilde{R}^c(x, e, f)$ is computed by a diagonal depth three circuit in the class $\Delta_3[n, l, 2k]$. This means, for some $b \in T$, $\tilde{R}^c(b, e, f) \neq 0$. That is,
$$r_{b,c}(e) = R(X^c)(e, b) \neq R(X^c)(f, b) = r_{b,c}(f).$$
This implies that $S$ is separating. This proves the claim.

It follows from the claim and Theorem 2.12 that $K[V]^G$ is integral over the subring generated by $S$.

For any $b \in T$ and $0 < c \leq l$, let $D_{b,c}$ be the circuit obtained by specializing the circuit $C[V, m, c]$ in Theorem 4.8 at $x = b$. Then $D_{b,c}$ computes $r_{b,c} = R(X^c)(v, b)$ as a polynomial in $v$. We specify $S$ by giving, for every invariant $r_{b,c} \in S$, the specification of $D_{b,c}$. By Theorem 4.13 the circuit $D_{b,c}$ has constant depth and $\text{poly}(N)$ bit-size. Hence, it can also be specified by a weakly skew straight-line program of $\text{poly}(N)$ bit size.

By our black-box derandomization hypothesis, the specification of $T$ can be computed in $\text{poly}(N)$ time. Once $T$ is computed, using Theorem 4.8 we can compute in $\text{poly}(N)$ time, for
each $b \in T$ and $c \leq l$, the specification of the circuit $D_{b,c}$ computing the invariant $r_{b,c} \in S$. Thus the specification of $S$ in the form of a circuit $D_{b,c}$ for each $r_{b,c}$, or the corresponding weakly skew straight-line program, can be computed in $\text{poly}(N)$ time. Hence, $S$ is a separating e.s.o.p.

Assuming the parallel black-box derandomization hypothesis, $T$, and hence $S$, can be computed by a uniform $AC^0$ circuit of $\text{poly}(N)$ bit-size with oracle access to $\text{DET}$.

This completes the proof of theorem 4.5 (1) assuming Theorem 4.8.

**Proof of Theorem 4.5 (2) assuming Theorem 4.8**

By Theorem 2.3, the black-box derandomization hypothesis holds for diagonal depth three circuits allowing a quasi-prefix. Hence, Theorem 4.5 (2) follows from (the proof of) Theorem 4.5 (1) inserting quasi-prefixes in appropriate places.

This completes the proof of Theorem 4.5 assuming Theorem 4.8.

### 4.5 Explicitness of $V/G$ for constant $m$

It remains to prove Theorem 4.8. Towards that end, we first prove some auxiliary lemmas.

First we turn to the computation of the Reynolds operator $R = R_G$, $G = SL_m(K)$. Consider the representation morphism $\psi : V \times G \to V$ given by: $(v, \sigma) \to \sigma^{-1}v$. Let $\psi^* : K[V] \to K[V] \otimes K[G]$ denote the corresponding comorphism. Given $f \in K[V]$, let $\psi^*(f) = \sum_i g_i \otimes h_i$, where $g_i \in K[V]$ and $h_i \in K[G]$.

**Lemma 4.12** (cf. Proposition 4.5.9 in [DK])

\[ R_G(f) = \sum_i g_i R_G(h_i). \]

This reduces the computation of $R_G$ on $K[V]$ to the computation of $R_G$ on $K[G]$. Since $G$, as an affine variety, has just one $G$-orbit, $R_G$ maps $K[G]$ to $K[G]^G = K$. Let $Z$ be an $m \times m$ variable matrix. Computation of $R_G$ on $K[G]$ can be reduced to the computation of $R_G$ on $K[Z]$. This is because $K[G] = K[Z]/J$, where $J$ is the principal ideal generated by $\det(Z) - 1$. If $g \in K[G]$ is represented by $f \in K[Z]$ then $R_G(g) = R_G(f) + J$. Furthermore, $K[Z]^G = K[\det(Z), \det(Z)^{-1}]$.

The computation of $R_G$ on $K[Z]$ can be done using Cayley’s $\Omega$ process as in [HI2]. Here $\Omega$ is a differential operator on $K[Z]$ defined as follows. For any $h(Z) \in K[Z],$

\[ \Omega(h(Z)) = \sum_{\pi \in S_m} \text{sign}(\pi) \frac{\partial^m h}{\partial z_{\pi_1} \partial z_{\pi_2} \cdots \partial z_{\pi_m}}, \]

where $S_m$ is the symmetric group on $m$ letters and $\pi$ ranges over all permutations of $m$ letters.

**Lemma 4.13** (cf. Proposition 4.5.27 in [DK]) Suppose $f \in K[Z]$ is homogeneous. If the degree of $f$ is $m^r$ then, for any nonnegative integer $p$,

\[ R_G\left(\frac{f}{\det(Z)^p}\right) = \det(Z)^{r-p} \frac{\Omega^p f}{c_{r,m}}, \]

33
where \( c_{r,m} = \Omega^r(\det(Z)^r) \in \mathbb{Z} \). If the degree of \( f \) is not divisible by \( m \), then \( R_G(f) = 0 \).

If \( g \in K[G] \) is represented by \( f \in K[Z] \), then \( R_G(g) = \frac{\Omega^r}{c_{r,m}} \), if the degree of \( f \) is \( mr \), and \( R_G(g) = 0 \) if the degree of \( f \) is not divisible by \( m \).

Write \( \det(Z)^r = \sum_{\alpha} a_\alpha z_{1,1}, \ldots, z_{m,m} \), where \( \alpha \) ranges over the monomials in \( z_{i,j}'s \) of degree \( mr \), and \( a_\alpha \in \mathbb{Z} \). Then

\[
\Omega^r = \sum_{\alpha} a_\alpha \left( \frac{\partial}{\partial z_{1,1}}, \ldots, \frac{\partial}{\partial z_{m,m}} \right). 
\]

The number of \( \alpha \)'s here is \( \binom{mr + m^2 - 1}{m^2 - 1} \) = poly(\( \deg(f)^{m^2} \)), when \( \deg(f) = mr \), and the bit-length of each \( a_\alpha \) is poly\( (m,r) = \text{poly}(\deg(f)) \). Hence \( \frac{\Omega^r}{c_{r,m}} \in \mathbb{Q} \), for \( f \in \mathbb{Q}[Z] \) of degree \( mr \), can be computed in poly(\( \deg(f)^{m^2}, \langle f \rangle \)) time, where \( \langle f \rangle \) denotes the total bit-length of the coefficients of \( f \). This can also be done fast in parallel. Thus:

**Corollary 4.14** Given \( g \in \mathbb{Q}[G] \subseteq K[G] \) represented as a polynomial \( f \in \mathbb{Q}[Z, \det(Z)^{-1}] \), \( R_G(g) \in \mathbb{Q} \) can be computed in poly(\( \deg(f)^{m^2}, \langle f \rangle \)) time. More strongly, this can be done by a uniform \( AC^0 \) circuit of poly(\( \deg(f)^{m^2}, \langle f \rangle \)) bit-size.

Now let \( \bar{G} = GL_m(K) \). Then \( V \) as in \eqref{21} is also a polynomial \( \bar{G} \)-representation in a natural way so that, as a \( G \)-module:

\[
V = \oplus_\lambda m(\lambda)V_\lambda(\bar{G}).
\]

Let \( u \in \bar{G} \) be a generic (variable) matrix. Let \( 0 < c \leq l = \text{poly}(n,d^{m^2}) \) and \( N = n^{m^2}d^{m^4} \) be as in Theorem 4.8. For \( X \) as in \eqref{20}, \( u \cdot X \) can be expressed as:

\[
u \cdot X = \sum_i x_i(u \cdot v_i) = \sum_i e_i(x,u)v_i,
\]

where \( e_i \in \mathbb{Q}[x,u] \) is a polynomial in \( x_j's \) and the entries of \( u \) that is linear in \( x_j's \) and has total degree \( \leq d \) in the entries of \( u \), since \( V \) is a representation of \( G \) of degree \( d \). Hence,

\[
u \cdot X^c = (u \cdot X)^c = \sum_\mu \mu \beta_\mu(v,x),
\]

where \( \mu \) ranges over the monomials in the entries of \( u \) of total degree at most \( dc \leq dl = \text{poly}(n,d^{m^2}) \) and \( \beta_\mu(v,x) \) is a polynomial of degree \( c \) in \( v = (v_1, \ldots, v_n) \) as well as \( x = (x_1, \ldots, x_n) \). The number of \( \mu \)'s here is \( \leq \binom{dc + m^2 - 1}{m^2 - 1} = \text{poly}(N) \).

**Lemma 4.15** Given \( n,m,d,c \) as above, \( N = n^{m^2}d^{m^4} \), and the specification \( \langle V, G \rangle \) of \( V \) and \( G \) as in \eqref{22}, one can compute in poly\( (N) \) time, and more strongly, by a uniform \( AC^0 \) circuit of poly\( (N) \) bit-size with oracle access to \( \text{DET} \), the specification of a circuit \( C' \) over \( \mathbb{Q} \) of poly\( (N) \) bit-size on the input variables \( v_1, \ldots, v_n \) and \( x_1, \ldots, x_n \) and with multiple outputs that compute the polynomials \( \beta_\mu(v,x) \)'s in \eqref{23}. The top (output) gates of \( C' \) are all addition gates. Furthermore, for any fixed \( h \in V \), the circuit \( C'_h \) obtained from \( C' \) by specializing the variables \( v_i's \) to the coordinates of \( h \) (in the standard monomial basis of \( V \)) is a diagonal depth three circuit with multiple outputs in the class \( \Delta_3[n,c,e], e = \text{poly}(N) \). By this, we mean that the sub-circuit of \( C' \) below each output gate is in \( \Delta_3[n,c,e] \).
Proof: We cannot compute \( \beta_{\mu}(v, x) \) in eq. (33) by expanding \((u \cdot X)^{c}\) as a polynomial in \( x, u, \) and \( v \), since the number of terms in this expansion is exponential in \( n \). But we can compute it by a constant depth circuit by evaluating \((u \cdot X)^{c}\) at several values of \( u \) and then performing multivariate Van der Monde interpolation in the spirit of [Str1] as follows.

First we show how to construct, for any fixed \( g \in GL_{m}(Q) \), a constant depth circuit \( A_{g} \) that computes the polynomial in \( v \) and \( x \) given by

\[
g \cdot X^{c} = (g \cdot X)^{c} = \left( \sum_{i} e_{i}(x, g) v_{i} \right)^{c},
\]

where \( e_{i}(x, g) \) is a linear form in \( x \) that is obtained by evaluating \( e_{i}(x, u) \) in eq. (32) at \( u = g \). Towards this end, we first construct a depth two circuit \( A'_{g} \) with addition gate at the top that computes the quadratic polynomial in \( v \) and \( x \)

\[
g \cdot X = \sum_{i} e_{i}(x, g) v_{i}
\]

obtained by instantiating (32) at \( u = g \). Recall that \( v_{1}, \ldots, v_{n} \) are the coordinates of \( V \) corresponding to the standard monomial basis \( B(V) \) of \( V \) compatible with the decomposition (31). Hence, using Lemma 4.6 (c), the coefficients of the linear form \( e_{i}(x, g) \), for given \( g \in GL_{m}(Q) \), can be computed in poly\((n, d^{m^2}, \langle g \rangle)\) time, and more strongly, by a uniform \( AC^{0} \) circuit of poly\((n, d^{m^2}, \langle g \rangle)\) bit-size with oracle access to \( DET \). After this, the specification of \( A'_{g} \) can also be computed in poly\((n, d^{m^2}, \langle g \rangle)\) time, and more strongly, by a uniform \( AC^{0} \) circuit of poly\((n, d^{m^2}, \langle g \rangle)\) bit-size with oracle access to \( DET \).

Next we construct \( A_{g} \) with a single multiplication gate of fan-in \( c \) at its top that computes the \( c \)-th power of \( g \cdot X \) computed by the output node of \( A'_{g} \). The polynomial \( A_{g}(v, x) \) computed by \( A_{g} \) is \((g \cdot X^{c})(v, x)\). Furthermore, for any fixed \( h \in V \), the circuit obtained by instantiating \( A_{g} \) at \( v = h \) is a depth two circuit with multiplication (powering) gate at the top.

Next we show how to efficiently construct a circuit \( C' \) for computing the polynomials \( \beta_{\mu} \)'s using \( A_{g} \)'s for several \( g \)'s of poly\((N)\) bit-length.

Let \( e \) be the number of monomials \( \mu \)'s in \( u_{i,j} \) with the degree in each \( u_{i,j} \) at most \( d' = dc \). Then \( e = O((dc)^{m^2}) = poly(N) \), since \( c \leq l = poly(n, d^{m^2}) \). Order these monomials lexicographically. For \( r \leq e \), let \( \mu_{r} \) denote the \( r \)-th monomial in this order. Choose \( m \times m \) non-negative integer matrices \( g_{1}, \ldots, g_{e} \) such that (1) the \( e \times e \) matrix \( B = [\mu_{r}(g_{s})] \), whose \( (s, r) \)-th entry, for \( s, r \leq e \), is \( \mu_{r}(g_{s}) \), is non-singular, and (2) every entry of each \( g_{s} \) is \( \leq d' \). We can choose such \( g_{s} \)'s explicitly so that \( B \) is a multivariate Van der Monde matrix as described in Section 3.9 in [MP]. Specifically, let \( E = [d']^{m^2} \) be the set of \( e \) integral points in \( Z^{m^2} \), where \( [d'] = \{0, \ldots, d'\} \). Order \( E \) lexicographically. Let \( g_{s} \) be the \( s \)-th point in \( E \) interpreted as an \( m \times m \) matrix. Then \( B \) is a non-singular multivariate Van der Monde matrix (cf. Sections 3.9 and 3.11 in [MP]). It can be computed in poly\((N)\) time, and more strongly, by a uniform \( AC^{0} \) circuit of poly\((N)\) bit-size. Its inverse \( B^{-1} \) can be computed by a uniform \( AC^{0} \) circuit of poly\((N)\) bit-size with oracle access to \( DET \).

Let \( \tilde{\beta} \) denote the column-vector of length \( e \) whose \( r \)-th entry, for \( r \leq e \), is \( \beta_{\mu_{r}}(v, x) \). Let \( \tilde{A} \) denote the column vector of length \( e \) whose \( s \)-the entry, for \( s \leq e \), is \( A_{g_{s}}(v, x) = (g_{s} \cdot X^{c})(v, x) \). Then, by (33),

\[
\tilde{A} = B\tilde{\beta} \quad \text{and} \quad \tilde{\beta} = B^{-1}\tilde{A}.
\]
Using the second equation, we can construct a constant depth circuit \( C' \) (with multiple outputs) for computing the entries of \( \beta \) using the constant depth circuits \( A_{g_s} \)'s constructed above. Each output gate of \( C' \) is an addition gate with fan-in \( e = \text{poly}(N) \). Each gate at the second level from the top is the \( c \)-th powering gate, because the top gate of each \( A_{g_s} \) is the \( c \)-th powering gate. For a fixed \( h \in V \), the circuit \( C'_h \) obtained by instantiating \( C' \) at \( v = h \) is thus a diagonal depth three circuit with multiple outputs in the class \( \Delta_3[n,c,e] \).

Since \( A_{g_s} \), for every \( g_s \in E \), and \( B^{-1} \) can be constructed in \( \text{poly}(N) \) time, the construction of \( C' \) takes \( \text{poly}(N) \) time. More strongly, it can be computed by a uniform \( AC^0 \) circuit of \( \text{poly}(N) \) bit-size with oracle access to \( DET \). Q.E.D.

Now we turn to the construction of the circuit \( C = C[V,m,c] \) for computing \( R(X^c) \), as required in Theorem 4.8, given \( n, d, m, c \) and the specification \( \langle V, G \rangle \) of \( V \) and \( G \) as in \(^{22}\).

Let \( u_{ij} \) denote the \((i,j)\)-th entry of the generic \( u \in G \), and \( u_{ij}^{-1} \), the \((i,j)\)-th entry of \( u^{-1} = \text{Adj}(u)/\text{det}(u) \). Substituting \( u^{-1} \) for \( u \) in eq.\(^{33}\), we get

\[
    u^{-1} \cdot X^c = (u^{-1} \cdot X)^c = \sum_{\mu} \mu' \beta_{\mu}(v,x), \tag{36}
\]

where \( \mu \) ranges as in eq.\(^{33}\), and \( \mu' \in \mathbb{Q}[u,\text{det}(u)^{-1}] \) is a polynomial in the entries of \( u \) and \( \text{det}(u)^{-1} \) obtained from \( \mu \) by substituting \( u_{i,j}^{-1} \) for \( u_{i,j} \). The degree of the numerator of \( \mu' \) is again \( \text{poly}(n,dm^2) \).

By Lemma 4.12 and eq.\(^{36}\),

\[
    R(X^c)(v,x) = \sum_{\mu} R_G(\mu') \beta_{\mu}(v,x). \nonumber
\]

Here \( R_G(\mu') \) is a rational number that can be computed in \( \text{poly}(N) \) time using Corollary 4.14 since the degree of \( \mu' \) is \( \text{poly}(n,dm^2) \). Let \( C' \) be the circuit for computing \( \beta_{\mu}' \)'s as in Lemma 4.15. The circuit \( C \) is obtained by adding a single addition gate that performs linear combinations of the various output nodes of \( C' \) computing \( \beta_{\mu}' \)'s, the coefficients in the linear combination being the \( \text{poly}(N) \)-time-computable rational numbers \( R_G(\mu') \). Since the top gates of \( C' \) are addition gates with fan-in \( e \), we can ensure, by merging the addition gates in the top two levels, that the depth of \( C \) is the same as that of \( C' \). The top gate of \( C \) after this merging is an addition gate with fan-in \( k = e^2 = \text{poly}(N) \).

Given \( n, d, m, c \), and \( \langle V, G \rangle \), the specification of \( C' \) can be computed in \( \text{poly}(N) \) time by Lemma 4.15. After this, the specification of the circuit \( C \) as above can also be computed in \( \text{poly}(N) \) time. More strongly, it can be computed by a uniform \( AC^0 \) circuit of \( \text{poly}(N) \) bit-size with oracle access to \( DET \).

For any fixed \( h \in V \), the circuit \( C_h \) obtained by specializing the variables \( v_i \)'s in \( C \) to the coordinates of \( h \) is a diagonal depth three circuit in the class \( \Delta_3[n,c,k] \), with \( k = e^2 = \text{poly}(N) \). This is because, by Lemma 4.15, \( C'_h \) is a diagonal depth three circuit with multiple outputs in the class \( \Delta_3[n,c,e] \), \( e = \text{poly}(N) \).

This completes the proof of Theorem 4.8. Q.E.D.

With this, we have also completed the proof of Theorem 4.5.
The following elementary fact was mentioned in Theorem 4.5, and (a) below has been used implicitly throughout this section.

**Lemma 4.16** Let $V$ be as in (21). Then (a) $\dim(V) = n \geq d$, and (b) $n = \Omega(2^{\Omega(m)})$, if $d = \Omega(m^2)$.

Hence $l$ and $N$ (as in Theorems 4.1 and 4.9) are $O(2^{\text{polylog}(n)})$ if $m = O(\sqrt{d})$.

This can be easily shown using the fact that the dimension of $V_\lambda(G)$ is equal to the number of semi-standard tableau of shape $\lambda$.

### 4.6 General $m$

The following is the full statement of Theorem 1.3 (b).

**Theorem 4.17** Suppose $K$ is an algebraically closed field of characteristic zero. Let $V$ as in (1) be a rational representation of $G = \text{SL}_m(K)$ of dimension $n$. Suppose an explicit FFT holds for $K[V]^G$ (cf. Conjecture 4.10).

(a) Suppose the black-box derandomization hypothesis for PIT over $K$ holds. Then $K[V]^G$ has a separating e.s.o.p. in a relaxed sense (cf. Definition 4.4).

(b) Suppose PIT for circuits over $K$ of size $\leq s$ has $O(2^s \epsilon)$-time-computable hitting set for any small constant $\epsilon > 0$. Then $K[V]^G$ has a separating subexponential-e.s.o.p. in a relaxed sense for any exponent $\delta > 0$.

(c) If a strongly explicit FFT holds for $K[V]^G$ (Definition 4.9), then $K[V]^G$ has a separating e.s.o.p. assuming the black-box derandomization hypothesis for SDIT.

(d) If $V/G$ is explicit (with the degree restriction as in Definition 4.9), then $K[V]^G$ has a separating e.s.o.p. assuming the black-box derandomization hypothesis for small degree PIT.

**Proof:**

(a): Existence of an explicit FFT for $K[V]^G$ is equivalent to explicitness of $V/G$ in a relaxed sense (cf. Definition 4.5). The proof is similar to that of Theorem 4.5 (1), using the assumed explicitness of $V/G$ in place of Theorem 4.8 and the black-box derandomization hypothesis for PIT in place of the black-box derandomization hypothesis for diagonal depth three circuits.

(b): The proof of (a) can be modified in a straightforward manner.

(c) and (d): The proof is similar to that of (a) using SDIT or small degree PIT instead of general PIT. Q.E.D.

We also note down a consequence of the proof of Theorem 4.17.

**Theorem 4.18**

(a) Suppose $V$ and $G$ are as in Theorem 4.17. Suppose also that Conjecture 4.10 holds. Then the problem of deciding if the closures of the $G$-orbits of two rational points in $V$ intersect belongs to co-RP.

(b) Suppose $V$ and $G$ are as in Theorem 4.5 with $m$ constant. Then the problem of deciding if the closures of the $G$-orbits of two rational points in $V$ intersect belongs to P.
Proof:

(a) The proof is similar to that of Theorem 3.6 using Conjecture 4.10 in place of Lemma 3.5.

(b) The proof is similar to that of Theorem 3.6 using Theorem 4.8 in place of Lemma 3.5.

We only need now non-black-box PIT for diagonal depth three circuits, for which there is a deterministic polynomial time algorithm [Sz]. Q.E.D.

4.7 Variant in positive characteristic

In this section we prove a variant of Theorem 4.17 in positive characteristic. Let $K$ be an algebraically closed field of arbitrary characteristic, $V$ a finite dimensional representation of $G = SL_m(K)$ specified by the action of the generators of $G$ on $V$, and $K[V]^G$ the associated invariant ring.

Definition 4.19 We say that an explicit FFT holds for $K[V]^G$ in a geometric sense if there exist circuits $C[V, m, c]'s$, and polynomials $f_{j,c}'s$, and $g_{j,c}'s$ as in Definition 4.9 such that the set $\{g_{j,c}\}$ is a separating set of invariants in $K[V]^G$ (rather than a generating set of invariants as in Definition 4.9).

A strongly explicit FFT for $K[V]^G$ in a geometric sense is defined similarly.

Theorem 4.20 Analogue of Theorems 4.17 also holds in positive characteristic if FFT therein is required to hold only in the geometric sense.

The proof is similar to that of Theorem 4.17 since Theorems 2.10, 2.12, and 4.1 hold in arbitrary characteristic. In view of [AV], we can also use in this result (ignoring the quasi-prefix) the BDH for depth four circuits instead of the BDH for general circuits.

4.8 Generalizations

In this section we briefly state generalizations of the preceding results to any connected reductive algebraic group instead of the special linear group.

Let $K$ be algebraically closed field of characteristic zero. Let $G$ be a connected reductive algebraic group over $K$ of the form $\prod G_i$ where each factor $G_i$ is either a torus, or a classical simple algebraic group. Let $V$ be a rational representation of $G$ of dimension $n$. Let $K[V]^G$ denote the ring of invariants. Since $G$ is reductive, $V$ decomposes as

$$V = \bigoplus_{\lambda} m(\lambda) V_{\lambda}(G),$$

where $\lambda$ ranges over the highest weights of $G$, $V_{\lambda}(G)$ denotes the irreducible Weyl module [Fu] of $G$ labelled by $\lambda$, and $m(\lambda)$ its multiplicity. We assume that $V$ and $G$ are specified succinctly by the tuple

$$\langle V, G \rangle := (n, m; (\lambda^1, m(\lambda^1)); \ldots; (\lambda^s, m(\lambda^s)))$$

that specifies $n$ and $m$ (in unary), and the multiplicity $m(\lambda^i)$ (in unary) of each Weyl module $V_{\lambda^i}(G)$ that occurs in the decomposition (37) with nonzero multiplicity. For each copy of $V_{\lambda}(G)$
that occurs in this decomposition, fix the monomial basis $B_\lambda$ of $V_\lambda(G)$ as defined in [RS]. We refer to it as the RS-basis of $V_\lambda(G)$. (We could also have used the standard monomial basis [LR] here. But this would make the calculations below a bit more involved.) This yields a basis $B(V)$ of $V$, which we call its RS-basis. The elements of $B_\lambda$ are indexed by LS (Lakshmibai-Seshadri)-paths $[^{LR}][^{RS}]$ instead of tableau now. Let $e_i$, $f_i$ and $k_i$'s denote the standard generators of the Lie algebra $\mathfrak{g}$ of $G$. Let $v_\lambda$ denote the highest weight vector of $V_\lambda(G)$. With every LS-path $\eta$ (dominated by the highest weight $\lambda$), the article [RS] associates a monomial $\mu_\eta$ in the generators $f_i$'s such that $\mu_\eta(v_\lambda)$ is the element of $B_\lambda$ indexed by $\eta$.

We can define an e.s.o.p. and the related notions in this general setting very much as in Definition 4.11 using the basis $B(V)$. We can also define explicitness and strong explicitness in this general setting very much as in Definition 4.9. The following is the generalization of Conjecture 4.10 in this setting.

**Conjecture 4.21** The categorical quotient $V/G$ for $V$ and $G$ as above is explicit in a relaxed sense in general. It is strongly explicit if $G$ is a product of classical simple algebraic groups and each $V_\lambda(G)$ in [37] is a subrepresentation of the tensor product of a constant number of standard representations, or their duals, of $G$.

By a standard representation of $G$, we mean the standard representation of any simple factor of $G$.

The following is the generalization of Theorem 4.5 and Theorem 4.17 in this setting.

**Theorem 4.22** (a) Analogue of Theorem 4.5 holds for $V$ and $G$ as above, when $\dim(G)$ is constant, except for the statement concerning parallelization of the construction of a separating e.s.o.p. or quasi-e.s.o.p.

(b) Analogues of Theorems 4.17, 4.18 and 4.20 also hold for $V$ and $G$ as above.

This result also generalizes to any explicit connected reductive algebraic group and its rational representation. By explicit, we mean the defining equations for $G$ and its action are written down explicitly (using straight-line programs).

**Proof:** (Sketch): Since the proof is very similar to that for the special linear group, we only sketch how to handle the differences. We only sketch how to extend the proof of Theorem 4.5 to prove (a), the case (b) being similar. Furthermore, we assume that $G \subseteq SL_m$ (with the standard embedding) is a classical simple algebraic group, the general case being similar.

(a) Let $I \subseteq K[SL_m]$ denote the ideal so that $K[G] = K[SL_m]/I$. Let $U$ be a variable $m \times m$ matrix. Identify $K[SL_m] = K[U]/(\det(U) - 1)$. Order the entries of $U$ row-wise. Fix a Gröbner basis for $I$ with respect to the reverse lexicographic degree ordering on the monomials in the entries of $U$. Since $m$ is constant such a Gröbner basis can be computed in constant time. Let $B'$ be the resulting basis of $K[G]$ consisting of the standard monomials in the variable entries of $U$. Let $K[G]_{\leq d} \subseteq K[G]$ be the subspace spanned by standard monomials of total degree $\leq d$ in the entries of $U$. Both $K[G]$ and $K[G]_{\leq d}$ are $G \times G$-modules, with the first copy of $G$ acting on the left and the second copy on the right. Let $B'_{\leq d} = B' \cap K[G]_{\leq d}$ be the restricted basis of $K[G]_{\leq d}$. We have the Peter-Weyl decomposition $[\text{Fu}]$

$$K[G] = \oplus_\lambda V_\lambda(G)^* \otimes V_\lambda(G), \quad (39)$$
where \( \lambda \) ranges over the highest weights of \( G \). Let

\[
B = \oplus \lambda B^*_\lambda \otimes B_\lambda
\]

be the RS-basis of \( K[G] \), and let \( B_{\leq d} = B \cap K[G]_{\leq d} \) be the restricted basis. The elements of \( B \) are indexed by the pairs \((\zeta^*, \eta)\) of LS-paths dominated by \((\lambda^*, \lambda)\) for some \( \lambda \). Let \( v_{\lambda^*, \lambda} = v^*_\lambda \otimes v_\lambda \) denote the highest weight vector of the \( G \times G \) irreducible module \( V_\lambda(G)^* \otimes V_\lambda(G) \subseteq K[G] \). With any pair \((\zeta^*, \eta)\) of LS-paths dominated by \((\lambda^*, \lambda)\), \([RS]\) associates a unique pair \((\mu_{\zeta^*}, \mu_\eta)\) of monomials in \( f_i \)'s such that the element \( b^{\lambda^*, \lambda}_{\zeta^*, \eta} \) of \( B^*_\lambda \otimes B_\lambda \) indexed by \((\zeta^*, \eta)\) is \((\mu_{\zeta^*}, \mu_\eta)v_{\lambda^*, \lambda} \), with \( \mu_{\zeta^*} \) acting on the left and \( \mu_\eta \) on the right.

The highest weight vectors \( v_{\lambda^*, \lambda} \in B_{\leq d} \) satisfy the equations

\[
(e_i, e_j)v_{\lambda^*, \lambda} = 0, \quad \text{for all } i, j,
\]

where \( e_i \)'s acts on the left and \( e_j \)'s on the right. Solving this system of equations, and classifying the solutions by weights, we get the specifications of all highest weight vectors \( v_{\lambda^*, \lambda} \in B_{\leq d} \) represented in the basis \( B'_{\leq d} \). (Here we are using the fact that, for each \((\lambda^*, \lambda)\), the highest weight vector \( v_{\lambda^*, \lambda} \in B \) is unique, since \( K[G] \) contains only one copy of \( V_\lambda(G)^* \otimes V_\lambda(G) \).)

Since \( V_\lambda(G) \) can be embedded in an appropriate \( K[G]_{\leq d} \) via the Peter-Weyl decomposition \([39]\), we can carry out all calculations on \( V_\lambda(G) \) within \( K[G]_{\leq d} \) using the bases \( B'_{\leq d}, B_{\leq d} \), and the transition matrices \( T_{\leq d} \) and \( T^{-1}_{\leq d} \). After this the analogues of Lemmas 1.6, 1.7 in this general setting are easy to prove (except for the statements concerning parallelization). The analogue of Corollary 1.14 is also easy to prove. We can not use Cayley’s \( \Omega \) process now as it is specific to the special linear group. But the Reynolds’ operator on \( K[G] \) corresponds to the projection onto the trivial \( G \times G \)-module in the Peter-Weyl decomposition \([39]\) of \( K[G] \). So \( R_G(w) \), for any \( w \in B'_{\leq d} \), can be calculated by first expressing \( w \) in the basis \( B_{\leq d} \) using the matrix \( T_{\leq d}^{-1} \), and then projecting it onto the trivial \( G \times G \)-module in the Peter-Weyl decomposition \([39]\) of \( K[G]_{\leq d} \). The rest of the proof is similar to the proof in the case of the special linear group. We omit the details. Q.E.D.

5 General explicit varieties

In this section we prove Theorems 1.1 and 1.2. For simplicity, we work mostly in characteristic zero, since the additional details for positive characteristic are entirely straightforward and are left to the reader.

5.1 Stronger form of black box derandomization of PIT

First, we define the stronger form of black-box derandomization of PIT for small degree circuits.
Let $K$ be an algebraically closed field of characteristic zero and $x = (x_1, \ldots, x_r)$ a set of $r$ variables. The stronger black-box derandomization problem in this context is to construct in poly$(s)$ time a hitting set against all nonzero polynomials $f(x) \in K[x]$ of degree $\leq d = O(s^a)$, $a > 0$ a constant, that can be approximated infinitesimally closely by arithmetic circuits over $K$ and $x$ of size $\leq s$.

By infinitesimally close approximation, we mean that, given any $\epsilon > 0$, there exists such a circuit $C = C_\epsilon$ of size $\leq s$ such that the distance $||C(x) - f(x)||_2$ between the coefficient vectors of $C(x)$ and $f(x)$ in the $L_2$-norm is less than $\epsilon$. The circuit $C$ can depend on $\epsilon$. By a hitting set, we mean a set $S_{r,s} \subseteq \mathbb{N}^r$ (or $\mathbb{Z}^r$) of test inputs such that for every nonzero $f(x)$ of degree $\leq d$ that can be approximated infinitesimally closely by circuits over $K$ of size $\leq s$, $S_{r,s}$ contains a test input $b$ such that $f(b) \neq 0$.

The strong black-box-derandomization hypothesis (strong BDH) for PIT for small degree circuits is that there exists a poly$(s)$-time-computable hitting set $S_{r,s}$. The strong black-box derandomization hypothesis for general PIT without any degree restriction is defined similarly. Parallel versions of these hypotheses are defined as in Section 2.1. A similar strong black-box derandomization hypothesis for SDIT (symbolic determinant identity testing), cf. Section 2.1 is that, given $m$, one can construct in poly$(m)$ time a hitting set against all nonzero homogeneous polynomials over $K$ of degree $m$ that can be approximated infinitesimally closely by symbolic determinants of size $m$. The strong black-box derandomization hypothesis for the symbolic permanent identity testing (SPIT) is similar, using the permanent in place of the determinant.

The strong BDH over algebraically closed fields of positive characteristic is defined similarly using the Zariski topology instead of the complex topology.

The strong black-box derandomization hypothesis above is counter-intuitive unlike the standard hypothesis in Section 2.1. As per a conjecture in [MS1] (cf. Section 4.2 therein), there exist integral polynomials of small degree that can be approximated infinitesimally closely by small arithmetic circuits but cannot be computed exactly by such circuits. Hence a priori there is no reason why there should exist easy-to-compute hitting sets against such hard-to-compute functions.

The following strengthening of Theorem 2.2 says that one can still compute efficiently in quasi-polynomial time a hitting set against such functions assuming a sub-exponential lower bound for infinitesimally close approximation of an exponential-time-computable multilinear integral function. A good candidate for such a multilinear polynomial is the permanent. It cannot be approximated infinitesimally closely by small arithmetic circuits as per the stronger form of the permanent vs. determinant conjecture in [MS1] (cf. Conjecture 4.3 and Proposition 4.4) therein. The result below is the main reason why the strong black-box derandomization hypothesis is expected to hold. This result is also the key to efficient derandomization of NNL for arbitrary explicit varieties (cf. Theorems 1.1 and 1.2) assuming lower bounds for infinitesimally close approximation.

**Theorem 5.1** Suppose $K$ is an algebraically closed field of characteristic zero.

(a) Suppose there exists an exponential-time-computable multilinear polynomial $p$ in $m$ variables with integral coefficients such that $p$ can not be approximated infinitesimally closely by arithmetic circuits over $K$ of $O(2^m)$ size for some $\epsilon > 0$, $m \to \infty$. Then PIT for small degree
circuits with size $\leq s$ and $n \leq s$ variables has $O(2^{\text{polylog}(s)})$-time-computable strong black-box derandomization.

(b) Suppose there exists an exponential-time-computable multilinear polynomial $p$ in $m$ variables with integral coefficients such that $p$ cannot be approximated infinitesimally closely by arithmetic circuits over $K$ of $O(m^s)$ size for any constant $a > 0$. Then PIT for small degree circuits with size $\leq s$ and $n \leq s$ variables has $O(2^s)$-time-computable strong black-box derandomization, for any constant $\epsilon > 0$.

(c) Analogues of (a) and (b) also hold allowing arithmetic circuits in the lower bound assumptions oracle gates for the permanent, using SPIT in place of PIT, and requiring the coefficients of $p$ to be nonnegative.

(d) If $K$ is an algebraically closed field of positive characteristic $q$, then an analogue of (a) holds assuming a stronger lower bound, namely, that $p^{\ell}$, $0 \leq \ell \leq m^\delta / \log q$, for some $\delta > 0$, can not be approximated infinitesimally closely by arithmetic circuits over $K$ of $O(2^m)$ size for some $\epsilon > 0$, $m \to \infty$. In particular, if $q > 2^{m^\delta}$, for some $\delta > 0$, then the analogue of (a) holds assuming that $p$ can not be approximated infinitesimally closely by arithmetic circuits over $K$ of $O(2^m)$ size for some $\epsilon > 0$, $m \to \infty$. The coefficients of $p$ are assumed to be in an extension of $F_q$. Similar analogue of (b) also holds with $l = O(\log m / \log q)$.

In Theorem 2.2 we required that the coefficients of $p$ have poly$(n)$ bit-length only to ensure that the bit-length of each input in the hitting set is polynomial even if the cardinality of the hitting set is quasi-polynomial or sub-exponential. This restriction is no longer be enforced in this section. This means the bit-length of an input in the hitting set constructed in (a) or (b) can be quasi-polynomial or sub-exponential, respectively.

The coefficients of $p$ are required to be nonnegative in (c) only to ensure (as would be required later in this case) that the hitting set is a subset of $\mathbb{N}^r$ (instead of $\mathbb{Z}^r$).

If the polynomial $p$ in (a) is polynomial-space-computable, then the proof below shows that PIT for small degree circuits with size $\leq s$ has parallel strong black-box derandomization that works in polylog$(s)$ time using $2^{\text{polylog}(s)}$ processors.

**Proof:** We extend the proof of Theorem 7.7 in [KI]. We only prove (a), the cases (b)-(d) being similar.

(a): To construct a hitting set as needed, let $m = (\log s)^e$, for a large enough constant $e$ to be fixed later. Construct an NW-design $[\mathbf{NW}]$ with this choice of $m$. By this we mean a family of sets $R_1, \ldots, R_n \subseteq [l]$, $l \leq m^2 = (\log s)^{2e}$, each of cardinality $m$, such that $|R_i \cap R_j| \leq \log n$ for all $i \neq j$. By $[\mathbf{NW}]$ (cf. Lemma 2.23 in [KI]) such a set system can be constructed in poly$(n, 2^l) = O(2^{\text{polylog}(s)})$ time.

This set system and the hard function $p(x_1, \ldots, x_m)$ together yield an arithmetic NW-generator NW$^p$. By this we mean the function

$\text{NW}^p : x = (x_1, \ldots, x_l) \in \mathbb{N}^l \rightarrow (p(x|_{R_1}), \ldots, p(x|_{R_n})) \in \mathbb{Z}^n$, \hspace{1cm} (40)

where $x_R$ denotes the tuple of the elements in $x$ indexed by $R$.

**Claim 5.2** The set $H = \{\text{NW}^p(a) \mid a \in [D]^l\}$, $D = dm + 1$, is a hitting set against every
nonzero polynomial $f(y)$, $y = (y_1, \ldots, y_n)$, of degree $\leq d = O(s^t)$, $t > 0$ a constant, that can be approximated infinitesimally closely by arithmetic circuits over $K$ of size $\leq s$.

Since $p$ is exponential-time-computable, $H$ is $O(2^{\text{polylog}(s)})$-time computable. So it remains to prove the claim.

Suppose to the contrary that $f(b) = 0$, for every $b \in H$, for some nonzero polynomial $f(y)$ of degree $\leq d$ that can be approximated infinitesimally closely by arithmetic circuits over $K$ of size $\leq s$.

Let $g_0(x_1, \ldots, x_l, y_1, \ldots, y_n) := f(y_1, \ldots, y_n)$. For $1 \leq i \leq n$, let $g_i(x_1, \ldots, x_l, y_{i+1}, \ldots, y_n)$ be the polynomial obtained from $f$ by replacing $y_1, \ldots, y_i$ by the polynomials $p(x|R_i)$, $1 \leq j \leq i$. Then $g_0 = f(NW^p(x))$ and the degree of each $g_i$ is $\leq dm < D$. Since $f(b) = 0$ for all $b \in H$, $g_n(a) = 0$ for all $a \in [D]^l$. Since $\deg(g_n) < D$, by the Schwarz-Zippel lemma $[Sc]$, $g_n$ is identically zero. But $g_0 = f$ is not identically zero. So there exists a smallest $0 \leq i < n$ such that $g_i$ is not identically zero but $g_{i+1}$ is identically zero. Fix this $i$. Since $g_i$ is not identically zero, we can set $y_{i+2}, \ldots, y_n$ and $x_j, j \not\in R_{i+1}$ to some integer values so that the restricted polynomial $\tilde{g}_i(x_1, \ldots, x_{j-1}, y_{i+1})$ remains a non-zero polynomial, where $R_i = \{x_{j+1}, \ldots, x_{j'}\}$. Let us denote this polynomial by renaming the variables as $g(x_1, \ldots, x_m)$.

Then $g(x_1, \ldots, x_m) = 0$ is a non-zero polynomial with degree $\leq dm$, but $g(x_1, \ldots, x_m, p(x_1, \ldots, x_m))$ is identically zero. By Guass’s Lemma, $h(x_1, \ldots, x_m, y) = p(x_1, \ldots, x_m) - y$ is a factor of $g(x_1, \ldots, x_m, y)$. By Theorem 2.3, $h(x_1, \ldots, x_m, y)$ has a circuit over $K$ of $\text{poly}(m, \deg(g)) = \text{poly}(s)$ size with oracles gates for $g$. Setting $y = 0$ in this circuit, we get a circuit for $p(x_1, \ldots, x_m)$ of $\text{poly}(s)$ size with oracle gates for $g$.

But $g$ has a circuit of size $O(n^2 \log n)$ with one oracle gate for $f$. This is because $|R_j \cap R_{i+1}|$, $j \leq i$, is at most log $n$ by the property of the NW-design. Hence, after the specialization of the variables $y_{i+2}, \ldots, y_n$ and $x_j, j \not\in R_{i+1}$, as above, each $p(x|R_j)$, $j \leq i$, gets restricted to a multilinear polynomial in at most log $n$ variables. This restricted polynomial can be computed brute-force by a circuit $C_j$ of size at most $O(\log n 2^{\log n}) = O(n \log n)$ size. We get a circuit for $g$ as desired by connecting the inputs $y_1, \ldots, y_i$ of the oracle for $f$ to the outputs of $C_1, \ldots, C_i$, respectively, and specializing the variables $y_{i+2}, \ldots, y_n$ to their integer values chosen above.

It follows that $p(x_1, \ldots, x_m)$ can be computed by an arithmetic circuit $C$ over $K$ of size $O(s^c)$ with oracle gates for $f$ for some constant $c > 0$ independent of $e$. Given any circuit $D_\delta$ of size $\leq s$ for approximating $f$ within precision $\delta > 0$, let $C_\delta$ denote the circuit obtained from $C$ by substituting $D_\delta$ for $f$. Since $f$ can be approximated infinitesimally closely by circuits of size $\leq s$, by choosing $\delta$ small enough, $C_\delta$ can approximate $p(x_1, \ldots, x_m)$ to any precision. The size of $C_\delta$ is $O(s^{c+1})$. Choosing $\epsilon$ large enough, the size of $C_\delta$ can be made $\leq 2^{\epsilon n}$ for any $\epsilon > 0$. This contradicts hardness of infinitesimally close approximation of $p$. Q.E.D.

The following result is the (easy) converse of Theorem 5.1(a) (ignoring the quasi-prefix).

**Proposition 5.3** Suppose $K$ is a field of characteristic zero.

Suppose PIT for small degree circuits has $O(\text{poly}(s))$-time-computable strong black-box derandomization. Then there exists an exponential-time-computable multilinear polynomial $p$ in $m$ variables such that $p$ cannot be approximated infinitesimally closely by arithmetic circuits over $K$ of $O(2^{m/a})$ size for some constant $a > 0$.  

43
Analogous converse of Theorem 5.1 (b) also holds.

Proof: The proof is similar that of Theorem 51 in [Ag].

Choose $s = 2^{n/a}$, where $a > 0$ is a large enough constant to be chosen later. Suppose there exists an $O(s^b)$-time-computable hitting set $T$ of size $s^b$ against all nonzero multilinear polynomials in $m$ variables that can be approximated infinitesimally closely by arithmetic circuits over $K$ of size $s$

Let $p(x)$, $x = (x_1, \ldots, x_m)$, be a multilinear polynomial such that

$$p(t) = 0, \quad \forall t \in T.$$  \hspace{1cm} (41)

Each condition here is a linear constraint on $2^m$ coefficients of $p(x)$. The number these constraints is $|T| \leq s^b = 2^{mb/a} < 2^m$ if $a > b$. Hence there is a non-zero $p(x)$ satisfying these constraints. One such $p(x)$ can be computed in $2^{O(m)}$ time by solving the linear system \hspace{1cm} (41).

By (41), this exponential-time computable $p(x)$ cannot be approximated infinitesimally closely by arithmetic circuits over $K$ of size $s$ since $T$ is a hitting set. Q.E.D.

By Theorem 5.1 and Proposition 5.3 strong black-box derandomization and sub-exponential lower bounds for infinitesimally close approximation of exponential-time-computable multilinear integral polynomials are essentially equivalent notions.

5.2 Explicit algebraic varieties

Next we define an explicit algebraic variety in general, motivated by the concrete examples of explicit varieties studied in Sections 3 and 4; cf. Example 1 in Section 5.2.1 below.

Definition 5.4 Let $K$ be an algebraically closed field of characteristic zero.

(a) A family $\{W_n\}$, $n \rightarrow \infty$, of affine varieties is called explicit if there exist a map $\psi_n : K^r \rightarrow K^m$:

$$v = (v_1, \ldots, v_r) \rightarrow (f_1(v), \ldots, f_m(v)), \quad \hspace{1cm} (42)$$

$r = poly(n), m = n^{o(1)}, \log m = O(poly(n))$, each $f_j$ a homogeneous polynomial of $poly(n)$ degree, and homogeneous polynomials $g_j(x)$, $x = (x_1, \ldots, x_n)$, $1 \leq j \leq m$, of $poly(n)$ degree such that:

1. $W_n$ is the Zariski-closure of the image $\text{Im}(\psi_n)$ of $\psi_n$. This means $W_n \cong \text{spec}(R)$, where $R$ is the subring of $K[v_1, \ldots, v_r]$ generated by $f_1(v), \ldots, f_m(v)$.

2. The polynomial $F_n(v,x) = \sum_j f_j(v)g_j(x)$ is uniformly $p$-computable \hspace{1cm} (V2). By uniform, we mean that one can compute in $poly(n)$ time a $poly(n)$-size circuit $C_n$ over $\mathbb{Q}$ that computes $F_n(v,x)$. Its degree $\text{deg}(F_n)$ is $poly(n)$.

3. The polynomials $g_j(x)$’s are linearly independent.

We call $\psi_n$ the map defining $W_n$, and $F_n$ the polynomial defining $W_n$. We specify $W_n$ succinctly by the circuit $C_n$. (Alternatively, we can specify $W_n$ by the circuits $C_{n,c}$’s, $1 \leq c \leq \text{deg}(F_n)$, where $C_{n,c}$ computes the degree $c$-component in $v$ of $F_n$.)
We say that \{W_n\} is strongly explicit if the circuit \(C_n\) is weakly skew.

(b) We say that \{W_n\} is weakly explicit, if \(F_n(v, x)\) above is equal to the permanent of a matrix \(D_n\) of \(\text{poly}(n)\) dimension such that (1) each entry of \(D_n\) is a homogeneous bilinear form in \(v\) and \(x\) over \(\mathbb{Q}\), and (2) the description of \(D_n\) is \(\text{poly}(n)\)-time-computable.

We say that \{W_n\} is positive if the coefficients of all bilinear functions that occur as the entries of \(D_n\) are non-negative.

(c) A family of projective varieties is called explicit (strongly explicit, weakly explicit, or positive) if the family of the affine cones of these varieties is explicit (respectively, strongly explicit, weakly explicit, or positive).

(d) A family explicit affine or projective varieties in a relaxed sense (without any degree restriction) is defined just as in (a) and (c) but without putting any restriction on the degrees of \(f_j, g_j\) and \(F_n\).

The definition of an explicit or weakly explicit variety over an algebraically closed field \(K\) of arbitrary characteristic is similar.

5.2.1 Examples of explicit varieties

(1) Explicit categorical quotients and related varieties: The variety \(V/G\), with \(V\) and \(G\) as in Theorem 3.4 is a strongly explicit variety with the defining map \(\psi = \pi_{V/G}\) as in [9]; cf. Lemma 3.5. Explicitness of \(V/G\) is a key ingredient in the proof of Theorem 3.4. The variety \(V/G\) for \(V\) and \(G\) as in Theorem 3.11 is also strongly explicit.

By Theorem 4.8, the variety \(V/G\), with \(V\) and \(G\) as in Theorem 4.5, is strongly explicit for constant \(m\). Explicitness of \(V/G\) is a key ingredient in the proof of Theorem 4.5. The variety \(V/G\) is explicit in a relaxed sense for any \(m\) as per Conjecture 4.10.

(2) Similarly, the Grassmanian (and \(G/P\) in general) is an explicit variety with the defining map \(\psi\) being the well-known Plücker map [Fu], as the reader can easily check.

(3) The orbit-closure associated with the determinant in [MS1] (in the context of the permanent vs. determinant problem) is explicit. The orbit-closure associated with the permanent in [MS1] (in the same context) is weakly explicit and positive. These varieties, which we shall denote by \(\Delta[\det, m]\) and \(\Delta[\perm, n, m]\), are defined as follows.

Let \(X\) be an \(m \times m\) variable matrix. Let \(Y\) be an \(n \times n\) submatrix of \(X\), say its lower-right \(n \times n\) subminor. Let \(z\) be any entry of \(X\) outside \(Y\). Let \(\mathcal{X}\) be the vector space over \(\mathbb{C}\) of homogeneous polynomials of degree \(m\) in the variable entries of \(X\). Thus \(g = \det(X)\) is an element of \(\mathcal{X}\). Then \(\mathcal{X}\) is a representation of \(GL_{m^2}(\mathbb{C})\), where \(\sigma \in GL_{m^2}(\mathbb{C})\) maps \(h(X) \in \mathcal{X}\) to \(h(\sigma^{-1} X)\), thinking of \(X\) as an \(m^2\)-vector. Let \(P(\mathcal{X})\) be the projective space associated with \(\mathcal{X}\). Then \(\Delta[\det, m] \subseteq P(\mathcal{X})\) is the closure of the orbit \(Gg \subseteq P(\mathcal{X})\). The variety \(\Delta[\perm, n, m] \subseteq P(\mathcal{X})\) is defined similarly using the homogeneous polynomial \(z^{m-n} \perm(Y) \in \mathcal{X}\) in place of the determinant.

The affine cone of \(\Delta[\det, m]\) is explicit with the defining map \(\psi : M_{m^2}(K) \to \mathcal{X}\) that maps \(v \in M_{m^2}(K)\) to \(\det(vX)\), thinking of \(X\) as an \(m^2\)-vector. The polynomial \(F\) defining \(\Delta[\det, m]\) in the terminology of Definition 5.4 is \(\det(vX)\). The monomials in the entries of \(v\) of degree \(m\) play the role of \(f_j\)'s and the monomials in the entries of \(x\) of degree \(m\) play the role of \(g_j\)'s.
in Definition 5.4. The dimension $t$ of the ambient space containing $\Delta[\det, m]$ is the number of monomials in the entries of $x$ of degree $m$. The $m$ here is different from the $m$ in Definition 5.4, which equals $t$ here.

The affine cone of $\Delta[\text{perm}, n, m]$ is weakly explicit and positive.

(4) Explicit variety associated with a $p$-computable polynomial:

Let $\{p_n(v, x)\}$, $v = (v_1, \ldots, v_r)$, $x = (x_1, \ldots, x_n)$, be a uniform $p$-computable family of polynomials over $K$ homogeneous in $v$. Let $p_n(v, x) = \sum \mu f_{\mu}(v)\mu(x)$, where $\mu$ ranges over all monomials in $x$ of degree $\leq \deg(p_n) = \text{poly}(n)$. Let $m$ be the number of such monomials. Let $\psi = \psi_n$ be the map

$$
\psi : v \in K^r \rightarrow (\ldots, f_{\mu}(v), \ldots) \in K^m.
$$

Let $g_{\mu}(x) = \mu(x)$. Then $W_n = \overline{\text{Im}(\psi_n)}$ is an explicit variety with the defining map $\psi_n$ and the defining polynomial $p_n$.

(5) Explicit toric variety associated with a $p$-computable polynomial:

Let $\{p_n(x)\}$, $x = (x_1, \ldots, x_n)$, be a uniform $p$-computable homogeneous polynomial over $x$ and $K$. Let $p_n(x) = \sum a_\mu \mu(x)$, where $a_\mu \in K$ and $\mu$ ranges over all monomials in $x$ of total degree $= \deg(p_n) = \text{poly}(n)$. Let $m$ be the number of such monomials. Consider the monomial map $\psi_n$:

$$
\psi_n : v = (v_1, \ldots, v_n) \in K^n \rightarrow (\ldots, a_\mu \mu(v), \ldots) \in K^m.
$$

Let $W_n = \overline{\text{Im}(\psi_n)}$, and $P(W_n)$ its projectivization. Then $P(W_n)$ is an explicit toric variety, with the defining polynomial

$$
F_n(v, x) = \sum_{\mu} a_\mu \mu(v)\mu(x),
$$

which is $p$-computable and uniform.

(6) The toric variety in characteristic zero associated with the Birkhoff polytope (cf. Section 6.2 in [DS]) is weakly explicit and positive.

(7) We call an explicit $W$ with $\dim(W) = 1$ an explicit curve. We define explicit surfaces, explicit three-folds, and so on, similarly.

### 5.3 Implication of strong black-box derandomization for explicit varieties

We now describe an implication of strong black-box derandomization for explicit varieties.

**Definition 5.5** Let $W = W_n$ be an explicit variety as in Definition 5.4, $z_1, \ldots, z_m$ the coordinates of $K^m$, and $\psi^*$ the comorphism of $\psi$ in (42). Note that $K[W]$ is graded, with $\text{deg}(z_j) = \text{deg}(f_j)$.

(a) We say that $s \in K[W]$ has a short specification if $\psi^*(s)$ has a straight-line program over $\mathbb{Q}$ and $v_1, \ldots, v_r$ of $O(\poly(n))$ bit-length that computes the polynomial function on $K^r$ corresponding to $\psi^*(s)$.

(b) We say that a set $S \subseteq K[W]$ is an explicit system of parameters (e.s.o.p.) for $K[W]$ if (1) each element $s \in S$ has a short specification as in (a) and is homogeneous of $\text{poly}(n)$ degree,
(2) $K[W]$ is integral over its subring generated by $S$, (3) the size of $S$ is $\text{poly}(n)$, and (4) the specification of $S$, consisting of a straight-line program for $\psi^*(s)$ for each $s \in S$ as in (a), can be computed in $\text{poly}(n)$ time.

An s.s.o.p. is defined by dropping the condition (4).

(c) We say that Noether's normalization lemma for $W$ (or its coordinate ring $K[W]$) is derandomized if $K[W]$ has an e.s.o.p.

(d) S.s.o.p., e.s.o.p., and derandomization in a relaxed sense (without degree restriction) are defined similarly by dropping the degree requirement in (b) (1). Quasi-e.s.o.p. and quasi-s.s.o.p. are defined by replacing polynomials by quasi-polynomials.

The following is a full statement of Theorem 1.1 (3) and (4).

Theorem 5.6 Let $K$ be an algebraically closed field of characteristic zero.

(a) The coordinate ring $K[W]$ of an explicit variety $W$ has (1) an e.s.o.p. if PIT for small degree circuits over $K$ has strong black box derandomization, and (2) a quasi-e.s.o.p. if there exists an exponential-time-computable multilinear function in $n$ variables with integral coefficients that cannot be approximated infinitesimally closely by arithmetic circuits over $K$ of size $O(2^n^\epsilon)$ for some $\epsilon > 0$. (Analogous statement also holds in a relaxed sense without any degree restriction on the explicit variety and PIT.)

(b) The coordinate ring of the explicit variety $\Delta[\det, m]$ (cf. Example 3 in Section 5.2.1) has (1) an e.s.o.p. if SDIT has strong black box derandomization, and (2) a quasi-e.s.o.p. if there exists an exponential-time-computable multilinear function in $n$ variables with integral coefficients that cannot be approximated infinitesimally closely by arithmetic circuits over $K$ of size $O(2^n^\epsilon)$ for some $\epsilon > 0$. The straight-line programs specifying an e.s.o.p. in (1) can also be assumed to be weakly skew.

(c) The e.s.o.p. constructed in (a) or (b) can also be assumed to be separating (as defined below).

(d) Analogue of (a) also holds if $K$ is an algebraically closed field of positive characteristic $p$, assuming the same lower bound as in (a) (2) if $p > 2^n^\delta$, for some $\delta > 0$, $n \rightarrow \infty$ (the coefficients of the multilinear polynomial are assumed to be in some extension of $F_p$). Otherwise, the lower bound assumption in (a) (2) is replaced by a stronger assumption, namely, that there exists an exponential-time-computable multilinear function $f$ in $n$ variables (with coefficients in some extension of $F_p$) such that $f^p^i$, $0 \leq i \leq n^\delta/\log p$, for some $\delta > 0$, can not be approximated infinitesimally closely by arithmetic circuits over $K$ of size $O(2^n^\epsilon)$ for some $\epsilon > 0$, $n \rightarrow \infty$. Similar analogues of (b) and (c) also hold in positive characteristic.

Here we say that $S$ is separating if for any two distinct points $u, v \in W$ there exists an $s \in S$ such that $s(u) \neq s(v)$. We say that Noether's Normalization Lemma for $K[W]$ is derandomized in a strong form if $K[W]$ has a separating e.s.o.p.

If the polynomial in (a) (2) is polynomial-space-computable, then the problem of constructing a quasi-s.s.o.p. for $K[W]$ belongs to quasi-DET.

Before we prove the result above, let us state its main corollary.
Theorem 5.7 Suppose $K$ is an algebraically closed field of characteristic zero. Suppose the permanent function of $n \times n$ matrices over $K$ cannot be approximated infinitesimally closely by arithmetic circuits over $K$ of size $O(2^{n^\epsilon})$ for some $\epsilon > 0$. Then the coordinate ring of any explicit variety has a quasi-e.s.o.p. In particular, the coordinate ring of $\Delta[\det, m]$ has a quasi-e.s.o.p.

The same result also holds if $K$ is an algebraically closed field of positive characteristic $p > 2n^\delta$, for some $\delta > 0$. Otherwise, an analogous result holds for $p$ different than 2 assuming that $p^i$-th power of the permanent, $0 \leq i \leq n^\delta / \log p$, for some $\delta > 0$, cannot be approximated infinitesimally closely by arithmetic circuits over $K$ of size $O(2^{n^\epsilon})$ for some $\epsilon > 0$, $n \to \infty$.

The proof of this result shows that the problem of constructing a quasi-s.s.o.p. for $\Delta[\det, m]$ or any explicit variety under the stated assumption belongs to quasi-$DET$.

The lower bound assumption in characteristic zero here in the terminology of [MS1] is that $\Delta[\perm, n, m] \nsubseteq \Delta[\det, m]$, if $m = O(2^{n^\epsilon})$ for some small enough $\epsilon > 0$, where the variety $\Delta[\perm, n, m]$ is as in Example (3) in Section 5.2. This is a stronger form of Conjecture 4.3 in [MS1]. If we assume instead (as in Conjecture 4.3 in [MS1]) that $\Delta[\perm, n, m] \nsubseteq \Delta[\det, m]$, and $m = O(poly(n))$, then it can be proved similarly that the coordinate ring of $\Delta[\det, m]$ has a subexponential e.s.o.p. (defined by replacing polynomials with subexponentials).

Proof of Theorem 5.6

We will only prove (a) and (b), (c) being a simple extension of (a) and (b), and (d) being a simple extension of (a)-(c). By Theorem 5.1(a), the statements (a) (2) and (b) (2) here can be reduced to (a) (1) and (b) (1), respectively, ignoring the quasi-prefix which can be taken into account easily. Hence it suffices to prove (a) (1) and (b) (1).

(a) (1): Let $W = W_n$ be an explicit variety as in Definition 5.3 and $C_n$ the circuit computing $F_n$ as there. Let $s = poly(n)$ be its size, and $d = poly(n)$ its degree.

By the strong black-box derandomization hypothesis, there exists a poly($s$)-time computable hitting set $T$ against all nonzero polynomials $h(x) = h(x_1, \ldots, x_n)$ of degree $\leq d$ that can be approximated infinitesimally closely by arithmetic circuits over $K$ of size $\leq s$.

For each $b \in T$ and $0 < c \leq \deg(F_n)$, define $h_{b,c}(z) := \sum_j z_j g_j(b) \in K[W]$, where $j$ ranges over all indices such that $\deg(f_j) = c$, and $z = (z_1, \ldots, z_m)$ denote the coordinates of $K^m$. Then $\deg(h_{b,c}) = c$. Let

$$S = \{ h_{b,c}(z) \mid b \in T, 0 < c \leq \deg(F_n) \} \subseteq K[W].$$

By Lemma 5.8 below, $S$ is an e.s.o.p.; cf. Definition 5.5

(b) (1): Use Lemma 5.9 instead of Lemma 5.8 Q.E.D.

Lemma 5.8 Suppose $W$ is an explicit variety and PIT for small degree circuits has strong black box derandomization. Let $S$ and $T$ be as in (43). Then:

(a) $W \cap Z(S) = \{0\}$, where $Z(S) \subseteq K^m$ is the zero set of $S$, and 0 denotes the origin in $K^m$.

(b) The coordinate ring $K[W]$ is integral over the subring generated by $S$.

(c) The set $S$ is an e.s.o.p.

Proof: Let $\psi = \psi_n$, $f_j$, $g_j$, and $F = F_n(v, x)$ be as in Definition 5.4.
(a) By Hilbert’s Nullstellansatz, we can assume that \( K = \mathbb{C} \), since \( F_n \), and hence \( W \), and \( Z(S) \) are defined over \( \mathbb{Q} \). Consider any nonzero point \( w = (w_1, \ldots, w_m) \in W \subseteq K^m \). We have to show that \( h_{b,c}(w) \neq 0 \) for some \( b \in T \) and \( 0 < c \leq \deg(F_n) \). Let \( F_w(x) = \sum_j w_j g_j(x) \). Recall that \( K[W] \) is graded, with \( \deg(z_j) = \deg(f_j) \). Let \( F_w(x)_c = \sum_j w_j g_j(x) \), where \( j \) ranges over all indices such that \( \deg(f_j) = c \). Then \( F_w(b)_c = h_{b,c}(w) \). So we have to show that \( F_w(b)_c \neq 0 \) for some \( b \in T \) and \( 0 < c \leq \deg(F_n) \).

Since \( W = \text{Im}(\psi) \), and the closure in the Zariski topology coincides with the closure in the complex topology (cf. Theorem 2.33 in [Mm]), there exists, for any \( \delta > 0 \), an \( h_{\delta} \in K^r \) such that \( ||\psi(h_{\delta}) - w||_2 \leq \delta/(mA) \), where \( A = \max\{ ||g_j||_2 \} \). Taking \( \delta \) to be small enough, we can assume that \( \psi(h_{\delta}) \neq 0 \). Since \( \psi(h_{\delta}) = (f_1(h_{\delta}), \ldots, f_m(h_{\delta})) \) and \( W \) is explicit, it follows from Definition 5.3 (a) (3) that \( F_n(h_{\delta}, x) = \sum_j f_j(h_{\delta})g_j(x) \) is not an identically zero polynomial in \( x \). Let \( C_n \) be the circuit computing \( F_n(v, x) \) as in Definition 5.3. Let \( C_{n,\delta} \) be the circuit obtained from \( C_n \) by specializing \( v \) to \( h_{\delta} \). Then the size of \( C_{n,\delta} \) is \( s = \text{size}(C_n) = \text{poly}(n) \) and the degree is \( d = \deg(C_n) = \text{poly}(n) \). Furthermore,

\[
||C_{n,\delta}(x) - F_w(x)||_2 = ||\sum_j (f_j(h_{\delta}) - w_j)g_j(x)||_2 \leq mA||\psi(h_{\delta}) - w||_2 \leq \delta.
\]

Since \( \delta \) can be made arbitrarily small, it follows that \( F_w(x) \) can be approximated infinitesimally closely by circuits of degree \( \leq d \) and size \( \leq s \). Since \( T \) is a hitting set, there exists \( b \in T \) such that \( F_w(b) \neq 0 \). Hence \( F_w(b)_c \neq 0 \) for some \( c \leq \deg(F_n) \). This proves (a).

(b) By (a) and Hilbert’s Nullstellansatz, it follows that, given any \( t \in K[W] \), \( t^l \) belongs to the ideal \( (S) \) in \( K[W] \) generated by \( S \) for some large enough positive integer \( l \). Since \( K[W] \) is graded, it now follows from the graded Noether’s normalization lemma (Lemma 2.11) that \( K[W] \) is integral over its subring generated by \( S \). This proves (b).

(c) We have to verify the properties (1)-(4) in Definition 5.5 (b).

1. We have to show that each \( h_{b,c}(z) \in S \) has a short specification. We have \( \psi^*(h_{b,c})(v) = F_n(v, b)_c \). Since \( W \) is explicit, cf. Definition 5.3, we can compute the description of the circuit \( C_n \) over \( \mathbb{Q} \) computing \( F_n \) in \( \text{poly}(n) \) time. Hence the total size of \( C_n \), including the bit-lengths of the constants in it, is \( \text{poly}(n) \). Using Van der Monde interpolation as in [Str1] (cf. also the proof of Lemma 4.15 where this technique was used), we can construct using \( C_n \) in \( \text{poly}(n) \) time a circuit \( C_{n,c} \), for every \( 0 \leq c \leq \deg(F_n) \), that computes the degree \( c \)-component (in \( v \)) of \( F_n \). The circuit \( C_{n,c,b} \) for computing for computing \( \psi^*(h_{b,c})(v) = F_n(v, b)_c \) is obtained by instantiating the circuit \( C_{n,c} \) at \( x = b \). Its total size (including the bit-lengths of the constants) is \( \text{poly}(n) \) and its degree is \( \text{poly}(n) \). This specification of \( C_{n,c,b} \) can be converted into a straight-line program of \( \text{poly}(n) \) bit-length. This shows that each \( h_{b,c}(z) \) (or rather \( \psi^*(h_{b,c}) \)) has a short specification.

2. It follows from (b) that \( K[W] \) is integral over the subring generated by \( S \).

3. Since the size of \( T \) is \( \text{poly}(s) = \text{poly}(n) \), and \( \deg(F_n) \) is \( \text{poly}(n) \), the size of \( S \) is clearly \( \text{poly}(n) \).

4. We saw above that the specification of each circuit \( C_{n,c,b} \) computing \( \psi^*(h_{b,c}) \) can be computed in \( \text{poly}(n) \) time. Hence it follows that the specification of \( S \), consisting of a circuit \( C_{n,c,b} \) computing \( \psi^*(h_{b,c}) \) for each \( h_{b,c} \in S \), can be computed in \( \text{poly}(n) \) time.

This shows that \( S \) is an e.s.o.p. Q.E.D.
Lemma 5.9 Suppose $\Delta[\det, m]$ is the explicit variety as in Example 3 in Section 5.2.1. Assume that SDIT has strong black box derandomization.

Then the set $S$ in (43) is an e.s.o.p. for the coordinate ring of $\Delta[\det, m]$. The straight-line programs of the elements in $S$ can also be assumed to be weakly skew.

Proof: The proof is just like that of Lemma 5.8. We only observe that in the case of $\Delta[\det, m]$ the defining polynomial $F_n(v, x)$ in Definition 5.4 is the determinant of a matrix $M_n$ of poly(n) size whose each entry is a bilinear function in $v$ and $x$; cf. Example 3 in Section 5.2.1. Furthermore, the specification of $M_n$ can be computed in poly(n) time. Hence we can use det($M_n$) in place of $C_n$ in the proof of Lemma 5.8. Then we can use SDIT in place of PIT for small degree circuits. The straight-line programs of the elements in $S$ can be assumed to be weakly skew since the determinant has a weakly skew straight-line program \[\text{MP}.\] Q.E.D.

Theorem 5.10 The e.s.o.p.’s in Theorems 5.6 and 5.7 can also be assumed to be strict in the following sense.

Let $W = W_n$ be an explicit variety defined by the polynomial $F_n$ and the circuit $C_n$ computing it (Definition 5.4). Let $f_j$ and $g_j$ be as in Definition 5.3. For any $0 \leq c \leq \deg(F_n)$, let $C_{n,c}$ be the circuit computing the degree $c$-component (in $v$) of $F_n$. It can be computed using $C_n$ in poly(n) time as in the proof of Lemma 5.8 (c). Alternatively, the explicit variety $W_n$ may be specified by giving the circuits $C_{n,c}$, $1 \leq c \leq \deg(F_n)$, instead of one circuit $C_n$. For any $b \in \mathbb{N}^n$ of poly(n) bit-length, let $C_{n,c,b}$ be the instantiation of $C_{n,c}$ at $x = b$.

We say that $s \in K[W]$ is strict if, for some $b \in \mathbb{N}^n$ of poly(n) bit-length, and $0 < c \leq \deg(F_n)$, $\psi^{-1}(s)(v) = C_{n,c,b}(v)$. This means $s = \sum_j z_j g_j(b)$ where $j$ ranges over all indices such that $\deg(f_j) = c$. Such a strict $s$ can be specified succinctly by the triple $(b, c, C_n)$ or the pair $(b, C_{n,c})$. Thus a strict e.s.o.p. has a short specification (cf. Definition 5.5 (a)) based on the circuit $C_n$ defining the variety $W_n$ itself. As such strictness is a natural form of shortness based on the succinct specification of the explicit variety. Strictness of the e.s.o.p.’s constructed in the proofs of Theorems 5.6 and 5.7 follows from the definition of $S$ as in (43). The e.s.o.p.’s constructed in the proofs of Theorems 1.4 (a) and 1.3 (b) are also strict. We say that Noether’s Normalization Lemma for the coordinate ring of $W_n$ has strict derandomization if it has a strict e.s.o.p. As we shall see below (Theorem 5.12), a strict s.s.o.p. always exists. By strict NNL, we mean the problem constructing a strict s.s.o.p. deterministically.

Theorem 5.10 has the following analogue for a weakly explicit but positive variety (Definition 5.4).

Given a weakly explicit but positive variety $W_n$, we say that $S$ is a strict, positive, weak e.s.o.p. for $K[W_n]$ if (1) $K[W]$ is integral over its subring generated by $S$, (2) the size of $S$ is poly(n), (3) for each $s \in S$, $\psi^{-1}(s) = \text{perm}(D_n(v, b))$, for some $b \in \mathbb{N}^n$ of poly(n) bit-length, where $D_n$ is the symbolic matrix as in Definition 5.4 (b), and (4) the specification of $S$ consisting of a symbolic permanent as in (3) for each $s \in S$ can be computed in polynomial time. Using the polynomial-time algorithm for computing a perfect matching and [JSV], given any $s \in S$ as in (3) and any rational non-negative $v$, whether $\psi^{-1}(s)(v)$ is nonzero can be decided in polynomial time and an approximate value of $\psi^{-1}(s)(v)$ can be computed efficiently by an FPRAS.
Theorem 5.11 Let $K$ be an algebraically closed field of characteristic zero. The coordinate ring $K[W]$ of a weakly explicit but positive variety $W$ has a separating, strict, positive, weak e.s.o.p. if SPIT has strong black box derandomization.

The proof is similar to that of Theorem 5.10 using SPIT instead of SDIT.

The following is a full statement of Theorem 1.1 (1) and (2).

Theorem 5.12 Let $K$ be an algebraically closed field of characteristic zero. Let $W = W_n$ be an explicit variety.

(a) A strict s.s.o.p. exists for $K[W_n]$.
(b) The problem of constructing an h.s.o.p. or verifying a strict s.s.o.p. for $K[W_n]$ belongs to EXPSPACE. This means it can be solved in $2^{\text{poly}(n)}$ space.
(c) The problem of constructing a strict s.s.o.p. for $K[W_n]$ belongs to EXPSPACE.
(d) Suppose $W_n$ has explicit defining (or close-to-defining) equations as in Definition 5.13 below, and also that GRH holds. Then the problems in (b) and (c) belong to $\text{REXP}^{\text{NP}}$.
(e) The statements (a)-(c) also hold if $K$ is an algebraically closed field of positive characteristic.

Analogous statement also holds for an explicit variety in a relaxed sense without any degree restriction.

Definition 5.13 We say that an explicit family $\{W_n\}$ of varieties has explicit defining equations if there exists a set $Q$ of polynomial functions over $K^m$ such that (1) $Q$ generates the ideal of $W_n \subseteq K^m$, (2) each element in $Q$ has a straight-line program over $Q$ and the coordinates $z_1, \ldots, z_m$ of $K^m$ of $O(2^{\text{poly}(n)})$ bit-length, and (3) the specification of $Q$ consisting of straight-line programs for its elements can be computed in $O(2^{\text{poly}(n)})$ time and poly($n$) work-space.

We say that $\{W_n\}$ has explicit close-to-defining equations if (1) is replaced by the weaker (1)': the zero set $W'$ of the polynomials in $Q$ is a variety containing $W$ of poly($n$) dimension.

The size of the straight-line programs in (1) is clearly $\Omega(m)$. This size is exponential in $n$ if $m$ is exponential in $n$, as would be the case in the intended applications. Hence the poly($n$) work-space restriction in (2) is an essentially optimal uniformity condition.

The hidden difficulty of constructible sets

By Theorem 4.17 and the unconditional PSPACE-algorithm for black-box derandomization of PIT (cf. the remark after Theorem 5.14), the problem of constructing an s.s.o.p. for $K[V]^G$ is in PSPACE unconditionally if $V/G$ is explicit. This proof does not extend to arbitrary explicit varieties. This is because the image of the map $\psi_n$ in (12) is a constructible set $\text{Mm}$ that need not be closed in general. In contrast, the image of the map $\pi_{V/G}$ in (23) is always closed (Theorem 2.10(a)). This fact is implicitly used in the proof of Theorem 2.12, a crucial ingredient in the proof of Theorem 4.17. The main reason for the high complexity of NNL for arbitrary explicit varieties at present (as in Theorem 5.12(c)) is ultimately that the image of $\psi_n$ is only constructible and not necessarily closed.
Proof of Theorem 5.12

(a) Analogue of Theorem 2.1 also holds for strong black-box derandomization. Specifically, the hitting set $B$ in Theorem 2.1 is also a hitting set against all non-zero polynomials that can be approximated infinitesimally closely by arithmetic circuits over $K$ and $r$ variables of size $≤ s$ and degree $≤ d$; cf. Theorem 4.4 in [HS] and its proof. We now use the hitting set $B$ given by Theorem 2.1 (with appropriate parameters) in place of the hitting set $T$ used in the proof of Theorem 5.6 (a) (1). Since the new hitting set $B$ cannot be computed efficiently, what we get now is an s.s.o.p. instead of an e.s.o.p.

(b): The proof for the construction of an h.s.o.p. is similar to that of Proposition 4.2. Specifically, we first compute defining equations for $W_n$ using Gröbner basis theory (specifically, Theorem 1 in [MR2]). Next we construct an h.s.o.p. using these defining equations and Lemma 2.14. All this can be done in exponential space. The space is exponential because the dimension of the ambient space $K^t$ containing $W_n$ is exponential in general. Verification of a strict s.s.o.p. can also be done in exponential space using the defining equations and a test for Hilbert’s Nullstellansatz as in the proof of Lemma 2.14.

(c) Enumerate all potential s.s.o.p.’s as in the proof of (a) corresponding to the exponentially many potential hitting sets $B$’s in Theorem 2.1 and test for each such $B$ if the resulting potential s.s.o.p. is indeed an s.s.o.p. using (b). By the proof of (a), the test is bound to succeed for some $B$.

(d) For the sake of simplicity, we assume that $W$ has explicit defining equations; otherwise replace $W$ by $W'$ in Definition 5.13. Furthermore, we only consider the problem of constructing an h.s.o.p., the other cases being similar. The proof for this is similar to that of Theorem 3.1 using the assumed explicit defining equations for $W$ in place of the equations of $V/G$ used therein.

(e) Modifications to the proof in characteristic zero are straightforward. Q.E.D.

The proof of Theorem 5.12 (c) also yields:

**Theorem 5.14** The problem of strong black-box derandomization of PIT belongs to EXPSPACE unconditionally in any characteristic.

In contrast, the problem of black-box derandomization of PIT belongs to PSPACE unconditionally (and to $PH$ assuming GRH), as can be shown easily using Theorem 2.1 and the PSPACE algorithm (resp. the PH algorithm assuming GRH) [Ko, Ko1] for Hilbert’s Nullstellansatz.

Yet, the black-box derandomization hypothesis may be essentially as hard to prove as the strong black-box derandomization hypothesis. This is because the set $W_{s,r}$ of polynomials computed by arithmetic circuits over $K$ of size $≤ s$ on $r$ variables is not a variety but rather a constructible set [Mm]. The set of polynomials that can be approximated infinitesimally closely by circuits of size $≤ s$ on $r$ variables is the variety $\overline{W}_{s,r}$ obtained by taking its closure. Black-box derandomization is a statement about the constructible set $W_{s,r}$, whereas strong black-box derandomization is a statement about the variety $\overline{W}_{s,r}$. The constructible set $W_{s,r}$ is so badly behaved in general (when there are no unnatural restrictions on circuits) that we may essentially be forced to prove the second stronger statement for its closure $W_{s,r}$. 

52
This is supported by the history of lower bounds for unrestricted arithmetic circuits.\footnote{In contrast, there are lower bounds and derandomization results for restricted classes of arithmetic circuits such as the depth three arithmetic circuits with constant top-fan-in whose proofs cannot be extended at present to infinitesimally close approximations.} For example, the basic idea in the proof of the quadratic determinantal lower bound for the permanent also yields the same lower bound for its infinitesimally close approximation. The quadratic lower bound for the determinant and the permanent in arithmetic depth-three circuits and other results based on the method of partial derivatives (e.g. \cite{SV}) also hold for infinitesimally close approximations. The current best lower bound for matrix multiplication\footnote{\cite{L3}} also goes via a lower bound for its border rank.

For this reason, the EXPSpace vs. $P$ gap for the strong BDH for PIT over an algebraically closed field may be viewed as a magnified form of the PSpace vs. $P$ gap for the standard BDH for PIT over an algebraically closed field. The hidden difficulty of dealing with constructible sets is quantified during this magnification.

By the result below (Theorem 5.15) this EXPSpace vs. $P$ gap in the complexity of the strong BDH is formally equivalent to the EXPSpace vs. $P$ gap in the complexity of (strict) NNL for explicit varieties.

### 5.4 Equivalence

The following is a precise statement of Theorem 1.2.

**Theorem 5.15** Let $K$ be an algebraically closed field of characteristic zero.

(a) (1) The strong black box derandomization of symbolic determinant identity testing (SDIT) over $K$ is equivalent to strict derandomization of Noether’s Normalization Lemma for $\Delta[\text{det}, m]$.

(2) A subexponential lower bound for an exponential-time-computable integral multilinear polynomial as in Theorem 7.1 (a) is also equivalent, ignoring quasi-prefixes, to strict derandomization of Noether’s normalization lemma for $\Delta[\text{det}, m]$.

(b) The strong black-box derandomization for SPIT is equivalent to strict derandomization of Noether’s normalization lemma for $\Delta[\text{perm}, m, m]$ (cf. Example 3 in Section 5.2.1).

(c) The strong black-box derandomization of general PIT over $K$ (without degree restrictions) is equivalent to strict derandomization of Noether’s normalization lemma for the orbit closure of the $P$-complete function $H(Y)$ defined in Section 6 of \cite{MST} (and denoted as $\Delta[H(Y)]$ there).

(d) The similarly defined strong black-box derandomization of PIT for depth three circuits over $K$ and $n$ variables with degree $\leq d$ and top fan-in $\leq k$ is equivalent to strict derandomization of Noether’s Normalization Lemma for the $k$-th secant variety $X(d,k,n)$ of the Chow variety defined below.

(e) The statements (a)-(d) also hold in positive characteristic replacing the lower bound assumption in (a) (2) by the one in Theorem 5.6 (d).

Let $S^d_n$ be the space of degree $d$ homogeneous forms in $n$ variables, and $P(S^d_n)$ the associated projective space. The variety $X(d,k,n) \subseteq P(S^d_n)$ here is, by definition \cite{L1}, the projective
closure of the set of polynomials that can be expressed as sum of \( k \) terms, each term a product of \( d \) linear forms.

The implication from a lower bound to NNL in (a) (2), already proved in Theorem 5.6 (a) (2), is the nontrivial direction of this result. The converse implication from strict NNL to strong black-box derandomization or lower bounds, proved below, is easy.

**Proof:** We only prove (a), the proof of (b)-(e) being similar. Since (a) (2) can be reduced to (a) (1) using Theorem 5.1 (a) and Proposition 5.3, we only prove (a) (1).

Strong black-box derandomization of SDIT implies strict derandomization of Noether’s normalization lemma for \( \Delta[\text{det}, m] \) by Theorem 5.10.

Conversely, suppose Noether’s normalization lemma for \( \Delta[\text{det}, m] \subseteq P(\mathcal{X}) \) has strict e.s.o.p. \( S \). Let \( I[\text{det}, m] \) be the ideal of \( \Delta[\text{det}, m] \) so that \( R[\text{det}, m] = K[\mathcal{X}]/I[\text{det}, m] \).

Let \( z_\alpha \)'s, where \( \alpha \) ranges over the monomials in the entries of \( \mathcal{X} \) of degree \( m \), be the coordinates of \( \mathcal{X} \). Thus each homogeneous form \( h(\mathcal{X}) \) of degree \( m \) can be written as \( \sum_\alpha z_\alpha(h(\mathcal{X})) \), where \( z_\alpha \in K \) denote the coordinates of \( h \in \Delta[\text{det}, m] \) considered as a point in \( P(\mathcal{X}) \).

Since \( S \) is strict, each element of \( S \) is of the form

\[
s_b := \sum_\alpha z_\alpha(h(b)),
\]

for some \( m \times m \) matrix \( b \in \mathbb{Z}^{m^2} \) of poly(n) bit-length, and the specification of \( S \) specifies each such \( b \). Let \( B = \{ b \mid s_b \in S \} \). Its bit-size is clearly poly(n). It is poly(n)-time computable since the specification of \( S \) as above is.

So we only have to prove that \( B \) is a hitting set against symbolic determinants of size \( m \).

Since \( S \) is an e.s.o.p., \( R[\text{det}, m] \) is integral over the subring generated by \( S \). Hence each \( z_\alpha \) satisfies a monic polynomial equation of the form:

\[
z_\alpha^k + a_{k-1}z_\alpha^{k-1} + \cdots + a_0 = 0, \ mod \ I[\text{det}, m],
\]

where each \( a_j \) is a non-constant homogeneous polynomial in the elements of \( S \). It follows that every element in \( S \) cannot vanish at any given (nonzero) \( h = h(\mathcal{X}) \in \Delta[\text{det}, m] \). Otherwise, every \( z_\alpha \) would vanish at \( h \), and hence, \( h \) would be identically zero.

Now suppose a nonzero polynomial \( h = h(\mathcal{X}) \) of degree \( m \) can be approximated infinitesimally closely by expressions of the form \( \det(X') \), where \( X' \) is an \( m \times m \) matrix whose each entry is a homogeneous linear form in the entries of \( \mathcal{X} \) with coefficients in \( K \). By the definition of \( \Delta[\text{det}, m] \) (cf. Example 3 in Section 5.2.1), it follows that \( h(\mathcal{X}) \) considered as a point in \( P(\mathcal{X}) \) lies in \( \Delta[\text{det}, m] \). Since \( h(\mathcal{X}) \) is not identically zero, it follows from the above argument that some \( s_b \in S \) does not vanish on \( h \); i.e., \( h(b) \neq 0 \). This means \( B \) is a hitting set against every nonzero polynomial \( h(\mathcal{X}) \) that can be approximately infinitesimally closely by symbolic determinants of size \( m \). In other words, SDIT has strong black-box derandomization. Q.E.D.
5.5 On derandomization of PIT

Finally, we formulate a few conjectures that may be helpful in derandomization of PIT.

Let \( W \subseteq K^m \) be an explicit variety as in Definition 5.4. Theorems 5.6 and 5.10 lead to:

**Conjecture 5.16**

(a) The coordinate ring \( K[W] \) of any explicit variety \( W \) has a strict separating e.s.o.p.

(b) The coordinate ring \( K[W] \) of a weakly explicit positive variety \( W \) has a strict separating positive weak e.s.o.p.

When \( W = \Delta[\text{det}, m] \), (a) implies black-box derandomization of SDIT (Theorem 5.15). The story for black-box derandomization of PIT (without degree restrictions) is similar, letting \( W \) be the variety associated with the \( P \)-complete function \( H(X) \) in [MS1] instead of \( \Delta[\text{det}, m] \).

**Conjecture 5.17**

(a) Any explicit variety has explicit close-to-defining equations (cf. Definition 5.13).

(b) The explicit varieties in Theorem 5.15 have explicit defining equations.

This in conjunction with GRH would put NNL for the explicit variety under consideration in the exponential hierarchy (cf. Theorem 5.12 (d)).

Since putting NNL for arbitrary explicit varieties in the exponential hierarchy unconditionally appears very difficult at present, it will be interesting studying the easier explicit varieties first (in the spirit of Theorems 1.3 (a) and 1.4 (b)) such as the general categorical quotients \( V/G \) (cf. Conjecture 4.10), explicit varieties associated with tame quivers [Br], explicit toric varieties [Stm1], explicit curves and surfaces.

**Acknowledgement:** The author is grateful to Michael Forbes and Amir Shpilka for bringing [SV] and [ASS] to his attention and for pointing out [FS3] an error in the preliminary version [Mu4] of this paper (cf. the remark after Theorem 1.4), and to Jonah Blasiak, Josh Grochow, Jimmy Qiao, and Joseph Landsberg for helpful comments.

**References**

[Ag] M. Agrawal, Proving lower bounds via pseudo-random generators, Proceedings of the FSTTCS, pages 92-105, 2005.

[ASS] M. Agrawal, C. Saha, N. Saxena, Quasi-polynomial hitting-set for set-depth-delta formulas, arXiv:1209.2333 [cs.CC], September, 2012.

[AV] M. Agrawal, V. Vinay, Arithmetic circuits: a chasm at depth four, FOCS 2008, pp. 67-75.

[AB] S. Arora, B. Barak, Computational complexity: a modern approach, Cambridge University Press, 2009.
V. Arvind, P. Joglekar, S. Srinivasan, Arithmetic circuits and Hadamard product of polynomials, in FSTTCS, pages 25-36, 2009.

J. Boutot, Singularités rationelles et quotients par les groupes reductifs, Invent. Math. 88, (1987), 65-68.

M. Brion, Representations of quivers, Preprint, Institute Fourier.

W. Bruns, J. Herzog, Cohen-Macaulay rings, Cambridge University Press, 1993.

L. Bruyn, C. Procesi, Semisimple representations of quivers, Transactions of the American Mathematical Society, vol. 317, no. 2, 1990, pp. 585-598.

P. Bürgisser, J. Landsberg, L. Manivel, J. Weyman, A overview of mathematical issues arising in the geometric complexity theory approach to $VP \neq VNP$, SIAM J. Comput., vol. 40, no. 4, 2011, pp. 1179-1209.

J. Cai, X. Chen, D. Li, Quadratic lower bound for permanent vs. determinant in any characteristic, comput. complex. 19 (2010), 37-56.

J. Canny, Some algebraic and geometric computations in PSPACE, in Proceedings of STOC 1988, 460-467.

S. Cook, A taxonomy of problems with fast parallel algorithms, Journal of Information and Control, vol. 64, issues 1-3, 1985.

L. Csanky, Fast parallel matrix inversion algorithms, SIAM J. Comput. 5 (1976) 618-623.

H. Derksen, Polynomial bounds for rings of invariants, Proc. Amer. Math. Soc. 129 (2001), 955-963.

H. Derksen and G. Kemper, Computational invariant theory, Encyclopaedia of mathematical sciences, Springer, 2000.

P. Diaconis and B. Sturmfels, Algebraic algorithms for sampling from conditional distributions, Annals of Statistics, 1998, vol. 26, no. 1, 363-397.

P. Doubilet, G. Rota, J. Stein, On the foundations of combinatorial theory, IX. Combinatorial methods in invariant theory, Studies in Appl. Math. 53. 1974. 185-216.

J. Drozd, Tame and wild matrix problems, Amer. Math. Soc. Transl. (2) 128 (1986), 31-55.

D. Eisenbud, Commutative algebra with a view toward algebraic geometry, Springer-Verlag, New York 1995.

H. Flenner, Rationale quasi-homogene singularitäten, Arch. Math. 36 (1981), 35-44.
[FS2] M. Forbes, A. Shpilka, Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs, ECCC, 19:115, 2012.

[FS3] M. Forbes, A. Shpilka, Explicit Noether normalization for simultaneous conjugation via polynomial identity testing, arXiv:1303.0084v2 [cs.CC], 2013.

[Fo] E. Formanek, Generating the ring of matrix invariants, in “Ring-theory-proceedings, Antwerp, 1985,” F. Van Oystaeyen, Editor, Lecture Notes in Math. No. 1195, Springer-Verlag, pp. 73-82, 1986.

[Fu] W. Fulton, J. Harris, Representation theory, A first course, Springer, 1991.

[Go] P. Gordon, Das Zerfallen der Curven in gerade Linien, Math. Ann. (1894), no. 45, 410-427.

[GKKS] A. Gupta, P. Kamath, N. Kayal, R. Saptharishi, Arithmetic circuits: a chasm at depth three, ECCC, Report No. 26, 2013.

[HS] J. Heintz, C. Schnorr, Testing polynomials that are easy to compute, Proceedings of the STOC, 1980, 262-272.

[Hl2] D. Hilbert, Über die vollen Invariantensysteme, Math. Ann. 42, 1893, 313-370.

[IM] O. Ibarra, S. Moran, Probabilistic algorithms for deciding equivalence of straight-line programs, JACM, 30 (1), 217-228, 1983.

[IW] R. Impagliazzo, A. Wigderson, $P = BPP$ unless $E$ has sub-exponential circuits: Derandomizing the XOR lemma, Proceedings of the 29th STOC, 1997.

[JSV] M. Jerrum, A. Sinclair, E. Vigoda, JACM, vol. 51, no. 4, July 2004, pp. 671-694.

[KI] V. Kabanets, R. Impagliazzo, Derandomizing polynomial identity tests means proving circuit lower bounds, Computational Complexity, 13(1-2), pages 1-46, 2004.

[KI1] E. Kaltofen, Factorization of polynomials given by straight-line programs, Randomness and Computation, vol. 5, Advances in Computing Research series, JAI press Inc., pp. 375-412, 1989.

[KI2] E. Kaltofen, G. Lecerf, Factorization of multivariate polynomials, in Handbook of Finite Fields, editors, G. Mullen and D. Panario, Discrete Mathematics and Its Applications, CRC press, 2013.

[KT] E. Kaltofen, B. Trager, Computing with polynomials given by black boxes for their evaluations: greatest common divisors, factorization, separation of numerators and denominators, J. Symbolic Comput., 9(3):301-320, 1990.

[KS2] N. Kayal, N. Saxena, Polynomial identity testing for depth 3 circuits, Computational Complexity 16 (2007), no. 2, 115-138.
[Ko1] P. Koiran, Hilbert’s Nullstellansatz is in the polynomial hierarchy, Journal of complexity 12, 273-286 (1996).

[Ko] J. Kollár, Sharp effective Nullstellansatz, J. Amer. Math. Soc. 1, 963-975.

[LR] V. Lakshmibai, K. Raghavan, Standard monomial theory, Encyclopaedia of mathematical sciences, Springer 2008.

[L1] J. Landsberg, Tensors: geometry and applications, graduate studies in mathematics, vol. 128, AMS, 2012.

[L2] J. Landsberg, Equations for secant varieties of Veronese and other varieties, arXiv:1111.4567v1 [math.AG], Nov. 2011.

[LR] J. Landsberg, N. Ressayre, Hypersurfaces with degenerate duals and the geometric complexity theory program, arXiv:1004.4802v1, April, 2010.

[L3] J. Landsberg, New lower bounds for the rank of matrix multiplication, arXiv:1206.1530v1 [cs.CC], June 2012.

[MP] G. Malod, N. Portier, Characterizing Valiant’s algebraic complexity classes, Journal of Complexity, 2007.

[MR1] E. Mayr, S. Ritscher, Degree bounds for Gröbner bases of lower dimensional polynomial ideals, Proceedings of ISSAC, 2010, pp. 21-27.

[MR2] E. Mayr, S. Ritscher, Space efficient Gröbner basis computation without degree bounds, Proceedings of ISAAC, 2011, pp. 257-264.

[MR] T. Mignon, N. Ressayre, A quadratic bound for the determinant and permanent problem, International Mathematics Research Notices (2004) 2004: 4241-4253.

[MP] B. Mourrain and V. Pan, Multivariate polynomials, duality, and structured matrices, Journal of complexity 16, 110-180 (2000).

[Mu2] K. Mulmuley, The GCT program toward the P vs. NP problem, CACM, vol. 55, no. 6, 98-107.

[Mu3] K. Mulmuley, On P vs. NP and Geometric complexity theory, JACM, vol. 58, no. 2, 2011.

[Mu4] K. Mulmuley, Geometric complexity theory V: equivalence between blackbox derandomization of polynomial identity testing and derandomization of Noether’s Normalization Lemma, abstract, FOCS 2012.

[Mu5] K. Mulmuley, Geometric complexity theory VI: The flip via positivity, technical report, computer science department, the university of Chicago, July 2010. Available at: http://ramakrishnadas.cs.uchicago.edu Revised version under preparation.
K. Mulmuley, M. Sohoni, Geometric complexity theory I: an approach to the P vs. NP and related problems, SIAM J. Comput., vol 31, no 2, pp 496-526, 2001.

K. Mulmuley, M. Sohoni, Geometric complexity theory II: towards explicit obstructions for embeddings among class varieties, SIAM J. Comput., vol. 38, no. 3, 2008, pp. 1175–1206.

D. Mumford, Algebraic geometry I: complex projective varieties, Springer, 1976.

D. Mumford, J. Fogarty, F. Kirwan: Geometric invariant theory. Springer-Verlag, 1994.

N. Nisan, A. Wigderson, Hardness vs. randomness, J. Comput. Sys. Sci., 49 (2): 149-167, 1994.

C. Pappacena, An upper bound on the length of a finite dimensional algebra, J. algebra 197 (1997), 535-545.

V. Popov, The constructive theory of invariants, Math. USSR Izvest. 10 (1982), 359-376.

V. Popov, E. Vinberg, Invariant theory, in Encyclopaedia of mathematical sciences, vol. 55, Springer-Verlag, 1989.

C. Procesi, The invariant theory of $n \times n$ matrices, Adv. in Math. 19 (1976), 306-381.

K. Raghavan, P. Sankaran, A new approach to standard monomial theory for classical groups, Transformation Groups, vol. 3, no. 1, 1998, pp. 57-73.

Y. Razmyslov, Trace identities of full matrix algebras over a field of characteristic zero, Comm. in Alg. 8 (1980), Math. USSR Izv. 8 (1974), 727-760.

N. Saxena, Diagonal circuit identity testing and lower bounds, Dagstuhl Seminar Proceedings 07411, 2007.

J. Schwarz, Fast probabilistic algorithms for verification of polynomial identities, JACM 27: 701-717.

A. Shpilka, private communication.

A. Shpilka, Ilya Volkovich, Read-once polynomial identity testing, Proceedings APPROX-RANDOM, 2009, 700-713.

A. Shpilka, A. Wigderson, Depth-3 arithmetic circuits over fields of characteristic zero, proceedings of the 14th Computational Complexity, pp. 87-96, 1999.

V. Strassen, Die berechnungskomplexität von elementarsymmetrischen funktionen und von interpolationskoefizienten. Numerische Mathematik, 20:238-251, 1973.
[Stm1] B. Sturmfels, Gröbner bases of toric varieties, Tôhoku Math. J. 43 (1991), 249-261.

[Stm2] B. Sturmfels, Algorithms in invariant theory, Springer-Verlag, 1993.

[V2] L. Valiant, Completeness classes in algebra, STOC, 1979.

[Wy] H. Weyl, The classical groups. Their invariants and representations, Princeton University Press, Princeton, N.J. 1939.