Separation bounds for polynomial systems

Ioannis Emiris, Bernard Mourrain, Elias Tsigaridas

▶ **To cite this version:**

Ioannis Emiris, Bernard Mourrain, Elias Tsigaridas. Separation bounds for polynomial systems. 2015. hal-01105276v2

HAL Id: hal-01105276

https://inria.hal.science/hal-01105276v2

Preprint submitted on 7 Feb 2015 (v2), last revised 28 Jun 2019 (v5)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Separation bounds for polynomial systems

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

February 7, 2015

Abstract

Based on recent advances on aggregate separation bounds for univariate polynomials, we extend these results to the isolated roots of zero-dimensional, as well as positive-dimensional and overdetermined polynomial systems. We exploit the structure of the given system, as well as bounds on the height of the sparse (or toric) resultant, by means of mixed volume, thus establishing adaptive bounds. Our bounds improve Canny's gap theorem [8]. Moreover, they exploit sparseness; they are in general comparable to the lower bounds on the absolute value of the root coordinates by Brownawell and Yap [6] which, however, were obtained under a strong hypothesis, namely the existence of a zero-dimensional projection. In an effort to evaluate the quality of our bounds, we present polynomial systems whose root separation is asymptotically not far from our bounds.

Our bounds are applied in order to estimate the bitsize of the eigenvalues and eigenvectors of an integer matrix, thus showing the problem is of polynomial bit complexity, in order to bound the value of a positive polynomial over the simplex, thus improving by at least one order of magnitude upon all existing bounds, and in order to asymptotically bound the number of steps of any subdivision-based algorithm that isolates all real roots of a polynomial system.

*Department of Informatics and Telecommunications, University of Athens, Greece. Email: emiris@di.uoa.gr

†Project Team Galaad, INRIA Méditerranée, Sophia-Antipolis, France. Email: mourrain@inria.fr

‡INRIA, Paris-Rocquencourt Center, POLSYS & Sorbonne Universités, UPMC Univ Paris 06, POLSYS, UMR 7606, LIP6, F-75005, Paris, France. Email: elias.tsigaridas@inria.fr

1 Introduction

A fundamental question in exact as well as numeric algebraic computing is to find all common roots, in some representation, of a system of multivariate polynomials. A major issue is to derive tight bounds on the theoretical and the practical complexity of various solvers. These 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.

Davenport [13] was first to introduce aggregate separation bounds for the real roots of a univariate polynomial, which depend on Mahler's measure, e.g. [26]. Johnson [21] and Mignotte [27] loosened the hypothesis on the bounds and extended them to complex roots.

For algebraic systems, a fundamental result is Canny's Gap theorem [8] on the separation bound for square zero-dimensional systems, see Thm 12. Yap [36] relaxed the zero-dimensional requirement by requiring it holds only on the affine part of the variety. A more recent lower bound on the absolute value of the root coordinates [6] 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 the Nullstellensatz, we refer to [24].

There has been vivid recent interest for a closely related problem, encountered in real optimization. Basu, Leroy, and Roy [2] and, more recently, Jeronimo and Perrucci [20] obtained lower bounds on the minimum value of a positive polynomial over the standard simplex. For this, they compute lower bounds on the roots of a polynomial system formed by the polynomial and all its partial derivatives. This problem is also treated in [6].

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. [7, 19, 25, 29, 35].

Our contribution. We improve the state of the art by new worst-case (aggregate) separation bounds for the isolated roots of polynomial systems which, moreover, are not necessarily zero-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 completeness, we offer precise statements at the risk of being technical. For bounding the number of complex roots of a well-constrained polynomial system, we employ mixed volume (Thm 4) which is the sharpest general bound available today, and allows us to exploit the structure implicit in many applications. Any future better bound on the number of roots can be used to improve our results. The main ingredients of our proof are resultants, including bounds on their height [33].

Our approach extends the known separation bound for single polynomial equations to zero-dimensional systems; we call our bound $\mathtt{DMM}_n$, after Davenport-Mahler-Mignotte. This improves upon Canny's Gap theorem by $\mathcal{O}(d^{n-1})$, where n is the number of variables and d bounds the polynomial degrees. Our bounds are within a factor of $\mathcal{O}(2^n)$ from optimal for certain systems constructed in the sequel. Hence, they are tight for n small (or constant) compared to the other parameters. Our bounds are comparable to those in [6] on the absolute value of root coordinates, but they constitute an improvement when expressed using mixed volumes. It seems nontrivial to apply sparse elimination theory with the approach of [6]. More importantly, our result is extended to positive-dimensional systems, and obtain results comparable to those by Brownawell and Yap [6] which, however, require a very strong hypothesis, namely the

existence of a zero-dimensional projection.

We illustrate our bounds on computing the eigenvalues and 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 proof to Bareiss' result [1] that the problem is of polynomial bit complexity.

We examine a key question in optimization, namely to bound the minimum of a positive polynomial over the standard simplex. Our approach significantly improves upon the three best known bounds [2, 6, 20], by at least one order of magnitude in almost all cases.

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.

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

This paper extends the work in [16] by providing: a new version of the DMM bound in dimension 1, complete detailed proofs of all statements, including a new approach for the proof of Thm 18, and a new Section 4.1, including an example which yields a single exponential lower bound for the separation between roots of a polynomial system, thus quantifying the tightness of our upper bound in the worst case. In addition, this paper introduces separation bounds for, possibly positive-dimensional, overdetermined polynomial systems.

A preliminary version of a large part of this paper's results appeared as [16].

Paper structure. We next introduce notation. In Section 2 we survey bounds for univariate polynomials. Then Section 3 derives and proves the multivariate version of our separation bound as Main Thm 5. An evaluation of its quality and comparisons to existing bounds are in Section 4, whereas the generalization to positive-dimensional systems is given in Section 5. In Section 6, we present the bounds for the overdetermined polynomial systems. The applications of our bounds are in Section 7.

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 with respect to x_i. By $\mathcal{L}(f)$ we denote the maximum bitsize of the coefficients of f (including a bit for the sign), i.e., the number of bits to write them as binary integers. For $a \in \mathbb{Q}$, $\mathcal{L}(a) \geq 1$ is the maximum bitsize of the numerator and denominator.

For a polynomial $f(x) = a_d \prod_{i=1}^{d}(x - z_i) \in \mathbb{C}[x]$, with $a_d \neq 0$, its Mahler measure is $\mathcal{M}(f) := |a_d| \prod_{i=1}^{d} \max\{1, |z_i|\}$. If we further assume that $f \in \mathbb{Z}[x]$ and $\mathcal{L}(f) = \tau$, then $\mathcal{M}(f) \leq \|f\|_2 \leq \sqrt{d+1}\|f\|_\infty = 2^\tau\sqrt{d+1}$, e.g. [26, 36]. Let us denote by $\texttt{lc}(f)$ and $\texttt{tc}(f)$ the leading and the trailing, nonzero coefficients of f, respectively.

Let $\Delta_{\gamma_i}(f)$, or Δ_i, denote the minimum distance between a root γ_i of f and any other root. Specifically, this is the Euclidean distance of γ_i to its closest root, denoted by γ_{c_i}. Hence $\Delta_i = |\gamma_i - \gamma_{c_i}|$ and $\gamma_i \neq \gamma_{c_i}$. We call this quantity *local separation bound*. We also use the notation $\Delta(\gamma_i, f)$ to indicate that we consider the local separation bound of γ_i as a root of f. If the polynomial is clear from the context, then may also use $\Delta(\gamma_i)$.

Let $\Delta(f) = \min_i \Delta_i(f)$, or $\mathsf{sep}(f)$, denote the *separation bound*, that is the minimum distance between all roots of f. Let $\mathsf{sep}(\Sigma)$ denote the separation bound for a well-constrained polynomial

system (Σ).

In the sequel we make use of $\mathbf{sr}_r(f, f')$, which denotes the r-th subresultant coefficient of the subresultant sequence of f and its derivative f'. Additional notation, needed in the multivariate case, is presented in Section 3.1.

2 Univariate separation bounds

Consider a real univariate polynomial f, not necessarily square-free, of degree d and its complex roots α_j in ascending magnitude.

There are various variants of aggregate separation bounds for the univariate case. We refer the reader to [34, 26, 13, 14, 21] and references therein. The next theorem gathers several useful versions of upper and separation bounds that exploit the product of differences of the form $\Delta_i = |\gamma_i - \gamma_{c_i}|$.

The bound in Eq. (1) is the well known Cauchy bound on the roots. The second bound, Eq. (2), is from [22]. A bound that exploits the multiplicities of the roots first appeared in [23]. We modify the proof to derive a version valid for polynomials with real coefficients; it appears in Eq. (3). The bound of Eq. (4) is derived from [32] after we modified the proof to make it valid for polynomials with real coefficients. Separation bounds valid for polynomials with real coefficients are useful to perform computations with polynomials having algebraic numbers as coefficients, or even transcedental numbers.

Theorem 1 ($\mathtt{DMM_1}$). *Let $f \in \mathbb{R}[X]$ be such that $\mathtt{lc}(f) = a_d$ and $\deg(f) = d$, not necessarily square-free; let f_r be its square-free part, where $\deg(f_r) = r \leq d$ and $\mathtt{lc}(f_r) = b_r$. Let the distinct roots of f be $\alpha_1, \ldots, \alpha_r$ and let $s_1, \ldots, s_r$ be the corresponding multiplicities. For any nonzero root α_k it holds*

$$\frac{|\mathtt{tc}(f)|}{2\,\|f\|_\infty} \leq |\alpha_k| \leq 2\frac{\|f\|_\infty}{|\mathtt{lc}(f)|} \ . \tag{1}$$

Let K be any subset of $\{1, \ldots, r\}$. It holds

$$\prod_{k\in K} \Delta_k \geq d^{-18d}\, \mathcal{M}\,(f)^{-15d}\ |\mathbf{sr}_r(f, f')|^3 \ , \tag{2}$$

where $\mathbf{sr}_r(f, f')$ is the r-th subresultant coefficient of the subresultant sequence of f and its derivative f'. If we take the multiplicities of the roots into account, then we have the following bound

$$\begin{aligned} \prod_{k\in K} \Delta_k^{m_k} \ &\geq\ (2\,r)^{-2\,d}\,|a_d|^d\,\|f\|_\infty^{-d}\,\|f_r\|_\infty^{-d}\,\mathcal{M}\,(f)^{1-r}\ |\mathtt{Res}(f, f_r')| \\ &\geq\ 2^{-6d^2\lg d}\,\|f\|_\infty^{1-3d}\,|a_d|^{2d}\,|b_r|^{-d}\,|\mathtt{Res}(f, f_r')| \ , \end{aligned} \tag{3}$$

where $m_k \leq s_k$, f_r' is the derivative of f_r, and $\mathtt{Res}$ stands for the resultant wrt x. Finally, if we are only interested in the separation bound, then the following, slightly tighter, inequality holds

$$\Delta(f) \geq \frac{1}{2}\,d^{-d-2}\,\|f\|_\infty^{-d}\,\sqrt{|\mathtt{t}|} \ , \tag{4}$$

where $\mathtt{t}$ is the trailing coefficient of the polynomial $\mathtt{Res}(f'(x), y - f(x)) \in \mathbb{R}[y]$.

Corollary 2 (DMM$_1$ in $\mathbb{Z}$). *With the above notation, if f has integer coefficients, then let $\mathcal{L}(f) = \tau$. In this case Eq. (1) simplifies to*

$$2^{-\tau-1} \leq \frac{1}{2\,\|f\|_\infty} \leq |\alpha_k| \leq 2\,\|f\|_\infty \leq 2^{\tau+1} \ , \tag{5}$$

following Eq. (2) we get

$$\prod_{k\in K} \Delta_k \geq d^{-18d}\,\|f\|_2^{-15d} \Rightarrow -\lg \prod_{k\in K} \Delta_k \leq 15\,d\tau + 33\,d\,\lg d \ ,$$

while following Eq. (3) we obtain the bound

$$\prod_{k\in K} \Delta_k^{m_k} \geq (2d^2)^{-6d^2}\,\|f\|_\infty^{1-3d} \Rightarrow -\sum_{k\in K} m_k\,\lg \Delta_k \leq 3\,d\tau + 6\,d^2\,\lg d \ .$$

Proof (of Thm 1): We use the notation $\mathtt{lc}(f) = a_d$ and $\mathtt{lc}(f_r) = b_r$.

The upper and lower bound on the roots that appears in (1) is (a slightly modified version of) the well known Cauchy bound and its proof could be found in many textbooks. e.g., [36, 28].

We refer the reader to [22, Thm 9] for the proof of the bound in Eq. (2).

For the bound of Eq. (3), first we consider the case where $K = \{1, \ldots, r\}$. The square-free factorization of f is $f = \prod_{i=1}^m q_i^i$, where $\mathrm{dg}(q_i) = d_i$, $\sum_{i=1}^m d_i = r$, $\sum_{i=1}^m i\,d_i = d$, and $f_r = \prod_{i=1}^m q_i$ is the square-free part of f. The leading coefficient of q_i is $\mathtt{q}_i$. It holds $\mathtt{lc}(f) = a_d = \prod_i \mathtt{q}_i^i$, and $\mathtt{lc}(f_r) = b_r = \prod_i \mathtt{q}_i$.

Let $\alpha_j^{(i)}$ be the roots of the q_i, where $1 \leq j \leq d_i$ and $1 \leq i \leq m$. Fix a root $\alpha_j^{(i)}$ and let β be the root of f_r that is closest. We use $\Delta(\alpha_j^{(i)})$ to denote the local separation bound of $\alpha_j^{(i)}$ as a root f or f_r, as $\Delta(\alpha_j^{(i)}) = \Delta(\alpha_j^{(i)}, f_r) = \Delta(\alpha_j^{(i)}, f)$. We also use $w = \alpha_j^{(i)} - \beta$ and by $f_r^{[k]}$ we denote the k-th derivative of f_r.

We consider the Taylor expansion of f_r and we have

$$0 = f_r(\beta) = f_r(\alpha_j^{(i)}) + \sum_{k=1}^{r} \frac{w^k}{k!} f_r^{[k]}(\alpha_j^{(i)}) = w\left(f_r^{[1]}(\alpha_j^{(i)}) + w\sum_{k=2}^{r} \frac{w^{k-2}}{k!} f_r^{[k]}(\alpha_j^{(i)})\right) \ .$$

It holds $\Delta(\alpha_j^{(i)}) = |\alpha_j^{(i)} - \beta| = |w|$. As $\alpha_j^{(i)} \neq \beta$ we have $w \neq 0$ and so

$$|f_r^{[1]}(\alpha_j^{(i)})| \leq \Delta(\alpha_j^{(i)}) \sum_{k=2}^{r} \frac{w^{k-2}}{k!} |f_r^{[k]}(\alpha_j^{(i)})| \ . \tag{6}$$

It holds that $|f_r^{[k]}(\alpha_j^{(i)})| \leq k!\|f_r\|_\infty \max\{1, |\alpha_j^{(i)}|\}^{r-1}$. Under the assumption $|w| = \Delta(\alpha_j^{(i)}) \leq 1$ and using the previous bound the summation at the right-hand side of Eq. (6) becomes

$$\sum_{k=2}^{r} \frac{|w|^{k-2}}{k!} |f_r^{[k]}(\alpha_j^{(i)})| \leq \|f_r\|_\infty \max\{1, |\alpha_j^{(i)}|\}^{r-1} \sum_{k=2}^{r} |w|^{k-2} \leq r\,\|f_r\|_\infty \max\{1, |\alpha_j^{(i)}|\}^{r-1}.$$

Using this bound and solving Eq. (6) for $\Delta(\alpha_j^{(i)})$ we get

$$\Delta(\alpha_j^{(i)}) \geq \frac{|f_r^{[1]}(\alpha_j^{(i)})|}{r\,\|f_r\|_\infty \max\{1, |\alpha_j^{(i)}|\}^{r-1}} \geq r^{-2}\,\|f_r\|_\infty^{-1}\ \max\{1, |\alpha_j^{(i)}|\}^{1-r}\,|f_r^{[1]}(\alpha_j^{(i)})| \ .$$

If $|w| = \Delta(\alpha_j^{(i)}) > 1$ then the previous inequality also holds as the right-hand side is less than one. This is a consequence of the following inequality that upper bounds the evaluation of $f_r^{[1]}$. Let $f_r = \sum_{\nu=0}^{r} b_\nu x^\nu$ then

$$|f_r^{[1]}(\alpha_j^{(i)})| \leq \sum_{\nu=0}^{r-1} (r-i)|b_{\nu+1}\,(\alpha_j^{(i)})^\nu| \leq r^2\,\|f_r^{[1]}\|_\infty\,\max\{1, |\alpha_j^{(i)}|\}^{r-1}\ .$$

Recall that $\mathcal{M}\,(q_i) = \mathtt{lc}(q_i)\,\prod_{j=1}^{d_i} \max\{1, |\alpha_j^{(i)}|\}$. We take into account the multiplicity of the root, i, and we consider the product over all the roots of q_i; then

$$\prod_{j=1}^{d_i} \Delta(\alpha_j^{(i)})^i \geq r^{-2\,i\,d_i}\,\|f_r\|_\infty^{-i\,d_i} \left(\frac{\mathcal{M}\,(q_i^i)}{|\mathtt{lc}(q_i)^i|}\right)^{1-r} \prod_{j=1}^{d_i} |f_r^{[1]}(\alpha_j^{(i)})|^i\ .$$

Next we consider the product over all the roots of f,

$$\prod_{i=1}^{m}\prod_{j=1}^{d_i} \Delta(\alpha_j^{(i)})^i \geq r^{-2\,\sum_i i\,d_i}\,\|f_r\|_\infty^{-\sum_i i\,d_i} \left(\prod_{i=1}^{m} \frac{\mathcal{M}\,(q_i^i)}{|\mathtt{lc}(q_i)^i|}\right)^{1-r} \prod_{i=1}^{m}\prod_{j=1}^{d_i} |f_r^{[1]}(\alpha_j^{(i)})|^i$$

$$\prod_{i=1}^{m}\prod_{j=1}^{d_i} \Delta(\alpha_j^{(i)})^i \geq r^{-2\,d}\,\|f_r\|_\infty^{-d}\,\mathcal{M}\,(f)^{1-r}\,|a_d|^{r-1} \prod_{i=1}^{m}\prod_{j=1}^{d_i} |f_r^{[1]}(\alpha_j^{(i)})|^i\ ,$$

where we used $\mathtt{lc}(f) = a_d = \prod_{i=1}^{m} \mathrm{q}_i^i$ and the multiplicative property of the Mahler measure, ie $\mathcal{M}\,(f) = \prod_{i=1}^{m} \mathcal{M}\,(q_i)^i$.

To bound $\prod_i \prod_j |f_r^{[1]}(\alpha_j^{(i)})|^i$ we exploit basic properties of the resultant,

$$\mathtt{Res}(f, f_r^{[1]}) = (\mathtt{lc}(f))^{r-1} \prod_{\alpha: f(\alpha)=0} f_r^{[1]}(\alpha) = a_d^{r-1} \prod_{i=1}^{m}\prod_{j=1}^{d_i} (f_r^{[1]}(\alpha_j^{(i)}))^i\ .$$

Putting the various inequalities together we derive the bound

$$\prod_{i=1}^{r} \Delta_i^{s_i} = \prod_{i=1}^{m}\prod_{j=1}^{d_i} \Delta(\alpha_j^{(i)})^i \geq r^{-2\,d}\,\|f_r\|_\infty^{-d}\,\mathcal{M}\,(f)^{1-r}\,\left|\mathtt{Res}(f, f_r^{[1]})\right|\ . \tag{7}$$

To cover the case where the product of the local separation bounds does not involve all the roots, we bound the missing factors and we modify the bound of Eq. 7 accordingly.

Using Cauchy's upper bound for the roots, Eq. (1), we get

$$\Delta(\alpha_k) = |\alpha_k - \beta| \leq |\alpha_k| + |\beta| \leq 4\frac{\|f\|_\infty}{|a_d|}\ , \tag{8}$$

where β is the root of f closest to α_k. Notice that the upper bound of the previous inequality is greater than 1. Let K be any subset of $\{1, \ldots, r\}$ and $0 \leq m_k \leq s_k$. Then, using repeatedly Eq. (8) we get

$$\prod_{k\in K} \Delta(\alpha_k)^{m_k} \leq \prod_{k\in K} \left(4\frac{\|f\|_\infty}{|a_d|}\right)^{m_k} \leq \left(4\frac{\|f\|_\infty}{|a_d|}\right)^{\sum_k m_k} \leq \left(4\frac{\|f\|_\infty}{|a_d|}\right)^{d}\ ,$$

which leads to

$$\prod_{i=1}^{r} \Delta_i^{s_i} = \prod_{k\in K} \Delta_k^{m_k} \prod_{k\notin K} \Delta_k^{m_k} \leq \prod_{k\in K} \Delta_k^{m_k} \left(4\frac{\|f\|_\infty}{|a_d|}\right)^{d} \Rightarrow \prod_{k\in K} \Delta_k^{m_k} \geq 4^{-d}\,|a_d|^d\,\|f\|_\infty^{-d} \prod_{i=1}^{r} \Delta_i^{s_i}\ . \tag{9}$$

By combining Eq. (9) and Eq. (7) we derive

$$\prod_{k\in K} \Delta_k^{m_k} \geq 4^{-d}\, r^{-2\,d}\, |a_d|^d\, \|f\|_\infty^{-d}\, \|f_r\|_\infty^{-d}\, \mathcal{M}\,(f)^{1-r}\, |\mathtt{Res}(f, f_r^{[1]})| \ .$$

Using basic properties of the norms and Mahler's measure we have

$$\|f_r\|_\infty \leq \|f_r\|_1 \leq 2^r \mathcal{M}\,(f_r) \leq 2^r \left|\frac{b_r}{a_d}\right| \mathcal{M}\,(f) \leq 2^r \left|\frac{b_r}{a_d}\right| \|f\|_2 \leq 2^r \left|\frac{b_r}{a_d}\right| (2d)^{1/2} \|f\|_\infty \ ,$$

and so

$$\prod_{k\in K} \Delta_k^{m_k} \geq 2^{-d^2-5d\lg d}\, \frac{|a_d|^{2d}}{|b_r|^d}\, \|f\|_\infty^{1-3d}\, |\mathtt{Res}(f, f_r')| \geq 2^{-6d^2\lg d}\, \frac{|a_d|^{2d}}{|b_r|^d}\, \|f\|_\infty^{1-3d}\, |\mathtt{Res}(f, f_r')| \ .$$

Separation bound. If we are only interested in the separation bound, that is the minimum of all local separation bounds, for our setting, we modify the proof of [32, Thm 4] to make it valid for polynomials with real coefficients. For this we need to compute a lower bound on $|f(\gamma)|$ where γ is a root of f' such that $f(\gamma) \neq 0$. We use the resultant $\mathtt{Res}(f'(x), y - f(x)) \in \mathbb{R}[y]$.

In the proof of [32, Thm 4] for deriving the lower bound on the separation bound, Eq. (19) is the following inequality

$$d^2\, \|f\|_1\, \Delta^2 \geq |f(\gamma)| \Rightarrow \Delta^2 \geq d^{-2}\, \|f\|_1^{-1}\, |f(\gamma)| \ ,$$

where γ is a root of the derivative of f such that $f(\gamma) \neq 0$. To lower bound this evaluation we consider the resultant $R = \mathtt{Res}(f'(x), y - f(x)) \in \mathbb{R}[y]$. The roots of this univariate polynomial are the evaluations of f at the roots of f'. It holds $\|R\|_\infty \leq \|f'\|_\infty^d\, d^d\, \|f\|_\infty \leq d^{2d} \|f\|_\infty^{2d}$. So the magnitude of the nonzero roots of R, $f(\gamma)$ is bounded from below as follows

$$|f(\gamma)| \geq \frac{|\mathtt{t}|}{2\,\|R\|_\infty} \geq 2^{-1}\, \mathtt{t}\, d^{-2d}\, \|f\|_\infty^{1-2d} \ ,$$

where $\mathtt{t}$ is the tailing coefficient of R. Putting all the inequalities together we obtain

$$\Delta \geq \frac{1}{2}\, d^{-d-2}\, \|f\|_\infty^{-d}\, \sqrt{|\mathtt{t}|} \ .$$

□

Proof (of Cor. 2): *(Integer polynomials.)* If the polynomials have integer coefficients, then we notice that the magnitude of the coefficients of the polynomials is at least 1 and we use the inequalities $|\mathtt{Res}(f, f_r^{[1]})| \geq 1$, $\mathcal{M}\,(f_r) \leq \mathcal{M}\,(f) \leq \|f\|_2$ and $\|f_r\| \leq 2^{d+\tau}$ to derive the three bounds of corollary. □

Remark 3. *The constants in the bounds of the previous theorem, especially in the case of polynomials with integer coefficients are not the best possible. They are not important for the asymptotic behavior of the bounds. However, they are important for some applications, e.g., for the implementation of subdivision algorithms. We present such an application in Section 7.2.*

We should also mention that if we know that the polynomial is square-free several simplifications are also possible.

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"*.

3 Multivariate separation bounds

This section generalizes $\texttt{DMM}_1$ to zero-dimensional polynomial systems. For details on well-constrained systems, see [11]. First we present additional notation and some preliminaris that we need to derive the bounds.

3.1 Additional notation and preliminaries

We now present some fundamental notions needed throughout the paper. The notation introduced here complements notation introduced at the end of Introduction.

Recall that $n > 1$ is the number of variables. Let $\mathbf{x}^{\mathbf{e}}$ denote the monomial $x_1^{e_1} \cdots x_n^{e_n}$, with $\mathbf{e} = (e_1, \ldots, e_n) \in \mathbb{Z}^n$. In the multivariate case, the input is a system of *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 it is possible to multiply Laurent polynomials by monomials without affecting their nonzero roots, in the sequel we assume there are no negative exponents. Let the polynomials be

$$f_i = \sum_{j=1}^{m_i} c_{i,j} \mathbf{x}^{a_{i,j}}, \quad 1 \le i \le n. \tag{10}$$

Let $\{a_{i,1}, \ldots, a_{i,m_i}\} \subset \mathbb{Z}^n$ be the support of f_i; its Newton polytope Q_i is the convex hull of the support. Let $\mathsf{MV}(Q_1, \ldots, Q_n) > 0$ be the *mixed volume* of convex polytopes $Q_1, \ldots, Q_n \subset \mathbb{R}^n$.

We consider the well-constrained polynomial system

$$(\Sigma): \ f_1(\mathbf{x}) = f_2(\mathbf{x}) = \cdots = f_n(\mathbf{x}) = 0, \tag{11}$$

where $f_i \in \mathbb{R}[\mathbf{x}^{\pm 1}]$, whose variety is assumed to be zero-dimensional and does not have any positive-dimensional component even at infinity. The more general case shall be considered in Section 5. We are interested in the system's toric roots, which lie in $(\mathbb{C}^*)^n$.

Let Q_0 be the unit standard simplex. Let $\mathsf{M}_i = \mathsf{MV}(Q_0, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n)$ and $\#Q_i$ denotes the number of lattice points in the closed polytope Q_i. Wlog, assume $\dim \sum_{i=0}^{n} Q_i = n$ and $\dim \sum_{i \in I} Q_i \ge j$ for any $I \subset \{0, \ldots, n\}$ with $|I| = j$, in other words the system is essential; otherwise, its roots would be defined by a smaller system.

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. A standard way to study a well-constrained system (Σ) through resultants is to add a linear polynomial f_0 and consider the $u-$resultant [15] of the overconstrained system; the latter is denoted by (Σ_0). The overconstrained system has Newton polytopes $Q_0, Q_1, \ldots, Q_n$. The following well-known theorem relates the number of isolated toric solutions of a polynomial system with the mixed volume. We commonly refer to it as the Bernstein's bound, or as the BKK bound.

Theorem 4. [4, 11, 17] *For $f_1, \ldots f_n \in \mathbb{C}[\mathbf{x}, \mathbf{x}^{-1}]$ with Newton polytopes $Q_1, \ldots, Q_n$, the number of common isolated solutions in $(\mathbb{C}^*)^n$, multiplicities counted, does not exceed $\mathsf{MV}(Q_1, \ldots, Q_n)$, independently of the corresponding variety's dimension.*

Let D be the number of roots $\in (\mathbb{C}^*)^n$ of (Σ), multiplicities counted, so $D \le \mathsf{M}_0$. Let $B = (n-1)\binom{D}{2}$, and let $\mathsf{dg}(f_i) = d_i \le d$. For $f_i \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$, let $\mathcal{L}(f_i) = \tau_i \le \tau$, $1 \le i \le n$. Let

$$D \le M_0 \le \prod_{i=1}^{n} d_i \le d^n, \quad B \le nD^2 \le n\prod_{i=1}^{n} d_i^2 \le nd^{2n},$$

$$\mathsf{M}_i \le \prod_{\substack{1\le j\le n\\ j\neq i}} d_j = D_i, \qquad \sum_{i=1}^{n} \mathsf{M}_i \le \sum_{i=1}^{n} D_i \le nd^{n-1},$$

$$\#Q_i \le n!\,\mathrm{vol}(Q_i) + n \le d_i^n + n \le 2d_i^n,$$

$$A = \prod_{i=1}^{n} \sqrt{\mathsf{M}_i}\, 2^{\mathsf{M}_i} \le 2^{nd^{n-1} + \frac{n^2-n}{2}\lg d},$$

$$C = \prod_{i=1}^{n} \|f_i\|_\infty^{M_i} \le 2^{\tau \sum_{i=1}^{n} \mathsf{M}_i} \le 2^{n\tau d^{n-1}},$$

$$h \le (n+1)^D \varrho \le (n+1)^{d^n} 2^{nd^{n-1}} d^{n^2 d^{n-1}},$$

$$\varrho = \prod_{i=1}^{n} (\#Q_i)^{M_i} \le 2^{\sum_{i=1}^{n} D_i} \prod_{i=1}^{n} d_i^{nD_i} \le 2^{nd^{n-1}}\, d^{n^2 d^{n-1}}.$$

Table 1. Notation needed for $\mathtt{DMM}_n$.

$\mathrm{vol}(\cdot)$ stand for Euclidean volume, and $\#Q_i$ for the number of lattice points in Q_i; the inequality connecting $\#Q_i$ and polytope volume in Table 1 is in [5]. Table 1 summarizes some important notation and states certain immediate properties.

Following the technique of u-resultant, we add an equation to (Σ) to obtain the system:

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

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

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

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 and corresponds to the number of solutions of the system. It is nonzero because we have assumed that the system has only isolated solutions, even at infinity. It holds that

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

The notation $|\cdot|$ denotes the absolute value. We use U_r to denote the square-free part of U. Finally, U_1 denotes the specialized u-resultant where $r_1 = -1$ and $r_i = 0$ for $i \neq 1$.

3.2 The $\mathtt{DMM}_n$ bound

In the sequel we present aggregate bounds that consider all the distinct roots of (Σ) by exploiting the system (Σ_0). As in the univariate case, Thm 1, we could consider any subset of the roots.

However, we choose to omit this case to simplify the presentation. For a root γ_j, γ_{c_j} is the root closest to it, under the Euclidean metric. Similarly to the univariate case we use the notation $\Delta_j = \|\gamma_j - \gamma_{c_j}\|_2$.

Main Theorem 5 (DMM$_n$). *Consider the zero-dimensional polynomial system (Σ) in (11), whose variety is assumed not to contain any positive-dimensional component, even at infinity. Let D be its number of solutions in $(\mathbb{C}^*)^n$, multiplicity counted, and let its distinct roots be $\gamma_1, \gamma_2, \ldots, \gamma_\ell$. Then*

$$\left(\frac{2^{D+3}\, n\varrho\, C}{\mathtt{lc}(U_1)}\right)^D \geq \prod_{1\leq j\leq \ell} \Delta_j \geq 2^{-\ell-15D-18D\lg D} (hC)^{-15D} B^{-(n-1)(\ell+15D^2)} \left|\mathbf{sr}_k(U)\right|^3 \ , \tag{15}$$

When the multiplicities of the roots, m_i, are taken into account, then we have the following bound

$$\left(\frac{2^{D+3}\, n\varrho\, C}{\mathtt{lc}(U_1)}\right)^D \geq \prod_{1\leq j\leq \ell} \Delta_j^{m_j} \geq B^{(1-n)D}\, 2^{-7\,D^2\,\lg D}\, |\mathtt{lc}(U)|^{2D}\, |\mathtt{lc}(U_r)|^{-D}\, \|U\|_\infty^{1-3d}\, |\mathtt{Res}(U, U_r')| \ , \tag{16}$$

while only for the separation bound we have the following inequality

$$\mathsf{sep}(\Sigma) \geq 2^{-D^2-4D\lg D}\, (\varrho\, C)^{-D} \sqrt{|\mathtt{tc}(U_1)|} \ , \tag{17}$$

where the precise definition of the specialized u-resultant U_1 is given just before Eq. (22). The nonzero coordinates of the roots are bounded as follows:

$$\frac{|\mathtt{tc}(U_1)|}{2^{D+1}\,\varrho\, C} \leq \frac{|\mathtt{tc}(U_1)|}{2\|U_1\|_\infty} \leq |\gamma_{j,i}| \leq 2\frac{\|U_1\|_\infty}{|\mathtt{lc}(U_1)|} \leq \frac{2^{D+1}\,\varrho\, C}{|\mathtt{lc}(U_1)|} \ . \tag{18}$$

Proof of main theorem 5. First, we establish the lower bound in (15). Let $\gamma_j = (\gamma_{j,1}, \ldots, \gamma_{j,n}) \in (\mathbb{C}^*)^n$, $1 \leq j \leq D$, be the solutions of (Σ), where f_i are defined in (10). We denote the set of solutions by $V \subset (\mathbb{C}^*)^n$.

We consider the system (Σ_0), Eq. (12), where the additional polynomial $f_0 = u + r_1 x_1 + r_2 x_2 + \cdots + r_n x_n$ has the new parameter u. It holds that $u = -\sum_i r_i\, \gamma_{j,i}$, for a solution γ_j. We choose properly the integer coefficients of $f_0, r_1, \ldots, r_n$, to ensure that the function

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

is injective. In this case f_0 is called a separating element. The existence of a separating element is ensured by the following proposition [3, 8, 15] .

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

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

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

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

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

Proof: The first inequality is well known. For the second let $B = (n-1)\binom{D}{2}$ and

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

□

Let us return to the proof of the Main Thm. From Eq. 14,

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

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 [33], see also Table (1), 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 bound the norm of U as follows:

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

If u_j are the distinct roots of U then, by the injectivity of f_0, it follows that $u_j = -\sum_{i=1}^{n} r_i \, \gamma_{j,i}$. The u-resultant has a stronger notion for 0-dimensional systems, since the multiplicities of its roots correspond to the multiplicities of the solutions of the system; we do not exploit this property further.

Proposition 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,*

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

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,

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

$$\left| \sum_{k=1}^{n} r_k \, \gamma_{i,k} - \sum_{k=1}^{n} r_k \, \gamma_{j,k} \right|^2 \le \sum_{k=1}^{n} r_k^2 \cdot \sum_{k=1}^{n} \left|\gamma_{i,k} - \gamma_{j,k}\right|^2 \Leftrightarrow \left|u_i - u_j\right|^2 \le \left(\sum_{k=1}^{n} r_k^2 \right) \cdot \|\gamma_i - \gamma_j\|_2^2 \ ,$$

and thus

$$\Delta_i = \|\gamma_i - \gamma_j\|_2 \ge \left(\sum_{k=1}^{n} r_k^2 \right)^{-1/2} \left|u_i - u_j\right| \ .$$

We denote by γ_{c_j} the root that is closest to γ_j. Since the previous bound holds for any pair of indices i and j, it also holds for j and c_j.

To prove the lower bound of Main Thm 5, we apply the previous inequality for all pairs j and c_j; there are ℓ. Then

$$\prod_{1\le j\le \ell} \Delta_j \ge \prod_{1\le j\le \ell} \|\gamma_j - \gamma_{c_j}\|_2 \ge \left(\sum_{k=1}^{n} r_k^2\right)^{-\frac{1}{2}\ell} \prod_{1\le j\le \ell} |u_j - u_{c_j}|. \tag{19}$$

It remains to bound the two factors of the RHS in 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

$$(\sum_{k=1}^{n} r_k^2)^{-\frac{1}{2}\ell} \ge 2^{-\ell}\, B^{(1-n)\ell}. \tag{20}$$

For the second factor of (19), we apply the univariate bound to U, Eq. (2) in Thm 1 and the bound that we have computed for $\|U\|_2$; thus:

$$\begin{aligned}\prod_{1\le j\le \ell} \left|u_j - u_{c_j}\right| &\ge D^{-18D}\, \mathcal{M}(U)^{-15D}\ |\mathbf{sr}_k(U,U')|^3 \ge 2^{-18D\lg D}\, \|U\|_2^{-15D} |\mathbf{sr}_k(U,U')|^3 \\ &\ge 2^{-18D\lg D}\, (2hCB^{(n-1)D})^{-15D} |\mathbf{sr}_k(U,U')|^3\ ,\end{aligned} \tag{21}$$

where $\mathbf{sr}_k(U,U')$ is the first non-vanishing subresultant coefficient in the subresultant sequence of U and its derivative, U'. Combining (19) with (20) and (21), we have the lower bound

$$\prod_{1\le j\le \ell} \Delta_j \ge 2^{-\ell}\, B^{(1-n)\ell}\, 2^{-18D\lg D}\, (2hCB^{(n-1)D})^{-15D} |\mathbf{sr}_k(U,U')|^3\ .$$

Regarding the bound that involves the multiplicities of the roots, we combine (19) and (21) with (3) to get

$$\prod_{1\le j\le \ell} \Delta_j^{m_j} \ge (\sum_{k=1}^{n} r_k^2)^{-\frac{1}{2}\sum_j m_j} \prod_{1\le j\le \ell} |u_j - u_{c_j}|^{m_j}.$$

$$\prod_{1\le j\le \ell} \Delta_j^{m_j} \ge 2^{-D}\, B^{(1-n)D}\, 2^{-6\,D^2\,\lg D}\, |\mathtt{lc}(U)|^{2D}\, |\mathtt{lc}(U_r)|^{-D}\, \|U\|_\infty^{1-3d}\, |\mathtt{Res}(U,U_r')|\ ,$$

where m_j is a number less than or equal to the multiplicity of u_i as a root of U and hence it bounds the multiplicity of γ_j as a root of the system.

In the case where the polynomials are in $\mathbb{Z}[\mathbf{x}]$, then $|\mathbf{sr}_k(U,U')| \ge 1$, $|a_d| \ge 1$, $|\mathtt{Res}(U,U_r')| \ge 1$. Thus we can omit these quantities from the bounds. To see this, recall that the univariate resultant can be computed as the determinant of the Sylvester matrix. Finally, we can bound b_r using Mignotte's bound. If the polynomials are in $\mathbb{Q}[\mathbf{x}]$ we can obtain similar bounds.

Upper and lower bounds on the roots. Now we establish the upper bound of Eq. (18). We specialize f_0 in (13) by setting $r_i = -1$, for some $i \in \{1,\ldots,n\}$, 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, denoted by $U_1 \in \mathbb{Z}[u]$. Its roots are the first coordinates of the isolated zeros of the system, namely $\gamma_{1,i}$, $1 \le i \le D$. Thus $\mathtt{dg}(U_1) \le D$.

The coefficients of U_1 are of the form, $\varrho_k\, \mathbf{c}_1^{\mathsf{M}_1}\mathbf{c}_2^{\mathsf{M}_2}\ldots\mathbf{c}_n^{\mathsf{M}_n}$, where $\varrho_k \in \mathbb{Z}$ and the interpretation of the rest of the formula is the same as before. Using [33], see also Table. (1), we obtain:

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

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

$$\|U_1\|_\infty \leq 2^D\, \varrho\, C \ , \tag{22}$$

and also $\|U_1\|_2 \leq \sqrt{D+1}\|U_1\|_\infty \leq \sqrt{D+1}\, 2^D\, \varrho\, C$.

From Cauchy's bound for the roots of univariate polynomials, e.g. [26], see also Eq. (1) in Thm 1, we know that for all the roots of U_1, $\gamma_{i,j}$, it holds that

$$\frac{|\mathtt{tc}(U_1)|}{2\|U_1\|_\infty} \leq |\gamma_{i,j}| \leq 2\frac{\|U_1\|_\infty}{|\mathtt{lc}(U_1)|} \ .$$

The inequality holds for all indices i, 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 $2^{D+1}\, \varrho\, C$ and $(2^{D+1}\, \varrho\, C)^{-1}$, resp. This proves Eq. (18).

Upper `DMM` bound. To prove the upper bound of Eq. (15) in Main Thm 5 we use the triangular inequality $\|a-b\|_2 \leq \|a\|_2 + \|b\|_2$. Then

$$\prod_{1\leq i\leq \ell} \|\gamma_i - \gamma_{c_i}\|_2^{m_i} \leq \prod_{1\leq i\leq \ell} (\|\gamma_i\|_2 + \|\gamma_{c_i}\|_2)^{m_i} \leq \prod_{1\leq i\leq \ell} (n\|\gamma_i\|_\infty + n\|\gamma_{c_i}\|_\infty)^{m_i} \leq \left(4n\frac{\|U_1\|_\infty}{\mathtt{lc}(U_1)}\right)^D \ ,$$

where the last inequality is due to Eq. (18).

Separation bound. To prove (17), let (i, j) be the pair of indices where the separation bound of (Σ) is attained. Then

$$\mathsf{sep}(\Sigma) = \|\gamma_i - \gamma_j\|_2 = \sqrt{\sum_{k=1}^{n} (\gamma_{i,k} - \gamma_{j,k})^2} \geq |\gamma_{i,1} - \gamma_{j,1}| \geq \mathsf{sep}(U_1),$$

where k is any index such that $\gamma_{i,k} \neq \gamma_{j,k}$ and $\mathsf{sep}(U_1)$ is the separation bound of U_1. To compute this we rely on Eq. (4), and

$$\mathsf{sep}(U_1) \geq \frac{1}{2}\, D^{-D-2}\, \|U_1\|_\infty^{-D}\, \sqrt{|\mathtt{tc}(U_1)|} \ ,$$

which completes the proof of (17) and, hence, the proof of Main Thm 5.

Corollary 9. *Under the hypothesis of Main Thm 5, 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*

$$\prod_{i=1}^{\ell} \Delta_i \ \geq\ 2^{-\eta_1} \tag{23}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-\eta_1} \qquad \textit{where} \quad \eta_1 = \widetilde{\mathcal{O}}(d^{2n-1}(d+\tau)) \ , \tag{24}$$

$$2^{-\eta_2} \leq |\gamma_{j,k}| \leq 2^{\eta_2} \qquad \textit{where} \quad \eta_2 = \widetilde{\mathcal{O}}(d^{n-1}(d+\tau)) \ . \tag{25}$$

An important aspect of innovation is to capture sparseness via mixed volumes:

Corollary 10. *Under the hypothesis of Main Thm 5, for $f_i \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$, $i = 1, \ldots, n$, we have*

$$\prod_{i=1}^{\ell} \Delta_i^{m_i} \geq 2^{-\eta_1} \qquad \text{where} \quad \eta_1 = 4\mathsf{M}_0^2 + 20n\mathsf{M}_0^2 \lg(n\mathsf{M}_0) + 4\mathsf{M}_0 \sum_{i=1}^{n} \mathsf{M}_i \left(\tau + \lg(\#Q_i)\right) \quad (26)$$

$$2^{-\eta_2} \leq |\gamma_{j,k}| \leq 2^{\eta_2} \qquad \text{where} \quad \eta_2 = 1 + \mathsf{M}_0 + \sum_{i=1}^{n} \mathsf{M}_i \left(\tau + \lg(\#Q_i)\right), \quad (27)$$

$$\mathsf{sep}(\Sigma) \geq 2^{-\eta_3} \qquad \text{where} \quad \eta_3 = \mathsf{M}_0(\mathsf{M}_0 + \lg \mathsf{M}_0 + \sum_{i=1}^{n} \mathsf{M}_i \left(\tau + \lg(\#Q_i)\right)) \ . \quad (28)$$

In the bounds of Cor. 10, when the polynomial f_i is of degree d_i and we do not know the mixed volume of the system we can set $\mathsf{M}_0 = \prod_{i=1}^{n} d_i$ and $\mathsf{M}_i = \prod_{k \neq i} d_k$.

The bounds on u-resultant are of independent interest, since the latter is used in many algorithms for solving polynomial systems, e.g. [3, 15].

Corollary 11. *For the u-resultant, $U \in \mathbb{R}[u]$, of the zero dimensional polynomial system it holds that* $\deg(U) \leq D$ *and* $\|U\|_\infty \leq \|U\|_2 \leq 2\, h\, C\, B^{(n-1)D} \leq 2\,(n+1)^D\, \varrho\, C\, B^{(n-1)D}$.

4 Comparisons and lower bounds

This section compares our results to the best existing bounds as well as to instances of systems illustrating that our bounds are not very far from the worst-case optimum.

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 zero-dimensional [36].

Theorem 12 (Gap theorem). [8] *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 Canny's bound becomes $2^{-(\lg 3 + \lg d + \tau) n d^n}$, which is worse than the bound in Eq. (25), by a factor of $O(d)$ in the exponent. In [6], they require that the system has a zero-dimensional projection; m is the number of polynomials and $b < n$ the dimension of the prime component where the zero-dimensional projection is considered. This bound is:

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

It is similar to ours in (18), and we make a comparison in the sequel. Nevertheless, Cor. 10 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. The following system was introduced in [8]:

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

The roots are $x_j = \left(2^{-\tau}\right)^{d^{j-1}}$, for $2^{\tau} \gg 1$. Our Main Thm 5 and its specialization with for integer coefficients using mixed volume, Cor. 10, implies $x_j \geq 2^{-1-(3+\tau)d^{n-1}-2(1+\tau)(n-2)d^{n-2}}$, which, if $\tau \gg d$, is off only by a factor of 2^n asymptotically. The negative exponent of our bound is $\mathcal{O}(\tau(d+n)d^{n-2})$, Canny's bound gives a negative exponent of $\mathcal{O}(n\tau d^{n-1})$, whereas the bound in [6] has negative exponent $\mathcal{O}(n^3 d^n + n\tau d^{n-1})$.

We present polynomial systems with bad separation bound in the sequel.

4.1 Recursive Mignotte polynomials

We consider the following triangular system

$$(M_n) \quad \begin{cases} A_1(\mathbf{x}) &= x_1^d - 2\,(a\,x_1 - 1)^2 \\ A_2(\mathbf{x}) &= x_1^{d/2} x_2^{d/2} - 2\left(x_2 - x_1^{d/4}\right)^2 \\ &\vdots \\ A_{n-1}(\mathbf{x}) &= x_{n-2}^{d/2} x_{n-1}^{d/2} - 2\left(x_{n-1} - x_{n-2}^{d/4}\right)^2 \\ A_n(\mathbf{x}) &= x_{n-1}^{d/2} x_n^{d/2} - 2\left(x_n - x_{n-1}^{d/4}\right)^2 \end{cases},$$

where $a \in \mathbb{Z}$, $a \geq 3$ and $d \geq 4$. The polynomial A_1 is the "classical" Mignotte polynomial [26]. It is not hard to see that other polynomials are also Mignotte since, for $2 \leq k \leq n$, we have $A_k(\mathbf{x}) = x_{k-1}^{d/2}\left(x_k^{d/2} - 2\left(\frac{1}{x_{k-1}^{d/4}} x_k - 1\right)^2\right)$, assuming that $x_{k-1} \neq 0$.

The polynomial A_1 is irreducible and has three positive roots, two of which very close to $1/a$, and it holds that

$$1/a - a^{-(d+2)/2} < \gamma_{1,1} < 1/a < \gamma_{1,2} < 1/a + a^{-(d+2)/2},$$

hence, for its separation bound, it holds

$$\mathsf{sep}(A_1) = |\gamma_{1,1} - \gamma_{1,2}| = \Delta_1 < 2\,a^{-(d+2)/2}\ .$$

If we substitute $x_1 = \gamma_{1,1}$ into A_2, then we obtain a Mignotte polynomial $A_2(\gamma_{1,1}, x_2)$ with coefficients that belong to a simple algebraic extension. If $\frac{1}{\gamma_{1,1}^{d/4}} \geq 3$, then it has three positive real roots, two of them very close to $\gamma_{1,1}^{d/4}$. We denote them by $\gamma_{2,1}$ and $\gamma_{2,2}$. For the separation bound of $A_2(\gamma_{1,1}, x_2)$ it holds

$$\Delta_2 \leq 2\left(1/\gamma_{1,1}^{d/4}\right)^{-(d/2+2)/2} \leq 2\,\gamma_{1,1}^{\frac{d}{4}(d/2+2)/2} \leq 2\,a^{-\frac{d}{4}(d/2+2)/2}\ .$$

If we continue similarly, then we get positive roots $\gamma_{k,1}$ and $\gamma_{k,2}$, where $1 \leq k \leq n$. We can easily prove by induction that $\frac{1}{\gamma_{k,1}^{d/4}} \geq 3$, for $1 \leq k \leq n$.

Theorem 13. *For the system (M_n), for $1 \leq k \leq n$, the following hold, for a positive root coordinate and for the separation bound:*

$$0 < \gamma_{k,1} < a^{-\left(\frac{d}{4}\right)^{k-1}}, \quad \Delta_k \leq 2\,a^{-(\frac{d}{4})^{k-1}(d/2+2)/2}, \text{ and } \Delta_n = \mathsf{sep}(M_n) \leq 2\,a^{-(\frac{d}{4})^{n-1}(d/2+2)/2}.$$

Proof: We know that $\gamma_{k,1} < \gamma_{k-1,1}^{d/4}$ so, by inductive hypothesis, we obtain

$$\gamma_{k,1} < \left(a^{-\left(\frac{d}{4}\right)^{k-2}}\right)^{d/4}\ .$$

For the second claim, it is enough to apply the bound we just established for $\gamma_{k-1,1}$ in

$$\Delta_k \leq 2\,(1/\gamma_{k-1,1}^{d/4})^{-(d/2+2)/2}\ .$$

For the $k = n$ we get the claimed bound for the n-th coordinate.

To prove the separation bound of the system we consider $\gamma_{1,1}$ the first positive root of $A_1(x_1)$, $\gamma_{2,1}$ the first positive root of $A(\gamma_{1,1}, x_2)$, abd we continue until $\gamma_{n-1,1}$, which the first positive real root of $A_{n-1}(\gamma_{1,1}, \gamma_{2,1}, \ldots, \gamma_{n-2,1}, x_{n-1})$. Then the polynomial $A_n(\gamma_{1,1}, \ldots, \gamma_{n-1,1}, x_n)$ has two roots, $\gamma_{n,1}$ and $\gamma_{n,2}$, that are very close. They are Δ_n close.

Now, conside the following two roots of (M_n), $\gamma_1 = (\gamma_{1,1}, \ldots, \gamma_{n-1,1}, \gamma_{n,1})$ and $\gamma_2 = (\gamma_{1,1}, \ldots, \gamma_{n-1,1}, \gamma_{n,2})$. For the them it holds that $\|\gamma_1 - \gamma_2\|_2 \leq \Delta_n$. □

In the case where $a = 2^\tau$, the previous theorem implies that the separation bound for the system and for the n-th coordinate is $2^{-\left(\frac{d}{4}\right)^{n+1}\tau} = 2^{-\widetilde{\mathcal{O}}(\tau d^{n+1})}$. The bound of Main Thm 5, specialized in Cor. 9, gives $2^{-\widetilde{\mathcal{O}}(\tau d^{2n})}$, which has, like our bounds, a linear second exponent, although our overall bound is still off by a factor of d^n in the exponent.

If we consider the aggregate version of DMM then we get that $\prod_{i=1}\|\gamma_i - \gamma_{c_i}\|_2 \leq (\Delta_n)^{2^n} = 2^{-\mathcal{O}(2^n\,\tau\, d^{n+1})}$ which is exponential, but still off by a factor of d^n in the exponent.

5 Positive-dimensional polynomial systems

We now consider the case that (Σ) is not zero-dimensional, or its variety contains a positive-dimensional component at infinity.

Then, the bounds of Main Thm 5 do not hold because they are based on bounding the infinite norm of the $u-$resultant which, in this case, 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 in the case of dense systems, Canny introduced the Generalized Characteristic Polynomial (GCP) [9]. We use its generalization to sparse resultants, called Toric GCP (TGCP) [12]: Consider (Σ_0) in (12) and perturb it:

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

where $p_i = \sum_{\mathbf{a}\in\mathcal{D}_i} s^{\omega_i(\mathbf{a})}\mathbf{x}^{\mathbf{a}}$, $\omega_i(\cdot)$ are positive-valued linear forms, s a new parameter, and $\mathcal{D}_i$ is the subset of vertices in Q_i corresponding to the monomials of f_i lying on the diagonal of the sparse resultant matrix constructed by using the $\omega_i(\cdot)$ as lifting functions. More precisely, the $\omega_i(\cdot)$ define a regular mixed subdivision of the Minkowski sum of the Newton polytopes which, in turn, yields a sparse resultant matrix [10, 11]. In the worst case, $\mathcal{D}_i$ contains all vertices of Q_i. Clearly, the 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 by $T \in (\mathbb{Z}[\mathbf{c}, \mathbf{r}])[u, s]$, 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 zero-dimensional component of the algebraic set defined by (Σ_0). We denote it by $T_U \in \mathbb{Z}([\mathbf{c}, \mathbf{r}])[u]$, and $\mathtt{dg}(T_U) \leq \mathsf{M}_0$. The roots of T_U are the isolated points of the variety and 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

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

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 with respect to 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

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

since every factor $\widetilde{\mathbf{c}}_{i,k}^{\mathsf{M}_i}$, contributes at most M_i coefficients; this expression defines A, C. The bound holds for (the absolute of) all coefficients of T, seen as a bivariate polynomial in s, u. Recall that $|\varrho_k| \le h$, for all k, where h is defined in Table (1).

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

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

The previous bound is the one on U multiplied by A (Cor. 11). Thus we extend Main Thm 5 to positive-dimensional systems by replacing C by AC in Main Thm 5, or U with T_U.

Theorem 14 (systems of dimension > 0). *Consider the polynomial system (Σ) in (11), which is not necessarily zero-dimensional. Let ℓ be the number of its distinct isolated solutions in $(\mathbb{C}^*)^n$, which are $\gamma_1, \gamma_2, \ldots, \gamma_\ell$. For a root γ_j, let γ_{c_j} be the root closest to it, under the Euclidean metric. Then*

$$\left(\frac{2^{D+3}\, n \varrho\, A\, C}{\mathtt{lc}(T_{U1})}\right)^D \ge \prod_{1\le j\le \ell} \Delta_j^{m_j} \ge B^{(1-n)D}\, 2^{-7\,D^2\,\lg D}\, |\mathtt{lc}(T_U)|^{2D}\, |\mathtt{lc}(T_{Ur})|^{-D}\, \|T_U\|_\infty^{1-3d}\, |\mathtt{Res}(T_U, T_{Ur}')|\ , \tag{29}$$

where T_{Ur} denotes the square-free part of the T_U, T_{U1} has a similar definition as U_1, $|\cdot|$ denotes absolute value and m_j upper-bounds the multiplicity of γ_j.

For the separation bound we have the following inequality

$$\mathsf{sep}(\Sigma) \ge 2^{-\mathsf{M}_0^2 - 4\mathsf{M}_0 \lg \mathsf{M}_0}\, (\varrho\, A\, C)^{-\mathsf{M}_0} \sqrt{|\mathtt{tc}(T_{U1})|}\ . \tag{30}$$

The nonzero coordinates of the roots are bounded as follows:

$$\frac{|\mathtt{tc}(T_{U1})|}{2^{\mathsf{M}_0+1}\, \varrho\, A\, C} \le \frac{|\mathtt{tc}(T_{U1})|}{2\|T_{U1}\|_\infty} \le |\gamma_{j,i}| \le 2\frac{\|T_{U1}\|_\infty}{|\mathtt{lc}(T_{U1})|} \le \frac{2^{\mathsf{M}_0+1}\, \varrho\, A\, C}{|\mathtt{lc}(T_{U1})|}\ . \tag{31}$$

Then

$$(2^{\mathsf{M}_0+1}\, \varrho\, A\, C)^\ell \ge \prod_{j=1}^\ell \Delta_j \ge 2^{-\ell-(\mathsf{M}_0-1)(\mathsf{M}_0+2)/2}\, (h\, A\, C)^{1-\mathsf{M}_0-\ell}\, B^{(1-n)(\mathsf{M}_0^2+\mathsf{M}_0(\ell-1)+\ell)},$$

$$(2^{\mathsf{M}_0}\, \varrho\, A\, C)^{-1} \le |\gamma_{j,k}| \le 2^{\mathsf{M}_0}\, \varrho\, A\, C, \tag{32}$$

$$\mathsf{sep}(\Sigma) \ge 2^{-(3\mathsf{M}_0+2)(\mathsf{M}_0-1)/2}\, (\sqrt{\mathsf{M}_0+1}\, \varrho\, A\, C)^{-\mathsf{M}_0}, \tag{33}$$

We also have the following, less accurate, bounds:

$$2^{-\eta_1} \leq |\gamma_{j,k}| \leq 2^{\eta_1} \qquad \text{where} \quad \eta_2 = (n^2-n)\lg\sqrt{d} + d^n + n(\tau + n\lg d + 2)d^{n-1}, \tag{34}$$

$$\prod_{j=1}^{\ell} \Delta_j \geq 2^{-\eta_2} \qquad \text{where} \quad \eta_1 = 2\,\eta_2\, d^n + (1 + 4\lg n + 4n\lg d)d^{2n}, \tag{35}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-\eta_3} \qquad \text{where} \quad \eta_3 = 2\,\eta_1\, d^n - (n^2-n)d^n \lg\sqrt{d}. \tag{36}$$

Remark 15. *Using the deformation technique and the TGCP, we have a slightly more general result. If a point on an irreducible component of positive dimension of the system at $s = 0$ is the limit of points of the perturbed system for $s \neq 0$, the same bounds applies on its coordinates.*

6 Overdetermined polynomial systems

The aforementioned bounds apply to well-constrained systems, namely when the number of unknowns equals the number of equations. In this section, we consider the case where the system contains more equations than unknowns.

Given an overdetermined system, we first perform a reduction to a square system using the result of [18]. Let $f_1, \ldots, f_p \in \mathbb{Z}[X_1, \ldots, X_n]$ be polynomials of positive degree, bounded by d. Denote by V the algebraic variety defined by $f_1 = \cdots = f_p = 0$. Given $\eta \in \overline{\mathbb{Z}}$, we denote by $\hat{f}_\eta$ the linear combination $f_1 + \eta^1 f_2 + \cdots + \eta^{p-1} f_p$.

Theorem 16. *[18, Section 3.4.1] Let $K \subset \mathbb{Z}$ of cardinal $p\,d^n + 1$. There exists $k = (k_1, \ldots, k_n) \in \Gamma^n$ such that each irreducible component of $\hat{V}$ defined by $\hat{f}_{k_1} = \cdots = \hat{f}_{k_n} = 0$ is either a component of V or a point.*

The previous theorem guarantees that if we consider the linear combinations to make our input system square, in the worst case, we add some isolated points. Therefore we can still recover the isolated points of the intial system.

We assume that all the polynmials $\hat{f}_i$ have the same Newton polytope Q. If this is not the case, we can set as Q be the convex hull of the union of Q_i, i.e. $Q = \cup_{i=1}^{p} Q_i$. If $\mathcal{L}(f_i) \leq \tau$, then $\mathcal{L}\left(\hat{f}_i\right) \leq \tau + n\lg d + \lg p$, where d is an upper bound on the degrees of f_i. Now our system is well defined and we can apply Thm 14 to obtain separation bounds for its isolated roots.

Let S denote the standard simplex. Let $s > 0$ be real number such that $\mathrm{vol}(Q) = s\,\mathrm{vol}(S) = s/n!$. Then $\mathsf{M}_0 = n!\,\mathrm{vol}(Q) = s^n$. Similarly $\mathsf{M}_i = s^{n-1}$. Now by applying Cor. 10 we get the following corollary:

Corollary 17. *Under the hypothesis of Main Thm 5, for $f_i \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$, $i = 1, \ldots, p$, that have degrees bounded by d and the same Newton polytope Q, we have the following bounds:*

$$2^{-\eta_1} \leq |\gamma_{j,k}| \leq 2^{-\eta_1} \quad \text{where} \quad \eta_1 = 1 + s^n + n\,s^{n-1}(\tau + n\lg d + \lg p + \lg(\#Q)), \tag{37}$$

$$\prod_{i=1}^{\ell} \Delta_i^{m_i} \geq 2^{-\eta_2} \qquad \text{where } \eta_2 = 4s^{2n} + 20ns^{2n}\lg(ns^n) + 4n\,s^{2n-1}\left(\tau + n\lg d + \lg p + \lg(\#Q)\right) \tag{38}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-\eta_3} \qquad \text{where} \quad \eta_3 = s^{2n} + s^n \lg s^n + n\,s^{2n-1}\left(\tau + n\lg d + \lg p + \lg(\#Q)\right) \tag{39}$$

In the case where the polynomials are dense and their degree is bounded by d, in the previous bounds we should replace s by d.

We can replace d^n in Thm 16 by $\mathrm{vol}(Q)$, but since this does not affect the asymptotics of the bounds, we decided not to do so.

7 Applications

We illustrate the bounds of Main Thm 5 in three 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]. Then, we employ our results to bound the number of steps that any subdivision algorithm has to perform in isolating the real roots of a well-defined polynomial system.

7.1 Eigenvalues and eigenvectors

Consider an $n \times n$ integer matrix A, with entries of bitsize $< \tau$. 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. [15].

Canny's Gap theorem [8] implies $|z| > (6 \cdot 2^\tau)^{-(n+1)2^n}$ for any eigenvalue or eigenvector element $z \neq 0$. Thus, in the worst case, we need $\mathcal{O}(n\,\tau\,2^n)$ bits to compute them. We get the same exponential behavior in n if we apply [36] or [6].

It is reasonable to assume that the system is zero-dimensional and apply (18) of Main Thm 5. 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 Main Thm 5 yields

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

where z is an eigenvalue or a nonzero coordinate of an eigenvector. This is exponentially better than the previous bounds. Eq. (17) from Main Thm 5 bounds the system's separation bound: $-\lg(\mathsf{sep}(\Sigma)) = \mathcal{O}(n^4 + n^3\tau)$. This is polynomial in the size of the input, and hence we obtain a new proof of Bareiss' result [1], namely that computing the eigenvalues and eigenvectors of an integer matrix has polynomial complexity.

7.2 Positive multivariate polynomials

We consider the following problem, studied in [2, 20]. Let $P \in \mathbb{Z}[x_1, \ldots, x_n]$ be a multivariate polynomial of degree d which, on the n-dimensional unit simplex $S = \{x \in \mathbb{R}^n \geq 0 \mid \sum_{i=1}^n x_i \leq 1\}$, takes only positive values. We are interested in computing a lower bound on its *minimum value* m.

Theorem 18. *Let τ bound the bitsize of the coefficients of polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$, and let $m^* = \min_{x \in S} P(x)$ over the unit simplex S. If $m^* > 0$, then*

$$\frac{1}{m^*} \leq 2^{(n^2+n)\lg\sqrt{d} + (2+3n+d+(n^2+3n+1)\lg d + (n+1)d\lg n)d(d-1)^{n-1}} \cdot 2^{(n+1)\tau d(d-1)^{n-1}}, \tag{40}$$

which simplifies to

$$-\lg m^* = \mathcal{O}(nd^n(n\lg d + d\lg n + \tau)) = \widetilde{\mathcal{O}}(d^n(d+\tau)).$$

Proof: We may assume that the minimum is attained inside the simplex and not on its boundary; if not, we apply a transformation which slightly changes the bitsize of P [2], that we will take into account at the end of the proof.

As the minimum is reached inside the simplex, it satisfies the following system in the unknowns m, x_i:

$$\begin{cases} \frac{\partial P}{\partial x_1}(x_1,\ldots,x_n) = \cdots = \frac{\partial P}{\partial x_n}(x_1,\ldots,x_n) = 0, \\ P(x_1,\ldots,x_n) = m. \end{cases} \tag{41}$$

We use Thm 14, since there is no guarantee that the system is zero-dimensional. However, Thm 14 provides bounds for the isolated points of the variety. Since the minimum could be attained on a nonzero dimensional component, we should argue that the bounds take care of this case. We use the TGCP method of Section 5 [9, 12], a property of the minimum of perturbed polynomials, also exploited in [20], and remark 15.

Let us consider the perturbed polynomial $P_s = P + s\,(x_1^d + \cdots + x_n^d)$, where s is a nonzero symbolic perturbation parameter. Now, the equations

$$f_i = \frac{\partial P_s}{\partial x_i}(x_1,\ldots,x_n) = \frac{\partial P}{\partial x_i}(x_1,\ldots,x_n) + s\,d\,x_i^{d-1}, \;\; i = 1,\ldots,n, \quad f_{n+1} = P_s - m$$

define the perturbed system $(\widetilde{\Sigma})$. Together with $f_0 = u + r_1x_1 + \cdots + r_nx_n + r_{n+1}m$ (where $u, r_1, \ldots, r_{n+1}$ are parameters), they define the overconstrained system $(\widetilde{\Sigma}_0)$, as in (12).

The resultant of $(\widetilde{\Sigma}_0)$ is nonzero because the resultant, with respect to $x_1,\ldots,x_n$, of $\frac{\partial P_s}{\partial x_i}(x_1,\ldots,x_n)$, $i = 1,\ldots,n$ and $u + r_1\,x_1 + \cdots + r_n\,x_n + r_{n+1}, P_s(x_1,\ldots,x_n)$, is nonzero, as a polynomial in s, and r_i. We deduce that $(\widetilde{\Sigma})$ is zero-dimensional for almost all values of s.

Hereafter we denote by (x_s^*, m_s^*) a minimum of P_s on the simplex S, i.e. $m_s^* = P_s(x_s^*) = \min_{x\in S} P_s(x)$. For any sequence $s_n \to 0$, we have a sequence $(x_{s_n}^*, m_{s_n}^*)$ of minima of P_{s_n} in the compact S, from which we can extract a subsequence s_n' and minima $(x_{s_n'}^*, m_{s_n'}^*)$ such that $m_{s_n'}^* = P(x_{s_n'}^*)$ and $s_n' \to 0$, $x_{s_n'}^* \to x^* \in S$, when $n \to \infty$. Since

$$m_{s_n'}^* = P_{s_n'}(x_{s_n'}^*) \le P_{s_n'}(x), \;\; \forall x \in S,$$

taking the limit we deduce that, $\forall x \in S$, $P(x^*) \le P(x)$, and that P reaches its minimum m^* on S at x^*.

As x^* is in the interior of S, so are the points $x_{s_n'}^*$ for n large enough. Thus $(x_{s_n'}^*, m_{s_n'}^*)$ is a sequence of points satisfying the perturbed system $(\widetilde{\Sigma})$ for n large enough. By remark 15, Thm 14 also bounds the coordinates of the limit point (x^*, m^*). Let us compute this bound.

We have $f_i = \frac{\partial P}{\partial x_i}$ and $f_{n+1} = P - m$. It holds that $\deg(f_{n+1}) = d$, $\deg(f_i) \le d-1$, $\|f_{n+1}\|_\infty \le 2^\tau$, $\|f_i\|_\infty \le d\|f_{n+1}\|_\infty \le d\,2^\tau$, $\mathsf{M}_{n+1} \le (d-1)^n$, $\mathsf{M}_i \le d(d-1)^{n-1}$, and $D \le \mathsf{M}_0 \le d(d-1)^n$. Using (31) we deduce $1/m \le 2^{\mathsf{M}_0}\,\varrho\,A\,C$. It remains to bound the various quantities involved, as defined in Table 1):

$$C \le \prod_{i=1}^{n+1} \|f_i\|_\infty^{\mathsf{M}_i} = \|f_{n+1}\|_\infty^{\mathsf{M}_{n+1}} \prod_{i=1}^{n+1} \|f_i\|_\infty^{\mathsf{M}_i} \le 2^{(n+1)\tau d(d-1)^{n-1} + nd(d-1)^{n-1}\lg d},$$

$$A = \prod_{i=1}^{n+1} \sqrt{\mathsf{M}_i}\,2^{\mathsf{M}_i} = \sqrt{\mathsf{M}_{n+1}}\cdot 2^{\mathsf{M}_{n+1}} \cdot \prod_{i=1}^{n} \sqrt{\mathsf{M}_i}\cdot 2^{\mathsf{M}_i} \le 2^{(n+1)d(d-1)^{n-1} + (n^2+n)\lg\sqrt{d}}.$$

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 (31) 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 $\frac{1}{m^*} \leq \frac{1}{m_{\texttt{DMM}p}}$, where

$$\frac{1}{m_{\texttt{DMM}p}} = 2^{(n^2+n)\lg\sqrt{d}+(2+3n+d+(n^2+3n+1)\lg d+(n+1)d\lg n)d(d-1)^{n-1}} \cdot 2^{(n+1)\tau d(d-1)^{n-1}},$$

which concludes the proof. □

In general, the system is not zero-dimensional. However, if we know that it is zero-dimensional, then we can apply Main Thm 5, and (18) to derive the following tighter bound:

$$\frac{1}{m^*} \leq 2^{((n+1)\tau+n+d+(n^2+3n+1)\lg d)d(d-1)^{n-1}}. \tag{42}$$

Let us compare with other bounds in the bibliography. In [2, Sec. 2, Rem. 2.17], the following bound was computed:

$$\frac{1}{m_{\texttt{BLR}}} = 2^{2^{n+3}n\tau d^{n+1}+2^{n+5}nd^{n+1}(2nd+d\lg n+n\lg d)}, \tag{43}$$

which also holds with no assumption, but is looser than ours.

In [6] the authors derive a bound for the minimum of the absolute value of a polynomial, namely $\frac{1}{m} \leq \frac{1}{m_{\texttt{BY}}}$, where

$$\frac{1}{m_{\texttt{BY}}} = ((n+2)^2 e^{n+3})^{(n+1)(n+2)d^{n+1}} (n^n(n+1)\,d\,2^\tau)^{(n+1)d^n}. \tag{44}$$

The authors use the terminology *evaluation bound* for their bound. It holds when there is a zero-dimensional projection, and they prove that this is always the case for system (41).

In [20], the following bound was computed:

$$\frac{1}{m^*} \leq \frac{1}{m_{\texttt{JP}}} = 2^{(\tau+1)d^{n+1}} d^{(n+1)d^{n+1}}, \tag{45}$$

which has no restriction on the corresponding polynomial system. It is comparable to our bound in general, but strictly looser when $d > n$.

Example 19. *Let us compute a lower bound on the value of* $f = (x+2y-3)^d + (x+2y-4)^d$, $d \in \{2, 8, 32\}$. *The polynomial is positive since 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, *then* $|\zeta_3| \geq 2^{-b}$, $b > 0$,

bound		$(d,\tau)=(2,5)$	$(8,20)$	$(32,85)$
[2], Eq. (43)	$\lvert\lg(m_{\mathtt{BLR}})\rvert$	27 136	6 684 672	1 604 321 280
[6], Eq. (44)	$\lvert\lg(m_{\mathtt{BY}})\rvert$	1 192	74 000	4 696 811
[20], Eq. (45)	$\lvert\lg(m_{\mathtt{JP}})\rvert$	72	15 360	3 309 568
Eq.(40)	$\lvert\lg(m_{\mathtt{DMM}_p})\rvert$	87	7 457	442 447
Eq.(42)	$\lvert\lg(m_{\mathtt{DMM}})\rvert$	54	5 201	324 506

Table 2. 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 $\tau\in\{5,20,85\}$, resp. The bounds hold for all polynomials with same characteristics.

bound $(n=3,d=10)$		$\tau=10$	$\tau=20$	$\tau=30$	$\tau=40$	$\tau=50$
[2], Eq. (43)	$\lvert\lg(m_{\mathtt{BLR}})\rvert$	678262344	697462344	716662344	735862344	755062344
[6], Eq. (44)	$\lvert\lg(m_{\mathtt{BY}})\rvert$	2740313	2780313	2820313	2860313	2900313
[20], Eq. (45)	$\lvert\lg(m_{\mathtt{JP}})\rvert$	242878	342878	442878	542878	642878
Eq.(40)	$\lvert\lg(m_{\mathtt{DMM}_p})\rvert$	151908	184308	216708	249108	281508
Eq.(42)	$\lvert\lg(m_{\mathtt{DMM}})\rvert$	78367	110767	143167	175567	207967

Table 3. Comparison of (the bitsize of) various bounds on the minimum value of a polynomial with $n=3$, $d=10$ and $\tau\in\{10,20,30,40,50\}$, respectively.

or $\zeta_3=0$. In Table 2, we present the above bounds on $\lg b$, whereas the true minimum value is 0. When the degree equals the number of variables ($d=2$), then our general bound is slightly weaker than $m_{\mathtt{JP}}$. When $d>n$, e.g. $d=4$ and $d=32$, our bound is tighter than $m_{\mathtt{JP}}$ by an order of magnitude. All other bounds are significantly looser in all cases.

Furthermore, Table 3 compares all bounds when the number of variables and the degree are fixed, namely $n=3$ and $d=10$, and we vary the bitsize $\tau\in\{10,20,30,40,50\}$. In Table 4, we fix the number of variables and the bitsize, $n=3$, $\tau=10$, and we vary the degree $d\in\{2,4,6,8,10\}$. In all cases our bounds are clearly superior.

7.3 General subdivision

We employ Main Thm 5, and equations (15) and (23), to bound the number of steps of a general subdivision algorithm to solve for the real roots of a well-defined polynomial system, as in (10). As is typically the case, we may assume the existence of an oracle which 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 for general n are found in [29, 31, 30], see also [3].

A straightforward derivation establishes the following:

Theorem 20. *Consider the polynomial system formed by the polynomials in (10). The number of steps* [1] *that a subdivision algorithm performs in order to compute isolating boxes for all the real roots of the system is $\widetilde{\mathcal{O}}(2^n\,(n^2+d+n\tau)\,d^{2n-1})$, where d and τ bound the degree and coefficient bitsize of each polynomial, D bounds the total number of (real) roots, and L is the side length of the hypercube containing all real roots.*

Remark 21. *If we specialize $n=1$ in the previous theorem, then we deduce that the number*

[1] you mean calls to the oracle?

bound ($n=3, \tau=10$)		$d=2$	$d=4$	$d=6$	$d=8$	$d=10$
[2], Eq. (43)	$\lvert\lg(m_{\mathtt{BLR}})\rvert$	253993	7636226	55504131	227057704	678262344
[6], Eq. (44)	$\lvert\lg(m_{\mathtt{BY}})\rvert$	4825	72898	361447	1129997	2740313
[20], Eq. (45)	$\lvert\lg(m_{\mathtt{JP}})\rvert$	240	4864	27657	94208	242878
Eq.(40)	$\lvert\lg(m_{\mathtt{DMM}_p})\rvert$	176	4273	21639	65372	151908
Eq.(42)	$\lvert\lg(m_{\mathtt{DMM}})\rvert$	117	2641	12457	35480	78367

Table 4. Comparison of (the bitsize of) various bounds on the minimum value of a polynomial with $n=3$, $\tau=10$ and $d \in \{2,4,6,8,10\}$, respectively.

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 bound is $\mathcal{O}(d^2 + d\tau)$ [13].

It is now straightforward to derive the first complexity bound of Milne's algorithm [29] in $\mathbb{R}^2$. This aggregate separation bound is also useful in the analysis of the subdivision algorithm based on continued fractions expansion [25] for polynomial system solving.

Acknowledgments. We thank M. Sombra for finding a missing factor in the original manuscript, and for bringing to our attention [33]. ET is partially supported by GeoLMI (ANR 2011 BS03 011 06), HPAC (ANR ANR-11-BS02-013) and an FP7 Marie Curie Career Integration Grant.

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] D.N. Bernstein. The number of roots of a system of equations. *Funct. Anal. and Appl.*, 9(2):183–185, 1975.

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

[6] W. D. Brownawell and C. K. Yap. Lower bounds for zero-dimensional projections. In *Proc. Annual ACM Symp. on Symbolic and Algebraic Computation (ISSAC)*, Seoul, Korea, 2009.

[7] 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 Symp. on Symbolic and Algebraic Computation (ISSAC)*, pages 87–94, Hagenberg, Austria, 2008.

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

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

[10] J.F. Canny and I.Z. Emiris. A subdivision-based algorithm for the sparse resultant. *J. ACM*, 47(3):417–451, May 2000.

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

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

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

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

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

[16] I.Z. Emiris, B. Mourrain, and E.P. Tsigaridas. The DMM bound: Multivariate (aggregate) separation bounds. In S. Watt, editor, *Proc. 35th ACM Int'l Symp. on Symbolic & Algebraic Comp. (ISSAC)*, pages 243–250, Munich, Germany, July 2010. ACM.

[17] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Boston, Birkhäuser, 1994.

[18] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In *Proc. Int. Meeting on Commutative Algebra, Cortona*. Citeseer, 1993.

[19] 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.

[20] G. Jeronimo and D. Perrucci. On the minimum of a positive polynomial over the standard simplex. *J. Symbolic Computation*, 45(4):434–442, 2010.

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

[22] Michael Kerber and Michael Sagraloff. A worst-case bound for topology computation of algebraic curves. *J. Symb. Comput.*, 47(3):239–258, 2012.

[23] Alexander Kobel and Michael Sagraloff. Improved complexity bounds for computing with planar algebraic curves. *arXiv preprint arXiv:1401.5690*, 2014.

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

[25] 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.

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

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

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

[29] 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.

[30] P. Pedersen. *Counting real zeros*. PhD thesis, New York University, 1991.

[31] 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.

[32] Siegfried M Rump. Polynomial minimum root separation. *Mathematics of Computation*, 33(145):327–336, 1979.

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

[34] E.P. Tsigaridas and I.Z. Emiris. On the complexity of real root isolation using continued fractions. *Theor. Comput. Sci.*, 392:158–173, 2008.

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

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