Univariate real root isolation in presence of logarithms

Adam Strzebonski, Elias Tsigaridas

Univariate real root isolation in presence of logarithms

Adam Strzeboński
Wolfram Research Inc.,100 Trade Centre Drive,
Champaign, IL 61820, U.S.A.
adams@wolfram.com

Elias P. Tsigaridas
POLSYS Project, INRIA Paris-Rocquencourt
UPMC, Univ Paris 06, LIP6, FRANCE
elias.tsigaridas@inria.fr

ABSTRACT

We present algorithmic, complexity and implementation results for the problem of isolating the real roots of a univariate polynomial $B \in L[x]$, where $L = \mathbb{Q}[\lg(\alpha)]$ and α is a positive real algebraic number. Our algorithms are based on approximating the coefficients of B up to a sufficient accuracy and then solving the approximate polynomial. For this we derive worst case (aggregate) separation bounds. We also estimate the expected number of real roots when we draw the coefficients from a specific distribution and illustrate our result experimentally. A generalization to bivariate polynomial systems is also presented. We implemented the algorithm in C as part of the core library of MATHEMATICA for the case $B \in \mathbb{Z}[\lg(q)][x]$ where q is positive rational number and we demonstrate its efficiency over various data sets.

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

Keywords real root isolation, separation bounds, linear form in logarithms, algebraic numbers

General Terms Algorithms, Experimentation, Theory

1. INTRODUCTION

We consider the problem of isolating the real roots of a univariate polynomial the coefficients of which are polynomials in the logarithm of a positive real algebraic number. We consider two variants of the problem. In the first variant the argument of the logarithm is a positive rational number. In the second the argument is a bivariate homogeneous polynomial evaluated at two real algebraic numbers. The reader can refer to the end of the section for a detailed presentation of the notation that we use. The first problem that we consider is the following:

Problem 1. *Consider the following square-free polynomial* $B_q = \sum_{i=0}^{d} b_i\, x^i$, *where* $b_i = \sum_{j=0}^{\nu} b_{i,j}\, (\lg(q))^j$, $b_{i,j} \in \mathbb{Z}$, $q \in \mathbb{Q}_+$, $\mathcal{L}(b_{i,j}) \leq \tau$, *and* $\mathcal{L}(q) \leq \tau$. *What is the bit complexity of isolating the real roots of* B_q*?*

The problem of isolating the real roots of a univariate polynomial is a well studied problem. However, most of the results focus on polynomials with rationals or algebraic numbers as coefficients. We are not aware of any complexity results that consider polynomials with transcendental numbers as coefficients.

Nevertheless, our approach for tackling the problem is based on approximating the coefficients of B_q in Problem 1 up to a sufficient precision and so it is closely related to univariate real solving algorithms that are numerical [27, 22], see also [24, 14], or are based on the bitstream model, e.g. [18, 11, 25]. For a detailed treatment of numerical solvers we refer the reader to [17, Chapter 15]. Our problem is similar to the problem of solving polynomials with coefficients in an extension field, [15, 29, 28], see also [7, 32, 31, 16] and references therein. We also refer to the recent work of Bates and Sottile [4] on Khovanskii–Rolle continuation algorithm that exploits logarithms of polynomial expressions. Our work could also be seen as a first step for understanding the ingredients needed for analyzing the complexity of this algorithm.

Our analysis is based on the result of Mignotte and Waldschmidt (Thm. 3) that provides effective lower bounds for a homogeneous linear form in two logarithms. We combine this result with univariate and multivariate separation bounds of polynomials and polynomial systems. The idea is to approximate the coefficients of B_q up to a sufficient precision and then isolate the real roots of the approximate polynomial. The precision is such that the number of the real roots remains the same and the isolated intervals of the approximate polynomial are also isolating intervals for the real roots of B_q. First we have to estimate what is exactly "sufficient accuracy". We treat the logarithm as a parameter. The separation bound of B_q turns out to be a univariate polynomial in this parameter. We estimate a lower bound on this evaluation by proving that it depends only on the closest root and the separation bound of the polynomial (Lemma 2) and combining it with Thm. 3. This approach saves us a factor compared to the straightforward approach of factoring the polynomial in linear factors and bounding the separation bound using Thm. 3 directly.

This approach turns out to be applicable for tackling a more general problem, Problem 2, where the argument of the logarithm is homogeneous bivariate polynomial evaluated at two real algebraic numbers. In this case we need to combine Thm. 3 with multivariate separation bounds. Problem 1 is

a simplified version of Problem 2, but its resolution depends on more elementary algebraic techniques. For this and for making the presentation easier for the reader we present both approaches.

We also estimate the expected number of real roots of B_q in the case where all the polynomials b_i have the same degree ν and their coefficients, $b_{i,j}$, are Gaussian random variables with mean zero and variance $\binom{d}{i}$. In this case the expected number of real roots is $\sqrt{d}$. This result agrees with our experiments. We implemented our algorithms in C as part of the core library of MATHEMATICA for the case $B \in \mathbb{Z}[\lg(q)][x]$ where q is positive rational number and we demonstrate its efficiency over various data sets. Our results support experimentally the $\sqrt{d}$ bound for the number of roots of random polynomials. Finally, we generalize our bounds to handle bivariate polynomial systems.

The rest of the paper is structured as follows. First we introduce our notation and in Section 2 we present the main tools that we will use throughout the paper. In Section 3 we present an algorithm for tackling Problem 1 as well as its complexity analysis, experimental results and the bound for the expected number of real roots. We present a more general version of Problem 1 in Section 4 and the extension to bivariate polynomial systems in Section 5.

The proofs of the various lemmata, as well as simplified versions of Problem 2 are presented in the Appendix.

Notation. In what follows $\mathcal{O}_B$, resp. $\mathcal{O}$, means bit, resp. arithmetic, complexity and the $\widetilde{\mathcal{O}}_B$, resp. $\widetilde{\mathcal{O}}$, notation means that we are ignoring logarithmic factors. For a polynomial $A = \sum_{i=0}^{d} a_i\, x^i \in \mathbb{Z}[x]$, $\mathsf{deg}(A) = d$ denotes its degree and $\mathcal{L}(A) = \tau$ the maximum bitsize of its coefficients, including a bit for the sign. For $a \in \mathbb{Q}$, $\mathcal{L}(a) \geq 1$ is the maximum bitsize of the numerator and the denominator. We write $\Delta_\alpha(A)$ to denote the minimum distance between a root α of a polynomial A and any other root. $\Delta(A) = \min_\alpha \Delta_\alpha(A)$ is the *separation bound*, that is the minimum distance between all the roots of A, and $\Sigma(A) = -\sum_{i=1}^{n} \lg \Delta_i(A)$. The Mahler measure of A is $\mathcal{M}(A) = a_d \prod_{|\alpha|\geq 1} |\alpha|$, where α runs through the complex roots of A. If $A \in \overline{\mathbb{Z}}[x]$ and $\mathcal{L}(A) = \tau$, then $\mathcal{M}(A) \leq \|A\|_2 \leq \sqrt{d+1}\|A\|_\infty = 2^\tau\sqrt{d+1}$. We denote by $\lg(\cdot)$, resp. $\ln(\cdot)$, the logarithm with base 2, resp. e. Let $L_q = \lg(q)$, where q is a positive rational number, and $L_H = \lg A(\gamma_1, \gamma_2)$, where $\gamma_{\{1,2\}}$ are real algebraic numbers and A is a bivariate homogeneous polynomial.

2. PRELIMINARIES

Real algebraic numbers are the real roots of univariate polynomials with integer coefficients; we denote their set by $\mathbb{R}_{\mathsf{alg}}$. For representing them we use the so-called *isolating interval representation*. If $\alpha \in \mathbb{R}_{\mathsf{alg}}$ then the representation consists of a square-free polynomial with integer coefficients, $A \in \mathbb{Z}[x]$, that has α as a real root, and an isolating interval with rational endpoints, $\mathcal{I} = [\mathsf{a}_1, \mathsf{a}_2]$, that contains α and no other root of the polynomial. We write $\alpha \cong (A, \mathcal{I})$. Such a representation could be also used for the real roots of polynomials with real number coefficients, provided that there is an algorithm for computing them.

The following proposition provides upper and aggregate bounds for the roots of a univariate polynomial. Various versions of the proposition could be found in e.g. [9, 8, 30]. We should mention that the constants that appear are not optimal. For multivariate bounds we refer to [13].

Proposition 1. *Let $f = \sum_{i=0}^{d} a_i x^i \in \mathbb{C}[x]$ be a square-free univariate polynomial of degree d such that $a_d a_0 \neq 0$. Let Ω be any set of k pairs of indices (i,j) such that $1 \leq i < j \leq d$, let the complex roots of A be $0 < |\gamma_1| \leq |\gamma_2| \leq \cdots \leq |\gamma_d|$, and let $\mathsf{disc}(f)$ be the discriminant of f. It holds*

$$\frac{|a_0|}{\|f\|_2} \leq |\gamma_i| \leq \frac{\|f\|_2}{|a_d|} \ , \tag{1}$$

$$\prod_{(i,j)\in\Omega} |\gamma_i - \gamma_j| \geq 2^{k-d-\frac{d(d-1)}{2}} |a_0|^k \mathcal{M}(f)^{1-d-k} \sqrt{|\mathsf{disc}(f)|} \geq 2^{k-d-\frac{d(d-1)}{2}} |a_0|^k \|f\|_2^{1-d-k} \sqrt{|\mathsf{disc}(f)|} \ . \tag{2}$$

If $f \in \mathbb{Z}[x]$ and the maximum coefficient bitsize is τ then

$$2^{-\tau-1} \leq |\gamma| \leq 2^{\tau+1} \ , \tag{3}$$

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

The following lemma provides a lower bound on the evaluation of a polynomial that depends on the closest root and on the aggregate separation bound of the polynomial.

Lemma 2. *Let $L \in \mathbb{C}$ and γ_1 the root of the square-free polynomial f that is closest to L. Then*

$$|f(L)| \geq |a_d|^7 |L-\gamma_1|^6 \mathcal{M}(f)^{-6} 2^{\lg \prod_i \Delta_i - 6} \ .$$

Proof: First we claim that there are at most six roots of f such that $|L-\gamma_i| \leq |\gamma_i - \gamma_{c_i}| = \Delta_j$, where γ_{c_i} is a the root closest to γ_i.

To prove the claim we proceed as follows: Suppose there were 7 roots such that $|L-\gamma_i| \leq |\gamma_i - \gamma_{c_i}|$. Number them so that $\mathsf{Arg}(\gamma_1 - L) \leq \mathsf{Arg}(\gamma_2 - L) \leq \cdots \leq \mathsf{Arg}(\gamma_7 - L)$, where $0 \leq \mathsf{Arg}(z) < 2\pi$. Then there are γ_i and γ_{i+1} such that $\mathsf{Arg}(\gamma_{i+1} - L) - \mathsf{Arg}(\gamma_i - L) < \pi/3$. Consider the triangle with vertices $L, \gamma_i, \gamma_{i+1}$. The measure of the angle at the vertex L is $< \pi/3$, hence one of the other angles, say the angle at the vertex γ_{i+1}, is greater than the angle at the vertex L. By the law of sines, the side facing a larger angle is longer, hence $|\gamma_i - L| > |\gamma_{i+1} - \gamma_i| \geq |\gamma_i - \gamma_{c_i}|$ and we get a contradiction.

Wlog let them be the first six ones. Then

$$\begin{aligned} |A(L)| &= |a_d| \prod_{i=1}^{d} |L-\gamma_i| = |a_d| \prod_{i=1}^{6} |L-\gamma_i| \prod_{j=7}^{d} |L-\gamma_j| \\ &\geq |a_d| |L-\gamma_1|^6 \frac{1}{\prod_{i=1}^{6} \Delta_i} \prod_{j=1}^{d} \Delta_j \\ &\geq |a_d|^7 |L-\gamma_1|^6 \mathcal{M}(f)^{-6} 2^{\lg \prod_i \Delta_i - 6} \ . \end{aligned}$$

For the last inequality we use $\Delta_i \leq 2\mathcal{M}(f)/|a_d|$, that in turn relies on $\Delta_i = |\gamma_i - \gamma_{c_i}| \leq |\gamma_i| + |\gamma_{c_i}| \leq 2\mathcal{M}(f)/|a_d|$. □

In the sequel we will use the previous lemma in conjunction with Thm. 3 and almost always L will be the logarithm of an algebraic number. It might be the case the L is a root of f and thus the evaluation $f(L)$ is zero. However, we omit this case as it can be detected rather easily and does not affect in any case the complexity of the algorithms that we consider.

We will also need the following theorem, due to Mignotte and Waldschmidt [21], that provides an effective lower bound on a homogeneous linear form with two logarithms of (real)

algebraic numbers with algebraic coefficients. This result generalizes a result by Gel'fond. A generalization that handles general linear forms is due to Baker, e.g. [3].

Theorem 3. *[21] Let $\Lambda = \beta\ln(\alpha_1) - \ln(\alpha_2)$, where $\beta, \alpha_1, \alpha_2$ are three non-zero algebraic numbers of degrees D_0, D_1, D_2, respectively, and of heights B, A_1, A_2. If D is the degree of $\mathbb{Q}$ over the field $\mathbb{Q}(\beta, \alpha_1, \alpha_2)$, and $T = \ln(B) + \ln\ln(A_1) + \ln\ln(A_2) + \ln(D)$, then $|\Lambda| > \exp(-5\cdot 10^{10}\cdot D^4\cdot\ln(A_1)\cdot\ln(A_2)\cdot T^2)$.*

3. AN ALGORITHM FOR B_Q

In Problem 1 we assume that the degree of all polynomials b_i is the same, ν. However, the bounds we present hold even if this is not the case and ν is the maximum of the degrees of b_i. The proof of following lemma is a simplification of the arguments in [2].

Lemma 4. *Let $q = \frac{q_1}{q_2}$ be a positive rational number different from 0 and 1, such that $1 \le q_1, q_2 \le 2^\tau$, where τ is a positive integer. Then $2^{-2\tau-1} \le |\lg(q)| \le \tau$.*

Proof: The right inequality follows from $1 \le q_1 \le 2^\tau$ and $1 \le q_2 \le 2^\tau$. From these bounds we can also deduce that $|q-1| \ge 2^{-\tau}$.

For every complex number z it holds $|e^z - 1| \le |z|e^{|z|}$. So

$$|q-1| = |e^{\ln(q)} - 1| \le \frac{|\lg(q)|}{\ln(2)}\, e^{|\ln(q)|} \ ,$$

and thus $|\lg(q)| \ge 2^{-2\tau-1}$. □

3.1 Separation bounds for B_q

We compute various bounds on the roots of B_q based on the first inequalities of Prop. 1. For this we need to compute a lower bound for $|\mathsf{disc}(B_q)|$ and an upper bound for $\|B_q\|_2$. Recall that $L_q = \lg\frac{q_1}{q_2}$, where q_1, q_2 are positive integers such that $\frac{q_1}{q_2}$ is different from 0 and 1 and $1 \le q_1, q_2 \le 2^\tau$.

First we compute bounds on the coefficients of B_q.

Lemma 5. *Let b_i be as in Problem 1, then $\exp(-10^{13}\,\nu^4\,\tau\,(\tau + \ln\tau + \ln\nu)^2) \le |b_i(L_q)| \le 2^\tau\,\tau^{\nu+1}$, or $2^{-\widetilde{\mathcal{O}}(\nu^4\tau^3)} \le |b_i(L_q)| \le 2^{\widetilde{\mathcal{O}}(\nu+\tau)}$.*

Proof: To bound b_i we proceed as follows:

$$|b_i(L_q)| = |\sum_{j=0}^{\nu} b_{i,j} L_q^j| \le 2^\tau \sum_{j=0}^{\nu} |L_q|^j \le 2^\tau \sum_{j=0}^{\nu} \tau^j$$
$$\le 2^\tau \frac{\tau^{\nu+1}-1}{\tau-1} \le 2^\tau\,\tau^{\nu+1} \ .$$

To compute a lower bound for $|b_i(L_q)|$ we assume that $\beta_{i,1}$ is the root closest to L_q and we apply Lemma 2, ie

$$|b_i(L_q)| > |b_{i,\nu}|^7\,|L_q - \beta_{i,1}|^6\,\mathcal{M}(b_i)^{-6}\,2^{\lg\prod_j \Delta_j(b_i) - 6} \ .$$

It holds $|b_{i,\nu}| \ge 1$; Theorem 3 implies that

$$|L_q - \beta_{i,1}| \ge \exp(-5\cdot 10^{10}\,\nu^4\,\tau\,(\tau + \ln\tau + \ln\nu)^2) \ ,$$

and $\mathcal{M}(b_i) \le (\nu+1)\|b_i\|_\infty \le 2^{\tau + \lg\nu + 1}$. Finally, using Proposition 1 we have $\lg\prod_j \Delta_j(b_i) \ge -3\nu^2 - 3\nu\tau - 4\nu\lg\nu$. Combining all the inequalities we get

$$|b_i(L_q)| \ge \exp(-10^{13}\,\nu^4\,\tau\,(\tau + \ln\tau + \ln\nu)^2) \ ,$$

$$\text{or} \quad |b_i(L_q)| \ge \exp(-\widetilde{\mathcal{O}}(\nu^4\tau^3)) \ ,$$

which concludes the proof. □

The previous lemma allows us to bound $\|B_q\|_2$. It holds $\|B_q\|_2^2 = \sum_{i=0}^{d} |b_i(L_q)|^2 \le d^2\,2^{2\tau+2}\,\tau^{2\nu+2}$, and so

$$\|B_q\|_2 \le d\,2^{\tau+1}\,\tau^{\nu+1} \ . \tag{5}$$

We bound the discriminant as follows:

Lemma 6. *Let B_q be as in Prob. 1, then $2^{-\widetilde{\mathcal{O}}(d^7\nu^4\tau^3)} \le |\mathsf{disc}(B_q)| \le 2^{\widetilde{\mathcal{O}}(d\nu + d\tau + \nu^4\tau^3)}$.*

Proof: We consider B_q as a bivariate polynomial in $\mathbb{Z}[L_q, x]$. To bound $|\mathsf{disc}(B_q)|$ we consider the identity

$$|\mathsf{disc}(B_q)| = \left|\frac{1}{b_d(L_q)}\mathtt{res}_x(B_q(L_q,x), \partial B_q(L_q,x)/\partial x)\right|$$
$$= \left|\frac{1}{b_d(L_q)} R_B(L_q)\right| \ , \tag{6}$$

where the resultant, $R_B \in \mathbb{Z}[L_q]$, can be computed as the determinant of the Sylvester matrix of $B_q(L_q, x)$ and $\partial B_q(L_q,x)/\partial x$, evaluated at L_q.

The Sylvester matrix is of size $(2d-1)\times(2d-1)$, the elements of which belong to $\mathbb{Z}[L_q]$. The determinant consists of $(2d-1)!$ terms.

Each term is a product of $d-1$ polynomials in L_q of degree at most ν and bitsize at most τ, times a product of d polynomials in L_q of degree at most $\nu-1$ and bitsize at most $\tau + \lg d$. The first product results a polynomial of degree $(d-1)\nu$ and bitsize $(d-1)\tau + (d-1)\lg d$. The second product results polynomials of degree $d(\nu-1)$ and bitsize $d\tau + d\lg(d(\nu-1))$. Thus, any term in the determinant expansion is a polynomial in L_q of degree less than $2d\nu$ and bitsize at most $2d\tau + 6d\lg(d\nu)$. The determinant itself, is a polynomial in L_q of degree at most $2d\nu$ and of bitsize $2d\tau + 10d\lg(d\nu)$.

We compute an upper bound of $|R_B(L_q)|$ as follows:

$$|R_B(L_q)| \le 2^{2d\tau + 10d\lg(d\nu)} \sum_{k=0}^{2d\nu} |L_q|^k \le 2^{2d\tau + 10d\lg(d\nu)}\,\tau^{2d\nu+1} \ .$$

For the lower bound, we consider R_B as a univariate polynomial, say in z, and let r be its leading coefficient. By ρ_k we denote its roots. If apply Lemma 2, by assuming that ρ_1 is closest root to L_q, then

$$|R_B(L_q)| > |r|^7\,|L_q - \rho_1|^6\,\mathcal{M}(R_B)^{-6}\,2^{\lg\prod_k \Delta_k(R_B) - 6} \ .$$

It holds $|r| \ge 1$, $\mathcal{M}(R_B) \le 2^{\widetilde{\mathcal{O}}(d\tau)}$, and $-\lg\prod_k \Delta_k(R_B) = \widetilde{\mathcal{O}}(d^2\nu^2 + d^2\nu\tau)$ We also use Theorem 3

$$|L_q - \rho_1| \ge \exp(-\widetilde{\mathcal{O}}(d^7\nu^4\tau^3)) \ .$$

By combining all the inequalities we get

$$|R_B(L_q)| \ge \exp(-\widetilde{\mathcal{O}}(d^7\nu^4\tau^3)) \ .$$

Combining Eq. (6) with the previous inequality and Lemma 5 we get

$$2^{-\widetilde{\mathcal{O}}(d^7\nu^4\tau^3)} \le |\mathsf{disc}(B_q)| \le 2^{\widetilde{\mathcal{O}}(d\nu + d\tau + \nu^4\tau^3)} \ .$$

which concludes the proof. □

We combine Lemma 5, Lemma 6 and Eq. (5) with Proposition 1 to derive the following separation bounds for B_q.

Lemma 7. *Let B_q be as in Problem 1 and let β_j be its roots. Then*

$$2^{-\widetilde{\mathcal{O}}(\nu^4\tau^3)} \leq |\beta_j| \leq 2^{\widetilde{\mathcal{O}}(\nu^4\tau^3)} \ ,$$

$$\Sigma(B_q) = -\lg \prod_{(i,j)\in\Omega} |\beta_i - \beta_j| \leq \widetilde{\mathcal{O}}(d^7\nu^4\tau^3) \ .$$

The previous bounds hold if instead of $\lg(\cdot) = \log_2(\cdot)$ we use any rational as a base of the logarithm. However if we use $\ln(\cdot)$ then it is not possible to use Thm. 3 anymore. In this case we should use the general bound of Baker for inhomogeneous linear forms in logarithms of algebraic numbers [3].

3.2 Isolating the real roots of B_q

The main idea behind the algorithm for isolating the real roots of B_q is to approximate its coefficients up to a specified accuracy so that the the resulting approximate polynomial, $\widetilde{B}_q$, has real roots that are close to the real roots of B_q. We isolate the real roots of $\widetilde{B}_q$ and the approximation is such that guarantees that the resulting isolating intervals are also isolating intervals for the real roots of B_q.

As stated in Problem 1, the polynomials $b_i \in \mathbb{Z}[y]$ have coefficients of maximum bitsize bounded by τ and degree bounded by ν.

We need to approximate the coefficients of B_q up to accuracy $\mathcal{O}(\Sigma(B_q) + d\,\sigma)$ [25], see also [27, 22, 18], where $\left|\frac{b_i(L_q)}{b_d(L_q)}\right| \leq 2^{\sigma}$ and $\Sigma(B_q) = -\sum_{i=1}^{n} \lg(\Delta_i(B_q))$. In this way the number of real roots of the approximate polynomial is the same as the number of real roots of B_q. Moreover, the isolating intervals we compute for the approximate polynomial are also isolating intervals for the roots of B_q.

Consequently the complexity of isolating the real roots would be $\widetilde{\mathcal{O}}_B(d^2(\Sigma(B_q) + d\,\sigma))$ [22, 19] or $\widetilde{\mathcal{O}}_B(d^3(\Sigma(B_q) + d\,\sigma))$ [27, 26], depending on the algorithm that we use for approximating the real roots.

We assume that first we compute a rational approximation of the input polynomial (up to the necessary precision) and then we apply the algorithms for isolating the roots directly to the rational polynomial. We can also use a recent approach [19] that modifies Pan's algorithm [22] and makes it adaptive with the same complexity estimate.

Lemma 7 indicates that

$$\Sigma(B_q) = \widetilde{\mathcal{O}}(d^7\nu^4\tau^3) \ . \tag{7}$$

To bound σ we use Lemma 5 and so $\left|\frac{b_i(L_q)}{b_d(L_q)}\right| \leq 2^{\widetilde{\mathcal{O}}(\nu^4\tau^3)}$, for all i. Hence,

$$\sigma = \widetilde{\mathcal{O}}(\nu^4\tau^3) \ , \tag{8}$$

and thus we should approximate the coefficients of B_q up to accuracy

$$\widetilde{\mathcal{O}}_B(\Sigma(B_q) + d\,\sigma) = \widetilde{\mathcal{O}}(d^7\nu^4\tau^3) \ .$$

We can isolate the real roots in $\widetilde{\mathcal{O}}(d^9\nu^4\tau^3)$ [22] or $\widetilde{\mathcal{O}}(d^{10}\nu^4\tau^3)$ [27, 26].

It remains to estimate the cost of computing successive approximations of $b_i(L_q)/b_d(L_q)$ up to accuracy of $\mathcal{O}(\Sigma(B_q) + d\sigma)$ bits after the binary point. Since $|b_i(L_q)/b_d(L_q)| \leq 2^{\sigma}$, to approximate each fraction, for $0 \leq i \leq d-1$, to accuracy ℓ, it is sufficient to approximate $b_i(L_q)$, for $0 \leq i \leq d$, up to precision $\mathcal{O}(\ell + \sigma)$. Hence, the algorithm requires approximation of $b_i(L_q)$, for $0 \leq i \leq d$, to precision $\mathcal{O}(\Sigma(B_q) + d\sigma) = \widetilde{\mathcal{O}}(d^7\nu^4\tau^3)$. By Lemma 5, $|b_i(L_q)| \geq 2^{-\widetilde{\mathcal{O}}(\nu^4\tau^3)}$, and therefore it is sufficient to approximate $b_i(L_q)$ to accuracy $\widetilde{\mathcal{O}}(d^7\nu^4\tau^3)$.

$d \setminus \nu$	10	20	50	100	200	500	1000
10	0.006	0.011	0.027	0.060	0.122	0.358	0.857
20	0.015	0.025	0.058	0.110	0.235	0.678	1.53
50	0.042	0.068	0.142	0.272	0.581	1.61	3.56
100	0.116	0.164	0.339	0.640	1.19	3.14	7.65
200	0.496	0.516	0.900	1.65	2.76	6.41	16.7
500	3.43	4.53	5.30	6.52	10.4	21.5	54.6
1000	25.5	23.1	27.7	36.8	45.7	79.9	173

Table 1. Uniformly distributed coefficients, $\tau = 10$

Approximation of $L_q = \lg(q)$ to accuracy of $t > 0$ bits yields an approximation of $b_{i,j}L_q^j$ to accuracy of at least

$$t - \lg|b_{i,j}| - \lg(j) - (j-1)\lg|2L_q| \geq t - \tau - \lg(\nu) - \nu(\lg(\tau)+1)$$

bits and an approximation of $b_i(L_q)$ to accuracy of at least $t - \tau - 2\lg(\nu) - \nu(\lg(\tau)+1)$ bits. Therefore the algorithm requires approximation of $\lg(q)$ to accuracy of $t = \widetilde{\mathcal{O}}(d^7\nu^4\tau^3)$ bits.

The cost of approximating $\lg(q)$ up to t bits is quasi-linear $\widetilde{\mathcal{O}}_B(t)$ [5], see also [6] and references therein. In our case the cost is $\widetilde{\mathcal{O}}_B(d^7\nu^4\tau^3)$. This bound is dominated by the complexity of real solving.

Theorem 8. *The Boolean complexity of isolating the real roots of B_q of Problem 1 is $\widetilde{\mathcal{O}}(d^9\nu^4\tau^3)$ or $\widetilde{\mathcal{O}}(d^{10}\nu^4\tau^3)$.*

3.3 Experiments

We present experimental results for an implementation of the algorithm isolating roots of the polynomial in Problem 1. The algorithm has been implemented in C as a part of the *Mathematica* system. We have implemented the modified version of Descartes' algorithm due to Sagraloff [25], that applies to polynomials with bitstream coefficients, see also [11, 18], and we adopted our bounds to it. The theoretical complexity of the algorithm is worse by factor than the one that we used in the previous section, but its implementation is easier.

The experiments have been run on a 64-bit Linux virtual machine with a 3 GHz Intel Core i7 processor and 6 GB of RAM. The timings are in given seconds.

Example 9. *(Random polynomials with uniformly distributed coefficients) For given values of d, ν and τ each instance (polynomial) was generated by selecting integer coefficients $b_{i,j}$ randomly w.r.t. the uniform distribution in $\mathbb{Z}\cap[-2^{\tau-1}, 2^{\tau-1}]$ and a positive rational number $q \neq 1$ with $L(q) \leq \tau$. Each timing is an average for 10 randomly generated problems. The results are in Table 1 and 2.*

Applying a least-squares fit to the experimental data yields proportionality of the computation time to $d^{1.4}\nu^{0.8}$. There is very little dependence of the computation time on the value of τ (see also the next section).

Example 10. *(Random polynomials with Gaussian distribution of coefficients) For given values of d and ν each problem was generated by setting $q = 3$ and selecting coefficients $b_{i,j}$ as nearest integers to real numbers selected randomly w.r.t. the Gaussian distribution with mean 0 and variance*

$d \setminus \nu$	10	20	50	100	200	500	1000
10	0.006	0.011	0.028	0.054	0.120	0.362	0.883
20	0.015	0.026	0.060	0.116	0.237	0.809	1.65
50	0.045	0.072	0.157	0.299	0.671	1.74	3.98
100	0.136	0.200	0.356	0.759	1.37	3.41	7.78
200	0.442	0.605	0.985	1.62	2.84	7.25	17.9
500	4.30	4.48	5.95	7.55	12.6	25.4	60.1
1000	20.5	30.4	30.4	34.8	44.7	81.4	183

Table 2. Uniformly distributed coefficients, $\tau = 1000$

$d \setminus \nu$	10	20	50	100	200	500	1000
10	0.004	0.005	0.013	0.028	0.072	0.290	0.992
	3.20	3.06	3.28	3.14	3.30	3.10	3.22
20	0.013	0.022	0.050	0.109	0.239	0.902	2.07
	4.40	4.18	4.56	4.48	4.66	4.28	4.14
50	0.080	0.118	0.191	0.406	0.794	2.34	5.33
	7.46	7.22	6.74	6.96	7.12	7.06	6.86
100	0.309	0.384	0.596	0.477	1.06	2.03	5.07
	9.92	10.12	9.98	10.12	9.90	10.44	10.02
200	1.75	2.19	2.49	4.10	6.56	9.42	18.8
	13.98	14.02	13.78	14.36	13.98	14.24	13.92
500	32.4	32.9	34.4	35.9	39.9	51.7	88.5
	22.92	22.50	22.46	22.10	21.92	22.72	22.80

Table 3. Gaussian distribution of coefficients

$\binom{d}{i}$). *Each result is an average for* 100 *randomly generated problems. For each value* d *and* ν *the upper section gives the computation time and the lower section gives the number of real roots. The results are in Table 3.*

Applying a least-squares fit to the experimental data yields proportionality of the computation time to $d^{1.7}\nu^{0.8}$. The average number of roots is, as expected, close to $\sqrt{d}$.

3.4 (Unsuccessful) Lower bounds

An obvious candidate polynomial for providing (matching) lower bounds for Lemma 7 is (a variant of) Mignotte polynomials [20]. Let $b(L_q) = \sum_{i=0}^{\nu} b_i \lg(q)^i$ where $q = b_i = 2^\tau$ and $B = x^d - 2(2^\tau b(L_q)x - 1)^2$. Now B has two of its real roots very close to $(2^\tau b(L_q))^{-1}$. The separation bound of B, $\Delta(B)$, is

$$\Delta(B) \geq 2\left(2^{2\tau}\frac{\tau^{\nu+1}-1}{\tau-1}\right)^{-(d+2)/2} = 2^{-\widetilde{\mathcal{O}}(d\tau+d\nu)} \ ,$$

which is not close to $2^{\widetilde{\mathcal{O}}(d^8\nu^5\tau^3)}$ of Lemma 7.

The dominating terms of the separation bounds that appear in Lemma 7 come from the lower bound of the discriminant (Lemma 6). The discriminant of B_q w.r.t. x is a univariate polynomial in L_q. A polynomial B_q with roots that match the separation bound of Lemma 7 should have discriminant that is a univariate polynomial with very small separation bound, for example a Mignotte polynomial. Currently, we are not aware of any technique that might be able to solve these kind of "reverse" problems.

Our unsuccessful attempt for providing lower bounds triggers the question of estimating the average behavior of the separation bounds. For this the first step is to estimate the expected number of real roots of B_q, when its coefficients are random variables.

Proposition 11. *[10] Let* $v(t) = (f_o(t), \ldots, f_n(t))^\top$ *be a vector of differentiable functions and* $c_0, \ldots, c_n$ *elements of a multivariate normal distribution with zero mean and covariance matrix* C*. The expected number of real zeros on an interval (or a measurable set)* I *of the equation* $c_0 f_0(t) + \cdots + c_n f_n(t) = 0$*, is*

$$\int_I \frac{1}{\pi}\|\boldsymbol{w}'(t)\|dt, \ \boldsymbol{w} = w(t)/\|w(t)\|.$$

where $w(t) = C^{1/2}v(t)$*. In logarithmic derivative notation, this is*

$$\frac{1}{\pi}\int_I \sqrt{\frac{\partial^2}{\partial x\,\partial y}\log\left(v(x)^\top C v(y)\right)|_{x=y=t}}dt.$$

We fix a logarithm L. For example $L = \lg(q)$ for a (fixed) positive rational number q, different from 0 and 1. Consider the polynomials $b_i = \sum_{j=0}^{\nu} b_{i,j}L^j$ where each of $b_{i,j}$ is a Gaussian random variable with mean zero and variance $\binom{d}{i}$. We denote this by $b_{i,j} \sim N(0, \binom{d}{i})$. Then

$$b_i \sim N(0, \binom{d}{i}\sum_{j=0}^{\nu} L^{2j}) = N(0, \binom{d}{i}\ell) \ .$$

In our case $v(x)^\top C v(y) = \ell(1 + x\,y)^d$, and the integral of Proposition 11 yields

$$\frac{1}{\pi}\int_{-\infty}^{\infty}\sqrt{\frac{\partial^2}{\partial x\,\partial y}\log \ell(1+x\,y)^d|_{x=y=t}}\,dt = \sqrt{d} \ .$$

This leads to the following lemma:

Lemma 12. *Let* B_q *as in Prob. 1 with a fixed* q*. Let all* b_i *have the same degree* ν *and* $b_{i,j} \sim N(0, \binom{d}{i})$*. Then the expected number of real roots of* B_q *is* $\sqrt{d}$*.*

Following the analysis of [12] the previous lemma allows to compute the distribution of the real roots and eventually to estimate the expected separation bound; which is $\mathrm{E}[\Delta(B_q)] = \widetilde{\mathcal{O}}(d)$ (for the aforementioned distribution of the coefficients). This is far from the worst case proved in Lemma 7 but agrees with the excellent running times of our implementation in Section 3.3. The bigger the (actual) separation bound, the less bits we need to isolate the real roots, and so the faster the subdivision algorithms perform.

4. A GENERALIZATION

We present a generalization of Problem 1 where the argument of the logarithm is a homogeneous bivariate polynomial evaluated at two real algebraic numbers. In the appendix we present the cases where the argument of the logarithm is a real algebraic number or a univariate polynomial evaluated at a real algebraic number. Even though these are simplified version of Problem 2, the algebraic techniques needed for the bounds are much simpler and the derived bounds are much simpler. As in the case where the argument is a rational number, we rely on Thm. 3 for computing the various upper and lower bounds.

The precise problem definition is as follows:

Problem 2. *Consider the square-free* $B_H = \sum_{i=0}^{d} b_i\,x^i$*, where* $b_i = \sum_{j=0}^{\nu} b_{i,j}\,(\lg(A(\gamma_1,\gamma_2)))^j$*,* $b_{i,j} \in \mathbb{Z}$*,* $\mathcal{L}(b_{i,j}) \leq \tau$*,* $A \in \mathbb{Z}[y_1, y_2]$ *is a homogeneous polynomial of degree* m *and* $\mathcal{L}(A) =$

τ and γ_1, resp. γ_2, is a real root of a polynomial $C_1 \in \mathbb{Z}[y]$, resp. $C_2 \in \mathbb{Z}[y]$, which is of degree n and $\mathcal{L}\left(C_{\{1,2\}}\right) = \tau$. We assume $A(\gamma_1, \gamma) > 0$ and $A(\gamma_1, \gamma_2) \neq 1$. What is the Boolean complexity of isolating the real roots of B_H?

We should warn the reader that the constants in the various bounds in the sequel are not the best possible.

Lemma 13. *Let $A \in \mathbb{Z}[y_1, y_2]$ be a homogeneous polynomial of degree m and $\mathcal{L}(A) = \tau$ and γ_1, resp. γ_2, be the positive real root of a polynomial $C_1 \in \mathbb{Z}[y]$, resp. $C_2 \in \mathbb{Z}[y]$, that is of degree n and $\mathcal{L}(C) = \tau$. Then $2^{-3n^2\tau - 5n^2 \lg(mn)} \leq |\lg A(\gamma_1, \gamma_2)| \leq 4m\tau$.*

Proof: Assume for the moment that we know positive integers t and T such that $|A(\gamma_1, \gamma_2)| \leq 2^T$ and $|A(\gamma_1, \gamma_2) - 1| \geq 2^{-t}$. Then from the inequality $|e^z - 1| \leq |z|e^{|z|}$ we deduce

$$\begin{gathered} |A(\gamma_1, \gamma_2) - 1| \leq |\ln A(\gamma_1, \gamma_2)| e^{|\ln A(\gamma_1, \gamma_2)|} \Rightarrow \\ |A(\gamma_1, \gamma_2) - 1| \leq \tfrac{|\lg A(\gamma_1, \gamma_2)|}{\ln(2)} |A(\gamma_1, \gamma_2)| \Rightarrow \\ 2^{-t-1} \leq |A(\gamma_1, \gamma_2) - 1|/2 \leq |\lg A(\gamma_1, \gamma_2)|\, 2^T \Rightarrow \\ 2^{-t-T-1} \leq |\lg A(\gamma_1, \gamma_2)| \ . \end{gathered}$$

It remains to specify t and T. For the real algebraic numbers γ_1 and γ_2 it holds

$$2^{-\tau} \leq |\gamma_{\{1,2\}}| \leq 2^{\tau}.$$

We bound T as follows:

$$|A(\gamma_1, \gamma_2)| \leq |\sum_{i=0}^{m} a_i \gamma_1^i \gamma_2^{m-i}| \leq \sum_{i=0}^{m} 2^{\tau}\, 2^{m\,\tau} \ ,$$

and so

$$|\lg A(\gamma_1, \gamma_2)| \leq (m+1)\tau + \lg(m+1) = T \ .$$

We choose $T = 4m\tau = \mathcal{O}(m\tau)$ to simplify the calculations.

To compute a bound for t we consider the polynomial $\bar{A}(y_1, y_2) = A(y_1, y_2) - 1$ and the following polynomial system:

$$\begin{cases} F_1 = z - [A(y_1, y_2) - 1] & = 0 \\ F_2 = C_1(y_1) & = 0 \\ F_3 = C_2(y_2) & = 0 \end{cases}$$

We will use a similar system in the sequel so we present various quantities that are related to it. For further details we refer the reader to [13].

A lower bound on z provides us a bound for t. To compute a bound for z we use the `DMM` bound from [13, Thm.3].

Let $\mathcal{D}$ be the mixed volume of the system, MV_i the mixed volume of the system if we discard the i-th polynomial, $\#(Q_i)$ the number of integer points of the Newton polytope of the i-th polynomial, for $1 \leq i \leq 3$, $\varrho = \prod_{i=1}^{3} (\#Q_i)^{\mathsf{MV}_i}$, and $\mathcal{C} = \prod_{i=1}^{3} \|F_i\|_{\infty}^{\mathsf{MV}_i}$.

The univariate polynomial that has the z-coordinates of the solution set of the system as roots, we call them ζ, has degree $\mathcal{D}$ and maximum coefficient bitsize $\varrho\, 2^{\mathcal{D}}\, \mathcal{C}$. It holds

$$|\zeta| \geq (\varrho\, 2^{\mathcal{D}}\, \mathcal{C})^{-1} \ .$$

In our case

$$\begin{gathered} \mathcal{D} = n^2, \mathsf{MV}_1 = n^2, \mathsf{MV}_2 = \mathsf{MV}_3 = n, \\ (\#Q_1) = m+1, (\#Q_2) = (\#Q_3) = n+1, \\ \varrho = (m+1)^{n^2} (n+1)^{2n}, \mathcal{C} \leq 2^{\tau(n^2+2n)}. \end{gathered}$$

The lower bound for ζ becomes

$$|\zeta| \geq 2^{-(n^2 + n^2 \lg(m+1) + 2n \lg(n+1) + \tau(n^2+2n))} \ ,$$

and hence

$$t = n^2 + n^2 \lg(m+1) + 2n \lg(n+1) + \tau(n^2+2n) \ .$$

We choose $t = 3n^2\tau + 5n^2 \lg(mn) = \widetilde{\mathcal{O}}(n^2\tau)$. □

Lemma 14. *Let b_i be as in Problem 2, then $2^{-\widetilde{\mathcal{O}}(n^{10}\nu^4\tau^3)} \leq |b_i(L_H)| \leq 2^{\widetilde{\mathcal{O}}(\nu+\tau)}$.*

Proof: For all i it holds

$$|b_i(L_H)| = |\sum_{j=0}^{\nu} L_H^j| \leq \sum_{j=0}^{\nu} 2^{\tau} (4m\tau)^j \leq (\nu+1) 2^{\tau} (4m\tau)^{\nu} \ ,$$

and so

$$|b_i(L_H)| \leq 2^{\tau + 8\nu \lg(m\tau)} \ .$$

We consider b_i as a univariate polynomial in y and so $b_i = \sum_{j=0}^{\nu} b_{i,j} y^i = b_{i,\nu} \prod_{j=1}^{\nu} (y - \beta_{i,j})$, where $\beta_{i,j}$ are its roots. In this way

$$|b_i(L_H)| = |b_{i,\nu}| \prod_{j=1}^{\nu} |\beta_{i,j} - L_H| \ .$$

We bound each factor $|L_H - \beta_{i,j}|$, for $1 \leq j \leq \nu$, using Theorem 3. For this we need to identify the real algebraic number that $A(\gamma_1, \gamma_2)$ represents. Consider the following polynomial system:

$$\begin{cases} F_1 = z - A(y_1, y_2) & = 0 \\ F_2 = C_1(y_1) & = 0 \\ F_3 = C_2(y_2) & = 0 \end{cases}$$

The system is almost identical to the one in the proof of Lemma 13 and so we get all the (worst case) bounds from that system.

If we eliminate y_1 and y_2 then we get a univariate polynomial in z among the solutions of which is the real algebraic number $A(\gamma_1, \gamma_2)$. The polynomial has degree n^2 and maximum coefficient bitsize $n^2 + n^2 \lg(m+1) + 2n \lg(n+1) + \tau(n^2+2n) = \widetilde{\mathcal{O}}(n^2\tau)$.

Assume that $\beta_{i,1}$ is the root closest to L_H. We notice that $|b_{i,\nu}| \geq 1$, $\mathcal{M}(b_i) \leq 2^{\tau + \lg \nu + 1}$, and $-\lg \prod_j \Delta(b_i) = \mathcal{O}(\nu^2 + \nu\tau)$. When we apply Thm. 3, after some lengthy calculations, we get

$$|L_H - \beta_{i,j}| \geq \exp(-5 \cdot 10^{10}\, n^{10}\, \nu^4\, \tau (2\tau^2 + 16 \lg^2(n\nu\tau))) \ .$$

Finally, we apply Lemma 2

$$|b_i(L_H)| > |b_{i,\nu}|^7\, |L_H - \beta_{i,1}|^6\, \mathcal{M}(b_i)^{-6}\, 2^{\lg \prod_j \Delta(b_i) - 6} \ ,$$

and we get $|b_i(L_H)| \geq \exp(-\mathcal{O}(n^{10}\nu^4\tau^3))$, which concludes the proof. □

An upper bound for $\|B_H\|_2$ is $\|B_H\|_2^2 = \sum_{i=0}^{d} |b_i(L_H)|^2 \Rightarrow \|B_H\|_2 \leq 2^{\tau + 8\nu \lg(m\tau) + \lg(d)}$.

Lemma 15. *Let B_H be as in Problem 2, then $2^{-\widetilde{\mathcal{O}}(d^7 n^8 \nu^4 \tau^3)} \leq |\mathsf{disc}(B_H)| \leq 2^{\widetilde{\mathcal{O}}(d\nu + d\tau + n^{10}\nu^4\tau^3)}$.*

Proof: As in the proof Lemma 6 we consider B_H as a bivariate polynomial in $\mathbb{Z}[L_H, x]$, and

$$|\mathsf{disc}(B_H)| = \left|\frac{1}{b_d(L_H)}\mathtt{res}_x(B_H(L_H,x), \partial B_H(L_H,x)/\partial x)\right| = \left|\frac{1}{b_d(L_H)}R_B(L_H)\right| \ . \tag{9}$$

The resultant $R_B \in \mathbb{Z}[L_H]$ is a univariate polynomial of degree at most $2d\nu$ and maximum coefficient bitsize $2d\tau + 10d\lg(d\nu)$. Therefore

$$|R_B(L_H)| \leq 2^{2d\tau+10d\lg(d\nu)}\sum_{k=0}^{2d\nu}|L_H|^k \leq 2^{2d\tau+10d\lg(d\nu)}(4m\tau)^{2d\nu+1} \ .$$

For the lower bound, let r be the leading coefficient of R_B and ρ_k its roots. Let ρ_1 be the root closest to L_H. Then $|r| \geq 1$, $\mathcal{M}(R_B) \leq 2^{2d\tau+12d\lg(d\nu)}$, $-\lg\prod_k \Delta(R_B) = \mathcal{O}(d^2\nu^2 + d^2\nu\tau)$. The application of Theorem 3 gives us

$$|L_H - \rho_1| \geq \exp(-\widetilde{\mathcal{O}}(d^7n^8\nu^4\tau^3)) \ .$$

Using Lemma 2 we get

$$|R_B(L_H)| > |r|^7\,|L_H-\rho_1|^6\,\mathcal{M}(R_B)^{-6}\,2^{\lg\prod_k\Delta_k(R_B)-6} \ ,$$

and thus

$$|R_B(L_H)| \geq \exp(-\widetilde{\mathcal{O}}(d^7n^8\nu^4\tau^3)) \ .$$

Combining Eq. (9) with the previous inequality and Lemma 14 we get

$$2^{-\widetilde{\mathcal{O}}(d^7n^8\nu^4\tau^3)} \leq |\mathsf{disc}(B_H)| \leq 2^{\widetilde{\mathcal{O}}(d\nu+d\tau+n^{10}\nu^4\tau^3)} \ ,$$

that concludes the proof. □

Lemma 16. *Let B_H be as in Problem 2 and let β_j be its roots. Then*

$$2^{-\widetilde{\mathcal{O}}(n^{10}\nu^4\tau^3)} \leq |\beta_j| \leq 2^{\widetilde{\mathcal{O}}(n^{10}\nu^4\tau^3)} \ ,$$

$$\Sigma(B_H) = -\lg\prod_{(i,j)\in\Omega}|\beta_i-\beta_j| \leq \widetilde{\mathcal{O}}(n^8\nu^4\tau^3(n^2+d^7)) \ .$$

When we have two or more logarithms and the polynomials are not homogeneous or if we have homogeneous polynomials and three or more logarithms then we are not able to compute separation bounds. In this case the separation bounds are closely connected to major open problems in number theory, like the *four exponentials conjecture*. For example, no effective lower bounds are known for the expression $|\lg(\alpha_1)\lg(\alpha_2) - \lg(\alpha_3)\lg(\alpha_4)|$, where $\alpha_{\{1,2,3,4\}}$ are (real) algebraic numbers.

4.1 Isolating the real roots of B_H

We proceed as in Section 3.2. We approximate the coefficients of B_H up to accuracy $\mathcal{O}(\Sigma(B_H) + d\,\sigma)$ [25], see also [27, 22, 18], where $\left|\frac{b_i(L_H)}{b_d(L_H)}\right| \leq 2^{\sigma}$.

From Lemma 16 we get $\Sigma(B_H) = \widetilde{\mathcal{O}}(n^8\nu^4\tau^3(n^2+d^7))$, and from Lemma 14 $\sigma = \widetilde{\mathcal{O}}(n^{10}\nu^4\tau^3)$. Therefore we should approximate the coefficients of B_H up to accuracy $\widetilde{\mathcal{O}}_B(\Sigma(B_H)+d\,\sigma) = \widetilde{\mathcal{O}}(n^8\nu^4\tau^3(n^2+d^7))$. We isolate the real roots of the polynomial in $\widetilde{\mathcal{O}}(d^2n^8\nu^4\tau^3(n^2+d^7))$ [22] or $\widetilde{\mathcal{O}}(d^3n^8\nu^4\tau^3(n^2+d^7))$ [27, 26].

Now we estimate the cost of approximating $b_i(L_q)/b_d(L_q)$ up to accuracy of $\mathcal{O}(\Sigma(B_H)+d\sigma)$ bits after the binary point.

Working as in Section 3.2 we deduce that we should approximate $L_H = \lg A(\gamma_1,\gamma_2)$ up to precision 2^{-t}, where $t = \mathcal{O}(\Sigma(B_q) + d\sigma) = \widetilde{\mathcal{O}}(n^8\nu^4\tau^3(n^2+d^7))$. The cost of this approximation is quasi-linear $\widetilde{\mathcal{O}}_B(t)$ [5], see also [6] and references therein. However, we should also approximate $A(\gamma_1,\gamma_2)$ up to this accuracy. Assume that we have isolating intervals $[\gamma_1]$, resp. $[\gamma_2]$, for the real algebraic number γ_1, resp. γ_2. Let their widths be 2^{-s}, where s is a positive integer that we should determine. That is $\mathtt{wid}[\gamma_1] = \mathtt{wid}[\gamma_2] = 2^{-s}$.

Recall that $2^{-\tau} \leq |\gamma_{\{1,2\}}| \leq 2^{\tau}$, and that $A = \sum_{i=0}^{m} a_i y_1^i y_2^{m-i}$ is a homogeneous bivariate polynomial of degree m.

For an expression E, let $[E]$ be its evaluation using interval arithmetic. Using the properties of interval arithmetic [1] we get that $\mathtt{wid}[a_i\gamma_1^i\gamma_2^{m-i}] \leq m2^{\tau(m-1)}2^{-s}$, and $\mathtt{wid}[A(\gamma_1,\gamma_2)] \leq m^2 2^{m\tau}2^{-s} \leq 2^{-t}$, which leads to $s = t + m\tau + 2\lg(m) = \widetilde{\mathcal{O}}(n^8\nu^5\tau^3(n^2+d^8))$.
We approximate γ_1 and γ_2 up to this accuracy in $\widetilde{\mathcal{O}}(n^{10}\nu^4\tau^3(n^2+d^7))$ [23].

Theorem 17. *The Boolean complexity of isolating the real roots of B_H of Problem 2 is $\widetilde{\mathcal{O}}(n^8\nu^4\tau^3(n^2+d^7)(n^2+d^2))$, or $\widetilde{\mathcal{O}}(n^8\nu^4\tau^3(n^2+d^7)(n^2+d^3))$.*

5. AN EXTENSION TO BIVARIATE POLYNOMIAL SYSTEMS

In this section we consider an extension of our bounds to bivariate polynomial systems. Let $L = L_q$ or $L = L_H$ (Section 3 and Section 4, respectively). The problem statement is as follows:

Problem 3. *Consider the, zero dimensional, polynomial system (S_L) $F_1(x,y) = F_2(x,y) = 0$, where $F_{1,2} \in (\mathbb{Z}[L])[x_1,x_2]$ and their total degree is bounded by d. Let $L = L_q = \lg(q)$, resp. $L = L_H = \lg A(\gamma_1,\gamma_2)$, be as in Problem 1, resp. Problem 2. The coefficients of F_1 and F_2 are polynomials in L of degree ν and maximum coefficient bitsize at most τ. What is the Boolean complexity of isolating the real roots of (S_L)?*

The complexity of the algorithms for solving bivariate polynomial systems depends heavily on the separation bound of the system. We will present separation bounds and we postpone the complete analysis of isolation for a future communication. We use the DMM bound [13]. Consider the polynomial system

$$(S_0) \quad F_1(x_1,x_2) = F_2(x_1,x_2) = u - x_1 = 0,$$

where u is a parameter. If we eliminate x_1 and x_2 from (S_0) then we get a univariate polynomial in u, $R \in (\mathbb{Z}[L])[u]$, which is called the u-resultant. The DMM bound bounds the separation of S_L using the separation bound of R. Asymptotically, the latter depends on a lower bound on the discriminant of its square-free part [13, Thm. 3]. Hence, it suffices to estimate this bound.

The coefficients of R are of the form $\varrho_k\,c_1^d\,c_2^d\,u^k$, where $0 \leq k \leq d^2$, $c_{\{1,2\}}$ denotes a monomial in the coefficients of $F_{\{1,2\}}$ of total degree d, and ϱ_k is an integer that depends on the integer points of the Newton polytopes of the polynomials and in our case is bounded by $|\varrho_k| \leq (d^2+2)^{2d}$. The degree of R wrt u is $\mathcal{O}(d^2)$.

Recall that the coefficients of $F_{\{1,2\}}$ are polynomials in L. Thus, the coefficients of R are also polynomials in L of degree at most $2d\nu$ and maximum coefficient bitsize $\widetilde{\mathcal{O}}(d\tau)$. If we compute the square-free part of R, then its coefficients are polynomials of degree bounded by $2d\nu$ and of maximum coefficient bitsize bounded by $2d\tau + 10d\lg(d) = \widetilde{\mathcal{O}}(d\tau)$ [33]. If $L = L_q = \lg(q)$ then we apply Lemma 6 and the logarithm of the separation bound of the system is $\widetilde{\mathcal{O}}(d^{17}\,\nu^4\,\tau^3)$. If $L = L_H = \lg A(\gamma_1, \gamma_2)$ then we apply Lemma 15 and the logarithm of the separation bound of the system is $\widetilde{\mathcal{O}}(n^8\,\nu^4\,d^7\,\tau^3(n^2 + d^{14}))$. The aforementioned bounds are quite pessimistic.

We could generalize the analysis for polynomial systems in n variables. The bounds are more technical in this case, but the main idea is the same as in the bivariate case. We can also generalize Lemma 12 to prove that the expected number of real roots of (S_L) is d, or $\sqrt{d^n}$ in the general case.

Acknowledgments. Both authors would like to thank an anonymous referee for her, or his, constructive comments which led to Lemma 2 and to an improvement of our original complexity bounds by a factor. ET is partially supported by the EXACTA grant of the National Science Foundation of China (NSFC 60911130369) and the French National Research Agency (ANR-09-BLAN-0371-01), GeoLMI (ANR 2011 BS03 011 06), HPAC (ANR ANR-11-BS02-013) and an FP7 Marie Curie Career Integration Grant.

6. REFERENCES

[1] G. Alefeld and J. Herzberger. *Introduction to interval computations*. Academic Press, 1983.

[2] A. Baker. Linear forms in the logarithms of algebraic numbers (IV). *Mathematika*, 15(02):204–216, 1968.

[3] A. Baker. The theory of linear forms in logarithms. *Transcendence Theory: Advances and Applications*, pages 1–27, 1977.

[4] D. J. Bates and F. Sottile. Khovanskii–rolle continuation for real solutions. *Foundations of Computational Mathematics*, 11(5):563–587, 2011.

[5] R. Brent. Fast multiple-precision evaluation of elementary functions. *J. of ACM*, 23(2):242–251, 1976.

[6] R. Brent and P. Zimmermann. *Modern computer arithmetic*, volume 18. Cambridge University Press, 2010.

[7] J.-S. Cheng, X.-S. Gao, and C.-K. Yap. Complete numerical isolation of real roots in zero-dimensional triangular systems. *J. Symbolic Computation*, 44:768–785, 2009.

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

[9] Z. Du, V. Sharma, and C. K. Yap. Amortized bound for root isolation via Sturm sequences. In D. Wang and L. Zhi, editors, *Int. Workshop on Symbolic Numeric Computing*, pages 113–129, Beihang University, Beijing, China, 2005. Birkhauser.

[10] A. Edelman and E. Kostlan. How may zeros of a random polynomial are real? *Bulletin AMS*, 32(1):1–37, 1995.

[11] A. Eigenwillig, L. Kettner, W. Krandick, K. Mehlhorn, S. Schmitt, and N. Wolpert. A Descartes Algorithm for Polynomials with Bit-Stream Coefficients. In V. Ganzha, E. Mayr, and E. Vorozhtsov, editors, *CASC*, volume 3718 of *LNCS*, pages 138–149. Springer, 2005.

[12] I. Z. Emiris, A. Galligo, and E. P. Tsigaridas. Random polynomials and expected complexity of bisection methods for real solving. In S. Watt, editor, *Proc. 35th ACM Int'l Symp. on Symbolic & Algebraic Comp. (ISSAC)*, pages 235–242, Munich, Germany, July 2010. ACM.

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

[14] J. Johnson and W. Krandick. Polynomial real root isolation using approximate arithmetic. In *Proc. Int'l Symp. on Symb. and Algebraic Comp. (ISSAC)*, pages 225–232. ACM, 1997.

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

[16] Z. Lu, B. He, Y. Luo, and L. Pan. An algorithm of real root isolation for polynomial system. In D. Wang and L. Zhi, editors, *Proc. 1st ACM Int'l Work. Symbolic Numeric Computation (SNC)*, pages 94–107, 2005.

[17] J. M. McNamee and V. Y. Pan. *Numerical methods for roots of polynomials (II)*, chapter 15. Elsevier, 2013.

[18] K. Mehlhorn and M. Sagraloff. A deterministic algorithm for isolating real roots of a real polynomial. *J. Symbolic Computation*, 46(1):70–90, 2011.

[19] K. Mehlhorn, M. Sagraloff, and P. Wang. From approximate factorization to root isolation. In *ISSAC*, pages 283–290, 2013.

[20] M. Mignotte. Some useful bounds. In B. Buchberger, G. Collins, and R. Loos, editors, *Computer Algebra: Symbolic and Algebraic Computation*, pages 259–263. Springer-Verlag, Wien, 2nd edition, 1982.

[21] M. Mignotte and M. Waldschmidt. Linear forms in two logarithms and Schneider's method. *Mathematische Annalen*, 231(3):241–267, 1978.

[22] V. Pan. Univariate polynomials: Nearly optimal algorithms for numerical factorization and rootfinding. *J. Symbolic Computation*, 33(5):701–733, 2002.

[23] V. Y. Pan and E. P. Tsigaridas. On the boolean complexity of real root refinement. In *ISSAC*, pages 299–306, Boston, USA, Jun 2013. ACM.

[24] F. Rouillier and Z. Zimmermann. Efficient isolation of polynomial's real roots. *J. of Computational and Applied Mathematics*, 162(1):33–50, 2004.

[25] M. Sagraloff. On the complexity of real root isolation. abs/1011.0344v1, 2010.

[26] M. Sagraloff. When Newton meets Descartes: A simple and fast algorithm to isolate the real roots of a polynomial. In *Proc. 37th ACM Int'l Symp. on Symbolic & Algebraic Comp. (ISSAC)*, pages 297–304, Grenoble, France, July 2012. ACM.

[27] A. Schönhage. The fundamental theorem of algebra in terms of computational complexity. Manuscript. Univ. of Tübingen, Germany, 1982. URL: http://www.iai.uni-bonn.de/~schoe/fdthmrep.ps.gz.

[28] A. Strzeboński and E. P. Tsigaridas. Univariate real root isolation in an extension field. In A. Leykin, editor, *Proc. 36th ACM Int'l Symp. on Symbolic & Algebraic Comp. (ISSAC)*, pages 321–328, San Jose, CA, USA, June 2011. ACM.

[29] A. Strzeboński and E. P. Tsigaridas. Univariate real root isolation in multiple extension fields. In *Proc. 37th ACM Int'l Symp. on Symbolic & Algebraic Comp. (ISSAC)*, pages 343–350, Grenoble, France, July 2012. ACM.

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

[31] B. Xia and L. Yang. An algorithm for isolating the real solutions of semi-algebraic systems. *J. Symbolic Computation*, 34:461–477, November 2002.

[32] B. Xia and T. Zhang. Real solution isolation using interval arithmetic. *Comput. Math. Appl.*, 52:853–860, September 2006.

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

APPENDIX

A. ADDITIONAL RESULTS

In this appendix we present simplified versions of Problem 2 that lead to less scary separation and complexity bounds. The proof techniques are the same, but the algebraic tools needed are more elementary.

A.1 The case of B_α

We generalize Problem 1 be letting the the argument of the logarithm to be a positive real algebraic number. In this section we let $L_\alpha = \lg(\alpha)$.

Problem 4. *Consider the square-free polynomial*

$$B_a = \sum_{i=0}^{d} b_i\, x^i, \qquad \text{where} \quad b_i = \sum_{j=0}^{\nu} b_{i,j}\, (\lg(\alpha))^j \quad ,$$

$b_{i,j} \in \mathbb{Z}$, $\mathcal{L}(b_{i,j}) \leq \tau$, and α is a positive real root of a polynomial $A \in \mathbb{Z}[x]$ of degree m and maximum coefficient bitsize τ. What is the Boolean complexity of isolating the real roots of B_α?

Lemma 18. *Let α be a positive root of a univariate polynomial $A \in \mathbb{Z}[x]$ that has degree m and maximum coefficient bitsize τ. Then $2^{-m\tau-1} \leq |\lg(\alpha)| \leq \tau + 1$.*

Proof: The right inequality follows from Cauchy's bound, since $|\alpha| \leq 2^{\tau+1}$.

For the left inequality we will use the trick of Lemma 4. First we need to bound $|\alpha - 1|$. Notice tat $\alpha - 1$ is a root of $\bar{A}(x) = A(x+1)$. The coefficients of $\bar{A}(x)$ are bounded by $(m+1)!2^\tau$. Using Cauchy's bound

$$|\alpha - 1| \geq 2^{\tau + 2m\lg(m)} \quad .$$

Using the inequality $|e^z - 1| \leq |z| e^{|z|}$, we get

$$|\alpha - 1| \leq \frac{|\lg(\alpha)|}{\ln(2)}\, |\alpha| \quad ,$$

and thus $|\lg(\alpha)| \geq 2^{m\tau-1}$, that concludes the proof. □

Lemma 19. *Let b_i be as in Problem 4, then*

$$2^{-\widetilde{\mathcal{O}}(m^4\nu^5\tau^3)} \leq |b_i(L_\alpha)| \leq 2^{\widetilde{\mathcal{O}}(\nu+\tau)}.$$

Lemma 20. *Let B_α be as in Problem 4, then*

$$2^{-\widetilde{\mathcal{O}}(d^7\nu^5m^4\tau^3)} \leq |\mathsf{disc}(B_\alpha)| \leq 2^{\widetilde{\mathcal{O}}(d\nu+d\tau+d^7\nu^5m^4\tau^3)} \quad .$$

Lemma 21. *Let B_α be as in Problem 4 and let β_j be its roots. Then*

$$2^{-\widetilde{\mathcal{O}}(m^4\nu^5\tau^3)} \leq |\beta_j| \leq 2^{\widetilde{\mathcal{O}}(m^4\nu^5\tau^3)} \quad ,$$

$$\Sigma(B_\alpha) = -\lg \prod_{(i,j)\in\Omega} |\beta_i - \beta_j| \leq \widetilde{\mathcal{O}}(d^8\nu^5m^4\tau^3) \quad .$$

A.2 The case of B_A

In this section we let $L_A = \lg(A(\gamma))$. Notice that the bounds that we compute are better than the one that we can obtain by computing the minimal polynomial of $A(\gamma)$ and using the bounds of Section A.1

Problem 5. *Consider the square-free polynomial*

$$B_A = \sum_{i=0}^{d} b_i\, x^i, \qquad \text{where} \quad b_i = \sum_{j=0}^{\nu} b_{i,j}\, (\lg(A(\gamma)))^j \quad ,$$

$b_{i,j} \in \mathbb{Z}$, $\mathcal{L}(b_{i,j}) \leq \tau$, $A \in \mathbb{Z}[x]$ is a polynomial of degree m and $\mathcal{L}(A) = \tau$ and γ is a positive real root of a polynomial $C \in \mathbb{Z}[x]$ that is of degree n and $\mathcal{L}(C) = \tau$. What is the Boolean complexity of isolating the real roots of B_A?

Lemma 22. *Le $\alpha = A(\gamma)$, where $A \in \mathbb{Z}[x]$ is a polynomial of degree m and maximum coefficient bitsize τ and γ is a positive real root of a polynomial $C \in \mathbb{Z}[x]$ that is of degree n and maximum coefficient bitsize τ. Then*

$$2^{-4m\tau-10m\lg m} \leq |\lg(\alpha)| \leq 2^{2m\tau+5m\lg m} \quad .$$

Proof: First we compute an upper bound on $A(\gamma)$. We consider the following resultant

$$|R| = \mathtt{res}_x(C(x), y - A(x)) = |c_n^m \prod_{i=1}^{m} (y - A(\gamma_i))|$$

The roots of R are the evaluation of A over all the roots of C. Hence, it suffices to bound the roots of R. The polynomial R belongs to $\mathbb{Z}[y]$. Its degree is m and its maximum coefficient bitsize is $\mathcal{L}(R) \leq 2m\tau + 5m\lg m$ [28]. Following Cauchy's bound we get

$$|A(\gamma)| \leq \max_i |A(\gamma_i)| \leq 2^{2m\tau+5m\lg m}$$

From the previous relation we deduce the left inequality.

We consider the polynomial $\bar{A}(x) = A(x) - 1$. It is of degree m and maximum bitsize τ. The resultant

$$|R| = |\mathtt{res}_x(C(x), y - \bar{A}(x))| = |c_n^m \prod_{i=1}^{m} (y - \bar{A}(\gamma_i))|$$

is a polynomial in $\mathbb{Z}[y]$ of degree m and bitsize $\mathcal{L}(R) = 2m\tau + 5m\lg m$ [28]. The roots of R are the evaluation of $\bar{A}$ over the roots of C. Hence, using Cauchy's bound

$$|A(\gamma) - 1| = \bar{A}(\gamma) \geq 2^{-2m\tau-5m\lg m}$$

Using the inequality $|e^z - 1| \leq |z| e^{|z|}$, we get

$$|A(\gamma) - 1| \leq \frac{|\lg A(\gamma)|}{\ln(2)}\, |A(\gamma)|$$

and thus

$$2^{-4m\tau-10m\lg m} \leq \lg A(\gamma)$$

□

Lemma 23. *Let b_i be as in Problem 4, then*

$$2^{-\widetilde{\mathcal{O}}(m^4n^5\nu^5\tau^3)} \leq |b_i(L_A)| \leq 2^{\widetilde{\mathcal{O}}(\nu+\tau)}.$$

Lemma 24. *Let B_A be as in Problem 5, then*

$$2^{-\widetilde{\mathcal{O}}(d^7n^6\nu^5m^4\tau^3)} \leq |\mathsf{disc}(B_A)| \leq 2^{\widetilde{\mathcal{O}}(d\nu+d\tau+d^7n^6\nu^5m^4\tau^3)} \quad .$$

Lemma 25. *Let B_A be as in Problem 5 and let β_j be its roots. Then*

$$2^{-\widetilde{\mathcal{O}}(m^4n^5\nu^5\tau^3)} \leq |\beta_j| \leq 2^{\widetilde{\mathcal{O}}(m^4n^5\nu^5\tau^3)} \quad ,$$

$$\Sigma(B_A) = -\lg \prod_{(i,j)\in\Omega} |\beta_i - \beta_j| \leq \widetilde{\mathcal{O}}(d^8n^6\nu^5m^4\tau^3) \quad .$$