The DMM bound: multivariate (aggregate) separation bounds

Ioannis Z. Emiris, Bernard Mourrain, Elias Tsigaridas

The DMM bound: multivariate (aggregate) separation bounds

Ioannis Z. Emiris* Bernard Mourrain† Elias P. Tsigaridas‡

June 9, 2009

Abstract

In this paper we present aggregate separation bounds for polynomials systems. We call the bounds Davenport-Mahler-Mignotte (DMM), and we prove that in most of the cases are close to optimal. The bounds are output-sensitive in the sense that they depend on the mixed volume of the tested systems. As a consequence, we improve the gap theorem [11] of Canny by a factor of d^{n-1}, where d is a bound on the degree of the polynomials, and n is their number.

We apply our bounds on the problem of computing the eigenvalues and eigenvectors of an integer matrix, and we improve the bound of [4] on the minimum of value of a positive polynomial over the standard simplex. We also apply our bounds to find a lower bound on the number of steps that a subdivision-based algorithm for polynomial system solving should perform, we provide for the first time the complexity of Milne's algorithm in the 2D case.

*Department of Informatics and Telecommunications, National Kapodistrian University of Athens, HELLAS. email: emiris(AT)di.uoa.gr

†INRIA Sophia-Antipolis Méditerranée, FRANCE. email: mourrain(AT)sophia.inria.fr

‡INRIA Sophia-Antipolis Méditerranée, FRANCE. email: elias.tsigaridas(AT)sophia.inria.fr

Contents

1 Introduction

One of the great challenges in algebraic algorithms is to understand in depth the theoretical and practical complexity of the algorithms based on exact arithmetic and to compare them with the ones from numerical analysis. The goal is not to compete with numerical algorithms, that rely on numerical, and probably unstable, computations but rather to contribute to a hybrid approach that will rely both on exact and approximate computations, namely *symbolic-numeric computation*. This approach will provide solid mathematical and algorithmic foundations, and efficient implementations for exact manipulation of general objects. The interplay between algebraic algorithms and applications is a fascinating research domain with many research challenges.

The aim is to provide a solid theoretical background, as well as efficient and robust implementations for algebraic algorithms that outperform the purely numerical ones and can treat all degenerate cases without exceptions. To design new algorithms that can support parallel computations, massive data sets, and the recent developments in GPU programming. There is an emerging need to use effective tools from algebraic algorithms, under the concept of symbolic-numeric computation, to tackle emerging problems that appear in non-linear computational geometry, in geometric modeling and computer aided design, in computational topology, in visibility computations in two and three dimensions, in robotics, in signal processing, in geographical information systems, just to mention few of the applications.

Computing the roots, real and complex, in some representation, of systems of multivariate polynomials is one of the central problems in both symbolic and numeric computation. The complexity analysis of exact algorithms for solving polynomials systems that are based on projection-like techniques, like resultant computations, rational univariate representation, Gröbner and normal form computations, depends on the so-called *separation bounds*. Moreover, both the analysis, as well as the actual running times of iterative algorithms that are based on subdivision techniques and/or refinements, relies on a good estimation of these bounds. For polynomial systems these bounds represent the minimum distance between two, possible complex roots, of the system under study. The Exact Geometric Computation (EGC) paradigm [43, 45], for example, exploits such bounds for effective and accurate computations. A famous result on separation bounds is the "Gap theorem" by Canny [11] stated more than twenty years ago, see also [42] for a slightly more generic result. A lower bound on the absolute value of the coordinates of the roots is computed in [7], where the only assumption on the system is that there is a zero dimensional projection. The upper and lower bounds that we present in Prop. 5 are similar to the ones in [7], but they are an improvement when they are expressed using mixed volumes. Constructive root bounds are also in this direction for example [8, 9] or [37], where the separation bounds are computed using information from the expression at hand. From the numerical point of view, let us mention the work of Dedieu [16], that connects the separation bound with the condition number.

Besides their obvious theoretical interest, separations bounds are of particular interest in non-linear computational geometry; a research domain that relies heavily on very demanding algebraic operations. Let us mention the computation of the Voronoi diagram of ellipses [23] and convex smooth pseudo-circles [24], the arrangement of conic sections in the plane [22]; and also algorithms that exploit refinements and subdivision techniques to compute the topology of a real plane [1, 2, 10, 13, 19, 25, 27, 28, 44], of a space curve [27], or topology and meshing of surfaces [5, 6]. The theoretical analysis of these algorithms, see for example [13, 17, 23, 25],

depends on separation bounds. A theoretical improvement of the separation bounds will affect a great number of algorithms in computational geometry.

Our Contribution

In this paper we consider the problem of computing bounds for the worst case separation bounds, that is the minimum distance, between the (complex) roots of a polynomial system, bounds for the product of (absolute) differences of roots, as well as upper and lower bounds on the coordinates. The bounds are computed as a function of the number of variables, the mixed volume of the system and the maximum norm of the polynomials. We treat only the case where the system is 0-dimensional, even though our techniques could be extended to positive-dimensional cases, using the toric characteristic polynomial [14].

Davenport [15] was the first that introduced aggregate separation bounds for the real roots of univariate polynomials, which depend on Mahler's measure, e.g.[29]. Mignotte [30, 31] loosen the hypothesis of the bounds and extend them to also hold for the complex roots. We extend the aggregation separation bound from a univariate polynomial to (zero dimensional) systems of polynomials (Th. 4) and we call this bound $\texttt{DMM}_n$, which stands for *Davenport-Mahler-Mignotte* bound. We also present an improved version of Canny's Gap theorem [11] (Prop. 5), which provides better upper/lower bounds and the separation bounds for polynomials systems. Our bounds are close to optimal (Sec. 3.4).

We illustrate our bounds on computing the eigenvalues and eigenvectors of an integer matrix (Sec. 4.1), and on the problem of estimating the minimum of a positive polynomials over the standard simplex (Sec. 4.2). Moreover, we compute a bound on the number of steps that any subdivision-based algorithm needs to perform in order to isolate the real roots of a polynomial system (Th. 11) inside a box. We use the latter bound to estimate the complexity of Milne's algorithm [32] in 2D.

The rest of the paper is structured as follows. Next, we introduce some notation, and Sec. 4 presents the univariate (Sec. 2.1) and the multivariate version (Th. 4 and Prop. 5 in Sec. 2.2) of the DMM bound. Sec. 3 is devoted to the proofs of Th. 4 and Prop. 5, as well as in proving the optimality of the proposed bounds Sec. 3.4. The two applications of the bounds are presented in Sec. 4, that is the eigenvalue and eigenvector problem Sec. 4.1, and the positive polynomial Sec. 4.2. Sec. 5 is devoted to subdivision algorithms We conclude in Sec. 6 with a summary of our results and future work.

Notation

In what follows $\mathcal{O}$, resp. $\mathcal{O}_B$, means bit, resp. arithmetic, complexity and the $\tilde{\mathcal{O}}_B$, resp. $\tilde{\mathcal{O}}$, notation means that we are ignoring logarithmic factors. For a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$, where $n \geq 1$, $\deg(f)$ denotes its total degree, while $\deg_{x_i}(f)$ denotes its degree w.r.t. x_i. By $\mathcal{L}(f)$ we denote the bitsize of the coefficients of f (including a bit for the sign). For $a \in \mathbb{Q}$, $\mathcal{L}(a) \geq 1$ is the maximum bitsize of the numerator and the denominator. Let $\mathrm{M}(\tau)$ denote the bit complexity of multiplying two integers of size τ, and $\mathrm{M}(d, \tau)$ the complexity of multiplying two univariate polynomials of degrees $\leq d$ and coefficient bitsize $\leq \tau$. Using FFT, $\mathrm{M}(\tau) = \tilde{\mathcal{O}}_B(\tau)$, and $\mathrm{M}(d, \tau) = \tilde{\mathcal{O}}_B(d\tau)$. To simplify notation, we will assume throughout the paper that for any polynomial it holds $\log(\mathrm{dg}(f)) = \mathcal{O}(\mathcal{L}(f))$.

Let $\mathrm{sep}(f)$, respectively $\mathrm{sep}(\Sigma)$, denote the separation bound, that is the minimum distance between two, possible complex, roots of the polynomial f, respectively polynomial system (Σ).

2 The DMM bound

2.1 The univariate case

Consider a real univariate polynomial A, not necessarily square-free, of degree d and its complex roots γ_j in ascending magnitude, where $j \in \{1, 2, \ldots, d\}$. The next theorem [41], concerns a bound on the product of differences of the form $|\gamma_i - \gamma_j|$, where $i, j \in \{1, 2, \ldots, d\}$. It slightly generalizes a theorem of Mignotte [29], which in turn generalizes a theorem due to Davenport [15], see also [18, 26]. For this, and because Mahler's measure is used, we call the bound **Davenport-Mahler-Mignotte** in dimension one, or $\mathtt{DMM}_1$ for short, where the subscript denotes the dimension,

Theorem 1 ($\mathtt{DMM}_1$)**.** *Let $A \in \mathbb{C}[X]$, with $\deg(A) = d$ and not necessarily square-free. Let Ω be any set of ℓ couples of indices (i, j) such that $1 \leq i < j \leq d$ and let the non-zero (complex) roots of A be $0 < |\gamma_1| \leq |\gamma_2| \leq \cdots \leq |\gamma_d|$. Then*

$$2^{\ell}\mathcal{M}(A)^{\ell} \geq \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{\ell - \frac{d(d-1)}{2}}\, \mathcal{M}(A)^{1-d-\ell} \sqrt{|\mathsf{disc}(A_{red})|},$$

where A_{red} is the square-free part of A. If $A \in \mathbb{Z}[x]$, $\ell \leq d$ and $\mathcal{L}(A) = \tau$, then

$$d^{d/2}\, 2^{2d\tau} \geq d^{\ell/2}\, 2^{2\ell\tau} \geq \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq d^{-d}\, 2^{-d^2-3\tau(\ell+d)} \geq d^{-d}\, 2^{-d^2-6d\tau}.$$

For the second inequality of the theorem we used the fact that $\mathcal{M}(A) \leq \|A\|_2 \leq (d+1)^{\frac{1}{2}}\, 2^{\tau}$, e.g. [3, 29, 31, 42]. Notice also that in the first inequality we can replace $\mathcal{M}(A)$ with $\|A\|_2$.

A similar theorem but with more strict hypotheses on the roots first appeared in [15] and the conditions were generalized in [18]; namely in order for the bound [15, 18] to hold the sets of indices i and j should be rearranged such that they form an acyclic graph where each node has out-degree at most one. The bound of Th. 1 has an additional factor of 2^{d^2} w.r.t. [15, 18], which plays no role when the polynomials is not square-free or when $d = \mathcal{O}(\tau)$. The current version of the theorem has very loose hypothesis and it could be used for non-square free polynomials, as well. This feature could be used to slightly simplify the proofs for the number of steps of subdivision-based solvers for univariate real root isolation. Nevertheless, it is possible that a more involved and technical proof, based on the technique in [30], may eliminate this factor.

Roughly speaking, $\mathtt{DMM}_1$ provides a bound on all the minimum distances between the roots of a polynomials. We can estimate that this quantity is almost equal to the separation bound, that is the minimum distance between two roots of a polynomial. The interpretation of this is, that not all roots of a polynomial can be very close together, or quoting James H. Davenport, *"not all [the distances between the roots] could be bad"*.

2.2 The multivariate case

Our purpose is to generalize the bound of the previous section to any dimension, that is to bound the product of differences of roots of zero dimensional polynomial systems.

Let n be the number of variables. We use the notation $\mathbf{x}^{\mathbf{e}}$ to denote the monomial (or the power product) $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$, where $\mathbf{e} = (e_1, e_2, \ldots, e_n) \in \mathbb{Z}^n$ is an exponent vector, or equivalently, an integer lattice point, and $n \in \mathbb{Z}_{n>1}$. Our input is n *Laurent polynomials* $f_1, f_2, \ldots, f_n \in K[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}] = K[\mathbf{x}, \mathbf{x}^{-1}]$. Since we can multiply Laurent polynomials by monomials without affecting their zeros, it is without loss of generality to assume that there are no negative exponents. The degree of the $\mathbf{x}^{\mathbf{e}}$ is $e_1 + e_2 + \cdots + e_n$, and the total degree of the original Laurent polynomial is the highest degree of any nonzero term in the new expression.

Let $A_i = \mathrm{supp}(f_i) = \{a_{i1}, \ldots, a_{i,m_i}\} \subset \mathbb{Z}^n$ denote the set of cardinality m_i of exponents vectors corresponding to monomials in f_i with non zero coefficients. We call this set the *support* of f_i, and

$$f_i = \sum_{j=1}^{m_i} c_{i,j} \mathbf{x}^{a_{i,j}}, \quad 1 \leq i \leq n, \tag{1}$$

and thus A_i is uniquely defined, given f_i. The *Newton polytope* $Q_i \subset \mathbb{R}^n$ is the convex hull of the support A_i. We consider the following polynomial system

$$f_1(\mathbf{x}) = f_2(\mathbf{x}) = \cdots = f_n(\mathbf{x}) = 0, \tag{2}$$

which we assume that it is zero dimensional, and we will also denote it by (Σ). We are interested for the (complex) roots of the system in $(\mathbb{C}^*)^n$, which are called toric.

Definition 2. *Given convex polytopes $Q_1, Q_2, \ldots, Q_n \subset \mathbb{R}^n$, there is a unique, up to a multiplication by a scalar, real-valued function $\mathrm{MV}(Q_1, Q_2, \ldots, Q_n)$, called mixed volume of $Q_1, Q_2, \ldots, Q_n$, which is multi-linear with respect to Minkowski addition and scalar multiplication.*

Theorem 3. *For polynomials $f_1, \ldots f_n \in K[\mathbf{x}, \mathbf{x}^{-1}]$ with Newton polytopes $Q_1, \ldots, Q_n \subset \mathbb{R}^n$, the number of common isolated solutions in $(\mathbb{C}^*)^n$, multiplicities counted, does not exceed $\mathrm{MV}(Q_1, \ldots, Q_n)$, independently of the dimension of corresponding variety.*

We use the notation $\mathrm{M}_i = \mathrm{MV}(Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n)$. Let D be the number of complex roots of the system (2). It holds that $D \leq \mathrm{M}_0 = \mathrm{MV}(Q_1, \ldots, Q_n)$. We also use the following abbreviations, $B = (n-1)\binom{D}{2}$, and $C = \prod_{i=1}^{n} \|f_i\|_\infty^{\mathrm{M}_i}$, to simplify the formulae that follow.

Theorem 4 ($\mathtt{DMM}_n$). *Consider the zero dimensional polynomial system (Σ) in (2). Let D be the number of complex solutions of the system in $(\mathbb{C}^*)^n$, which are $0 < |\gamma_1| \leq |\gamma_2| \leq \cdots \leq |\gamma_D|$. Let Ω be any set of ℓ couples of indices (i,j) such that $1 \leq i < j \leq D$. Then the following holds*

$$2^{\ell} \prod_{i=1}^{n} \|f_i\|_{\infty}^{\mathsf{M}_i \ell} \geq \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{-\ell-(D-1)(D+2)/2}\, C^{1-D-\ell}\, B^{-(n-1)(D^2+D(\ell-1)+\ell)} \sqrt{|\mathsf{disc}(U_{red})|},$$

where U_{red} corresponds to the square-free part of the $u-$resultant of the system, and $\mathsf{disc}(U_{red})$ to its discriminant.

In the case were $f_i \in \mathbb{Z}[\mathbf{x}]$ and $\mathcal{L}(f_i) = \tau$, the following proposition presents a simplified bound for $\mathtt{DMM}_n$, as well as an inequality for the separation bound, and an improvement of the "gap theorem" of Canny [11]. We use the inequalities $D \leq d^n$, $\sum_{i=1}^{n} \mathsf{M}_i \leq n d^{n-1}$, and $B \leq nD^2 \leq nd^{2n}$. Moreover, we observe that $C < 2^{n\tau D}$, and that if $D = d^n$, then $C \leq 2^{\tau \sum_{i=1}^{n} \mathsf{M}_i} \leq 2^{n\tau d^{n-1}}$.

Proposition 5 ($\mathtt{DMM}_n$ **and Improved Gap theorem**). *Consider the zero dimensional polynomial system (Σ) in (2), where $f_i \in \mathbb{Z}[\mathbf{x}]$ and $\mathcal{L}(f_i) = \tau$, for $1 \leq i \leq n$, and $\gamma_{j,k}$ stands for the k-th coordinate, $1 \leq k \leq n$, of the j-th, $1 \leq j \leq D$, complex solution of the system, $1 \leq \ell \leq D$, and Ω is as in Th. 4. Then it holds*

$$2^{-n\tau D} \leq 1/C \leq |\gamma_{j,k}| \leq C \leq 2^{n\tau D}, \tag{3}$$

$$\mathsf{sep}(\Sigma) \geq 2^{(1-D)(D+2)/2}\, (D+1)^{-D/2}\, C^{-D} \geq 2^{-2n\tau D^2}\, D^{-D}, \tag{4}$$

$$2^{n\tau D^2 + D} \geq (2C)^D \geq \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{-3n\tau D^2}\, (nD)^{-nD^2}. \tag{5}$$

In the case where $D = d^n$, then

$$2^{-n\tau d^{n-1}} \leq |\gamma_{j,k}| \leq 2^{n\tau d^{n-1}}, \tag{6}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-2d^{2n} - n\tau d^{2n-1} - 1}\, d^{-nd^n/2} \tag{7}$$

$$2^{d^n + n\tau d^{2n-1}} \geq \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{-2n\tau d^{2n-1} - d^{2n}/2}\, n^{-nd^{2n}/2}\, d^{-n^2 d^{2n}}. \tag{8}$$

The proof of the right inequality of Th. 4 is presented in Sec. 3.1, while the proof of the left is in Sec. 3.2. The proofs of the lower and upper bounds on the roots and the separation bound of Prop. 5 are presented in Sec. 3.3.

We can drop the assumption that (Σ) is zero-dimensional, and let D correspond to the number of isolated (complex) solutions of (2). For this we can use the generalized characteristic polynomial [12], and/or the toric generalized characteristic polynomial [14]. We postpone this exposition for a future communication.

3 Proof of the main theorem

3.1 Proof of the lower bound

Let $\gamma_i = (\gamma_{i,1}, \gamma_{i,2}, \ldots, \gamma_{i,n}) \in (\mathbb{C}^*)^n$, where $1 \leq i \leq D$, be the complex solutions of (Σ) defined in Eq. (1), We also denote the set of solutions as $V \subset (\mathbb{C}^*)^n$. We insert an additional equation in (Σ), thus obtaining the following over-constrained system

$$f_0(\mathbf{x}) = f_1(\mathbf{x}) = \cdots = f_n(\mathbf{x}) = 0, \tag{9}$$

which will also call (Σ_0), and f_0 is the polynomial

$$f_0 = u + r_1 x_1 + r_2 x_2 + \cdots + r_n x_n, \tag{10}$$

where $r_1, \ldots, r_n$ are integers to be defined in the sequel and u is a new parameter. We will compute the resultant of the new system. The (new) variable u takes the value $-\sum_i r_i \gamma_{j,i}$, on a solution $\gamma_j = (\gamma_{j,1}, \ldots, \gamma_{j,n})$ of (Σ). We choose the coefficients of f_0 in such a way, so that to ensure that the function

$$\begin{array}{rccc} f_0 & : & V & \to & (\mathbb{C}^*)^n \\ & & \gamma & \mapsto & f_0(\gamma) \end{array} .$$

is injective. The following proposition, e.g. [3, 20, 21, 39], allows us to choose the so-called *separating element*, that ensures the injectivity property of f_0.

Proposition 6. *Let $V \subset \mathbb{C}^n$ with cardinality D. The finite set of linear forms*

$$\left\{ x_1 + i\, x_2 + \cdots + i^{n-1}\, x_n \;\middle|\; 0 \leq i \leq B = (n-1)\binom{D}{2} \right\}$$

contains at least one element that takes distinct values on the elements of V. We call this form separating element.

The previous proposition allows us to bound the coefficients of f_0.

Corollary 7. *For $f_0 \in V$ it holds that $\|f_0\|_\infty \leq B^{n-1}$, and $\|f_0\|_\infty \leq \|f_0\|_2 \leq 2B^{n-1} = 2(n-1)^{n-1}\binom{D}{2}^{n-1}$.*

Proof: Recall that $B = (n-1)\binom{D}{2}$. The first inequality is evident from the definition of the infinite norm. For the second inequality, we have

$$\begin{aligned} \|f_0\|_\infty \leq \|f_0\|_2 &\leq \sqrt{1 + B^2 + B^4 + \cdots + (B^2)^{n-1}} \\ &\leq \sqrt{\tfrac{B^{2n}-1}{B^2-1}} \leq \sqrt{\tfrac{B^{2n-2}}{1-1/B^2}} \leq \sqrt{4B^{2n-2}} = 2B^{n-1}. \end{aligned}$$

□

We consider the resultant of (Σ_0) to eliminate the variables $\mathbf{x}$. The resultant is a univariate polynomial with respect to u, the coefficients of which are homogeneous polynomials in the coefficients of the polynomials of the system, e.g. [35]. This resultant is called $u-$*resultant*. To be more specific the resultant is of the form

$$U(u) = \cdots + u^k \mathbf{r}_k^{D-k} \mathbf{c}_{1,k}^{\mathsf{M}_1} \mathbf{c}_{2,k}^{\mathsf{M}_2} \cdots \mathbf{c}_{n,k}^{\mathsf{M}_n} + \ldots,$$

where $\mathbf{c}_{j,k}^{\mathsf{M}_j}$ denotes a monomial in coefficients of the polynomial f_j that has total degree M_j. Similarly, $\mathbf{r}_k$ is a monomial in the coefficients of f_0 of total degree $D-k$.

The degree of U, with respect to u is D. It holds that

$$\left|\mathbf{c}_{1,k}^{\mathsf{M}_1}\,\mathbf{c}_{2,k}^{\mathsf{M}_2}\,\ldots\,\mathbf{c}_{n,k}^{\mathsf{M}_n}\right| \leq C = \prod_{i=1}^{n} \|f_i\|_\infty^{\mathsf{M}_i}, \tag{11}$$

From Cor. 7 we have that $|\mathbf{r_k}| \leq \|f_0\|_\infty \leq B^{n-1}$, for all k. Now we have all the ingredients to bound the 2-norm of U. We proceed as follows

$$\begin{aligned}
\|U\|_2^2 &\leq \sum_{k=0}^{D} \left|\mathbf{r}_k^{D-k}\mathbf{c}_{1,k}^{\mathsf{M}_1}\mathbf{c}_{2,k}^{\mathsf{M}_2}\ldots\mathbf{c}_{n,k}^{\mathsf{M}_n}\right|^2 \\
&\leq \sum_{k=0}^{D} \left|C\,(B^{n-1})^{D-k}\right|^2 \\
&\leq C^2 \sum_{k=0}^{D} (B^{2n-2})^{D-k} \\
&\leq C^2 \sum_{k=0}^{D} (B^{2n-2})^{k} \\
&\leq C^2\,\tfrac{(B^{2n-2})^{D+1}-1}{B^{2n-2}-1} \\
&\leq C^2\,4\,(B^{2n-2})^{D} \\
&\leq 4\,C^2\,B^{2(n-1)D},
\end{aligned}$$

and so

$$\|U\|_\infty \leq \|U\|_2 \leq 2\,C\,B^{(n-1)D} \leq 2\,(n-1)^{(n-1)D}\binom{D}{2}^{(n-1)D}\prod_{i=1}^{n}\|f_i\|_\infty^{\mathsf{M}_i}.$$

For a similar result concerning the height of the resultant, we refer the reader to [40].

If u_j are the distinct roots of U, then by recalling the previous discussion about the injective nature of f_0, we deduce that $u_j = -\sum_{i=1}^{n} r_i\,\gamma_{j,i}$. Actually the $u-$resultant is even stronger concept, since the multiplicities of the roots of U correspond to the multiplicities of the solutions of the system, but we will not exploit this feature further.

We need the following lemma.

Lemma 8 (Cauchy-Bunyakovsky-Schwartz). *Let $a_1, a_2, \ldots, a_n \in \mathbb{C}$ and $b_1, b_2, \ldots, b_n \in \mathbb{C}$. Then,*

$$|\bar{a}_1\,b_1 + \cdots + \bar{a}_n\,b_n|^2 \leq \left(|a_1|^2 + \cdots + |a_n|^2\right)\left(|b_1|^2 + \cdots + |b_n|^2\right),$$

where $\bar{a}_i$ denotes the complex conjugate of a_i, and $1 \leq i, \leq n$. Equality holds if, for all i, $a_i = 0$ or if there is a scalar λ such that $b_i = \lambda\,a_i$.

Consider two distinct solutions, γ_i and γ_j, of (Σ), and let u_i and u_j be the corresponding roots of U. Using Lem. 8 we get

$$\begin{aligned}
|r_1(\gamma_{i,1}-\gamma_{j,1}) + \cdots + r_n(\gamma_{i,n}-\gamma_{j,n})|^2 &\leq \left(r_1^2+\cdots+r_n^2\right)\left(|\gamma_{i,1}-\gamma_{j,1}|^2+\cdots+|\gamma_{i,n}-\gamma_{j,n}|^2\right) \quad \Leftrightarrow \\
\left|\textstyle\sum_{k=1}^{n} r_k\,\gamma_{i,k} - \sum_{k=1}^{n} r_k\,\gamma_{j,k}\right|^2 &\leq \textstyle\sum_{k=1}^{n} r_k^2 \cdot \sum_{k=1}^{n} |\gamma_{i,k}-\gamma_{j,k}|^2 \quad \Leftrightarrow \\
|u_i - u_j|^2 &\leq \left(\textstyle\sum_{k=1}^{n} r_k^2\right)\cdot|\gamma_i-\gamma_j|^2,
\end{aligned}$$

and thus

$$|\gamma_i - \gamma_j| \geq \left(\sum_{k=1}^{n} r_k^2\right)^{-1/2} |u_i - u_j|\,.$$

To prove the lower bound of Th. 4, we should apply the previous inequality for all the pairs in the set Ω, where $|\Omega| = \ell$. Doing so, we get

$$\prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq \left(\sum_{k=1}^{n} r_k^2\right)^{-\frac{1}{2}\ell} \prod_{(i,j)\in\Omega} |u_i - u_j|. \tag{12}$$

It remains to bound the two factors of the right hand-side of the previous inequality. To bound the first factor we use Cor. 7. It holds

$$\sum_{k=1}^{n} r_k^2 \leq 1 + \sum_{k=1}^{n} r_k^2 \leq \|f_0\|_2^2 \leq 4\, B^{2n-2}, \tag{13}$$

and so

$$\left(\sum_{k=1}^{n} r_k^2\right)^{-\frac{1}{2}\ell} \geq 2^{-\ell}\, B^{(1-n)\ell}. \tag{14}$$

For the second factor of (12) we apply $\texttt{DMM}_1$ to U; and thus

$$\begin{aligned} \textstyle\prod_{(i,j)\in\Omega} |u_i - u_j| &\geq 2^{\ell - D(D-1)/2}\, \|U\|_2^{1-D-\ell}\, \sqrt{\mathsf{disc}(U_{red})} \\ &\geq 2^{(1-D)(D+2)/2} \left(C\, B^{(n-1)D}\right)^{1-D-\ell} \sqrt{\mathsf{disc}(|U_{red}|)}. \end{aligned} \tag{15}$$

Combining (12) with (14) and (15), we have

$$\prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{-\ell-(D-1)(D+2)/2}\, C^{1-D-\ell}\, B^{-(n-1)(D^2+D(\ell-1)+\ell)} \sqrt{\mathsf{disc}(U_{red})},$$

and the proof of the lower bound is completed.

In the case where the polynomials are in $\mathbb{Z}[\mathbf{x}]$, then it holds that the absolute value of the discriminant of a square-free polynomial is ≥ 1, and we can omit it from the inequality. If the polynomials are in $\mathbb{Q}[\mathbf{x}]$ the bounds are almost the same, since they depend on Mahler's measure.

3.2 Proof of the upper bound

We will prove the upper bound of Th. 4, using a technique from polynomial system solving, which is called *hiding a variable*, see for example [21]. The idea is to consider the square system (Σ), see Eq. (2, as an over-constrained system of n polynomials in $n-1$ variables. We consider polynomials $f_i \in \mathbb{Z}[x_t][x_1, \ldots, x_{t-1}, x_{t+1}, \ldots x_n]$, for some $t \in \{1, \ldots, n\}$. As before $D \leq \mathsf{M}_0 = \mathsf{MV}(Q_1, \ldots, Q_n)$, and let $\gamma_j = (\gamma_{j,1}, \ldots, \gamma_{j,n})$ be all the complex solutions of (2), where $1 \leq j \leq D$.

Let $x = x_t$ and let $R(x) \in \mathbb{Z}[x]$ denote the univariate polynomial, the roots of which are the $k-$th coordinates of the isolated zeros of the system, viz. $\gamma_{k,i}$, where $1 \leq i \leq D$. That is R is the resultant of the system, that eliminates all the variables, except x_k. The degree of R is bounded by D. Moreover, it is separately homogeneous in the coefficients of each f_i and its degree in these coefficients equals M_i [35]. Thus, the coefficient of R are of the form $\mathbf{c}_1^{\mathsf{M}_1}\mathbf{c}_2^{\mathsf{M}_2}\ldots\mathbf{c}_n^{\mathsf{M}_n}$, with the same interpretation as in the previous section. From (11) we deduce that

$$\|R\|_\infty \leq C = \prod_{i=1}^{n} \|f_i\|_\infty^{\mathsf{M}_i},$$

and so

$$\|R\|_\infty \leq \|R\|_2 \leq \sqrt{D+1}\,C.$$

From Cauchy's bound for the roots of univariate polynomials e.g. [29], we know that for all the roots of R is holds that $1/C \leq 1/\|R\|_\infty \leq |\gamma_{k,i}| \leq \|R\|_\infty \leq C$. The inequality holds for all the indices k and i. Hence, all the roots of the system in $(\mathbb{C}^*)^n$ are contained in annulus in $\mathbb{C}^n$, defined as the difference of the volumes of two spheres centered at the origin, with radii C and $1/C$, respectively.

Now we are ready to prove the upper bound of Th. 4. For all $a, b \in \mathbb{C}$ it holds that

$$|a-b| \leq 2\max\{|a|,|b|\}. \tag{16}$$

Consider the multiset $\overline{\Omega} = \{j \mid (i,j) \in \Omega\}$, where $\left|\overline{\Omega}\right| = \ell$, then

$$\prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \leq 2^\ell \prod_{j\in\overline{\Omega}} |\gamma_j| \leq 2^\ell\, C^\ell \leq 2^\ell \prod_{i=1}^{n} \|f_i\|_\infty^{\mathsf{M}_i\,\ell}.$$

3.3 Additional inequalities

One of the first multivariate separation bounds was due to Canny, which is the following.

Theorem 9 (Gap theorem). *[11] Let $\mathcal{P}(d,c)$ be the class of polynomials of degree d and coefficient magnitude c. Let $f_1(x_1,\ldots,x_n),\ldots f_n(x_1,\ldots,x_n) \in \mathcal{P}(d,c)$ be a collection of n polynomials in n variables which has only finitely-many solutions. If $\gamma_j = (\gamma_{j,1},\ldots\gamma_{j,n})$ is a solution of the system, then for any k either $\gamma_{j,k} = 0$ or $|\gamma_{j,k}| > (3dc)^{-n\,d^n}$.*

To improve the previous theorem, we apply bounds on R, the resultant of (Σ) used in the previous section, see Eq. (2). We assume that the polynomials of the system are in $\mathbb{Z}[\mathrm{x}]$. We also use the inequalities $D \leq d^n$, $\sum_i \mathsf{M}_i \leq nd^{n-1}$, and $B \leq nD^2 \leq nd^{2n}$. Moreover, we observe that $C < 2^{n\tau D}$, and that if $D = d^n$, then $C \leq 2^{\tau\sum_i \mathsf{M}_i} \leq 2^{n\tau d^{n-1}}$.

Recall, that we obtained R by eliminating all variables but x_j, and that the roots of R are the k-th coordinates of the solutions. By applying the standard Cauchy bound for univariate polynomials, for example [31], we get that the absolute value of the non-zero roots of R, and thus the absolute value of the k-th coordinates of the solutions of (Σ), is bigger $1/\|R\|_\infty \geq 1/C$, and smaller than $\|R\|_\infty \leq C$; which proves (3).

Actually the inequality of Eq. (3) improves the famous Gap theorem of Canny [11] by a factor of 2^d. If the total degree of all the polynomials is bounded by d and the coefficients are bounded by 2^τ then Canny's theorem states that either $\gamma_{j,k} = 0$ or $|\gamma_{j,k}| > (3d)^{-nd^n}\,2^{-n\tau d^n}$. Observing that $\sum_i \mathsf{M}_i = nd^{n-1}$ (3) induces the inequality $\gamma_{j,k} > 2^{n\tau d^{n-1}}$. A similar bound for not necessarily zero dimensional systems, but without using mixed volumes appeared in [7].

For proving (4), let (i,j) be the pair of indices where the separation bound of (Σ) is attained. Then

$$\mathsf{sep}(\Sigma) = |\gamma_i - \gamma_j| = \sqrt{\sum_{k=1}^{n} (\gamma_{i,k} - \gamma_{j,k})^2} \geq |\gamma_{i,k} - \gamma_{j,k}| \geq \mathsf{sep}(R),$$

where k is any index such that $\gamma_{i,k} \neq \gamma_{j,k}$ and $\mathsf{sep}(R)$ is the separation bound of R. An easy bound on the latter could be derived by applying $\mathtt{DMM}_1$ (Th. 1) to R with $\ell = 1$, that is

$$\mathsf{sep}(R) \geq 2^{1-\binom{D}{2}}\,\|R\|_2^{-D} \geq 2^{(1-D)(D+2)/2}\,(D+1)^{-D/2}\,C^{-D} \geq 2^{(1-D)(D+2)/2}\,(D+1)^{-D/2} \prod_{i=1}^{n} \|f_i\|_\infty^{-D\,\mathsf{M}_i},$$

which completes the proof of (4).

Remark 10. *It is tempting to try to prove the lower bound of Th. 4 by applying* DMM$_1$ *to* R*, instead of* U*, as we did in the previous section. Doing so, will allow us to eliminate the factor* $B^{-(n-1)(D^2+\ell(D+1)-D)}$ *from the result.*

However, if we apply DMM$_1$ *to* R *is not obvious at all that the requirements of Th. 1 are fulfilled, i.e. the ordering of (the coordinates of) the roots is preserved. This is why we choose the* $u-$*resultant approach. Moreover, the bounds on* $u-$*resultant are of independent interest, since many algorithms, e.g. [3, 21, 39], for system solving depending on them.*

3.4 Optimality of the result

We consider the following system, which is due to Canny [11].

$$\begin{aligned} Lx_1^2 &= x_1 \\ x_j &= x_{j-1}^d \quad 1 \leq j \leq n \end{aligned}$$

The root of the system are $x_j = \left(\frac{1}{L}\right)^{d^{j-1}}$, for $L \gg 1$. The improved version of Gap theorem (Prop. 5) states that $x_j \geq 2^{-nd^{n-1}\lg L}$, which is off only by a factor of 2^n.

We conjecture that the following system achieves the separation bound.

$$\begin{aligned} x_1\left(x_1^d - 2(Lx_1-1)^2\right) &= 0 \\ x_j\left(x_j^d - 2(x_{j-1}x_j-1)^2\right) &= 0 \quad 1 \leq j \leq n \end{aligned}$$

4 Some applications

We illustrate the bounds of Prop. 5 in two applications. The first one concerns computations of eigenvalues and eigenvectors of a matrix, ans is a standard example for exploiting the superiority of mixed volumes against the Bézout bound. The second application is about lower bounds of positive multivariate polynomials, and it is inspired from [4].

4.1 Eigenvalues and eigenvectors

Consider A to be a $n \times n$ integer matrix, the elements of which are $\leq 2^\tau$. We are interested in computing the eigenvalues of A, say λ, and its eigenvectors, say $\mathbf{v} = (v_1, \ldots, v_n)^\top$. The problem can be reduced to solving a polynomial system, with n equations of the form $f_j = \sum_{j=1}^n a_{i,j}v_j - \lambda v_i$, where $1 \leq i \leq n$ and $1 \leq j \leq n$, and the equation $f_{n+1} = \sum_{i=1}^n v_i^2 - 1$. The unknowns of the system are $v_1, \ldots, v_n$ and λ. That is, we obtain a well constrained polynomial system with $n+1$ polynomials and $n+1$ unknowns. It holds that $\|f_j\|_\infty \leq 2^\tau$, and $\|f_{n+1}\|_\infty \leq 2$.

The degree of each equation is 2, thus the Bézout bound for the system is 2^{n+1}, which is a big overestimation. The actual number of (complex) solutions is $2n$, and this is also the mixed volume of the system, e.g. [21].

Using the Gap theorem (Th. 9), we estimate the absolute value of the non-zero eigenvalues, and the non-zero elements of the eigenvectors, is $> (6 \cdot 2^\tau)^{-(n+1)2^n}$. Thus, in the worst case, we need at least $\mathcal{O}(n\,\tau\,2^n)$ bits to compute them.

It holds that $\mathsf{MV}_j = 2n$, where $1 \leq j \leq n$, and $\mathsf{MV}_{n+1} = n$. Thus

$$C = \prod_{j=1}^{n} \|f_j\|_\infty^{\mathsf{MV}_j} \|f_{n+1}\|_\infty^{\mathsf{MV}_{n+1}} \leq 2^{\tau \sum_{j=1}^{n} \mathsf{MV}_j} \; 2^n = 2^{2n^2\tau+n}.$$

Using the improved version of Gap theorem, see Eq. (6), we estimate that absolute value of the non-zero eigenvalues is $> 1/C > 2^{-2n^2\tau-n}$.

Moreover, using Eq. (7), we deduce that the separation bound of the system is $\geq 2^{-4n^3\tau-2n}\, n^{-2n}$, thus the number of bits that we need in order to compute the eigenvalues/eigenvectors is $\tilde{\mathcal{O}}_B(n^3\tau)$. The previous arguments and bound, is an alternative proof to Bareiss, e.g.[3], that the problem of computing the eigenvalues and eigenvectors of a integer matrix can be solved in polynomial time; since a polynomial number of bits is needed.

4.2 Positive multivariate polynomials

We consider the following problem, studied in [4]. Let $P \in \mathbb{Z}[x_1, \ldots, x_n]$ be a multivariate polynomial of degree d taking only positive values on the $n-$dimensional simplex

$$S = \left\{ x \in \mathbb{R}^n \geq 0 \;\middle|\; \sum_{i=1}^{n} x_i \leq 1 \right\}.$$

We are interested in computing a bound on its minimum value. We may assume that the minimum is attained inside the simplex, since we can always assure that by a transformation that slightly changes the bitsize of P. See [4] for details. Let τ be an upper bound on the bitsize of the coefficients of P. Writing

$$m = \min_S P > 0,$$

we consider the problem of finding an explicit bound $m_{n,d,\tau}$, depending only on n, d and τ, such that $0 < m_{m,d,\tau} < m$.

Under a non-degeneracy assumption on the following polynomial system

$$\begin{cases} P(x_1, \ldots, x_n) = m \\ \frac{\partial P}{\partial x_1}(x_1, \ldots, x_n) = \cdots = \frac{\partial P}{\partial x_n}(x_1, \ldots, x_n) = 0 \end{cases}.$$

Let $P_i = \frac{\partial P}{\partial x_i}$, $1 \leq i \leq n$, and $P_0 = P$. It holds that $\|P_i\|_\infty \leq d\|P_0\|_\infty \leq d\, 2^\tau$, thus

$$C < \prod_{i=0}^{n} \|P_i\|_\infty^{\mathsf{M}_i} \leq \prod_{i=0}^{n} (d\, 2^\tau)^{d^n} \leq d^{(n+1)d^n}\, 2^{(n+1)\tau d^n}.$$

If we apply (6) we get

$$m > \frac{1}{C} \geq d^{-(n+1)d^n}\, 2^{-(n+1)\tau d^n}.$$

In [4, Sec. 2, Rem. 2.17], the following estimation was computed

$$\frac{1}{m_{n,d,\tau}} \leq (2^\tau)^{2^{n+3}d^{n+1}n}\, 2^{2^{n+6}d^{n+2}n^2}\, n^{2^{n+5}d^{n+2}n} d^{2^{n+5}d^{n+1}n^2}.$$

Out bound is better by at least a factor of

$$2^d 2^{2^{n+6}d^{n+2}n^2}\, n^{2^{n+5}d^{n+2}n}.$$

5 Subdivision algorithms

We will use the $\mathtt{DMM}_n$, Th. 4 and Eq. (5) & (8), to compute the number of steps that a subdivision algorithm performs to isolate the real roots of a well-defined polynomial system. We assume the existence of an oracle that outputs the number of real roots inside a box in $\mathbb{Q}^n$.

As an application we compute the complexity of the subdivision algorithm based on Milne's volume function [32] in 2D. Our analysis can easily be extended to dimension n, however it is not clear what is the exact bit complexity of the elimination steps needed. This is of independent interest, and we omit this discussion for a future communication.

5.1 The number of subdivision steps

Suppose that we want compute isolating (hyper-)boxes for the real roots of a system of polynomial equations as the one formed by the polynomials in (1). In our disposal we have an oracle that, given a box, returns the number of real roots of the system in it. Our aim is to compute the number of calls to the oracle that are needed in order to compute isolating boxes for all the real roots of a system. A realization of the oracle can be considered using the results of [32] or [34, 36], see also [3].

Suppose that initially all the roots of the system are contained in a hypercube of side C, see Prop. 5. At the h step of the subdivision algorithm, we have to call the oracle to count the number of real roots of the system in hypercubes then that have sides equal to $C/2^h$.

We may consider the whole process of the subdivision algorithm as a 2^n-ary tree, where each node holds a hypercube and the root of the tree holds the initial one. Each leaf of the tree contains contains a hypercube that isolates a real root of the system, and if there are at most R real roots, this is also the number of the leaves of the tree. The hypercubes that correspond to the leaves of the tree have diagonals that are at least $\Delta_j = |\gamma_j - \gamma_{c_j}|$, and the lengths of their edges are at least $|\gamma_{j,i} - \gamma_{c_j,i}|$, where $1 \leq i \leq n$. It holds that

$$\Delta_j = |\gamma_j - \gamma_{c_j}| \geq |\gamma_{j,i} - \gamma_{c_j,i}|,$$

for any index i. The number of nodes from a leaf to the root of the tree is $\left\lceil \log \frac{C}{\Delta_j} \right\rceil$.

The number of subdivisions, $\#(T)$, that the algorithm performs equals the number of nodes of the subdivision tree, which is

$$\#(T) = \sum_{j=1}^{R} \left\lceil \log \frac{C}{\Delta_j} \right\rceil = R + R \lg C - \lg \prod_{j=1}^{R} \Delta_j. \tag{17}$$

It suffices to bound the various quantities that appears in previous equation. From Prop. 5 we get $C \leq \prod_{i=1}^{n} \|f_i\|_\infty^{\mathsf{M}_i}$, and so $\lg C \leq \sum_{i=1}^{n} \mathsf{M}_i \lg \|f_i\|_\infty$. If the total degree of the polynomials is bounded by d, and $\|f_i\|_\infty \leq 2^\tau$, then $\lg C \leq n\,\tau\, d^{n-1}$.

To bound $\prod_{j=1}^{R} \Delta_j$ we use Th. 4 with $\ell = R$. The hypotheses of the theorem, concerning the indices of the roots, are not fulfilled when symmetric products occur. In this case, we factorize quantity as $\prod_{i=1}^{R} \Delta_i = \prod_{i=1}^{R_1} \Delta_i \prod_{i=1}^{R_2} \Delta_i$, where $R_1 + R_2 = R$ and the factors are such that no symmetric products occur.

$$\prod_{i=1}^{R} \Delta_i = \prod_{i=1}^{R_1} \Delta_i \prod_{R=1}^{R_2} \Delta_i \geq 2^{-R-(D-1)(D+2)}\, C^{2-2D-R}\, B^{-(n-1)(2D^2+D(R+2)+R)}.$$

If we take into account that $R \leq D$, then

$$-\log \prod_{i=1}^{R} \Delta_i \leq 2D^2 + 6nD^2 \lg nD^2 + 3D \sum_{i=1}^{n} \mathsf{M}_i \lg \|f_i\|_\infty.$$

Thus, for the number of subdivisions we have

$$\begin{array}{rcl} \#(T) & \leq & 2D^2 + D + 6nD^2 \lg nD^2 + 4D \sum_{i=1}^{n} \mathsf{M}_i \lg \|f_i\|_\infty \\ & \leq & 7nD^2 \lg nD^2 + 4D \sum_{i=1}^{n} \mathsf{M}_i \lg \|f_i\|_\infty \\ & = & \mathcal{O}(nD^2 \lg nD + D \sum_{i=1}^{n} \mathsf{M}_i \lg \|f_i\|_\infty) \end{array}$$

In the worst case, we have $D \leq d^n$. If the total degree of the polynomials is bounded by d, and $\|f_i\|_\infty \leq 2^\tau$, then the total number of steps becomes $\#(T) = \mathcal{O}(n^2 d^{2n} \lg nd + n\tau d^{2n-1})$.

We can now state the following theorem.

Theorem 11. *Consider the polynomial system formed by the polynomials in (1). The number of steps that a subdivision algorithm performs in order to compute isolating boxes for all the real roots of the system is* $\mathcal{O}(nD^2 \lg nD + D \sum_{i=1}^{n} \mathsf{M}_i \lg \|f_i\|_\infty)$ *or* $\mathcal{O}(nD^2 \lg nD + D \sum_{i=1}^{n} \mathsf{M}_i \lg \|f_i\|_\infty)$.

Remark 12. *If we specialize* $n = 1$ *in the previous theorem, then we deduce that the number of steps of subdivisions algorithms for real root isolation of univariate integer, not necessarily square-free, polynomials is* $\mathcal{O}(d\tau + d^2 \lg d)$. *The optimal bound is* $\mathcal{O}(d^2 + d\tau)$ *[15].*

5.2 The complexity of Milne in 2D

We study the complexity of Milne's algorithm [32] for isolating the real roots of a polynomial system in two variables. Milne's, so-called, *volume function*, provides a realization of the oracle needed by the subdivision algorithms.

We will use the following results for the analysis.

Proposition 13. *[17, 38] We can compute* $\mathbf{SQ}(f, g)$, *any polynomial in* $\mathbf{SR}(f, g)$, *and* $\mathtt{Res}(f, g)$ *w.r.t.* x *in* $\tilde{\mathcal{O}}_B(q(p+q)^{k+1}d\tau)$. *The degree of* $\mathbf{SR}(f, g)$ *in* $y_1, \ldots, y_k$ *is* $\mathcal{O}(d(p+q))$ *and the bitsize is* $\mathcal{O}((p+q)\tau)$.

Proposition 14. *[17] We can evaluate* $\mathbf{SR}(f, g)$ *at* $x = \mathsf{a}$ *where* $\mathsf{a} \in \mathbb{Q} \cup \{\infty\}$ *and* $\mathcal{L}(\mathsf{a}) = \sigma$, *in* $\tilde{\mathcal{O}}_B(q(p+q)^{k+1}d \max\{\tau, \sigma\})$.

Let $f, g \in \mathbb{Z}[x, y]$ with total degrees bounded by d and bitsize bounded by τ. We are interested in isolating the real roots of the polynomial system $f(x, y) = g(x, y) = 0$, which we assume that is zero dimensional.

We introduce new parameter u, a and b and we want to eliminate a and b from the following set of polynomials

$$\{f(a, b), g(a, b), V = u + (x - a)(y - b)\},$$

where V is the volume function. After elimination a polynomial $h \in (\mathbb{Z}[x, y])[u]$ is obtained. We consider the evaluation of $\mathbf{SR}(h, h_u)$ over 0, where h_u is the derivative of h w.r.t. u. Now consider a box in the plane. We evaluate the sequence on each vertex of the box, and we count the number of sign variations. The number of real roots of the system inside the box, is $\frac{1}{4}$ the sum of the sign variations. We refer the reader to [32] for details.

Let us now study the complexity of the algorithm. We perform the elimination using iterated resultants.

Using Prop. 13 we can compute $h_1 = \mathtt{Res}_a(f(a,b), V(u,x,y,a,b)) \in \mathbb{Z}[u,x,y,a,b]$ in $\tilde{\mathcal{O}}_B(d^7\tau)$. The total degree of h_1 is $\mathcal{O}(d^2)$ and $\mathcal{L}(h_1) = \tilde{\mathcal{O}}(d\tau)$. Similarly we obtain the polynomial $h_2 = \mathtt{Res}_a(g(a,b), V(u,x,y,a,b)) \in \mathbb{Z}[u,x,y,a,b]$. Finally, $h = \mathtt{Res}_b(h_1,h_2) \in \mathbb{Z}[x,y,u]$ can be computed in $\tilde{\mathcal{O}}_B(d^{12}\tau)$. The degree of h with respect to u is $\mathcal{O}(d^2)$ since the resultant of h_1 and h_2 has always the factor $u^{\mathrm{dg}(f(x,0))\mathrm{dg}(g(x,0))} = u^{d^2}$. The degree of h with respect to x,y is $\tilde{\mathcal{O}}_B(d^4)$ and $\mathcal{L}(h) = \tilde{\mathcal{O}}(d^3\tau)$.

Next, we compute the signed polynomial remainder sequence of h and h_u and we evaluate it at 0. This costs $\tilde{\mathcal{O}}_B(d^{15}\tau)$. The evaluated sequence contains $\mathcal{O}(d^2)$ polynomials in $\mathbb{Z}[x,y]$ of degrees $\tilde{\mathcal{O}}_B(d^6)$ and bitsize $\tilde{\mathcal{O}}_B(d^5\tau)$.

Each polynomial in the sequence can be evaluated over a rational number of bitsize σ in $\tilde{\mathcal{O}}_B(d^{17}(\tau + d\sigma))$, and thus all of them in $\tilde{\mathcal{O}}_B(d^{19}(\tau + d\sigma))$. [1]

In the worst case we have to perform evaluations over rational number with bitsize that equals the separation bound, i.e. $\tilde{\mathcal{O}}(d^3\tau)$. Hence, the evaluation of the sequence, in the worst case costs $\tilde{\mathcal{O}}_B(d^{23}\tau)$.

Th. 11 indicates that the number of steps that we need to perform is $\mathcal{O}(d^4 \lg d + d^3\tau)$.

The overall cost of the algorithm is $\tilde{\mathcal{O}}_B(d^{27}\tau + d^{26}\tau^2)$.

Theorem 15. *Let $f, g \in \mathbb{Z}[x,y]$ with total degrees bounded by d and bitsize bounded by τ. Using the algorithm of Milne [32], we can isolate the real roots of the system $f = g = 0$, $\tilde{\mathcal{O}}_B(d^{27}\tau + d^{26}\tau^2)$, or $\tilde{\mathcal{O}}_B(N^{28})$, where $N = \max\{d,\tau\}$.*

A more involved analysis using bounds on mutli-point evaluation of multivariate polynomials [33] could save at least two factor from the complexity bound of the previous theorem.

6 Conclusion and Future work

We introduced the $\mathtt{DMM}_n$ bound, which is a an aggregate separation bound for the (complex) roots of a polynomial system, which improves and extends the "Gap theorem" of Canny. We applied the bounds to two applications, that is to the computation of eigenvectors and eigenvalues, and to the estimation of the minimum of a positive polynomial over the standard simplex. We also used $\mathtt{DMM}_n$ to bound the number of steps that a subdivision-based solver in dimension $n > 1$, and we computed the complexity of Milne's algorithm for solving polynomial systems in $\mathbb{R}^2$.

Even though $\mathtt{DMM}_n$ is a big improvement and also has an expression with respect to the mixed volume of the system, thus exploits sparsity, it still remains a worst-case separation bound. The polynomial systems appear in practice have a small number of real roots and all their roots, real and complex, are well separated. Hence, $\mathtt{DMM}_n$ is still a big overestimation. It is quite challenging to derive average case version(s) of $\mathtt{DMM}_n$.

[1] The the evaluation a bivariate polynomial of total degree n and bitsize L, over a rational number of bitsize σ, costs $\tilde{\mathcal{O}}_B(n^2(L + d\sigma))$. To see this consider the polynomial univariate in x. Then its coefficients, $\mathcal{O}(n)$, are univariate polynomials in y. We evaluate each of them in $\tilde{\mathcal{O}}_B(n(n\sigma + L))$, and all of them in $\tilde{\mathcal{O}}_B(n^2(n\sigma + L))$. After these $\mathcal{O}(n)$ evaluations, we have a polynomial in x of degree $\mathcal{O}(n)$ and bitsize $\mathcal{O}(n\sigma + L)$, to evaluate over a rational of bitsize σ. This costs $\tilde{\mathcal{O}}_B(n(n\sigma + L)$.

Acknowledgments

I. E. and B. M. are partially supported by Marie-Curie Network "SAGA", FP7 contract PITN-GA-2008-214584. B. M. and E. T. acknowledge partial support by contract ANR-06-BLAN-0074 "Decotes".

References

[1] L. Alberti and B. Mourrain. Visualisation of implicit algebraic curves. In M. Alexa, S. Gortler, and T. Ju, editors, *Pacific Graphics*, pages 303–312, Hawaii, U.S.A., 2007. IEEE Computer Society.

[2] L. Alberti, B. Mourrain, and J. Wintz. Topology and arrangement computation of semi-algebraic planar curves. *Computer Aided Geometric Design*, 25:631–651, 2008.

[3] S. Basu, R. Pollack, and M-F. Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 2nd edition, 2006.

[4] S. Basu, R. Leroy, and M-F. Roy. A bound on the minimum of the real positive polynomial over the standard simplex. Technical Report arXiv:0902.3304v1, arXiv, Feb 2009.

[5] E. Berberich, M. Kerber, and M. Sagraloff. Exact geometric-topological analysis of algebraic surfaces. In *24th Proc. Annual ACM Symp. on Computational Geometry*, pages 164–173. ACM New York, NY, USA, 2008.

[6] 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*, Mathematics and Visualization series, chapter 5, pages 181–229. Springer-Verlag, 2006.

[7] W. D. Brownawell and C. K. Yap. Lower Bounds for Zero-Dimensional Projections. In *34th Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation (ISSAC)*, KIAS, Seul, Korea, 2009.

[8] C. Burnikel, S. Funke, K. Mehlhorn, S. Schirra, and S. Schmitt. A separation bound for real algebraic expressions. *Algorithmica*, 55(1):14–28, 1995.

[9] C. Burnikel, R. Fleischer, K. Mehlhorn, and S. Schirra. A strong and easily computable separation bound for arithmetic expressions involving radicals. *Algorithmica*, 27(1):87–99, 2000.

[10] M. Burr, S.W. Choi, B. Galehouse, and C. K. Yap. Complete subdivision algorithms, II: Isotopic meshing of singular algebraic curves. In *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation (ISSAC)*, pages 87–94, Hagenberg, Austria, 2008.

[11] J. Canny. *The Complexity of Robot Motion Planning*. ACM – MIT Press Doctoral Dissertation Award Series. MIT Press, Cambridge, MA, 1987. ISBN 0-262-03136-1.

[12] J. Canny. Generalised characteristic polynomials. *J. Symbolic Computation*, 9(3):241–250, 1990.

[13] J. Chen, S. Lazard, L. Peñaranda, M. Pouget, F. Rouillier, and E. P. Tsigaridas. On the topology of planar algebraic curves. In *25th Proc. Annual ACM Symp. on Computational Geometry*, Aarhus, Denmark, 2009. (to appear).

[14] C. D Andrea and I.Z. Emiris. Computing sparse projection operators. *Contemporary Mathematics*, 286:121–140, 2001.

[15] J. H. Davenport. Cylindrical algebraic decomposition. Technical Report 88–10, School of Mathematical Sciences, University of Bath, England, available at: http://www.bath.ac.uk/masjhd/, 1988.

[16] J.-P. Dedieu. Estimations for the separation number of a polynomial system. *J. Symbolic Computation*, 24(6):683–693, 1997.

[17] D. I. Diochnos, I. Z. Emiris, and E. P. Tsigaridas. On the complexity of real solving bivariate systems. In C. W. Brown, editor, *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation (ISSAC)*, pages 127–134, Waterloo, Canada, 2007.

[18] A. Eigenwillig, V. Sharma, and C. K. Yap. Almost tight recursion tree bounds for the Descartes method. In *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation (ISSAC)*, pages 71–78, New York, USA, 2006.

[19] A. Eigenwillig, M. Kerber, and N. Wolpert. Fast and exact geometric analysis of real algebraic plane curves. In *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation (ISSAC)*, pages 151–158. ACM New York, NY, USA, 2007.

[20] M. Elkadi and B. Mourrain. *Introduction á la résolution des systémes polynomiaux*, volume 59 of *Mathḿatiques et Applications*. Springer, 2007. ISBN 978-3-540-71646-4.

[21] I. Z. Emiris. *Sparse Elimination and Applications in Kinematics*. PhD thesis, Computer Science Division, Univ. of California at Berkeley, December 1994.

[22] I. Z. Emiris, A. Kakargias, S. Pion, M. Teillaud, and E. P. Tsigaridas. Towards and open curved kernel. In J. Snoeyink and J-D. Boissonnat, editors, *Proc. 20th Annual ACM Symp. on Computational Geometry (SoCG)*, pages 438–446, New York, USA, Jun 8–11 2004. ACM.

[23] I. Z. Emiris, E. P. Tsigaridas, and G. M. Tzoumas. Predicates for the exact Voronoi diagram of ellipses under the Euclidean metric. *Int. J. of Computational Geometry and its Applications*, 2007. special issue devoted to SoCG 2007.

[24] I. Z. Emiris, E. P Tsigaridas, and G. M. Tzoumas. Exact Delaunay graph of smooth convex pseudo-circles: General predicates, and implementation for ellipses. In *Proc. SIAM/ACM Joint Conf. Geometric & Solid Modeling*, San Francisco, 2009. (to appear).

[25] X.-S. Gao J.-S. Cheng and C. K. Yap. Complete numerical isolation of real zeros in general triangular systems. In *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation (ISSAC)*, pages 92–99, 2007. (To Appear, JSC 2009).

[26] J. R. Johnson. *Algorithms for Polynomial Real Root Isolation*. PhD thesis, The Ohio State University, 1991.

[27] C. Liang, B. Mourrain, and J-P. Pavone. Subdivision Methods for the Topology of 2d and 3d Implicit Curves. In B. Juetller and R. Piene, editors, *Geometric Modeling and Algebraic Geometry*, pages 199–214. Springer, 2007. ISBN 978-3-540-72184-0.

[28] L. Lin and C. K. Yap. Adaptive isotopic approximation of nonsingular curves: the parametrizability and non-local isotopy approach. In *25thProc. Annual ACM Symp. on Computational Geometry*, page to appear, Aarhus, Denmark, June 2009.

[29] M. Mignotte. *Mathematics for computer algebra*. Springer-Verlag, New York, 1991.

[30] M. Mignotte. On the Distance Between the Roots of a Polynomial. *Appl. Algebra Eng. Commun. Comput.*, 6(6):327–332, 1995.

[31] M. Mignotte and D. Ştefănescu. *Polynomials: An algorithmic approach*. Springer, 1999.

[32] P. S. Milne. On the solution of a set of polynomial equations. In B. Donald, D. Kapur, and J. Mundy, editors, *Symbolic and Numerical Computation for Artificial Intelligence*, pages 89–102. Academic Press, 1992.

[33] M. Nüsken and M. Ziegler. Fast multipoint evaluation of bivariate polynomials. In S. Albers and T. Radzik, editors, *ESA*, volume 3221 of *Lecture Notes in Computer Science*, pages 544–555. Springer, 2004. ISBN 3-540-23025-4.

[34] P. Pedersen. *Counting real zeros*. PhD thesis, New York Univ., NY, 1991.

[35] P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Math. Zeitschrift*, 214:377–396, 1993.

[36] P. Pedersen, M-F. Roy, and A. Szpirglas. Counting real zeros in the multivariate case. In F. Eyssette and A. Galligo, editors, *Computational Algebraic Geometry*, volume 109 of *Progress in Mathematics*, pages 203–224. Birkhäuser, Boston, 1993. (Proc. MEGA '92, Nice).

[37] S. Pion and C. K. Yap. Constructive root bound method for k-ary rational input numbers. In *Proc. 18th ACM Symp. on Computational Geometry*. ACM Press, June 2003. San Diego, California.

[38] D. Reischert. Asymptotically fast computation of subresultants. In *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation (ISSAC)*, pages 233–240, 1997.

[39] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *J. of Applicable Algebra in Engineering, Communication and Computing*, 9(5): 433–461, 1999.

[40] M. Sombra. The height of the mixed sparse resultant. *Amer. J. Math.*, 126:1253–1260, 2004.

[41] E. P. Tsigaridas and I. Z. Emiris. On the complexity of real root isolation using Continued Fractions. *Theoretical Computer Science*, 392:158–173, 2008.

[42] C. K. Yap. *Fundamental Problems of Algorithmic Algebra*. Oxford University Press, New York, 2000.

[43] C. K. Yap. Towards exact geometric computation. *Computational Geometry: Theory and Applications*, 7:3–23, 1997.

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

[45] C. K. Yap and T. Dubé. The exact computation paradigm. In D.-Z. Du and F. K. Hwang, editors, *Computing in Euclidean Geometry*, volume 4 of *Lecture Notes Series on Computing*, pages 452–492. World Scientific, Singapore, 2nd edition, 1995.