Lower Bounds for Zero-Dimensional Projections

[Extended Abstract] *

W. Dale Brownawell†
Department of Mathematics
Penn State University
University Park, PA 16802
USA
wdb@math.psu.edu

Chee K. Yap‡
Courant Institute of Mathematical Sciences
New York University, New York, NY 10012, USA
and
Korea Institute of Advanced Study, Seoul, Korea
yap@cs.nyu.edu

ABSTRACT

Let I be an ideal generated by polynomials $P_1, \ldots, P_m \in \mathbb{Z}[X_1, \ldots, X_n]$, and $\mathfrak{P}$ be an isolated prime component of I. If the projection of $\text{Zero}(\mathfrak{P}) \subseteq \mathbb{C}^n$ onto the first coordinate is a finite set, and $\overline{\zeta} = (\zeta_1, \ldots, \zeta_n) \in \text{Zero}(\mathfrak{P})$ where $\zeta_1 \neq 0$, then we prove a lower bound on $|\zeta_1|$ in terms of n, m and the maximum degree D and maximum height H of the polynomials.

Categories and Subject Descriptors

F.2.2 [**Analysis of Algorithms and Problem Complexity**]: Nonnumerical Algorithms and Problems —*Geometrical Problems and Computations*; I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms—*Algebraic Algorithms*

General Terms

Algorithms, Theory

Keywords

Exact numerical algorithms, Zero Bounds, Nullstellensatz, Chow Form, Transcendence Theory

1. INTRODUCTION

Many computational problems in Computational Science and Engineering (CSE) are formulated in Euclidean space $\mathbb{R}^n$, or more generally, in a continuum. Practitioners invariably solve such problems by numerical methods. Such methods generally do not guarantee topological or geometric correctness criteria. To address this, and particularly to eliminate the associated problems of numerical nonrobustness, computational geometers in the last decade have developed a highly successful approach called Exact Geometric Computation [29]. This approach is encoded in libraries such as `LEDA` [21] and `CGAL` [12], with a large user base in research and the industry. The critical problem in this approach is to decide numerical zero [25, 29]. Practical methods for deciding numerical zero depend on existence of constructive zero bounds [19]. This paper is a contribution towards developing such zero bounds.

This idea of exact computation by numerical means is often viewed as an oxymoron because it is implicitly assumed that to compute exactly, we must resort to the "symbolic" (in the sense of "non-numeric") methods of computer algebra. Also, the area of "numerical computer algebra" is recently associated with the emerging subfield of computer algebra in which standard algebraic problems are generalized to the setting in which inputs are given by inexact numerical data (e.g., [27]). For instance, for polynomials with inexact coefficients, the classical problems of root finding or computing polynomial GCD can be turned into suitable optimization problems. But exact numerical computation in this paper is not an implicit reference to inexact inputs: our goal is to seek exact and efficient solutions of standard problems, but by means of numerical approximations.

There are many reasons for such interest in numerical approximations. Perhaps foremost is that approximations are natural and desirable for those CSE problems whose solutions are embedded in the continuum. Numerical solutions yield direct information about this embedding. E.g., if the solution is a real algebraic number x, then a numerical approximation $\widetilde{x}$ gives us immediate information about the approximate location of x in the continuum. This is more useful than, say, the "standard representation" of x as an algebraic number [9, p. 159]. Traditional computer algebra often forces us to adopt a viewpoint that is too general, with an attendant high cost. Consider the basic problem of computing a real algebraic set $V = \text{Zero}(f_1, \ldots, f_m) \subseteq \mathbb{R}^n$ where $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$. The problem of meshing an implicit surface [1] is an important instance of this problem (with $m = 1$). Computer algebra offers us algorithms based on computing in polynomial ideals, or cylindrical algebraic decomposition (CAD). These tools are sledge hammers for applications such as meshing because we are literally interested in V *qua set*, not its underlying scheme. Viewing V as

*The authors would like to thank KIAS sponsoring the Zero Workshop, Jul 19-22, 2007, thereby making this joint work possible.

†This author's work is partially supported by NSF Grant DMS-0355390.

‡This author's work is partially supported by NSF Grant CCF-0728977.

a set, we care little about multiplicities of points in V. Some numerical algorithms (e.g., Newton methods) may require knowledge about multiplicities, but the required knowledge might be a lot less than what schematology offers. As an illustration, consider the case where V is zero dimensional and $(f_1, \ldots, f_m)$ is a triangular system $(m = n)$. In [8], our "complete" numerical method for this case only distinguishes between odd and even multiplicities, not the exact multiplicities. Thus, we need to develop "stripped-down" algebraic tools that are more suited to the needs at hand.

A widely applicable example of such stripped-down algebraic tools is zero bounds. Numerical approximations, when combined with such bounds, can achieve the exactness that is traditionally associated with symbolic methods. One of the earliest examples is determining algebraic identities from Mignotte [22]. More recent examples include purely numerical algorithms for intersecting Bezier curves in the presence of tangential intersections [30], and for computing the topology of real algebraic curves in the presence of isolated singularities [6]. In the Core Library [31, 17, 11], zero bounds allow us to do exact algebraic number manipulation via numerical approximation. Our approach requires only upper bounds on a small number of numerical parameters (such as degree and height) of our algebraic quantities. They are relatively inexpensive to track, and so most of the computational cost resides with the arithmetic operations on approximate numbers. When combined with techniques such as numerical filters [18], the libraries `LEDA` and `CGAL` demonstrate that exact algebraic computation is viable in many real world applications.

The examples in the preceding paragraph represent a new breed of 'pure' numerical algebraic algorithms in which the only algebraic information we use are zero bounds. We stress 'pure' because there are various degrees of using numerical information in algebraic computation. E.g., the Thom encoding of algebraic numbers (e.g., [28, p. 209]) is purely algebraic, while the isolating interval encoding [5] uses numerical approximation. Unfortunately, the isolating interval encoding still carries a heavy algebraic component (each arithmetic operation requires a polynomial resultant computation). This fact greatly limits the wide use of isolated intervals in numerical computations – in particular, it would not be viable in the applications of `LEDA` or `CGAL` libraries. In computational curves and surfaces, some approaches (e.g., [26]) might be classified as a hybrid between algebraic and numerical. In the area of CAD, similar hybrid methods [16, 10] have been shown to be highly effective. It is interesting to note that most computer algebra textbooks list several alternative methods for representing and computing with algebraic numbers (e.g., [9, Section 4.2]), but the possibility of numerical approaches is not mentioned.

Exact numerical algorithms represent a pathway to practical and effective algorithms. The effectivity of numerical methods is derived from their **adaptive complexity**: unlike algebraic methods, numerical ones exhibit a highly variable running time for inputs of a given size. Slowness is correlated with the distance of the input to singularities. Thus the running time tends to be fast for most inputs, as singular inputs have measure zero. Practitioners favor numerical algorithms because they are easy to understand and simple to implement: usually, one needs only one number type, "approximate real numbers". This role can be assumed by dyadic numbers (or bigfloats) which are easily available in modern software. Thus, we avoid explicit manipulation of polynomials or algebraic operations such as resultants.

In order to obtain exact results by numerical approximation, we only need to compute to sufficiently high precision to make exact comparisons. Each comparison is enclosed in a while-loop in which successive iterations are carried out with increasing precision. A comparison with nonequality outcome will eventually succeed in this while-loop; but for the comparison with an equality outcome, we must use a zero-bound as the termination criterion. Any improvement in zero bounds is easily translated into a corresponding speed-up of such algorithms (with minimal change in the underlying algorithm). In short, *improved zero bounds is not just theoretical, but yields tangible algorithmic speedup.* See [18] for more details.

2. OVERVIEW OF THE MAIN RESULT

Let $P_1, \ldots, P_m \in \mathbb{Z}[X_1, \ldots, X_n]$ be polynomials whose degrees are at most D, and whose heights are at most H. Here, the height of a polynomial is the maximum of the absolute values of its coefficients. Let $\textsc{Zero}(P_1, \ldots, P_m) \subseteq \mathbb{C}^n$ be the zero set for the polynomials, also known as an (affine) variety. If $\widehat{P}_i$ is the homogenization of P_i by a new variable X_0, then we have the corresponding projective variety $\textsc{Zero}(\widehat{P}_1, \ldots, \widehat{P}_m) \subseteq \mathbb{P}^n(\mathbb{C})$. In the following, assume $\textsc{Zero}(\widehat{P}_1, \ldots, \widehat{P}_m)$ is a d-dimensional projective variety $(0 \leq d < n)$.

By a **zero bound** for $P_1, \ldots, P_m$ (or for the ideal $(P_1, \ldots, P_m)$) we mean a function $B(D, H, n, m)$ such that for all $\overline{\zeta} = (\zeta_1, \ldots, \zeta_n) \in$
$\textsc{Zero}(P_1, \ldots, P_m)$, if $\zeta_1 \neq 0$ then $|\zeta_1| \geq B(D, H, n, m)$. Alternatively, if $(\zeta_0, \zeta_1, \ldots, \zeta_n) \in \textsc{Zero}(\widehat{P}_1, \ldots, \widehat{P}_m)$ and $\zeta_0 \neq 0$ then $|\zeta_1/\zeta_0| \geq B(D, H, n, m)$. Note that we could also focus on ζ_i for any choice of $i = 1, \ldots, n$; we choose $i = 1$ for convenience. Canny [7] showed that, when $m = n$ and $d = 0$, then $B(D, H, n) := B(D, H, n, n) = (3DH)^{-nD^n}$ is a zero bound. Yap [28, Theorem 11.45, p. 350] relaxed the requirement that $d = 0$: he only required the affine part of $\textsc{Zero}(\widehat{P}_1, \ldots, \widehat{P}_m)$ to be a finite set. More precisely, for $m = n$ and $|\textsc{Zero}(P_1, \ldots, P_n)| < \infty$, then a zero bound is given by

$$B(D, H, n) = (2^{3/2} N K)^{-nD^{n-1}} 2^{-(n+1)D^n} \tag{1}$$

where $N = \binom{1+nD}{n}$ and $K = \sqrt{\binom{n+D-1}{D}}H$. The present paper aims to further relax the conditions under which we obtain zero bounds: we only require that the projection of some primary component of $\textsc{Zero}(P_1, \ldots, P_m)$ onto the first coordinate to be a finite set.

The tools for our proof arose in transcendence theory, as in [3]. We recall that the ability to control degrees in Chow form elimination were useful in giving sharp bounds [2] for the degrees in the Hilbert Nullstellensatz. In this note, we observe that the ability to control heights in [3] is well-suited for a general zero bound dealing with projections:

Let $\Pi_i(S) \subseteq \mathbb{C}$ denote the projection of a set $S \subseteq \mathbb{C}^n$ to its i-th coordinate. WLOG, we consider $i = 1$.

THEOREM 1. *Let $I := (P_1, \ldots, P_m) \in A := \mathbb{Z}[X_1, \ldots, X_n]$. Let $\mathfrak{P}$ be an isolated prime component of I with $\Pi_1(\textsc{Zero}(\mathfrak{P}))$ a finite set. If $\overline{\zeta} = (\zeta_1, \ldots, \zeta_n) \in \textsc{Zero}(\mathfrak{P})$ and $\zeta_1 \neq 0$, then*

$$|\zeta_1| \geq ((n+1)^2 e^{n+2})^{-n(n+1)D^{n-d}} (d^{n-d-1} mH)^{-(n-d)D^{n-d-1}},$$

where

- $\dim \mathfrak{P} = d$,
- $H \geq \mathrm{Height}(P_i)$, *and*
- $D \geq \deg(P_i)$, $i = 1, \ldots, m$.

Application to Evaluation Bounds. For a non-zero polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$, let its **evaluation bound** $EV(f)$ be given by

$$EV(f) := \inf\{|f(p)| : p \in \mathbb{C}^n, f(p) \neq 0, \nabla f(p) = \mathbf{0}\}$$

where $\nabla f(p) = ((\partial_1 f)_p, \ldots, (\partial_n f)_p)$ is the gradient of f at p. Here, $(\partial_i f)_p$ denotes the partial derivative of f with respect to X_i evaluated at p. In ISSAC 2008 [6], our numerical algorithm for detecting singularities of a real algebraic curve needs a lower bound on $EV(f)$. The bound (for the case $n = 2$) derived in [6] may be simplified to $EV(f)^{-1} \leq D^{8D^3} 2^{4LD^2}$ where $D \geq 2$, $\deg(f) \leq D$, and $\mathrm{Height}(f) < 2^L$. Taking logs to base 2 (with $\lg := \log_2$) we get:

$$-\lg EV(f) \leq 4D^2(2D \lg D + L). \tag{2}$$

Similar evaluation bounds were used in [8]. We can use Theorem 1 to obtain a general lower bound for $EV(f)$ for all n, using the following observation (see also [6]):

Lemma 1. *Let $f \in \mathbb{C}[X_1, \ldots, X_n]$, and let $I_f := \{f - Z, \partial_1 f, \ldots, \partial_n f\} \subseteq \mathbb{C}[Z, X_1, \ldots, X_n]$ where Z is a new variable. Then $\textsc{Zero}(I_f) \subseteq \mathbb{C}^{n+1}$ and the projection $\Pi_Z(\textsc{Zero}(I_f))$ onto the Z-coordinate is a finite set.*

Proof. View f as a regular map on varieties, $f : X \to Y$ where $X = \mathbb{C}^n$ and $Y = \mathbb{C}$. From Harris [14, Prop.14.4], there is a Zariski open set $U \subseteq \mathbb{C}$ such that for all $p \in f^{-1}(U)$, the differential $d_f(p)$ is surjective. Note that

$$d_f(p) = \nabla f(p) = ((\partial_1 f)_p, \ldots, (\partial_n f)_p).$$

Surjectivity means $\nabla f(p) \neq (0, \ldots, 0) = \mathbf{0}$. Using the contrapositive, $\nabla f(p) = \mathbf{0}$ implies $f(p) \in \mathbb{C} \setminus U$. Clearly, $(z, p) = (z, x_1, \ldots, x_n) \in \textsc{Zero}(I_f)$ iff $z = f(x_1, \ldots, x_n)$ and $\nabla f(x_1, \ldots, x_n) = \mathbf{0}$. We conclude that $z \in \mathbb{C} \setminus U$. Thus $\Pi_Z(\textsc{Zero}(I_f)) \subseteq \mathbb{C} \setminus U$; but the Zariski closed set $\mathbb{C} \setminus U$ is a finite set. Q.E.D.

This lemma tells us that $EV(f)$ is the infimum over a finite set of positive numbers, and hence $EV(f) > 0$.

Before we can apply Theorem 1 to the ideal $I = I_f := (f - Z, \partial_1 f, \ldots, \partial_n f)$, we need an observation: if $I = \cap_i Q_i$ is an irredundant primary decomposition, then $\textsc{Zero}(I) = \cup_i \textsc{Zero}(\mathfrak{P}_i)$ where $\mathfrak{P}_i$ is the associated prime of Q_i. Thus, for any j, $\textsc{Zero}(I)$ *has finite projection onto the jth component if and only if each $\mathfrak{P}_i$ has finite projection onto the jth component.*

Corollary 2. *For a non-zero $f \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree $\leq D$ and height $< 2^L$,*

$$EV(f) \geq ((n+2)^2 e^{n+3})^{-(n+1)(n+2)D^{n+1}} (n^n(n+1)D2^L)^{-(n+1)D^n}. \tag{3}$$

For $n = 2$, this yields

$$-\lg EV(f) \leq 3D^2(44.9D + L + \lg 12D). \tag{4}$$

Proof. Consider the ideal $I_f \subseteq \mathbb{Z}[Z, X_1, \ldots, X_n]$. Since the projection onto the Z-coordinate of $\textsc{Zero}(I_f) \subseteq \mathbb{C}^{n+1}$ is finite, the same finiteness property holds for any prime component $\mathfrak{P}$ of I_f. If $\overline{\zeta} = (\zeta_0, \zeta_1, \ldots, \zeta_n) \in \textsc{Zero}(\mathfrak{P})$, and $\zeta_0 \neq 0$, then $EV(f) \geq |\zeta_0|$. We now apply Theorem 1 to $\mathfrak{P}$ to give a lower bound on $|\zeta_0|$ (and hence on $EV(f)$). Our bound (3) comes directly from the inequality in Theorem 1: both variables n and m in Theorem 1 are replaced by $n + 1$, and H is replaced by $D2^L$. Specializing (3) to the case $n = 2$, we get

$$EV(f) \geq (4^2 e^5)^{-12D^3} (12D2^L)^{-3D^2}.$$

Taking logs to base 2, we obtain the bound in (4). Q.E.D.

Note that new bound (4) is comparable to the earlier bound in (2); in fact, the new bound is superior for large enough D. When (3) is restricted to the case $m = n$, our new bound is compares quite well to the affine bound of (1) (see the discussion [28, p. 350–351]).

In fact, Theorem 1 above is a special case of the following more general result, where here Π_1 is projection from $\mathbb{P}^n(\mathbb{C})$ onto the first *affine* coordinate of finite points: $\Pi_1(\zeta_0 : \cdots : \zeta_n) := \zeta_1/\zeta_0$.

Theorem 2. *Let the ideal I be generated by the homogeneous polynomials $\widehat{P}_1, \widehat{P}_2, \ldots, \widehat{P}_r \in \mathbb{Z}[X_0, \ldots, X_n]$ and have an isolated prime component $\mathfrak{P}$ of dimension d for which $\Pi_1(\textsc{Zero}(\mathfrak{P}))$ is finite. Assume further that* $\deg \widehat{P}_i \leq d_i$ *and* $\mathrm{Height}\, \widehat{P}_i \leq H_i$,

- $d_1 \geq d_2 \geq \cdots \geq d_r$ *and*
- $H_1 \geq H_2 \geq \cdots \geq H_r$.

If $\overline{\zeta} = (\zeta_1, \ldots, \zeta_n) \in \textsc{Zero}(\mathfrak{P})$ and $\zeta_1 \neq 0$, then

$$1/|\zeta_1| \leq 1+((n+1)^2 e^{n+2})^{n(n+1)\Delta} \prod_{i=1}^{n-d} ((r-i)H_i d_1 \cdots d_{i-1})^{\Delta/d_i},$$

where $\Delta = d_1 \cdot \cdots \cdot d_{n-d}$.

This result in turn will follow, using an improvement of Lemma 5 of [4], from the following result:

Theorem 3. *Let the homogeneous prime ideal $\mathfrak{P} \subset A$ have dimension d. Let the homogeneous polynomials $\widehat{P}_1, \ldots, \widehat{P}_m \in \mathfrak{P}$, form a regular sequence on $A_{\mathfrak{P}}$, where $m + d = n$, and let the $\widehat{P}_i$ have degrees $d_1, \ldots, d_m \geq 1$ and heights bounded by $H_1, \ldots, H_m$. Let the projection $\Pi_1(\textsc{Zero}(\mathfrak{P}))$ be a finite set. If $\overline{\zeta} = (\zeta_1, \ldots, \zeta_n) \in \textsc{Zero}(\mathfrak{P})$ and $\zeta_1 \neq 0$ then*

$$1/|\zeta_1| \leq 1 + ((n+1)^2 e^{n+2})^{n(n+1)\Delta} \prod_{i=1}^{m} H_i^{\Delta/d_i},$$

where $\Delta = d_1 \cdot \cdots \cdot d_m$.

3. PRELIMINARIES

Let $\mathfrak{P} \subseteq \mathbb{Z}[X_0, X_1, \ldots, X_n] =: A$ be a homogeneous prime ideal of dimension d, $\mathfrak{P} \bigcap \mathbb{Z} = (0)$. We use the basic facts about Chow forms as they were developed by Nesterenko for applications in transcendence theory. For more general background, see [15]. The **Chow Form** of $\mathfrak{P}$ is the polynomial

$$F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d)$$

in indeterminates $\overline{u}_i = (u_{i0}, \ldots, u_{in})$, $i = 0, \ldots, d$, such that

- $F_{\mathfrak{P}}$ is irreducible in $\mathbb{Z}[\overline{u}_0, \ldots, \overline{u}_d]$ and
- $F_{\mathfrak{P}} = 0$ is the necessary and sufficient condition for the $d+1$ "generic" hyperplanes

  $$H_i\colon \overline{u}_i \cdot \overline{x} := u_{i0}X_0 + \cdots + u_{in}X_n = 0$$

  to intersect at a zero of $\mathfrak{P}$.

Then, as the latter property does not favor one H_i over any other, $F_{\mathfrak{P}}$ is invariant (up to sign) under permutation of the sets of variables $\overline{u}_0, \ldots, \overline{u}_d$, and we can define the degree of $\mathfrak{P}$ to be the degree of $F_{\mathfrak{P}}$ with respect to any one of the $\overline{u}_i$, say $\overline{u}_0$:

$$\delta(F_{\mathfrak{P}}) := \deg_{\overline{u}_0} F_{\mathfrak{P}}.$$

This is equivalent to the various other definitions of the degree of $\mathfrak{P}$. In addition,

- these generic hyperplanes $\{H_i = 0\}$ meet the zeroes of $\mathfrak{P}$ in $g := \deg \mathfrak{P}$ points $\overline{\alpha}_1, \ldots, \overline{\alpha}_g \in \mathbb{P}^n(C)$,

where C is an algebraic closure of $\mathbb{Q}(\overline{u}_0, \ldots, \overline{u}_{d-1})$. We have the following key factorization result, which goes back at least to van der Waerden, where we have chosen

$$\overline{\alpha} = (1 : \alpha_1 : \cdots : \alpha_n) = \overline{\alpha}^{(1)}.$$

Lemma 1. *[[23], Lemma 2] For a homogeneous prime ideal $\mathfrak{P} \subset A$ of dimension d with, say, $X_0 \notin \mathfrak{P}$ and $\mathfrak{P} \bigcap \mathbb{Z} = (0)$, there is a finite Galois extension L of $\mathbb{Q}_{d-1} := \mathbb{Q}(\overline{u}_0, \ldots, \overline{u}_{d-1})$ such that in $L(\overline{u}_d)$, the Chow form $F_{\mathfrak{P}}$ factors as*

$$F_{\mathfrak{P}}(\overline{u}_0, \ldots, \overline{u}_d) = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} \overline{\alpha}^{(i)} \cdot \overline{u}_d,$$

as i runs over all the embeddings of $\mathbb{Q}_{d-1}(\alpha_1, \ldots, \alpha_n)$ into L and where $a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \in \mathbb{Z}[\overline{u}_0, \ldots, \overline{u}_{d-1}]$.

In [23], Nesterenko defined what we will call the resultant $\texttt{res}(F, Q)$ of a Chow form $F_{\mathfrak{P}}$, factored as above, and a homogeneous polynomial $Q \in \mathbb{Z}[X_0, \ldots, X_n]$:

$$\texttt{res}(F_{\mathfrak{P}}, Q) = a(\overline{u}_0, \ldots, \overline{u}_{d-1})^{\deg Q} \prod_{i=1}^{g} Q(\overline{\alpha}^{(i)})$$

Moreover he proved what will, for us, be the key auxiliary result:

Lemma 2. *([24], Lemmas 5 and 6) Let Q be homogeneous in A and lie outside the homogeneous prime ideal $\mathfrak{P}$ of A of dimension d, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be a complete list of all the minimal prime ideals in A associated to $(\mathfrak{P}, Q)$ such that $\mathfrak{p}_j \cap \mathbb{Z} = (0)$. Then there are unique $b, f_1, \ldots, f_t \in \mathbb{N}$ such that*

$$\texttt{res}(F_{\mathfrak{P}}, Q) = \pm b F_1^{f_1} \ldots F_t^{f_t},$$

where

- *F_j is a Chow form of $\mathfrak{p}_j$, $j = 1, \ldots, t$,*
- *$\delta(\texttt{res}(F_{\mathfrak{P}}, Q)) = \delta(F_{\mathfrak{P}})\delta(Q)$, and*
- $$\operatorname{ht} \texttt{res}(F_{\mathfrak{P}}, Q) \leq \delta(Q) \cdot \operatorname{ht} F_{\mathfrak{P}} + \delta(F_{\mathfrak{P}}) \cdot \operatorname{ht} Q + (n + d \log(n+1))\delta(F_{\mathfrak{P}}) \cdot \delta(Q),$$

where $\delta(Q) := \deg Q$ and $\operatorname{ht} Q := \log height(Q)$.

Here we mean that if $d = 0$, then $\texttt{res}(F_{\mathfrak{P}}, Q) \in \mathbb{Z}$ is non-zero and the final bound holds on $\operatorname{ht} \texttt{res}(F_{\mathfrak{P}}, Q)$.

Notice that all these constructions extend multiplicatively to unmixed cycles, that is, formal integral sums of homogeneous prime ideals of given dimension – with the sole change that d in the last inequality is replaced by $2d$ on multiplying and collecting coefficients.

To get our proofs started, we remark that for a homogeneous polynomial Q, since Cramer's Rule shows that the condition that the point $(X_0; X_1; \ldots; X_n) \in \mathbb{P}^n$ lie on n generic hyperplanes

$$\begin{array}{ccc} u_{00}X_0 + \ldots + u_{0n}X_n & = 0 \\ \vdots & \vdots \\ u_{n-1,0}X_0 + \ldots + u_{n-1,n}X_n & = 0 \end{array}$$

is that all X_i be a common non-zero multiple of its corresponding formal cofactor Δ_i in the matrix

$$\begin{bmatrix} X_0 & X_1 & \ldots & X_n \\ u_{00} & u_{01} & \ldots & u_{0n} \\ & & \ldots & \\ u_{n-1,0} & u_{n-1,1} & \ldots & u_{n-1,n} \end{bmatrix}$$

Then the point lies on the hypersurface determined by Q exactly when

$$Q(\Delta_0, \ldots, \Delta_n)$$

vanishes. Then, proceeding multiplicatively, we have the following result:

Lemma 3. *If Q is a homogeneous polynomial in A with decomposition into irreducible factors $Q = \prod Q_i^{e_i}$, the cycle $Z = \sum e_i Q_i$ has Chow form*

$$F_Q = \prod_i F_{Q_i}^{e_i} = Q(\Delta_0, \ldots, \Delta_n).$$

Finally, we will make use of a technical lemma that controls how much the height of a factor of a polynomial may exceed the height of the original polynomial. Although its content precedes Gelfond, and its content has been sharpened, he gives a convenient form which has been widely used in transcendence considerations.

Lemma 4. *[[13], Lemma II, p. 135] Let $G_1, \ldots, G_s \in \mathbb{C}[y_1, \ldots, y_y]$ have heights $H_1, \ldots, H_s$ and $G = G_1, \ldots, G_s$ have height H. Then*

$$H_1 \ldots H_s \leq H e^{\Delta},$$

where $\Delta := \sum \deg_{y_i} G$.

4. PROOF OF THEOREM 3

Let $\widehat{P}_1, \ldots, \widehat{P}_m \in \mathbb{Z}[X_0, \ldots, X_n]$ form a regular sequence on $A_{\mathfrak{P}}$, i.e. each $\widehat{P}_i$ is a non-zero-divisor on $A_{\mathfrak{P}}/(\widehat{P}_1, \ldots, \widehat{P}_{i-1})A_{\mathfrak{P}}$, and set $h_i := \log H_i$.

1. Define the sequence of Chow forms

$$F_1, F_2, \ldots, F_m$$

by the following strategy:

- $F_1 = F_{(\widehat{P}_1)}$ (the Chow form of $\widehat{P}_1$) and

- for $i \geq 2$, F_i is obtained from $R_i := \texttt{res}(F_{i-1}, \widehat{P}_i)$ by omitting all factors of R_i arising from prime ideals not lying in $\mathfrak{P}$.

This latter step corresponds to localization at $\mathfrak{P}$, by removing components whose associated prime ideals do do lie in $\mathfrak{P}$. Thus, each F_i corresponds in at least some sense to the primary decomposition of $(\widehat{P}_1, \ldots, \widehat{P}_i)A_{\mathfrak{P}}$.

2. Base Case: We have the upper bound from Lemma 3 that

- $\delta(F_1) \leq d_1$
- $\mathrm{ht}\, F_1 \leq \log H_1 + n^2 d_1$.

3. For $2 \leq i \leq m$, we apply inductively Lemmas 2 and 4 to find that

- $\delta(F_i) \leq d_1 \cdots d_i$
- $\mathrm{ht}(F_i) \leq \sum_{1 \leq j \leq i} h_j d_1 \ldots \widehat{d_j} \ldots d_i + (n(n+1)(n+2+2\log(n+1))d_1 \ldots d_i$

4. Now let us consider F_m, whose only underlying prime ideals are of dimension $d = n - m = \dim \mathfrak{P}$ and which lie inside $\mathfrak{P}$. In other words $\mathfrak{P}$ is the only underlying prime ideal and $F_m = F_{\mathfrak{P}}^e$ for some $e \in \mathbb{N}$. Therefore, when we factor F_m as in Lemma 1:

$$F_m(\overline{u}_0, \ldots, \overline{u}_d) = a(\overline{u}_0, \ldots, \overline{u}_{d-1})^e \prod_{i=1}^{g} (\overline{\alpha}^{(i)} \cdot \overline{u}_d)^e,$$

where

- $g \cdot e \leq d_1 \ldots d_m$ and
- $\mathrm{ht}(F_m) \leq \sum_{1 \leq j \leq m} h_j d_1 \ldots \widehat{d_j} \ldots d_m + n(n+1)(n+2+2\log(n+1))d_1 \cdots d_m$.

5. Now we know that $\Pi_1(\textsc{Zero}(\mathfrak{P})) = \{\alpha_1^{(1)}, \ldots, \alpha_1^{(g)}\}$, where the exponents represent conjugates of $\alpha_1 := \alpha_1^{(1)}$ under the g embeddings of $\mathbb{Q}(\overline{\alpha}^{(1)}) := \mathbb{Q}_{d-1}(\alpha_1^{(1)}, \ldots, \alpha_n^{(1)})$ into L fixing $\mathbb{Q}_{d-1}$. This means in particular that $\alpha_1^{(1)}$ is algebraic (over $\mathbb{Q}$), and its conjugates $\alpha_1^{(1)}, \ldots, \alpha_{\underline{1}}^{(g)}$ are conjugates over $\mathbb{Q}$. (Each of its embeddings into $\overline{\mathbb{Q}}$ extends to an embedding of $\mathbb{Q}(\overline{\alpha}^{(1)})$ into L.) Therefore we know that $-\alpha_1^{(1)}$ is a root of the polynomial

$$f(X) := \prod (X + \alpha_1^{(i)}) \in \mathbb{Q}[X].$$

6. Setting $u_{d,2} = \cdots = u_{d,n} = 0$ in

$$F_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} (\overline{\alpha}^{(i)} \cdot \overline{u}_d) \in \mathbb{Z}[\overline{u}_0, \ldots, \overline{u}_d]$$

gives a polynomial which we shall call $G_{\mathfrak{P}}$ (even though it also depends on f).

$$\begin{aligned} G_{\mathfrak{P}} &= a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \prod_{i=1}^{g} (1 \cdot u_{d0} + \alpha_1^{(i)} u_{d1}) \\ &\in \mathbb{Z}[\overline{u}_1, \ldots, \overline{u}_{d-1}, u_{d0}, u_{d1}]. \end{aligned}$$

In other words,

$$G_{\mathfrak{P}} = a(\overline{u}_0, \ldots, \overline{u}_{d-1}) \widehat{f}(u_{d0}, u_{d1}).$$

By (the proof of) Gauss's Lemma, we find that there is an $a_0 \in \mathbb{N}$ such that, in $\mathbb{Z}[\overline{u}_0, \ldots, \overline{u}_{d-1}]$,

$$a(\overline{u}_0, \ldots, \overline{u}_{d-1}) = a'(\overline{u}_0, \ldots, \overline{u}_{d-1}) a_0,$$

and $a_0 \widehat{f}(u_{d0}, u_{d1}) \in \mathbb{Z}[u_{d0}, u_{d1}]$. In particular, $(-\alpha, 1)$ is a zero of $a_0 \widehat{f}(u_{d0}, u_{d1}) \in \mathbb{Z}[u_{d0}, u_{d1}]$, which polynomial in turn is a factor in $\mathbb{Z}_d$ of the part of F_m involving u_{d0}, u_{d1} and hence of the corresponding part of $\texttt{res}(F_{m-1}, \widehat{P}_m)$ and therefore satisfies the bounds established for F_m in paragraph 4 above.

7. Dehomogenizing gives

- $a_0 f(X) \in \mathbb{Z}[X]$
- $\mathrm{ht}\, a_0 f(X) \leq \sum_{1 \leq j \leq m} h_j d_1 \ldots \widehat{d_j} \ldots d_m + n(n+1)(n+2+2\log(n+1))d_1 \cdots d_m$.

for which $a_0 f(\alpha_1) = 0$. From upper bounds on the height of an integral polynomial satisfied by α_1, we have the usual corresponding lower bound on $|\alpha_1|$.

5. PROOF OF THEOREM 2

For this result, we prove a variant of Lemma 1 of [20]:

Lemma 5. *Let $\mathfrak{P}$ be an isolated prime component of dimension d of the ideal I generated by the homogeneous polynomials $\widehat{P}_1, \widehat{P}_2, \ldots, \widehat{P}_r \in \mathbb{Z}[X_0, \ldots, X_n]$ for which*

- *$\widehat{P}_i \leq d_i$ and*
- *Height $\widehat{P}_i \leq H_i$, $i = 1, \ldots, r$.*

Then there is a sequence of homogeneous polynomials $\widehat{Q}_1, \ldots, \widehat{Q}_{n-d}$ which is regular on $A_{\mathfrak{P}}$ and for which

- *$\deg \widehat{Q}_i \leq d_i$ and*
- *Height $\widehat{Q}_i \leq (r-i) d_1 \cdots d_{i-1} H_i$.*

Proof. The proof selects the $\widehat{Q}_i$ recursively, starting with $\widehat{Q}_1 := \widehat{P}_1$. Then for $2 \leq i \leq n-d$, we notice that the ideal $I_{i-1} := (\widehat{Q}_1, \ldots, \widehat{Q}_{i-1}) A_{\mathfrak{P}} \cap A$ consists of what remains of the primary decomposition of $(\widehat{Q}_1, \ldots, \widehat{Q}_{i-1})$ in A after removing all primary components not contained in $\mathfrak{P}$. (Compare [4], or Zariski-Samuel.) We choose $\widehat{Q}_i$ to lie in I but outside the $t(i) \leq \deg I_{i-1} \leq d_1 \ldots d_{i-1}$ prime ideals $\mathfrak{p}_{i-1,1}, \ldots, \mathfrak{Q}_{i-1,t(i)}$ of I_{i-1}.

Masser and Wüstholz point out that, since not all the $\widehat{P}_j$ are contained in any of the $\mathfrak{p}_{i-1,j}$, the coefficients $\overline{c} := (c_2, \ldots, c_r)$ such that (our assumption on the finiteness of $\Pi_i(\textsc{Zero}(\mathfrak{P}))$ implies that $X_0 \notin \mathfrak{P}$)

$$c_2 \widehat{P}_2 + \cdots + c_r X_0^{\deg \widehat{P}_2 - \widehat{P}_r} \widehat{P}_{t(i)} \in \mathbb{Q} \otimes \mathfrak{p}_{i-1,j}$$

form a proper subspace $V_{i,j}$ of $\mathbb{Q}^r$. Take a non-zero $\lambda_j := (l_{j2}, \ldots, l_{jr}) \in V_j^{\perp}$. As remarked in [20],

$$\text{all } \overline{c} \cdot \lambda_j \neq 0 \Rightarrow \widehat{Q}_i' = c_2 \widehat{P}_2 + \cdots + c_r X_0^{\deg \widehat{P}_2 - \widehat{P}_r} \widehat{P}_r \in I \backslash \bigcup_j \mathfrak{p}_{i-1,j}.$$

That is, it suffices to locate $c_2, \ldots, c_r$ so that

$$T(c_2, \ldots, c_r) := \prod_j (l_{j2} c_2 + \cdots + l_{jr} c_r)$$

is non-zero. However, as this is a non-zero polynomial of degree $t(i) \geq 1$ in each variable c_l, the usual argument using the number of zeros of a one-variable polynomial shows that we can find an argument $\overline{c} \in \mathbb{Z}^{r-1}$ with each $|c_l| \leq (t(i)+1)/2$ where T does not vanish, i.e. such that

$$\widehat{Q}'_i := c_2\widehat{P}_2 + \cdots + c_r X_0^{\deg \widehat{P}_2 - \deg \widehat{P}_r} \widehat{P}_r \notin \mathfrak{p}_{i-1,j}, \quad j = 1, \ldots, t(i).$$

In our case, we want to also control the height of the polynomials as much as we can, and we would not like to have the large height H_2 entering into the height bounds for all $\widehat{Q}_i$.

The preceding construction shows that we can force $\widehat{P}_2$ to appear in $\widehat{Q}_2$ by choosing $c_2 \neq 0$ but still satisfying $|c_2| \leq (1+t(2))/2$. Notice then that, since $\widehat{P}_2$ has occurred with non-zero coefficient in $\widehat{Q}_2$, which latter polynomial then lies in every $\mathfrak{p}_{2,j}A_{\mathfrak{P}} \bigcap A$ for $\mathfrak{p}_{2,j}$ associated to I_2, then it is easy to form a non-zero linear combination of $\widehat{Q}_2$ and $\widehat{Q}'_3$ containing no $\widehat{P}_2$ and yet lying in none of the $\mathfrak{p}_{2,j}$. This means that the polynomials $\widehat{P}_3, \ldots, \widehat{P}_r$ do not all lie in any $\mathfrak{p}_{2,j}$, and we can start over with this shorter list of polynomials and apply the same construction as above to find

$$\widehat{Q}_2 := c_3\widehat{P}_3 + \cdots + c_r X_0^{\deg \widehat{P}_3 - \deg \widehat{P}_r} \widehat{P}_r \notin \mathfrak{p}_{2,j}, \quad j = 1, \ldots, t(2).$$

This means that, as far as escaping prime ideals $\mathfrak{p}_{2,j}$, we can ignore $\widehat{P}_2$. This same reasoning applies inductively to $\widehat{P}_2, \ldots, \widehat{P}_{i-1}$ in the construction of each $\widehat{Q}_i$.

In this way, we obtain a sequence of polynomials

$$\widehat{Q}_i := c_i\widehat{P}_i + \cdots + c_r X_0^{\deg \widehat{P}_i - \widehat{P}_r} \widehat{P}_r \notin \mathfrak{p}_{i-1,j}, \quad c_j \in \mathbb{Z}, j = i, \ldots, t(i)$$

such that, since $t(i) \leq d_1 \cdots d_i$,

- $\widehat{Q}_1, \ldots, \widehat{Q}_{n-d}$ is a regular sequence on $A_{\mathfrak{P}}$,
- $\deg \widehat{Q}_i \leq d_i$ and $\text{Height}\, \widehat{Q}_i \leq (r-i)d_1 \cdots d_{i-1} \cdot H_i$, $i = 1, \ldots, n-d$.

Now we apply Theorem 3 to conclude.

This actually gives $d_1 \cdots d_{i-1} \sum_{j=i+1}^{r} H_j$. In fact we get the even smaller bound $(1 + d_1 \ldots d_{i-1})(\sum_{j=i+1}^{r} H_j)/2$.

6. FINAL REMARKS.

Our main result provides a zero bound for an ideal $I = (P_1, \ldots, P_m) \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ conditioned on the hypothesis that I has a finite projection onto the first coordinate. We gave an application of this result to evaluation bounds. Such evaluation bounds will become increasingly important as we seek to develop exact algebraic algorithms based purely on numerical approximations.

The general shape of these inequalities looks about right. However it is certain that the constants can be improved. For example, Gelfond's inequality really involves something factors like

$$\sqrt{1 + \deg y_i}\, 2^{\deg y_i}$$

rather than $e^{\deg y_i}$. Moreover Nesterenko has not optimized constants. For sharper, but perhaps unwieldy, estimates, one should look at Philippon's eliminant forms, which allow one to essentially appeal to Mahler measures and which yield somewhat sharper looking "arithmetic Bezout theorems" at the cost of complexity. However if one is interested only in the general shape in terms of the classical heights and degrees, the improvement should be mild.

Finally it might be of interest to carry out this same procedure for multihomogeneous ideals. That would involve "multiprojections".

7. REFERENCES

[1] J.-D. Boissonnat, D. Cohen-Steiner, B. Mourrain, G. Rote, and G. Vegter. Meshing of surfaces. In J.-D. Boissonnat and M. Teillaud, editors, Effective Computational Geometry for Curves and Surfaces. Springer, 2006. Chapter 5.

[2] W. D. Brownawell. Bounds for the degrees in the Nullstellensatz. Annals of Math., 126:577–591, 1987.

[3] W. D. Brownawell. Local Diophantine Nullstellen inequalities. Journal A.M.S., 1:311–322, 1988.

[4] W. D. Brownawell and D. W. Masser. Multiplicity estimates for analytic functions, II. Duke Math. J., 47:273–295, 1980.

[5] B. Buchberger, G. E. Collins, and R. Loos, editors. Computer Algebra. Springer-Verlag, Berlin, 2nd edition, 1983.

[6] M. Burr, S. Choi, B. Galehouse, and C. Yap. Complete subdivision algorithms, II: Isotopic meshing of singular algebraic curves. In Proc. Int'l Symp. Symbolic and Algebraic Computation (ISSAC'08), pages 87–94, 2008. Hagenberg, Austria. Jul 20-23, 2008.

[7] J. F. Canny. Generalized characteristic polynomials. J. of Symbolic Computation, 9:241–250, 1990.

[8] J.-S. Cheng, X.-S. Gao, and C.-K. Yap. Complete numerical isolation of real zeros in zero-dimensional triangular systems. J. of Symbolic Computation, page ???, 2008. Special Issue of JSC based on ISSAC 2007.

[9] H. Cohen. A Course in Computational Algebraic Number Theory. Springer-Verlag, 1993.

[10] G. E. Collins, J. R. Johnson, and W. Krandick. Interval arithmetic in cylindrical algebraic decomposition. J. of Symbolic Computation, 34:145–157, 2002.

[11] Z. Du. Guaranteed Precision for Transcendental and Algebraic Computation made Easy. Ph.D. thesis, New York University, Department of Computer Science, Courant Institute, May 2006. From http://cs.nyu.edu/exact/doc/.

[12] A. Fabri, E. Fogel, B. Gärtner, M. Hoffmann, L. Kettner, S. Pion, M. Teillaud, R. Veltkamp, and M. Yvinec. The CGAL manual. 2003. Release 3.0.

[13] A. Gel'fond. Algebraic and Transcendental Numbers. Dover Publications, 1934.

[14] J. Harris. Algebraic Geometry. Springer-Verlag, 1992.

[15] W. Hodge and D. Pedoe. Methods of Algebraic Geometry, volume 1-3. Cambridge University Press, 1994.

[16] H. Hong. An efficient method for analyzing the topology of plane real algebraic curves. Mathematics and Computers in Simulation, 42:571–582, 1996.

[17] V. Karamcheti, C. Li, I. Pechtchanski, and C. Yap. A Core library for robust numerical and geometric computation. In 15th ACM Symp. Computational Geometry, pages 351–359, 1999.

[18] C. Li, S. Pion, and C. Yap. Recent progress in Exact Geometric Computation. J. of Logic and Algebraic Programming, 64(1):85–111, 2004. Special issue on "Practical Development of Exact Real Number Computation".

[19] C. Li and C. Yap. A new constructive root bound for algebraic expressions. In 12th SODA, pages 496–505,

Jan. 2001.

[20] D. W. Masser and G. Wüstholz. Fields of large transcendence degree generated by values of elliptic functions. Inventiones Math., 72:407–464, 1983.

[21] K. Mehlhorn and S. Näher. LEDA: a platform for combinatorial and geometric computing. volume 38, pages 96–102, 1995.

[22] M. Mignotte. Identification of algebraic numbers. J. of Algorithms, 3:197–204, 1982.

[23] Y. V. Nesterenko. Bounds for the characteristic function of a prime ideal. Math. USSR Sbronik, 51:9–32, 1985. Transl. of Mat. Sbornik 123(165) No. 1:11-34, 1984.

[24] Y. V. Nesterenko. On the algebraic independence of algebraic powers of algebraic numbers. Math. USSR Sbornik, 51:429–454, 1985. Transl. of Mat. Sbornik 123(165), No. 4:435-459, 1984.

[25] D. Richardson. How to recognize zero. J. of Symbolic Computation, 24:627–645, 1997.

[26] R. Seidel and N. Wolpert. On the exact computation of the topology of real algebraic curves. In Proc. 21st ACM Symp. on Comp. Geometry, pages 107–116, 2005. Pisa, Italy.

[27] H. H. Stetter. Numerical Polynomial Algebra. SIAM, 2004.

[28] C. K. Yap. Fundamental Problems of Algorithmic Algebra. Oxford University Press, 2000.

[29] C. K. Yap. Robust geometric computation. In J. E. Goodman and J. O'Rourke, editors, Handbook of Discrete and Computational Geometry, chapter 41, pages 927–952. Chapman & Hall/CRC, Boca Raton, FL, 2nd edition, 2004.

[30] C. K. Yap. Complete subdivision algorithms, I: Intersection of Bezier curves. In 22nd ACM Symp. on Comp. Geometry, pages 217–226, July 2006.

[31] C. K. Yap and T. Dubé. The exact computation paradigm. In D.-Z. Du and F. K. Hwang, editors, Computing in Euclidean Geometry, pages 452–492. World Scientific Press, Singapore, 2nd edition, 1995.