Faster Real Feasibility via Circuit Discriminants

Frederic Bihan
UFR SFA, Campus Scientifique
73376 Le Bourget-du-Lac Cedex
France
Frederic.Bihan@universite-savoie.fr

J. Maurice Rojas
TAMU 3368
Department of Mathematics
Texas A&M University
College Station, Texas
77843-3368 USA
rojas@math.tamu.edu

Casey E. Stella
18409 Newell Road
Shaker Heights, OH 44122
USA
cestella@gmail.com

Rojas dedicates this paper to the memory of his dear friend, Richard Adolph Snively, 1955–2005.

ABSTRACT

We show that detecting real roots for honestly \(n\) variate \((n+2)\)-nomials (with integer exponents and coefficients) can be done in time polynomial in the sparse encoding for any fixed \(n\). The best previous complexity bounds were exponential in the sparse encoding, even for \(n\) fixed. We then give a characterization of those functions \(k(n)\) such that the complexity of detecting real roots for \(n\) variate \((n+k(n))\)-nomials transitions from \(P\) to \(NP\)-hardness as \(n \to \infty\). Our proofs follow in large part from a new complexity threshold for deciding the vanishing of \(\mathcal{A}\)-discriminants of \(n\) variate \((n+k(n))\)-nomials. Diophantine approximation, through linear forms in logarithms, also arises as a key tool.

Keywords
sparse, real, feasibility, polynomial-time, discriminant chamber

1. INTRODUCTION AND MAIN RESULTS

Consider real feasibility: the problem of deciding the existence of real roots for systems of polynomial equations. In addition to having numerous practical applications (see, e.g., [BC-V03]), real feasibility is an important motivation behind effectiveness estimates for the Real Nullstellensatz (e.g., [Ste74, BG-V03]), real feasibility is an important motivation behind having numerous practical applications (see, e.g., [Par03, Las07]). In particular, real solving of sparse polynomial systems arises in concrete applications such as satellite orbit mechanics [AM09], and real solving clearly involves real feasibility as an initial step. We are thus inspired to derive new algorithms and complexity lower bounds for real feasibility, in the refined setting of sparse polynomials.

To state our results, let us first clarify some basic notation concerning sparse polynomials and some well-known complexity classes. Recall that \(R^*\) is the multiplicative group of nonzero elements in any ring \(R\).

\[
\text{Definition 1.1. When } a_j \in \mathbb{R}^n, \text{ the notations } a_j = (a_{j,1}, \ldots, a_{j,n}), x^j = x_1^{a_{j,1}} \cdots x_n^{a_{j,n}}, \text{ and } x = (x_1, \ldots, x_n) \text{ will be understood. If } f(x) := \sum_{j=1}^{m} c_j x^j \text{ where } c_j \in \mathbb{R}^* \text{ for all } j, \text{ and the } a_j \text{ are pair-wise distinct, then we call } f \text{ a (real) } n\text{-variate } m\text{-nomial, and we define } \text{Supp}(f) := \{a_1, \ldots, a_m\} \text{ to be the support of } f. \text{ We also let } F_{n,m} \text{ denote the set of all } n\text{-variate } m\text{-nomials within } \mathbb{Z}[x_1, \ldots, x_n]. \text{ Finally, for any } m \geq n + 1, \text{ we let } F_{n,m} \subseteq F_{n,m} \text{ denote the subset consisting of those } f \text{ with } \text{Supp}(f) \text{ not contained in } (\mathbb{R}^n - \{0\})^n. \text{ We also call any } f \in F_{n,m} \text{ an honest } n\text{-variate } m\text{-nomial (or honestly } n\text{-variate) }.
\]

For example, \(1 + 7x_1^2x_2^3x_3^4 - 43x_1^{99} - 693x_2^{297} - 2x_3^{23} - x_4^{43}\) is a 4-variante trinomial with support contained in a line segment, but it has a real root \(x \in \mathbb{R}^4\) if the honestly univariate trinomial \(1 + 7y_1 - 43y_1^{99}\) has a real root \(y_1 \in \mathbb{R}\). More generally (via Lemma 2.3 of Section 2.2 below), it will be natural to restrict to \(F_{n,n+k}\) (with \(k \geq 1\)) to study the role of sparsity in algorithmic complexity over the real numbers.

We will work with some well-known complexity classes from the classical Turing model, briefly reviewed in the Appendix. (A more complete introduction can be found in [Pap95].) In particular, our underlying notion of input size is clarified in Definition 2.1 of Section 2.2 below, and illustrated in Example 1.1 immediately following our first main theorem. So for now, let us just recall the basic inclusions \(NC^1 \subseteq P \subseteq NP \subseteq \text{PSPACE}\). While it is known that \(NC^1 \neq \text{PSPACE}\) the properness of each of the remaining inclusions above is a famous open problem.

1.1 Sparse Real Feasibility and \(\mathcal{A}\)-Discriminant Complexity

\[
\text{Definition 1.2. Let } \mathbb{R}_+ \text{ denote the positive real numbers and let } \text{FEAS}_k \text{ (resp. } \text{FEAS}_p) \text{ denote the problem}
\]
of deciding whether an arbitrary system of equations from
$$\bigcup_{n \in \mathbb{N}} \mathbb{Z}[x_1, \ldots, x_n]$$ has a real root (resp. a root with all
coordinates positive). Also, for any collection $\mathcal{F}$ of tuples chosen
from $\bigcup_{n \in \mathbb{N}} \mathbb{Z}[x_1, \ldots, x_n]^e$, we let $\text{FEAS}_\mathcal{F}(\mathcal{F})$ (resp.
$\text{FEAS}_\mathcal{F}(\mathcal{F})$) denote the natural restriction of $\text{FEAS}_\mathcal{F}$ (resp.
$\text{FEAS}_\mathcal{F}$) to inputs in $\mathcal{F}$. 

It has been known since the 1980s that $\text{FEAS}_\mathcal{F} \in \text{PSPACE}$
[Can88], and an NP-hardness lower bound was certainly known
earlier. However, no sharper bounds in terms of sparsity
were known earlier in the Turing model until our first
main theorem.

**Theorem 1.3.** Let $Z_+(f)$ denote the zero set of $f$ in $\mathbb{R}^n$.
Then:

1. For any fixed $n$, $\text{FEAS}_n(\mathcal{F}_n)$ and $\text{FEAS}_n(\mathcal{F}_n+1)$
   are in $\text{NC}^3$. In particular, when $f \in \mathcal{F}_n+1$, $Z_+(f)$
is either empty or diffeotopic [BS] to $\mathbb{R}^{n-1}$, with each case
actually occurring.

2. For any fixed $\varepsilon > 0$, both $\text{FEAS}_n(\mathcal{F}_n+\varepsilon)$
   and $\text{FEAS}_n(\mathcal{F}_n+\varepsilon)$ are NP-hard.

Slightly sharper algorithmic complexity bounds hold when
we instead work in the BSS model over $\mathbb{R}$ (thus counting
arithmetical operations instead of bit operations), and this
is detailed in [BPR09].

**Example 1.4.** A very special case of Assertion (1) of
Theorem 1.3 implies that one can decide — for any nonzero
c1, \ldots, c5 \in \mathbb{Z}$ and $D \in \mathbb{N}$ — whether
c1 + c2x13 + c3x12 + c4x22D + c5x3x4 has a root in $\mathbb{R}$, using a number of bit operations
polynomial in
$$\log(D) + \log(|c[1]| + 1) \cdots (|c| + 1).$$

The best previous results (e.g., via the critical points method,
infinite-simials, and rational univariate reduction, as detailed
in [BPR09]) would yield a bound polynomial in
$D + \log(|c[1]| + 1) \cdots (|c| + 1)$ instead. 

We thus see that for sparse polynomials, large degree can be far
less of a complexity bottleneck over $\mathbb{R}$ than over $\mathbb{C}$. Theorem 1.3 is
proved in Section 2.3 below. The underlying techniques include $\mathcal{A}$-discriminants (a.k.a.
sparse discriminants) (cf. Section 2.3), Viro’s Theorem from toric
gometry (see the Appendix, or [GKZ94, Thm. 5.6]), and effective
estimates on linear forms in logarithms [Bak77, Nes03].

In particular, for any collection $\mathcal{F}_A$ of $n$-variate $m$-nomials
with support $\mathcal{A}$, there is a $\mathcal{A}$-discriminant $\Delta_A$ in the coefficients
($c_i$) called the $\mathcal{A}$-discriminant. Its real zero set partitions $\mathcal{F}_A$ into chambers
connected components of the complement) on which the zero set of an $f \in \mathcal{F}_A$ has constant
topological type. A toric deformation argument employing
Viro’s Theorem enables us to decide whether a given
chamber consists of $f$ having empty or non-empty $Z_+ (f)$. For
any $\mathcal{A} \subseteq \mathbb{N}^e$ of cardinality $n + 2$ (in sufficiently general
position), there is then a compact formula for the $\mathcal{A}$-discriminant
that enables us to pick out which chamber contains a given
$f$: one simply computes the sign of a linear combination of
logarithms. Our resulting algorithms are thus quite
implementable, requiring only fast approximation of logarithms
and some basic triangulation combinatorics for Supp($f$).

**Example 1.5.** Consider $A := \{0, 0, 0\}, (999, 0, 0), (73, 0, 19),
(0, 2009, 0), (74, 293, 1\}$, which gives us the family of trivariate
pentanomials $\mathcal{F}_A := \{c_1 + c_2x_1^{12} + c_3x_1^{12} + c_4x_2^{12} + c_5x_3^{12} + c_6x_1x_2x_3 | \ c_i \in \mathbb{R}^e\}$. Suppose
further that $f \in \mathcal{F}_A$ is an element satisfying $c_1, c_2, c_3, c_4 > 0$ and $c_5 < 0$. Then it then turns out via Lemma 2.13 (cf.
Section 2.4 below) that $Z_+(f)$ has a degeneracy off the
$\mathcal{A}$-discriminant, $\Delta_A(c)$ := 
$$-27886408 \cdot 27886408 - 27886408 \cdot 27886408 - 27886408 \cdot 7377857 - 2006991 \cdot 2006991 - 5561433 \cdot 5561433 \cdot 3813292.$$ 

While we review $\mathcal{A}$-discriminants in Section 2.3 below, it is
important to observe now how the computational complexity
of $\mathcal{A}$-discriminants closely parallels that of $\text{FEAS}_\mathcal{F}$; compare Theorem 1.3 above with Theorem 1.7 below.

**Definition 1.6.** Let $\text{ADISC}_\mathcal{F}$ (resp. $\text{ADISC} > \mathcal{F}$) denote
the problem of deciding whether $\Delta_A(f)$ vanishes (resp.
determining the sign of $\Delta_A(f)$) for an input polynomial $f$
with integer coefficients, where $A := \text{Supp}(f)$. Finally, let
$\text{ADISC}_\mathcal{F}$ (resp. $\text{ADISC}_\mathcal{F}$) be the natural restriction
of $\text{ADISC}_\mathcal{F}$ (resp. $\text{ADISC}_\mathcal{F}$) to inputs in some family $\mathcal{F}$.

**Theorem 1.7.**

1. $\text{ADISC}_\mathcal{F}(\mathcal{F}_n+1) \in \mathcal{P}$ and, for any fixed $n$,
   $\text{ADISC}_\mathcal{F}(\mathcal{F}_n+1) \in \mathcal{P}$.

2. For any fixed $\varepsilon > 0$, both $\text{ADISC}_\mathcal{F}(\mathcal{F}_n+\varepsilon)$
   and $\text{ADISC}_\mathcal{F}(\mathcal{F}_n+\varepsilon)$ are NP-hard.

Theorem 1.7 is proved in Section 2.4 after the development
of some necessary theory in Section 2 below.

### 1.2 Related Work

Earlier work on algorithmic fewnomial theory has
mainly gone in directions other than polynomial-time
algorithms. For example, Gabrielov and Vorobjov have given
singly exponential time algorithms for weak stratifications
of semi-Pfaffian sets [GV01] — data from which one can compute
homology groups of real zero sets of a class of functions
more general than sparse polynomials. Our approach thus
highlights a subproblem where faster and simpler algorithms
are possible.

Focussing on feasibility, rather than the elementary results
$\text{FEAS}_\mathcal{F}(\mathcal{F}_1) \in \mathcal{NCO}$ and $\text{FEAS}_\mathcal{F}(\mathcal{F}_2) \in \mathcal{NCO}$, there
appear to have been no earlier complexity upper bounds of
the form $\text{FEAS}_\mathcal{F}(\mathcal{F}_m) \in \mathcal{P}$, or even $\text{FEAS}_\mathcal{F}(\mathcal{F}_m) \in \mathcal{NP}$,
for $m \geq 3$. (With the exception of [Ry05], algorithmic
work on univariate real polynomials has focussed on
algorithms that are quasi-linear in the degree. See, e.g., [LM01].)
Echoing the parallels between \textsc{FEAS}_8 and \textsc{ADISC}_> provided by Theorems \[1.5\] and \[1.7\] both \textsc{FEAS}_8 (\textsc{F}_1,4) \in \mathbb{P} and \textsc{ADISC}_>(\textsc{F}_1,4) \in \mathbb{P} are open problems.

As for earlier complexity lower bounds for \textsc{FEAS}_8 in terms of sparsity, we are unaware of any. Indeed, it is not even known whether \textsc{FEAS}_8(\mathbb{Z}[x_1, \ldots , x_n]) is \textsc{NP}-hard for some fixed \(n\). Also, complexity lower bounds for the vanishing of discriminants of \(n\)-variate \((n + k(n))\)-nominals (with \(k\) a slowly growing function of \(n\)) appear to be new. However, recent work shows that the geometry of discriminants chambers can be quite intricate already for \(f \in \textsc{F}_3,3+3\) \[DRRS07\]. Also, it was known even earlier that deciding the vanishing of sparse discriminants of \textsc{univariate} \(m\)-nominals (with \(m\) unbounded) is already \textsc{NP}-hard with respect to randomized reductions \[KR09\]. Considering Theorems \[1.5\] and \[1.7\] one may thus be inclined to conjecture that \textsc{FEAS}_8(\mathbb{Z}[x_1]) is \textsc{NP}-hard. Curiously, over a different family of complete fields (the \(p\)-adic rationals), one can already prove that detecting roots for \textsc{univariate} \(m\)-nominals (with \(m\) unbounded) is \textsc{NP}-hard with respect to randomized reductions \[IRR07\].

2. BACKGROUND AND AUXILIARY RESULTS

After recalling a basic complexity construction, we will present some tools for dealing with \(n\)-variate \((n+1)\)-nomials, and then move on to \(n\)-variate \((n+k)\)-nomials with \(k \geq 2\).

All proofs for the results of this section are in the Appendix.

2.1 A Key Reduction

To measure the complexity of our algorithms, let us fix the following definitions for input size:

Definition 2.1. For any \(a \in \mathbb{Z}\), we define its size, \text{size}(a), to be \(1 + \log(1 + |a|)\). More generally, we define the size of a matrix \(U = [u_{i,j}] \in \mathbb{Z}^{m \times n}\) to be \(\sum_{i,j} \text{size}(u_{i,j})\). Also, for any \(f(x) = \sum_{i=1}^{m} c_i x^i \in \mathbb{Z}[x_1, \ldots , x_n]\), we define size(f) to be \(\sum_{i=1}^{m} \text{size}(c_i) + \text{size}(a_1)\). Finally, for \(F = \{f_1, \ldots , f_k\} \in (\mathbb{Z}[x_1, \ldots , x_n])^k\), we define size(F) = \(\sum_{i=1}^{k} \text{size}(f_i)\).

A key construction we will use later in our \textsc{NP}-hardness proofs is a refinement of an old trick for embedding Boolean satisfiability into real/complex satisfiability. We refer to the well-known 3\textsc{CNF SAT} problem, reviewed in the Appendix.

Proposition 2.2. Given any 3\textsc{CNF SAT} instance \(B(X)\) with \(n\) variables and \(N\) clauses, let \(W_B\) denote \(((\{1\} \times \mathbb{P}_3^N) \cup (\mathbb{P}_3^N \times \{1\}))^{4N-n}\). Then there is an \((8N-n) \times (8N-n)\) polynomial system \(F_B\) with the following properties:

1. \(B(X)\) is satisfiable iff \(F_B\) has a root in \([1,2]^n \times W_B\).

2. \(F_B\) has no more than \(33N - 4n\) monomial terms, \text{size}(F_B) = O(N)\), and every root of \(F_B\) in \((\mathbb{P}_3)^{8N-n}\) lies in \([1,2]^n \times W_B\) and is degenerate.

Also, if we define \(t_M(z_1, \ldots , z_M)\) to be \(1 + z_1^{M+1} + \cdots + z_{M+1}^{M+1} - (M+1)z_1 \cdots z_M\), then

3. \(t_M\) is nonnegative on \(\mathbb{R}_+^M\) with a unique positive root at \((1, \ldots , 1)\) that happens to be the only degenerate root of \(t_M\) in \(\mathbb{C}^M\).

4. If \(\varepsilon > 0\), \(f \in \mathcal{F}_{n,n+k}\), and \(M := \left\lceil k^{1/\varepsilon}\right\rceil\), then \(f(x) + t_M(z) \in \mathcal{F}_{n+\varepsilon^{k+1}}\) for \(n = n + M\) and some positive \(\delta \leq \varepsilon\).

In particular, size(f(x) + t_M(z)) = O(size(f)^{1/\varepsilon})\.

The seemingly mysterious polynomial \(t_M\) defined above will be useful later when we will need to decrease the difference between the number of terms and variables in certain polynomials.

2.2 Efficient Linear Algebra on Exponents

A simple and useful change of variables is to use monomials in new variables.

Definition 2.3. For any ring \(R\), let \(R_{m\times n}^N\) denote the set of \(m \times n\) matrices with entries in \(R\). For any \(M = [m_{i,j}] \in R_{m \times n}^N\) and \(y = (y_1, \ldots , y_n)\), we define the formal expression \(y^M := (y_1^{m_{1,1}} \cdots y_n^{m_{1,n}} \cdots y_1^{m_{m,1}} \cdots y_n^{m_{m,n}})\). We call the substitution \(x := y^M\) a monomial change of variables. Also, for any \(z := (z_1, \ldots , z_n)\), we set \(x := (x_1z_1, \ldots , x_nz_n)\). Finally, let \(\mathbb{GL}_n(R)\) denote the group of all matrices in \(R_{m\times n}\) with determinant \(\pm 1\) (the set of \textsc{unimodular} matrices).

Proposition 2.4. (See, e.g., \[LRW03\] Prop. 2.) For any \(U, V \in \mathbb{R}^{n \times n}\), we have the formal identity \((xy)^U = (x^U)(y^V)\). Also, if \(det U \neq 0\), then the function \(e_U(x) := x^U\) is an analytic automorphism of \(R^n\), and preserves smooth points and singular points of positive zero sets of analytic functions. Moreover, if \(det U > 0\), then \(e_U\) in fact induces a diffeotopy on any positive zero set of an analytic function. Finally, \(U \in \mathbb{GL}_n(R)\) implies that \(e_U^V(R^n) = R^n\) and that \(e_U\) maps distinct open orthants of \(R^n\) to distinct open orthants of \(R^n\).

Proposition 2.3 with minor variations, has been observed in many earlier works (see, e.g., \[LRW03\]). Perhaps the only new ingredient is the observation on diffeotopy, which follows easily from the fact that \(\mathbb{GL}_n(R)\) (the set of all \(n \times n\) real matrices with positive determinant) is a connected Lie group.

Recall that the \textit{affine span} of a point set \(A \subseteq \mathbb{R}^n\), \(Aff(A)\), is the set of all real linear combinations \(\sum_{a \in A} c_a a\) satisfying \(\sum_{a \in A} c_a = 0\).

Lemma 2.5. Given any \(f \in \mathcal{F}_{n,m}\) with \(d = \dim\ Aff(Supp(f)) < n < m\), we can find (using a number of bit operations polynomial in \(\text{size}(\text{Supp}(f))\)) a \(U \in \mathbb{GL}_n(\mathbb{Z})\) such that \(\gamma(y) := f(y^U) \in \mathcal{F}_{d,m}\) and \(g\) vanishes in \(\mathbb{R}_+^n\) (resp. \(\mathbb{R}_+^n\)) iff \(f\) vanishes in \(\mathbb{R}_+^n\) (resp. \(\mathbb{R}_+^n\)). In particular, there is an absolute constant \(c\) such that \(\text{size}(U) = O(\text{size}(\text{Supp}(f))^{\gamma})\).

To study \(Z_+(f)\) when \(f \in \mathcal{F}_{n,n+1}\) it will help to have a much simpler canonical form. In what follows, we use \# for set cardinality and \(c_i\) for the \(i\)-th standard basis vector of \(\mathbb{R}^n\).

Lemma 2.6. For any \(f \in \mathcal{F}_{n,n+1}\) we can compute \(\ell \in \{0, \ldots , n\}\) within \(NC^1\) and \(\gamma \in \mathbb{R}_+\) such that \(\tilde{f}(x) := \gamma + x_1 + \cdots + x_\ell - x_{\ell+1} - \cdots - x_n\) satisfies: (1) either \(f \neq \tilde{f}\) has exactly \(\ell + 1\) positive coefficients, and (2) \(Z_+(\tilde{f})\) and \(Z_+(f)\) are diffeotopic.

Corollary 2.7. Suppose \(f \in \mathcal{F}_{n,n+1}\) and \(\text{Supp}(f) = \{a_1, \ldots , a_{n+1}\} \subseteq \mathbb{R}^n\). Then
1. If $f$ has a root in $\mathbb{R}_+^n \iff$ not all the coefficients of $f$ have the same sign. In particular, $Z_+(f)$ is diffeotopic to either $\mathbb{R}_+^n$ or $\emptyset$.

2. If all the coefficients of $f$ have the same sign, then $f$ has a root in $(\mathbb{R}_+^n)^* \iff$ there are indices $i \in [n]$ and $j, j' \in [n + 1]$ with $a_{i,j} - a_{i,j'}$ odd.

2.3 Combinatorics and Topology of Certain $A$-Discriminants

The connection between topology of discriminant complements and computational complexity dates back to the late 1970s, having been observed relative to (a) the membership problem for semi-algebraic sets [DL79] and (b) the approximation of roots of univariate polynomials [Sma87]. Our goal here is a precise connection between $\mathbb{F}A$ and $A$-discriminant complements. (See also [DPRS07] for further results in this direction.)

DEFINITION 2.8. [GKZ93, Ch. 1 & 9–11] Given any $A = \{a_1, \ldots, a_m\} \subset \mathbb{Z}^n$ of cardinality $m$ and $c_1, \ldots, c_m \in \mathbb{C}^n$, we define

\[ \nabla_A \subset \mathbb{P}^{m-1}_R \quad \text{the } A\text{-discriminant variety} \]

— to be the closure of the set of all $[c_1 : \cdots : c_m] \in \mathbb{P}^{m-1}_R$ such that $f(x) = \sum_{i=1}^m c_i x^a_i$ has a degenerate root in $\mathbb{C}^n$. We then define $\Delta_A \subset \mathbb{Z}[c_1, \ldots, c_m] \{0\}$ — the $A$-discriminant — to be the (up to sign) irreducible defining polynomial of $\nabla_A$. Also, when $\nabla_A$ has complex codimension at least 2, we set $\Delta_A$ to the constant 1. For convenience, we will sometimes write $\Delta_A(f)$ in place of $\Delta_A(c_1, \ldots, c_m)$.

To prove our results, it will actually suffice to deal with a small subclass of $A$-discriminants.

DEFINITION 2.9. We call $A \subset \mathbb{R}^n$ a (non-degenerate) circuit if $A$ is affinely dependent, but every proper subset of $A$ is affinely independent. Also, say that $A$ is a degenerate circuit if $A$ contains a point $a$ and a proper subset $B$ such that $a \in B$, $A \setminus a$ is affinely independent, and $B$ is a non-degenerate circuit.

For instance, both $\mathbb{C}$ and $\mathbb{R}^1$ are circuits, but $\mathbb{R}^2$ is a degenerate circuit. In general, for any degenerate circuit $A$, the subset $B$ named above is always unique.

The relevance of $A$-discriminants to $m$-nomial zero sets can be summarized as follows.

DEFINITION 2.10. Following the notation of Definition 2.8, we call any connected component of $\mathbb{P}^{m-1}_R \setminus (\nabla_A \cup \{x_1 : \cdots : x_m\} | x_1 \cdots x_m = 0)$ a (real) $A$-discriminant chamber. Also, given any subsets $X, Y \subset \mathbb{R}_+^n$, we say that they are isotopic (resp. diffeotopic) if there is a continuous (resp. differentiable) function $H : [0, 1] \times X \rightarrow \mathbb{R}_+^n$ such that $H(t, \cdot)$ is a homeomorphism (resp. diffeomorphism) for all $t \in [0, 1], H(0, \cdot) = \text{identity on } X$, and $H(1, X) = Y$. Finally, for any $A \subset \mathbb{R}^n$ of cardinality $m$, let $F_A$ denote the set of all $n$-variate $m$-nomials with support $A$.

REMARK 2.11. Note that when $A$ has cardinality $m$, we may naturally identify elements of $\mathbb{P}^{m-1}_R$ (resp. $\mathbb{R}^{m-1}_R$) with equivalence classes determined by nonzero complex (resp. real) multiples of elements of $F_A$.

This terminology comes from matroid theory and has nothing to do with circuits from complexity theory.

The topology of toric real zero sets is known to be constant on discriminant chambers (see, e.g. [GRZ94], Ch. 11, Sec. 5A, Prop. 5.2, pg. 382). However, we will need a refinement of this fact to positive zero sets, so we derive this directly for $A$ in sufficiently general position — non-degenerate circuits in particular.

LEMMA 2.12. Following the notation above, suppose $A \subset \mathbb{R}^n$ is such that the minimum of any linear form on $A$ is minimized at no more than $n + 1$ points. Also let $C$ be any $A$-discriminant chamber. Then $f, g \in C \iff Z_+(f)$ and $Z_+(g)$ are diffeotopic.

There is then a very compact description for $\nabla_A$ when $A$ is a circuit.

LEMMA 2.13. Suppose $A = \{a_1, \ldots, a_{n+2}\} \subset \mathbb{Z}^n$ is a non-degenerate circuit, $f$ is a polynomial with support $A$, $\hat{A}$ is the $(n+1) \times (n+2)$ matrix whose $i, j$ column is $\{1\} \times a_j$, $\hat{A}$ is the submatrix of $\hat{A}$ obtained by deleting the $\emptyset$ column, and $b_j := (-1)^j \det \hat{A}_j/\beta$ where $\beta = \gcd(\det \hat{A}_1, \ldots, \det \hat{A}_{n+2})$.

Then:

1. $\Delta(c_1, \ldots, c_{n+2})$ is, up to a multiple by a nonzero monomial term, $\prod_{i=1}^{n+2} \left( \sum_{j=1}^{n+2} c_j a_i \right) - 1$. Also, $(b_1, \ldots, b_{n+2})$ can be computed in $\mathbb{P}$.

2. $\prod_{i=1}^{n+2} (\text{sign}(c_1 b_1 c_i b_j) c_i c_j b_i b_j = 1$ for some $c_1 : \cdots : c_{n+2} \in \mathbb{P}^{n+2}_R$ with $\text{sign}(c_1 b_1) = \cdots = \text{sign}(c_{n+2} b_{n+2})$.

3. $\hat{A}$ has exactly two triangulations: one with simplices $\{\text{Conv}(A \setminus \{b_i\}) | \text{sign}(b_i) > 0\}$, and the other with simplices $\{\text{Conv}(A \setminus \{b_i\}) | \text{sign}(b_i) < 0\}$. Moreover, the preceding description also holds when $A$ is a degenerate circuit.

2.4 Complexity of Circuit Discriminants and Linear Forms in Logarithms

Theorem [L77] is a central tool behind the upper bounds and lower bounds of Theorem [L83] and is precisely where diophantine approximation enters our scenery. To wit, the proof of Assertion (1) of Theorem [L77] makes use of the following powerful result.

NESTERENKO-MATVEEV THEOREM. [Nes03] Thm. 2.1, Pg. 55. For any integers $c_1, a_1, \ldots, c_N, a_N$ with $a_i \geq 2$ for all $i$, define $\Lambda(c, \alpha) := c_1 \log(\alpha_1) + \cdots + c_N \log(\alpha_N)$. Then $\Lambda(c, \alpha) \neq 0 \Rightarrow \log \left( \frac{1}{\Lambda(c, \alpha)} \right)$ is bounded above by

\[ 2.9(N + 2)^{9/2}(2e)^{2N+6} (2 + \log \max(c_i)) \prod_{j=1}^{N} \log|\alpha_j|. \]

Assertion (1) of Theorem [L77] will follow easily from the two algorithms we state below, once we prove their correctness and verify their efficiency. However, we will first need to recall the concept of a gcd-free basis. In essence, a gcd-free basis is nearly as powerful as factorization into primes, but is far easier to compute.

DEFINITION 2.14. [BS92, Sec. 8.4] For any subset $\{a_1, \ldots, a_N\} \subset \mathbb{N}$, a gcd-free basis is a pair of sets $\{\gamma_i\}_{i=1}^{N-1}, \{\epsilon_i\}_{i \in N \setminus \{0\}}$ such that (1) $\gcd(\gamma_i, \gamma_j) = 1$ for all $i \neq j$, and (2) $a_i = \prod_{j=1}^{N-1} \gamma^{\epsilon_{ij}}$ for all $i$.  

---
Algorithm 2.15.
Input: Integers \( \alpha_1, \beta_1, u_1, v_1, \ldots, \alpha_N, \beta_N, u_N, v_N \).
Output: A true declaration as to whether \( \alpha_1^{u_1} \cdots \alpha_N^{u_N} = \beta_1^{v_1} \cdots \beta_N^{v_N} \).
Description:
0. If \( \prod_{i=1}^{N} (\text{sign} \, \alpha_i)^{u_i} \mod 2 \neq \prod_{i=1}^{N} (\text{sign} \, \beta_i)^{v_i} \mod 2 \) then output “They are not equal.” and STOP.
1. Replace the \( \alpha_i \) and \( \beta_i \) by their absolute values and then construct, via Theorem 2.7 of the Appendix, a god-free basis \((\{y_i\})_{i=1}^{N}, \{c_{ij}\}_{(i,j) \in [2N] \times [N]} \) for \( \alpha_1, \ldots, \alpha_N, \beta_1, \ldots, \beta_N \).
2. If \( \sum_{i=1}^{N} c_{ij}v_i = \sum_{i=1}^{2N} c_{ij}v_i \) for all \( j \in [n] \) then output “They are equal.” and STOP.
3. Output “They are not equal.”

Algorithm 2.16.
Input: Positive integers \( \alpha_1, u_1, \ldots, \alpha_M, u_M \) and \( \beta_1, v_1, \ldots, \beta_N, v_N \) with \( \alpha_i, \beta_i \geq 2 \) for all \( i \).
Output: The sign of \( \alpha_1^{u_1} \cdots \alpha_M^{u_M} - \beta_1^{v_1} \cdots \beta_N^{v_N} \).
Description:
0. Check via Algorithm 2.15 whether \( \alpha_1^{u_1} \cdots \alpha_M^{u_M} = \beta_1^{v_1} \cdots \beta_N^{v_N} \). If so, output “They are equal.” and STOP.
1. Let \( U := \max \{u_1, \ldots, u_M, v_1, \ldots, v_N\} \) and \( E := \frac{2^\frac{1}{2}}{\log (2e)} \left( 2^{M+2N+6} (1 + \log U) \right) \times \left( \prod_{i=1}^{M} \log |\alpha_i| \right) \left( \prod_{i=1}^{N} \log |\beta_i| \right) \).
2. For all \( i \in [M] \) \((\text{resp. } i \in [N])\), let \( A_i \) \((\text{resp. } B_i)\) be a rational number agreeing with \( \log |\alpha_i| \) \((\text{resp. } \log |\beta_i|)\) in its first \( 2 + E \log 2 + E \log 2 + \log 2 N \) leading bits.
3. Output the sign of \( \left( \sum_{i=1}^{M} A_i \right) - \left( \sum_{i=1}^{N} V_i \right) \) and STOP.

Lemma 2.17. Algorithms 2.15 and 2.16 are both correct. Moreover, following the preceding notation, Algorithms 2.15 and 2.16 run within a number of bit operations asymptotically linear in, respectively,
\[ \sum_{i=1}^{N} \left( \log (u_i) \log (\alpha_i) + \log (v_i) \log (\beta_i) \right)^2 \]
and
\[ (M + N)(30)^{M+N} L(\log U) \left( \prod_{i=1}^{M} L(\log (\alpha_i)) \right) \left( \prod_{i=1}^{N} L(\log (\beta_i)) \right), \]
where \( L(x) := \log^2(x) \log \log (x) \).

2.5 Positive Feasibility for Circuits

For a real polynomial supported on a non-degenerate circuit, there are just two ways it can fail to have a positive root: a simple way and a subtle way. This is summarized below. Recall that the Newton polytope of \( f \) is simply Newt(\( f \)) := Conv(Supp(\( f \))), where Conv(\( S \)) denotes the convex hull (smallest convex set) containing \( S \).

Theorem 2.18. Suppose \( f(x) = \sum_{i=1}^{n+2} c_i x^{\alpha_i} \in F_{-n,n+2} \).
Supp(\( f \)) is a non-degenerate circuit, and \( b \) is the vector from Lemma 2.13. Then Newt(\( f \)) is empty iff one of the following conditions holds:

1. All the \( c_i \) have the same sign.
2. Newt(\( f \)) is an \( n \)-simplex and, assuming \( a_i \) is the unique element of \( A \) lying in the interior of Newt(\( f \)), we have \( -\text{sign}(a_i) = \text{sign}(c_i) \) for all \( i \neq j \), and
\[ \prod_{i=1}^{n+2} \left( \text{sign}(b_i, c_i) \right) > 1. \]

Positive feasibility for polynomials supported on degenerate circuits can then essentially be reduced to the non-degenerate circuit case in some lower dimension. An additional twist arises from the fact that the zero sets of polynomials supported on degenerate circuits are, up to a monomial change of variables, the graphs of polynomials supported on non-degenerate circuits.

Theorem 2.19. Suppose \( f(x) = \sum_{i=1}^{n+2} c_i x^{\alpha_i} \in F_{-n,n+2} \) has support \( A \subseteq \mathbb{R}^n \) that is a degenerate circuit with non-degenerate subcircuit \( B = \{ a_1, \ldots, a_j \} \), and \( b \) is the vector defined in Lemma 2.13 (ignoring the non-degeneracy assumption for \( A \)). Then, when not all the coefficients of \( f \) have the same sign, \( Z_+(f) \) is empty if both the following conditions hold:

a. Conv(\( B \)) is a \((j-2)\)-simplex and, permuting indices so that \( a_j \) is the unique element of \( B \) lying in the relative interior of Conv(\( B \)), we have \( -\text{sign}(c_j) = \text{sign}(c_i) \) for all \( i \neq j \).

b. \( \prod_{i=1}^{n+2} \left( \text{sign}(b_i, c_i) \right) \text{sign}(b_j, c_j) > 1. \)

3. THE PROOFS OF OUR MAIN RESULTS: THEOREMS 1.7 AND 1.3

We go in increasing order of proof length.

3.1 Proving Theorem 1.7

Assertion (1): First note that any input \( f \) must have support \( A = \{a_1, \ldots, a_{n+2}\} \) equal to either a degenerate circuit or a non-degenerate circuit. Recalling Assertion (1) of Theorem 2.13, observe then that the vector \( b := (b_1, \ldots, b_{n+2}) \) has a zero coordinate if \( A \) is a degenerate circuit, and \( b \) can be computed in time polynomial in size(\( A \)). If \( A \) is a degenerate circuit then (following easily from the definition) \( \Delta_A \) must be identically 1, thus leaving Assertion (1) of our present theorem trivially true. So let us assume henceforth that \( A \) is a non-degenerate circuit, and that \( c_j \) is the coefficient of \( x^{a_j} \) in \( f \) for all \( j \).

Via Assertion (1) of Lemma 2.13 once again, Assertion (1) of Theorem 1.7 follows routinely from the complexity bounds from Lemma 2.14. In particular, the latter lemma tells us that the bit complexity of ADISC_{\( n \}} for input coefficients \( (c_1, \ldots, c_{n+2}) \), is polynomial in \( \sum_{i=1}^{n+2} \log(c_i) \) (following the notation of Lemma 2.13); and the same is true for ADISC_{\( n \}} provided \( n \) is fixed. The classical Hadamard inequality \( \text{Maj}^2 \) then tells us that size(\( b \)) is \( O(n \log(n) \max_i \{a_{ik}\}) \). So the complexity of ADISC_{\( n \}} is indeed polynomial in size(\( f \)); and the same holds for ADISC_{\( n \}} when \( n \) is fixed.

Assertion (2): We will construct an explicit reduction of 3CNF SAT to ADISC_{\( n \}}. In particular, to any 3CNF SAT instance \( X(W) \) with \( N \) clauses and \( n \) variables, let us first consider \( F_B = \{f_1, \ldots, f_{N-n} \} \) — the associated \( (8N - n) \times (8N - n) \) polynomial system as detailed in Definition 1.11 of the Appendix and Proposition 2.2 of Section 2.1.
Let us then set $M := \left(\max\{0, 17N - 2n\} + 2\right)^{1/\varepsilon}$ and define the single polynomial $f_{B}$ to be
\[ f_{1} + \lambda_{1}f_{2} + \cdots + \lambda_{N-N-1}f_{N-N} + \lambda_{N-N}f_{M}\]
Letting $A$ be the support of $f_{B}$, it is then easily checked (from Definition 2.1 of the Appendix and Proposition 2.2) that $A$ is affinely independent and $f_{B}$ is in $F^{*}_{16N-2n+M,n'}$ for some $N' \leq 33N - 4n + M + 2$.
By the Cayley Trick (GRZ41) Prop. 1.7, pp. 274) we then obtain that $\Delta_{A}(f_{B}) = 0$ iff
\[(*) \quad F_{B} \text{ has a degenerate root in } (P_{L})^{2N-n} \text{ and } t_{M} \text{ has a degenerate root in } (C^{M})^{*}.\]
(Since Newton($t_{M}$) is a simplex, it is easily checked that $t_{M}$ has no complex degenerate roots at infinity.) By Proposition 2.2 the degenerate roots of $F_{B}$ are exactly $\{1, 2\}^{n} \times W_{B}$, and $t_{M}$ has a unique degenerate root by construction. So $(*)$ holds iff $B(X)$ has a satisfying assignment. We have thus reduced 3CNF SAT to detecting the vanishing of a particular $A$-discriminant.

To conclude, observe that the number of terms of $f_{B}$ is only slightly larger than its number of variables, thanks to Proposition 2.2. In particular, size($f_{B}$) = $O(size(B)^{1/\varepsilon})$ and $f_{B} \in \bigcup_{n \in \mathbb{N}} F_{n,n+n'}^{*}$ for some $\delta \in (0, \varepsilon]$. Clearly then, $\text{ADISC}_{-}\left(\bigcup_{n \in \mathbb{N}} F_{n,n+n'}^{*}\right) \subseteq P \implies P = \text{NP}$, thus proving our first desired NP-hardness lower bound.

The NP-hardness of $\text{ADISC}_{-}\left(\bigcup_{n \in \mathbb{N}} F_{n,n+n'}^{*}\right)$ then follows immediately since $\text{ADISC}_{-}\left(\bigcup_{n \in \mathbb{N}} F_{n,n+n'}^{*}\right)$ is a refinement of $\text{ADISC}_{-}\left(\bigcup_{n \in \mathbb{N}} F_{n,n+n'}^{*}\right)$.

3.2 Proving Theorem 1.3

Assertion (2): We will give an explicit reduction of 3CNF SAT to $\text{FEAS}_{1}\left(\bigcup_{n \in \mathbb{N}} F_{n,n+n'}^{*}\right)$. Attaining such a reduction will require little effort, thanks to our earlier reduction used to prove Assertion (2) of Theorem 1.7.

In particular, for any 3CNF SAT instance $B$ with $N$ clauses and $n$ variables, let us recall the system $F_{B} = (f_{1}, \ldots, f_{N+n})$ from Definition 2.1 of the Appendix and Proposition 2.2. Let us then define $M$ to be $\left(\max\{0, 42N - n\} + 2\right)^{1/\varepsilon}$ and define $g_{B}(x, z, z)$ to be $f_{B}^{*}(x) + \cdots + f_{B}^{*}(x) + \lambda_{M}(z_{1}, \ldots, z_{M})$. It is then easily checked that $f_{B} \in F_{n,n+n'}^{*}$ for some $N' \leq 42N + M + 2$.
Moreover, $B$ has a satisfying assignment iff $g_{B}$ has a positive root. (Indeed, any root of $f_{B}$ has a unique negative coordinate of $x$, $z$, and $z_{M}$.) We have thus reduced 3CNF SAT to a special case of $\text{FEAS}_{1}$.

Now observe that the number of terms of $g_{B}$ is only slightly larger than its number of variables, thanks to Proposition 2.2. In particular, size($g_{B}$) = $O(size(B)^{1/\varepsilon})$ and $g_{B} \in \bigcup_{n \in \mathbb{N}} F_{n,n+n'}^{*}$ for some $\delta \in (0, \varepsilon]$. Clearly then, $\text{FEAS}_{1}\left(\bigcup_{n \in \mathbb{N}} F_{n,n+n'}^{*}\right) \subseteq P \implies P = \text{NP}$, thus proving one of our desired NP-hardness lower bounds.

To conclude, we now need to prove the NP-hardness of $\text{FEAS}_{1}\left(\bigcup_{n \in \mathbb{N}} F_{n,n+n'}^{*}\right)$. This we do by employing our preceding argument almost verbatim. The only difference is that we instead use the polynomial $h_{B}(x, z) := f_{B}^{*}(x) + \cdots + f_{B}^{*}(x) + \lambda_{M}(z_{1}, \ldots, z_{M})$, and observe that $t_{M}(z_{1}, \ldots, z_{M})$ is nonnegative on all of $R^{n}$. So we are done.

Assertion (0): Our topological assertion follows immediately from Lemma 2.6 and Corollary 2.7.

To obtain our algorithmic assertions, simply note that by Assertion (1) of Corollary 2.7, detecting positive roots for $f$ reduces to checking whether all the coefficients have the same sign. This can clearly be done by $n$ sign evaluations and $n - 1$ comparisons, doable in logarithmic parallel time. So the inclusion involving $\text{FEAS}_{1}$ is proved.

Let us now show that we can detect roots in $(R^{*})^{n}$ within NC$^{1}$. Employing our algorithm from the last paragraph, we can clearly assume the signs of the coefficients of $f$ are all identical (for otherwise, we would have detected a root in $R_{+}^{n}$ and finished). So then, by Assertion (2) of Corollary 2.7, we can simply do a parity check (trivially doable in NC$^{1}$) of the entries of $[a_{2} - a_{1}, \ldots, a_{n+1} - a_{1}]$.

To conclude, we simply observe that our algorithm for detecting roots in $(R^{*})^{n}$ trivially extends to root detection in $R_{+}^{n}$: Any root of $f$ in $R_{+}^{n}$ must lie in some coordinate subspace $L$ of minimal positive dimension. So, on $L$, the $n$-variate $(n + 1)$-nomial $f$ would restrict to an $f' \in F_{n',n'+1}^{*}$ with $n' \leq n$ and support a subset of the columns of a submatrix of $A$. So then, we must check whether (a) all the coefficients of $f'$ have the same sign or (if not), (b) a submatrix of $[a_{2} - a_{1}, \ldots, a_{n+1} - a_{1}]$ has an odd entry. In other words, $f$ has a root in $R_{+}^{n} \iff f$ has a root in $(R^{*})^{n} \cup \{0\}$. Since checking whether $f$ vanishes at $0$ is the same as checking whether $f$ is missing a constant term, checking for roots in $R_{+}^{n}$ is thus also in NC$^{1}$.

Remark 3.1. Note that checking whether a given $f \in F_{n,n+2}^{*}$ lies in $F_{n,n+2}^{*}$ can be done within NC$^{2}$: one simply finds $d = \dim$ Supp($f$) in NC$^{2}$ by computing the rank of the matrix whose columns are $a_{2} - a_{1}, \ldots, a_{n+1} - a_{1}$ (via the parallel algorithm of Canny [CSa76]), and then checks whether $d = n$.

Assertion (1): The algorithm we use to prove $\text{FEAS}_{1}(F_{n,n+2}^{*}) \subseteq P$ for fixed $n$ is described just below. Note also that once we have $\text{FEAS}_{1}(F_{n,n+2}^{*}) \subseteq P$ for fixed $n$, it easily follows that $\text{FEAS}_{1}(F_{n,n+2}^{*}) \subseteq P$: The polynomial obtained from an $f \in F_{n,n+2}^{*}$ by setting any non-empty subset of its variables to $0$ clearly lies in $F_{n',n'+2}^{*}$ for some $n' < n$ (modulo a permutation of variables). Thus, since we can apply changes of variables like $x_{i} \mapsto -x_{i}$ in $P$, and since there are exactly $3^{n}$ sequences of the form $(e_{1}, \ldots, e_{n})$ with $e_{i} \in \{0, \pm 1\}$ for all $i$, it thus clearly suffices to show that $\text{FEAS}_{1}(F_{n,n+2}^{*}) \subseteq P$ for fixed $n$.

We thus need only prove correctness, and a suitable complexity bound, for the following algorithm:

**Algorithm 3.2.**

**Input:** A coefficient vector $c := (c_{1}, \ldots, c_{n+2})$ and a (possibly degenerate) circuit $A = (a_{1}, \ldots, a_{n+2})$ of cardinality $n + 2$.

**Output:** A true declaration as to whether $Z_{+}(f)$ is empty or not, where $f(x) := \sum_{i=1}^{n} c_{i}x^{i}$.

**Description:**

1. If all the $c_{i}$ have the same sign then output $"Z_{+}(f) = \emptyset"$ and STOP.

2. Let $b = (b_{1}, \ldots, b_{n+2}) \in Z^{n}$ be the vector obtained by applying Lemma 2.13 to $A$. If $b \equiv -b$ has a unique negative coordinate $b_{j}$, and $c_{j}$ is the unique negative coordinate of $c$ or $-c$, then do the following:
   a) Replace $b$ by $-\text{sign}(b)_{j}b$, replace $c$ by $-\text{sign}(c)_{j}c$, and then reorder $b$, $c$, and $A$ by the same permutation so that $b_{j} < 0$ and $|b_{j}| > 0$ iff $i < j'$.
(b) If \( j' < n + 2 \) and
\[
b_{j'}^b \Pi_{i=1}^{j'-1} c_i^{-b_i} = c_{j'}^{-b_{j'}} \Pi_{i=1}^{n+1} b_i \]
then output \( \text{“}Z_+(f) = \emptyset\text{”} \) and STOP.

(c) Decide via Algorithm 2.17 whether
\[
b_{j'}^b \Pi_{i=1}^{j'-1} c_i^{-b_i} > c_{j'}^{-b_{j'}} \Pi_{i=1}^{n+1} b_i.\]
If so, output \( \text{“}Z_+(f) = \emptyset\text{”} \) and STOP.

3. Output \( “Z_+(f) \text{ is non-empty!”} \) and STOP.

The correctness of Algorithm 2.12 follows directly from Theorems 2.10 and 2.18. In particular, note that \( b_i \) is simply the signed volume of \( \text{Conv}(A \setminus \{a_i\}) \). So the geometric interpretation of \( b \) or \(-b\) having a unique negative coordinate is that the convex hull of the unique non-degenerate subcircuit of \( A \) is a simplex, with \( a_i \) lying in its relative interior. Similarly, the geometric interpretation of \( j' < n + 2 \) is that \( A \) is a non-degenerate circuit. Finally, the product comparisons from Steps (b) and (c) simply decide the product inequalities stated in Theorem 2.18 and Theorem 2.19.

So now we need only bound complexity, and this follows immediately from Lemma 2.17 (assuming we use Algorithm 2.15 for Step (b)).

It is worth noting that we need to compute the sign of a linear combination of logarithms only when the unique non-degenerate subcircuit \( B \) of \( A \) is a simplex, and all “vertex” coefficients have sign opposite from the “internal” coefficient. Also, just as in Remark 2.1, checking whether a given \( f \in \mathcal{F}_{n,n+2} \) lies in \( \mathcal{F}_{n,n+2}^{\text{NC}} \) can be done within \( \text{NC}^2 \) by computing \( d = \dim \text{Supp}(f) \) efficiently. Moreover, from our preceding proof, we see that deciding whether a circuit is degenerate (and extracting \( B \) from \( A \) when \( A \) is degenerate) can be done in \( \text{NC}^2 \) as well, since we can set \( \beta = 1 \) if we only want the signs of \( b_1, \ldots, b_{n+2} \).

Acknowledgements

The authors thank Francisco Santos for earlier discussions on counting regular triangulations, and Frank Sottile for inviting the second author to an April 2008 meeting at the Institute Henri Poincare where a version of these results was presented. Thanks also to Dima Pasechnik for discussions, and Sue Geller and Bruce Reznick for detailed commentary, and Ivan Moskovich for discussions on Random Analytic Surfaces and Complexity, Coding, and Communication. Finally, we thank Philip Pêbay and David C. Thompson for their great hospitality at Sandia National Laboratories where this paper was completed.

4. REFERENCES

[AM09] Avendaño, Martin and Mortari, Daniele, “The Multi-Impulse Orbit Transfer Problem,” preprint, Texas A&M University, 2009.

[AR09] Avendaño, Martin and Rojas, J. Maurice, “A Critical Radius for Low Complexity,” in preparation, 2009.

[Bil79] Bach, Eric and Shallit, Jeff, Algorithmic Number Theory, Vol. I: Efficient Algorithms, MIT Press, Cambridge, MA, 1996.

[Bak77] Baker, Alan, “The Theory of Linear Forms in Logarithms,” in Transcendence Theory: Advances and Applications: proceedings of a conference held at the University of Cambridge, Cambridge, Jan.–Feb., 1976, Academic Press, London, 1977.

[BHRPR09] Bastani, Osbert; Hillar, Chris; Popov, Dimitar; and Rojas, J. Maurice, “Sums of Squares, Randomization, and Sparse Polynomials,” in preparation, 2009.

[BG-V03] Basu, Saugata and Gonzalez-Vega, Laureano, Algorithmic and Quantitative Real Algebraic Geometry, Papers from the DIMACS Workshop on Algorithmic and Quantitative Aspects of Real Algebraic Geometry in Mathematics and Computer Science held at Rutgers University, Piscataway, NJ (March 12–16, 2001), DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 60.

[BPR06] Basu, Saugata; Pollack, Ricky; and Roy, Marie-Francoise, Algorithms in Real Algebraic Geometry, Algorithms and Computation in Mathematics, vol. 10, Springer-Verlag, 2006.

[Ber] Bernstein, Daniel J., “Computing Logarithm Intervals with the Arithmetic-Geometric Mean Iterations,” available from http://cr.yp.to/papers.html.

[Ble] Blekherman, Grigory, “Convexity properties of the cone of nonnegative polynomials,” Discrete Comput. Geom. 32 (2004), no. 3, pp. 345–371.

[Cay88] Canny, John F., “Some Algebraic and Geometric Computations in \( \text{PSPACE} \),” Proc. 20th ACM Symp. Theory of Computing, Chicago, (1988), ACM Press.

[Csa76] Csanky, L., “Fast Parallel Matrix Inversion Algorithms,” SIAM J. Comput. 5 (1976), no. 4, pp. 618–623.

[DRRS07] Dickenstein, Alicia; Rojas, J. Maurice; Rusek, Korben; and Shih, Justin, “A-Discriminants and Extremal Real Algebraic Geometry,” Moscow Mathematical Journal, vol. 7, no. 3, (July–September, 2007).

[DL79] Dobkin, David and Lipton, Richard, “On the Complexity of Computations Under Varying Sets of Primitives,” J. of Computer and System Sciences 18, pp. 86–91, 1979.

[VD82] van der Dries, Lou, “A generalization of the Tarski-Seidenberg theorem, and some nondefinability results,” Bull. Amer. Math. Soc. (N.S.) 15 (1986), no. 2, pp. 189–193.

[VD98] van der Dries, Lou, Tame topology and o-minimal structures, London Mathematical Society Lecture Note Series, 248, Cambridge University Press, Cambridge, 1998.

[EMP06] Algebraic geometry and geometric modeling, papers from a workshop held at University of Nice-Sophia Antipolis, Nice, Sept. 27–29, 2004, (edited by Mohamed Elkadi, Bernard Mourrain and Ragni Piene), Mathematics and Visualization, Springer-Verlag, Berlin, 2006.

[GV04] Gabrielov, Andrei and Vorobjov, Nicolai, “Complexity of computations with Pfaffian and Noetherian functions,” Normal Forms, Bifurcations and Finiteness Problems in Differential Equations, pp. 211–250, Kluwer, 2004.

[GJ79] Garey, Michael R. and Johnson, David S.
Complexity, special issue for the 2002 Foundations of Computation Mathematics (FOCM) meeting, February 2005, pp. 87–110.

[RS99] Rojas, J. Maurice and Sethuraman, Swaminathan, “Refined Asymptotics for Sparse Sums of Squares,” extended abstract, submitted for publication. Also available as Math Arxiv preprint 0901.3786.

[Sch00] Schmid, Joachim, “On the Complexity of the Real Nullstellensatz in the 0-Dimensional Case,” J. Pure Appl. Algebra 151 (2000), no. 3, pp. 301–308.

[Sma87] Smale, Steve, “On the Topology of Algorithms I,” Journal of Complexity 3 (1987), no. 2, pp. 81–89.

[Sto98] Storjohann, Arne, “Computing Hermite and Smith normal forms of triangular integer matrices,” Linear Algebra Appl. 282 (1998), no. 1–3, pp. 25–45.

[Ste74] Stengle, G., “A nullstellensatz and a positivstellensatz in semialgebraic geometry,” Math. Ann. 207 (1974) pp. 87–97.

[Sus79] Sussmann, Héctor J., “Subanalytic sets and feedback control,” J. Differential Equations 31 (1979), no. 1, pp. 31–52.

[Tar51] Tarski, Alfred, A Decision Method for Elementary Algebra and Geometry, prepared for publication by J. C. C. McKinsey, University of California Press, Berkeley and Los Angeles, California, 1951.

Appendix: Complexity, Viro Diagrams, and Postponed Proofs

4.1 Complexity Classes and 3CNFSAT

A complete and rigorous description of the complexity classes we used can be found in [Pap95]. So for the convenience of the reader, we briefly review the following definitions:

NC The family of functions computable by Boolean circuits with size polynomial in the input size and depth $O(\log^*\text{InputSize})$.

P The family of decision problems that can be done within time polynomial in the input size.

NP The family of decision problems where a “Yes” answer can be verified within time polynomial in the input size.

PSPACE The family of decision problems solvable within polynomial-time, provided a number of processors exponential in the input size is allowed.

Definition 4.1. Recall that 3CNFSAT is the problem of deciding whether an $n$-variate Boolean formula of the form $B(X) = C_1(X) \land \cdots \land C_N(X)$ has a satisfying assignment, where each clause $C_i$ is of one of the following forms:

\[ X_i \lor \neg X_j \lor X_k, \quad X_i \lor \neg X_j \lor \neg X_k, \quad X_i \lor X_j \lor X_k, \quad X_i \lor X_j \lor \neg X_k, \]

$i, j, k \in [n]$ are pairwise distinct, $\lceil \frac{n}{3} \rceil \leq N \leq 8 \left\lfloor \frac{n}{3} \right\rfloor$, and a satisfying assignment consists of an assignment of values from $\{\text{True}, \text{False}\}$ to the variables $X_1, \ldots, X_n$, yielding the equality $B(X) = \text{True}$ [GJ79]. We then define size$(B) := ^{\text{This is the one time we will mention circuits in the sense of complexity theory: Everywhere else in this paper, our circuits will be combinatorial objects as in Definition 2.9}}$
3N, \(a(x_1, x_2, x_3) := (x_1 - 2)(x_2 - 2)(x_3 - 2)\), and \(b(x_1) := (x_1 - 1)x_1 - 2\). Finally, to any 3CNFSAT clause \(C_i\) as above, we associate a \(4 \times 3\) polynomial system \(H_{C_i}\) as follows: we respectively map clauses of the form \(X_i \lor X_j \lor X_k\), \(X_i \lor X_j \lor \neg X_k\), \(X_i \lor \neg X_j \lor \neg X_k\), \(\neg X_i \lor \neg X_j \lor \neg X_k\) to quadruples of the form

\[
(a(x_1, x_2, x_3), b(x_1), b(x_2), b(x_3)),
\]

and we associate to the 3CNFSAT instance \(B(X)\) an \((8N - n) \times (8N - n)\) polynomial system with integral coefficients, \(F_B\), defined to be

\[
(H_{C_1}, \ldots, H_{C_{\Sigma}}, (u_{1, 1} - 1(v_{1, 1} - 1), \ldots, (u_{4N - n} - 1(v_{4N - n} - 1)).
\]

In particular, assigning True (resp. False) to \(X_i\) will correspond to setting \(x_i = 2\) (resp. \(x_i = 1\)).

Note that \(F_B\) has a natural and well-defined zero set in \((P^1)^{8N - n}\) since its Newton polytopes are either axis-parallel line segments or 3-cubes, and we can multihomogenize with \(8N - n\) extra variables.

**Proof of Proposition 2.2** Assertions (1) and (2) of Proposition 2.2 are elementary. In particular, the last \(4N - n\) polynomials of \(F_B\) simply ensure that \(F_B\) has enough variables so that it is square. Assertion (3) follows easily from the classical Arithmetic-Geometric Inequality [HLPS89 Sec. 2.5, pp. 16–18]. Assertion (4) follows easily upon observing the inequalities \(k \leq \left(k^1/e\right)^2 = M^k < (n + M)^k\) and the fact that \(\text{Newt}(t M) = M\)-dimensional.

### 4.2 Digression on Viro Diagrams

Let us recall an elegant result of Oleg Viro on the classification of certain real algebraic hypersurfaces. In what follows, we liberally paraphrase from Proposition 5.2 and Theorem 5.6 of [GKZ91 Ch. 5, pp. 378–393].

**Definition 4.2.** Given any finite point set \(A \subset \mathbb{R}^n\), let us call any function \(\omega : A \rightarrow \mathbb{R}\) a lifting, denote by \(\pi : \mathbb{R}^{n+1} \rightarrow \mathbb{R}^n\) the natural projection which forgets the last coordinate, and let \(\hat{A} := \{(a, \omega(a)) \mid a \in A\}\). We then say that the polyhedral subdivision \(\Sigma_\omega\) of \(A\) defined by \(\pi(Q) = Q\) a lower facet of \(\text{Conv}\hat{A}\) of dimension \(\dim\hat{A}\) is induced by the lifting \(\omega\), and we call \(\Sigma_\omega\) a lifting induced by a lifting if every cell of \(\Sigma_\omega\) is a simplex. Finally, given any \(f(x) := \sum_{a \in A} c_a x^a \in \mathbb{Z}[x_1, \ldots, x_n]\), we define \(f_{\omega, c}(x) := \sum_{a \in A} c_a \omega(a)x^a\) as the toric perturbation of \(f\) (corresponding to the lifting \(\omega\)).

**Definition 4.3.** Following the notation above, suppose \(\dim\hat{A} = n\) and \(A\) is equipped with a triangulation \(\Sigma\) induced by a lifting and a function \(\omega : A \rightarrow \{\pm\}\) which we will call a distribution of signs for \(A\). We then locally define a piece-wise linear manifold — the Viro diagram \(V_{A}(\Sigma, s)\) — in the following local manner: For any \(n\)-cell \(C \subset \Sigma\), let \(L_C\) be the convex hull of the set of midpoints of edges of \(C\) with vertices of opposite sign, and then define \(V_{A}(\Sigma, s) := \bigcup_{C \in \text{an}\ n\text{-cell}} L_C\). When \(A = \text{Supp}(f)\) and \(s\) is the corresponding sequence of coefficient signs, then we also call \(V(f) := V_{A}(\Sigma, s)\) the Viro diagram of \(f\).

---

**Example 4.4.** The following figure illustrates 6 circuits of cardinality 4, each equipped with a triangulation induced by a lifting, and a distribution of signs. The corresponding (possibly empty) Viro diagrams are drawn in thicker lines.

**Viro's Theorem.** Suppose \(f(x) = \sum_{a \in A} c_a x^a\) is in \(\mathbb{R}[x_1, \ldots, x_n]\) with \(\text{Supp}(f) = A\) and \(\dim\hat{A} = n\), \(\omega\) is any lifting of \(A\), and define \(s_f(a) = \text{sign}(c_a)\) for all \(a \in A\). Then for any sufficiently small \(\varepsilon > 0\), \(Z_+(f_{\omega, \varepsilon})\) is isotopic to \(V_{\Sigma}(\Sigma, s_f)\). In particular, \(V_{\Sigma}(\Sigma, s_f)\) is a disjoint finite union of piece-wise linear manifolds, each possibly having a non-empty boundary.

**Lemma 4.5.** Suppose \(A\) is a circuit, \(\Sigma\) is a triangulation of \(A\), \(n = \dim\hat{A}\), and \(s\) is any distribution of signs on \(A\). Then \(Z_+(f)\) smooth \(\Rightarrow Z_+(f)\) is isotopic to \(V_{\Sigma}(\omega, s_f)\) \(\text{and} \partial V_{\Sigma}(\Sigma, s_f)\) for some \(\Sigma\).

**Proof of Lemma 4.5.** By Lemma 4.4 it easily follows that \(A\) has at most 2 discriminant chambers in \(R_+^{n+2}\), and each such chamber contains a unique toric perturbation. Since the topology of \(Z_+(f)\) is constant on any discriminant chamber containing \(f\) by Lemma 2.1, we are done.

Another important consequence of Viro's Theorem deals with how "roots at infinity" sometimes imply the existence of non-compact connected components for a positive zero set.

**Lemma 4.6.** Assume \(f\) has support such that every facet of \(\text{Newt}(f)\) is a simplex and coefficients such that \(V(f)\) intersects \(\partial \text{Newt}(f)\) for every underlying triangulation. Then \(Z_+(f)\) has a non-compact connected component.

Employing our current notation, Lemma 4.4 follows directly from Lemma 15 of [LRW03].

### 4.3 More Postponed Proofs

**Proof of Lemma 2.5.** Lemma 2.5 follows immediately from the following well-known factorization for integer matrices and its recent complexity bounds.

**Definition 4.7.** [Hi82, Sto98] Given any \(M \in \mathbb{Z}^{m \times n}\), the Hermite factorization of \(M\) is an identity of the form \(UMV = M\) where \(U \in \mathbb{G}_{m\times m}\) and \(H = [h_{ij}] \in \mathbb{Z}^{m \times n}\) is non-negative and upper triangular, with all off-diagonal entries smaller than the positive diagonal entry in the same column. Finally, the Smith factorization of \(M\) is an identity of the form \(UMV = S\) where \(U \in \mathbb{G}_{m\times m}, V \in \mathbb{G}_{n\times n}\), and \(S = [s_{ij}] \in \mathbb{Z}^{m \times n}\) is diagonal, with \(s_{ij}\) for all \(i\).
Proof of Lemma 2.6: Computing our desired canonical form \( f \) boils down to reordering monomials, performing a monomial change of variables, and a rescaling.

First, let us replace \( f \) by \( \text{sign}(c_1) f \) and reorder the terms of \( f \) supported on \( \{a_2, \ldots, a_{n+1}\} \) so that \( c_2, \ldots, c_{n+1} \) (resp. \( c_{n+2}, \ldots, c_{2n+1} \)) are positive (resp. negative), for some unique \( n' \in \{1, \ldots, n, n+1\} \). We then form the \( n \times n \) matrix \( B \) whose \( i \times j \) column is \( a_{i+1} - a_i \), for \( i \in \{1, \ldots, n\} \). If necessary, let us also swap the terms supported on \( \{a_2, a_3\} \) (or \( \{a_n, a_{n+1}\} \)), before defining \( B \), so that det \( B > 0 \) and the sign condition defining \( \ell \) is still preserved. (If \( n = 1 \) then we can simply reorder terms so that \( a_1 < a_2 \) and define \( B \) accordingly.)

Letting \( \tilde{f}(x) := f_{\frac{n'}{n'+1}} \) we then obtain by Proposition 2.4 that \( Z_1(f) \) and \( Z_1(\tilde{f}) \) are diffeotopic. Moreover, we clearly have that \( \tilde{f}(x) := c_0 + c_2 x_1 + \cdots + c_{n+1} x_n \) (remember we have permuted the terms of \( f \), and thus the \( c_i \) as well) where \( c_1 > 0 \). So we can now define \( \tilde{f}(x) \) to be \( \tilde{f}(\frac{x_{(1)} \cdots x_{(n+1)}}{n+1}) \), define \( \gamma \) to be the constant term of \( \tilde{f} \), and set \( \ell := \ell - 1 \). It is then easily verified that the coefficients of \( x_1, \ldots, x_\ell \) (resp. \( x_{\ell+1}, \ldots, x_n \)) are all 1 (resp. \( -1 \)).

Since \( \tilde{f} \) was defined by rescaling the variables of \( \tilde{f} \), and reorder the terms accordingly.

\begin{itemize}
  \item **Assertion (1):** Employing the canonical form \( \tilde{f}(x) = \gamma + \sum_{i=1}^{\ell} x_i - x_{\ell+1} - \cdots - x_n \) of Lemma 2.6 (with \( \ell > 0 \) and \( \ell \in \{0, \ldots, n\} \), by construction), the desired equivalence will follow upon proving that \( \tilde{f} \) has a root in \( \mathbb{R}^{\ell} \leftrightarrow \ell < n \). The latter equivalence is trivially true. By Lemma 2.6 once more, the statement on diffeotopy type can be reduced to the special case of \( \tilde{f} \), which is also immediate.
  \item **Assertion (2):** Dividing by a suitable monomial term, we can clearly assume that \( a_1 = 0 \) and all the coefficients of \( f \) are positive. So it suffices to prove that \( f \) has a root in \( \mathbb{R}^{\ell} \leftrightarrow \ell \) there are indices \( i \in [n] \) and \( j \in \{2, \ldots, n+1\} \) with \( a_{i,j} \neq 0 \). Writing \( f(x) := c_0 + c_2 x_2 + \cdots + c_{n+1} x_{n+1} \), let us now prove the last equivalence.
\end{itemize}

First, recall that subanalytic sets are those sets defined by projections of feasible sets of systems of analytic inequalities. In particular, \( C \) is a subanalytic set, and \( C \) is thus path connected since \( C \) admits a decomposition into connected cells. The existence of such a decomposition follows immediately from the \( \omega \)-minimality of subanalytic sets \( \text{vd} \text{D97} \). Moreover, \( C \) is path connected via differentiable paths by the classical density of \( C^* \) functions among \( C^1 \) functions (see, e.g., Hir94 Ch. 2).

So let \( m = \#A \) and let \( \phi := [0_1, \cdots, \phi_m] : [0, 1] \to C \) be any differentiable path connecting \( f \) and \( g \). Also let \( T \) be the positive part of the real toric variety corresponding to \( \text{Conv}(A) \), \( I_A := \{(t, x) \in \mathbb{R}^{n-1} \times T \mid \sum_{i=1}^{n-1} c_i x_i = 0\} \) the underlying (real) incidence manifold, and let \( \pi \) denote the natural projection mapping \( \mathbb{R}^{n-1} \times T \to \mathbb{R}^{n-1} \). Note then that \( \phi \) induces an embedded smooth compact submanifold \( M \subseteq I_A \), consisting of all those \((t, x)\) with \( c = \phi(t) \) and \( \sum_{i=1}^{n-1} c_i x_i = 0 \) for some \( t \). In particular, we see that \( M \) is fibered over \([0, 1]\) and that \( \psi = \phi^{-1} \circ \pi \) is a Morse function on \( M \) with no critical points in \([0, 1]\). More to the point, we obtain a natural flow on \( M \) inducing a diffeotopy \( \delta \) between the zero sets of \( f \) and \( g \) in \( T \) [Hir94] Thm. 2.2, pg. 153].

To conclude, we simply observe that the intersection of \( \psi^{-1}(t) \) with toric infinity is smooth for all \( t \in [0, 1] \) (by our assumption on the facets of \( \text{Conv}(A) \)) and so \( \delta \) restricts to a diffeotopy between \( Z_1(f) \) and \( Z_1(g) \).

\begin{proof}[Proof of Lemma 2.17]
We first recall the following theorem:

**Theorem 4.9. [BS96] Thm. 4.8.7, Sec. 4.8** Following the notation of Definition 2.12, there is a \( \text{gcd} \)-free basis for \( \{\alpha_1, \ldots, \alpha_N\} \), with \( \eta_i, \text{size}(\gamma_i) \), and \( \text{size}(\varepsilon_j) \) each polynomial in \( \sum_{i=1}^{N} \text{size}(\alpha_i) \), for all \( i \) and \( j \). Moreover, one can always find such a \( \text{gcd} \)-free basis using just \( O\left( \left( \sum_{i=1}^{N} \text{size}(\alpha_i) \right)^2 \right) \) bit operations.

Returning to the proof of Lemma 2.17, note then that Algorithm 2.16 is correct and runs in the time stated by Theorem 4.9 and the naive complexity bounds for integer multiplication.

To prove the remaining half of our lemma, observe that the sign of \( \alpha_1^1 \cdots \alpha_n^M - \beta_1^1 \cdots \beta_n^M \) is the same as the sign of \( S := \sum_{i=1}^{N} u_i \log \alpha_i - \sum_{i=1}^{N} v_i \log \beta_i \). Clearly then, \( |S - \left( \sum_{i=1}^{N} u_i A_i - \sum_{i=1}^{N} v_i B_i \right) | < E/2 \) by the Nesterenko-Matveev Theorem. So Step (3) of Algorithm 2.16 indeed computes the sign of \( S \) and we thus obtain correctness.

To see that Algorithm 2.16 runs within the time stated, first note that the algorithm computes \( M \) (resp. \( N \)) approximations of logs of positive integers, each of size \( O(\max \log |\alpha_i|) \).
First we observe that via an argument almost identical to the last paragraph, we can conclude by studying the two cases $Z_+(f_B) = \emptyset$ and $\#Z_+(f_B) = 1$, combined with all our assumptions so far.

By Theorem 2.18 applied to $f_B$, we see that Conditions (a) and (b) must hold (and the inequality in (b) strictly so), with the possible exception of the equalities $\text{sign}(c_{j'}) = \text{sign}(c_i)$ for all $i > j'$.

To further simplify matters, observe that if all the coefficients of $f_B$ have the same sign then, by assumption, we must have a coefficient of $f_B$ differing in sign from $c_j$. So then, $f_B(\mathbb{R}_+^{n-j-2})$ contains a ray of the same sign. Therefore $Z_+(f)$ is non-empty. We may therefore also assume that not all the coefficients of $f_B$ have the same sign.

We can therefore conclude by studying the two cases $Z_+(f_B) = \emptyset$ and $\#Z_+(f_B) = 1$, combined with all our assumptions so far.

By Theorem 2.18 applied to $f_B$, we see that Conditions (a) and (b) must hold (and the inequality in (b) strictly so), with the possible exception of the equalities $\text{sign}(c_{j'}) = \text{sign}(c_i)$ for all $i > j'$.

To further simplify matters, observe that if all the coefficients of $f_B$ have the same sign then, by assumption, we must have a coefficient of $f_B$ differing in sign from $c_j$. So then, $f_B(\mathbb{R}_+^{n-j-2})$ contains a ray of the same sign. Therefore $Z_+(f)$ is non-empty. We may therefore also assume that not all the coefficients of $f_B$ have the same sign.

We can therefore conclude by studying the two cases $Z_+(f_B) = \emptyset$ and $\#Z_+(f_B) = 1$, combined with all our assumptions so far.
holds with equality). That $g$ attains only nonnegative values is then clearly equivalent to the inequality
\[ 1 + x_1 + \cdots + x_{j'-2} \geq \gamma x^\alpha \]
which is in turn equivalent to
\[ (1 - \alpha_1 - \cdots - \alpha_{j'-2})(1 + x_1 + \cdots + x_{j'-2}) \geq \prod_{i=1}^{j'-2} \left( \frac{(1 - \alpha_1 - \cdots - \alpha_{j'-2})x^\alpha}{\alpha_i} \right)^{a_i} \]
or
\[ (1 - \alpha_1 - \cdots - \alpha_{j'-2}) + \alpha_1 u_1 + \cdots + \alpha_{j'-2} u_{j'-2} \geq \prod_{i=1}^{j'-2} u_i^{\alpha_i} \]
upon substituting $x_i = \alpha_i u_i / (1 - \alpha_1 - \cdots - \alpha_{j'-2})$. The last inequality is simply the weighted Arithmetic-Geometric Inequality [HLP88] so we are done. ■