Computing Complex Dimension Faster and Deterministically (Extended Abstract)

J. Maurice Rojas*

Department of Mathematics
City University of Hong Kong
83 Tat Chee Avenue
Kowloon, HONG KONG
mamrojas@math.cityu.edu.hk
http://math.cityu.edu.hk/~mamrojas

1 Introduction and Main Results

We give a new complexity bound for calculating the complex dimension of an algebraic set. Our algorithm is completely deterministic and approaches the best recent randomized complexity bounds. We also present some new, significantly sharper quantitative estimates on **rational univariate representations (RUR)** of roots of polynomial systems. As a corollary of the latter bounds, we considerably improve a recent algorithm of Koiran for deciding the emptiness of a hypersurface intersection over $\mathbb{C}$, given the truth of the Generalized[1] Riemann Hypothesis (GRH).

Let $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$, $\boldsymbol{F} := (f_1, \ldots, f_m)$, and let Z_F be the complex zero set of F. We will first consider the complexity of computing the complex dimension $\dim Z_F$ relative to the BSS model over $\mathbb{C}$. (See [BCSS98] for further background on this computational model.)

First recall the usual notions of input size: With the Turing model, we will assume that any input polynomial is given as a sum of monomial terms, with all coefficients **and** exponents written in, say, base 2. The corresponding notion of **sparse size** is then simply the total number of bits in all coefficients and exponents. For example, the sparse size of $x_1^D + ax_1^3 + b$ is $\mathcal{O}(\log D + \log a + \log b)$. The sparse size can be extended to the BSS model over $\mathbb{C}$ simply by counting just the total number of bits necessary to write down the exponents (thus ignoring the size of the coefficients).

Curiously, efficient **randomization-free** algorithms for computing $\dim Z_F$ are hard to find in the literature. So we present such an algorithm, with an explicit complexity bound.

Theorem 1 *Let D the maximum of the total degrees of $f_1, \ldots, f_m$. Also let $\mathbf{O}$ be the origin, and $e_1, \ldots, e_n$ the standard basis vectors, in $\mathbb{R}^n$. Normalize n-dimensional volume $\mathrm{Vol}_n(\cdot)$ so that the standard n-simplex (with vertices $\mathbf{O}, e_1, \ldots, e_n$) has n-volume 1. Finally, let k be the total number of monomial terms in F, counting reptitions between distinct f_i. Then there is a deterministic algorithm which computes $\dim Z_F$ within $\mathcal{O}(n^{2.312} 11^n k V_F^{7.376})$ arithmetic operations, where $V_F := \mathrm{Vol}_n(Q_F)$ and Q_F is the convex hull of[2] the union of $\{\mathbf{O}, e_1, \ldots, e_n\}$ and the set of all exponent vectors of F.*

Via a height[3] estimate from theorem 3 later in this section one can also derive a similar bound on the bit complexity of dimension computation. We clarify the benefits of our result over earlier bounds in section 1.1 and give an example in section 1.2. The algorithm for theorem 1, and its correctness proof, are stated in section 2.

*May 3, 2000 version. This research was partially supported by a Hong Kong CERG grant.

[1] The **Riemann Hypothesis (RH)** is an 1859 conjecture equivalent to a sharp quantitative statement on the distribution of primes. GRH can be phrased as a generalization of this statement to prime ideals in an arbitrary number field. Further background on these RH's can be found in [LO77, BS96].

[2] i.e., smallest convex set in $\mathbb{R}^3$ containing...

[3] The (absolute logarithmic) **height** of an algebraic number can be defined as the sparse size of its minimal polynomial. An analogous characterization of this important number-theoretic invariant can also be given for any algebraic point in $\mathbb{C}^n$ [Sil95, Mal00b, KPS00].

There is, however, a fundamentally different approach which, given the truth of GRH, places a special case of the above problem in an even better complexity class. In particular, let **HN** denote the problem of deciding whether Z_F empty, given that the coefficients of all f_i are integers. Then by a recent result of Koiran [Koi96], we know that $\mathbf{HN} \in \mathbf{AM}$, given the truth of GRH. Koiran's conditional result gives the smallest complexity class known to contain **HN**. (Without GRH, we only know that $\mathbf{HN} \in \mathbf{PSPACE}$ [Can88].) Indeed, independent of GRH, while it is known that $\mathbf{NP} \subseteq \mathbf{AM} \subseteq \mathbf{PSPACE}$ [Pap95], the properness of each inclusion is still an open problem.

The simplest summary of Koiran's algorithm is that it uses reduction modulo specially selected primes to decide feasibility over $\mathbb{C}$. (His algorithm is unique in this respect since all previous algorithms for **HN** worked primarily in the ring $\mathbb{C}[x_1, \ldots, x_n]/\langle F\rangle$.) The key observation behind Koiran's algorithm is that an F infeasible (resp. feasible) over $\mathbb{C}$ will have roots in $\mathbb{Z}/p\mathbb{Z}$ for only finitely many (resp. a positive density of) primes p. (We give an explicit example of an improved version of Koiran's algorithm a bit later in section 1.2.)

A refined characterization of the difference between positive and zero density, which significantly improves Koiran's algorithm, can be given in terms of our framework as follows:

Theorem 2 *Following the notation above, assume now that* $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ *and let* $\sigma(F)$ *be the maximum of* $\log|c|$ *as* c *ranges over the coefficients of all the monomial terms of* F. *Then there exist* $a_F, A_F \in \mathbb{N}$, *with the following properties:*

(a) F *infeasible over* $\mathbb{C} \Longrightarrow$ *the reduction of* F *mod* p *has a root in* $\mathbb{Z}/p\mathbb{Z}$ *for at most* a_F *distinct primes* p.

(b) *Given the truth of GRH,* F *feasible over* $\mathbb{C} \Longrightarrow$ *for each* $t \geq 4963041$, *the sequence* $\{A_F t^3, \ldots, A_F(t+1)^3 - 1\}$ *contains a prime* p *such that the reduction of* F *mod* p *has a root in* $\mathbb{Z}/p\mathbb{Z}$.

(c) *We have* $a_F = \mathcal{O}(n^3 D V_F(4^n D \log D + \sigma(F) + \log m))$ *and* $A_F = O([\frac{e^n}{\sqrt{n}} V_F(\sigma(F) + m(n \log D + \log m))]^4)$.

In particular, the bit-sizes of a_F *and* A_F *are both* $\mathcal{O}(n \log D + \log \sigma(F))$ *— sub-quadratic in the sparse size of* F. *Simple explicit formulae for* a_F *and* A_F *appear in remarks 5 and 6 of section 2.*

The proof of theorem 2 is based in part on a new, highly refined version of effective univariate reduction.

Theorem 3 *Following the notation above, and the assumptions of theorem 2, there exist a univariate polynomial* $h_F \in \mathbb{Z}[u_0]$ *and a point* $u_F := (u_1, \ldots, u_n) \in \mathbb{Z}^n$ *with the following properties:*

0. *The degree of* h_F *is* $\leq V_F$.

1. *For any irreducible component* W *of* Z_F, *there is a point* $(\zeta_1, \ldots, \zeta_n) \in W$ *such that* $u_1\zeta_1 + \cdots + u_n\zeta_n$ *is a root of* h_F. *Conversely, if* $m \leq n$, *all roots of* h_F *arise this way.*

2. F *has only finitely many complex roots* $\Longrightarrow$ *the splitting field of* h_F *over* $\mathbb{Q}$ *is exactly the field* $\mathbb{Q}[x_i \mid (x_1, \ldots, x_n) \in \mathbb{C}^n$ *is a root of* $F]$.

3. *The coefficients of* h_F *satisfy* $\sigma(h_F) = \mathcal{O}(\frac{e^n}{\sqrt{n}} V_F(\sigma(F) + m(n \log D + \log m)))$.

4. $m \leq n \Longrightarrow$ *the deterministic arithmetic complexity of computing* u_F, *and all the coefficients of* h_F, *is* $\mathcal{O}(n^{1.312} 11^n V_F^{7.376})$.

5. *We have* $\log(1 + |u_i|) = \mathcal{O}(n^2 \log D)$ *for all* i.

Note that we have thus obtained the existence of points of bounded height on the positive-dimensional part of Z_F, as well as a bound on the height of any point in the zero-dimensional part of Z_F. Put more simply, via a slight variation of the proof of theorem 3, we obtain the following useful bound:

Theorem 4 *Following the notation of theorem 3, any irreducible component* W *of* Z_F *contains a point* $(\zeta_1, \ldots, \zeta_n)$ *such that for all* i, *either* $x_i = 0$ *or* $|\log|x_i|| = \mathcal{O}(\frac{e^n}{\sqrt{n}} V_F(\sigma(F) + m(n \log D + \log m)))$. ■

Our final main result is a refinement of theorem 3 which will also prove quite useful.

Theorem 5 *[Roj99c] Following the notation of theorem 3, one can pick* u_F *and* h_F *(still satisfying (0)–(5)) so that there exist* $a_1, \ldots, a_n \in \mathbb{N}$ *and* $h_1, \ldots, h_n \in \mathbb{Z}[u_0]$ *with the following properties:*

6. *The degrees of* $h_1, \ldots, h_n$ *are all bounded above by* V_F.

7. *For any root* $\theta = u_1\zeta_1 + \cdots + u_n\zeta_n$ *of* h_F, $\frac{h_i(\theta)}{a_i} = \zeta_i$ *for all* i.

8. *For all* i, *both* $\log a_i$ *and* $\sigma(h_i)$ *are bounded above by* $\mathcal{O}(\frac{e^n}{\sqrt{n}} V_F^3(\sigma(F) + m(n \log D + \log m)))$.

9. *$m \leq n \implies$ the deterministic arithmetic complexity of computing all the coefficients of $h_1, \ldots, h_n$ is $\mathcal{O}(n^{2.312} 11^n V_F^{7.376})$.*

Explicit formulae for all these asymptotic estimates appear below in remarks 3, 4, 5, 6, and 8. The proofs for all our results (except theorem 3), appear in section 2. The proof of theorem 3 appears in the appendix. However, let us first compare our results to earlier work.

1.1 Related Results Over $\mathbb{C}$

We point out that we have tried to balance generality, sharpness, and ease of proof in our bounds. In particular, our bounds fill a lacuna in the literature where earlier bounds seemed to sacrifice generality for sharpness, or vice-versa.

To clarify this trade-off, first note that $\mathcal{I}_F \leq V_F \leq D^n$, where $\mathcal{I}_F$ is the number of irreducible components of Z_F. (The first inequality follows immediately from theorem 3, while the second follows from the observation that Q_F always lies in a copy of the standard n-simplex scaled by a factor of D.) So depending on the shape of Q_F, and thus somewhat on the sparsity of F, one can typically expect V_F to be much smaller than D^n. For example, the 3×3 example from section 1.2 below gives $D^n = 13824$ and $V_F = 243$. More generally, it is easy to see that the factor of improvement can even reach D^{n-1}, if not more [Roj00a].

Our algorithm for computing $\dim Z_F$ gives the first deterministic complexity bound which is polynomial in V_F. In particular, while harder problems were already known to admit **PSPACE** complexity bounds, the corresponding complexity bounds were either polynomial (or worse) in D^n, or stated in terms of a non-uniform computational model.[4] Our algorithm for the computation of $\dim Z_F$ thus gives a significant speed-up over earlier work.

For example, via the work of Chistov and Grigoriev from the early 1980's on quantifier elimination over $\mathbb{C}$ [CG84], it is not hard to derive a deterministic complexity bound of $\mathcal{O}((mD)^{n^4})$ for the computation of $\dim Z$. More recently, [GH93] gave a randomized complexity bound of $m^{\mathcal{O}(1)} D^{\mathcal{O}(n)}$. Theorem 1 thus clearly improves the former bound. Comparison with the latter bound is a bit more difficult since the exponential constants and derandomization complexity are not explicit in [GH93].

[4] For example, some algorithms in the literature are stated in terms of **arithmetic networks**, where the construction of the underlying network is not included in the complexity estimate.

As for faster algorithms, one can seek complexity bounds which are polynomial in even smaller quantities. For example, if one has an irreducible algebraic variety $V \subseteq \mathbb{C}^n$ of complex dimension d, one can define its **affine geometric degree**, $\delta(V)$, to be the number of points in $V \cap H$ where H is a generic $(n-d)$-flat. More generally, we can define $\delta(Z_F)$ to be the sum of $\delta(V)$ as V ranges over all irreducible components of Z_F. It then follows (from theorem 1 and a consideration of intersection multiplicities) that $\mathcal{I}_F \leq \delta(Z_F) \leq V_F$. Similarly, one can attempt to use mixed volumes of several polytopes (instead of a single polytope volume) to lower our bounds.

We have avoided refinements of this nature for the sake of simplicity. Another reason it is convenient to have bounds in terms of V_F is that the computation of $\delta(Z_F)$ is even more subtle than the computation of polytopal n-volume. For example, when n is fixed, $\mathrm{Vol}_n(Q)$ can be computed in polynomial time simply by triangulating the polytope Q and adding together the volumes of the resulting n-simplices [GK94]. However, merely deciding $\delta(Z_F) > 0$ is already **NP**-hard for $(m,n) = (2,1)$, via a result of Plaisted [Pla84]. As for varying n, computing $\delta(Z_F)$ is #**P**-hard, while the computation of polytope volumes is #**P**-complete. (The latter result is covered in [GK94, KLS97], while the former result follows immediately from the fact that the computation of $\delta(Z_F)$ includes the computation of V_F as a special case.) More practically, for any fixed $\varepsilon_1, \varepsilon_2 > 0$, there is an algorithm which runs in time polynomial in the sparse encoding of F (and thus polynomial in n) which produces a random variable that is within a factor of $1-\varepsilon_1$ of $\mathrm{Vol}_n(Q_F)$ with probability $1-\varepsilon_2$ [KLS97]. The analogous result for mixed volume is known only for certain families of polytopes [GS00], and the existence of such a result for $\delta(Z_F)$ is still an open problem.

In any event, we point out that improvements in terms of $\delta(Z_F)$ for our bounds are possible, and these will be pursued in a later version of this paper. Similarly, the exponents in our complexity bounds can be considerably lowered if randomization is allowed. Furthermore, Lecerf has recently announced a randomized complexity bound for computing $\dim Z_F$ which is polynomial in $\max_i\{\delta(Z_{(f_1,\ldots,f_i)})\}$ [Lec00].[5] However, the complexity of derandomizing Lecerf's algorithm is not

[5] The paper [Lec00] actually solves the harder problem of computing an algebraic description of a non-empty set of points in every irreducible component of Z_F, and distinguishing which component each set belongs to.

yet clear.

As for our result on prime densities (theorem 2), part (a) presents the best current bound polynomial in V_F. An earlier density bound, polynomial in $D^{n^{\mathcal{O}(1)}}$ instead, appeared in [Koi96].

Part (b) of theorem 2 appears to be new, and makes explicit an allusion of Koiran in [Koi96].

Remark 1 *Pascal Koiran has also given an* **AM** *algorithm (again depending on GRH) for deciding whether the complex dimension of an algebraic set is less than some input constant [Koi97].* ■

Regarding our height bound, the only other results stated in polytopal terms are an earlier version of theorem 3 announced in [Roj99b], and independently discovered bounds in [KPS00, Prop. 2.11] and [Mai00, Cor. 8.2.3]. The bound from [KPS00] applies to a slightly different problem, but implies (by intersecting with a generic linear subspace with reasonably bounded coefficients)[6] a bound of $\mathcal{O}((4^n D \log n + n\sigma)V_F)$ for our setting. Their bound thus results in a slightly stronger exponential dependence on n. The bound from [Mai00, Cor. 8.2.3] uses Arakelov intersection theory, holds only for $m = n$, and the statement is more intricate (involving a sum of several mixed volumes). So it is not yet clear when [Mai00, Cor. 8.2.3] is better than theorem 3. In any case, our result has a considerably simpler proof than either of these two alternative bounds: We use only resultants and elementary linear algebra and factoring estimates.

We also point out that the only earlier bounds which may be competitive with theorem 3, [KPS00, Prop. 2.11], and [Mai00, Cor. 8.2.3] are polynomial in D^n and make various non-degeneracy hypothesis, e.g., $m = n$ and no singularities for Z_F (see [Can87] and [Mal00a, Thm. 5]). As for bounds with greater generality, [FGM90] gives a height bound for general quantifier elimination which, unfortunately, has a factor of the form $2^{(n \log D)^{\mathcal{O}(r)}}$ where r is the number of quantifier alternations.

As for our refinement of theorem 3, the approach of RUR for the roots of polynomial systems is not new, and even dates back to Kronecker. RUR also goes under the name of "effective primitive element theorem" and important precursors to our theorem 5 are stated in [Can88] and [Koi96, Thm. 4]. Nevertheless, the use of **toric resultants** (cf. section 2), which form the core of our algorithms here, was not studied in the context of RUR until the late 1990's (see, e.g., [Roj99c]). Also, theorem 5 appears to be the first statement giving bounds on $\sigma(h_i)$ which are polynomial in V_F. More recently, an algorithm for RUR with randomized complexity polynomial in $\max_i\{\delta(Z_{(f_1,\ldots,f_i)})\}$ was derived in [GLS99]. However, their algorithm makes various nondegeneracy assumptions (such as $m = n$ and that F form a complete intersection) and the derandomization complexity is not stated.

As for the factors in our complexity and height estimates which are explicitly exponential in n (e.g., e^n and 11^n), these can be replaced by a quantity no worse than $\mathcal{O}(n^{2.376})$ in certain cases. In general, this can be done whenever there exists an expression for a particular toric resultant (cf. section 2) as a single determinant, or the divisor of a determinant, of a matrix of size $\mathcal{O}(nV_F)$. The existence of such formulae has been proven in various cases, e.g., when all the Newton polytopes are axis-parallel parallelepipeds [WZ94]. Also, such formulae have been observed (and constructed) experimentally in various additional cases of practical interest [EC93]. Finding compact formulae for resultants is an area of active research which thus has deep implications for the complexity of algebraic geometry.

Finally, we note that we have avoided Gröbner basis techniques because there are currently no known complexity or height bounds polynomial in V_F using these methods for the problems we consider. A further complication is that there are examples of ideals, generated by polynomials of degree ≤ 5 in $\mathcal{O}(n)$ variables, where every Gröbner basis has a generator of degree 2^{2^n} [MM82]. This is one obstruction to deriving sharp explicit complexity bounds via a naive application of Gröbner bases. Nevertheless, we point out that Gröbner bases are well-suited for other difficult algebraic problems, and their complexity is also an area of active research.

1.2 A Sparse 3×3 Example

The solution of sparse polynomial systems is a problem with numerous applications outside, as well as inside, mathematics. The analysis of chemical reactions [GH99] and the computation of equilibria in game-theoretic models [MM95] are but two diverse examples.

More concretely, consider the following system

[6] Martin Sombra pointed this out in an e-mail to the author.

of 3 polynomial equations in 3 variables:

$$\begin{array}{rcl} 144+2x-3y^2+x^7y^8z^9 & = & 0 \\ -51+5x^2-27z+x^9y^7z^8 & = & 0 \\ 7-6x+8x^8y^9z^7-12x^8y^8z^7 & = & 0. \end{array} \qquad (1)$$

Let us see if the system (1) has any **complex** roots and, if so, count how many there are.

Note that the total degree[7] of each polynomial above is 24. By an $18^{\underline{\text{th}}}$-century theorem of Étienne Bézout [Sha94], we can bound from above the number of complex roots of (1), assuming this number is finite, by $24 \cdot 24 \cdot 24 = \mathbf{13824}$. However, a more precise $20^{\underline{\text{th}}}$-century bound can be obtained by paying closer attention to the monomial term structure of (1): Considering the convex hull of the exponent vectors of each equation in (1), one obtains three tetrahedra. These are the **Newton polytopes** of (1), and their **mixed volume**, by a beautiful theorem of David N. Bernshtein from the 1970's [Ber75], turns out to be a much better upper bound on the number of complex roots (assuming there are only finitely many). For our polynomial system (1), this bound is **145**.

Now to decide whether (1) has any complex roots, we can attempt to find a univariate polynomial whose roots are some simple function of the roots of (1). **Elimination theory** allows one to do this, and a particularly effective combinatorial algorithm is given in theorem 1. For example, the roots of $\boldsymbol{P(u)} := 268435456u^{145} - 138160373760u^{137} - 30953963520u^{130} + \cdots - \underline{2947435596503653060289376000}u^{44} + \cdots - 48803823903916800u^2 + 8681150210659989300$ are exactly those numbers of the form $\alpha\beta\gamma$, where (α, β, γ) ranges over all the roots of (1) in $\mathbb{C}^3$. The above **univariate reduction** thus tells us that our example indeed has finitely many complex roots — exactly 145, in fact. The above polynomial took less than 13 seconds to compute using a naive application of **resultants** and factorization on the computer algebra system `Maple`. Interestingly, computing the same univariate reduction via a naive application of **Gröbner bases** (on the same machine with the same version of `Maple`) takes over 3 hours and 51 minutes.

Admittedly, computing polynomials like the one above can be an unwieldy approach to deciding whether (1) has a complex root. An alternative algorithm, discovered by Pascal Koiran in [Koi96] and improved via theorem 2, makes a remarkable simplification depending on conjectural properties of the distribution of prime ideals in number fields.

For instance, an unoptimized implementation of this alternative algorithm would run as follows on our example:

Assumption 1 The truth of the Generalized Riemann Hypothesis (GRH).

Step 1 Pick a (uniformly distributed) random integer $t \in \{10^7, \ldots, 10^7 + 2 \cdot 10^{11}\}$.

Step 2 Via an oracle in **NP**, decide if there is a prime $p \in \{8 \cdot 10^{20} \cdot t^3, \ldots, 8 \cdot 10^{20} \cdot (t+1)^3 - 1\}$ such that the mod p reduction of (1) has a root in $\mathbb{Z}/p\mathbb{Z}$. If so, declare that (1) has a complex root. Otherwise, declare that (1) has no complex root. ■

The choice of the constants above was assisted via our preceding theorems. In particular, the constants are simply chosen to be large enough to guarantee that, under GRH, the algorithm never fails (resp. fails with probability $\leq \frac{1}{3}$) if (1) has a complex root (resp. does not have a complex root). Thus, for our example, the algorithm above will always give the right answer regardless of the random choice in Step 1. Note also that while the prime we seek above may be quite large, the number of **digits** needed to write any such prime is at most **55** — not much bigger than 53, which is the total number of digits needed to write down the coefficients and exponent vectors of (1). For the sake of completeness, we observe that the number of real (resp. rational) roots of (1) is exactly **11** (resp. **0**).

2 Proofs of Our Results Over $\mathbb{C}$: Theorems 1, 3, 4, 5, and 2

While our proof of theorem 2 will not directly require knowledge of resultants, our proofs of theorems 1, 3, 4, and 5 are based on the **toric resultant**.[8] This operator allows us to reduce all the computational algebraic geometry we will encounter to matrix and univariate polynomial arithmetic, with almost no commutative algebra machinery.

Remark 2 *Another advantage of using toric resultants is their algorithmic uniformity. Further-*

[7]The **total degree** of a polynomial is just the maximum of the sum of the exponents in any monomial term of the polynomial.

[8]Other commonly used prefixes for this modern generalization of the classical resultant [Van50] include: sparse, mixed, sparse mixed, $\mathcal{A}$-, $(\mathcal{A}_1, \ldots, \mathcal{A}_k)$-, and Newton. Resultants actually date back to work Cayley and Sylvester in the $19^{\underline{\text{th}}}$ century, but the toric resultant incorporates some combinatorial advances from the late $20^{\underline{\text{th}}}$ century.

more, since our algorithms reduce to standard matrix arithmetic in a particularly structured way, parallelizing is quite straightforward. ■

Since we do not have the space to give a full introduction to resultants we refer the reader to [Emi94, GKZ94, Stu98] for further background. The necessary facts we need are all summarized in the appendix of this paper. In what follows, we let $[j]:=\{1,\ldots,j\}$.

2.1 The Proof of Theorem 1

Our algorithm can be stated briefly as follows:

Step 0 If f_i is indentically 0 for all i, declare that Z_F has dimension n and stop. Otherwise, let $i:=n-1$.

Step 1 For each $j\in[2k+1]$, compute an $(i+1)n$-tuple of integers $(\varepsilon_1(j),\ldots,\varepsilon_n(j),\varepsilon_{(1,1)}(j),\ldots,\varepsilon_{(i,n)}(j))$ via lemma 1 and the polynomial system (2) below.

Step 2 Via theorem 3, check if the polynomial system

$$\begin{aligned}&\varepsilon_1(j)f_1+\cdots+\varepsilon_1(j)^m f_m\\&\qquad+\varepsilon_1(j)^{m+1}l_1+\cdots+\varepsilon_1(j)^{m+i}l_i=0\\&\qquad\qquad\vdots\\&\varepsilon_n(j)f_1+\cdots+\varepsilon_n(j)^m f_m\\&\qquad+\varepsilon_n(j)^{m+1}l_1+\cdots+\varepsilon_n(j)^{m+i}l_i=0\end{aligned}\tag{2}$$

has a root for more than half of the $j\in[2k+1]$, where $l_t:=\varepsilon_{(t,1)}x_1+\cdots+\varepsilon_{(t,n)}x_n$ for all t.

Step 3 If so, declare that Z_F has dimension i and stop. Otherwise, if $i\geq 1$, set $i\mapsto i-1$ and go to Step 1.

Step 4 Via theorem 5 and a univariate gcd computation, check if the system (2) has a root which is also a root of F.

Step 5 If so, declare that Z_F has dimension 0 and stop. Otherwise, declare Z_F empty and stop.

Via the lemma and theorem applied above, we see that Step 2 gives a "yes" answer iff the intersection of $Z_{\tilde F}$ with a generic codimension i flat is finite (and nonempty), where $\tilde F$ is an n-tuple of generic linear combinations of the f_i. Thus Step 2 gives a "yes" answer iff $\dim Z_{\tilde F}=i$. Lemma 7 below tells us that $\dim Z_F=\dim Z_{\tilde F}$ if $\dim Z_F\geq 1$. Otherwise, Step 5 correctly decides whether Z_F is empty whenever Z_F is finite. Thus the algorithm is correct.

As for the complexity of our algorithm, letting $\mathcal{S}$ (resp. $\mathcal{U}$, $\mathcal{U}'$) be the complexity bound from lemma 1 (resp. theorems 3 and 5), we immediately obtain a deterministic arithmetic complexity bound of
$\mathcal{S}+(n-2)(2k+1)\mathcal{U}+\mathcal{U}'+kV_F\mathcal{O}(V_F\log^2 V_F)=$
$\mathcal{O}(k\log k+kn^{2.312}e^{2.376n}V_F^{7.376}+n^{2.312}e^{2.376}V_F^{7.376})$
$=\mathcal{O}(n^{2.312}e^{2.376n}kV_F^{7.376})$. ■

Lemma 1 *Suppose $G(w,v)$ is a formula of the form $\exists x_1\in\mathbb{C}\cdots\exists x_n\in\mathbb{C}$ $(g_1(x,w,v)=0)\wedge\cdots\wedge(g_m(x,w,v)=0)$, where $g_1,\ldots,g_m\in\mathbb{C}[x_1,\ldots,x_n,w_1,\ldots,w_k,v_1,\ldots,v_r]$. Then there is a sequence $v(1),\ldots,v(2k+1)\in\mathbb{C}^r$ such that for all $w\in\mathbb{C}^k$, the following statement holds: $G(w,v(j))$ is true for at least half of the $j\in[2k+1]\iff G(w,v)$ is true for a Zariski-open set of $v\in\mathbb{C}^r$. Furthermore, this sequence can be computed within $\log\sigma+(k+n+r)\log D$ arithmetic operations, where σ (resp. D) is the maximum bit-size of any coefficient (resp. maximum degree) of any g_i.* ■

The above lemma is actually just a special case of theorem 5.6 of [Koi97].

2.2 The Proof of Theorem 4

Since we only care about the size of $|x_i|$, we can simply pick $u_0=-1$, $u_i=1$, all other $u_j=0$, and apply the polynomial h_F from theorem 3. (In particular, differing from the proof of theorem 3, we need not worry if our choice of $(u_1,\ldots,u_n)$ results in two distinct $\zeta\in Z_F$ giving the same value for $\zeta_1u_1+\cdots+\zeta_nu_n$.) Thus, by following almost the same proof as assertion (3) of theorem 3, we can beat the height bound from theorem 3 by a summand of $\mathcal{O}(n^2V_F\log D)$. ■

Remark 3 *Via theorem 8 from the appendix (and a classic root size estimate of Cauchy [Mig92]), we easily see that the asymptotic bound for $|\log|x_i||$ can be replaced by the following explicit quantities:* $\log\left\{\frac{e^{13/6}}{\pi}\sqrt{m_F+1}\cdot 2^{V_F}4^{m_F}\sqrt{2}^{V_F}\sqrt{\mu}^{m_F}(c+1)^{m_F}\right\}$ *if $m\leq n$, or the log of* $\frac{e^{13/6}}{\pi}\sqrt{m_F+1}\cdot 2^{V_F}4^{m_F}\sqrt{2}^{V_F}\times\sqrt{\mu}^{m_F}(m(mV_F+1)^{m-1}c+1)^{m_F}$ *for $m>n$.* ■

2.3 The Proof of Theorem 5

All portions, save assertion (8), follow immediately from [Roj99c, Main Theorem 2.1]. To prove assertion (8), we will briefly review the computation of $h_1,\ldots,h_n$ (which was already detailed at greater length in [Roj99c]). Our height bound will then follow from some elementary polynomial and linear algebra bounds.

In particular, recall the following algorithm for computing $h_1,\ldots,h_n$ (the polynomial Pert used below is defined in the appendix):

Step 2 If $n=1$, set $h_1(\theta):=\theta$ and stop. Otherwise, for all $i\in[n]$, let $q_i^-(t)$ be the square-free part of $\mathrm{Pert}_A(t,u_1,\ldots,u_{i-1},u_i-1,u_{i+1},\ldots,u_n)$.

Step 3 Define $q_i^\star(t)$ to be the square-free part of $\mathrm{Pert}_A(t,u_1,\ldots,u_{i-1},u_i+1,u_{i+1},\ldots,u_n)$ for all $i\in[n]$.

Step 4 For all $i\in[n]$ and $j\in\{0,1\}$, let $r_{i,j}(\theta)$ be the reduction of $\mathcal{R}_j(q_i^-(t),q_i^\star((\alpha+1)\theta-\alpha t))$ modulo $h(\theta)$.

Step 5 For all $i\in[n]$, define $g_i(\theta)$ to be the reduction of $-\theta-\frac{r_{i,1}(\theta)}{r_{i,0}(\theta)}$ modulo $h(\theta)$. Then define a_i to be the least positive integer so that $h_i(t):=a_ig_i\in\mathbb{Z}[t]$.

Following the notation of the algorithm above, the polynomial $\mathcal{R}_0(f,g)+\mathcal{R}_1(f,g)t$ is known as the **first subresultant** of f and g and can be computed as follows: Letting $f(t)=\alpha_0+\alpha_1t+\cdots+\alpha_{d_1}t^{d_1}$ and $g(t)=\beta_0+\beta_1t+\cdots+\beta_{d_2}t^{d_2}$, consider the following $(d_1+d_2-2)\times(d_1+d_2-1)$ matrix

$$\begin{bmatrix}
\beta_0 & \cdots & \beta_{d_2} & 0 & \cdots & 0 & 0\\
0 & \beta_0 & \cdots & \beta_{d_2} & 0 & \cdots & 0\\
\vdots & \ddots & \ddots & & \ddots & \ddots & \vdots\\
0 & \cdots & 0 & \beta_0 & \cdots & \beta_{d_2} & 0\\
0 & 0 & \cdots & 0 & \beta_0 & \cdots & \beta_{d_2}\\
\alpha_0 & \cdots & \alpha_{d_1} & 0 & \cdots & 0 & 0\\
0 & \alpha_0 & \cdots & \alpha_{d_1} & 0 & \cdots & 0\\
\vdots & \ddots & \ddots & & \ddots & \ddots & \vdots\\
0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_{d_1} & 0\\
0 & 0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_{d_1}
\end{bmatrix}$$

with d_1-1 "β rows" and d_2-1 "α rows." Let M_1^1 (resp. M_0^1) be the submatrix obtained by deleting the last (resp. second to last) column. We then define $\mathcal{R}_i(f,g):=\det(M_i^1)$ for $i\in\{0,1\}$.

Continuing our proof of Theorem 5, we see that we need only bound the coefficient growth of the intermediate steps of our preceding algorithm. Thanks to theorem 8, this is straightforward: First note that $\sigma(q_i^-)=\log((V_F+1)\cdot 2^{V_F})+\sigma(\bar{h}_F)$, where $\bar{h}_F$ is the square-free part of h_F. (This follows trivially from expressing the coefficients of a univariate polynomial $f(t+1)$ in terms of the coefficients of $f(t)$.) Via lemma 5 we then see that $\sigma(\bar{h}_F)=\log(\sqrt{V_F+1}\cdot 2^{V_F})+\sigma(h_F)$, and thus $\sigma(q_i^-)=\mathcal{O}(\sigma(h_F))$. Similarly, $\sigma(q_i^\star)=\mathcal{O}(\sigma(h_F))$ as well.

To bound the coefficient growth when we compute $r_{i,j}$ note that the coefficient of t_i in $q_i^\star(2\theta-t)$ is exactly $(-1)^i\sum_{j=i}^d\binom{j}{i}(2\theta)^j\alpha_j$, where α_j is the coefficient of t^j in $q_i^\star(t)$. Thus, via Hadamard's lemma again, we see that $|r_{i,j}(\theta)|\leq\left(\sqrt{V_F+1}\cdot e^{\sigma(h_F)}\right)^{V_F-1}\times\left(\sqrt{V_F+1}\cdot V_F2^{V_F}(2\theta)^{V_F}e^{\sigma(h_F)}\right)^{V_F-1}$ for all i,j. Since $r_{i,j}$ is itself a polynomial in θ of degree $V_F(V_F-1)$, the last inequality then easily implies that $\sigma(r_{i,j})=\mathcal{O}(V_F\sigma(h_F))$.

To conclude, note that for any univariate polynomials $f,g\in\mathbb{Z}[t]$ with degree $\leq D$, $\sigma(fg)=\mathcal{O}(\sigma(f)+\sigma(g)+\log D)$. Via long division it also easily follows that the quotient q and remainder r of f/g satisfy $aq,ar\in\mathbb{Z}[t]$ and $\sigma(aq),\sigma(ar)=\mathcal{O}(D(\sigma(f)+\sigma(g)))$, for some positive integer a with $\log a=\mathcal{O}(\sigma(g))$.

So by assertion (3) of theorem 3 we obtain $\log(a_i),\sigma(h_i)=\mathcal{O}(V_F^2\sigma(h_F))$, which implies our desired bound. ■

Remark 4 *An immediately consequence of our proof is that the asymptotic bound from assertion (8) can be replaced by the following explicit bound:* $V_F\times\left\{(V_F-1)\left[\log\left(V_F(V_F+1)^4 64^{V_F}\right)+2\sigma(h_F)\right]+\sigma(h_F)\right\}+\sigma(h_F)+\log V_F$. ■

2.4 The Proof of Theorem 2

Proofs of Parts (a) and (c): We first recall the following useful effective arithmetic Nullstellensatz of Krick, Pardo, and Sombra.

Theorem 6 *Suppose $f_1,\ldots,f_m\in\mathbb{Z}[x_1,\ldots,x_n]$ and $f_1=\cdots=f_m=0$ has* **no** *roots in $\mathbb{C}^n$. Then there exist polynomials $g_1,\ldots,g_m\in\mathbb{Z}[x_1,\ldots,x_n]$ and a positive integer a such that $g_1f_1+\cdots+g_mf_m=a$. Furthermore, $\log a\leq 2(n+1)^3DV_F[\sigma(F)+\log m+2^{2n+4}D\log(D+1)]$.* ■

The above theorem is a portion of corollary 3 from [KPS00].

The proof of part (a) is then almost trivial: By assumption, theorem 6 tells us that the mod p reduction of F has a root in $\mathbb{Z}/p\mathbb{Z}\Longrightarrow p$ divides a. Since the number of divisors of an integer a is no more than $1+\log a$ (since any prime power other than 2 is bounded below by e), we arrive at our desired asymptotic bound on a_F. So the first half of (c) is proved. ■

Remark 5 *Following the notation of theorem 2, we thus obtain the following explicit bound:* $a_F \leq 1+2(n+1)^3 D V_F[\sigma(F)+\log m+2^{2n+4} D\log(D+1)]$. ■

Proofs of Parts (b) and (c): Recall the following version of the discriminant.

Definition 1 *Given any polynomial* $f(x_1)=\alpha_0+\alpha_1 x_1+\cdots+\alpha_D x_1^D \in \mathbb{Z}[x_1]$ *with all* $|\alpha_i|$ *bounded above by some integer c, define the* **discriminant of f**, $\boldsymbol{\Delta_f}$, *to be* $\frac{(-1)^{D(D-1)/2}}{\alpha_D}$ *times the following* $(2D-1)\times(2D-1)$ *determinant:*

$$\det\begin{bmatrix} \alpha_0 & \cdots & \alpha_D & 0 & \cdots & 0 & 0 \\ 0 & \alpha_0 & \cdots & \alpha_D & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_D & 0 \\ 0 & 0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_D \\ \alpha_1 & \cdots & D\alpha_D & 0 & \cdots & 0 & 0 \\ 0 & \alpha_1 & \cdots & D\alpha_D & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_1 & \cdots & D\alpha_D & 0 \\ 0 & 0 & \cdots & 0 & \alpha_1 & \cdots & D\alpha_D \end{bmatrix},$$

where the first $D-1$ *(resp. last* D*) rows correspond to the coefficients of* f *(resp. the derivative of* f*).* ■

Our proof of part (b) begins with the following observation.

Theorem 7 *Suppose* $f\in\mathbb{Z}[x_1]$ *is a square-free polynomial of degree* D *with exactly* i_f *factors over* $\mathbb{Q}[x_1]$*. Let* $N_f(t)$ *denote the* **total** *number of distinct roots of the mod p reductions of* f *in* $\mathbb{Z}/p\mathbb{Z}$*, counted over all primes* $p\leq t$*. Then the truth of GRH implies that* $|i_f\pi(t)-N_f(t)|<2\sqrt{t}(D\log t+\log|\Delta_f|)+D\log|\Delta_f|$*, for all* $t>2$. ■

A slightly less explicit version of the above theorem appeared in [Koi96, Thm. 9], and the proof is almost the same as that of an earlier result of Adleman and Odlyzko for the case $i_f=1$ [AO83, Lemma 3]. (See also [Wei84].) The only new ingredient is an explicit version of the effective Chebotarev density theorem due to Oesterlé [Oes79]. (Earlier versions of theorem 7 did not state the asymptotic constants explicitly.)

The proof of part (b) is essentially a chain of elementary analytic bounds which flows from applying theorem 7 to the polynomial h_F from theorem 1. However, a technicality which must be considered is that h_F might not be square-free (i.e., Δ_{h_F} may vanish). This is easily taken care of by an application of the following immediate corollary of lemmata 4 and 5.

Corollary 1 *Following the notation above, let g be the square-free part of f and let* D' *be the degree of g. Then* $\log|\Delta_g|\leq D'(D\log 2+\log(D'+1)+\log c)$. ■

Another technical lemma we will need regards the existence of sufficiently many primes interleaving a simple sequence.

Lemma 2 *The number of primes in the open interval* $(At^3, A(t+1)^3)$ *is at least* $\lfloor\frac{1}{12}\cdot\frac{At^2}{\log t+\log A}\rfloor$*, provided* $A,t>e^5\approx 148.413\ldots$

This lemma follows routinely (albeit a bit tediously) from theorem 8.8.4 of [BS96], which states that for all $t>5$, the t^{th} prime lies in the open interval $(t\log t, t(\log t+\log\log t))$.

Our main strategy for proving part (b) is thus the following: Let N_F be the obvious analogue of N_f for **systems** of polynomials. We will then attempt to find constants t_0 and A_F such that $N_F(A_F(t+1)^3-1)-N_F(A_F t^3)>1$ for all $t\geq t_0$.

Via theorems 3 and 5, and a consideration of the primes dividing the a_i (the denominators in our rational univariate representation of Z_F), it immediately follows that $|N_F(t)-N_{h_F}(t)|\leq V_F\sum_{i=1}^n(\log a_i+1)$, for all $t>0$. We are now ready to derive an inequality whose truth will imply $N_F(A_F(t+1)^3-1)-N_F(A_F t^3)>1$: By theorem 7, lemma 2, the triangle inequality, and some elementary estimates on $\log t$, t^3, and their derivatives, it suffices to require that $A_F t^2$ strictly exceed $12(\log A_F+\log t)$ times the following quantity: $2(1+\sqrt{2})\sqrt{3A_F t^3}[V_F(\log(3A_F t^3)+1)+\log|\Delta_g|]+V_F(\log|\Delta_g|+\sum_{i=1}^n\log a_i+n)+1$, for all $t>\max\{t_0,e^5\}$, where g denotes the square-free part of h_F. (Note that we also used the fact that $i_g\geq 1$.)

A routine but tedious estimation then shows that we can actually take $t_0=1296(\frac{1+\log 3}{3}+\log 1296)\approx 4963040.506...$, and A_F as in the statement of part (b). So part (b) is proved at last. Careful accounting of the estimates then easily yields the explicit upper bound for A_F we state below. So the final half of part (c) is proved as well. ■

Remark 6 *The constant* $1296(\frac{1+\log 3}{3}+\log 1296)$ *arises from trying to find the least t for which* $t^2\geq\alpha\log^4 t$*, where, roughly speaking,* α *ranges over the constants listed in the expressions for* A_F, B_F, C_F, D_F *below:*
$A_F\leq\lceil 1296B_F^2\log^4 B_F+36C_F^2\log^2 C_F+2D_F\log D_F\rceil$, *where* $B_F:=72\sqrt{3}(1+\sqrt{2})V_F$, $C_F:=24\sqrt{3}(1+\sqrt{2})\log|\Delta_g|+2$, *and* $D_F:=12V_F(\log|\Delta_g|+\sum_{i=1}^n\log a_i+n)+13$. ■

3 Acknowledgements

The author thanks Felipe Cucker, Steve Smale, and Martin Sombra for useful discussions, in person and via e-mail.

References

[AO83] Adleman, Leonard and Odlyzko, Andrew, *"Irreducibility Testing and Factorization of Polynomials,"* Mathematics of Computation, 41 (164), pp. 699–709, 1983.

[BS96] Bach, Eric and Shallit, Jeff, *Algorithmic Number Theory, Vol. I: Efficient Algorithms,* MIT Press, Cambridge, MA, 1996.

[Ber75] Bernshtein, D. N., *"The Number of Roots of a System of Equations,"* Functional Analysis and its Applications (translated from Russian), Vol. 9, No. 2, (1975), pp. 183–185.

[BP94] Bini, Dario and Pan, Victor Y. *Polynomial and Matrix Computations, Volume 1: Fundamental Algorithms,* Progress in Theoretical Computer Science, Birkhäuser, 1994.

[BCSS98] Blum, L., Cucker, F., Shub, M., Smale, S., *Complexity and Real Computation,* Springer-Verlag, 1998.

[BZ88] Burago, Yu. D. and Zalgaller, V. A., *Geometric Inequalities,* Grundlehren der mathematischen Wissenschaften 285, Springer-Verlag (1988).

[Can87] Canny, John F., *"The Complexity of Robot Motion Planning Problems,"* ACM Doctoral Dissertation Award Series, ACM Press (1987).

[Can88] ____________, *"Some Algebraic and Geometric Computations in PSPACE,"* Proc. $20^{\underline{\text{th}}}$ ACM Symp. Theory of Computing, Chicago (1988), ACM Press.

[CG84] Chistov, A. L., and Grigoriev, Dima Yu, *"Complexity of Quantifier Elimination in the Theory of Algebraically Closed Fields,"* Lect. Notes Comp. Sci. 176, Springer-Verlag (1984).

[EC93] Emiris, Ioannis Z. and Canny, John, *"Efficient Incremental Algorithms for the Sparse Resultant and Mixed Volume,"* J. Symbolic Comput. 20 (1995), no. 2, pp. 117–149.

[Emi94] Emiris, Ioannis Z., *"Sparse Elimination and Applications in Kinematics,"* Ph.D. dissertation, Computer Science Division, U. C. Berkeley (December, 1994), available on-line at `http://www.inria.fr/saga/emiris`.

[EM99] Emiris, Ioannis Z. and Mourrain, Bernard, *"Matrices in Elimination Theory,"* J. of Symbolic Computation, 28(1&2):3-44, 1999.

[EP99] Emiris, Ioannis Z. and Pan, Victor, *"Techniques for Exploiting Structure in Matrix Formulae of the Sparse Resultant,"* Toeplitz matrices: structures, algorithms and applications (Cortona, 1996), Calcolo 33 (1996), no. 3-4, 353–369 (1998).

[FGM90] Fitchas, N., Galligo, A., and Morgenstern, J., *"Precise Sequential and Parallel Complexity Bounds for Quantifier Elimination Over Algebraically Closed Fields,"* Journal of Pure and Applied Algebra, 67:1–14, 1990.

[GH99] Gatermann, Karin and Huber, Birk, *"A Family of Sparse Polynomial Systems Arising in Chemical Reaction Systems,"* Preprint ZIB (Konrad-Zuse-Zentrum für Informationstechnik Berlin) SC-99 27, 1999.

[GKZ94] Gel'fand, I. M., Kapranov, M. M., and Zelevinsky, A. V., *Discriminants, Resultants and Multidimensional Determinants,* Birkhäuser, Boston, 1994.

[GH93] Giusti, Marc and Heintz, Joos, *"La détermination des points isolés et la dimension d'une variété algébrique peut se faire en temps polynomial,"* Computational Algebraic Geometry and Commutative Algebra (Cortona, 1991), Sympos. Math. XXXIV, pp. 216–256, Cambridge University Press, 1993.

[GLS99] Giusti, M., Lecerf, G., and Salvy, B., *"A Gröbner-Free Alternative to Polynomial System Solving,"* preprint, TERA, 1999.

[GK94] Gritzmann, Peter and Klee, Victor, *"On the Complexity of Some Basic Problems in Computational Convexity II: Volume and Mixed Volumes,"* Polytopes: Abstract, Convex, and Computational (Scarborough, ON, 1993), pp. 373–466, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 440, Kluwer Acad. Publ., Dordrecht, 1994.

[GS00] Gurvits, Leonid and Samorodnitsky, Alex, "A Deterministic Polynomial-Time Algorithm for Approximating Mixed Discriminant and Mixed Volume," Proceedings of STOC 2000, ACM Press, 2000.

[KLS97] Kannan, R., Lovasz, L, and Simonovitz, M., *"Random Walks and an $\mathcal{O}^*(n^5)$ Volume Algorithm for Convex Bodies,"* Random Structures Algorithms, **11** (1997), no. 1, pp. 1–50.

[Koi96] Koiran, Pascal, *"Hilbert's Nullstellensatz is in the Polynomial Hierarchy,"* DIMACS Technical Report 96-27, July 1996. (**Note:** This preprint considerably improves the published version which appeared in Journal of Complexity in 1996.)

[Koi97] ____________, *"Randomized and Deterministic Algorithms for the Dimension of Algebraic Varieties,"* Proceedings of the $38^{\underline{\text{th}}}$ Annual IEEE Computer Society Conference on Foundations of Computer Science (FOCS), Oct. 20–22, 1997, ACM Press.

[KPS00] Krick, T., Pardo, L.-M., and Sombra, M., *"Sharp Arithmetic Nullstellensatz,"* submitted for publication, also downloadable from `http://xxx.lanl.gov/abs/math.AG/9911094`.

[LO77] Lagarias, Jeff and Odlyzko, Andrew, *"Effective Versions of the Chebotarev Density Theorem,"* Algebraic Number Fields: L-functions and Galois Properties (Proc. Sympos. Univ. Durham, Durham, 1975), 409–464, Academic Press, London, 1977.

[Lec00] Lecerf, Grégoire, *"Computing an Equidimensional Decomposition of an Algebraic Variety by Means of Geometric Resolutions,"* submitted to the proceedings of the International Symposium on Symbolic Algebra and Computation (ISSAC) 2000.

[Mai00] Maillot, Vincent, *"Géométrie D'Arakelov Des Variétés Toriques et Fibrés en Droites Intégrables,"* Mém. Soc. Math. France, to appear.

[Mal00a] Malajovich-Muñoz, Gregorio, *"Condition Number Bounds for Problems with Integer Coefficients,"* Journal of Complexity, to appear.

[Mal00b] ________________________, *"Transfer Theorems for the* $\mathbf{P} \neq \mathbf{NP}$ *Conjecture,"* Journal of Complexity, to appear.

[MM82] Mayr, E. and Meyer, A., *"The Complexity of the Word Problem for Commutative Semigroups and Polynomial Ideals,"* Adv. Math. **46**, 305–329, 1982.

[MM95] McKelvey, Richard D., and McLennan, Andrew, *"The Maximal Number of Regular Totally Mixed Nash Equilibria,"* preprint, Department of Economics, University of Minnesota, 1995.

[Mig92] Mignotte, Maurice, *Mathematics for Computer Algebra,* translated from the French by Catherine Mignotte, Springer-Verlag, New York, 1992.

[Oes79] Oesterlé, Joseph, *"Versions Effectives du Théorème de Chebotarev sous l'Hypothèse de Riemann Généralisée,"* Astérisque **61** (1979), pp. 165–167.

[Pap95] Papadimitriou, Christos H., *Computational Complexity,* Addison-Wesley, 1995.

[Pla84] Plaisted, David A., *"New NP-Hard and NP-Complete Polynomial and Integer Divisibility Problems,"* Theoret. Comput. Sci. 31 (1984), no. 1–2, 125–138.

[Roj99a] Rojas, J. Maurice, *"Toric Intersection Theory for Affine Root Counting,"* Journal of Pure and Applied Algebra, vol. 136, no. 1, March, 1999, pp. 67-100.

[Roj99b] ________________, *"On the Complexity of Diophantine Geometry in Low Dimensions,"* Proceedings of the 31[st] Annual ACM Symposium on Theory of Computing (STOC '99, May 1-4, 1999, Atlanta, Georgia), 527-536, ACM Press, 1999.

[Roj99c] ________________, *"Solving Degenerate Sparse Polynomial Systems Faster,"* Journal of Symbolic Computation, vol. 28 (special issue on elimination theory), no. 1/2, July and August 1999, pp. 155–186.

[Roj00a] ________________, *"Low-Dimensional Varieties and the Frontier to Tractability,"* Contemporary Mathematics, Proceedings of a Conference on Hilbert's Tenth Problem and Related Subjects (University of Gent, November 1-5, 1999), edited by Jan Denef, Leonard Lipschitz, Thanases Pheidas, and Jan Van Geel, AMS Press.

[Sch80] Schwartz, J., *"Fast Probabilistic Algorithms for Verification of Polynomial Identities,"* J. of the ACM 27, 701–717, 1980.

[Sha94] Shafarevich, Igor R., *Basic Algebraic Geometry I,* second edition, Springer-Verlag (1994).

[Sil95] Silverman, Joseph H., *The Arithmetic of Elliptic Curves,* corrected reprint of the 1986 original, Graduate Texts in Mathematics 106, Springer-Verlag (1995).

[Stu94] Sturmfels, Bernd, *"On the Newton Polytope of the Resultant,"* Journal of Algebraic Combinatorics, 3: 207–236, 1994.

[Stu98] ________________, *"Introduction to Resultants,"* Applications of Computational Algebraic Geometry (San Diego, CA, 1997), 25–39, Proc. Sympos. Appl. Math., 53, Amer. Math. Soc., Providence, RI, 1998.

[Van50] van der Waerden, B. L., *Modern Algebra,* 2[nd] edition, F. Ungar, New York, 1950.[9]

[9]Shamefully, the sections on resultants were removed from later editions of this book.

[WZ94] Weiman, Jerzy and Zelevinsky, Andrei, *"Multigraded Formulae for Multigraded Resultants,"* J. Algebraic Geom. 3 (1994), no. 4, pp. 569–597.

[Wei84] Weinberger, Peter, *"Finding the Number of Factors of a Polynomial,"* Journal of Algorithms, 5:180–186, 1984.

4 Appendix: Background on Toric Resultants and The Proof of Theorem 3

Recall that the **support**, **Supp(*f*)**, of a polynomial $f \in \mathbb{C}[x_1, \dots, x_n]$ is simply the set of exponent vectors of the monomial terms appearing[10] in f. The support of the **polynomial system** $F = (f_1, \dots, f_m)$ is simply the m-tuple **Supp(*F*)** $:= (\mathrm{Supp}(f_1), \dots, \mathrm{Supp}(f_m))$. Let $\bar{\mathcal{A}} = (\mathcal{A}_1, \dots, \mathcal{A}_{m+1})$ be any $(m+1)$-tuple of non-empty finite subsets of $\mathbb{Z}^n$ and set $\mathcal{A} := (\mathcal{A}_1, \dots, \mathcal{A}_m)$. If we say that F has **support contained in** $\mathcal{A}$ then we simply mean that $\mathrm{Supp}(f_i) \subseteq \mathcal{A}_i$ for all $i \in [m]$.

Definition 2 *Following the preceding notation, suppose we can find line segments* $[v_1, w_1], \dots, [v_{m+1}, w_{m+1}]$ *with* $\{v_i, w_i\} \subseteq \mathcal{A}_i$ *for all* i *and* $\mathrm{Vol}_m(L) > 0$*, where* L *is the convex hull of* $\{\mathbf{O}, w_1 - v_1, \dots, w_{m+1} - v_{m+1}\}$*. Then we can associate to* $\bar{\mathcal{A}}$ *a unique (up to sign) irreducible polynomial* $\mathrm{Res}_{\bar{\mathcal{A}}} \in \mathbb{Z}[c_{i,a} \mid i \in [m+1] \ , \ a \in \mathcal{A}_i]$ *with the following property: If we identify* $\bar{\mathcal{C}} := (c_{i,a} \mid i \in [m+1] \ , \ a \in \mathcal{A}_i)$ *with the vector of coefficients of a polynomial system* $\bar{F}$ *with support contained in* $\bar{\mathcal{A}}$ *(and constant coefficients), then* $\bar{F}$ *has a root in* $(\mathbb{C}^*)^n \Longrightarrow \mathrm{Res}_{\bar{\mathcal{A}}}(\bar{\mathcal{C}}) = 0$*. Furthermore, for all* i*, the degree of* $\mathrm{Res}_{\bar{\mathcal{A}}}$ *with respect to the coefficients of* f_i *is no greater than* V_F*.* ■

That the toric resultant can actually be defined as above is covered in detail in [Stu94, GKZ94].

Another operator much closer to our purposes is the **toric perturbation** of F.

Definition 3 *Following the notation of definition 2, assume further that* $m = n$*,* $\mathrm{Supp}(F) = \mathcal{A}$*, and* $\mathrm{Supp}(F^*) \subseteq \mathcal{A}$*. We then define* $\mathrm{Pert}_{(F^*, \mathcal{A}_{n+1})}(u) \in \mathbb{C}[u_a \mid a \in \mathcal{A}_{n+1}]$ *to be the coefficient of the term of* $\mathrm{Res}_{\bar{\mathcal{A}}}(f_1 - sf_1^*, \dots, f_n - sf_n^*, \sum_{a \in \mathcal{A}_{n+1}} u_a x_a)$ $\in \mathbb{C}[s][u_a \mid a \in \mathcal{A}_{n+1}]$ *of* **lowest** *degree in* s*.* ■

The geometric significance of Pert can be summarized as follows: For a suitable choice of F^*, $\mathcal{A}_{n+1}$, and $\{u_a\}$, Pert satisfies all the properties of the polynomial h_F from theorem 3 in the special case

[10]We of course fix an ordering on the coordinates of the exponents which is compatible with the usual ordering of $x_1, \dots, x_n$.

$m=n$. In essence, Pert is an algebraic deformation which allows us to replace the positive-dimensional part of Z_F by a finite subset which is much easier to handle.

To prove theorems 1, 3, and 5 we will thus need a good complexity estimate for computing Res and Pert.

Lemma 3 *Following the notation above, let $\mathcal{R}_F$ (resp. $\mathcal{P}_F$) be the number of deterministic arithmetic operations needed to evaluate $\mathrm{Res}_{\bar{\mathcal{A}}}$ (resp. $\mathrm{Pert}_{(F^*,\mathcal{A}_{n+1})}$) at any point in $\mathbb{C}^{k+n+1}$ (resp. $\mathbb{C}^{2k+n+1}$), where $\mathcal{A} \subseteq \mathrm{Supp}(F)$ and $\mathcal{A}_{n+1} := \{\mathbf{O}, e_1, \ldots, e_n\}$. Also let r_F be the total degree of $\mathrm{Res}_{\bar{\mathcal{A}}}$ as a polynomial in the coefficients of $\bar{F}$ and set $m_F := e^{1/8}\frac{e^n}{\sqrt{n+1}}V_F$. (Note that $e^{1/8} \leq 1.3315$.) Then $r_F \leq (n+1)V_F$, $\mathcal{R}_F \leq (n+1)r_F\mathcal{O}(m_F^{2.376}) = \mathcal{O}(n^{0.812}e^{2.376n}V_F^{3.376})$, and $\mathcal{P}_F \leq (r_F+1)\mathcal{R}_F + O(r_F \log r_F) = \mathcal{O}(n^{1.812}e^{2.376n}V_F^{4.376})$. Furthermore, $k \leq mV_F$.* ■

The bound on $\mathcal{R}_F$ (resp. $\mathcal{P}_F$) follows directly from [EC93] (resp. [Roj99c]), as well as a basic complexity result on the **inverse discrete Fourier transform** [BP94, pg. 12]. The very last bound follows from a simple lattice point count.

Admittedly, such complexity estimates seem rather mysterious without any knowledge of how Res and Pert are computed. So let us now give a brief summary: The key fact to observe is that, in the best circumstances, one can express Res as the determinant of a sparse structured matrix $M_{\bar{\mathcal{A}}}$ (a **toric resultant matrix**) whose entries are either 0 or polynomials in the coefficients of $\bar{F}$ [EC93, Emi94, EP99, EM99]. In fact, the constant m_F in our theorem above is nothing more than an upper bound, easily derived from [EC93] and [Roj99c], on the number of rows and columns of $M_{\bar{\mathcal{A}}}$.

However, it is more frequent that Res is but a **divisor** of such a determinant, and further work must be done. Fortunately, in [EC93, Emi94], there are general randomized and deterministic algorithms for extracting Res.

The Proof of Theorem 3

Curiously, precise estimates on coefficient growth in toric resultants are absent from the literature. So we supply such an estimate below. In what follows, we use u_i in place of u_{e_i}.

Theorem 8 *Following the notation of lemma 3, suppose the coefficients of F (resp. F^*) have absolute value bounded above by c (resp. c^*) for all $i \in [n]$ and $u_1, \ldots, u_n \in \mathbb{C}$. Also let $\|u\| := \sqrt{u_1^2 + \cdots + u_n^2}$ and let μ denote the maximal number of monomial terms in any f_i. Then the coefficient of u_0^i in $\mathrm{Pert}_{(F^*,\mathcal{A}_{n+1})}$ has absolute value bounded above by $\frac{e^{13/12}}{\sqrt{\pi}}\sqrt{m_F+1} \cdot 4^{m_F - i/2}\|u\|^{V_F - i}(\sqrt{\mu}(c+c^*))^{m_F}\binom{V_F}{i}$, assuming that $\det M_{\bar{\mathcal{A}}} \neq 0$ under the substitution $(F - sF^*, u_0 + u_1x_1 + \cdots + u_nx_n) \mapsto \bar{F}$. (Note also that $\frac{e^{13/12}}{\sqrt{\pi}} \leq 1.66691$.)*

Proof: Let c_{ij} denote the coefficient of $u_0^i s^j$ in $\det M_{\bar{\mathcal{A}}}$, under the substitution $(F - sF^*, u_0 + u_1x_1 + \cdots + u_nx_n) \mapsto \bar{F}$. Our proof will consist of computing an upper bound on $|c_{ij}|$, so we can conclude simply by maximizing over j and then invoking a quantitative lemma on factoring.

To do this, we first observe that one can always construct a toric resultant matrix with exactly n_F rows corresponding to f_{n+1} (where $\delta(Z_F) \leq n_F \leq V_F$), and the remaining rows corresponding to $f_1, \ldots, f_n$. (This follows from the algorithms we have already invoked in lemma 3.) Enumerating how appropriate collections rows and columns can contain i entries of u_0 (and j entries involving s), it is easily verified that c_{ij} is a sum of no more than $\binom{V_F}{i}\binom{m_F - i}{j}$ subdeterminants of $M_{\bar{\mathcal{A}}}$ of size no greater than $m_F - i - j$. The coefficient c_{ij} also receives similar contributions from some larger subdeterminants since the rows of $M_{\bar{\mathcal{A}}}$ corresponding to $f_1, \ldots, f_n$ involve terms of the form $\gamma + \varepsilon s$.

Via lemma 4 below, we can then derive an upper bound of $\binom{V_F}{i}\binom{m_F - i}{j}\|u\|^{V_F - i}(\sqrt{\mu}(c+c^*))^{m_F - j}$ on $|c_{ij}|$. However, what we really need is an estimate on the coefficient c_i of u_0^i of $\mathrm{Pert}_{(F^*,\mathcal{A}_{n+1})}$, assuming the non-vanishing of $\det M_{\bar{\mathcal{A}}}$. To estimate c_i, we simply apply lemma 5 below (observing that $\mathrm{Pert}_{(F^*,\mathcal{A}_{n+1})}$ is a divisor of an $m_F \times m_F$ determinant) to obtain an upper bound of $\sqrt{m_F+1} \times 2^{m_F}\binom{V_F}{i}\max_j\left\{\binom{m_F - i}{j}\right\}\|u\|^{V_F - i}(\sqrt{\mu}(c+c^*))^{m_F}$ on $|c_i|$. We can then finish via the elementary inequality $\binom{m_F - i}{j} \leq \frac{e^{13/12}}{\sqrt{\pi}}2^{m_F - i}$, valid for all j (which in turn is a simple corollary of Stirling's formula). ■

A simple result on the determinants of certain symbolic matrices, used above, is the following.

Lemma 4 *Suppose A and B are complex $N \times N$ matrices, where B has at most N' nonzero rows. Then the coefficient of s^j in* $\det(A+sB)$ *has absolute value no greater than $\binom{N'}{j} v^{N-j}(v+w)^j$, where v (resp. w) is any upper bound on the Hermitian norms of the rows of A (resp. B).* ■

The lemma follows easily by reducing to the case $j=0$, via the multilinearity of the determinant. The case $j=0$ is then nothing more than the classical **Hadamard's lemma** [Mig92].

The lemma on factorization we quoted above is the following.

Lemma 5 *[Mig92] Suppose $f \in \mathbb{Z}[x_1, \ldots, x_N]$ has total degree D and coefficients of absolute value $\leq c$. Then $g \in \mathbb{Z}[x_1, \ldots, x_N]$ divides $f \Longrightarrow$ the coefficients of g have absolute value $\leq \sqrt{D+1} \cdot 2^D c$.* ■

We are now ready to prove theorem 3:

Proof of Theorem 3:

(The Case $m=n$): The existence of an h_F satisfying (0)–(5) will follow from setting $h_F(u_0) := \mathrm{Pert}_{(F^*, \mathcal{A}_{n+1})}(u_0)$ for $\mathcal{A}_{n+1}$ as in lemma 3, F^* as in lemma 6 below, and picking several $(u_1, \ldots, u_n)$ until a good one is found. Assertion (0) of theorem 3 thus follows trivially. That the conclusion of lemma 6 implies assertion (1) is a consequence of [Roj99c, Def. 2.2 and Main Theorem 2.1].

To prove assertions (1)–(5) together we will then need to pick $(u_1, \ldots, u_n)$ subject to a final technical condition. In particular, consider the following method: Pick $\varepsilon \in [1 + \binom{V_F}{2}]$ and set $u_i := \varepsilon^i$ for all $i \in [n]$. The worst that can happen is that a root of h_F is the image two distinct points in Z_F under the map $(\zeta_1, \ldots, \zeta_n) \mapsto u_1\zeta_1 + \cdots + u_n\zeta_n$, thus obstructing assertion (2). (Whether this happens can easily be checked within $\mathcal{O}(V_F \log V_F)$ arithmetic operations via a gcd calculation detailed in [Roj99c, Sec. 5.2], after first finding the coefficients of h_F.) Otherwise, it easily follows from Main Theorems 2.1 and 2.4 of [Roj99c] (and theorem 5 above and theorem 8 below) that h_F satisfies assertions (1)–(3) and (5).

Since there are at most $\binom{V_F}{2}$ pairs of points (ζ_1, ζ_2), picking $(u_1, \ldots, u_n)$ as specified above **will** eventually give us a good $(u_1, \ldots, u_n)$. The overall arithmetic complexity of our search for u_F and h_F is, thanks to lemma 3, $\left(\binom{V_F}{2} + 1\right) \cdot (V_F \mathcal{P}_F + \mathcal{O}(V_F \log V_F))$. This proves assertion (4), and we are done. ■

Remark 7 *Note that we never actually had to compute V_F above: To pick a suitable u, we simply keep pick choices (in lexicographic order) with successively larger and larger coodinates until we find a suitable u.* ■

(The Case $m<n$): Take $f_{n+1} = \cdots = f_m = f_n$. Then we are back in the case $m=n$ and we are done. ■

(The Case $m>n$): Here we employ an old trick: We substitute generic linear combinations of $f_1, \ldots, f_m$ for $f_1, \ldots, f_n$. In particular, set $\tilde{f}_i := f_1 + \varepsilon_i f_2 + \cdots + \varepsilon_i^{m-1} f_m$ for all $i \in [n]$. It then follows from lemma 7 below that, for generic $(\varepsilon_1, \ldots, \varepsilon_n)$, $Z_{\tilde{F}}$ is the union of Z_F and a (possibly empty) finite set of points. So by the $m=n$ case, and taking into account the larger value for c in our application of theorem 8, we are done. ■

Remark 8 *Via theorem 8, we thus see that the asymptotic bound of assertion (3) can be replaced by essentially the same explicit quantities as detailed in remark 3. The only difference is that we replace $\sqrt{2}$ by $\sqrt{n}\left(\binom{V_F}{2}+1\right)^n$. This accounts for the slightly larger asymptotic estimate.* ■

Lemma 6 *Following the notation above let $\mathcal{A}_i^* = \{\mathbf{O}, e_1, \ldots, e_n\} \cup \bigcup_{j=1}^n \mathcal{A}_j$ for all $i \in [n]$ and $k^* := n\#\mathcal{A}_1$, where # denotes set cardinality. Also let $\mathcal{C}^*$ be the coefficient vector of F^*. Then there is an F^* such that (i)* $\mathrm{Supp}(F^*) \subseteq \mathcal{A}^*$, *(ii) $\mathcal{C}^* = (1, \ldots, 1)$, (iii) F^* has exactly V_F roots in $(\mathbb{C}^*)^n$ counting multiplicities, and (iv)* $\det M_{\bar{\mathcal{A}}} \neq 0$ *under the substitution $(F - sF^*, u_0 + u_1x_1 + \cdots + u_nx_n) \mapsto \bar{F}$.* ■

The above lemma is a paraphrase of [Roj99c, Definition 2.3 and Main Theorem 2.3].

Lemma 7 *Following the notation above, let $S \subset \mathbb{C}$ be any finite set of cardinality $\geq mV_F + 1$. Then there is an $(\varepsilon_1, \ldots, \varepsilon_n) \in S^n$ such that every irreducible component of $Z_{\tilde{F}}$ is either an irreducible component of Z_F or a point.* ■

The proof is essentially the same as the first theorem of [GH93, Sec. 3.4.1], save that we use part (0) of theorem 3 in place of Bézout's Theorem.