Root separation for reducible monic polynomials of odd degree

Andrej Dujella and Tomislav Pejković

Dedicated to the memory of Professor Sibe Mardešić

Abstract

We study root separation of reducible monic integer polynomials of odd degree. Let $\mathrm{H}(P)$ be the naïve height, $\mathrm{sep}(P)$ the minimal distance between two distinct roots of an integer polynomial $P(x)$ and $\mathrm{sep}(P) = \mathrm{H}(P)^{-e(P)}$. Let $e_r^*(d) = \limsup_{\deg(P)=d,\, \mathrm{H}(P)\to+\infty} e(P)$, where the limsup is taken over the reducible monic integer polynomials $P(x)$ of degree d. We prove that $e_r^*(d) \leq d-2$. We also obtain a lower bound for $e_r^*(d)$ for d odd, which improves previously known lower bounds for $e_r^*(d)$ when $d \in \{5, 7, 9\}$.

1 Introduction

All the polynomials that we deal with in this paper have integer coefficients. For any such polynomial, we can look at how close two of its real or complex roots can be. Since we can always find polynomials with distinct roots as close as desired, we need to introduce some measure of size for polynomials with which we can compare this minimal separation of roots. This is done by bounding the degree and most usually using the naïve height, that is, the maximum of the absolute values of the coefficients of a polynomial.

The problem of minimal root separation for polynomials with fixed degree has been completely solved only in the trivial case of quadratic polynomials. Best possible separation exponent is also known for nonmonic cubic polynomials (see [7, 10]). For monic cubic polynomials, complete resolution would

[0]2010 Mathematics Subject Classification: 11C08, 12D10, 11B37.

Key words: integer polynomials, root separation.

The authors were supported by the Croatian Science Foundation under the project no. 6422. A. D. acknowledges support from the QuantiXLie Center of Excellence.

be equivalent to proving or disproving the well known Hall's conjecture [5]. Therefore, resolving the problem completely for polynomials of larger degree seems entirely out of reach.

However, if we restrict ourselves to reducible monic polynomials, then the cubic case becomes easy and the quartic case has been solved by the authors [6]. Thus, we are interested in the separation properties of the reducible monic polynomials of degree at least 5.

Let $P(x)$ be a polynomial of degree $d \geq 2$, naïve height $\mathrm{H}(P)$ and with at least two distinct roots. The *polynomial root separation* of $P(x)$ is

$$\mathrm{sep}(P) := \min_{\substack{P(\alpha)=P(\beta)=0,\\ \alpha\neq\beta}} |\alpha - \beta|.$$

The quantity $e(P)$ is defined by

$$\mathrm{sep}(P) = \mathrm{H}(P)^{-e(P)}.$$

Following the notation introduced in [5], for $d \geq 2$, we set

$$e(d) := \limsup_{\deg(P)=d,\, \mathrm{H}(P)\to+\infty} e(P)$$

and

$$e_r^*(d) := \limsup_{\deg(P)=d,\, \mathrm{H}(P)\to+\infty} e(P),$$

where the latter limsup is taken over the reducible monic integer polynomials $P(x)$ of degree d.

There are some other variants of polynomial root separation problem like p-adic root separation, where $|\alpha - \beta|$ is replaced by $|\alpha - \beta|_p$ (see [9]), and absolute root separation, where $|\alpha - \beta|$ is replaced by $||\alpha| - |\beta||$ (see [4]), but they will not be treated in this paper.

Obviously, we have $e(d) \geq e_r^*(d)$. A classical result of Mahler [8] says that $e(d) \leq d - 1$ for every $d \geq 2$. It is easy to see that $e_r^*(2) = 0$ and $e_r^*(3) = 1$, while the main result of [6] shows that $e_r^*(4) = 2$. The best current lower bounds for the values we are interested in are $e_r^*(5) \geq 2$ from [5] and the following general result by Bugeaud and Dujella [3]

$$e_r^*(d) \geq \frac{2d}{3} - 1 \text{ for even } d \geq 6, \quad e_r^*(d) \geq \frac{2d}{3} - \frac{5}{3} \text{ for odd } d \geq 7.$$

In particular, this implies that $e_r^*(7) \geq 3$ and $e_r^*(9) \geq \frac{13}{3}$. The mentioned result from [3] is obtained by constructing the parametric family of polynomials $Q_{d,n}(x) = (x^2 - (n^2 + 3n + 1)x + (n + 2))q_{d-2,n}(x)$, where $q_{d-2,n}(x)$ is a

recursive sequence of polynomials of even degree. For d odd, the polynomials $Q_{d,n}(x) = x(x^2 - (n^2 + 3n + 1)x + (n + 2))q_{d-3,n}(x)$ were used, so it is not surprising that results for odd degrees are sightly weaker and, in particular, for $d = 5$ the lower bound $e_r^*(5) \geq \frac{5}{3}$ from [3] is weaker than the bound $e_r^*(5) \geq 2$ from [5].

In this paper, we mainly consider odd degree polynomials. In Section 2 we improve the upper bound $e_r^*(d) \leq d-1$ which follows from [8] by proving that $e_r^*(d) \leq d-2$ for $d \geq 2$. In Section 3, we will construct a parametric family of reducible monic polynomials of odd degree with good root separation properties. Although the obtained lower bound will be asymptotically weaker compared with the bound from [3], it will improve all previously known lower bounds on $e_r^*(d)$ for $d \in \{5, 7, 9\}$. We show that

$$e_r^*(5) \geq \frac{7}{3}, \quad e_r^*(7) \geq \frac{17}{5}, \quad e_r^*(9) \geq \frac{31}{7}.$$

2 Upper bounds

Our first goal is to we improve the upper bound $e_r^*(d) \leq d-1$ which follows from [8] by proving that $e_r^*(d) \leq d-2$ for $d \geq 2$. Note that we already know that $e_r^*(d) = d-2$ for $d = 2, 3, 4$, so we may assume $d \geq 5$ here.

Let $P(x)$ be a monic polynomial of degree d, reducible over the rationals. Gauss's Lemma shows that we can factor $P(x)$ into two nonconstant monic polynomials with integer coefficients. If $P(x) = Q(x)R(x)$, where $Q(x)$ and $R(x)$ are integer polynomials of positive degrees n and m, respectively, and $\alpha, \beta \in \mathbb{C}$ are such that $Q(\alpha) = R(\beta) = 0$, then a version of Liouville's inequality (see [1, Theorem A.1]) ensures that

$$|\alpha - \beta| \gg \mathrm{H}(Q)^{-m}\,\mathrm{H}(R)^{-n}, \tag{1}$$

where the constant implied in the Vinogradov symbol $\gg$ here and further on depends only on m and n.

Gelfond's Lemma [1, Lemma A.3] says that

$$2^{-m-n}\,\mathrm{H}(Q)\,\mathrm{H}(R) \leq \mathrm{H}(P) \leq 2^{m+n}\,\mathrm{H}(Q)\,\mathrm{H}(R). \tag{2}$$

Now (1) and (2) and the fact that $\mathrm{H}(Q) \geq 1$, $\mathrm{H}(R) \geq 1$ give

$$|\alpha - \beta| \gg \mathrm{H}(P)^{-\max\{m,n\}}.$$

Mahler's general result shows that

$$\mathrm{sep}(Q) \gg \mathrm{H}(Q)^{-n+1} \gg \mathrm{H}(P)^{-n+1} \tag{3}$$

and

$$\operatorname{sep}(R) \gg \mathrm{H}(R)^{-m+1} \gg \mathrm{H}(P)^{-m+1}. \tag{4}$$

Combining the last three inequalities, we obtain

$$\operatorname{sep}(P) \gg \mathrm{H}(P)^{-\max\{m,n\}}. \tag{5}$$

If $\min\{m,n\} \geq 2$, we have $\max\{m,n\} \leq d-2$ and (5) shows that $\operatorname{sep}(P) \gg \mathrm{H}(P)^{-d+2}$.

We see that the only case that needs to be considered more thoroughly in order to prove the upper bound $e_r^*(d) \leq d-2$ is when one of the polynomials $Q(x)$, $R(x)$ is linear and we have a root of $Q(x)$ and a root of $R(x)$ which are very close. Without loss of generality, assume that $Q(x) = x - c$, $R(c) \neq 0$ and $R(c+\varepsilon) = 0$, where c is an integer and ε is small, but nonzero, say $0 < |\varepsilon| < 1$.

An easy bound $|c+\varepsilon| \leq m\,\mathrm{H}(R)$ is obtained by substituting $x = c+\varepsilon$ into $R(x)$ and comparing the leading term with the rest.

If $|c+\varepsilon| \geq 3$, then $|c+\varepsilon| \geq |c|-|\varepsilon| \geq |c|-1 \geq |c|/2$ since $|c| \geq |c+\varepsilon|-|\varepsilon| \geq |c+\varepsilon|-1 \geq 2$. The first inequality in (2) together with $\mathrm{H}(Q) = \max\{1,|c|\}$ and $|c|/2 \leq |c+\varepsilon| \leq m\,\mathrm{H}(R)$ gives

$$|c| \ll \mathrm{H}(P)^{1/2}. \tag{6}$$

In case $|c+\varepsilon| < 3$, we have $|c| \leq |c+\varepsilon| + |\varepsilon| < 4$ and since $\mathrm{H}(P) \geq 1$, inequality (6) also holds.

Rolle's mean value theorem gives

$$1 \leq |R(c)| = |R(c+\varepsilon) - R(c)| = |R'(t)| \cdot |\varepsilon|, \tag{7}$$

where t is between c and $c+\varepsilon$ and thus in the interval $(c-1, c+1)$. Since

$$\mathrm{H}(R') \leq m\,\mathrm{H}(R) \ll \mathrm{H}(P) \quad \text{and} \quad |t| < |c| + 1 \ll \mathrm{H}(P)^{1/2},$$

we have

$$|R'(t)| \ll \mathrm{H}(P)^{\frac{m-1}{2}} + \mathrm{H}(P) \cdot \mathrm{H}(P)^{\frac{m-2}{2}} \ll \mathrm{H}(P)^{\frac{m}{2}},$$

where we used the fact that $R(x)$ is monic and $R'(x)$ is of degree $m-1$. Comparing with (7), we obtain

$$|\varepsilon| \gg \mathrm{H}(P)^{-m/2} \gg \mathrm{H}(P)^{-(d-1)/2} \gg \mathrm{H}(P)^{-d+3} \tag{8}$$

since $d \geq 5$ (we get $|\varepsilon| \gg \mathrm{H}(P)^{-(d-1)/2} \gg \mathrm{H}(P)^{-d+2}$ for $d \geq 3$).

Hence, we proved the following theorem.

Theorem 1. *For $d \geq 2$, it holds that $e_r^*(d) \leq d-2$.*

3 Lower bounds

We would like to improve the lower bound $e_r^*(5) \geq 2$ from [5]. By (8), we see that this bound cannot be improved by considering degree 5 polynomials which have a linear factor. Thus, we have to consider products of two monic polynomials of degrees 2 and 3.

We made some experiments in order to find suitable degree 5 polynomials with $e(P) > 2$. We consider monic cubic polynomials with coefficients of moderate size. For such a polynomial, we choose one of its real roots γ and then apply the LLL-algorithm to a matrix of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ N & \lfloor N\gamma \rceil & \lfloor N\gamma^2 \rceil \end{pmatrix},$$

with suitably chosen large positive integer N, to construct quadratic polynomials with a root close to γ (the method is explained e.g. in [11, Chapter 6]). Among the polynomials obtained in the experiments, we have noted two collections of polynomials with $e(P)$ approaching $\frac{7}{3}$:

$$s_n(x) = (x^3 - 2nx^2 + (2-2n)x + 2)(x^2 + (-2n^2 - 2n)x + 2n + 2)$$

and

$$p_n(x) = (x^3 + nx - 1)(x^2 + n^2x - n).$$

Indeed, $s_n(x)$ has two close roots with asymptotic expansions

$$\frac{1}{n} + \frac{1}{2n^4} - \frac{1}{2n^5} + \frac{1}{2n^6} + O(\frac{1}{n^8}) \quad \text{and} \quad \frac{1}{n} + \frac{1}{2n^4} - \frac{1}{2n^5} + \frac{1}{2n^6} + \frac{1}{4n^7} + O(\frac{1}{n^8}),$$

while $p_n(x)$ has two close roots with asymptotic expansions

$$\frac{1}{n} - \frac{1}{n^4} + \frac{3}{n^7} + O(\frac{1}{n^{10}}) \quad \text{and} \quad \frac{1}{n} - \frac{1}{n^4} + \frac{2}{n^7} + O(\frac{1}{n^{10}}).$$

Hence, we proved that $e_r^*(5) \geq \frac{7}{3}$. Moreover, it is easy to see that the polynomials $p_n(x)$ can be generalized to arbitrary odd degree.

Let $d \geq 5$ be an odd number. To obtain a lower bound on $e_r^*(d)$, we construct a family $(P_{d,n})_{n\geq 1}$ of reducible monic polynomials of degree d (such that $P_{5,n} = p_n$), depending on the parameter n, with root separation asymptotically

$$\operatorname{sep}(P_{d,n}) \ll \mathrm{H}(P_{d,n})^{-\frac{d^2-2d-1}{2d-4}}, \quad n \to +\infty. \tag{9}$$

This will give

$$e_r^*(d) \geq \frac{d^2-2d-1}{2d-4} = \frac{d}{2} - \frac{1}{2d-4}. \tag{10}$$

The bound (10) is comparable with best known lower bounds for separation of irreducible monic and nonmonic polynomials ($e_{irr}^*(d) \geq \frac{d}{2} - \frac{1}{4}$, $e_{irr}(d) \geq \frac{d}{2} + \frac{d-2}{4(d-1)}$ see [3, 2]). Although it is asymptotically weaker than the bound $e_r^*(d) \geq (2d-5)/3$ from [3], it is better than $e_r^*(d) \geq (2d-5)/3$ for $d = 5$, $d = 7$ and $d = 9$, and it is also better than $e_r^*(5) \geq 2$ from [5].

For $k, n \in \mathbb{Z}_{\geq 2}$, let

$$\begin{aligned} Q(x) &= Q_{k,n}(x) = x^2 + n^k x - n, \\ R(x) &= R_{k,n}(x) = \frac{x^{2k+1} - Q(x)}{x^2 - n} = x \cdot \frac{x^{2k} - n^k}{x^2 - n} - 1 \\ &= x(x^{2(k-1)} + nx^{2(k-2)} + \cdots + n^{k-1}) - 1. \end{aligned}$$

We omit k and n from the index of polynomials $Q_{k,n}(x)$ and $R_{k,n}(x)$ for easier writing. It is clear that $Q(x)$ and $R(x)$ are monic integer polynomials of degrees 2 and $2k-1$ and heights n^k and n^{k-1}, respectively. Thus $Q(x)R(x)$ is a reducible monic polynomial of degree $2k+1$ and height $n^{2k-1} - 1$ which is attained only in the quadratic term.

Quadratic polynomial $Q(x)$ has roots $(-n^k \pm \sqrt{n^{2k} + 4n})/2$, so that one root is close to $-n^k$ and the other root, which we denote by

$$\alpha = \frac{2n}{n^k + \sqrt{n^{2k} + 4n}},$$

is close to n^{1-k}, more precisely, $0 < \frac{1}{2}n^{1-k} < \alpha < n^{1-k}$.

We also have

$$R(\alpha) = \frac{\alpha^{2k+1}}{\alpha^2 - n} < 0, \quad R(2\alpha) = \frac{(2\alpha)^{2k+1} - 2\alpha^2 - n}{(2\alpha)^2 - n} > 0$$

since the terms other than $-n$ in the numerator and the denominator are very small. Therefore, the polynomial $R(x)$ has a root β in the interval $(\alpha, 2\alpha)$.

Using the mean value theorem, we conclude that there is $t \in (\alpha, \beta)$ such that

$$0 < R'(t)(\beta - \alpha) = R(\beta) - R(\alpha) = \frac{\alpha^{2k+1}}{n - \alpha^2} < 2n^{(2k+1)(1-k)-1}. \tag{11}$$

It is easily seen that $R'(t) > n^{k-1}$ and employing this inequality in (11) gives

$$0 < \beta - \alpha < \frac{2n^{(2k+1)(1-k)-1}}{n^{k-1}} = 2n^{1-2k^2}.$$

This implies

$$\operatorname{sep}(Q \cdot R) < 2\,\mathrm{H}(Q \cdot R)^{\frac{1-2k^2}{2k-1}}.$$

For an odd integer $d \geq 5$, we take $k = (d-1)/2$ and define $P_{d,n}(x) := Q_{k,n}(x)R_{k,n}(x)$ obtaining a family that satisfies (9).

Corollary 1. *It holds that*

$$\frac{7}{3} \leq e_r^*(5) \leq 3, \quad \frac{17}{5} \leq e_r^*(7) \leq 5, \quad \frac{31}{7} \leq e_r^*(9) \leq 7.$$

References

[1] Y. Bugeaud, Approximation by algebraic numbers. Cambridge Tracts in Mathematics, Cambridge, 2004.

[2] Y. Bugeaud and A. Dujella, *Root separation for irreducible integer polynomials*, Bull. Lond. Math. Soc. **43** (2011), 1239–1244.

[3] Y. Bugeaud and A. Dujella, *Root separation for reducible integer polynomials*, Acta Arith. **162** (2014), 393–403.

[4] Y. Bugeaud, A. Dujella, T. Pejković and B. Salvy, *Absolute real root separation*, Amer. Math. Monthly, to appear.

[5] Y. Bugeaud and M. Mignotte, *Polynomial root separation*, Intern. J. Number Theory **6** (2010), 587–602.

[6] A. Dujella and T. Pejković, *Root separation for reducible monic quartics*, Rend. Semin. Mat. Univ. Padova **126** (2011), 63–72.

[7] J.-H. Evertse, *Distances between the conjugates of an algebraic number*, Publ. Math. Debrecen **65** (2004), 323–340.

[8] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262.

[9] T. Pejković, *P-adic root separation for quadratic and cubic polynomials*, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **20** (2016), 9–18.

[10] A. Schönhage, *Polynomial root separation examples*, J. Symbolic Comput. **41** (2006), 1080–1090.

[11] N. P. Smart, The Algorithmic Resolution of Diophantine Equations, Cambridge University Press, Cambridge, 1998.

Separacija korijena za reducibilne normirane polinome neparnog stupnja

Andrej Dujella i Tomislav Pejković

Sažetak. U ovom članku proučavamo separaciju korijena reducibilnih normiranih polinoma neparnog stupnja. Neka je $\mathrm{H}(P)$ visina, $\mathrm{sep}(P)$ minimalna udaljenost različitih korijena polinoma $P(x)$ s cjelobrojnim koeficijentima, te $\mathrm{sep}(P) = \mathrm{H}(P)^{-e(P)}$. Neka je $e_r^*(d) = \limsup_{\deg(P)=d,\, \mathrm{H}(P)\to+\infty} e(P)$, gdje se limsup uzima po svim reducibilnim normiranim cjelobrojnim polinomima $P(x)$ stupnja d. Dokazujemo da vrijedi $e_r^*(d) \leq d-2$. Također, dobivamo donju ogradu za $e_r^*(d)$ za neparan d, koja poboljsšava prethodno poznate donje ograde za $e_r^*(d)$ za $d \in \{5,7,9\}$.

Andrej Dujella
Department of Mathematics
Faculty of Science
University of Zagreb
Bijenička cesta 30
10000 Zagreb, Croatia
E-mail address: duje@math.hr

Tomislav Pejković
Department of Mathematics
Faculty of Science
University of Zagreb
Bijenička cesta 30
10000 Zagreb, Croatia
E-mail address: pejkovic@math.hr