Separation bounds for polynomial systems

Ioannis Z. Emiris, Bernard Mourrain, Elias Tsigaridas

HAL Id: hal-01105276
https://inria.hal.science/hal-01105276v5

Submitted on 28 Jun 2019

Separation bounds for polynomial systems

Ioannis Emiris

Department of Informatics & Telecommunications, National and Kapodistrian University of Athens, Greece, and ATHENA Research & Innovation Center, Maroussi, Greece.

Bernard Mourrain

Université Cote d'Azur, Inria Méditerranée, Project Team Aromath, Sophia-Antipolis, France.

Elias Tsigaridas

Sorbonne Université, CNRS, INRIA, Laboratoire d'Informatique de Paris 6, LIP6, Équipe POLSYS, 4 place Jussieu, F-75005, Paris, France

Abstract

We rely on aggregate separation bounds for univariate polynomials to introduce novel worst-case separation bounds for the isolated roots of zero-dimensional, 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 upon Canny's Gap theorem [9]. Moreover, they exploit sparseness and they apply without any assumptions on the input polynomial system. To evaluate the quality of the bounds, we present polynomial systems whose root separation is asymptotically not far from our bounds.

We apply our bounds to three problems. First, we use them to estimate the bitsize of the eigenvalues and eigenvectors of an integer matrix; thus we provide a new proof that the problem has polynomial bit complexity. Second, we bound the value of a positive polynomial over the simplex: we improve by at least one order of magnitude upon all existing bounds. Finally, we asymptotically bound the number of steps of any purely subdivision-based algorithm that isolates all real roots of a polynomial system.

Keywords: Separation bound, sparse resultant, DMM, arithmetic Nullstellensätze, height of the resultant, polynomial system, positive polynomial, subdivision algorithm

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. In this context we

---

aim for tight bounds on the theoretical and the practical complexity of various solvers. The complexity bounds typically depend on *separation bounds*, that is 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. In addition is one of the fundamental quantities that appear in the analysis of symbolic algorithms.

Davenport [14] was the first to introduce aggregate separation bounds for the real roots of a univariate polynomial, which depend on Mahler's measure, e.g., [27]. Johnson [23] and Mignotte [28] loosened the hypothesis on the bounds and extended them to complex roots.

For algebraic systems, a fundamental result is Canny's Gap theorem [9] on the separation bound for square zero-dimensional systems, see Theorem 12. Yap [37] 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 [25].

There has been vivid interest for a closely related problem, encountered in real optimization. Basu, Leroy, and Roy [2] and Jeronimo and Perrucci [22] 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, 21, 26, 30, 36].

Our contribution. We improve the state-of-the-art by introducing 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 (Theorem 4) which is the sharpest general bound, and allows us to exploit the structure that is implicit in many applications. We can use any future better bound on the number of roots to improve these results. The main ingredients of our proof are resultants, including bounds on their height [34]. For other recent bound for the height of the resultant based on arithmetic Nullstellensatz we refer the reader to [13].

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 a factor $\mathcal{O}(d^{n-1})$, 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 we express them using mixed volumes. It seems nontrivial to apply sparse elimination theory with the approach of Brownawell and Yap [6]. More importantly, we extend our result to positive-dimensional systems, and we obtain results comparable to those by [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,

2

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 has 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, 22], by at least one order of magnitude in almost all cases.

Finally, we offer an upper bound on the number of steps of any pure subdivision-based algorithm exhibiting linear convergence and 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 DMM_n. Another open question is to express the positive-dimensional bound with respect to the dimension of the excess component.

A preliminary version of a large part of this paper's results appeared as [17]. This paper extends the work in [17] 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 Theorem 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.

Paper structure. We next introduce notation. In Section 2 we survey bounds for univariate polynomials. Section 3 derives and proves the multivariate version of our separation bound as Main Theorem 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. $\mathscr{O}_B$, resp. $\mathscr{O}$, stands for bit, resp. arithmetic, complexity and $\widetilde{\mathscr{O}}_B$, resp. $\widetilde{\mathscr{O}}$, means we are ignoring logarithmic factors. We use lg for $\log_2$. For a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, where $n \geq 1$, $\deg(f)$ denotes its total degree, while $\deg_{x_i}(f)$ denotes its degree with respect to x_i. By $h(f)$ 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 $a \in \mathbb{Q}$, $h(a) \geq 1$ 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 reciprocal is $\mathrm{recip}(f) = x^d f(1/x)$. The Mahler measure of f is $\mathscr{M}(f) := |a_d| \prod_{i=1}^{d} \max\{1, |z_i|\}$. If we further assume that $f \in \mathbb{Z}[x]$ and $h(f) = \tau$, then $\mathscr{M}(f) \leq \|f\|_2 \leq \sqrt{d+1}\|f\|_\infty \leq 2^\tau \sqrt{d+1}$, e.g., [27, 37]. Let us denote by $\mathrm{lc}(f)$ and $\mathrm{tc}(f)$ 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 the *local separation*. We also use the notation $\Delta(\gamma_i, f)$ to indicate that we consider the local separation 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 $\mathrm{sep}(f)$, denote the *separation bound*, that is the minimum distance between all roots of f. Let $\mathrm{sep}(\Sigma)$ denote the separation bound for a well-constrained polynomial system (Σ).

In the sequel we make use of $\mathtt{sr}_r(f, f')$, which stands for 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

This section studies (separation) bounds on the roots of a univariate polynomial f with complex coefficients, not necessarily square-free, of degree d. We denote the complex roots of f by α_j, in ascending magnitude.

There are several variants of (aggregate) separation bounds for the univariate case. We refer the reader to [35, 27, 14, 15, 23] and references therein. The theorem that we present in the sequel 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 [18, Thm. 11]. A bound that exploits the multiplicities of the roots first appeared in [24]. We modify the proof to derive a version valid for polynomials with complex coefficients; it appears in Eq. (3). The bound of Eq. (4) is derived from [33] after we modified the proof to make it valid for polynomials with complex coefficients. Separation bounds valid for polynomials with complex coefficients, besides being interested on their own, are useful because we can easily modify them to get bounds for polynomials having algebraic numbers as coefficients, or even transcendental numbers.

Theorem 1 (DMM$_1$). *Let $f \in \mathbb{C}[x]$ be such that $\mathrm{lc}(f) = a_d$ and $\deg(f) = d$, not necessarily square-free; let f_r be its square-free part, where $\deg(f_r) = r \leq d$ and $\mathrm{lc}(f_r) = b_r$. We assume $r \geq 2$ to avoid trivial cases. 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

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

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

$$\prod_{k \in K} \Delta_k \geq 2^{-2d(\lg d + 1)} |a_d|^{-1} \mathscr{M}(f)^{-2(r-1)} |\mathtt{sr}_{d-r}(f, f')| \quad , \tag{2}$$

where $\mathtt{sr}_{d-r}(f, f')$ is the $(d-r)$-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

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

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

$$\Delta(f) \geq 2^{-3/2 - 3d - 2\lg d - 7/2 d \lg d} \|f\|_\infty^{-d + \frac{\nu}{2} + \frac{1}{2}} \sqrt{|\mathtt{t}|} \quad , \tag{4}$$

4

where t *is the minimum of the trailing (non-zero) coefficient of the polynomial* $\texttt{res}(f'(x), y - f(x)) \in \mathbb{C}[y]$ *and trailing coefficient of* $\texttt{res}(\mathrm{recip}(f)'(x), y - \mathrm{recip}(f)(x)) \in \mathbb{C}[y]$ *and* v *the corresponding order.*

Corollary 2 (DMM$_1$ in $\mathbb{Z}$). *With the notation of Thm. 1 if f has integer coefficients and $\hbar(f) = \tau$, then Eq. (1) simplifies to*

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

Following Eq. (2) we get

$$\prod_{k \in K} \Delta_k \geq 2^{-4d \lg d} \|f\|_2^{-2d+2} \Rightarrow -\lg \prod_{k \in K} \Delta_k \leq 8d \lg d + 2d\tau = \mathcal{O}(d \lg d + d\tau) \ ,$$

while following Eq. (3) we obtain the bound

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

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

The upper (and the lower) bound on the roots of f in (1) is (a slightly modified version of) the well known Cauchy bound and its proof could be found in many textbooks, for example [37, 29].

We deduce the bound of Eq. (2) from [18, Thm. 11]:

$$\prod_{k \in K} \Delta_k \geq (r/\sqrt{3})^{-|K|} r^{-r} 3^{-\min\{d, 2d-2r\}/3} \mathcal{M}(f)^{-2(r-1)} |a_d|^{-1} |\mathrm{sr}_{d-r}(f, f')|$$

$$\geq d^{-2d} 3^{|K|/2 - \min\{d, 2d-2r\}/3} |a_d|^{-1} \mathcal{M}(f)^{-2(r-1)} |\mathrm{sr}_{d-r}(f, f')|$$

$$\geq 2^{-2d} d^{-2d} |a_d|^{-1} \mathcal{M}(f)^{-2(r-1)} |\mathrm{sr}_{d-r}(f, f')|$$

since $|K| \leq r \leq d$ and $3^{-1/2} > 2^{-2}$.

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 $\deg(q_i) = d_i$, $\sum_{i=1}^m d_i = r$, $\sum_{i=1}^m i d_i = d$, q_i is the product of the irreducible factors of multiplicity i of f and $f_r = \prod_{i=1}^m q_i$ is the square-free part of f. The leading coefficient of q_i is q_i. It holds $\mathrm{lc}(f) = a_d = \prod_i \mathsf{q}_i^i$, and $\mathrm{lc}(f_r) = b_r = \prod_i \mathsf{q}_i$.

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 of $\alpha_j^{(i)}$ as a root f or f_r, that is $\Delta(\alpha_j^{(i)}) = \Delta(\alpha_j^{(i)}, f_r) = \Delta(\alpha_j^{(i)}, f)$. We also use $w := \beta - \alpha_j^{(i)}$ 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

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

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

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

5

We have

$$|f_r^{[k]}(\alpha_j^{(i)})| \le \sum_{l=k}^r \frac{l!}{(l-k)!} \|f_r\|_\infty \max\{1, |\alpha_j^{(i)}|\}^{r-k}. \tag{7}$$

Under the assumption $|w| = \Delta(\alpha_j^{(i)}) \le 1$ and using the previous bound, the summation at the right-hand side of Eq. (6) becomes

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

Using this bound and Eq. (6) we get

$$\Delta(\alpha_j^{(i)}) \ge \frac{|f_r^{[1]}(\alpha_j^{(i)})|}{2^{r+1} \|f_r\|_\infty \max\{1, |\alpha_j^{(i)}|\}^{r-1}} \ge 2^{-r-1} \|f_r\|_\infty^{-1} \max\{1, |\alpha_j^{(i)}|\}^{1-r} |f_r^{[1]}(\alpha_j^{(i)})| \ . \tag{8}$$

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 Eq. (7), which yields

$$|f_r^{[1]}(\alpha_j^{(i)})| \le \sum_{l=1}^r l \|f_r\|_\infty \max\{1, |\alpha_j^{(i)}|\}^{r-1}$$

$$\le \frac{1}{2} r(r+1) \|f_r\|_\infty \max\{1, |\alpha_j^{(i)}|\}^{r-1} \le 2^{r+1} \|f_r\|_\infty \max\{1, |\alpha_j^{(i)}|\}^{r-1}$$

since $r(r+1) \le 2^{r+2}$ for $r \ge 0$.

Recall that $\mathcal{M}(q_i) = \mathrm{lc}(q_i) \prod_{j=1}^{d_i} \max\{1, |\alpha_j^{(i)}|\}$. We take into account the multiplicity of the root, which is i, and we consider the product over all the roots of q_i; then using Eq. (8) we get

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

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

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

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

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

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

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

6

Putting the various inequalities together we obtain the bound

$$\prod_{i=1}^{r} \Delta_i^{s_i} = \prod_{i=1}^{m}\prod_{j=1}^{d_i} \Delta(\alpha_j^{(i)})^i \geq 2^{-(r+1)d} \|f_r\|_\infty^{-d} \mathscr{M}(f)^{1-r} |\mathtt{res}(f, f_r^{[1]})| \ . \tag{9}$$

To account for the case where the product of the local separations does not involve all roots, we bound the missing factors and we modify the bound of Eq. (9) accordingly.

Using Cauchy's upper bound for the roots, Eq. (1), for any root $\alpha_j^{(i)}$, we get

$$\Delta(\alpha_j^{(i)}) = |\alpha_j^{(i)} - \beta| \leq |\alpha_j^{(i)}| + |\beta| \leq 4 \frac{\|f\|_\infty}{|a_d|} \ , \tag{10}$$

where β is the root of f closest to $\alpha_j^{(i)}$. Notice that the upper bound of the previous inequality is greater than 1, since $\|f\|_\infty = \max_k |a_k|$. Let K be any subset of $\{1, \ldots, r\}$ and $0 \leq m_k \leq s_k$. Then, using repeatedly Eq. (10), we get

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

Now we have

$$\prod_{i=1}^{r} \Delta_i^{s_i} = \prod_{k \in K} \Delta_k^{m_k} \prod_{k \in K} \Delta_k^{-m_k} \prod_{i=1}^{r} \Delta_k^{s_i} \leq \prod_{k \in K} \Delta_k^{m_k} \left(4 \frac{\|f\|_\infty}{|a_d|}\right)^{-\sum_{k \in K} m_k + d} \ , \tag{11}$$

which leads to

$$\prod_{k \in K} \Delta_k^{m_k} \geq 4^{-d} |a_d|^d \|f\|_\infty^{-d} \prod_{i=1}^{r} \Delta_i^{s_i} \ . \tag{12}$$

By combining Eq. (12) and Eq. (9) we derive

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

that proves the first inequality of Eq. (3). To prove the second inequality of Eq. (3) we use the basic properties of the norms and Mahler's measure to obtain the following bound

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

If we apply the latter bound to the first inequality of Eq. (3) we get

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

that proves the second inequality of Eq. (3).

Separation bound. Now we prove Eq. (4). To obtain this bound we modify the proof of [33, Thm 4] to make it valid for polynomials with complex coefficients.

Let α and β be the two roots for which the separation bound, Δ, is attained. We assume that at least one of the α and β has modulus less than 1, say β. We treat the case where both have modulus greater than one in the sequel. Moreover, let γ be the root of the derivative f' such that $f'(\gamma) \neq 0$ and $|\beta - \gamma|$ is minimal. It holds [33, Lemma 4]

$$|\beta - \gamma| \leq 2d\Delta \ . \tag{13}$$

The proof technique of [33, Thm 4] to get the lower bound on the separation bound exploits Eq. (19), which is the following inequality

$$d^2 \|f\|_1 |\beta - \gamma|^2 \geq |f(\gamma)| \ .$$

If we use Eq. (10) and the properties of the norms, then we have the following lower bound for the separation

$$\Delta \geq (2d^2)^{-1} \|f\|_\infty^{-1} |f(\gamma)|)^{\frac{1}{2}} \ .$$

It remains to bound the evaluation $|f'(\gamma)|$. For this we consider the resultant $R = \texttt{res}(f'(x), y - f(x)) \in \mathbb{C}[y]$. The roots of this univariate polynomial are the evaluations of f at the roots of f'. Let $f = \sum_{i=0}^d a_i x^i$ and $f' = \sum_{j=0}^{d-1}(j+1)a_{j+1}x^j = \sum_{j=0}^{d-1} b_j x^j$. It holds $|b_j| \leq d|a_j| \leq d\|f\|_\infty$, for all j. If we consider R as a multivariate polynomial, that is $R \in \mathbb{Z}[a_i, b_j][y]$, then its coefficients are integers with magnitude $\rho \leq 2^{2d+4d\lg d}$, see Table (1), Eq. (18), and Eq. (19)

Seeing R as a univariate polynomial in y, its coefficients, say c_k for $0 \leq k \leq d - 1$, are homogeneous polynomials in a_i and b_j of degree $2d - k - 1$. More specifically, they are homogeneous polynomials in the coefficients a_i of degree $d - k - 1$, and homogeneous in the coefficients b_j of degree d.

Let us take $\tilde{f} = \frac{f}{\|f\|_\infty}$ and use $\tilde{R}(y) = \texttt{res}(\tilde{f}', y - \tilde{f})$. The coefficient $\tilde{c}_k$ of y^k in $\tilde{R}(y)$ is $\|f\|_\infty^{2d-k-1}$ times the coefficient c_k of y^k in $R(y)$.

Each term of $\tilde{c}_k$ is a product of an integer, of magnitude at most ρ, of coefficients of $\tilde{f}$ of total degree $d - k - 1$, and of coefficients of $\tilde{f}$ of total degree d. Since $\|f\|_\infty = 1$, each term of $\tilde{c}_k$ has magnitude ρ. There are less than $(4d)^{2d}$ terms, and so

$$|\tilde{c}_k| \leq (4d)^{2d}\rho d^d \leq 2^{6d+7d\lg d},$$

which leads to

$$\|\tilde{R}\|_\infty \leq 2^{6d+7d\lg d} \ .$$

So the magnitude of the nonzero roots of $\tilde{R}$, $\tilde{f}(\gamma)$ is bounded from below as follows

$$|\tilde{f}(\gamma)| \geq \frac{|\tilde{t}|}{2\|\tilde{R}\|_\infty} \geq 2^{-1}2^{-6d-7d\lg d}|\tilde{t}| \ ,$$

where $\tilde{t}$ is the trailing (non-zero) coefficient of $\tilde{R}$ of order v. By homogeneity, we have $\tilde{t} = \|f\|_\infty^{-2d+v+1}t$ and $|\tilde{f}(\gamma)| = \|f\|_\infty^{-1}|f(\gamma)|$. Putting all the inequalities together we obtain

$$\Delta(f) \geq 2^{-3/2-3d-2\lg d-7/2d\lg d}\|f\|_\infty^{-d+\frac{v}{2}+\frac{1}{2}}\sqrt{|t|}.$$

If both α and β have modulus greater than 1, then we use the same arguments, mutatis mutandis, for $\text{recip}(f)$. $\qquad\qquad\square$

Proof of Corollary 2. (Root bounds for 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 $|\texttt{res}(f, f_r^{[1]})| \geq 1$ and $\mathscr{M}(f_r) \leq \mathscr{M}(f) \leq \|f\|_2$ to derive the three bounds of the corollary. $\qquad\square$

Remark 3. *The constants in the bounds of Thm 1, and especially in Cor. 2 where the polynomials have integer coefficients, are not the best possible. This is not important for the asymptotic behavior of the bounds. However, this has importance for some applications, e.g., for the implementation of subdivision-based 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, $\texttt{DMM}_1$ provides a bound on all distances between consecutive roots of a polynomial. This quantity is, asymptotically, almost equal to the separation. 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 preliminary observations that we use to derive the bounds.

3.1. Additional notation and preliminaries

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

Let $n > 1$ be the number of variables. Let $\mathbf{x^e}$ 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

$$f_i = \sum_{j=1}^{m_i} c_{i,j} \mathbf{x}^{a_{i,j}}, \quad 1 \leq i \leq n. \tag{14}$$

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

$$(\Sigma): \ f_1(\mathbf{x}) = f_2(\mathbf{x}) = \cdots = f_n(\mathbf{x}) = 0, \tag{15}$$

where $f_i \in \mathbb{R}[\mathbf{x}^{\pm 1}]$. Initially we assume that the corresponding variety is zero-dimensional and does not have any positive-dimensional component even at infinity. We consider the more general case 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 $\dim \sum_{i \in I} Q_i \geq j$ 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.

9

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

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

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

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

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

$$\rho = \prod_{i=1}^{n} (\#Q_i)^{\mathsf{M}_i} \leq 2^{\sum_{i=1}^{n} D_i} \prod_{i=1}^{n} d_i^{nD_i} \leq 2^{nd^{n-1}} d^{n^2 d^{n-1}},$$

$$h \leq (n+1)^D \rho \leq (n+1)^{d^n} 2^{nd^{n-1}} d^{n^2 d^{n-1}}.$$

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

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 [16] 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 (Bernstein, Khovanskii, and Kushnirenko).

Theorem 4. [4, 11, 19] *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 $D \leq \mathsf{M}_0$. Let $B = (n-1)\binom{D}{2}$ and let $\deg(f_i) = d_i \leq d$. For $f_i \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$, let $\hbar(f_i) = \tau_i \leq \tau$, $1 \leq i \leq n$. Let $\mathrm{vol}(\cdot)$ 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. We provide straightforward upper bounds for the various quantities using the total degrees of the input polynomials.

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

$$(\Sigma_0): \ f_0(\mathbf{x}) = f_1(\mathbf{x}) = \cdots = f_n(\mathbf{x}) = 0, \tag{16}$$

where

$$f_0 = u + r_1 x_1 + r_2 x_2 + \cdots + r_n x_n, \tag{17}$$

$r_1, \ldots, r_n \in \mathbb{Z}$ 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 that are homogeneous polynomials in the coefficients of (Σ_0):

$$U(u) = \cdots + \rho_k u^k \mathbf{r}_k^{D-k} \mathbf{c}_{1,k}^{\mathsf{M}_1} \mathbf{c}_{2,k}^{\mathsf{M}_2} \cdots \mathbf{c}_{n,k}^{\mathsf{M}_n} + \ldots, \tag{18}$$

where $\rho_k \in \mathbb{Z}$, $\mathbf{c}_{j,k}^{\mathsf{M}_j}$ denotes a monomial in the 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 complex solutions of the system. It is nonzero because we have assumed that the system has only isolated solutions, even at infinity. It holds that

$$\left| \mathbf{c}_{1,k}^{\mathsf{M}_1} \mathbf{c}_{2,k}^{\mathsf{M}_2} \cdots \mathbf{c}_{n,k}^{\mathsf{M}_n} \right| \leq C = \prod_{i=1}^{n} \|f_i\|_{\infty}^{\mathsf{M}_i}. \tag{19}$$

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 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, Theorem 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, let γ_{c_j} be 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 Eq. (15). We assume that the corresponding variety does not contain any positive-dimensional component, even at infinity. Let D be the number of solutions in $(\mathbb{C}^*)^n$, multiplicity counted, and let the distinct roots be $\gamma_1, \gamma_2, \ldots, \gamma_\ell$. Then*

$$\left(\frac{2^{D+3} n \rho C}{\mathrm{lc}(U_1)} \right)^D \geq \prod_{1 \leq j \leq \ell} \Delta_j \geq 2^{2-2\ell-4D \lg D} (hC)^{-2(\ell-1)} B^{-2(n-1)(\ell-1)D} |\mathsf{sr}_k(U)| . \tag{20}$$

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

$$\left(\frac{2^{D+3} n \rho C}{\mathrm{lc}(U_1)} \right)^D \geq \prod_{1 \leq j \leq \ell} \Delta_j^{m_j} \geq B^{(1-n)D} 2^{-7D^2} |\mathrm{lc}(U)|^{2D} |\mathrm{lc}(U_r)|^{-D} \|U\|_{\infty}^{1-2D-\ell} |\mathsf{res}(U, U_r')| . \tag{21}$$

When we consider only the separation bound we have the following inequality

$$\mathrm{sep}(\Sigma) \geq (2D)^{-4D} (2^D \rho C)^{-D-v/2-1/2} \sqrt{|\mathrm{tc}(U_1)|} , \tag{22}$$

where the precise definition[1] of the specialized u-resultant U_1 appears in the paragraph before Eq. (27). The nonzero coordinates of the roots are bounded as follows:

$$\frac{|\mathrm{tc}(U_1)|}{2^{D+1} \rho C} \leq \frac{|\mathrm{tc}(U_1)|}{2\|U_1\|_{\infty}} \leq |\gamma_{j,i}| \leq 2 \frac{\|U_1\|_{\infty}}{|\mathrm{lc}(U_1)|} \leq \frac{2^{D+1} \rho C}{|\mathrm{lc}(U_1)|} . \tag{23}$$

---

[1]U_1 denotes the specialized u-resultant where $r_1 = -1$ and $r_i = 0$ for $i \neq 1$.

Proof of main theorem 5. First, we establish the lower bound in (20). 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 as in (14). We denote the set of solutions by $V \subset (\mathbb{C}^*)^n$.

We consider the system (Σ_0), Eq. (16), 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 following proposition [3, 9, 16] ensures the existence of a separating element.

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

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

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

Corollary 7. *For any $f_0 \in \mathscr{F}$ 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 $B = (n-1)\binom{D}{2}$; then

$$\|f_0\|_\infty \leq \|f_0\|_2 \leq \sqrt{1 + B^2 + B^4 + \cdots + (B^2)^{n-1}}$$

$$= \sqrt{\frac{B^{2n}-1}{B^2-1}} = \sqrt{\frac{B^{2n-2}}{1-1/B^2}} \leq \sqrt{4B^{2n-2}}.$$

$\square$

Let us return to the proof of the Main Theorem. From Eq. (18), it follows that

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

From Corollary 7, we have that $|\mathbf{r}_k|^{D-k} \leq \|f_0\|_\infty^{D-k} \leq (B^{n-1})^{D-k}$, for all k. Let $|\rho_k| \leq h$, for all k. Then using [34], see also Table 1, we obtain:

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

We bound the (various) norm of U as follows:

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

12

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,*

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

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

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

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

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

and thus

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

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 Theorem 5, we apply the previous inequality for all pairs j and c_j; there are ℓ such pairs. Then

$$\prod_{1 \leq j \leq \ell} \Delta_j \geq \prod_{1 \leq j \leq \ell} \|\gamma_j - \gamma_{c_j}\|_2 \geq \left(\sum_{k=1}^{n} r_k^2\right)^{-\frac{1}{2}\ell} \prod_{1 \leq j \leq \ell} |u_j - u_{c_j}|. \tag{24}$$

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

$$\left(\sum_{k=1}^{n} r_k^2\right)^{-\frac{1}{2}\ell} \geq 2^{-\ell} B^{(1-n)\ell}. \tag{25}$$

For the second factor of (24), we apply the univariate bound to U, Eq. (2) in Theorem 1 and the bound that we have computed for $\|U\|_2$; thus:

$$\prod_{1 \leq j \leq \ell} |u_j - u_{c_j}| \geq 2^{-4D\lg D} \mathcal{M}(U)^{-2(\ell-1)} |\text{sr}_k(U,U')| \geq 2^{-4D\lg D} \|U\|_2^{-2(\ell-1)} |\text{sr}_k(U,U')|$$

$$\geq 2^{-4D\lg D} (2hCB^{(n-1)D})^{-2(\ell-1)} |\text{sr}_k(U,U')| , \tag{26}$$

where $\text{sr}_k(U,U')$ is the first non-vanishing subresultant coefficient in the subresultant sequence of U and its derivative, U'. Combining (24) with (25) and (26), we have the lower bound

$$\prod_{1 \leq j \leq \ell} \Delta_j \geq 2^{-\ell} B^{(1-n)\ell} 2^{-4D\lg D} (2hCB^{(n-1)D})^{-2(\ell-1)} |\text{sr}_k(U,U')| .$$

13

Regarding the bound that involves the multiplicities of the roots, we combine (24) and (26) with (3) to get

$$\prod_{1 \leq j \leq \ell} \Delta_j^{m_j} \geq \left(\sum_{k=1}^{n} r_k^2\right)^{-\frac{1}{2}\Sigma_j m_j} \prod_{1 \leq j \leq \ell} |u_j - u_{c_j}|^{m_j}.$$

$$\prod_{1 \leq j \leq \ell} \Delta_j^{m_j} \geq 2^{-D} B^{(1-n)D} 2^{-6D^2} |\mathrm{lc}(U)|^{2D} |\mathrm{lc}(U_r)|^{-D} \|U\|_\infty^{1-2d-\ell} |\mathrm{res}(U,U_r')| \ ,$$

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.

When the polynomials are in $\mathbb{Z}[\mathbf{x}]$, then $|\mathrm{sr}_k(U,U')| \geq 1$, and $|a_d| \geq 1$, hence $|\mathrm{res}(U,U_r')| \geq 1$. Thus, we can omit these quantities from the bounds. To see this, recall that we can compute the univariate resultant as the determinant of the Sylvester matrix. Finally, we can bound b_r using Mignotte's bound that bounds the norm of the divisors of a polynomial. 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. (23). We specialize f_0 in (17) by setting $r_i = -1$, for some $i \in \{1,\ldots,n\}$, and $r_j = 0$, where $1 \leq j \leq n$ and $j \neq i$. 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 $\gamma_{1,i}$, $1 \leq i \leq D$. Thus $\deg(U_1) \leq D$.

The coefficients of U_1 are of the form $\rho_k \mathbf{c}_1^{M_1} \mathbf{c}_2^{M_2} \ldots \mathbf{c}_n^{M_n}$, where $\rho_k \in \mathbb{Z}$ and the interpretation of the rest of the formula is the same as before. Using [34], see also Table 1, we obtain

$$|\rho_k| \leq \prod_{i=0}^{n} (\#Q_i)^{M_i} = (\#Q_0)^D \prod_{i=1}^{n} (\#Q_i)^{M_i} = 2^D \rho,$$

as the Newton polytope of f_0 is a simplex in dimension 1. It also holds $|\mathbf{c}_1^{M_1} \mathbf{c}_2^{M_2} \ldots \mathbf{c}_n^{M_n}| \leq C$. Combining the two inequalities we deduce that

$$\|U_1\|_\infty \leq 2^D \rho C \ , \tag{27}$$

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

From Cauchy's bound for the roots of univariate polynomials, e.g. [27], see also Eq. (1) in Theorem 1, we know that for all the roots of U_1, $\gamma_{i,j}$, it holds that

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

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 $2^{D+1}\rho C$ and $(2^{D+1}\rho C)^{-1}$, respectively. This proves Eq. (23).

Upper DMM bound. To prove the upper bound of Eq. (20) in Main Theorem 5 we use the triangular inequality $\|a-b\|_2 \leq \|a\|_2 + \|b\|_2$. Then

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

where the last inequality is due to Eq. (23).

14

Separation bound. To prove Eq. (22), let (i, j) be the pair of indices where the separation bound of (Σ) is attained. Then,

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

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

$$\mathsf{sep}(U_1) \geq (2D)^{-4D} \|U_1\|_{\infty}^{-D-\nu/2-1/2} \sqrt{|\mathsf{tc}(U_1)|} \ ,$$

which completes the proof of (22), and by this, the proof of Main Theorem 5.

For the rest of the section, since we refer to the degree of Laurent polynomials, we may assume that their Newton polytope has been translated to lie in the positive quadrant with minimal total degree. The toric elimination parameters of the system, such as mixed volume, are invariant under this operation. In short, our polynomials could be Taylor polynomials throughout this section, examined in terms of their Newton polytopes.

Corollary 9. *Under the hypothesis of Main Theorem 5, for $f_i \in \mathbb{Z}[\mathbf{x}]$, $\deg(f_i) \leq d$ and $h(f_i) \leq \tau$, we have*

$$\prod_{i=1}^{\ell} \Delta_i \geq 2^{-\eta_1} \tag{28}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-\eta_1} \qquad \qquad where \quad \eta_1 = \widetilde{\mathscr{O}}(d^{2n-1}(d+\tau)) \ , \tag{29}$$

$$2^{-\eta_2} \leq |\gamma_{j,k}| \leq 2^{\eta_2} \qquad \qquad where \quad \eta_2 = \widetilde{\mathscr{O}}(d^{n-1}(d+\tau)) \ . \tag{30}$$

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

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

$$\prod_{i=1}^{\ell} \Delta_i^{m_i} \geq 2^{-\eta_1} \qquad where \quad \eta_1 = 7\mathsf{M}_0^2 + 6n\mathsf{M}_0^2 \lg(n\mathsf{M}_0^2) + 3\mathsf{M}_0 \sum_{i=1}^{n} \mathsf{M}_i (\tau + \lg(\#Q_i)) \tag{31}$$

$$2^{-\eta_2} \leq |\gamma_{j,k}| \leq 2^{\eta_2} \qquad \qquad where \quad \eta_2 = 1 + \mathsf{M}_0 + \sum_{i=1}^{n} \mathsf{M}_i (\tau + \lg(\#Q_i)), \tag{32}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-\eta_3} \qquad \qquad where \quad \eta_3 = \mathsf{M}_0(5\lg(2\mathsf{M}_0) + \sum_{i=1}^{n} \mathsf{M}_i (\tau + \lg(\#Q_i))) \ . \tag{33}$$

In the bounds of Corollary 10, when the polynomial f_i has 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, many algorithms for solving polynomial systems use them to establish complexity bounds, e.g., [3, 16].

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*

$$\|U\|_{\infty} \leq \|U\|_2 \leq 2hCB^{(n-1)D} \leq 2(n+1)^D \rho CB^{(n-1)D}.$$

15

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 [37].

Theorem 12 (Gap theorem). [9] *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 $|\gamma_{j,k}| > (3dc)^{-nd^n}$.*

Let $h(f_i) = \tau$, then Canny's bound becomes $2^{-(\lg 3 + \lg d + \tau)nd^n}$, which is worse than the bound in Eq. (30), by a factor of $\mathcal{O}(d)$ in the exponent. In [6], they require that the system has a zero-dimensional projection. Let m be the number of polynomials and $b < n$ the dimension of the prime component where the zero-dimensional projection is considered. Then, the bounds from [6] is

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

This bound is similar to ours in Eq. (23) We make a comparison in the sequel. Nevertheless, the bound from Corollary 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 [9]:

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

The roots are $x_j = (2^{-\tau})^{d^{j-1}}$, for $2^\tau \gg 1$. Our Main Theorem 5, and its specialization with integer coefficients using mixed volume Corollary 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 bounds in the next section.

4.1. Recursive Mignotte polynomials

We present a polynomial system that attains an exponentially, with respect to the input parameters, separation bound. We consider the following triangular system

$$(M_n) \quad \begin{cases} A_1(\mathbf{x}) & = & x_1^d - 2(ax_1 - 1)^2 \\ A_2(\mathbf{x}) & = & x_1^{d/2} x_2^{d/2} - 2\left(x_2 - x_1^{d/4}\right)^2 \\ & \vdots & \\ A_{n-1}(\mathbf{x}) & = & x_{n-2}^{d/2} x_{n-1}^{d/2} - 2\left(x_{n-1} - x_{n-2}^{d/4}\right)^2 \\ A_n(\mathbf{x}) & = & x_{n-1}^{d/2} x_n^{d/2} - 2\left(x_n - x_{n-1}^{d/4}\right)^2 \end{cases},$$

where $a \in \mathbb{Z}$, $a \geq 3$ and $d \geq 4$. Polynomial A_1 is the "classical" Mignotte polynomial [27]. It is not hard to see that other polynomials are also Mignotte-like since, for $2 \leq k \leq n$, we have

$$A_k(\mathbf{x}) = x_{k-1}^{d/2}\left(x_k^{d/2} - 2\left(\frac{1}{x_{k-1}^{d/4}} x_k - 1\right)^2\right), \text{ assuming that } x_{k-1} \neq 0.$$

16

The polynomial A_1 is irreducible over $\mathbb{Q}$ 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

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

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

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

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:*

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

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

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

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

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

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 $A(\gamma_{1,1}, x_2)$, and we continue until $\gamma_{n-1,1}$, which is 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, consider 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 them it holds that $\|\gamma_1 - \gamma_2\|_2 \leq \Delta_n$. $\square$

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 $2^{-\left(\frac{d}{4}\right)^n \tau} = 2^{-\widetilde{\mathcal{O}}(\tau d^n)}$. The bound of Main Theorem 5, specialized in Corollary 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 $\prod_{i=1} \|\gamma_i - \gamma_{c_i}\|_2 \leq (\Delta_n)^{2^n} = 2^{-\mathcal{O}(2^n \tau d^n)}$ which is exponential, but still off by a factor of d^n in the exponent.

17

5. Positive-dimensional polynomial systems

This section considers the case where (Σ) is not zero-dimensional, in other words the corresponding variety contains a positive-dimensional component, possibly at infinity. Then, the bounds of Main Theorem 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; any component of positive dimension is known as excess component.

To overcome the existence of excess components in the case of dense systems, Canny introduced the Generalized Characteristic Polynomial (GCP) [8]. We use its generalization to sparse resultants, called Toric GCP (TGCP) [12]. Consider (Σ_0) in (16) 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 $p_i = \sum_{\mathbf{a} \in \mathscr{D}_i} s^{\omega_i(\mathbf{a})} \mathbf{x}^{\mathbf{a}}$, $\omega_i(\cdot)$ are positive-valued linear forms, s a new parameter, and $\mathscr{D}_i$ 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, $\mathscr{D}_i$ contains all vertices of Q_i. Clearly, the perturbation does not alter neither 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 $\deg(T_U) \le \mathsf{M}_0$. 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. (18), we get

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

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 assume 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

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

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

18

Now, observe that $k \leq \mathsf{M}_0$. 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 zero-dimensional case:

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

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

Theorem 14 (Systems of dimension > 0). *Consider the polynomial system* (Σ) *in (15), 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*

$$\left(\frac{2^{D+3} n \rho A C}{\mathrm{lc}(T_{U1})} \right)^D \geq \prod_{1 \leq j \leq \ell} \Delta_j^{m_j} \geq B^{(1-n)D} 2^{-7D^2} |\mathrm{lc}(T_U)|^{2D} |\mathrm{lc}(T_{Ur})|^{-D} \|T_U\|_\infty^{1-2D-\ell} |\mathtt{res}(T_U, T'_{Ur})| \ , \tag{34}$$

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

$$\mathrm{sep}(\Sigma) \geq 2^{-\mathsf{M}_0^2 - 4\mathsf{M}_0 \lg \mathsf{M}_0} (\rho A C)^{-\mathsf{M}_0} \sqrt{|\mathrm{tc}(T_{U1})|} \ . \tag{35}$$

The nonzero coordinates of the roots are bounded as follows:

$$\frac{|\mathrm{tc}(T_{U_1})|}{2^{\mathsf{M}_0+1} \rho A C} \leq \frac{|\mathrm{tc}(T_{U_1})|}{2\|T_{U_1}\|_\infty} \leq |\gamma_{j,i}| \leq 2 \frac{\|T_{U_1}\|_\infty}{|\mathrm{lc}(T_{U_1})|} \leq \frac{2^{\mathsf{M}_0+1} \rho A C}{|\mathrm{lc}(T_{U_1})|} \ . \tag{36}$$

Morover, for the aggregate version of the separation bound it holds

$$(2^{\mathsf{M}_0+1} \rho A C)^\ell \geq \prod_{j=1}^\ell \Delta_j \geq 2^{2-2\ell-4\mathsf{M}_0 \lg \mathsf{M}_0} (\rho A C)^{-2(\ell-1)} B^{2(1-n)(\ell-1)\mathsf{M}_0},$$

$$\mathrm{sep}(\Sigma) \geq 2^{-\mathsf{M}_0^2 - 4\mathsf{M}_0 \lg \mathsf{M}_0} (\rho A C)^{-\mathsf{M}_0} \sqrt{\mathrm{tc}(|T_{U_1}|)} \ . \tag{37}$$

We also have the following, less accurate, bounds, when we consider polynomials with integer cofficients:x

$$2^{-\eta_1} \leq |\gamma_{j,k}| \leq 2^{\eta_1} \qquad \text{where} \qquad \eta_1 = (n^2 - n) \lg \sqrt{d} + d^n + n(\tau + n \lg d + 2) d^{n-1}, \tag{38}$$

$$\prod_{j=1}^\ell \Delta_j \geq 2^{-\eta_2} \qquad\qquad \text{where} \qquad \eta_2 = 2\eta_2 d^n + (1 + 4 \lg n + 4n \lg d) d^{2n}, \tag{39}$$

$$\mathrm{sep}(\Sigma) \geq 2^{-\eta_3} \qquad\qquad\quad \text{where} \qquad \eta_3 = 2\eta_1 d^n - (n^2 - n) d^n \lg \sqrt{d}. \tag{40}$$

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.*

19

6. Overdetermined polynomial systems

The aforementioned bounds apply to well-constrained systems, namely when the number of unknowns equals the number of equations. This section discusses 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 [20]. 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. *[20, Sec. 3.4.1] Let $K \subset \mathbb{Z}$ of cardinality $p\,d^n + 1$. 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.*

This 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 initial system.

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

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

Corollary 17. *Under the hypothesis of Main Theorem 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:*

$$2^{-\eta_1} \leq |\gamma_{j,k}| \leq 2^{-\eta_1} \quad where \quad \eta_1 = 1 + s^n + n s^{n-1}(\tau + n \lg d + \lg p + \lg(\#Q)), \tag{41}$$

$$\prod_{i=1}^{\ell} \Delta_i^{m_i} \geq 2^{-\eta_2} \qquad where\ \eta_2 = 7s^{2n} + 6ns^{2n}\lg(ns^{2n}) + 3ns^{2n-1}(\tau + n\lg d + \lg p + \lg(\#Q)) \tag{42}$$

$$\mathsf{sep}(\Sigma) \geq 2^{-\eta_3} \qquad where \quad \eta_3 = s^{2n} + s^n \lg s^n + n s^{2n-1}(\tau + n\lg d + \lg p + \lg(\#Q)) \tag{43}$$

If the polynomials are dense of degree d, then in the previous bounds we should replace s by d. We can also replace d^n in Theorem 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 Theorem 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 lower bounds positive multivariate polynomials, inspired by [2]. Thirdly, we use 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 $f_j = \sum_{j=1}^n a_{i,j} v_j - \lambda v_i$, $1 \le i \le n$, $1 \le j \le n$, and $f_{n+1} = \sum_{i=1}^n v_i^2 - 1$. We have $\|f_j\|_\infty \le 2^\tau$, $\|f_{n+1}\|_\infty \le 2$. The Bézout bound is 2^{n+1}, whereas the actual number of (complex) solutions is $2n$, which equals the mixed volume, e.g. [16].

Canny's Gap theorem [9] implies $|z| > (6 \cdot 2^\tau)^{-(n+1)2^n}$ for any eigenvalue or eigenvector element $z \ne 0$. 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 [37, Thm. 11.45] or [6, Thm. 2] to the corresponding polynomial system.

It is reasonable to assume that the system is zero-dimensional and apply Eq. (23) of Main Theorem 5. It holds that $\mathsf{M}_j = 2n$, $\mathsf{M}_{n+1} = n$, $(\#Q_{n+1}) \le 2^{n+2}$, and $(\#Q_i) \le 2^{n+2}$ where $1 \le j \le n$, and $C = \|f_{n+1}\|_\infty^{\mathsf{M}_{n+1}} \prod_{j=1}^n \|f_j\|_\infty^{\mathsf{M}_j} \le 2^{\tau \sum_{j=1}^n \mathsf{M}_j} 2^n = 2^{2n^2\tau+n}$, $\rho \le \prod_{i=1}^{n+1} (\#Q_i)^{\mathsf{M}_i} \le (\#Q_{n+1})^{\mathsf{M}_{n+1}} \prod_{i=1}^n (\#Q_i)^{\mathsf{M}_i}$; hence $\rho \le (2^{n+2})^n \prod_{i=1}^n (2^{n+2})^{2n} \le 2^{2n^3+5n^2+2n}$.

The solutions lie in $\mathbb{C}^{n+1}$. The lower bound of Main Theorem 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. (22) from Main Theorem 5 bounds the system's separation bound: $-\lg(\mathrm{sep}(\Sigma)) = \mathcal{O}(n^4 + n^3\tau)$. 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, 22]. Let $P \in \mathbb{Z}[x_1, \ldots, x_n]$ be a multivariate polynomial of degree d which, on the n-dimensional unit simplex $S = \{x \in \mathbb{R}^n \ge 0 \mid \sum_{i=1}^n x_i \le 1\}$, takes only positive values. Our goal is to compute 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*

$$\frac{1}{m^*} \le \frac{1}{m_{DMMp}} = 2^{(n^2+n)\lg\sqrt{d}+(2+3n+d+(n^2+3n+1)\lg d+(n+1)d\lg n)d(d-1)^{n-1}} \cdot 2^{(n+1)\tau d(d-1)^{n-1}}, \quad (44)$$

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 first assume that the minimum is attained inside the simplex and not on its boundary.

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

$$\begin{cases} \frac{\partial P}{\partial x_1}(x_1, \ldots, x_n) = \cdots = \frac{\partial P}{\partial x_n}(x_1, \ldots, x_n) = 0, \\ P(x_1, \ldots, x_n) = m. \end{cases} \quad (45)$$

We use Theorem 14, since there is no guarantee that the system is zero-dimensional. However, Theorem 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 [8, 12], a property of the minimum of perturbed polynomials, also exploited in [22], 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

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

define the perturbed system $(\widetilde{\Sigma})$. Together with $f_0 = u + r_1 x_1 + \cdots + r_n x_n + r_{n+1} m$ (where $u, r_1,\ldots,r_{n+1}$ are parameters), they define the overconstrained system $(\widetilde{\Sigma}_0)$, as in (16).

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 sub-sequence 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, Theorem 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 (36) we deduce $1/m \le 2^{\mathsf{M}_0} \rho A C$. 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, $(\#Q_{n+1}) \le 2d^{n+1}$, $(\#Q_i) \le 2(d-1)^{n+1}$, and so

$$\rho = \prod_{i=1}^{n+1} (\#Q_i)^{\mathsf{M}_i} = (\#Q_{n+1})^{\mathsf{M}_{n+1}} \prod_{i=1}^{n} (\#Q_i)^{\mathsf{M}_i}$$

$$\le (2d^{n+1})^{(d-1)^n} \cdot \prod_{i=1}^{n} (2d^n)^{d(d-1)^{n-1}} \le 2^{(n+1)(1+(n+1)\lg d)d(d-1)^{n-1}}$$

We apply (36) using the previous inequalities, and get

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

If the minimum m^* is not reached inside the simplex, then it is reached at a vertex or in the (relative) interior of a face of S, which is a simplex in lower dimension. If the minimum is reached at a vertex $e_i = (0,\dots,0,1,0,\dots 0)$ or at the origin $(0,\dots,0)$ and positive, then $m^* \in \mathbb{N}^*$ and $\frac{1}{m^*} \le 1$ and (44) is clearly satisfied.

If the minimum is reached in the interior of a face of S, the restriction of P on such a face is obtained by substituting some of the variables x_i by 0 and some other variables by $1 - x_{i_1} - \cdots - x_{i_l}$. By [2][Lemma 2.3], this transforms the polynomial P into a new polynomial with the degree bounded by d and the bitsize of its coefficients bounded by $\tau + 1 + d \lg n$. Replacing this in the previous inequality, we get $\frac{1}{m^*} \le \frac{1}{m_{\mathrm{DMM}p}}$, where

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

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 Theorem 5, and Eq. (23) to derive the following tighter bound:

$$\frac{1}{m^*} \le \frac{1}{m_{\mathrm{DMM}}} = 2^{((n+1)\tau+n+d+(n^2+3n+1)\lg d)d(d-1)^{n-1}}. \tag{46}$$

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

$$\frac{1}{m_{\mathrm{BLR}}} = 2^{2^{n+3}n\tau d^{n+1}+2^{n+5}nd^{n+1}(2nd+d\lg n+n\lg d)}, \tag{47}$$

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 $\frac{1}{m} \le \frac{1}{m_{\mathrm{BY}}}$, where

$$\frac{1}{m_{\mathrm{BY}}} = ((n+2)^2 e^{n+3})^{(n+1)(n+2)d^{n+1}} (n^n(n+1)d\,2^\tau)^{(n+1)d^n}. \tag{48}$$

The authors use the terminology *evaluation bound* for their bound. It holds when there is a zero-dimensional projection. They prove that this is always the case for the system (45).

In [22], the following bound was computed:

$$\frac{1}{m^*} \le \frac{1}{m_{\mathrm{JP}}} = 2^{(\tau+1)d^{n+1}} d^{(n+1)d^{n+1}}, \tag{49}$$

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 $|\zeta_3| \ge 2^{-b}$, $b > 0$, 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_{JP}. When $d > n$, e.g. $d = 4$ and $d = 32$, our bound is tighter than m_{JP} by an order of magnitude. All other bounds are significantly looser in all cases.*

23

bound		$(d,\tau)=(2,5)$	$(8,20)$	$(32,85)$
[2], Eq. (47)	$\lvert \lg(m_{\text{BLR}}) \rvert$	27 136	6 684 672	1 604 321 280
[6], Eq. (48)	$\lvert \lg(m_{\text{BY}}) \rvert$	1 192	74 000	4 696 811
[22], Eq. (49)	$\lvert \lg(m_{\text{JP}}) \rvert$	72	15 360	3 309 568
Eq.(44)	$\lvert \lg(m_{\text{DMM}_p}) \rvert$	87	7 457	442 447
Eq.(46)	$\lvert \lg(m_{\text{DMM}}) \rvert$	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. (47)	$\lvert \lg(m_{\text{BLR}}) \rvert$	678262344	697462344	716662344	735862344	755062344
[6], Eq. (48)	$\lvert \lg(m_{\text{BY}}) \rvert$	2740313	2780313	2820313	2860313	2900313
[22], Eq. (49)	$\lvert \lg(m_{\text{JP}}) \rvert$	242878	342878	442878	542878	642878
Eq.(44)	$\lvert \lg(m_{\text{DMM}_p}) \rvert$	151908	184308	216708	249108	281508
Eq.(46)	$\lvert \lg(m_{\text{DMM}}) \rvert$	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.

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 Theorem 5, and Equations (20) and (28) to bound the number of steps of a general pure subdivision algorithm to solve for the real roots of a well-defined polynomial system, as in (14). 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 [30, 32, 31], see also [3]. We should mention though that the bound on the number of subdivisions holds for subdivision algorithms that achieve linear convergence. They do not apply to algorithms that achieve quadratic convergence towards the roots, for example using (modifications of) Newton operators. Nevertheless, even though such fast convergent algorithms are rather well studied in the univariate case, for polynomial systems are more rare.

A straightforward derivation establishes the following bound for the number of subdivision steps of linear convergent algorithms:

Theorem 20. *Consider the polynomial system formed by the polynomials in (14). The number of calls to an oracle that a pure 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 of steps of subdivisions algorithms for real root isolation of univariate integer, not necessarily*

bound ($n = 3, \tau = 10$)		$d = 2$	$d = 4$	$d = 6$	$d = 8$	$d = 10$
[2], Eq. (47)	$|\lg(m_{\text{BLR}})|$	253993	7636226	55504131	227057704	678262344
[6], Eq. (48)	$|\lg(m_{\text{BY}})|$	4825	72898	361447	1129997	2740313
[22], Eq. (49)	$|\lg(m_{\text{JP}})|$	240	4864	27657	94208	242878
Eq.(44)	$|\lg(m_{\text{DMM}_p})|$	176	4273	21639	65372	151908
Eq.(46)	$|\lg(m_{\text{DMM}})|$	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.

square-free, polynomials is $\mathscr{O}(d^2 \lg d + d\tau)$. The bound in Davenport [14] for the univariate case is $\mathscr{O}(d^2 + d\tau)$.

It is now straightforward to derive the first complexity bound of Milne's algorithm [30] in $\mathbb{R}^2$. This aggregate separation bound is also useful in the analysis of the subdivision algorithm based on continued fractions expansion [26] for polynomial system solving.

References

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

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

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

[4] Bernstein, D., 1975. The number of roots of a system of equations. Funct. Anal. and Appl. 9, 183–185.

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

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

[7] Burr, M., Choi, S., Galehouse, B., Yap, C.K., 2008. Complete subdivision algorithms, II: Isotopic meshing of singular algebraic curves, in: Proc. 33th ACM Int'l Symp. on Symbolic & Algebraic Comp. (ISSAC), Hagenberg, Austria. pp. 87–94.

[8] Canny, J., 1990. Generalised characteristic polynomials. J. Symbolic Computation 9, 241–250.

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

[10] Canny, J.F., Emiris, I.Z., 2000. A subdivision-based algorithm for the sparse resultant. J. ACM 47, 417–451.

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

[12] D'Andrea, C., Emiris, I.Z., 2001. Computing sparse projection operators, in: Symbolic Computation: Solving Equations in Algebra, Geometry, & Engineering. AMS, Providence. volume 286 of *Contemporary Mathematics*, pp. 121–140.

[13] D'Andrea, C., Krick, T., Sombra, M., 2013. Heights of varieties in multiprojective spaces and arithmetic nullstellensatze. Annales Scientifiques de l'ENS 4, 549–627.

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

[15] Eigenwillig, A., Sharma, V., Yap, C.K., 2006. Almost tight recursion tree bounds for the Descartes method, in: Proc. 31th ACM Int'l Symp. on Symbolic & Algebraic Comp. (ISSAC), Genoa, Italy. pp. 71–78.

[16] Emiris, I.Z., 1994. Sparse Elimination and Applications in Kinematics. Ph.D. thesis. Computer Science Division, Univ. of California at Berkeley.

[17] Emiris, I.Z., Mourrain, B., Tsigaridas, E.P., 2010. The DMM bound: Multivariate (aggregate) separation bounds, in: Watt, S. (Ed.), Proc. 35th ACM Int'l Symp. on Symbolic & Algebraic Comp. (ISSAC), ACM Press, Munich, Germany. pp. 243–250.

[18] Escorcielo, P., Perrucci, D., 2017. On the davenport–mahler bound. Journal of Complexity 41, 72–81.

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

[20] Giusti, M., Heintz, J., 1993. 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.

[21] González-Vega, L., Trujillo, G., 1997. 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.

[22] Jeronimo, G., Perrucci, D., 2010. On the minimum of a positive polynomial over the standard simplex. J. Symbolic Computation 45, 434–442.

[23] Johnson, J.R., 1991. Algorithms for Polynomial Real Root Isolation. Ph.D. thesis. The Ohio State Univ.

[24] Kobel, A., Sagraloff, M., 2015. Improved complexity bounds for computing with planar algebraic curves. J. Complexity 31.

[25] Krick, T., Pardo, L., Sombra, M., 2001. Sharp estimates for the arithmetic Nullstellensatz. Duke Math. J. 109, 521–598.

[26] Mantzaflaris, A., Mourrain, B., Tsigaridas, E., 2009. Continued fraction expansion of real roots of polynomial systems, in: Proc. Symbolic-Numeric Comput., Kyoto. pp. 85–94. doi:10.1145/1577190.1577207.

[27] Mignotte, M., 1991. Mathematics for Computer algebra. Springer, New York.

[28] Mignotte, M., 1995. On the distance between the roots of a polynomial. Appl. Algebra Eng. Commun. Comput. 6, 327–332.

[29] Mignotte, M., Ştefănescu, D., 1999. Polynomials: An algorithmic approach. Springer.

[30] Milne, P.S., 1992. On the solution of a set of polynomial equations, in: Donald, B., Kapur, D., Mundy, J. (Eds.), Symbolic & Numerical Computation for AI, pp. 89–102.

[31] Pedersen, P., 1991. Counting real zeros. Ph.D. thesis. New York University.

[32] Pedersen, P., Roy, M.F., Szpirglas, A., 1993. Counting real zeros in the multivariate case, in: Eyssette, F., Galligo, A. (Eds.), Computational Algebraic Geometry. Birkhäuser, Boston. volume 109 of *Progress in Mathematics*, pp. 203–224.

[33] Rump, S., 1979. Polynomial minimum root separation. Math. of Computation 33, 327–336.

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

[35] Tsigaridas, E., Emiris, I., 2008. On the complexity of real root isolation using continued fractions. Theor. Comput. Sci. 392, 158–173.

[36] Yakoubsohn, J.C., 2005. Numerical analysis of a bisection-exclusion method to find zeros of univariate analytic functions. J. Complexity 21, 652–690.

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