2012 IEEE 53rd Annual Symposium on Foundations of Computer Science

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

(Abstract)

Dedicated to Sri Ramakrishna

Ketan D. Mulmuley
Computer Science Department
The University of Chicago
Chicago, U.S.A.
mulmuley@cs.uchicago.edu

***Abstract*—It is shown that black-box derandomization of polynomial identity testing (PIT) is essentially equivalent to derandomization of Noether's Normalization Lemma for explicit algebraic varieties, the problem that lies at the heart of the foundational classification problem of algebraic geometry. Specifically:**

(1) It is shown that in characteristic zero black-box derandomization of the symbolic trace identity testing (STIT) brings the problem of derandomizing Noether's Normalization Lemma for the ring of invariants of the adjoint action of the general linear group on a tuple of matrices from EXPSPACE (where it is currently) to P. Next it is shown that assuming the Generalized Riemann Hypothesis (GRH), instead of the black-box derandomization hypothesis, brings the problem from EXPSPACE to quasi-PH, instead of P. Thus black-box derandomization of STIT takes us farther than GRH. Variants of the main implication are also shown assuming, instead of the black-box derandomization hypothesis in characteristic zero, Boolean lower bounds for constant-depth threshold circuits or uniform Boolean conjectures, in conjunction with GRH. These results may explain in a unified way why proving lower bounds or derandomization results for arithmetic circuits in characteristic zero or constant-depth Boolean threshold circuits, or proving uniform Boolean conjectures without relativizable proofs has turned out to be so hard, and also why GRH has turned out to be so hard from the complexity-theoretic perspective. Thus this investigation reveals that the foundational problems of Geometry (classification and GRH) and Complexity Theory (lower bounds and derandomization) share a common root difficulty that lies at the junction of these two fields. We refer to it as the GCT chasm.

(2) It is shown that black-box derandomization of PIT in a strengthened form implies derandomization of Noether's Normalization Lemma in a strict form for any explicit algebraic variety.

(3) Conversely, it is shown that derandomization of Noether's Normalization Lemma in a strict form for specific explicit varieties implies this strengthened form of blackbox derandomization of PIT and its various variants.

(4) A unified geometric complexity theory (GCT) approach to derandomization and classification is formulated on the basis of this equivalence.

(5) It is illustrated by showing that Noether's Normalization Lemma for the ring of invariants of any explicit linear action of a classical algebraic group can be quasi-derandomized (unconditionally) if the dimension of the group is constant.

I. Introduction

Noether's Normalization Lemma, proved by Hilbert [22], is the basis of a large number of foundational results in algebraic geometry such as Hilbert's Nullstellansatz. It also lies at the heart of the foundational classification problem of algebraic geometry. For any projective variety $V \subseteq P(K^s)$ of dimension n, where K is an algebraically closed field of characteristic zero and $P(K^s)$ is the projective space associated with K^s, the lemma says that any *random* (generic) linear map $\psi : K^s \to K^m$, for any $m \geq n+1$, is regular (well defined) on V. Furthermore, for any such ψ, $\psi(V) \subseteq P(K^m)$, the image of V, is closed in $P(K^m)$, and (2) the fibre $\psi^{-1}(p)$, for any point $p \in \psi(V)$, is a finite set. In our context s will be exponential in n and m will be polynomial in n. In this case Noether's Normalization Lemma expresses the variety V, embedded in the ambient space $P(K^s)$ of exponential dimension, as a finite cover of the variety $\psi(V)$, embedded in the ambient space $P(K^m)$ of polynomial dimension. This is its main significance from the complexity-theoretic perspective. Deterministic construction or even verification of ψ is however very difficult in general. For general V, the current best algorithms for deterministic construction and verification based on a recent fundamental advance [36] in Gröbner basis theory take in the worst case space that is exponential n and time that is double exponential in n. (Before [36] the time bound was double exponential in s, and hence, triple exponential in n.) Nothing better can be expected in general because [35], [37] also prove a matching exponential space lower bound for the computation of Gröbner basis in this general setting.

By the results in this article, black-box derandomization of polynomial identity testing (PIT) [19], [27], [28], [2], [50], [54] in characteristic zero is essentially *equivalent* to the seemingly impossible task of bringing this worst-case double exponential time bound down to polynomial for *explicit* algebraic varieties. We call such efficient deterministic

0272-5428/12 $26.00 © 2012 IEEE
DOI 10.1109/FOCS.2012.15

construction *derandomization of Noether's Normalization Lemma*. Black-box derandomization of PIT is important, because by the fundamental hardness vs. randomness principle [27], [19], [28], [2] 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 show that, assuming the Generalized Riemann Hypothesis (GRH) instead of the black-box derandomization hypothesis, the problem of derandomizing Noether's Normalization Lemma for the ring of invariants of the adjoint action of the general linear group on a tuple of matrices can be brought down to quasi-PH, instead of P. Thus black-box derandomization of PIT takes us farther than GRH. Variants of the main implication are also shown assuming, instead of the black-box derandomization hypothesis in characteristic zero, Boolean lower bounds for constant-depth threshold circuits or uniform Boolean conjectures such as $EXP^{NP} \not\subseteq \Sigma_2^P \cap \Pi_2^P$, in conjunction with GRH. These results may explain in a unified way why proving lower bounds or derandomization results for arithmetic circuits in characteristic zero or constant-depth Boolean threshold circuits, or proving uniform Boolean conjectures such as $EXP^{NP} \not\subseteq \Sigma_2^P \cap \Pi_2^P$ has turned out to be so hard, and also why GRH has turned out to be so hard from the complexity-theoretic perspective. Thus this investigation reveals that the foundational problems of geometry (classification and GRH) and complexity theory (lower bounds and derandomization) share a common root difficulty that lies at the junction of these two fields. We refer to this difficulty, or a chasm in the terminology of [3], as the *GCT chasm*. This is meant to be a common abbreviation for the *geometric chasm in complexity theory* and the *complexity-theory chasm in geometry*, since the chasm is both of these simultaneously. 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. The approach proposed in this article and its sequel [44] is one such approach. There may be several others.

On the negative side, the equivalence in this article says that black-box derandomization of PIT in characteristic zero would necessarily require proving, either directly or by implication, results in algebraic geometry that seem impossible on the basis of the current knowledge. On the positive side, it says that if the fundamental derandomization and lower bound conjectures of complexity theory are true, then a large class of fundamental problems in algebraic geometry which appear intractable are actually tractable in the complexity-theoretic sense.

We also formulate a unified geometric complexity theory (GCT) approach to derandomization and classification based on this equivalence. It is illustrated by showing that Noether's Normalization Lemma for the ring of invariants of any explicit linear action of a classical algebraic group can be quasi-derandomized (unconditionally) if the dimension of the group is constant.

This article belongs to a series of articles on a GCT approach to the fundamental problems of complexity theory. See [40] for an informal overview of the earlier articles in this series, and [41] for a formal overview. All proofs are omitted in this abstract. The proofs and details can be found in the full version of the paper on the arXiv [43]. We now state the main results in this article in more detail.

II. Implications of the fundamental hypotheses in geometry and complexity theory

Let K be a field of characteristic zero. By black-box derandomization of PIT over K, we mean the problem of constructing an explicit hitting set [27], [19], [28], [2], [50], [54] 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. 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. The fundamental black-box derandomization hypothesis in complexity theory [19], [27], [28], [2], [50], [54] is that such explicit hitting sets exist.

In our first result, we consider a restricted form of PIT called symbolic trace identity testing (STIT). It is closely related to the symbolic determinant identity testing (SDIT) [28].

By a symbolic trace over K, we mean a polynomial of the form trace($A(x)^l$), where $A(x)$ is an $m \times m$ symbolic matrix whose each entry is a homogeneous 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 (poly(m, r)-time computable) hitting set $S_{r,m}$ of test inputs in $\mathbb{N}^r$ such that, for any symbolic trace polynomial trace($A(x)^l$), $l \leq m$, that is not identically zero, there exists a test input $b \in S_{r,m}$ such that trace($A(b)^l$) $\neq 0$.

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 $G = SL_m(K)$:

$$(A_1, \ldots, A_r) \to (PA_1P^{-1}, \ldots, PA_rP^{-1}), \qquad (1)$$

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. By an invariant we mean a polynomial

$f(U_1, \ldots, U_r)$ in the variable entries of U_i's such that

$$f(U_1, \ldots, U_r) = f(PU_1P^{-1}, \ldots, PU_rP^{-1}),$$

for all $P \in SL_m(K)$. Let $n = \dim(V) = rm^2$. It is known that $K[V]^G$ is finitely generated [22], [49], [52].

When K is algebraically closed, by Noether's Normalization Lemma [16], 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 is equivalent to the one given in the beginning of the 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 $\dim(K[V]^G) \leq n$. It is known that any suitably randomly chosen S of this cardinality has the required property. Such an optimal S is called an h.s.o.p. (homogeneous system of parameters) of $K[V]^G$. In the context of complexity theory, we only require that S be small (of poly(n) size) and do not insist on optimality. As we shall see below (cf. the remark after Theorem 7), this is crucial.

Specifically, 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 its subring generated by S, and (3) each invariant $s = s(U_1, \ldots, U_r)$ in S has a weakly skew straight-line program [34] over $\mathbb{Q}$ of poly(n) bit-length. Here (3) is equivalent [34] 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 rational coefficients of poly(n) bit length. By [9], [34], it follows that, given such a weakly-skew straight-line program of an invariant $s \in S$ and any rational matrices $A_1, \ldots, A_r \in M_m(\mathbb{Q})$, 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.

A quasi-s.s.o.p. is defined by replacing the poly(n) bounds by $O(2^{\text{polylog}(n)})$ bounds. A subexponential-s.s.o.p. with an exponent $\delta > 0$ is defined by replacing the poly(n) bounds by $O(2^{O(n^\delta)})$ bounds.

It can be shown that an s.s.o.p. exists. By the first fundamental theorem for matrix invariants [49], [52], a set S of exponential size that generates $K[V]^G$ can be constructed in exponential time and polynomial space. In contrast, the construction or even verification of an s.s.o.p. turns out to be a formidable challenge. The techniques in this paper in conjunction with the recent results in Gröbner basis theory [36], [37] show that an s.s.o.p. for $K[V]^G$ can be constructed (or verified) in space that is exponential in n and time that is double exponential in n. This is so even requiring the cardinality of S to be only polynomial (instead of optimal) or subexponential. By the following result, assuming black-box derandomization of STIT over an algebraically closed K, the problem of constructing an s.s.o.p. comes down from $EXPSPACE$ to P. Assuming GRH, instead of the black-box derandomization hypothesis, the problem comes down to quasi-PH instead.

Let us 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. A quasi-e.s.o.p. is defined by replacing the poly(n) bounds by $O(2^{\text{polylog}(n)})$ bounds. A subexponential-e.s.o.p. with an exponent $\delta > 0$ is defined by replacing the poly(n) bounds by $O(2^{O(n^\delta)})$ bounds.

Theorem 1: Let K be an algebraically closed field of characteristic zero. Let V and G be as above.
(a) Suppose the black-box derandomization hypothesis for STIT over K holds. Then Noether's Normalization Lemma for $K[V]^G$ can be derandomized. This means $K[V]^G$ has an e.s.o.p. Analogous result holds, after replacing the poly(n) bound everywhere by $O(n^{O(\log n)})$ bound, if we assume black-box derandomization over K of PIT for depth four circuits instead of STIT.
(b) Suppose there exists an $O(2^{s^\epsilon})$-time-computable hitting set against symbolic traces over K of size and degree $\leq s$, for any $\epsilon > 0$. Then $K[V]^G$ has a subexponential-e.s.o.p. for any exponent $\delta > 0$.
(c) Suppose GRH holds. Then the problem of derandomizing Nother's Normalization Lemma for $K[V]^G$ belongs to $\Delta_3^{quasiP} \subseteq$ quasi-PH. This means there is a quasi-polynomial time algorithm, with an access to the NP^{NP}-oracle, for constructing a quasi-s.s.o.p. for $K[V]^G$.

The results in (a) and (b) also hold for K that is not algebraically closed (e.g. $\mathbb{Q}$) with a suitably weaker definition of derandomization of Noether's Normalization Lemma in this case. There is also a weaker variant of (c) for Merlin-Arthur games.

The variety $V/G = \text{spec}(K[V]^G)$ here, called a categorical quotient [45], is a basic prototype of the moduli space of representations of a *wild quiver* [13]. The phrase wild here (meaning intractable) has a precise mathematical meaning [15]. It has the same connotations in geometric invariant theory as the phrase "NP-complete" in complexity theory. There is also a result for wild quivers [6] analogous to the NP-completeness result. It says that a solution to the problem of classifying representations of any wild quiver implies a solution for every other quiver. Theorem 1 can be generalized to moduli spaces of representations of any wild quiver. By this generalization, black-box derandomization of STIT over an algebraically closed field K of characteristic zero implies derandomization of Noether's Normalization Lemma over K for the analogous invariant ring associated with any wild quiver and dimension data.

The following result is a variant of Theorem 1 (a) and (b) assuming, instead of the black-box derandomization hypothesis, arithmetic lower bounds, or Boolean lower bounds in conjunction with GRH.

Let nonuniform $NC[d(n), S(n)]$ denote the class of Boolean functions that can be computed by nonuniform Boolean circuits of depth $d(n)$ and size $S(n)$, and $TC^0[S(n)]$ the class of Boolean functions that can be computed by constant-depth Boolean threshold circuits of size $S(n)$. Let nonuniform NC^i denote nonuniform $NC[\log^i n, \text{poly}(n)]$. The prefix i.o. in front of a complexity class denotes its "infinitely-often" version [28].

Theorem 2: Let K be an algebraically closed field of characteristic zero. Let V and G be as above.
(a) Suppose EXP has a multilinear integral function with a subexponential arithmetic lower bound. Then $K[V]^G$ has a quasi-e.s.o.p.

The arithmetic lower bound assumption here is that there exists an exponential-time-computable multilinear polynomial $f(x_1, \ldots, x_r)$ with integral coefficients of poly(r) bit-length such that f can not be computed by an arithmetic circuit over K of (1) $O(2^{r^a})$ size and $O(r^a)$ depth, for some constant $a > 0$, or alternatively, (2) $O(2^{r/a'})$ size and constant depth for some constant $a' > 0$.
(b) Suppose EXP has a multilinear integral function with a polynomial arithmetic lower bound. Then $K[V]^G$ has a subexponential-e.s.o.p for any exponent $\delta > 0$.

The arithmetic lower bound assumption here is that f as in (a) cannot be computed by an arithmetic circuit over K of $O(\log^2 r)$ depth and $O(r^a)$ size for any constant $a > 0$.
(c) Suppose EXP has a subexponential Boolean lower bound and that GRH holds. Then $K[V]^G$ has a quasi-e.s.o.p.

The Boolean lower bound assumption here is that $EXP \not\subseteq$ i.o. nonuniform-$NC\,[n^{\epsilon}, 2^{n^{\epsilon}}]$, for some constant $\epsilon > 0$, or alternatively, that $EXP \not\subseteq i.o.TC^0[2^{n/a'}]$, for some constant $a' > 0$. The prefix i.o. can be removed from the assumptions and added to the conclusions.
(d) Suppose EXP has a polynomial Boolean lower bound and that GRH holds. Then $K[V]^G$ has a subexponential-e.s.o.p. for any exponent $\delta > 0$.

The Boolean lower bound assumption here is that (1) $EXP \not\subseteq$ i.o. nonuniform-NC^3, or alternatively, that (2) $EXP \not\subseteq i.o.TC^0[n^{O(\sqrt{n}\log n)}]$. The prefix i.o. can be removed from the assumptions and added to the conclusions.
(e) Suppose $EXP \not\subseteq MA$ and that GRH holds. Then there is a subexponential time algorithm for constructing a subexponential-s.s.o.p. for $K[V]^G$, for any exponent $\delta > 0$, that is correct for infinitely many n.
(f) The results in (a)-(e) also hold, replacing EXP by EXP^{NP} in the assumptions and giving the algorithm for constructing S an access to the NP-oracle. The uniform lower bound assumption in (e) is replaced in this case by the uniform assumption that $EXP^{NP} \not\subseteq \Sigma_2^P \cap \Pi_2^P$, or alternatively, that $NEXP \not\subseteq MA$.

The next result generalizes Theorems 1 and 2 to any finite dimensional rational representation V of G assuming that an explicit first fundmental theorem (FFT) akin to that for matrix invariants in [49], [52] holds for V.

Let $G = SL_m(K)$ and V any rational representation of G of dimension n. Since G is reductive [18], V can be decomposed as a direct sum of irreducible representations of G:

$$V = \sum_{\lambda} m(\lambda) V_{\lambda}(G). \qquad (2)$$

Here $\lambda : \lambda_1 \geq \ldots \geq \lambda_l$, $l < m$, is a partition, i.e., a sequence of nonnegative integers, and $V_\lambda(G)$ is the irreducible representation of G (Weyl module [18]) labelled by λ. We assume that V is specified succinctly by giving n and m (in unary) and the multiplicities $m(\lambda)$'s (in binary) for all λ's that occur with nonzero multiplicity in this decomposition. The *degree* d of V is defined to be $\max\{|\lambda| = \sum \lambda_i\}$, where λ ranges over such partitions. Fix the standard monomial basis [14], [33] 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 $\sigma \in G$.

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 poly(n, m), (3) every invariant in S is homogeneous of poly(n, m) degree, and (4) every $s \in S$ has a small specification in the form of a weakly skew straight-line program [34] of poly(n, m) bit-length over $\mathbb{Q}$ and the coordinates $v_1, \ldots, v_n$ of V. Here (4) is equivalent [34] to (4)': every $s \in S$ can be expressed as the determinant of a matrix of poly(n, m) size whose entries are (possibly non-homogeneous) linear combinations of $v_1, \ldots, v_n$ with rational coefficients of poly(n, m) bit length. We say that S is an s.s.o.p. in a relaxed sense if the straightline programs in (4) are not required to be weakly skew.

We call a subset $S \subseteq K[V]^G$ 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 poly(n, m) time, given n, m, and the nonzero multiplicities $m(\lambda)$'s of $V_\lambda(G)$'s as in eq.(2). An e.s.o.p. in a relaxed sense or a quasi-e.s.o.p. is defined similarly.

The following result generalizes Theorems 1 and 2 in this context assuming blackbox derandomization of general PIT (instead of STIT) and an explicit FFT akin to that for matrix invariants in [49], [52].

Theorem 3: Suppose K is an algebraically closed field of characteristic zero. Let V as in (2) be a rational representation of $G = SL_m(K)$ of dimension n. Suppose an explicit FFT (defined formally in the full version) akin to that for matrix invariants [49], [52] holds for V.
(a) Suppose the black-box derandomization hypothesis for PIT over K holds. Then $K[V]^G$ has an e.s.o.p. in a relaxed sense.

Analogues and variants of Theorem 1 (b)-(c) and Theorem 2 also hold in this context.

This result also holds for an explicit linear representation of any classical algebraic group in characteristic zero.

If G has constant dimension, then Noether's Normalization Lemma for $K[V]^G$ can be quasi-derandomized unconditionally:

Theorem 4: Suppose K is an algebraically closed field of characteristic zero. Let V as in (2) be a rational representation of $G = SL_m(K)$ of dimension n. Suppose m is constant, or more generally, $O(\text{polylog}(n))$. Then $K[V]^G$ has a quasi-e.s.o.p. Furtheremore, such a quasi-e.s.o.p. can be constructed by a uniform AC^0 circuit of quasi-polynomial size with oracle access to DET.

The earlier algorithms for Noether Normalization of $K[V]^G$ based on Gröbner basis theory took space that is exponential in n and time that is double exponential in n even when m is constant.

In the first draft of this paper, Theorem 4 was stated and proved conditionally, assuming the black-box derandomization hypothesis for diagonal depth three circuits [53]. The author is grateful to Amir Shpilka for pointing out that this hypothesis (allowing a quasi prefix) is a consequence of the fundamental black-box derandomization technique in [50], [54] for restricted PIT's. Hence, Theorem 4 holds unconditionally.

In all intended applications of GCT, the rank m of the underlying group is nonconstant and large. In the context of black-box derandomization of PIT, this rank is polynomial in the size parameter of the circuits (cf. Theorem 6 below). The proof of Theorem 4 sheds no light on how to handle this general case since the size of the e.s.o.p. constructed in it is exponential in m. As we shall see in Section V, the general case as in Theorem 3 is far harder than the case when m is constant, as expected.

III. Equivalence

The categorical quotients $V/G = \text{spec}(K[V]^G)$ studied above are fundamental examples of what we call *explicit* algebraic varieties defined formally in the full version. A large class of algebraic varieties that are studied in algebraic geometry are explicit. The following results say that derandomization of PIT is essentially equivalent to derandomization of Noether's Normalization Lemma for explicit varieties.

Let K be an algebraically closed field of characteristic zero.

Theorem 5: A strengthened form of black-box derandomization of PIT over K (defined in the full version) implies derandomization of Noether's Normalization Lemma for the coordinate ring of any explicit algebraic variety over K.

In the context of symbolic determinant identity testing (SDIT) [28], we have the following equivalence.

Theorem 6: (Equivalence) A strengthened form of black-box derandomization of SDIT over K (defined in the full version) is equivalent to derandomization of Noether's Normalization Lemma (in a certain strict form) for the explicit algebraic variety $\Delta[\det, m]$ associated with the determinant in [42] in the context of the permanent vs. determinant problem.

See the full version for the full statements of these results. There is a similar result for the general PIT. It uses instead the variety in [42] associated with the complexity class P in the context of the algebraic P vs. NP problem.

IV. Proof technique

The proof of Theorem 1 (a) and (b) is based on the fundamental works in geometric invariant theory, specifically, the first and second fundamental theorems (FFT and SFT) for matrix invariants in [49], [52], and the properties of the categorical quotient $V/G = \text{spec}(K[V]^G)$ proved in [45]. The basic idea of the proof of Theorem 1 (a) is to construct in poly(n) time, using these FFT and SFT, a symbolic trace polynomial $T(v, y)$ over K, where $v = (v_1, \ldots, v_n)$ are the coordinates of V and $y = (y_1, \ldots, y_n)$ are auxillary variables, such that $T(v, y)$ can be expressed as a linear combination of certain symbolic traces over y with coefficients in $\mathbb{Q}[v]$ that generate $K[V]^G$. Specializing the y-variables of $T(v, y)$ at the elements of an explicit hitting set provided by the black-box derandomization hypothesis for STIT yields a small explicit set $S \subseteq K[V]^G$ of invariants with small specifications in the form of symbolic traces. The ring $K[V]^G$ is shown to be integral over the subring generated by S using the properties of the categorical quotient V/G in [45] in conjunction with Noether's Normalization Lemma. This shows that S is an e.s.o.p. and proves Theorem 1 (a). The proof of Theorem 1 (b) is a variation of this idea.

Theorem 2 (a) and (b) are reduced to Theorem 1 (a) and (b), respectively, using the fundamental equivalence between black-box derandomization of PIT and circuit lower bounds for EXP [19], [27], [28], [2], efficient factorization of multivariate polynomials given by straightline programs [29], and the depth reduction for arithmetic circuits [61], [3],

[25]. Theorem 2 (c) and (d) are reduced to Theorem 2 (a) and (b) using the fundamental connection between Boolean and algebraic complexities in [8], [24] based on the effective version [32] of the Chebotarev density theorem provided by the GRH, and the TC^0-algorithms for division and iterated multiplication [20]. Theorem 2 (e) is reduced to Theorem 2 (d) using the the fundamental connection between nonuniform and uniform Boolean lower bounds [30], [4], [26]. Theorem 2 (f) is obtained by extending the proof of Theorem 2 (c), (d) and (e), plugging the NP-oracle in the right places.

A similar extension of the proof of Theorem 2 (c), plugging the NP^{NP}-oracle in the right places, yields a quasi-e.s.o.p. S for $K[V]^G$ giving the algorithm for constructing S access to the NP^{NP} oracle, and assuming (i) GRH, and (ii) a subexponential circuit size lower bound for Δ_3^{EXP}. But (ii) holds unconditionally by the fundamental subexponential circuit size lower bound for Δ_3^{EXP} [23], [39]. This implies that S is a quasi-e.s.o.p., with an access to the NP^{NP} oracle, assuming GRH alone. This proves Theorem 1 (c). For its weaker variant for Merlin-Arthur games, one uses the fundamental circuit lower bound for MA_{EXP} [39] instead in the last step.

The proof of Theorem 3 is obtained by generalizing the proofs of Theorems 1 and 2, using the assumed explicit FFT in place of the explicit FFT for matrix invariants in [49], [52], [17], in conjunction with the algorithm in [22] for constructing finitely many generators for $K[V]^G$, computational invariant theory [59], [11], the bounds for the degrees of the generators for $K[V]^G$ in [47], [11], and standard monomial theory [33], [14].

The proof of Theorem 4 differs from the proof of Theorem 3 in two places. First, we prove an explicit FFT for constant m unconditionally. This is the heart of the proof. Second, one only needs the black-box (quasi) derandomization hypothesis for diagonal depth three circuits [53] in this case. As already mentioned, this hypothesis is a consequence of the proof technique in [50], [54]. Hence quasi-derandomiztion of Noether's Normalization Lemma follows unconditionally when m is constant. This proves Theorem 4.

Theorems 5 and 6 are proved by abstracting the ideas in the proofs of Theorems 1, 3, and 4.

V. History

Derandomization of Noether's Normalization Lemma for $K[V]^G$ as in Theorem 1 is the heart of the problem of classifying normal forms of r-tuples of $m \times m$ matrices over K under simultaneous conjugation by $SL_m(K)$. When $r = 1$, this normal form is just the Jordan normal form. For $r \geq 2$, this century-old classification problem of invariant theory is widely regarded as "impossible" or "hopeless"; cf. [6], [13]. This is the reason behind the terminology wild (cf. [15]). By [45], the points of V/G are in one-to-one correspondence with the closed G-orbits in V. If we restrict ourselves to only closed orbits as in [45], then the classification problem is to find an explicit description of the categorical quotient V/G. The best explicit description that one could hope for is an explicit free resolution of $K[V]^G$ over the free ring $K[S]$ generated by the symbols corresponding to an e.s.o.p. S. The heart of such an explicit description is, of course, the construction of an e.s.o.p. This is precisely the problem of derandomizing Noether's Normalization Lemma that can be solved (cf. Theorem 1) assuming black-box derandomization of STIT. The general ring $K[V]^G$ in Theorem 3 is a basic prototype of the ring the arises similarly in the context of the fundamental classification (moduli) problem [45] of algebraic geometry.

That $K[V]^G$ in Theorem 3 is finitely generated is the celebrated result of Hilbert [22]. 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 this result was nonconstructive. This was severely criticized by Gordon as "theology and not mathematics". Noether's Normalization Lemma as well as the Nullstellansatz were proved by Hilbert in the course of his second constructive proof of this result in response to this criticism. It is fair to say that this constructive proof and its various mathematical ingradients such as the Normalization Lemma and the Nullstellansatz changed the course of algebraic geometry in the twentieth century. But Hilbert could only show that his algorithm for constructing finitely many generators for $K[V]^G$ worked in finite time. He could not prove any explicit upper bound on its running time. Such a bound was proved in [47] a century later, and improved significantly in [11]. This improved analysis, in conjunction with the techniques in this paper and a recent fundamental advance [36] in Gröbner basis theory, yields an algorithm to compute a small S of poly(n, m) size such that $K[V]^G$ is integral over the subring generated by S. The resulting algorithm needs in the worst case space that is exponential in n and time that is double exponential in n (even when m is constant). Theorem 1 (a) says that this double exponential time bound can be brought down to polynomial for the ring $K[V]^G$ of matrix invariants therein assuming black-box derandomization of STIT. Theorem 3 (a) says the same for the general $K[V]^G$ assuming explicit FFT and black-box derandomization of PIT. Theorem 4 says the same for the general $K[V]^G$ unconditionally (allowing a quasi prefix) if m is constant. Classical invariant theory mainly focussed on the case when m is constant. For example, Hilbert's paper [22] mainly focussed on the case when $m = 4$. Thus Theorem 4 does address unconditionally the case that classical invariant theory focussed on.

The EXPSPACE-algorithm for constructing a small S mentioned above uses the Gröbner basis algorithm in [36]. The latter algorithm works for any algebraic variety presented by a set of generators for its ideal. The upper bound on its running time in [36] depends only on the dimension of the variety, the dimension of the ambient space in which the variety is embedded, and a bound on the degrees of the generators of its ideal. The matching worst-case double exponential time and exponential space lower bound in [35], [37] for the running time of this Gröbner basis algorithm basically means that we can not go any further than EXPSPACE using such general algebraic geometry. What is needed is *explicit algebraic geometry*, or specifically, an *explicit Gröbner basis* (as formally defined in the full version) that depends on the deeper structure of the specific variety at hand. In the context of the categorical quotient V/G for V and G as in Theorem 3, this means we need (at least) a good set of generators for the ring $K[V]^G$ with a sufficiently explicit set of relations among them. When $d = 1$, this problem is completely solved by the first and second fundamental theorems (FFT and SFT) of invariant theory in Weyl's classic book [62], though the complexity issues are not specifically addressed there. An explicit Gröbner basis in this case is constructed in [59]. Explicit FFT and SFT for the ring of matrix invariants in Theorem 1 are proved in [49], [52], [17]. An explicit Gröbner basis in this case is still not known. Proving explicit FFT and SFT for the general $K[V]^G$ in Theorem 3 has turned out to be extremely hard. This problem and its variants have been the focus of an intensive study in invariant theory in the last century. For small d (≤ 8) and small m (≤ 4) explicit FFT's and SFT's were proved in classical invariant theory; cf. [48] for their survey. An explicit FFT for any constant m, the key ingradient in the proof of Theorem 4, is proved in the full version of this article. For almost all other cases, the problem of proving explicit FFT and SFT (and, more strongly, constructing explicit Gröbner bases) appears "completely unsolvable" (cf. page 238 in [48]). For this reason, bringing the problem of constructing an s.s.o.p. for the general $K[V]^G$ with nonconstant large m from EXPSPACE to even the exponential hierarchy unconditionally is a massive challenge.

The problem of constructing an e.s.o.p. for the coordinate ring of $\Delta[\det, m]$, which by Theorem 6 is essentially equivalent to black-box derandomization of SDIT, is even harder since $\Delta[\det, m]$ is not even normal [31], unlike $V/G = \text{spec}(K[V]^G)$.

VI. The GCT chasm

In the mathematics literature, the phrases such as "explicit", "impossible", "hopeless" and "completely unsolvable" are only used informally. Complexity theory gives them precise meaning. Specifically, we interpret an explicit system of parameters (e.s.o.p.) as a polynomial-time-computable system of parameters that is easy to evaluate. Explicit FFT, SFT, and Gröbner bases are defined formally in the full version. We interpret the phrases "impossible", "hopeless", and "completely unsolvable" as referring to the seemingly impossible task of bringing the double exponential time bound for the construction of an s.s.o.p. down to polynomial. Of course, the worst interpretation for complexity theory and geometry would result if the problem of constructing an s.s.o.p. for the invariant ring in Theorem 1 turns out to be EXPSPACE-hard or even PSPACE-hard. Such a possibility cannot be ruled out at the outset, since the computation of the Gröbner basis, on which the current EXSPACE-algorithm for constructing an s.s.o.p. is based, is EXPSPACE-complete in general [35], [37].

Such an EXPSPACE-hardness result in conjunction with Theorem 1 (a) would imply that the black-box derandomization hypothesis for STIT is false in characteristic zero. Even only $PSPACE$-hardness would imply the same conclusion or that $PSPACE \subseteq P$. NP-hardness would imply the same conclusion or that $P = NP$. The same conclusion would also follow if the problem is not hard for any of these complexity classes, but is an intermediate problem in $EXPSPACE$ that is not in P (akin to the intermediate problems in NP which are neither NP-complete nor in P). If the problem is indeed not in P, then this is the most likely scenario (though formally proving that the problem is intermediate is a challenge). Similarly, if the problem of constructing a quasi-e.s.o.p. is an intermediate problem in $EXPSPACE$ that is not in quasi-PH, then Theorem 1 (c) would imply that GRH is false. If the problem of constructing a subexponential e.s.o.p. is an intermediate problem in EXPSPACE that is not in $E = DTIME(2^{O(n)}) \subseteq EXPTIME$, then Theorem 2 (b) would imply that the fundamental conjecture in [60] that the permanent does not have small circuits for all n is false in characteristic zero. It would also then follow from Theorem 2 (d) that either GRH is false or $EXP \subseteq i.o.P/$poly. If the latter happens, it should not be too surprising if $EXP \subseteq P/$poly as well. This would imply [4] that $EXP = PSPACE = PH = MA$.

If GRH and the fundamental derandomization and lower bound conjectures of complexity theory are still true (as we believe) despite these seemingly insurmountable odds, then their proofs seem far beyond the reach of the existing techniques in mathematics. In view of the magnitude of the difficulty, such unconditional proofs may require massive foundational extension and synthesis of the techniques of algebraic geometry and complexity theory.

Theorems 1 and 2 may thus explain why proving black-box derandomization results for unrestricted (depth four) PIT, proving superpolynomial constant-depth-arithmetic-circuit or Boolean-TC^0-circuit lower bounds for even EXP^{NP}, or proving even very conservative uniform Boolean conjectures such as $EXP^{NP} \not\subseteq \Sigma_2^P \cap \Pi_2^P$ has turned out to be so hard. In contrast, there are already known derandomization results for several versions of restricted PIT's in characteristic zero (cf. the survey [56] and the references therein), a quadratic lower bound for depth three circuits in characteristic zero [55], a quadratic determinantal lower bound for the permanent [38], superpolynomial AC^0 lower bounds for parity and majority (cf. [7] and the references therein), a superpolynomial ACC lower bound for EXP^{NP} [63], and uniform hierarchy theorems such as $EXP^{NP} \not\subseteq \Delta_2^P$, along with the known barriers [5], [51], [1] to the proof techniques of some of these lower bounds. Since non-black-box derandomization of PIT is closely related to circuit lower bounds for $NEXP$ [28], Theorem 2 (f) may explain why even partial non-black-box derandomization of PIT has turned out to be so hard. Theorem 1 (c) and (a) may explain the difficulty of GRH and the classification problem in algebraic geometry from the complexity-theoretic perspective. All this may provide a unified explanation for the difficulty of the fundamental problems of geometry (GRH and classification) and complexity theory (derandomization and lower bounds).

The results in this paper thus reveal that the foundational problems of geometry (classification and GRH) and complexity theory (lower bounds and derandomization) share a common root difficulty, namely, the problem of derandomizing Noether's Normalization Lemma, that lies at the junction of these two fields. We refer to this difficulty, or a chasm in the terminology of [3], as the *GCT chasm.* This is meant to be a common abbreviation for the *geometric chasm in complexity theory* and the *complexity-theory chasm in geometry*, since the chasm is both of these simultaneously. This does not mean that a synthesis of geometry and complexity theory is necessary for crossing it. In principle, nothing is necessary other than the axioms of Peano Arithmetic. But in reality, given the enormity of the chasm, a synthesis in some form may be necessary. 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. The approach proposed in this article and its sequel [44] is one such approach. There may be several other GCT approaches. It would be interesting to explore such alternatives.

We conjecture that e.s.o.p.'s exist for the $K[V]^G$'s under consideration and the coordinate rings of explicit varieties in general: i.e., Noether's Normalization Lemma for these rings can be derandomized (as suggested by Theorems 1, 2, 3, 5 and 6), the classification problems of algebraic geometry can be solved in the complexity-theoretic sense (cf. the full version), and the GCT chasm can be crossed.

VII. A GCT APPROACH TO DERANDOMIZATION OF PIT

The equivalence between black-box derandomization of PIT and derandomization of Noether's Normalization Lemma (Theorems 1, 2, 3, 5 and 6) leads to the following GCT approach to derandomization of PIT with several intermediate steps.

The goal is to bring down the problem of derandomizing Noether's Normalization Lemma for $\Delta[\det, m]$ from EXPSPACE (where it is currently) to P (eventually) step by step: from EXPSPACE to the exponential hierarchy first, then (moving through the exponential hierarchy) to EXP, then to PSPACE, then to PH, and finally (moving through PH) to P. Once the problem (in a strict form) is in P, it follows from Theorem 6 that SDIT is in P, the story for general PIT being similar. Since the geometry of $\Delta[\det, m]$ is extremely hard, the intermediate goal is to carry out these steps as far as possible for the explicit varieties that are simpler than $\Delta[\det, m]$ first, such as the categorical quotients V/G in Theorems 1 and 3 (which are still wild), or even simpler (non-wild) explicit varieties such as the explicit quiver varieties associated with tame quivers [13], explicit toric varieties [58], explicit curves, surfaces, and so forth. Though such intermediate results would not imply derandomization results for any class of circuits, they can form a crucial chain of steps leading to the eventual derandomization of PIT.

Theorem 4 that quasi-derandomizes Noether's Normalization Lemma for $K[V]^G$ unconditionally, when m is constant, is one such intermediate result. This concrete derandomization result for the invariant ring of focus in classical invariant theory hopefully illustrates the general approach in a nontrivial special case. The following is another intermediate result for the invariant rings in Theorems 1 and 3.

Theorem 7: Assume that GRH holds.
(a) Let $K[V]^G$ be as in Theorem 1. Then the problem of constructing an h.s.o.p. for $K[V]^G$ or verifying if $K[V]^G$ is integral over a given set $S \subseteq K[V]^G$ of invariants (specified as straight-line programs) belongs to $REXP^{NP}$. (Exponentially long oracle queries are allowed.)
(b) Let $K[V]^G$ be as in Theorem 3. Suppose explicit FFT and SFT (formally defined in the full version) hold for $K[V]^G$. Then the problem of constructing an h.s.o.p. for $K[V]^G$ or verifying if $K[V]^G$ is integral over a given $S \subseteq K[V]^G$ belongs to $REXP^{NP}$.
(c) Suppose an explicit SFT (formally defined in the full version) holds for an explicit variety W. Then the problems of constructing an h.s.o.p. and verifying or constructing a (strict) s.s.o.p. for the coordinate ring of W belong to $REXP^{NP}$.

Comparison of (a) and (b) with Theorems 1 and 3 suggests that the verification of s.s.o.p.'s in general is harder than the construction of specific s.s.o.p.'s. as in these earlier theorems, and that the construction of an h.s.o.p. is harder than the construction of an s.s.o.p. Assuming GRH, the problem of constructing an s.s.o.p. for an arbitrary explicit variety can only be put in the exponential hierarchy as in (c) and not in the polynomial hierarchy as in Theorem 1 (c) for the ring of matrix invariants.

The proof of (a) is based on the first and second fundamental theorems for matrix invariants [49], [52], [17] and the fundamental work [24] that shows that Hilbert's Nullstellansatz is in RP^{NP} assuming GRH; the proof of

(b) and (c) is similar.

Theorem 7 suggests the following approach to derandomization of SDIT (the story for general PIT being similar).

1) Prove an explicit SFT for the explicit variety $\Delta[\det, m]$ in Theorem 6. This puts the problem of constructing an s.s.o.p. for $\Delta[\det, m]$ in the exponential hierarchy assuming GRH (Theorem 7).
2) Construct an explicit Gröbner basis for the ideal $I[\det, m]$ of $\Delta[\det, m]$, as an aid for the journey from the exponential hierarchy to P, and use it to derandomize Noether's Normalization Lemma for $\Delta[\det, m]$ in a strict form; cf. the full version. This would imply derandomization of SDIT by Theorem 6.

We conjecture that explicit Gröbner bases (formally defined in the full version) exist for explicit varieties. The goal is to carry out these steps as far as possible for intermediate explicit varieties simpler than $\Delta[\det, m]$ first. At present, these steps can be carried out fully only for the simplest explicit varieties such as the Grassmanian and G/P for which explicit Gröbner basis theory, also called the theory of Hodge algebras [10] in this context, exists.

The GCT approach to derandomization above is extended in the full version to classification, and in the sequel [44] to the arithmetic permanent vs. determinant and other hardness conjectures in complexity theory.

Acknowledgment

The research in this article was supported by NSF grant CCF-1017760. The author is grateful to Josh Grochow for helpful comments and to Amir Shpilka for pointing out that the black-box derandomization hypothesis for diagonal depth three circuits follows from [50], [54].

References

[1] S. Aaronson, A. Wigderson, Algebrization: a new barrier in complexity theory, ACM transactions on computing theory, 1(1), 2009.

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

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

[4] L. Babai, L. Fortnow, N. Nisan, A. Wigderson, BPP has subexponential simulations unless EXPTIME has publishable proofs. Comput. Complexity 3:307-318, 1993.

[5] T. Baker, J. Gill, R. Soloway, Relativization of the $P =?NP$ question, SIAM J. Comput. 4, 431-442, 1975.

[6] G. Belitskii, V. Sergeichuk, Complexity of matrix problems, Linear Algebra and its applications, vol. 361, 2003, pp. 203-222.

[7] R. Boppana, M. Sipser: The complexity of finite functions, Handbook of Theoretical Computer Science, vol. A, Edited by J. van Leeuwen, North Holland, Amsterdam, 1990, 757–804.

[8] P. Bürgisser, Completeness and reduction in algebraic complexity theory, Algorithms and Computation in Mathematics, vol. 7, Springer, 1998.

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

[10] C. DeConcini, D. Eisenbud, C. Procesi, Hodge algebras, asterique, 91, societe mathematique de france, 1982.

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

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

[13] H. Derksen, J. Weyman, Quiver representations, Notices of the AMS, vol. 52, no. 2, 200-206.

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

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

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

[17] 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.

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

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

[20] W. Hesse, E. Allender, D. Barrington, Uniform constant-depth threshold circuits for division and iterated multiplication, JCSS, vol. 65, issue 4, 2002, pp. 695-716.

[21] D. Hilbert, Über die Theorie der algebraischen Formen, Math. Ann. 36, 1890, 473-534.

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

[23] R. Kannan, Circuit-size lower bounds and non-reducibility to sparse sets. Information and Control, 55:40-46, 1982.

[24] P. Koiran, Hilbert's Nullstellansatz is in the polynomial hierarchy, Journal of complexity 12, 273-286 (1996).

[25] P. Koiran, Arithmetic circuits: the chasm at depth four gets wider, arXiv:1006.4700v4 [cs.CC], 2012.

[26] R. Impagliazzo, V. Kabanets, A. Wigderson. In search of an easy witness: exponential versus probabilistic time. JCSS 65(4):672-694, 2002.

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

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

[29] 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.

[30] R. Karp, R. Lipton, Turing machines that take advice, L'Enseignement Mathematique, 28, pp. 191-209.

[31] S. Kumar, Geometry of orbits of permanents and determinants, arXiv:1007.1695, July 2010.

[32] J. Lagarias, A. Odlyzko, Effective versions of the Cheboterev density theorem, In Algebraic Number Fields, Proc. 1975 Durham Symposium, pages 409-464, Academic press, N.Y. 1977.

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

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

[35] E. Mayr, and A. Meyer, The complexity of the word problems for commutative semigroups and polynomial ideals, Advances in mathematics, 46 (3): 305-329, 1982.

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

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

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

[39] P. Miltersen, N. Vinodchandran, O. Watanabe, Super-polynomial versus half-exponential circuit size in the exponential hierarchy, In Proc. 5th annual International Conference on Computing and Combinatorics, 99.

[40] K. Mulmuley, The GCT program toward the P vs. NP problem, CACM, vol. 55, no. 6, pp. 98-107, 2012.

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

[42] 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.

[43] K. Mulmuley, Geometric complexity theory V: Equivalence between blackbox derandomization of polynomial identity testing and derandomization of Noether's normalization lemma, full version to be available on the arXiv and also at: http://ramakrishnadas.cs.uchicago.edu.

[44] K. Mulmuley, Geometric complexity theory VI: The flip via positivity, technical report, computer science department, the university of Chicago, July 2010. Revised version under preparation.

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

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

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

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

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

[50] R. Raz, A. Shpilka, Deterministic polynomial identity testing in non commutative models, Computational Complexity, 14(1): 1-19, 2005.

[51] A. Razborov, S. Rudich, Natural proofs, J. Comput. System Sci., 55 (1997), pp. 24-35.

[52] 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.

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

[54] A. Shpilka, I. Volkovich, Read-once polynomial identity testing, Proceedings APPROX-RANDOM, 2009, 700-713.

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

[56] A. Shpilka, A. Yehudayoff, Arithmetic circuits: a survey of recent results and open questions, Foundations and trends in Theoretical Computer Science: vol. 5: No. 3-4, pp 207-388.

[57] V. Strassen, Die berechnungskomplexiät von elementarsymmetrischen funktionen und von interpolationskoeffizienten. Numerische Mathematik, 20:238-251, 1973.

[58] B. Sturmfels, Gröbner bases of toric varieties, Töhoku Math. J. 43 (1991), 249-261.

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

[60] L. Valiant: The complexity of computing the permanent. Theoretical Computer Science 8 , 189-201 (1979).

[61] L Valiant, S. Skyum, S. Berkowitz, C. Rackoff, Fast parallel computation of polynomials using few processors, In SIAM J. Computing, pp. 641-644, vol. 12, no. 4, 1983.

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

[63] R. Williams, Non-uniform ACC circuit lower bounds, CCC, 2011.