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. The algorithm approximates the coefficients of B up to a sufficient accuracy and then solves 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 results 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 real algebraic 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 introduction for a detailed presentation of the notation that we use. The first problem that we consider is the following:

Problem 1. *Consider the square-free polynomial*

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

$b_{i,j} \in \mathbb{Z}$, $\mathcal{L}(b_{i,j}) \leq \tau$, 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?

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. We present the first complexity bounds for the real solving problem for a family of polynomials with coefficients involving logarithms of algebraic numbers. In addition, our implementation is the first complete one for solving exactly polynomial with such transcendental numbers as coefficients.

We tackle the problem by approximating the coefficients of B_α up to a sufficient precision. In this way we relate it to numerical univariate real solving algorithms [30, 26], see also [28, 17], and to algorithms based on the bitstream model, e.g. [23, 13, 29]. For a detailed treatment of numerical solvers we refer the reader to [22, Chapter 15]. Problem 1 is an significant generalization of the problem of solving polynomials with coefficients in an extension field, [18, 32, 31], see also [8, 35, 34, 20] 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 this algorithm.

To obtain the various bounds we have to combine several algebraic techniques in a novel way and to provide new evaluation and perturbation bounds; the latter turn out to be useful in other applications as well. Our analysis is based on effective lower bounds of linear forms in two logarithms; a result due to Mignotte and Waldschmidt (Thm. 3). We combine this bound with univariate and multivariate separation and evaluation bounds of polynomials and polynomial systems. The idea is to approximate the coefficients of B_α 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 from the isolated intervals of the approximate polynomial we can derive isolating intervals for the real roots of B_α.

First, we need to quantify "sufficient accuracy". We treat the logarithm as a parameter and the separation bound of B_α 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 one of factoring the polynomial in linear factors and bounding the separation 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 a homogeneous bivariate polynomial evaluated

at two real algebraic numbers. It is a simplified version of Problem 1. However, while the resolution of the latter depends on combinations of univariate separation bounds, Problem 2 depends on successive applications of aggregate multivariate separation bounds and applications of Thm. 3. 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_α 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 $\sqrt{d}$. 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 of this kind. Finally, we generalize our bounds to handle bivariate polynomial systems. We prove a perturbation bound for the roots of a bivariate polynomial system that is applicable to a broader context.

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 5 and the extension to bivariate polynomial systems in Section 6.

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 $A = \sum_{i=0}^{d} a_i\, x^i \in \mathbb{Z}[x]$, $\mathtt{deg}(A) = d$ 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 $A \in \mathbb{Z}[x]$ 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 $L_\alpha = \lg(\alpha)$, where α is a positive algebraic number, and $L_H = \lg A(\gamma_1, \gamma_2)$, where $\gamma_{\{1,2\}}$ are real algebraic and A is a bivariate homogeneous polynomial and $A(\gamma_1, \gamma_2) > 0$.

2. PRELIMINARIES

Real algebraic numbers are the real roots of univariate polynomials with integer coefficients; we denote their set by $\mathbb{R}_{\mathsf{alg}}$. We represent them using the *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, $\mathcal{I} = [\mathtt{a}_1, \mathtt{a}_2]$, that contains α and no other root of the polynomial. We write $\alpha \cong (A, \mathcal{I})$. Such a representation could be also used to represent the real roots of polynomials with real numbers as 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, e.g. [11, 9, 33]. The aggregate version of Eq. (2) comes from [19].

Proposition 1 (`DMM1`). *Let $f = \sum_{i=0}^{d} a_i x^i \in \mathbb{R}[x]$ be a univariate polynomial of degree d such that $a_d a_0 \neq 0$. The distinct roots of f are $\alpha_1, \ldots, \alpha_r$. For any root α_k it holds*

$$\frac{|a_0|}{2\,\|f\|_\infty} \leq |\alpha_k| \leq 2\frac{\|f\|_\infty}{|a_d|} \quad . \tag{1}$$

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

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

where $\mathbf{sr}_r(f, f')$ is the r-th subresultant coefficient of the subresultant sequence of f and its derivative f'.

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. For another proof with slightly different bounds, suggested by one of the reviewers, we refer the reader to the appendix.

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

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

Proof: There are at most six roots of f such that $|L - \gamma_i| \leq |\gamma_i - \gamma_{c_i}| = \Delta_i$, where γ_{c_i} is the root closest to γ_i. This is a consequence of the vertex degree of planar nearest neighbor graphs [16]. Wlog let them be the first six ones. Then

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

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 that 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 [25]. It 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. *[25] Let $\Lambda = \beta \log(\alpha_1) - \log(\alpha_2)$, where log is any determination of the logarithm, and $\beta, \alpha_1, \alpha_2$ are three non-zero algebraic numbers of degrees D_0, D_1, D_2, respectively. Let A_i be a bound on the height of α_i such that $\exp(|\log(\alpha_i)|) \leq A_i$, for $i \in \{1, 2\}$. B is an upper bound on the height of β and e^{D_0}. If D is the degree over $\mathbb{Q}$ of the field $\mathbb{Q}(\beta, \alpha_1, \alpha_2)$, and $T = \ln(B) + \ln\ln(A_1) + \ln\ln(A_2) + \ln(D)$, then $|\Lambda| > \exp(-5 \cdot 10^{10} \cdot D^4 \cdot \ln(A_1) \cdot \ln(A_2) \cdot T^2)$.*

Remark 4. *If the height of α is H, then*

$$\exp(|\lg(\alpha)|) \leq \exp(|\ln(\alpha)|/\ln 2) \leq (2H)^{1/(\ln 2)} \leq 4H^2.$$

Therefore, if the height of α_i is H_i, then $A_i = 4H_i^2$.

If the height of β is $H_0 = 2^\tau$, then to meet both conditions on B we consider $B = H_0\, 2^{2D_0} = 2^{\tau+2D_0}$.

3. AN ALGORITHM FOR B_α

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. In what follows we assume that L_α is indeed a transcendental number. This could be tested using Lindemann–Weierstrass theorem. The following lemma is based on arguments in [2].

Lemma 5. *Let α be a positive real root of a univariate polynomial $A \in \mathbb{Z}[x]$ that has degree m and maximum coefficient bitsize τ. Then $2^{-2\tau-m-2} \leq |\lg(\alpha)| \leq \tau + 1$.*

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

For the left inequality, first we need to bound $|\alpha-1|$. Notice that $\alpha - 1$ is a root of $\bar{A}(x) = A(x+1)$. The coefficients of $\bar{A}(x)$ are bounded by $2^{m+\tau}$. Using Cauchy's bound

$$|\alpha - 1| \geq 2^{-\tau-m-1} \ .$$

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

$$|\alpha - 1| \leq |e^{\ln(\alpha)} - 1| \leq \frac{|\lg(\alpha)|}{\lg(e)}\,|\alpha| \ ,$$

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

Lemma 6. *Let b_i be as in Problem 1, then*

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

Proof: To bound b_i we proceed as follows:

$$|b_i(L_\alpha)| = |\sum_{j=0}^{\nu} b_{i,j} L_\alpha^j| \leq 2^\tau \sum_{j=0}^{\nu} |L_\alpha|^j \leq 2^\tau \sum_{j=0}^{\nu} (\tau+1)^j$$
$$\leq 2^{\tau+\nu+1}\tau^{\nu+1} \leq 2^{\tau+2\nu\lg(2\tau)} \ .$$

To compute a lower bound for $|b_i(L_\alpha)|$ we assume that $\beta_{i,1}$ is the root of $b_i(y)$ closest to L_α and we apply Lemma 2, i.e.

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

It holds $|b_{i,\nu}| \geq 1$; Theorem 3 and Remark 4 imply

$$|L_\alpha - \beta_{i,1}| \geq \exp(c_1\, m^4\,\nu^4\,\tau\,(\tau+\nu+\ln(m\tau\nu))^2) \ ,$$

where c_1 is constant that can be computed explicitly.

Landau's inequality gives $\mathcal{M}\,(b_i) \leq (\nu+1)\|b_i\|_\infty \leq 2^{\tau+\lg\nu+1}$. Finally, using Proposition 1 we have $\lg\prod_j \Delta_j(b_i) \geq -3\nu^2 - 3\nu\tau - 4\nu\lg\nu$. Combining all the inequalities we get

$$|b_i(L_\alpha)| \geq \exp(c_2\, m^4\,\nu^4\,\tau\,(\tau+\nu+\ln(m\tau\nu))^2) \ ,$$

$$\text{or} \quad |b_i(L_\alpha)| \geq \exp(-\widetilde{\mathcal{O}}(m^4\,\nu^4\,\tau\,(\tau^2+\nu^2))) \ ,$$

where c_2 is constant that can be computed explicitly. □

The previous lemma allows us to bound $\|B_\alpha\|_2$. It holds $\|B_\alpha\|_2^2 = \sum_{i=0}^d |b_i(L_\alpha)|^2 \leq (d+1)\,2^{2\tau+2}\,\tau^{2\nu+2}$, and so

$$\|B_\alpha\|_2 \leq d\,2^{\tau+1}\,\tau^{\nu+1} \ . \tag{3}$$

Lemma 7. *Let B_α be as in Problem 1, then*

$$2^{-\widetilde{\mathcal{O}}(d^6\nu^4m^4\tau(\nu^2+\tau^2))} \leq |\mathsf{disc}(B_\alpha)| \leq 2^{\widetilde{\mathcal{O}}(d\nu+d\tau+m^4\,\nu^4\,\tau\,(\tau^2+\nu^2))} \ .$$

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

$$|\mathsf{disc}(B_\alpha)| = \left|\frac{1}{b_d(L_\alpha)}\mathtt{res}_x(B_\alpha(L_\alpha,x), \partial B_\alpha(L_\alpha,x)/\partial x)\right|$$
$$= \left|\frac{1}{b_d(L_\alpha)}R_B(L_\alpha)\right| \ , \tag{4}$$

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

The Sylvester matrix is of size $(2d-1)\times(2d-1)$, the elements of which belong to $\mathbb{Z}[L_\alpha]$. The determinant consists of $(2d-1)!$ terms. Each term is a product of $d-1$ polynomials in L_α of degree at most ν and bitsize at most τ, times a product of d polynomials in L_α 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_α of degree less than $2d\nu$ and bitsize at most $2d\tau + 6d\lg(d\nu)$. The determinant itself is a polynomial in L_α 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:

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

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_α, then

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

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

$$|L_\alpha - \rho_1| \geq \exp(-\mathcal{O}(d^4\nu^4m^4\tau(d\nu+d\tau+\lg(d\nu m\tau))^2)) \ .$$

By combining all the inequalities we get

$$|R_B(L_\alpha)| \geq \exp(-\mathcal{O}(d^4\nu^4m^4\tau(d\nu+d\tau+\lg(d\nu m\tau))^2)) \ .$$

Eq. (4) with the previous inequality and Lemma 6 imply

$$2^{-\widetilde{\mathcal{O}}(d^6\nu^4m^4\tau(\nu^2+\tau^2))} \leq |\mathsf{disc}(B_\alpha)| \leq 2^{\widetilde{\mathcal{O}}(d\nu+d\tau+m^4\,\nu^4\,\tau\,(\tau^2+\nu^2))} \ .$$

which concludes the proof. □

We combine Lemma 6, Lemma 7 and Eq. (3) with Proposition 1 to derive the following (separation) bounds for B_α.

Lemma 8. *Let B_α be as in Problem 1 and let β_j be its roots. Then*

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

$$\Sigma(B_\alpha) = -\lg\prod_{(i,j)\in\Omega}|\beta_i - \beta_j| = \widetilde{\mathcal{O}}(d^6\nu^4m^4\tau(\nu^2+\tau^2)) \ .$$

3.1 Isolating the real roots of B_α

The main idea behind the algorithm for isolating the real roots of B_α is to approximate its coefficients up to a specified accuracy so that the resulting approximate polynomial, $\widetilde{B}_\alpha$, has real roots that are close to the real roots of B_α. We isolate the real roots of $\widetilde{B}_\alpha$ and the approximation is such that it guarantees that the resulting isolating intervals are also isolating intervals for the real roots of B_α. Several approaches are known in this context [29, 30, 26, 23], We follow [24, Theorem 3].

We divide by the leading coefficient to make the polynomial monic. 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.

Let σ be such that $\left|\frac{b_i(L_\alpha)}{b_d(L_\alpha)}\right| \leq 2^\sigma$ and ρ such that $\rho = \max_j\{1, \max\{1, |\log|\beta_j||\}\}$, that is a logarithmic root bound for the roots of B_α.

If we approximate the coefficients of B_α up to accuracy $\mathcal{O}(d\rho + \Sigma(B_\alpha))$, then we can approximate the roots (of $\widetilde{B}_\alpha$) in $\widetilde{\mathcal{O}}_B(d^3 + d^2\sigma + d\Sigma(B_\alpha))$. In this way the number of real roots of $\widetilde{B}_\alpha$ is the same as the number of real roots of B_α. Moreover, from the isolating intervals of $\widetilde{B}_\alpha$ we can derive isolating intervals for the roots of B_α. We refer the reader to [24] for a comprehensive treatment.

We bound the various quantities. Lemma 8 indicates that

$$\Sigma(B_\alpha) = \widetilde{\mathcal{O}}(d^6\nu^4 m^4 \tau(\nu^2 + \tau^2)) \ . \tag{5}$$

To bound σ we use Lemma 6 and so, for all i, $\left|\frac{b_i(L_\alpha)}{b_d(L_\alpha)}\right| \leq 2^{\widetilde{\mathcal{O}}(m^4\,\nu^4\,\tau\,(\tau^2+\nu^2))}$. And thus

$$\sigma = \widetilde{\mathcal{O}}(m^4\,\nu^4\,\tau\,(\tau^2 + \nu^2)) \ . \tag{6}$$

The same bound holds for ρ. Hence we need to approximate the coefficients of B_α up to accuracy

$$\widetilde{\mathcal{O}}(d\rho + \Sigma(B_\alpha)) = \widetilde{\mathcal{O}}(d^6\nu^4 m^4 \tau(\nu^2 + \tau^2)) \ .$$

We can isolate the real roots in $\widetilde{\mathcal{O}}(d^3 + d^7\nu^4 m^4 \tau(\nu^2 + \tau^2))$.

It remains to estimate the cost of obtaining the approximation on the coefficients of B_α, that is successive approximations of $b_i(L_\alpha)/b_d(L_\alpha)$ up to accuracy of $\mathcal{O}(d\rho + \Sigma(B_\alpha))$ bits after the binary point. Since $|b_i(L_\alpha)/b_d(L_\alpha)| \leq 2^\sigma$, to approximate each fraction, for $0 \leq i \leq d-1$, to desired accuracy ℓ, it is sufficient to approximate $b_i(L_\alpha)$, for $0 \leq i \leq d$, up to precision $\mathcal{O}(\ell + \sigma)$.

The algorithm requires approximation of $b_i(L_\alpha)$, for $0 \leq i \leq d$, to precision $\mathcal{O}(d\rho + \Sigma(B_\alpha) + \sigma)$. Hence, it is sufficient to approximate $b_i(L_q)$ to accuracy $\widetilde{\mathcal{O}}(d^6\nu^4 m^4 \tau(\nu^2 + \tau^2))$.

Approximation of L_α to accuracy of $t > 0$ bits yields an approximation of $b_{i,j}L_\alpha^j$ to accuracy of at least

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

bits and an approximation of $b_i(L_\alpha)$ to accuracy of at least $t - \tau - 2\lg(\nu) - \nu(\lg(\tau) + 1)$ bits. Therefore, we need an approximation of $\lg(\alpha)$ up to $t = \widetilde{\mathcal{O}}(d^6\nu^4 m^4 \tau(\nu^2 + \tau^2))$ bits.

For this we need to approximate α up to this accuracy and then evaluate $\lg(\alpha)$. The cost of the first operation is $\widetilde{\mathcal{O}}_B(m^2\tau + m\,t)$ [27]. The cost of approximating the logarithm up to t bits is quasi-linear $\widetilde{\mathcal{O}}_B(t)$ [6], see also [7] and references therein.

After we have obtained the approximation of L_α, say $\tilde{L}$ we need construct the approximated coefficients of B_α by evaluating the polynomials b_i (of degree ν) at $\tilde{L}$; there are $d+1$ polynomials. Each evaluation costs $\widetilde{\mathcal{O}}_B(\nu t)$ [5] and so the overall cost is $\widetilde{\mathcal{O}}_B(d\nu t) = \widetilde{\mathcal{O}}_B(d^7\nu^5 m^4 \tau(\nu^2 + \tau^2))$.

$d \setminus \nu$	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, $\tau = 10$

$d \setminus \nu$	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, $\tau = 1000$

Theorem 9. *The Boolean complexity of isolating the real roots of B_α of Problem 1 is $\widetilde{\mathcal{O}}(d^3 + d^7\nu^5 m^4 \tau(\nu^2 + \tau^2))$.*

4. EXPERIMENTS

We present experimental results for an implementation of the algorithm isolating roots of the polynomial in Problem 1 in the special case where the algebraic number α is a rational. 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 [29], that applies to polynomials with bitstream coefficients, see also [13, 23], 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 10. *(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 $\mathcal{L}(q) \leq \tau$. 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 11. *(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*

$d \setminus \nu$	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

w.r.t. the Gaussian distribution with mean 0 *and variance* $\binom{d}{i}$. *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 $\sqrt{d}$.

4.1 Random polynomials

We were not able to construct polynomials that achieve the separation bounds of Lemma 8. It is not clear whether the effective lower bounds of Theorem 3 are tight. Our experimental results of the previous section suggest that this is not the case for random polynomials. In addition, this observation triggers the question of estimating the average behavior of the separation bounds. The first step is to estimate the expected number of real roots of B_q, when its coefficients are random variables.

Proposition 12. *[12] 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* $c_0 f_0(t) + \cdots + c_n f_n(t) = 0$, *for* $w(t) = C^{1/2}v(t)$, *is*

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

In logarithmic derivative notation it 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, or $L = \lg(\alpha)$, where α is a positive real algebraic number. 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 12 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 13. *Let* B_α *as in Prob. 1 with a fixed* α. *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, mutatis mutandis, the analysis of [14, Lemma 3.2] the previous lemma allows us to compute the distribution of the real roots and eventually to estimate the expected separation bound; which is $\mathrm{E}[-\lg\Delta(B_\alpha)] = \mathcal{O}(\lg d)$ (for the aforementioned distribution of the coefficients), *for the real roots*. This is far from the worst case proved in Lemma 8 but agrees with the excellent running times of our implementation in Section 4. The bigger the (actual) separation bound, the less bits we need to isolate the real roots, and so the faster the algorithms perform. For estimating the expected separation bounds for the complex roots, we need to compute (expected) lower bounds on the discriminant. We are not aware of such bounds.

5. 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. As in the case of Problem 1 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* $b_i = \sum_{j=0}^{\nu} b_{i,j}\,(\lg(A(\gamma_1,\gamma_2)))^j$, $b_{i,j} \in \mathbb{Z}$, $\mathcal{L}(b_{i,j}) \le \tau$, $A \in \mathbb{Z}[y_1, y_2]$ *is a homogeneous polynomial of degree* m *and* $\mathcal{L}(A) = \tau$ *and* γ_1, *resp.* γ_2, *is a real root of a polynomial* $C_1 \in \mathbb{Z}[y]$, *resp.* $C_2 \in \mathbb{Z}[y]$, *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 14. *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* $2^{-3n^2\tau - 5n^2\lg(mn) - 4m\tau} \le |\lg A(\gamma_1,\gamma_2)| \le 4m\tau$.

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

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

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

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

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 on DMM we refer the reader to [15].

A lower bound on z provides us with a lower bound for t. To compute a bound for z we use the DMM bound from [15, 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

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

Notice that it is exactly the use of mixed volume that allows us to take $\mathcal{D} = n^2$ instead of mn^2 which is the Bézout bound.

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

Proof: For all i it holds

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

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. Let $\beta_{i,1}$ the root closest to L_H; we apply Lemma 2

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

It holds $|b_{i,\nu}| \geq 1$, $\mathcal{M}(b_i) \leq 2^{\tau + \lg \nu + 1}$, and $-\lg \prod_j \Delta(b_i) = \mathcal{O}(\nu^2 + \nu\tau)$.

To bound $|L_H - \beta_{i,1}|$ we use Theorem 3. For this we need to identify the real algebraic number $A(\gamma_1,\gamma_2)$ 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 14 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 $n^2 + n^2 \lg(m+1) + 2n \lg(n+1) + \tau(n^2+2n) = \widetilde{\mathcal{O}}(n^2\tau)$. Then, Thm 3 implies that

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

By combining all the bounds we obtain the bound $|b_i(L_H)| > 2^{-\mathcal{O}(n^{10}\,\nu^4\,\tau(\tau+\nu+\lg(n\nu\tau))^2)}$, 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 16. *Let B_H be as in Problem 2, then $2^{-\widetilde{\mathcal{O}}(d^6 n^8 \nu^4 \tau(\nu^2+\tau^2))} \leq |\mathsf{disc}(B_H)| \leq 2^{\widetilde{\mathcal{O}}(d\nu + d\tau + n^{10}\nu^4\tau(\tau^2+\nu^2))}$.*

Proof: As in the proof Lemma 7 we consider B_H as a bivariate polynomial in $\mathbb{Z}[L_H, x]$, and

$$\begin{aligned} |\mathsf{disc}(B_H)| &= \left| \frac{1}{b_d(L_H)} \mathtt{res}_x(B_H(L_H,x), \partial B_H(L_H,x)/\partial x) \right| \\ &= \left| \frac{1}{b_d(L_H)} R_B(L_H) \right| \ . \end{aligned} \tag{7}$$

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

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

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

$$|L_H - \rho_1| \geq \exp(-\widetilde{\mathcal{O}}(d^6 n^8 \nu^4 \tau(\nu^2 + \tau^2))) \ .$$

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

$$|R_B(L_H)| \geq \exp(-\widetilde{\mathcal{O}}(d^6 n^8 \nu^4 \tau(\nu^2 + \tau^2))) \ .$$

Combining Eq. (7) with the previous inequality and Lemma 15 we get

$$2^{-\widetilde{\mathcal{O}}(d^6 n^8 \nu^4 \tau(\nu^2+\tau^2))} \leq |\mathsf{disc}(B_H)| \leq 2^{\widetilde{\mathcal{O}}(d\nu + d\tau + n^{10}\nu^4\tau(\tau^2+\nu^2))} \ ,$$

that concludes the proof. □

Lemma 17. *Let B_H be as in Problem 2 and let β_j be its roots. Then*

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

$$\Sigma(B_H) = -\lg \prod_{(i,j)\in\Omega} |\beta_i - \beta_j| \widetilde{\mathcal{O}}(d^6 n^8 \nu^4 \tau(\nu^2+\tau^2)) .$$

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.

5.1 Isolating the real roots of B_H

We proceed as in Section 3.1 and we use the same notation. We approximate the coefficients of B_H up to accuracy $\mathcal{O}(d\rho + \Sigma(B_H))$ and we isolate the real roots in $\widetilde{\mathcal{O}}_B(d^3 + d^2\sigma + d\Sigma(B_H))$. From Lemma 17 we get $\Sigma(B_H) = \widetilde{\mathcal{O}}(d^6 n^8 \nu^4 \tau(\nu^2+\tau^2))$. Moreover, $\rho = \widetilde{\mathcal{O}}(n^{10}\nu^4\tau(\tau^2+\nu^2))$ and $\sigma = \widetilde{\mathcal{O}}(n^{10}\nu^4\tau(\tau^2+\nu^2))$.

We need to estimate the cost of approximating $b_i(L_H)/b_d(L_H)$ up to accuracy of $\mathcal{O}(d\rho + \Sigma(B_H))$ bits after the binary point. Working as in Section 3.1 we deduce that we should approximate $L_H = \lg A(\gamma_1, \gamma_2)$ up to precision 2^{-t}, where $t = \mathcal{O}(d\rho + \Sigma(B_H))$. The cost of this approximation is quasi-linear $\widetilde{\mathcal{O}}_B(t)$ [6].

In addition, 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 $\widetilde{\mathcal{O}}_B(n^2\tau + ns) = \widetilde{\mathcal{O}}_B(n^2\tau + nm\tau + nt)$ [27].

It remains to estimate the cost of computing the approximated coefficients of B_H. After we have computed a approximation of L_H, say $\tilde{L}_H$, we need perform the evaluation $b_i(\tilde{L}_H)$; there are $d+1$. Each costs $\widetilde{\mathcal{O}}_B(\nu s)$ and the overall cost is $\widetilde{\mathcal{O}}_B(d\nu s)$.

Combining all the bounds we have the following theorem

Theorem 18. *The Boolean complexity of isolating the real roots of B_H of Problem 2 is $\widetilde{\mathcal{O}}_B(n^9\nu^4 d^2\tau(\tau^2+\nu^2)(n^2+d^5) + m\tau(n+d\nu))$.*

6. AN EXTENSION TO BIVARIATE POLYNOMIAL SYSTEMS

In this section we consider bivariate polynomial systems. Let $L = L_q$ or $L = L_H$ (Section 3 and Section 5, 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 present the separation bounds and we sketch the analysis of isolation process. We use the `DMM` bound [15]. 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, $R_1 \in (\mathbb{Z}[L])[u]$, which is called the u-resultant. The `DMM` bound bounds the separation of S_L using the separation bound of R_1. Asymptotically, the latter depends on a lower bound on the discriminant of its square-free part [15, Thm. 3]. Hence, it suffices to estimate this bound.

The coefficients of R_1 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_1 wrt u is $\mathcal{O}(d^2)$.

Recall that the coefficients of $F_{\{1,2\}}$ are polynomials in L. Thus, the coefficients of R_1 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_1, then its coefficients are polynomials of degree bounded by $2d\nu$ and of maximum coefficient bitsize bounded by $2d\tau + 10d\lg(d) = \widetilde{\mathcal{O}}(d\tau)$ [36]. If $L = L_\alpha$ then we apply Lemma 7 and the logarithm of the separation bound of the system is $\widetilde{\mathcal{O}}(d^7\nu^{10}m^4\tau(\nu^2+d^2\tau^2))$. We can obtain a similar bound if $L = L_H = \lg A(\gamma_1,\gamma_2)$ and we apply Lemma 16. In both cases, it seems that the bounds are quite pessimistic. We can also obtain the bounds by modifying accordingly the `DMM` bound [15].

To compute R_1 (or R_2 if we choose to eliminate x_2) we treat L as a new variable. The projection on x_1, that is the computation of R_1 costs $\widetilde{\mathcal{O}}_B(d^5\nu\tau)$ ([10, Prop. 8 and Lemma 9]). The cost is the same for projection on the x_2-axis. Using the previous bounds and the results of Sections 3.1 and 5.1 we can isolate the roots of the two projections. For the L_α case this cost is $\widetilde{\mathcal{O}}_B(d^2\nu^4 + d^8\nu^{12}m^4\tau(\nu^2+d^2\tau^2))$. It remains to match the x_1 and x_2 coordinates. For example, we can use one of the three strategies in [10]. The main operation needed is the computation of sign of a univariate polynomial like B_α evaluated at a real algebraic number. We postpone the detailed analysis for a future communication

Another way to solve the system is to approximate L up to an accuracy, substitute this value to the polynomials $F_{\{1,2\}}$, and then solve the system. We need a perturbation bound for the roots of a bivariate system, similar to the one(s) for univariate polynomials [30, Theorem 19.1].

Theorem 19. *Consider a 0-dimensional polynomial system $F = 0$, where $F = (F_1, F_2)$ and $F_{\{1,2\}}$ are bivariate polynomials of degree d. The roots of system are contained in a disc with center the origin and radius r. Let $\widetilde{F} = (\widetilde{F}_1, \widetilde{F}_2)$ be a λ approximation of F, that is $\|F_i - \widetilde{F}_i\|_\infty \leq 2^{-\lambda}$. Then the zeros of F, $\alpha_1, \ldots, \alpha_{d^2}$, and the zeros of $\widetilde{F}$, $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_{d^2}$,*

could be numbered such that, for $j \in [n]$,

$$|\alpha_j - \widetilde{\alpha}_j| \leq 2^{\eta+1},$$

where $\eta = -\lambda/d^2 + 2\tau/d^2 + 12\lg(2d))/d + 4\lg(d)/d^2 + \lg(r) + 2$.

Proof: We consider the polynomial system (S_0) and its resultant, R; after eliminating x_1 and x_2. 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 $|\varrho_k| \leq (d^2+2)^{2d}$. The degree of R wrt u is $\mathcal{O}(d^2)$.

If we replace the polynomials $F_{\{1,2\}}$ by it approximations $\widetilde{F}_{\{1,2\}}$ and compute the resultant of the perturbed system, $\widetilde{R}$, this is also a polynomial in u of degree $\mathcal{O}(d^2)$. Its terms are of the form $\varrho_k\, \widetilde{c}_1^d\, \widetilde{c}_2^d\, u^k$, where $0 \leq k \leq d^2$, $\widetilde{c}_{\{1,2\}}$ denotes a monomial in the coefficients of $\widetilde{F}_{\{1,2\}}$ of total degree d, and ϱ_k is as before.

The inequality $\|F_i - \widetilde{F}_i\|_\infty \leq 2^{-\lambda}$ implies $\|R - \widetilde{R}\|_\infty \leq 2^{-\lambda+2d\tau+12d\lg(2d)}$.

Let $\alpha_{j,1}$, for $j \in [d^2]$, be the roots of R, and respectively $\widetilde{\alpha}_{j,1}$ the roots of $\widetilde{R}$. Recall that the roots of R are the x_1 coordinates of the system. Using [30, Theorem 19.1] we have the following inequality $|\alpha_{i,1} - \widetilde{\alpha}_{i,1}| \leq 2^\eta$ where $\eta = -\lambda/d^2 + 2\tau/d^2 + 12\lg(2d))/d + 4\lg(d)/d^2 + \lg(r) + 2$.

We obtain the same bound if we replace $u - x_1$ with $u - x_2$ in (S_0). Thus, for any root α_j of F and $\widetilde{\alpha}_i$ of $\widetilde{F}$ we have $|\alpha_i - \widetilde{\alpha}_i| \leq 2^{\eta+1}$. □

Using the previous theorem we can mimic the procedure of the univariate case. We estimate the separation bound of (S_0) as presented in the beginning of the section. Next, we approximate L to an accuracy of this order, and we obtain two approximate polynomials, and thus a perturbed system. We solve the approximate system using a numerical subdivision solver, e.g [21], and from the isolating boxes of the perturbed system we can derive isolating boxes for the roots of (S_0) by applying Thm 19.

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 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.

7. 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] M. Bodrato and A. Zanoni. Long integers and polynomial evaluation with Estrin's scheme. In *Proc. 11th Int'l Symp. on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, pages 39–46. IEEE, 2011.

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

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

[8] 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.

[9] 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.

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

[11] 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.

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

[13] 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.

[14] 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.

[15] 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.

[16] D. Eppstein, M. S. Paterson, and F. F. Yao. On nearest-neighbor graphs. *Discrete & Computational Geometry*, 17(3):263–282, 1997.

[17] 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.

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

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

[20] 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.

[21] A. Mantzaflaris, B. Mourrain, and E. P. Tsigaridas. On continued fraction expansion of real roots of polynomial systems, complexity and condition numbers. *Theoretical Comput. Sci.*, 412(22):2312–2330, 2011.

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

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

[24] K. Mehlhorn, M. Sagraloff, and P. Wang. From approximate factorization to root isolation with application to cylindrical algebraic decomposition. *Journal of Symbolic Computation*, 66(0):34 – 69, 2015.

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

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

[27] 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.

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

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

[30] 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.

[31] 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.

[32] 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.

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

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

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

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

APPENDIX

The following is an alternative version of Lemma 2.

Lemma 20. *Let $L \in \mathbb{C}$ and γ_1 the root of the square-free polynomial f that is closest to L. Then*

$$|f(L)| \geq |a_d|^2 \, |L-\gamma_1| \, 2^{-d} \, \mathcal{M}(f) \, 2^{\lg \prod_j \Delta_j} \quad .$$

Proof: As γ_1 is the root closest to L it holds $|L-\gamma_i| \geq |\gamma_1-\gamma_i|/2$. Then

$$\begin{aligned}
|f(L)| &= |a_d| \prod_{j=1}^{d} |L-\gamma_j| = |a_d||L-\gamma_1| \prod_{j\neq 1} |L-\gamma_j| \\
&\geq |a_d||L-\gamma_1| \prod_{j\neq 1} |\gamma_1-\gamma_j|/2 \\
&\geq |a_d| \, |L-\gamma_1| \, 2^{1-d} \prod_{j\neq 1} |\gamma_1-\gamma_j| \\
&\geq |a_d| \, |L-\gamma_1| \, 2^{1-d} \prod_{j\neq 1} \Delta_j \\
&\geq |a_d| \, |L-\gamma_1| \, 2^{1-d} \frac{1}{\Delta_1} \prod_{j} \Delta_j \\
&\geq |a_d| \, |L-\gamma_1| \, 2^{1-d} \frac{|a_d|}{2\mathcal{M}(f)} 2^{\lg \prod_j \Delta_j} \quad .
\end{aligned}$$

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