The DMM bound: Multivariate (aggregate) separation bounds

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

May 14, 2010

Abstract

In this paper we derive aggregate separation bounds, named after Davenport-Mahler-Mignotte (DMM), on the isolated roots of polynomial systems, specifically on the minimum distance between any two such roots. The bounds exploit the structure of the system and the height of the sparse (or toric) resultant by means of mixed volume, as well as recent advances on aggregate root bounds for univariate polynomials, and are applicable to arbitrary positive dimensional systems. We improve upon Canny's gap theorem [7] by a factor of $\mathcal{O}(d^{n-1})$, where d bounds the degree of the polynomials, and n is the number of variables. One application is to the bitsize of the eigenvalues and eigenvectors of an integer matrix, which also yields a new proof that the problem is strongly polynomial. We also compare against recent lower bounds on the absolute value of the root coordinates by Brownawell and Yap [5], obtained under the hypothesis there is a 0-dimensional projection. Our bounds are in general comparable, but exploit sparseness; they are also tighter when bounding the value of a positive polynomial over the simplex. For this problem, we also improve upon the bounds in [2, 16]. Our analysis provides a precise asymptotic upper bound on the number of steps that subdivision-based algorithms perform in order to isolate all real roots of a polynomial system. This leads to the first complexity bound of Milne's algorithm [22] in 2D.

Categories and Subject Descriptors: F.2 [Theory of Computation]: Analysis of Algorithms and Problem Complexity; I.1 [Computing Methodology]: Symbolic and algebraic manipulation: Algorithms

1 Introduction

One of the great challenges in algebraic algorithms is to fully understand the theoretical and practical complexity of methods based on exact arithmetic. One goal may be towards hybrid symbolic-numeric approaches that exploit both exact and approximate computations. Computing all roots, in some representation, of systems of multivariate polynomials is a fundamental question in both symbolic and numeric computation. The complexity analysis and the actual runtimes typically depend on *separation bounds*, i.e. the minimum distance between any two, possibly complex, roots of the system. This is particularly true for algorithms based on subdivision techniques and, more generally, for any numerical solver seeking to certify its output. Hence, separation bounds are of great use in areas such as computational geometry and geometric modeling.

*National Kapodistrian University of Athens, Greece. Email: `emiris(at)di.uoa.gr`
†INRIA Méditerranée, Sophia-Antipolis, France. Emai: `mourrain(at)inria.fr`
‡Århus University, Denmark. Email: `elias.tsigaridas(at)gmail.com`

Davenport [11] was first to introduce aggregate separation bounds for the real roots of a univariate polynomial, which depend on Mahler's measure, e.g. [20]. Mignotte [21] loosened the hypothesis on the bounds and extended them to complex roots.

As for algebraic systems, a fundamental result is Canny's Gap theorem [7], on the separation bound for square 0-dimensional systems, see Th. 10. Yap [31] relaxed the 0-dimensional requirement by requiring it holds only on the affine part of the variety. A recent lower bound on the absolute value of the root coordinates [5] applies to those coordinates for which the variety's projection has dimension 0, and does not require the system to be square. For arithmetic bounds applied to Nullstellensatz we refer to [18].

Basu, Leroy, and Roy [2] and, recently, Jeronimo and Perrucci [16] considered the closely related problem of computing a lower bound for the minimum value of a positive polynomial over the standard simplex. For this, they compute lower bounds on the roots of polynomial system formed by the polynomial and all its partial derivatives. This problem is also treated in [5].

Separation bounds are important for estimating the complexity of subdivision-based algorithms for solving polynomial systems, that depend on exclusion/inclusion predicates or root counting techniques, e.g. [30, 19, 6, 22, 15].

Our contribution. We derive worst-case (aggregate) separation bounds for the roots of polynomial systems, which are not necessarily 0-dimensional. The bounds are computed as a function of the number of variables, the norm of the polynomials, and a bound on the number of roots of well-constrained systems. For the latter we employ mixed volume in order to exploit the sparse structure that appears in many applications. Any future better bound can be used to improve our results. The main ingredients of our proof are resultants, including bounds on their height [28].

We extend the known separation bound for single polynomial equations to 0-dimensional systems, and call it $\mathtt{DMM}_n$, after *Davenport-Mahler-Mignotte*. This improves upon Canny's Gap theorem by $\mathcal{O}(d^{n-1})$. Our bounds are within a factor of $\mathcal{O}(2^n)$ from optimal for certain systems, which is good for n small (or constant) compared to the other parameters. They are comparable to those in [5] on the absolute value of root coordinates, but they are an improvement when expressed using mixed volumes. It seems nontrivial to apply sparse elimination theory to the approach of [5]. More importantly, our result is extended to positive-dimensional systems, thus addressing a problem that has only been examined very recently in [5].

We illustrate our bounds on computing the eigenvalues / eigenvectors of an integer matrix, and improve upon Canny's bound by a factor exponential in matrix dimension. Thanks to mixed volume, we derive a bound polynomial in the logarithm of the input size, hence offering a new alternative to Bareiss' result [1] that the problem is of polynomial bit complexity. We also bound the minimum of a positive polynomial over the standard simplex and improve upon the 3 best known bounds [2, 5, 16], when the total degree is larger than the number of variables.

Finally, we upper bound the number of steps for any subdivision based algorithm using a real-root counter in a box to isolate the real roots of a system in a given domain. This leads to the first complexity bound of Milne's algorithm [22] in $\mathbb{R}^2$. This aggregate separation bound is also useful in the analysis of the subdivision algorithm based on continued fractions expansion [19] for polynomial system solving.

The polynomial systems in practice have a small number of real roots and all roots, real and complex, are well separated; it is challenging to derive an average-case $\mathtt{DMM}_n$. Another open question is to express the positive-dimensional bound wrt the dimension of the excess component.

Paper structure. We introduce some notation, then Sec. 2 derives and proves the multivariate version of DMM as main Thm. 3. Its near-optimality and comparisons to existing bounds are in Sec. 3, which also extends it to positive-dimensional systems. Two applications of our bounds are in Sec. 4. Sec. 5 is devoted to subdivision algorithms.

Notation. $\mathcal{O}$, resp. $\mathcal{O}_B$, means bit, resp. arithmetic, complexity and $\widetilde{\mathcal{O}}_B$, resp. $\widetilde{\mathcal{O}}$, means 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 maximum 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 denominator. For simplicity, we assume, for any polynomial, $\log(\mathsf{dg}(f)) = \mathcal{O}(\mathcal{L}(f))$. Let $\mathsf{sep}(f)$, resp. $\mathsf{sep}(\Sigma)$, denote the separation bound, i.e. the minimum distance between two, possibly complex, roots of polynomial f, resp. system (Σ). For $f = a_d \prod_{i=1}^{d}(x - z_i) \in \mathbb{C}[x]$, with $a_d \neq 0$, its Mahler measure is $\mathcal{M}(f) := 4|a_d| \prod_{i=1}^{d} \max\{1, |z_i|\}$.

2 The DMM bound

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 [29] bounds the product of differences of the form $|\gamma_i - \gamma_j|$. It slightly generalizes a theorem in [20], which in turn generalizes [11], see also [17, 13].

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

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

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

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

The second inequality follows from: $\mathcal{M}(f) \leq \|f\|_2 \leq (d+1)\|f\|_\infty \leq (d+1)^{\frac{1}{2}}\, 2^{\tau}$, e.g. [20, 31]. In the first inequality we can replace $\mathcal{M}(f)$ by $\|f\|_2$.

The bound of Thm. 1 has an additional factor of 2^{d^2} wrt [11, 13], which is, asymptotically, not significant when the polynomial is not square-free or $d = \mathcal{O}(\tau)$. The current version of the theorem has very loose hypotheses and applies to non-squarefree polynomials.

Roughly, $\mathtt{DMM}_1$ provides a bound on all distances between consecutive roots of a polynomial. This quantity is, asymptotically, almost equal to the separation bound. The interpretation is that not all roots of a polynomial can be very close together or, quoting J.H. Davenport, *"not all [distances between the roots] could be bad"*.

The multivariate case. This section generalizes $\mathtt{DMM}_1$ to 0-dimensional polynomial systems. Let $n > 1$ be the number of variables. We use $\mathbf{x}^{\mathbf{e}}$ to denote the monomial $x_1^{e_1} \cdots x_n^{e_n}$, with $\mathbf{e} = (e_1, \ldots, e_n) \in \mathbb{Z}^n$. The input is *Laurent polynomials* $f_1, \ldots, f_n \in K[x_1^{\pm}, \ldots, x_n^{\pm}] = K[\mathbf{x}, \mathbf{x}^{-1}]$, where $K \subset \mathbb{C}$ is the coefficient field. Since we can multiply Laurent polynomials by monomials without affecting their nonzero roots, in the sequel we assume there are no negative exponents. Let the polynomials be

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

Let $\{a_{i,1},\dots,a_{i,m_i}\} \subset \mathbb{Z}^n$ be the support of f_i; its Newton polytope Q_i is the convex hull of the support. Let $\mathsf{MV}(Q_1,\dots,Q_n) > 0$ be the *mixed volume* of convex polytopes $Q_1,\dots,Q_n \subset \mathbb{R}^n$. Here is Bernstein's bound, known also as BKK bound.

Theorem 2. *For $f_1,\dots f_n \in \mathbb{C}[\mathbf{x},\mathbf{x}^{-1}]$ with Newton polytopes $Q_1,\dots,Q_n$, the number of common isolated solutions in $(\mathbb{C}^*)^n$, multiplicities counted, does not exceed $\mathsf{MV}(Q_1,\dots,Q_n)$, independently of the corresponding variety's dimension.*

We consider polynomial system

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

where $f_i \in \mathbb{R}[\mathbf{x}^{\pm 1}]$, which we assume to be 0-dimensional. We are interested in its roots in $(\mathbb{C}^*)^n$, which are called toric. We denote by Q_0 the convex hull of the unit standard simplex. Let $\mathsf{M}_i = \mathsf{MV}(Q_0,\dots,Q_{i-1},Q_{i+1},\dots,Q_n)$, and $\#Q_i$ denote the number of lattice points in the closed polytope Q_i. Wlog, assume $\dim \sum_{i=0}^n Q_i = n$ and $\dim \sum_{i\in I} Q_i \geq j$ for any $I \subset \{0,\dots,n\}$ with $|I| = j$. We consider the *sparse (or toric) resultant* of a system of $n+1$ polynomial equations in n variables, assuming we have fixed the $n+1$ supports. It provides a condition on the coefficients for the solvability of the system, and generalizes the classical resultant of n homogeneous polynomials, by taking into account the supports of the polynomials. For details, see [9].

Let D be the number of roots $\in (\mathbb{C}^*)^n$ of (Σ), multiplicities counted, so $D \leq \mathsf{M}_0$. We also use $B = (n-1)\binom{D}{2}$, and $\mathsf{dg}(f_i) = d_i \leq d$. If $f_i \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$, $\mathcal{L}(f_i) = \tau_i \leq \tau$, $1 \leq i \leq n$. Now $\mathrm{vol}(\cdot)$ stands for Euclidean volume, and $(\#Q_i)$ for the number of lattice points in Q_i; the inequality connecting $(\#Q_i)$ and polytope volume is in [4]. We present the abbreviations and inequalities used throughout the paper:

$$\begin{aligned}
& D \leq M_0 \leq \prod_{i=1}^n d_i \leq d^n, \quad B \leq nD^2 \leq n\prod_{i=1}^n d_i^2 \leq nd^{2n}, \\
& \mathsf{M}_i \leq \prod_{\substack{1\leq j\leq n \\ j\neq i}} d_j = D_i, \qquad \sum_{i=1}^n \mathsf{M}_i \leq \sum_{i=1}^n D_i \leq nd^{n-1}, \\
& (\#Q_i) \leq n!\,\mathrm{vol}(Q_i) + n \leq d_i^n + n \leq 2d_i^n, \\
& A = \prod_{i=1}^n \sqrt{\mathsf{M}_i}\, 2^{\mathsf{M}_i} \leq 2^{nd^{n-1} + \frac{n^2-n}{2}\lg d}, \\
& C = \prod_{i=1}^n \|f_i\|_\infty^{M_j} \leq 2^{\tau \sum_{i=1}^n \mathsf{M}_i} \leq 2^{n\tau d^{n-1}}, \\
& h \leq (n+1)^D \varrho \leq (n+1)^{d^n} 2^{nd^{n-1}} d^{n^2 d^{n-1}}, \\
& \varrho = \prod_{i=1}^n (\#Q_i)^{M_i} \leq 2^{\sum_{i=1}^n D_i} \prod_{i=1}^n d_i^{nD_i} \leq 2^{nd^{n-1}} d^{n^2 d^{n-1}}.
\end{aligned} \tag{3}$$

Theorem 3 ($\mathtt{DMM}_n$). *Consider the 0-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* $1 \leq i < j \leq D$ *and* $\gamma_i \neq \gamma_j$. *Then the following holds*

$$(2^{D+1}\,\varrho\, C)^{\ell} \geq \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{-\ell-(D-1)(D+2)/2}\,(h\,C)^{1-D-\ell}\, B^{(1-n)(D^2+D(\ell-1)+\ell)}\,\sqrt{|U_r|}, \tag{4}$$

where $|U_r|$ *denotes the discriminant of the square-free part of the* $u-$*resultant, and* $|\cdot|$ *denotes absolute value. If* $f_i \in \mathbb{Z}[\mathbf{x}]$ *and* $\gamma_{j,k}$ *stands for the* k*-th coordinate,* $1 \leq k \leq n$*, of* γ_j*, then:*

$$(2^D\,\varrho\, C)^{-1} \leq |\gamma_{j,k}| \leq 2^D\,\varrho\, C, \tag{5}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-(3D+2)(D-1)/2}\,(\sqrt{D+1}\,\varrho\, C)^{-D}. \tag{6}$$

The following corollary employs mixed volumes.

Corollary 4. *Under the hypothesis of Th. 3, for* $f_i \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$*,* $i = 1, \ldots, n$*, we have*

$$\begin{aligned} &2^{\mathsf{M}_0\,(1+\mathsf{M}_0+\sum_{i=1}^{n}\mathsf{M}_i\,(\tau+\lg(\#Q_i)))} \\ &\qquad \geq \prod\nolimits_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq \\ &2^{-2\,\mathsf{M}_0\,\sum_{i=1}^{n}\mathsf{M}_i\,(\tau+\lg(\#Q_i))\,-2\,\mathsf{M}_0^2\,(1+\lg(n+1)+n\,\lg(n)+2\,n\,\lg(\mathsf{M}_0))}, \end{aligned}$$

$$2^{-(\mathsf{M}_0+\sum_{i=1}^{n}\mathsf{M}_i\,(\tau+\lg(\#Q_i)))} \leq |\gamma_{j,k}| \leq 2^{\mathsf{M}_0+\sum_{i=1}^{n}\mathsf{M}_i\,(\tau+\lg(\#Q_i))} \tag{7}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-\mathsf{M}_0(\frac{3}{2}\mathsf{M}_0+\lg(\mathsf{M}_0)+\sum_{i=1}^{n}\mathsf{M}_i\,(\tau+\lg(\#Q_i)))}. \tag{8}$$

Corollary 5. *Under the hypothesis of Th. 3, for* $f_i \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$*,* $\mathsf{dg}(f_i) \leq d$ *and* $\mathcal{L}(f_i) \leq \tau$*, we have*

$$\prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{-(3+4\lg n+4n\lg d)d^{2n}}\,2^{-2n(1+n\lg d+\tau)d^{2n-1}}, \tag{9}$$

$$2^{-d^n-n(\tau+n\lg d+1)d^{n-1}} \leq |\gamma_{j,k}| \leq 2^{d^n+n(\tau+n\lg d+1)d^{n-1}}, \tag{10}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-2d^{2n}-n(2n\lg d+\tau)d^{2n-1}}. \tag{11}$$

Proof of main theorem. Let us first establish the lower bound. Let $\gamma_i = (\gamma_{i,1}, \ldots, \gamma_{i,n}) \in (\mathbb{C}^*)^n$, $1 \leq i \leq D$, be the solutions of (Σ), where f_i are defined in (1), We denote the set of solutions as $V \subset (\mathbb{C}^*)^n$. We add an equation to (Σ) to obtain:

$$(\Sigma_0):\ f_0(\mathbf{x}) = f_1(\mathbf{x}) = \cdots = f_n(\mathbf{x}) = 0, \tag{12}$$

where

$$f_0 = u + r_1 x_1 + r_2 x_2 + \cdots + r_n x_n, \tag{13}$$

$r_1, \ldots, r_n \in \mathbb{Z}$ to be defined in the sequel, and u is a new parameter. Now $u = -\sum_i r_i\,\gamma_{j,i}$, on a solution γ_j. We choose properly the coefficients of f_0 to ensure that the function

$$f_0 : V \to \mathbb{C}^*\ :\ \gamma \mapsto f_0(\gamma)$$

is injective. The separating element shall ensure injectivity [3, 7, 14, 27].

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

$$\mathcal{F} = \{u_i = x_1 + i\, x_2 + \cdots + i^{n-1}\, x_n \,|\, 0 \le i \le B = (n-1)\binom{D}{2}\}$$

contains at least one separating element, *which takes* distinct *values on V.*

Corollary 7. *For $f_0 \in \mathcal{F}$ it holds that $\|f_0\|_\infty \le B^{n-1}$, and*

$$\|f_0\|_\infty \le \|f_0\|_2 \le 2B^{n-1} = 2(n-1)^{n-1}\binom{D}{2}^{n-1}.$$

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

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

□

We consider the $u-$*resultant* U of (Σ_0) that eliminates $\mathbf{x}$. It is univariate in u, with coefficients homogeneous polynomials in the coefficients of (Σ_0), e.g. [9]:

$$U(u) = \cdots + \varrho_k\, u^k\, \mathbf{r}_k^{D-k} \mathbf{c}_{1,k}^{\mathsf{M}_1} \mathbf{c}_{2,k}^{\mathsf{M}_2} \cdots \mathbf{c}_{n,k}^{\mathsf{M}_n} + \ldots, \tag{14}$$

where $\varrho_k \in \mathbb{Z}$, $\mathbf{c}_{j,k}^{\mathsf{M}_j}$ denotes a monomial in coefficients of f_j with total degree M_j, and $\mathbf{r}_k^{D-k}$ denotes 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

$$\left| \mathbf{c}_{1,k}^{\mathsf{M}_1}\, \mathbf{c}_{2,k}^{\mathsf{M}_2} \,\ldots\, \mathbf{c}_{n,k}^{\mathsf{M}_n} \right| \le C = \prod_{i=1}^{n} \|f_i\|_\infty^{\mathsf{M}_i}, \tag{15}$$

From Cor. 7 we have that $|\mathbf{r_k}| \le \|f_0\|_\infty \le B^{n-1}$, for all k. Let $|\varrho_k| \le h$, for all k. Then using [28], see also Eq. (4), we get that

$$h \le \prod_{i=0}^{n} (\#Q_i)^{\mathsf{M}_i} = (\#Q_0)^D \prod_{i=1}^{n} (\#Q_i)^{\mathsf{M}_i} = (n+1)^D \varrho.$$

We can bound the norm of U:

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

and so

$$\|U\|_\infty \le \|U\|_2 \le 2\, h\, C\, B^{(n-1)D} \le 2\,(n+1)^D\, \varrho\, C\, B^{(n-1)D}.$$

If u_j are the distinct roots of U, then by recalling 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, since the multiplicities of its roots correspond to the multiplicities of the solutions of the system, but we will not exploit this further.

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

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

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

Consider γ_i, γ_j and let u_i, u_j be the corresponding roots of U. Using Prop. 8,

$$|r_1(\gamma_{i,1} - \gamma_{j,1}) + \cdots + r_n(\gamma_{i,n} - \gamma_{j,n})|^2 \le \left(r_1^2 + \cdots + r_n^2\right)^2 \left(|\gamma_{i,1} - \gamma_{j,1}|^2 + \cdots + |\gamma_{i,n} - \gamma_{j,n}|^2\right) \Leftrightarrow$$

$$\left|\sum_{k=1}^{n} r_k\, \gamma_{i,k} - \sum_{k=1}^{n} r_k\, \gamma_{j,k}\right|^2 \le \sum_{k=1}^{n} r_k^2 \cdot \sum_{k=1}^{n} |\gamma_{i,k} - \gamma_{j,k}|^2 \Leftrightarrow |u_i - u_j|^2 \le \left(\sum_{k=1}^{n} r_k^2\right) \cdot |\gamma_i - \gamma_j|^2,$$

and thus

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

To prove the lower bound of Th. 3, we apply the previous inequality for all pairs in Ω, $|\Omega| = \ell$. So we get

$$\prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \ge \left(\sum_{k=1}^{n} r_k^2\right)^{-\frac{1}{2}\ell} \prod_{(i,j)\in\Omega} |u_i - u_j|. \tag{16}$$

It remains to bound the two factors of RHS of the previous inequality. To bound the first we use Cor. 7. It holds $\sum_{k=1}^{n} r_k^2 \le 1 + \sum_{k=1}^{n} r_k^2 \le \|f_0\|_2^2 \le 4\, B^{2n-2}$, so

$$(\sum_{k=1}^{n} r_k^2)^{-\frac{1}{2}\ell} \ge 2^{-\ell}\, B^{(1-n)\ell}. \tag{17}$$

For the second factor of (16) we apply $\mathtt{DMM}_1$ to U; and thus

$$\begin{aligned} \textstyle\prod_{(i,j)\in\Omega} |u_i - u_j| \ge&\ \ 2^{\ell - D(D-1)/2}\, \|U\|_2^{1-D-\ell} \sqrt{|U_r|} \\ \ge&\ \ 2^{(1-D)(D+2)/2}\, (h\, C\, B^{(n-1)D})^{1-D-\ell} \sqrt{|U_r|}. \end{aligned} \tag{18}$$

Combining (16) with (17) and (18), we have the lower bound. 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.

Let us now establish the upper bound. We specialize f_0 in (13) by setting $r_i = -1$, for some $i \in \{1, \dots, n\}$, and $r_j = 0$, where $1 \le j \le n$ and $j \ne i$. Wlog assume $r_1 = -1$. We compute the $u-$resultant of the system, which we call $\mathcal{R}_1 \in \mathbb{Z}[u]$. Its roots are the first coordinates of the isolated zeros of the system, viz. $\gamma_{1,i}$, $1 \le i \le D$. Thus $\mathsf{dg}(\mathcal{R}_1) \le D$.

The coefficients of $\mathcal{R}_1$ are of the form, $\varrho_k\, \mathbf{c}_1^{\mathsf{M}_1} \mathbf{c}_2^{\mathsf{M}_2} \dots \mathbf{c}_n^{\mathsf{M}_n}$, where $\varrho_k \in \mathbb{Z}$ and the interpretation of the rest of the formula is the same as in the previous section. Using [28], see also Eq. (4), we get that

$$|\varrho_k| \le \prod_{i=0}^{n} (\#Q_i)^{\mathsf{M}_i} = (\#Q_0)^D \prod_{i=1}^{n} (\#Q_i)^{\mathsf{M}_i} = 2^D\, \varrho,$$

since now f_0 is a simplex in dimension 1. It also holds that $|\mathbf{c}_1^{\mathsf{M}_1} \mathbf{c}_2^{\mathsf{M}_2} \dots \mathbf{c}_n^{\mathsf{M}_n}| \le C$. Combining the two inequalities we deduce that

$$\|\mathcal{R}_1\|_\infty \le 2^D\, \varrho\, C,$$

and also $\|\mathcal{R}_1\|_\infty \leq \|\mathcal{R}_1\|_2 \leq 2^D \sqrt{D+1}\, \varrho\, C$.

From Cauchy's bound for the roots of univariate polynomials, e.g. [20], we know that for all the roots of $\mathcal{R}_1$ it holds that $(2^D \varrho C)^{-1} \leq 1/\|\mathcal{R}_1\|_\infty \leq |\gamma_{i,j}| \leq \|\mathcal{R}_1\|_\infty \leq 2^D \varrho C$. The inequality holds for all the indices i and j. Hence, all roots of the system in $(\mathbb{C}^*)^n$ are contained in a high-dimensional annulus in $\mathbb{C}^n$, defined as the difference of the volumes of two spheres centered at the origin, with radii $2^D \varrho C$ and $(2^D \varrho C)^{-1}$, resp. This proves Eq. (5).

Now we are ready to prove the upper bound of Eq. (4) in Th. 3. For all $a, b \in \mathbb{C}$ it holds that

$$|a-b| \leq 2 \max\{|a|, |b|\}\,. \tag{19}$$

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

$$\prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \leq 2^\ell \prod_{j\in\overline{\Omega}} |\gamma_j| \leq 2^\ell \,(2^D \varrho\, C)^\ell \leq (2^{D+1} \varrho\, C)^\ell.$$

For proving (6), let (i,j) be the pair of indices where the separation bound of (Σ) is attained. Then

$$\mathsf{sep}(\Sigma) = |\gamma_i - \gamma_j| = \sqrt{\sum_{k=1}^{n} (\gamma_{i,k} - \gamma_{j,k})^2} \geq |\gamma_{i,1} - \gamma_{j,1}| \geq \mathsf{sep}(\mathcal{R}_1),$$

where k is any index such that $\gamma_{i,k} \neq \gamma_{j,k}$ and $\mathsf{sep}(\mathcal{R}_1)$ is the separation bound of $\mathcal{R}_1$. An easy bound on the latter can be derived by applying Th. 1 to $\mathcal{R}_1$ with $\ell = 1$: $\mathsf{sep}(\mathcal{R}_1) \geq 2^{1-\binom{D}{2}} \|\mathcal{R}_1\|_2^{-D} \geq 2^{(1-D)(D+2)/2} (D+1)^{-D/2} (2^D \varrho C)^{-D} \geq 2^{-(3D+2)(D-1)/2} (\sqrt{D+1}\,\varrho\, C)^{-D}$, which completes the proof of (6).

Remark 9. *It is tempting to try to prove the lower bound of Th. 3 by applying* $\mathtt{DMM}_1$ *to* $\mathcal{R}_1$, *instead of* U, *as we did in the previous section. This would allow us to eliminate the factor* $B^{-(n-1)(D^2+\ell(D+1)-D)}$ *from the result. However, if we apply* $\mathtt{DMM}_1$ *to* $\mathcal{R}_1$, *it is not obvious that the requirements of Th. 1 hold, i.e. that the ordering of (the coordinates of) the roots is preserved. Moreover, the bounds on the* $u-$*resultant are of independent interest, since the latter is used in many algorithms for system solving, e.g. [3, 14, 27].*

3 Comparisons and extensions

One of the first multivariate separation bounds was due to Canny, later generalized to the case when only the affine part of the variety is 0-dimensional [31].

Theorem 10 (Gap theorem). *[7] Let* $f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})$ *be polynomials of degree* d *and coefficient magnitude* c, *with finitely-many common solutions when homogenized. If* $\gamma_j \in \mathbb{C}^n$ *is such a solution, then for any* k, *either* $\gamma_{j,k} = 0$ *or* $|\gamma_{j,k}| > (3dc)^{-n\,d^n}$.

Let $\mathcal{L}(f_i) = \tau$, then this becomes $2^{(\lg 3 + \lg d + \tau) n d^n}$, which is worse than the bound in Eq. (10), by a factor of $O(d^{n-1})$. In [5], they only require that the system has a 0-dimensional projection; m is the number of polynomials and $b < n$ the dimension of the prime component where the 0-dimensional projection is considered. The bound is:

$$|\gamma_{ij}| \geq ((n+1)^2\, e^{n+2})^{-n(n+1)d^n} \,(b^{n-b-1}\, m\, 2^\tau)^{-(n-b)d^{n-b-1}},$$

This is similar to ours in (5), and we make a comparison in the sequel. Moreover, Cor. 4 does not depend on the (total) degree of the equations, but rather on mixed volume, which is advantageous for sparse systems.

A natural question is how close are the bounds to optimum. Let us consider the following system [7]:

$$2^\tau x_1^2 = x_1,\, x_j = x_{j-1}^d,\, 2 \le j \le n.$$

The roots are $x_j = (2^{-\tau})^{d^{j-1}}$, for $2^\tau \gg 1$. Th. 3 implies $x_j \ge 2^{-d^n - n(\tau + n\lg d + 1)d^{n-1}}$, which, if $\tau \gg d$, is off only by a factor of 2^n asymptotically. The negative exponent of our bound is $\mathcal{O}(n(n\lg d + \tau)d^{n-1})$, Canny's bound gives a negative exponent of $(\lg 3 + \lg d + \tau)nd^n = \mathcal{O}(n\tau d^n)$. The bound from [5] has negative exponent: $n(n+1)(2\lg(n+1)+n+2)d^n + n(\lg n + \tau)d^{n-1} = \mathcal{O}(n^3 d^n + n\tau d^{n-1})$.

We now consider the case that (Σ) is not 0-dimensional. Then, the bounds of Th. 3 do not hold because they are based on bounding the infinite norm of the $u-$resultant, which is identically zero. Specifically, the (sparse) resultant vanishes identically when the specialized coefficients of the polynomials are not generic enough, i.e. the variety has positive dimension, or, simply, if the variety has a component of positive dimension at infinity, known as excess component.

To overcome the latter, Canny introduced the Generalized Characteristic Polynomial (GCP) [8] for dense systems. We use its generalization, called Toric GCP (TGCP) [10]. We consider (Σ_0) in (12) and perturb it:

$$(\widetilde{\Sigma}_0) \quad \begin{cases} \widetilde{f}_0 = f_0 = 0, \\ \widetilde{f}_i = f_i + p_i = 0, \quad 1 \le i \le n, \end{cases}$$

where $p_i = \sum_{\mathbf{a}\in\mathcal{D}_i} s^{\omega_i(\mathbf{a})}\mathbf{x}^{\mathbf{a}}$, $\omega_i(\cdot)$ are (suitable) linear forms, s a new parameter, and $\mathcal{D}_i$ is the subset of vertices in Q_i corresponding to monomials of f_i on the diagonal of some sparse resultant matrix; at worst, $\mathcal{D}_i$ contains the vertices of Q_i. This perturbation does not alter the support of the polynomials nor the mixed volume of the system.

The TGCP is the sparse resultant of $(\widetilde{\Sigma}_0)$, denoted $T \in (\mathbb{Z}[\mathbf{c},\mathbf{r}])[u,s]$, where $\mathbf{c}$ corresponds to the coefficients of f_i and $\mathbf{r}$ to the coefficients of f_0. The lowest-degree nonzero coefficient of T, seen as univariate polynomial in s, is a projection operator: it vanishes on the projection of any 0-dimensional component of the algebraic set defined by (Σ_0). We call this $T_U \in \mathbb{Z}([\mathbf{c},\mathbf{r}])[u]$, and $\mathsf{dg}(T_U) \le \mathsf{M}_0$. The roots of T_U are the isolated points of the variety plus some points embedded in its positive-dimensional components. It remains to bound the coefficients of T_U. Repeating the construction of U in Eq. (14), we get

$$T_U = \cdots + \underbrace{\varrho_k\, u^k \mathbf{r}_k^{\mathsf{M}_0 - k}\, \widetilde{\mathbf{c}}_{1,k}^{\mathsf{M}_1}\, \widetilde{\mathbf{c}}_{2,k}^{\mathsf{M}_2} \cdots \widetilde{\mathbf{c}}_{n,k}^{\mathsf{M}_n}}_{t_k} + \ldots,$$

where $\rho_k \in \mathbb{Z}$, and $\widetilde{\mathbf{c}}_{i,k}^{\mathsf{M}_i}$ is a monomial in the coefficients c_{ij}, s, of total degree M_i. It is an overestimation, wrt the height of T, if we suppose that $\widetilde{\mathbf{c}}_{i,k}$ is obtained by adding s^λ to each coefficient of $\mathbf{c}_{i,k}$, where $\lambda = \max_{i,\mathbf{a}}\{\omega_i(\mathbf{a})\}$. If we expand $\widetilde{\mathbf{c}}_{i,k}^{\mathsf{M}_i}$, the absolute value of the coefficients of s is bounded by $\binom{\mathsf{M}_i}{\mathsf{M}_i/2}\|f_i\|_\infty^{\mathsf{M}_i} \le 2^{\mathsf{M}_i}\|f_i\|_\infty^{\mathsf{M}_i}/\sqrt{\mathsf{M}_i}$. If we expand the term t_k of T, the degree of s is bounded by $\lambda \cdot \prod_{i=1}^n \mathsf{M}_i$, and the coefficients are bounded by

$$\prod_{i=1}^n \mathsf{M}_i \cdot |\varrho_k| \cdot |\mathbf{r}_k|^{\mathsf{M}_0 - k} \cdot \prod_{i=1}^n 2^{\mathsf{M}_i}\|f_i\|_\infty^{\mathsf{M}_i}/\sqrt{\mathsf{M}_i} =$$

$$|\varrho_k| \cdot |\mathbf{r}_k^{\mathsf{M}_0 - k}| \cdot \prod_{i=1}^n \sqrt{\mathsf{M}_i} \cdot 2^{\mathsf{M}_i} \cdot \|f_i\|_\infty^{\mathsf{M}_i} = |\mathbf{r}_k|^{\mathsf{M}_0 - k}\, h\, A\, C,$$

since every factor $\widetilde{\mathbf{c}}_{i,k}^{\mathsf{M}_i}$, contributes at most M_i coefficients. The bound holds for (the absolute of) all the coefficients of T if we consider it as bivariate polynomial in s, u. Recall that $|\varrho_k| \leq h$, for all k, where h is defined in Eq. (4). This expression also defines A, C.

Now $k \leq \mathsf{M}_0$. If we consider T_U as a univariate polynomial in s, then its coefficients are univariate polynomials in u, with degree $\leq \mathsf{M}_0$. For the 2-norm of T_U, we use a summation as in the 0-dimensional case, and get

$$\|T_U\|_\infty \leq \|T_U\|_2 \leq 2\, h\, A\, C\, B^{(n-1)\mathsf{M}_0}.$$

The previous bound is the one on U multiplied by A. Thus we can provide a theorem extending Th. 3 to positive-dimensional systems, by replacing C by AC, in Th. 3,

Theorem 11 ($\mathtt{DMM}_{\boldsymbol{n}}$ with excess components). *Consider the polynomial system (Σ) in (2), which is not necessarily 0-dimensional, and where it holds that $f_i \in \mathbb{Z}[\mathbf{x}]$, $\mathsf{dg}(f_i) \leq d$, and $\mathcal{L}(f_i) \leq \tau$. Let D be the number of the isolated points of the solution set 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 $1 \leq i < j \leq D$, and $\gamma_{j,k}$ stands for the k-th coordinate of γ_j. Then the following holds*

$$(2^{\mathsf{M}_0+1}\, \varrho\, C\, A)^\ell \geq \prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{-\ell-(\mathsf{M}_0-1)(\mathsf{M}_0+2)/2}\, (h\, C\, A)^{1-\mathsf{M}_0-\ell}\, B^{(1-n)(\mathsf{M}_0^2+\mathsf{M}_0(\ell-1)+\ell)},$$

$$(2^{\mathsf{M}_0}\, \varrho\, C\, A)^{-1} \leq |\gamma_{j,k}| \leq 2^{\mathsf{M}_0}\, \varrho\, C\, A, \tag{20}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-(3\mathsf{M}_0+2)(\mathsf{M}_0-1)/2}\, (\sqrt{\mathsf{M}_0+1}\, \varrho\, C\, A)^{-\mathsf{M}_0}, \tag{21}$$

We also have the following, less accurate bounds:

$$\prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{-(n^2-n)d^n \lg\sqrt{d}-(3+4\lg n+4n\lg d)d^{2n}} \cdot 2^{-2n(2+n\lg d+\tau)d^{2n-1}}, \tag{22}$$

$$2^{(n^2-n)\lg\sqrt{d}-d^n-n(\tau+n\lg d+2)d^{n-1}} \leq |\gamma_{j,k}| \leq 2^{(n^2-n)\lg\sqrt{d}+d^n+n(\tau+n\lg d+2)d^{n-1}}, \tag{23}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-(n^2-n)d^n\lg\sqrt{d}-2d^{2n}-n(2n\lg d+\tau+1)d^{2n-1}}. \tag{24}$$

4 Applications

We illustrate the bounds of Th. 3 in two applications. The first concerns matrix eigenvalues and eigenvectors, and is a standard illustration of the superiority of mixed volumes against Bézout's bound. The second is lower bounds of positive multivariate polynomials, inspired by [2].

Eigenvalues and eigenvectors. Consider an $n \times n$ integer matrix A, with elements $\leq 2^\tau$. We are interested in its eigenvalues λ, and its eigenvectors $\mathbf{v} = (v_1, \ldots, v_n)^\top$. This is equivalent to solving $f_j = \sum_{j=1}^n a_{i,j}v_j - \lambda v_i$, $1 \leq i \leq n$, $1 \leq j \leq n$, and $f_{n+1} = \sum_{i=1}^n v_i^2 - 1$. We have $\|f_j\|_\infty \leq 2^\tau$, $\|f_{n+1}\|_\infty \leq 2$. The Bézout bound is 2^{n+1}, whereas the actual number of (complex) solutions is $2n$, which equals the mixed volume, e.g. [14].

Canny's Gap theorem [7] implies $|z| > (6 \cdot 2^\tau)^{-(n+1)2^n}$, for any eigenvalue or eigenvector element $z \neq 0$. Thus, we need $\mathcal{O}(n\,\tau\,2^n)$ bits. We get the same exponential behavior in n if we apply [31] or [5].

It is reasonable to assume that the system is 0-dimensional and apply (5) of Th. 3. It holds that $\mathsf{M}_j = 2n$, $\mathsf{M}_{n+1} = n$, $(\#Q_{n+1}) \leq 2^{n+2}$, and $(\#Q_i) \leq 2^{n+2}$ where $1 \leq j \leq n$, and $C = \|f_{n+1}\|_\infty^{\mathsf{M}_{n+1}} \prod_{j=1}^n \|f_j\|_\infty^{\mathsf{M}_j} \leq 2^{\tau \sum_{j=1}^n \mathsf{M}_j}\, 2^n = 2^{2n^2\tau+n}$, $\varrho \leq \prod_{i=1}^{n+1} (\#Q_i)^{\mathsf{M}_i} \leq (\#Q_{n+1})^{\mathsf{M}_{n+1}} \prod_{i=1}^n (\#Q_i)^{\mathsf{M}_i}$; hence $\varrho \leq (2^{n+2})^n \prod_{i=1}^n (2^{n+2})^{2n} \leq 2^{2n^3+5n^2+2n}$.

The solutions lie in $\mathbb{C}^{n+1}$. The lower bound of Th. 3 yields

$$|z| > 2^{-2n^3-5n^2-5-2n^2\tau},$$

where z is an eigenvalues or element of eigenvector. This is exponentially better than the previous bounds. Eq. (6) from Th. 3 bounds the system's separation bound: $-\lg(\mathsf{sep}(\Sigma)) \leq 4n^3\tau + n\lg n + 4\,n^4 + 10\,n^3 + 12\,n^2 + n - 1 = \mathcal{O}(n^4 + n^3\tau)$. This is polynomial in the size of the input, and hence we obtain a new proof of Bareiss' result [1], that computing the eigenvalues and eigenvectors of an integer matrix is a polynomial problem.

Positive multivariate polynomials. We consider the following problem, studied in [2]. Let $P \in \mathbb{Z}[x_1, \ldots, x_n]$ be a multivariate polynomial of degree d which on the n-dimensional simplex takes only positive values. We are interested in computing a bound on its *minimum value*, m. We may assume that the minimum is attained inside the simplex; if not, apply a transformation which slightly changes the bitsize of P [2]. Let τ bound the bitsize of the coefficients of P. We wish to find compute a lower bound on m, greater than zero, depending on n, d, τ. Equivalently, we have a system with unknowns m, x_i:

$$\begin{cases} \frac{\partial P}{\partial x_1}(x_1, \ldots, x_n) = \cdots = \frac{\partial P}{\partial x_n}(x_1, \ldots, x_n) = 0, \\ P(x_1, \ldots, x_n) = m. \end{cases} \tag{25}$$

We use Th. 11, since there is no guarantee that the system is 0-dimensional. However, Th. 11 provides bounds for the isolated points of the variety. Since the minimum could be attained on a non-zero dimensional component, we should argue that the bounds take care of this case. We consider all the irreducible components of the variety defined by (25). Each of them contains a point for which the bounds of Th. 11 apply. Such a point is the limit of a solution of the perturbed system depending on the parameter s when $s \to 0$. Moreover, it is a zero of the first non-zero coefficient T_U, seen as a polynomial in s [8, 10]; Th. 11 bounds these zeros. Now, on each of these components, the value of m is constant, since the gradient of P is 0, and so the bounds apply for it as well.

Let $P_i = \frac{\partial P}{\partial x_i}$ and $P_{n+1} = P - m$. It holds that $\deg(P_{n+1}) = d$, $\deg(P_i) \leq d-1$, $\|P_{n+1}\|_\infty \leq 2^\tau$, $\|P_i\|_\infty \leq d\|f_{n+1}\|_\infty \leq d\,2^\tau$, $\mathsf{M}_{n+1} \leq (d-1)^n$, $\mathsf{M}_i \leq d(d-1)^{n-1}$, and $D \leq \mathsf{M}_0 \leq d(d-1)^n$. Using (20) we deduce $1/m \leq 2^D\,\varrho\, C\, A$. It remains to bound the various quantities involved, defined in (4):

$$\begin{aligned} C &\leq \prod_{i=1}^{n+1} \|P_i\|_\infty^{\mathsf{M}_i} = \|P_{n+1}\|_\infty^{\mathsf{M}_{n+1}} \prod_{i=1}^{n+1} \|P_i\|_\infty^{\mathsf{M}_i} \\ &\leq (2^\tau)^{(d-1)^n} \prod_{i=1}^{n} (d\,2^\tau)^{d(d-1)^{n-1}} \leq 2^{\tau(d-1)^n} (d\,2^\tau)^{nd(d-1)^{n-1}} \\ &\leq 2^{(n+1)\tau d(d-1)^{n-1} + nd(d-1)^{n-1}\lg d}, \end{aligned}$$

$$\begin{aligned} A &= \prod_{i=1}^{n+1} \sqrt{\mathsf{M}_i}\, 2^{\mathsf{M}_i} = \sqrt{\mathsf{M}_{n+1}} \cdot 2^{\mathsf{M}_{n+1}} \cdot \prod_{i=1}^{n} \sqrt{\mathsf{M}_i} \cdot 2^{\mathsf{M}_i} \\ &\leq (d-1)^{n/2} \cdot 2^{(d-1)^n} \cdot d^{n/2}(d-1)^{n(n-1)/2} \cdot 2^{nd(d-1)^{n-1}} \\ &\leq 2^{(n+1)d(d-1)^{n-1} + (n^2+n)\lg\sqrt{d}}. \end{aligned}$$

Moreover, $(\#Q_{n+1}) \leq 2d^{n+1}$, $(\#Q_i) \leq 2(d-1)^{n+1}$, and so

$$\begin{aligned}\varrho = \prod_{i=1}^{n+1} (\#Q_i)^{M_i} &= (\#Q_{n+1})^{M_{n+1}} \prod_{i=1}^{n} (\#Q_i)^{M_i} \\ &\leq (2d^{n+1})^{(d-1)^n} \cdot \prod_{i=1}^{n} (2d^n)^{d(d-1)^{n-1}} \leq 2^{(n+1)(1+(n+1)\lg d)d(d-1)^{n-1}}\end{aligned}$$

We apply (10) using the previous inequalities, and get

$$\frac{1}{m} \leq 2^{(n^2+n)\lg\sqrt{d}+(1+2n+d+(n^2+3n+1)\lg d)d(d-1)^{n-1}} \cdot 2^{(n+1)\tau d(d-1)^{n-1}}.$$

To assure that the minimum is attained inside the simplex, we apply a transformation that preserves the degree, but the bitsize of the polynomial is now bounded by $\tau + 1 + d\lg(n)$. Replacing this in the previous inequality, we get $\frac{1}{m} \leq \frac{1}{m_{\mathtt{DMMp}}}$, where

$$\frac{1}{m_{\mathtt{DMMp}}} = 2^{(n^2+n)\lg\sqrt{d}+(2+3n+d+(n^2+3n+1)\lg d} \cdot 2^{(n+1)d\lg n)d(d-1)^{n-1}} \cdot 2^{(n+1)\tau d(d-1)^{n-1}}. \tag{26}$$

If we know that the system is zero dimensional then we could use Th. 3. Of course this is not always the case, hence we state the following bound, using (5), just as a reference.

$$\frac{1}{m} \leq \frac{1}{m_{\mathtt{DMM}}} = 2^{((n+1)\tau+n+d+(n^2+3n+1)\lg d)d(d-1)^{n-1}}. \tag{27}$$

Let us compare the $m_{\mathtt{DMM}_p}$ with other bounds that appear in the bibliography. In [2, Sec. 2, Rem. 2.17], the following estimation was computed,

$$\begin{aligned}\frac{1}{m_{\mathtt{BLR}}} &= 2^{2^{n+3}nd^{n+1}(\tau+8nd)} n^{2^{n+5}d^{n+2}n} d^{2^{n+5}d^{n+1}n^2} \\ &= 2^{2^{n+3}n\tau d^{n+1}+2^{n+5}nd^{n+1}(2nd+d\lg n+n\lg d)}.\end{aligned} \tag{28}$$

which also holds with no assumption, but it is looser than $m_{\mathtt{DMM}_p}$.

In [5] the authors derive a bound for the minimum of the absolute value of a polynomial, $\frac{1}{m} \leq \frac{1}{m_{\mathtt{BY}}}$, i.e.

$$\frac{1}{m_{\mathtt{BY}}} = ((n+2)^2 e^{n+3})^{(n+1)(n+2)d^{n+1}} \left(n^n(n+1)\,d\,2^\tau\right)^{(n+1)d^n}. \tag{29}$$

The authors use the terminology *evaluation bound* for their bound. It holds when there is a 0-dimensional projection; they prove that this is always the case for (25).

In [16] the following bound was computed:

$$\frac{1}{m} \leq \frac{1}{m_{\mathtt{JP}}} = 2^{(\tau+1)d^{n+1}} d^{(n+1)d^{n+1}}, \tag{30}$$

which has no restriction on the corresponding polynomial system. It is comparable to $m_{\mathtt{DMM}_p}$ in general, but strictly looser when $d > n$.

Example 12. *Let us compute a lower bound on the value of $f = (x+2y-3)^d + (x+2y-4)^d$, where $d \in \{2, 8, 32\}$. The polynomial is positive as it is a sum of squares. Consider the ideal $I = (f - z, f_x, f_y) \subset \mathbb{Z}[x, y, z]$. If $(\zeta_1, \zeta_2, \zeta_3)$ belongs to the zero set of I_f, then $|\zeta_3| \geq 2^{-b}$, $b > 0$. In Tab. 1 we present the estimations of $\lg b$ by the previous bounds. The true value is $b = 0$. When the degree is comparable to the number of variables ($d = 2$), then our bound and $m_{\mathtt{JP}}$ are comparable. When $d > n$, e.g. $d = 4$ and $d = 32$, then $m_{\mathtt{DMMp}}$ is better than $m_{\mathtt{JP}}$ by an order of magnitude.*

5 Subdivision algorithms

We use our results to bound the number of steps that any subdivision algorithm performs to isolate the real roots of a well-defined polynomial system. Then, we bound the complexity of Milne's algorithm in 2d. Our analysis can easily be extended to $\mathbb{R}^n$, however it is not clear what is the exact bit complexity of the elimination steps needed.

We use $\mathtt{DMM}_n$, Th. 3, and Eq. (4) & (9), to bound the number of steps of a subdivision algorithm to isolate the real roots of a well-defined polynomial system as in (1). We assume the existence of an oracle that counts the number of real roots of the system inside a box in $\mathbb{Q}^n$. Our aim is to compute the number of calls to the oracle in order to compute isolating (hyper-)boxes for all real roots. Realizations of such oracles are in [22, 25, 24], see also [3].

Suppose all roots of the system lie in a hypercube of side C, see Th. 3. At step h of the algorithm, the oracle counts the number of roots in hypercubes of side $C/2^h$. We consider the whole subdivision algorithm as a 2^n-ary tree T, where at each node we associate a hypercube, and to the root of the tree we associate the initial hypercube. Let $\#(T)$ denote the number of nodes. We will prune some leaves of T to obtain tree T' where it is easier to count its nodes.

We proceed as follows. If v is a leaf and has a sibling that it is not a leaf, then we prune v. If $u_1, \dots, u_k$, for some positive integer k, are leaves and siblings, such that they have no sibling that is not a leave, then we prune all of them except one that possess a hypercube that contains a real root. Notice that there is always at least one such node in $u_1, \dots, u_k$, because otherwise, the subdivision process in this path would have stopped one level before. If there exists more than one such node in $u_1, \dots, u_k$, then we keep arbitrarily one of them. It holds that $\#(T) \leq 2^n \#(T')$, and we will count the nodes in T'.

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 also bounds the number of the leaves of T'. The hypercubes that correspond to the leaves of the tree have diagonals that are at least $\Delta_j = |\gamma_j - \gamma_{c_j}|$, where γ_{c_j} is the root closest to γ_j. The length of their edges is 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 $\left\lceil \log \frac{C}{\Delta_j} \right\rceil$. Hence the number of nodes in $\#(T')$ is

$$\#(T') = \sum_{j=1}^{R} \left\lceil \log \frac{C}{\Delta_j} \right\rceil \leq R + R \lg C - \lg \prod_{j=1}^{R} \Delta_j. \tag{31}$$

To bound the various quantities that appear, we will rely on Eq. (4) and Th. 3. 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 Eq. (4) of Th. 3 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. Then

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

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

$$\begin{aligned}-\log \prod_{i=1}^{R} \Delta_i &\leq 2D^2 + 3D \lg C + 3D \lg h + 5n\, D^2 \lg B \\ &\leq 8(\lg n + n \lg d) d^{2n} + 3n(n \lg d + \tau) d^{2n-1},\end{aligned}$$

and for the total number of nodes of T' we have

$$\begin{array}{rl}(\#T') \leq & R + R\lg C - \lg\prod_{j=1}^{R}\Delta_j \leq D + D\lg C - \lg\prod_{j=1}^{R}\Delta_j \\ \leq & 2d^n(n\tau d^{n-1}) + 8(\lg n + n\lg d)d^{2n} + 3n(n\lg d+\tau)d^{2n-1} \\ = & \widetilde{\mathcal{O}}(n(n+d+\tau)d^{2n-1}),\end{array}$$

and hence $(\#T) = \widetilde{\mathcal{O}}(2^n\, n(n+d+\tau)\, d^{2n-1})$.

Theorem 13. *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* $\widetilde{\mathcal{O}}(2^n\, D\,(D+\lg C))$ *or* $\widetilde{\mathcal{O}}(2^n\,(d+\tau)\,d^{2n-1})$.

Remark 14. *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* $\mathcal{O}(d^2\lg d + d\tau)$. *The optimal bound is* $\mathcal{O}(d^2+d\tau)$ *[11].*

We now bound the complexity of Milne's algorithm [22] for isolating all real roots of a bivariate polynomial system. Milne's, so-called, *volume function* realizes the required oracle, see [15, 32] for experimental results. By $\mathbf{SR}(f,g)$ we denote the signed polynomial remainder sequence of f, g.

Proposition 15. *[26, 12] We compute* $\mathbf{SQ}(f,g)$, *any polynomial in* $\mathbf{SR}(f,g)$, *and* $\mathtt{Res}(f,g)$ *wrt* x *in* $\widetilde{\mathcal{O}}_B(q(p+q)^{k+1}d\tau)$. *The degree of* $\mathbf{SR}(f,g)$ *in* $y_1,\ldots,y_k$ *is* $\mathcal{O}(d(p+q))$ *and the bitsize is* $\mathcal{O}((p+q)\tau)$. *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* $\widetilde{\mathcal{O}}_B(q(p+q)^{k+1}d\max\{\tau,\sigma\})$.

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 to be 0-dimensional. We introduce new parameters u, a, b and we eliminate a, b from the polynomials $\{f(a,b), g(a,b), V=u+(x-a)(y-b)\}$, where V is the volume function. After elimination, we obtain a polynomial $h\in(\mathbb{Z}[x,y])[u]$. We compute the Sturm sequence of h and its derivative w.r.t. u, h_u, and we evaluate the sequence over $u=0$. We obtain a sequence of bivariate polynomials in x, y. 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 inside the box is $\frac{1}{4}$ the sum of the sign variations [22].

We perform the elimination using iterated resultants. Using Prop. 15 we compute $h_1 = \mathtt{Res}_a(f(a,b),V(u,x,y,a,b)) \in \mathbb{Z}[u,x,y,a,b]$ in $\widetilde{\mathcal{O}}_B(d^7\tau)$. The total degree of h_1 is $\mathcal{O}(d^2)$ and $\mathcal{L}(h_1)=\widetilde{\mathcal{O}}(d\tau)$. Similarly, we obtain polynomial $h_2=\mathtt{Res}_a(g(a,b),V(u,x,y,a,b))\in\mathbb{Z}[u,x,y,a,b]$. Finally, $h=\mathtt{Res}_b(h_1,h_2)\in\mathbb{Z}[x,y,u]$ is computed in $\widetilde{\mathcal{O}}_B(d^{12}\tau)$. The degree of h in u is $\mathcal{O}(d^2)$ since the resultant of h_1,h_2 has the factor $u^{\mathtt{dg}(f(x,0))\mathtt{dg}(g(x,0))}=u^{d^2}$. The degree of h in x,y is $\widetilde{\mathcal{O}}_B(d^4)$ and $\mathcal{L}(h)=\widetilde{\mathcal{O}}(d^3\tau)$.

We compute the signed polynomial remainder sequence of h, h_u and evaluate it at 0. This costs $\widetilde{\mathcal{O}}_B(d^{15}\tau)$. The evaluated sequence contains $\mathcal{O}(d^2)$ polynomials in $\mathbb{Z}[x,y]$ of degrees $\widetilde{\mathcal{O}}_B(d^6)$ and bitsize $\widetilde{\mathcal{O}}_B(d^5\tau)$. Each polynomial in the sequence is evaluated over a rational number of bitsize σ in $\widetilde{\mathcal{O}}_B(d^{17}(\tau+d\sigma))$, and thus all of them in $\widetilde{\mathcal{O}}_B(d^{19}(\tau+d\sigma))$.

In the worst case, σ equals the bitsize of the separation bound, i.e. $\widetilde{\mathcal{O}}(d^3\tau)$. Hence, the evaluation of the sequence costs $\widetilde{\mathcal{O}}_B(d^{23}\tau)$. Th. 13 indicates that we need to perform this evaluation $\mathcal{O}(d^4\lg d + d^3\tau)$ times.

Theorem 16. *Let* $f,g\in\mathbb{Z}[x,y]$ *with total degrees bounded by* d *and bitsize bounded by* τ. *Using the algorithm of Milne [22], we can isolate the real roots of the system* $f=g=0$ *in* $\widetilde{\mathcal{O}}_B(d^{27}\tau + d^{26}\tau^2)$.

bound		$(d,\tau)=(2,5)$	$(8,20)$	$(32,85)$
[2], Eq. (28)	$\lvert\lg(m_{\mathtt{BLR}})\rvert$	27 136	6 684 672	1 604 321 280
[5], Eq. (29)	$\lvert\lg(m_{\mathtt{BY}})\rvert$	1 192	74 000	4 696 811
[16], Eq. (30)	$\lvert\lg(m_{\mathtt{JP}})\rvert$	72	15 360	3 309 568
Eq.(26)	$\lvert\lg(m_{\mathtt{DMM}_p})\rvert$	87	7 457	442 447
Eq.(27)	$\lvert\lg(m_{\mathtt{DMM}})\rvert$	54	5 201	324 506

Table 1. Comparison of (the bitsize of) various bounds on the minimum value of the polynomial $f=(x+2y-3)^d+(x+2y-4)^d$, for $d\in\{2,8,32\}$ and $\tau\in\{8,20,85\}$, resp. The bounds hold for all polynomials with same characteristics.

Bounds on mutli-point evaluation of multivariate polynomials [23] could save at least two factors in the previous theorem.

Acknowledgment. E.T. thanks M. Sombra for finding a missing factor in the original manuscript, and brought to our attention [28]. IZE and BM are partially supported by Marie-Curie Network "SAGA", FP7 contract PITN-GA-2008-214584. ET is partially supported by an individual postdoctoral grant from the Danish Agency for Science, Technology and Innovation.

References

[1] E.H. Bareiss. Sylvester's identity and multistep integer-preserving Gaussian elimination. *Math. of Comput.*, 22(103):565–578, 1968.

[2] 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.

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

[4] H. F. Blichfeldt. A new principle in the geometry of numbers, with some applications. *Trans. AMS*, 15(3):227–235, 1914.

[5] W. D. Brownawell and C. K. Yap. Lower bounds for zero-dimensional projections. In *Proc. ISSAC*, KIAS, Seoul, Korea, 2009.

[6] M. Burr, S.W. Choi, B. Galehouse, and C. K. Yap. Complete subdivision algorithms, II: Isotopic meshing of singular algebraic curves. In *Proc. ISSAC*, pages 87–94, Hagenberg, Austria, 2008.

[7] J. Canny. *The Complexity of Robot Motion Planning.* ACM Doctoral Dissertation Award Series. MIT Press, 1987.

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

[9] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Number 185 in GTM. Springer, New York, 2nd edition, 2005.

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

[11] J. H. Davenport. Cylindrical algebraic decomposition. Technical Report 88–10, School of Math. Sciences, Univ. Bath, http://www.bath.ac.uk/masjhd/, 1988.

[12] D. I. Diochnos, I. Z. Emiris, and E. P. Tsigaridas. On the asymptotic and practical complexity of solving bivariate systems over the reals. *J. Symb. Comput.*, 44(7):818–835, 2009.

[13] A. Eigenwillig, V. Sharma, and C. K. Yap. Almost tight recursion tree bounds for the Descartes method. In *Proc. ISSAC*, pages 71–78, New York, USA, 2006.

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

[15] L. González-Vega and G. Trujillo. Multivariate Sturm-Habicht sequences: Real root counting on n-rectangles and triangles. *Real Algebraic and Analytic Geometry (Segovia, 1995), Rev. Mat. Univ. Complut. Madrid*, 10:119–130, 1997.

[16] G. Jeronimo and D. Perrucci. On the minimum of a positive polynomial over the standard simplex. *CoRR*, abs/0906.4377, 2009.

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

[18] T. Krick, L.M. Pardo, and M. Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Mathematical Journal*, 109(3):521–598, 2001.

[19] A. Mantzaflaris, B. Mourrain, and E.P. Tsigaridas. Continued fraction expansion of real roots of polynomial systems. In *Proc. Symbolic-Numeric Comput.*, pages 85–94, Kyoto, 2009.

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

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

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

[23] 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.

[24] P. Pedersen. *Counting real zeros*. PhD thesis, NY Univ., 1991.

[25] 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.

[26] D. Reischert. Asymptotically fast computation of subresultants. In *Proc. ISSAC*, pages 233–240, 1997.

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

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

[29] Elias P. Tsigaridas and Ioannis Z. Emiris. On the complexity of real root isolation using Continued Fractions. *Theor. Comput. Sci.*, 392:158–173, 2008.

[30] J-C. Yakoubsohn. Numerical analysis of a bisection-exclusion method to find zeros of univariate analytic functions. *J. Complexity*, 21(5):652–690, 2005.

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

[32] Z. Zafeirakopoulos. Study and benchmarks for real root isolation methods. Master's thesis, Dept. Informatics & Telecoms, University of Athens, 2009. www.zafeirakopoulos.info/content/publications/thesis.pdf.