



HAL
open science

Root Separation for Trinomials

Pascal Koiran

► **To cite this version:**

Pascal Koiran. Root Separation for Trinomials. Journal of Symbolic Computation, 2019, 95, pp.151-161. ensl-01585049v3

HAL Id: ensl-01585049

<https://ens-lyon.hal.science/ensl-01585049v3>

Submitted on 24 Oct 2018

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

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

Root Separation for Trinomials

Pascal Koiran

LIP*, Ecole Normale Supérieure de Lyon, Université de Lyon.

October 25, 2018

Abstract

We give a separation bound for the complex roots of a trinomial $f \in \mathbb{Z}[X]$. The logarithm of the inverse of our separation bound is polynomial in the size of the sparse encoding of f ; in particular, it is polynomial in $\log(\deg f)$. It is known that no such bound is possible for 4-nomials (polynomials with 4 monomials). For trinomials, the classical results (which are based on the degree of f rather than the number of monomials) give separation bounds that are exponentially worse.

As an algorithmic application, we show that the number of real roots of a trinomial f can be computed in time polynomial in the size of the sparse encoding of f . The same problem is open for 4-nomials.

1 Introduction

Root separation is a classical topic in the study of polynomials in a real or complex variable. As a motivation, note for instance that a lower bound on the separation between the real roots of a polynomial provides information on the accuracy with which each real root should be approximated in order to obtain isolating intervals. The following inequality due to Mahler [12] (see also [15]) is an example of a well-known result on root separation. More recent results can be found e.g. in [3, 4].

Theorem 1 (Mahler). *Let $f \in \mathbb{Z}[X]$ be a squarefree (i.e., without multiple roots) polynomial of degree $d \geq 2$. If x_1, x_2 are two distinct complex roots of f we have*

$$|x_1 - x_2| > \sqrt{3}(d+1)^{-(2d+1)/2} H^{-d+1}$$

where H denotes the maximum of the absolute values of the coefficients of f .

The first result of this paper is a separation bound for the real roots of a trinomial, which we later extend to complex roots.

*UMR 5668 ENS Lyon, CNRS, UCBL. The author is supported by ANR project CompA (code ANR-13-BS02-0001-01). Email: Pascal.Koiran@ens-lyon.fr

Theorem 2. Consider a nonzero trinomial $f(x) = ax^\alpha + bx^\beta + cx^\gamma \in \mathbb{Z}[X]$ where $\alpha < \beta < \gamma$ and $\log \max(|a|, |b|, |c|, \alpha, \beta, \gamma) \leq s$ for some $s \geq 1$. For any two distinct real roots x_1, x_2 of f we have $|x_1 - x_2| \geq \exp(-Cs^3)$ where C is an absolute constant.

For a polynomial $f(X) = \sum_{i=1}^k a_i X^{\alpha_i} \in \mathbb{Z}[X]$ with k nonzero coefficients, let us define the sparse size of f as the sum of the bit sizes¹ of the coefficients and exponents of f , i.e., as

$$\sum_{i=1}^k [\log(1 + |a_i|) + \log(1 + \alpha_i)]. \quad (1)$$

We sometimes use the name "size of the sparse encoding of f " for the same quantity. For $K = \mathbb{R}$ or $K = \mathbb{C}$, we denote by $\sigma_K(f)$ the separation of the real (respectively, complex) roots of f , i.e., the minimum distance between two distinct roots of f in K ; and we denote the inverse of this number by $\sigma_K^{-1}(f)$. Theorem 2 therefore shows that the real roots of trinomials are well separated, i.e., $\log(\sigma_{\mathbb{R}}^{-1}(f))$ is polynomially bounded in the sparse size of f . This is already false for polynomials with 4 terms: Michael Sagraloff [18] has given a family of examples showing that for 4-nomials, $\log \sigma_{\mathbb{R}}^{-1}(f)$ can be exponential in the sparse size of f . Note also that in Theorem 1, $\log \sigma_{\mathbb{C}}^{-1}(f)$ is polynomial (in fact, almost linear) in $\deg f$ rather than in $\log(\deg f)$, and this is unavoidable in the dense case [15].

As an algorithmic application of Theorem 2 we show that the number of real roots of a trinomial f can be computed in time polynomial in the sparse size of f . Our model of computation is the standard Turing machine model. An algorithm for the same problem was already proposed in [17] but their computational model is different: instead of the Turing machine model, they use an arithmetic model (i.e., they count the number of arithmetic operations of their algorithm rather than the number of bit-level operations).

The proof of Theorem 2 is fairly short but somewhat technical. Here is an overview of the argument. It follows from Descartes' rule of signs that a polynomial with t monomials has at most $t - 1$ positive real roots. For a trinomial we have at most 2 positive real roots, and a grand total of 5 real roots at most. The hardest task is to separate two roots of the same sign. Assume for instance that $0 < x_1 < x_2$. By Rolle's theorem there must exist a point m between the two roots where $f'(m) = 0$. Dividing by x^α if necessary, we can assume that f has a nonzero constant term. Hence f' is a binomial and we can compute explicitly m and $f(m)$. The lower bound on $|x_1 - x_2|$ then follows from two ingredients:

- (i) We use Baker's theorem on linear forms in logarithms to show that $|f(m)|$ cannot be "too small."

¹Throughout the paper, \log will denote the natural logarithm.

(ii) We show that $|f'|$ cannot be “too large” on $[0, m]$.

A lower bound on $m - x_1$ follows from (i) and (ii), and this is in turn a lower bound on $x_2 - x_1$. Step (ii) is elementary but can only be achieved under an additional assumption on the exponents β and γ such as e.g. $\gamma \geq 2\beta$. Fortunately, if this condition is not satisfied we can work with the reciprocal polynomial $f^R(x) = x^\gamma f(1/x)$ instead.

In the computer science literature, Baker’s theorem was used by Eteessami et al. [7] to compare “succinctly represented integers.” The same result² was published a little earlier by Bastani et al. [2] with essentially the same proof (instead of Baker’s theorem, they rely on a variation by Nesterenko). We use Baker’s theorem in essentially the same way as [2] and [7], but instead of a comparison algorithm we derive a separation bound.

The role of Rolle’s theorem in the proof of Theorem 2 is the main obstacle toward a separation result for complex roots. There is fortunately a significant body of work on adaptations of Rolle’s theorem to the complex domain (see e.g. [14]). We use the Grace-Heawood theorem and a variation due to Marden [13].

Organization of the paper

We begin in Section 2 with a proof of our separation bound for real roots (Theorem 2) because it is simpler than the corresponding proof for the complex domain, and it provides the ingredients needed for our algorithmic application. This application (counting the number of real roots of a trinomial in polynomial time) appears in Section 3. In Section 4 we extend Theorem 2 to complex roots, first for squarefree trinomials and then in Theorem 18 for all trinomials. We conclude in Section 5 with two open problems. Throughout the paper, C_1, C_2, \dots denote suitable positive constants.

2 Separation of Real Roots

In this section we give a proof of Theorem 2. Baker’s theorem on linear forms in logarithms is our main tool. More precisely, we use the following version by Baker and Wüstholz [1].

Theorem 3. *Given two real numbers $s, t \geq 1$, let $a = (a_1, \dots, a_n)$ be a list of n positive rational numbers such that $a_i = p_i/q_i$ where the positive integers p_i, q_i satisfy $\log \max(p_i, q_i) \leq s$ for all i ; let $b = (b_1, \dots, b_n)$ be a list of n arbitrary integers such that $\log |b_i| \leq t$ for all i . Let*

$$\Lambda(a, b) = b_1 \log a_1 + b_2 \log a_2 + \dots + b_n \log a_n.$$

²Eteessami et al. then give an application to maximum probability parsing, a topic that is not considered in [2] or in the present paper.

If $\Lambda(a, b) \neq 0$ then $|\Lambda(a, b)| \geq \exp[-C(n)ts^n]$, where

$$C(n) = 18(n+1)!n^{n+1}32^{n+2}\log(2n).$$

The theorem established in [1] is in fact more general: the a_i 's are allowed to be algebraic numbers rather than just integers. The version stated in [7] is *less* general than Theorem 3 since it considers only the case when the a_i 's are integers. That paper also provides a detailed discussion, geared towards the nonexpert in number theory, of the translation from the general statement in [1] (where the role of the absolute value of integers is played by the Weil height of algebraic numbers) to a more elementary setting.

We will need to apply Theorem 3 for $n = 2$ only. Note that a linear form in 2 logarithms of rational numbers can obviously be rewritten as a linear form in 4 logarithms of integers. However, this would result in a severe degradation of our bounds due to the presence of the factor s^n in the lower bound for $|\Lambda(a, b)|$ provided by Theorem 3.

Proposition 4. *Let $g(x) = a_1x^\beta + a_2$ where a_1, a_2 are two nonzero integers and β is a positive rational number. Write $\beta = \beta_1/\beta_2$, where β_1 and β_2 are positive integers. We evaluate the binomial g at a rational point p/q where p, q are positive integers.*

Assume that $\log \max(p, q, |a_1|, |a_2|) \leq s$ and $\log \max(\beta_1, \beta_2) \leq t$ where $s, t \geq 1$. If $g(p/q) \neq 0$ then $|g(p/q)| \geq \exp(-C_1ts^2)$.

Proof. We can assume that a_1 and a_2 are of opposite signs: otherwise, $|g(p/q)| \geq |a_2| \geq 1$. Assume for instance that $a_2 < 0$ and $a_1 > 0$.

In order to compare $a_1(p/q)^\beta$ to $|a_2|$, we compare the logarithms of these numbers. Let

$$\delta = \log[a_1(p/q)^\beta] - \log |a_2| = [\beta_2 \log(a_1/|a_2|) + \beta_1 \log(p/q)]/\beta_2.$$

By Theorem 3, the absolute value of the numerator is lower bounded by $\exp[-C(2)ts^2]$. Since $\beta_2 \leq e^t$ we have $|\delta| \geq \exp[-C(2)ts^2 - t]$. Consider first the case $\delta > 0$. We have $\log[a_1(p/q)^\beta] = \log |a_2| + \delta$, therefore $a_1(p/q)^\beta \geq |a_2|e^\delta \geq |a_2|(1 + \delta)$ and $a_1(p/q)^\beta - |a_2| \geq |a_2|\delta \geq \exp[-C(2)ts^2 - t]$. We now turn our attention to the case $\delta < 0$, and distinguish two subcases.

(i) If $\delta \leq -1$ we have $a_1(p/q)^\beta \leq |a_2|/e$, hence $|g(p, q)| \geq |a_2|(1 - 1/e) \geq 1 - 1/e$.

(ii) If $-1 \leq \delta \leq 0$ then by convexity of the exponential function:

$$a_1(p/q)^\beta = |a_2|e^\delta \leq |a_2|[1 + \delta(1 - 1/e)].$$

Hence $a_1(p/q)^\beta - |a_2| \leq \delta(1 - 1/e)|a_2| \leq -(1 - 1/e)\exp[-C(2)ts^2 - t]$.

In all cases, $|g(p/q)| \geq \exp(-C_1ts^2)$ for some suitable constant $C_1 > C(2)$. \square

Lemma 5. Consider a trinomial $f(x) = a + bx^\beta + cx^\gamma \in \mathbb{Z}[X]$ where $\gamma > \beta$. If $f'(m) = 0$ at some point $m > 0$ then $m = |b\beta/c\gamma|^{1/(\gamma-\beta)}$ and

$$f(m) = a + b \left(1 - \frac{\beta}{\gamma}\right) m^\beta = a + b \left(1 - \frac{\beta}{\gamma}\right) \left|\frac{b\beta}{c\gamma}\right|^{\beta/(\gamma-\beta)}.$$

This follows from a routine calculation. Note that b and c must be nonzero.

Lemma 6. Consider a trinomial $f(x) = a + bx^\beta + cx^\gamma \in \mathbb{Z}[X]$ where $\gamma > \beta$, $a \neq 0$ and $\log \max(|a|, |b|, |c|, \beta, \gamma) \leq s$ for some $s \geq 1$. If $f'(m) = 0$ at some point $m > 0$ where $f(m) \neq 0$ then $|f(m)| \geq \exp(-C_2 s^3)$.

This follows from Lemma 5 and Proposition 4 (which we apply with $t = s$). Note that we need the hypothesis $a \neq 0$ in order to apply this proposition.

Lemma 7. Consider a trinomial $f(x) = a + bx^\beta + cx^\gamma \in \mathbb{Z}[X]$ where $\gamma \geq 2\beta$. If $f'(m) = 0$ at some point $m > 0$ then $\sup_{x \in [0, m]} |f'(x)| \leq b^2 \beta$.

Proof. The supremum is reached at 0, or at a point $r \in]0, m[$ where $f''(r) = 0$. We are in the first case if (and only if) $\beta = 1$, and then $f'(0) = b$. In the second case,

$$f'(r) = b\beta \left(1 - \frac{\beta-1}{\gamma-1}\right) \left|\frac{b\beta(\beta-1)}{c\gamma(\gamma-1)}\right|^{(\beta-1)/(\gamma-\beta)}. \quad (2)$$

This follows from a direct computation, or an application of Lemma 5 to $f'(x) = b\beta x^{\beta-1} + c\gamma x^{\gamma-1}$ (which we can treat as a trinomial without a constant term). Taking into account the condition $\gamma \geq 2\beta$, we see that the exponent $(\beta-1)/(\gamma-\beta)$ in (2) is smaller than 1. The result then follows from the crude upper bound: $\left|\frac{b\beta(\beta-1)}{c\gamma(\gamma-1)}\right| \leq |b|$. \square

Remark 8. In the previous lemma, we can bound $|f'|$ without using the second derivative of f . Since f' has a positive root, b and c must be of opposite signs. Hence for $x \geq 0$, $|f'(x)| = |b\beta x^{\beta-1} + c\gamma x^{\gamma-1}| \leq \max(|b|\beta x^{\beta-1}, |c|\gamma x^{\gamma-1})$ and $\sup_{x \in [0, m]} |f'(x)| \leq \max(|b|\beta m^{\beta-1}, |c|\gamma m^{\gamma-1}) = |b| \cdot \beta \cdot |b\beta/c\gamma|^{(\beta-1)/(\gamma-\beta)} \leq b^2 \beta$. This is the same bound as in the statement of Lemma 7, but slightly worse than (2). One advantage of the proof of Lemma 7 is that (2) shows that some relation between β and γ (such as $\gamma \geq 2\beta$) is necessary in order to obtain a good control on $|f'|$.

Before proving our root separation result, we recall Cauchy's bound [5]. A number of similar bounds can be found in [16], chapter 8.

Proposition 9. Let $P(X) = \sum_{i=0}^d a_i X^i$ be a complex polynomial of degree d . For any root x of P , we have

$$|x| \leq 1 + \max \left(\frac{|a_0|}{|a_d|}, \frac{|a_1|}{|a_d|}, \dots, \frac{|a_{d-1}|}{|a_d|} \right).$$

Corollary 10. Let $P(X) = \sum_{i=0}^d a_i X^i$ be a complex polynomial with $a_0 \neq 0$. For any root x of P , we have

$$|x| \geq \frac{1}{1 + \max \left(\frac{|a_d|}{|a_0|}, \frac{|a_{d-1}|}{|a_0|}, \dots, \frac{|a_1|}{|a_0|} \right)}.$$

Moreover, for a polynomial $f(X) = \sum_{i=0}^d f_i X^i \in \mathbb{Z}[X]$ with $|f_i| \leq M$ for all i , any nonzero root x of f satisfies $|x| \geq 1/(M+1)$.

The first part of this corollary follows from an application of Proposition 9 to the reciprocal polynomial $P^R(X) = X^d P(1/X)$. The second part follows from the first by factoring out the highest power of x which divides f . We can now give the proof of our main result.

Proof of Theorem 2. We first consider the case where one of the two roots, e.g. x_1 , is equal to 0. By the second part of Corollary 10 we have $|x_1 - x_2| \geq 1/(1 + e^s)$. If the two roots are nonzero and of opposite signs, for the same reason we have $|x_1 - x_2| \geq 2/(1 + e^s)$. It therefore remains to consider the case where the two roots are nonzero and of the same sign.

Assume for instance that $0 < x_1 < x_2$. The first coefficient a must be nonzero, otherwise f is a binomial and can have at most one positive root. Also, we may (and will) assume that $\alpha = 0$ by factoring out x^α if necessary. By Rolle's theorem, there is a point $m \in]x_1, x_2[$ where $f'(m) = 0$. Since f is a trinomial it can have at most two positive roots, hence $f(m) \neq 0$. We can therefore apply Lemma 6 and conclude that $|f(m)| \geq \exp(-C_2 s^3)$. Such a lower bound is useful because

$$|x_2 - x_1| \geq |m - x_1| \geq \frac{|f(m) - f(x_1)|}{\sup_{x \in [x_1, m]} |f'(x)|} \geq \frac{|f(m)|}{\sup_{x \in [0, m]} |f'(x)|}.$$

At this point, we need to distinguish two further cases.

(i) If $\gamma \geq 2\beta$ we can apply Lemma 7 and conclude that

$$|x_2 - x_1| \geq \frac{\exp(-C_2 s^3)}{b^2 \beta} \geq \exp(-C_2 s^3 - 3s).$$

(ii) If $\gamma < 2\beta$ we consider the reciprocal polynomial $f^R(x) = x^\gamma f(1/x) = c + bx^{\gamma-\beta} + ax^\gamma$. In f^R the ratio of the two highest exponents is

$$\frac{\gamma}{\gamma - \beta} = \frac{1}{1 - \beta/\gamma} \geq 2.$$

It follows that f^R falls within the scope of case (i); since $1/x_1$ and $1/x_2$ are roots of f^R , the lower bound from case (i) applies to $|\frac{1}{x_1} - \frac{1}{x_2}|$. This yields a lower bound on $|x_2 - x_1|$ since

$$|x_2 - x_1| = x_1 x_2 \left| \frac{1}{x_1} - \frac{1}{x_2} \right|$$

and we have already obtained the lower bound $x_2 \geq x_1 \geq 1/(1 + e^s)$.

We conclude that $|x_1 - x_2| \geq \exp(-Cs^3)$ in all cases, for some appropriate constant $C > C_2$. \square

3 Computing the Number of Real Roots

We now give an algorithmic application of Theorem 2.

Theorem 11. *The number of real roots of a trinomial $f(x) = ax^\alpha + bx^\beta + cx^\gamma \in \mathbb{Z}[X]$ can be computed in time polynomial in the sparse size of f .*

Proof. We will assume that the 3 coefficients a, b, c are nonzero: if one coefficient vanishes f is a binomial and we leave this easy case to the reader. It is also easy to reduce to the counting of positive roots: f has 0 as a root if and only if $\alpha > 0$, and the number of negative roots of f is the number of positive roots of $f(-x)$. It therefore remains to decide whether the input trinomial f has 0, 1 or 2 positive roots. Dividing by x^α if necessary, we will further assume that $\alpha = 0$. If a and c are of opposite signs, f has exactly one positive root: it must have a root since f takes opposite signs at 0 and $+\infty$, and for the same reason we cannot have two roots.

When a and c are of the same sign, there are 0 or 2 positive roots and we determine which of these two values is the correct one using Lemma 5. More precisely, assume for instance that a and c are positive. We'll have 2 positive roots if and only if there exists $m > 0$ such that $f'(m) = 0$ and $f(m) < 0$. By Lemma 5, we are in this case if and only if $b < 0$ and

$$\frac{a\gamma}{|b(\gamma - \beta)|} < \left| \frac{b\beta}{c\gamma} \right|^{\beta/(\gamma - \beta)}.$$

This is equivalent to

$$\left| \frac{a\gamma}{b(\gamma - \beta)} \right|^{\gamma - \beta} < \left| \frac{b\beta}{c\gamma} \right|^\beta,$$

and therefore to:

$$(a\gamma)^{\gamma - \beta} (c\gamma)^\beta < |b\beta|^\beta |b(\gamma - \beta)|^{\gamma - \beta}. \quad (3)$$

The latter inequality is an instance of the problem of comparing "succinctly represented integers" [7]. As pointed out above, it is shown in [7] and [2] how to solve this problem in polynomial time using Baker's theorem. \square

As pointed out by an anonymous referee, checking (3) amounts to computing the sign of the so-called “ A -discriminant” of the trinomial $a+bx^\beta+cx^\gamma$ (Proposition 1.8 in [8], chapter 9).

The first version of this paper³ claims that Theorem 11 follows from the algorithm of Jindal and Sagraloff [11] for the isolation of real roots of sparse polynomials. As pointed out by Michael Sagraloff (personal communication), this requires a more careful justification. I wrote that the complexity of their algorithm is polynomial in the sparse size of f and in $\log \sigma_{\mathbb{R}}^{-1}(f)$. This was a misstatement of their result: even if the real roots of f are well separated, their algorithm may not run in polynomial time if f has two conjugate complex roots with very small imaginary parts. In the full version of their paper [10], Jindal and Sagraloff show that the conjugate complex roots of trinomials are well separated. This implies that the real roots of trinomials can indeed be isolated in polynomial time. In their paper, Jindal and Sagraloff provide explicit constants for their separation bound. This is required for an actual implementation of their algorithm, especially for the correct treatment of double roots (see Section 9 of [10] for details). The fact that conjugate complex roots of trinomials are well separated also follows from the results of the next section, where we show that *all* complex roots of trinomials are well separated.

4 Separation of Complex Roots

In this section we show that the separation bound of Theorem 2 also applies to complex roots of trinomials. We begin with the the easy case of binomials. In this case, the nonzero roots are uniformly distributed on a circle.

Proposition 12. *Consider a binomial $f(x) = bx^\beta + cx^\gamma \in \mathbb{Z}[X]$ with $b, c \neq 0$ and $\beta < \gamma$. For any two complex roots x_1, x_2 of f we have:*

$$|x_1 - x_2| \geq \frac{1}{|c|} \sqrt{2 \left(1 - \cos \frac{2\pi}{\gamma - \beta} \right)}.$$

Proof. Set $\varepsilon = 1$ if b and c are of opposite signs, $\varepsilon = -1$ if they are of the same sign. The roots of f are the $\gamma - \beta$ numbers of the form $x = |b/c|^{1/(\gamma-\beta)} \xi$, where $\xi^{\gamma-\beta} = \varepsilon$. In addition, 0 is a root of multiplicity β if $\beta \geq 1$. The distance between the origin and any other root is $|b/c|^{1/(\gamma-\beta)} \geq 1/|c|$. The distance between any two other roots is at least

$$|1 - e^{2i\pi/(\gamma-\beta)}|/|c| = \frac{1}{|c|} \sqrt{2 \left(1 - \cos \frac{2\pi}{\gamma - \beta} \right)}.$$

□

³arxiv.org/abs/1709.03294v1

4.1 Squarefree trinomials

In order to extend Theorem 2 to the complex domain, a suitable adaptation of Rolle's theorem is needed. The following one is due to Grace and Heawood (see for instance Theorem 5.1 in Marden's survey [14]; for a proof, see Theorem 23.1 in his book [13] or Theorem 4.3.1 in [16]).

Theorem 13. *If z_1 and z_2 are two distinct roots of a polynomial $f \in \mathbb{C}[X]$ of degree n , then at least one zero of f' lies in the disk of center $M = (z_1 + z_2)/2$ and radius*

$$r = \frac{|z_1 - z_2|}{2} \cot(\pi/n).$$

Here is an analogue of Lemma 5:

Lemma 14. *Consider a trinomial $f(x) = a + bx^\beta + cx^\gamma \in \mathbb{Z}[X]$ where $\gamma > \beta$. If $f'(m) = 0$ at some point $m \in \mathbb{C}^*$ then $m = |b\beta/c\gamma|^{1/(\gamma-\beta)}\xi$ where $\xi^{\gamma-\beta} = \pm 1$. Moreover,*

$$f(m) = a + b \left(1 - \frac{\beta}{\gamma}\right) m^\beta = a + b \left(1 - \frac{\beta}{\gamma}\right) \left|\frac{b\beta}{c\gamma}\right|^{\beta/(\gamma-\beta)} \xi^\beta.$$

The complex analogue of Lemma 6 is:

Lemma 15. *Consider a trinomial $f(x) = a + bx^\beta + cx^\gamma \in \mathbb{Z}[X]$ where $\gamma > \beta$, $a \neq 0$ and $\log \max(|a|, |b|, |c|, \beta, \gamma) \leq s$ for some $s \geq 1$. If $f'(m) = 0$ at some point $m \in \mathbb{C}$ where $f(m) \neq 0$ then $|f(m)| \geq \exp(-C_3 s^3)$.*

Proof. At $m = 0$ we have $|f(m)| = |a| \geq 1$. It therefore remains to study the case $m \neq 0$. Consider the complex number ξ from Lemma 14. If ξ^β is real then $\xi^\beta = \pm 1$ and the result follows from Proposition 4 just like in Lemma 6.

If $\xi^\beta \notin \mathbb{R}$, let us write $\xi^\beta = \cos \theta + i \sin \theta$ with $\sin \theta \neq 0$. Define also:

$$r = b \left(1 - \frac{\beta}{\gamma}\right) \left|\frac{b\beta}{c\gamma}\right|^{\beta/(\gamma-\beta)}.$$

By Lemma 14 we have $f(m) = a + r(\cos \theta + i \sin \theta)$ so that

$$|f(m)|^2 = (a + r \cos \theta)^2 + (r \sin \theta)^2 = a^2 + r^2 + 2ar \cos \theta.$$

Consider now the case where a and r are of opposite signs. We have $|f(m)|^2 = (a + r)^2 + 2ar(\cos \theta - 1) \geq (a + r)^2$. If $a + r \neq 0$ then $|a + r| \geq \exp(-C_2 s^3)$ by Lemma 6 and we are done.

If $a + r = 0$ then $|f(m)|^2 = 2a^2(1 - \cos \theta) \geq 2(1 - \cos \theta)$. Recall from Lemma 14 that $\xi^{2(\gamma-\beta)} = 1$. Hence we may assume that $\theta = 2k\pi/n$ where $n = 2(\gamma - \beta)$ and $k \in \{1, \dots, 2n - 1\}$ ($k = 0$ is impossible due to the assumption $\sin \theta \neq 0$). To conclude, we note that $1 - \cos \theta \geq 1 - \cos(2\pi/n) \geq$

$1 - \cos(\pi/\gamma)$. For large values of γ we have $\cos(\pi/\gamma) = 1 - \pi^2/(2\gamma^2) + o(1/\gamma^2)$. Hence there is a constant γ_0 such that $\cos(\pi/\gamma) < 1 - 1/\gamma^2$ for all $\gamma \geq \gamma_0$. Under this condition we have $1 - \cos \theta \geq 1/\gamma^2 \geq e^{-2s}$ and $|f(m)| \geq e^{-s}$. For $\gamma < \gamma_0$ we have $|f(m)|^2 \geq 2(1 - \cos \theta) \geq 2[1 - \cos(\pi/\gamma)] > 2[1 - \cos(\pi/\gamma_0)]$. Since γ_0 is an absolute constant, there is a constant $c \geq 1$ such that the bound $|f(m)| \geq e^{-cs}$ applies to both cases $\gamma \geq \gamma_0$ and $\gamma < \gamma_0$.

The case where a and r are of the same sign is handled by a similar argument, noting that this time we have:

$$|f(m)|^2 = (a - r)^2 + 2ar(1 + \cos \theta) \geq (a - r)^2.$$

□

We are now ready to obtain a separation bound in the complex domain. As a first step, we consider only the case where f is squarefree.

Proposition 16. *Consider a nonzero squarefree trinomial $f(x) = ax^\alpha + bx^\beta + cx^\gamma \in \mathbb{Z}[X]$ where $\alpha < \beta < \gamma$ and $\log \max(|a|, |b|, |c|, \alpha, \beta, \gamma) \leq s$ for some $s \geq 1$. For any two distinct complex roots x_1, x_2 of f we have $|x_1 - x_2| \geq \exp(-C_4 s^3)$.*

Proof. If one of the two roots is equal to 0, the argument used in the proof of Theorem 2 (namely, Corollary 10) still applies. We will therefore assume that x_1 and x_2 are nonzero. Again, we assume that $\alpha = 0$ by factoring out x^α if necessary.⁴ Then we appeal to the complex version of Rolle's theorem: by Theorem 13 there is a point such that $f'(m) = 0$ in the disk of center $M = (x_1 + x_2)/2$ and radius

$$r = \frac{|x_1 - x_2|}{2} \cot(\pi/\gamma). \quad (4)$$

Since f is squarefree, $f(m) \neq 0$ so that $|f(m)| \geq \exp(-C_3 s^3)$ by Lemma 15. Let us denote by $I = [m, x_1]$ the line segment joining m to x_1 in the complex plane. Like in the real case, we have $|f(x_1) - f(m)| \leq |m - x_1| \sup_{z \in I} |f'(z)|$ so that

$$|m - x_1| \geq \frac{|f(m)|}{\sup_{z \in I} |f'(z)|}. \quad (5)$$

This lower bound on $|m - x_1|$ is useful since:

$$\frac{|x_1 - x_2|}{2} \cot(\pi/\gamma) \geq |m - M| \geq |m - x_1| - |x_1 - M| = |m - x_1| - |x_1 - x_2|/2.$$

The first inequality holds true because m belongs to the circle of center M and radius given by (4). As a result, we have

$$|x_1 - x_2| \geq \frac{2|m - x_1|}{1 + \cot(\pi/\gamma)}. \quad (6)$$

⁴We already have $\alpha \leq 1$ before the factorization since f is assumed to be squarefree.

If $m = 0$, the lower bound on $|x_1|$ from Corollary 10 recalled at the beginning of the proof applies to the the numerator of (6). As to the denominator, note that $\cot(\pi/\gamma) = \gamma/\pi + o(\gamma)$ for large γ . As a result there is a constant $A > 0$ such that $1 + \cot(\pi/\gamma) \leq A\gamma$ for all $\gamma \geq 1$. We therefore have a lower bound of the form $|x_1 - x_2| \geq \exp(-C_5s)$ in the case $m = 0$. This is better than the lower bound claimed in the statement of Proposition 16, so we'll assume that $m \neq 0$ in the remainder of the proof.

Our next goal is to bound $\sup_{z \in I} |f'(z)|$ in order to apply (5) and (6). Note that for $z \in I$ we have $|z| \leq \max(|m|, |x_1|)$. We distinguish two cases:

- (i) If $|x_1| \leq (1 + 1/\gamma)|m|$ then $|z| \leq (1 + 1/\gamma)|m|$ for all $z \in I$. We have $|f'(z)| \leq |b\beta||z|^{\beta-1} + |c\gamma||z|^{\gamma-1}$. Since $(1 + 1/\gamma)^\gamma \leq e$ we have for any $z \in I$:

$$|f'(z)| \leq e(|b\beta||m|^{\beta-1} + |c\gamma||m|^{\gamma-1}) = 2e|b\beta||m|^{\beta-1}.$$

From the explicit value $|m| = |b\beta/c\gamma|^{1/(\gamma-\beta)}$ computed in Lemma 14 we have

$$|f'(z)| \leq 2e|b\beta||b\beta/c\gamma|^{(\beta-1)/(\gamma-\beta)}. \quad (7)$$

At this point, like in the proof of Theorem 2 we need to throw in the additional assumption $\gamma \geq 2\beta$. Under this assumption, from (7) we have $|f'(z)| \leq 2eb^2\beta$. Combining (5) and (6) we have:

$$|x_1 - x_2| \geq \frac{\exp(-C_3s^3)}{eb^2\beta(1 + \cot(\pi/\gamma))},$$

which yields the desired bound. If $\gamma < 2\beta$, we work instead with the reciprocal polynomial f^R instead of f like in the proof of Theorem 2. Note that f^R is squarefree since f is.

- (ii) If $|x_1| \geq (1+1/\gamma)|m|$ then $|m-x_1| \geq |m|/\gamma$. Since $|m| = |b\beta/c\gamma|^{1/(\gamma-\beta)}$ we have $|m| \geq \exp(-2s)$. Inequality (6) then yields a lower bound of the form $|x_1 - x_2| \geq \exp(-C_5s)$, and we are done.

□

4.2 The general case

In order to obtain our final result on root separation, it remains to get rid of the assumption that f is squarefree. For this, we shall use a version of Theorem 13 that can take multiple zeros into account. The following result is due to Marden ([13], Theorem 25.1).

Theorem 17. *Let $f \in \mathbb{C}[X]$ be a polynomial of degree n . If z_1 and z_2 are two distinct roots of f of respective multiplicities k_1 and k_2 , then at least one zero*

p (different from z_1 and z_2) of f' lies in the disk of center $M = (z_1 + z_2)/2$ and radius

$$\rho = \frac{|z_1 - z_2|}{2} \cot(\pi/2q)$$

where $q = n + 1 - k_1 - k_2$.

For the present paper, the main advantage of Theorem 17 over Theorem 13 is not so much the role played by the multiplicities k_1, k_2 than the guarantee that p is distinct from z_1 and z_2 . As far as we know, there is no such guarantee in Theorem 13.

Theorem 18. *Consider a nonzero trinomial $f(x) = ax^\alpha + bx^\beta + cx^\gamma \in \mathbb{Z}[X]$ where $\alpha < \beta < \gamma$ and $\log \max(|a|, |b|, |c|, \alpha, \beta, \gamma) \leq s$ for some $s \geq 1$. For any two distinct complex roots x_1, x_2 of f we have $|x_1 - x_2| \geq \exp(-C_6 s^3)$.*

Proof. Like in the proofs of Theorem 2 and Proposition 18 we'll work without loss of generality under the assumptions $\alpha = 0$ and $\gamma \geq 2\beta$. Also, we only have to treat the case where the roots x_1 and x_2 are nonzero. Let m be the root of f' introduced in the proof of Proposition 18. In the case $f(m) \neq 0$, we have obtained in that proof the lower bound $|x_1 - x_2| \geq \exp(-C_4 s^3)$. If $f(m) = 0$, m is a double root of f and we can apply Theorem 17 with $z_1 = x_1$, $z_2 = m$, $k_1 = 1$ and $k_2 = 2$. Hence there exists a zero p of f' , distinct from m and x_1 , in the disk of center $M' = (x_1 + m)/2$ and radius

$$\rho = \frac{|x_1 - m|}{2} \cot \frac{\pi}{2(\gamma - 2)}.$$

Since m and p are two distinct roots of the binomial f' , by Proposition 12 we have

$$|m - p| \geq \frac{1}{|c\gamma|} \sqrt{2 \left(1 - \cos \frac{2\pi}{\gamma - 1} \right)}. \quad (8)$$

After this lower bound on $|m - p|$, we shall give an upper bound. Recall that m lies in the disk of center $M = (x_1 + x_2)/2$ and radius r defined in (4). By the triangle inequality,

$$|x_1 - m| \leq r + |x_1 - x_2|/2 = \frac{|x_1 - x_2|}{2} [1 + \cot(\pi/\gamma)], \quad (9)$$

hence

$$\rho \leq \frac{|x_1 - x_2|}{4} [1 + \cot(\pi/\gamma)] \cot \frac{\pi}{2(\gamma - 2)}. \quad (10)$$

Another application of the triangle inequality shows that

$$|m - p| \leq |m - M'| + \rho = |m - x_1|/2 + \rho.$$

From (9) and (10) we have

$$|m - p| \leq \frac{|x_1 - x_2|}{4} [1 + \cot(\pi/\gamma)] [1 + \cot \frac{\pi}{2(\gamma - 2)}]. \quad (11)$$

To conclude, we just have to put together (8) and (11). The first inequality provides a lower bound of the form $|m - p| \geq \exp(-C_7s)$ and the second one an upper bound of the form $|m - p| \leq \exp(C_8s)|x_1 - x_2|$. As a result, $|x_1 - x_2| \geq \exp(-(C_7 + C_8)s)$. \square

5 Final Remarks

In this paper we have obtained a separation bound for the complex roots of trinomials, and we have derived an (easier) algorithmic result: the number of real roots of a trinomial can be computed in polynomial time. We conclude with two open problems about trinomials and 4-nomials.

1. Is it possible to determine in polynomial time the sign of a trinomial f at a rational point? The algorithm should run in time polynomial in the bit size of the rational point p/q and of the sparse encoding of f as defined by (1).

The sign of a binomial at a rational point can be evaluated in polynomial time using Baker's theorem (this is a special case of the comparison problem for succinctly represented integers [2, 7]). In time polynomial in the sparse encoding of a polynomial $f \in \mathbb{Z}[X]$ (with any number of monomials) one can also compute its sign at an integer point [6], and one can determine all of its rational roots [9].

2. Is it possible to count the number of real roots of a 4-nomial f in time polynomial in the sparse size of f ? An algorithm for this problem was proposed in [2]. The authors perform an average-case analysis in the arithmetic model as well as in the Turing machine model. Like the present paper, they rely on Baker's theorem. Ideally, one would like to have an algorithm with a worst case polynomial running time in the Turing machine model.

Acknowledgements

I would like to thank Yann Bugeaud and Michael Sagraloff for their feedback on the first version of this paper. In particular, Michael Sagraloff pointed out that in Section 3 the appeal to the root isolation algorithm from his joint paper with Gorav Jindal [11] needed a more careful justification. Thanks also go to the anonymous referees for their careful reading of the manuscript and suggesting additional references.

References

- [1] Alan Baker and Gisbert Wüstholz. Logarithmic forms and group varieties. *J. Reine Angew. Math*, 442(19-62):34–57, 1993.

- [2] Osbert Bastani, Christopher J Hillar, Dimitar Popov, and Maurice Rojas. Randomization, sums of squares, near-circuits, and faster real root counting. *Contemporary Mathematics*, 556:145–166, 2011.
- [3] Yann Bugeaud, Andrej Dujella, Tomislav Pejkovic, and Bruno Salvy. Absolute real root separation. *arXiv preprint arXiv:1606.01131*, 2016.
- [4] Yann Bugeaud and Maurice Mignotte. Polynomial root separation. *International Journal of Number Theory*, 6(03):587–602, 2010.
- [5] Augustin Cauchy. *Mémoire sur la résolution des équations numériques et sur la théorie de l'élimination*. 1829.
- [6] Felipe Cucker, Pascal Koiran, and Steve Smale. A polynomial time algorithm for diophantine equations in one variable. *Journal of Symbolic Computation*, 27(1):21–29, 1999.
- [7] Kousha Etessami, Alistair Stewart, and Mihalis Yannakakis. A note on the complexity of comparing succinctly represented integers, with an application to maximum probability parsing. *ACM Transactions on Computation Theory (TOCT)*, 6(2):9, 2014.
- [8] Israel M. Gelfand, Mikhail Kapranov, and Andrei Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Birkhäuser, 1994.
- [9] Hendrik W. Lenstra, Jr. Finding small degree factors of lacunary polynomials. In *Number Theory in Progress*, pages 267–276, 1999.
- [10] Gorav Jindal and Michael Sagraloff. A polynomial time algorithm for computing real roots of sparse real polynomials. Expanded version of [11], in preparation.
- [11] Gorav Jindal and Michael Sagraloff. A polynomial time algorithm for computing real roots of sparse real polynomials. In *Proc. ISSAC 2017 (42nd International Symposium on Symbolic and Algebraic Computation)*. ACM Press, 2017.
- [12] Kurt Mahler. An inequality for the discriminant of a polynomial. *The Michigan Mathematical Journal*, 11(3):257–262, 1964.
- [13] Morris Marden. *Geometry of polynomials*. Number 3 in Mathematical Surveys and Monographs. American Mathematical Society, 1966.
- [14] Morris Marden. The search for a Rolle’s theorem in the complex domain. *The American Mathematical Monthly*, 92(9):643–650, 1985.
- [15] Maurice Mignotte. Some useful bounds. In *Computer algebra*, pages 259–263. Springer, 1982.
- [16] Qazi Ibadur Rahman and Gerhard Schmeisser. *Analytic theory of polynomials*. Number 26 in London Mathematical Society monographs (new series). Oxford University Press, 2002.
- [17] Maurice Rojas and Yinyu Ye. On solving univariate sparse polynomials in logarithmic time. *Journal of Complexity*, 21(1):87–110, 2005.
- [18] Michael Sagraloff. A near-optimal algorithm for computing real roots of sparse polynomials. In *Proc. ISSAC 2014 (39th International Symposium on Symbolic and Algebraic Computation)*, pages 359–366. ACM Press, 2014.