Real and p-adic root separation for cubic and quartic polynomials

Tomislav Pejković

Abstract

We study real and p-adic root separation exponents for cubic and quartic integer polynomials, both for unrestricted sequences and for one-parameter families $F(T,X) \in \mathbb{Z}[T,X]$, where T is the parameter and X is the polynomial variable. For cubic families whose coefficients are polynomials in T, continued fractions over $\mathbb{Q}((T^{-1}))$ give the exponents $e_{\mathrm{irr}}^{\mathrm{poly}}(3) = e^{\mathrm{poly}}(3) = 2$. For quartics, we construct an irreducible family with exponent $9/4$ and reducible families with exponents tending to $5/2$. If h is the largest degree in T among the coefficients of a fixed quartic family F, we prove $e(F) \le 5/2 - 1/(2h)$. It follows that $e_{\mathrm{red}}^{\mathrm{poly}}(4) = e^{\mathrm{poly}}(4) = 5/2$ and $9/4 \le e_{\mathrm{irr}}^{\mathrm{poly}}(4) \le 5/2$. The families recover the known unrestricted lower bound $e_{\mathrm{red}}(4) \ge 5/2$ and improve the irreducible lower bound to $e_{\mathrm{irr}}(4) \ge 9/4$. Assuming Hall's conjecture, a direct argument with the classical quartic invariants gives another proof that $e_{\mathrm{red}}(4) = e(4) = 5/2$. The polynomial dependence on T also allows us to obtain integer polynomials with very close p-adic roots. For every prime p, we show that p-adic root separation exponents satisfy $e_{\mathrm{irr}}(3,p) = e(3,p) = 2$, $e_{\mathrm{irr}}(4,p) \ge 9/4$, and $5/2 \le e_{\mathrm{red}}(4,p) \le e(4,p) \le 3$.

2020 Mathematics Subject Classification. Primary 11C08. Secondary 11J61, 11J68, 11J70.
Key words and phrases. Root separation, integer polynomials, polynomially parametrized families, p-adic roots, continued fractions, Hall's conjecture.

1 Introduction

Let $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ be a separable polynomial of degree $n \ge 2$. Its height is

$$H(P) = \max_{0 \le j \le n} |a_j|,$$

and $\mathrm{sep}(P)$ denotes the minimum distance between two roots of P. When $H(P) > 1$, write

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

We denote by $e(n)$, $e_{\mathrm{irr}}(n)$, and $e_{\mathrm{red}}(n)$ the corresponding limsups of $e(P)$ as the height of P tends to infinity over all separable degree-n integer polynomials, over irreducible polynomials, and over reducible polynomials. For example,

$$e(n) = \limsup_{\substack{P \in \mathbb{Z}[X] \text{ separable} \\ \deg P = n,\ H(P) \to \infty}} e(P) = \limsup_{\substack{P \in \mathbb{Z}[X] \text{ separable} \\ \deg P = n,\ H(P) \to \infty}} \frac{-\log \mathrm{sep}(P)}{\log H(P)}, \tag{1}$$

and similarly if we restrict to irreducible or reducible polynomials. Irreducibility always means irreducibility over $\mathbb{Q}$. Thus

$$e(n) = \max\{e_{\mathrm{irr}}(n), e_{\mathrm{red}}(n)\}.$$

Mahler's classical estimate gives $e(n) \le n-1$ [16]. Apart from the trivial quadratic case, the only degree for which the exact value is known is $n=3$. Evertse proved $e_{\mathrm{irr}}(3)=2$ [11, Theorem 1.1], and Schönhage later gave an explicit construction [21]. Hence

$$e_{\mathrm{irr}}(3) = e(3) = 2.$$

We also consider polynomially parametrized families. Let $F(T,X) \in \mathbb{Z}[T,X]$ have degree n in X, nonzero discriminant with respect to X, and $H(F(t,X)) \to \infty$ as the positive integer t tends to infinity. We omit the finitely many values of t for which the degree in X drops or the discriminant vanishes, and put

$$e(F) = \limsup_{t\to\infty} \frac{-\log \operatorname{sep}(F(t,X))}{\log H(F(t,X))}.$$

Let $e^{\mathrm{poly}}(n)$ be the supremum of $e(F)$ over all such families. We define $e^{\mathrm{poly}}_{\mathrm{irr}}(n)$ by taking the limsup along irreducible specializations and then the supremum over families with infinitely many such specializations. The quantity $e^{\mathrm{poly}}_{\mathrm{red}}(n)$ is defined analogously using reducible specializations. Then

$$\begin{aligned} e^{\mathrm{poly}}_{\mathrm{irr}}(n) &\le e^{\mathrm{poly}}(n) \le e(n), & e^{\mathrm{poly}}_{\mathrm{red}}(n) &\le e^{\mathrm{poly}}(n), \\ e^{\mathrm{poly}}_{\mathrm{irr}}(n) &\le e_{\mathrm{irr}}(n), & e^{\mathrm{poly}}_{\mathrm{red}}(n) &\le e_{\mathrm{red}}(n). \end{aligned}$$

Schönhage's construction uses regular continued fractions of real numbers, but its coefficient heights grow exponentially with the sequence index [21]. The polynomially parametrized cubic family recorded in [17, Remark 4.1, p. 17] has root separation exponent $25/14$. We prove

$$e^{\mathrm{poly}}_{\mathrm{irr}}(3) = e^{\mathrm{poly}}(3) = 2.$$

Starting with the irreducible cubic $9X^3 - 4TX^2 - 2$, we expand one of its roots as a continued fraction in the field $\mathbb{Q}((T^{-1}))$ of formal Laurent series in T^{-1} with rational coefficients [22]. The primitive minimal polynomials of the successive complete quotients form a sequence of irreducible polynomially parametrized families whose exponents tend to 2. The first transformations also recover the mentioned family from [17, Remark 4.1, p. 17].

For irreducible quartics, Bugeaud and Dujella proved

$$e_{\mathrm{irr}}(4) \ge \frac{13}{6}$$

by an explicit polynomially parametrized family [5, Theorem 1]. For reducible quartics, they constructed a polynomially parametrized family with exponent $7/3$ [6, Theorem 1 and Section 2]. For reducible monic quartics, Dujella and Pejković proved that the corresponding exponent is exactly 2 [10, Theorem 1].

We construct an irreducible polynomially parametrized family of quartics with exponent $9/4$ and reducible families F_m with exponents

$$\frac{5m+1}{2m+1} = \frac{5}{2} - \frac{3}{4m+2}, \qquad m \ge 1.$$

The latter exceed $7/3$ for $m \ge 5$ and tend to $5/2$. If h is the largest degree in T among the coefficients of a fixed polynomially parametrized quartic family, the classical invariants I and J of a binary quartic, together with a degree estimate for $4I^3 - J^2$, give

$$e(F) \le \frac{5}{2} - \frac{1}{2h} < \frac{5}{2}.$$

Thus the previous results give

$$e_{\mathrm{irr}}(4) \geq \frac{9}{4} \quad \text{and} \quad e_{\mathrm{red}}^{\mathrm{poly}}(4) = \frac{5}{2}.$$

The irreducible family and the universal upper bound give

$$\frac{9}{4} \leq e_{\mathrm{irr}}^{\mathrm{poly}}(4) \leq \frac{5}{2}$$

and so also $e^{\mathrm{poly}}(4) = \frac{5}{2}$.

The unrestricted lower bound

$$e_{\mathrm{red}}(4) \geq \frac{5}{2}$$

was already obtained in a recent paper [18, Theorem 1]. Its proof uses a Pell-type sequence of cubic and linear factors from [1] with resultant of absolute value 2. The coefficients of that sequence grow exponentially with the index, so the sequence is not polynomially parametrized in the sense used here. The same paper [18] shows that separations with exponent greater than 2 for reducible quartics are governed by approximation of real cubic numbers by rational numbers [18, Proposition 2]. It also proves $e_{\mathrm{red}}(4) = 5/2$ under Hall's conjecture by applying Badziahin's estimate [1].

Our direct argument with the classical quartic invariants applies to every separable quartic. Under Hall's conjecture it gives

$$e_{\mathrm{red}}(4) = e(4) = \frac{5}{2}.$$

It therefore also gives the conditional upper bound $e_{\mathrm{irr}}(4) \leq 5/2$.

As a secondary application, the reducible families answer two questions posed by Badziahin about approximation of cubic algebraic Laurent series by rational functions [1, Section 6, penultimate paragraph]. The precise result is stated in Subsection 3.5.

One reason for imposing polynomial dependence on T is that the families constructed here admit direct p-adic specializations. After substituting $T = p^{-k}$ and clearing denominators, the extreme degrees in T determine both the Archimedean heights and the p-adic sizes of the coefficients. The Newton polygons locate roots according to their p-adic absolute values. The discriminant and resultant identities and the linear fractional transformations used in the real constructions remain valid after specialization. Together with Hensel's lemma, these facts identify pairs of roots that are much closer to each other than the remaining pairs and determine the order of their distance.

Let us give an overview of our results on p-adic root separation. Fix a prime p and normalize the absolute value by $|p|_p = p^{-1}$. For a separable $P \in \mathbb{Z}[X]$, let $\mathrm{sep}_p(P)$ be the minimum p-adic distance between its roots in $\overline{\mathbb{Q}}_p$. The height remains the Archimedean coefficient height $H(P)$. We define $e_{\mathrm{irr}}(n,p)$, $e_{\mathrm{red}}(n,p)$, and $e(n,p)$ by the same limsups as in (1) with sep replaced by sep_p. The general estimate

$$\mathrm{sep}_p(P) \geq n^{-3n/2} H(P)^{-n+1}$$

holds for every separable integer polynomial of degree n [19, Lemma 2.3, p. 17]. It gives $e(n,p) \leq n-1$. Previously, Pejković proved $e_{\mathrm{irr}}(3,p) \geq 25/14$ for $p \neq 2$ [17, Section 4, pp. 15–17]. More recently, Beresnevich and Dixon proved $e_{\mathrm{irr}}(n,p) \geq (n+1)/3$ for every $n \geq 2$ and every prime p [2, Theorem 2.1]. Substituting $T = p^{-k}$ in the families constructed above and clearing denominators, we prove, for every prime p,

$$e_{\mathrm{irr}}(3,p) = e(3,p) = 2, \qquad e_{\mathrm{irr}}(4,p) \geq \frac{9}{4}, \qquad \frac{5}{2} \leq e_{\mathrm{red}}(4,p) \leq e(4,p) \leq 3.$$

Assuming the *abc* conjecture, we also obtain $e_{\mathrm{red}}(4,p) = e(4,p) = 5/2$ for every prime p.

Throughout the paper, constants implicit in O, $\ll$, $\gg$, and $\asymp$ may depend on a fixed polynomial family. In the p-adic section they may also depend on p. They never depend on the parameter tending to infinity.

2 Cubic polynomials

For

$$\xi = c_m T^m + c_{m-1} T^{m-1} + \cdots \in \mathbb{Q}((T^{-1})),$$

the polynomial part is the sum of the terms with nonnegative powers of T. Starting with $\xi_0 = \xi$, let a_j be the polynomial part of ξ_j and, whenever $\xi_j \neq a_j$, put

$$\xi_{j+1} = \frac{1}{\xi_j - a_j}.$$

This gives the usual continued fraction $\xi = [a_0, a_1, a_2, \ldots]$ for a formal Laurent series [22].

We start with the polynomial

$$G(T,X) = 9X^3 - 4TX^2 - 2.$$

Eisenstein's criterion at 2, applied in $\mathbb{Z}[T][X]$, shows that G is irreducible over $\mathbb{Q}(T)$. The same criterion shows that $G(t,X)$ is irreducible over $\mathbb{Q}$ for every integer t. Its discriminant is

$$\mathrm{Disc}_X\, G = -4(128T^3 + 2187). \tag{2}$$

The polynomial $G(T,X)$, regarded as a polynomial in X over $\mathbb{Q}((T^{-1}))$, has a root ξ_0 whose Laurent expansion, obtained by successively comparing coefficients in $G(T,\xi_0) = 0$, begins

$$\xi_0 = \frac{4}{9}T + \frac{9}{8T^2} + O(T^{-5}).$$

Apply the preceding continued fraction algorithm to ξ_0. Starting with $G_0 = G$, let $G_{j+1}(T,X)$ be the primitive polynomial in $\mathbb{Z}[T,X]$, fixed up to sign, obtained by clearing denominators in

$$X^3 G_j\left(T, a_j(T) + \frac{1}{X}\right). \tag{3}$$

Since (3) is induced by a linear fractional transformation of determinant -1, $\mathrm{Disc}_X\, G_{j+1}$ is a nonzero rational multiple of $\mathrm{Disc}_X\, G_j$. Hence its degree in T remains equal to 3. The transformation preserves irreducibility over $\mathbb{Q}(T)$. It also preserves irreducibility after specialization. Indeed, if $G_j(t,X)$ is irreducible, then none of its roots equals $a_j(t)$ and the inverse transformation $x \mapsto a_j(t) + 1/x$ carries any factorization of the transformed cubic back to a factorization of $G_j(t,X)$. Starting from $G(t,X)$, all specializations at integer values of T considered below are therefore irreducible.

Theorem 2.1. *We have*

$$e_{\mathrm{irr}}^{\mathrm{poly}}(3) = e^{\mathrm{poly}}(3) = 2.$$

More precisely, if h_j is the largest degree in T of a coefficient of G_j, then, as $t \to \infty$ through positive integers,

$$H(G_j(t,X)) \asymp t^{h_j}, \qquad \mathrm{sep}(G_j(t,X)) \asymp t^{-2h_j+3/2},$$

and $h_j \to \infty$.

Proof. Put $s = T^{-1}$ and write $X = TY$. Then $G(T, X) = 0$ becomes

$$9Y^3 - 4Y^2 - 2s^3 = 0.$$

At $(s, Y) = (0, 4/9)$ the left-hand side vanishes, while its partial derivative with respect to Y is $16/9 \neq 0$. The holomorphic implicit function theorem [12, Appendix 3, p. 193] therefore gives some $\rho > 0$ and a holomorphic solution $Y = y(s)$ on $|s| < \rho$, with $y(0) = 4/9$. Comparison of coefficients shows that the formal power series solution with this constant term is unique. Consequently, the Taylor series of y is $s\xi_0(s^{-1})$. Thus the Laurent series defining ξ_0 converges for $|T| > \rho^{-1}$, and its sum there is $Ty(T^{-1})$.

Since G is irreducible over $\mathbb{Q}(T)$, the continued fraction of ξ_0 does not terminate. Hence $\xi_j - a_j \neq 0$ for every j. The reciprocal of a nonzero convergent Laurent series containing only negative powers is again convergent for all sufficiently large $|T|$ and has a polynomial part of positive degree. Since $a_0 = 4T/9$, induction shows that, for each fixed j, the Laurent series defining ξ_j converges for all sufficiently large $|T|$ and

$$q_j := \deg a_j \geq 1.$$

For large positive real t, denote its value by $\xi_j(t)$. Since $\xi_j(t) = a_j(t) + O(t^{-1})$, we have

$$|\xi_j(t)| \asymp t^{q_j}.$$

Besides ξ_j, denote the other two roots of G_j by η_j and ζ_j. For all sufficiently large positive t, equation (2) shows that $\eta_0(t)$ and $\zeta_0(t)$ are complex conjugates. Since $\xi_0(t) \asymp t$, Vieta's formulas give

$$|\eta_0(t)|^2 = \eta_0(t)\zeta_0(t) = \frac{2}{9\xi_0(t)} \asymp t^{-1}.$$

Thus

$$|\eta_0(t)|, |\zeta_0(t)| \asymp t^{-1/2}.$$

Under the transformation,

$$\eta_{j+1} = \frac{1}{\eta_j - a_j}, \qquad \zeta_{j+1} = \frac{1}{\zeta_j - a_j}.$$

Since $|a_j(t)| \asymp t^{q_j}$, induction gives $\eta_j(t), \zeta_j(t) \to 0$ as $t \to \infty$.

Let $A_j(T)$ be the leading coefficient of G_j as a polynomial in X. Writing

$$G_j(T, X) = A_j(T)(X - \xi_j)(X - \eta_j)(X - \zeta_j),$$

Vieta's formulas show that the coefficient of X^2 has order $t^{\deg A_j + q_j}$. The remaining coefficients have no larger order because $\eta_j(t), \zeta_j(t) = o(1)$. Hence

$$h_j = \deg A_j + q_j.$$

For large positive t, the closest roots are η_j and ζ_j, whereas $|\xi_j - \eta_j| \asymp |\xi_j - \zeta_j| \asymp t^{q_j}$. Therefore, using the discriminant and (2),

$$t^3 \asymp |\operatorname{Disc} G_j(t, X)| \asymp t^{4h_j}|\eta_j - \zeta_j|^2.$$

This gives

$$\operatorname{sep}(G_j(t, X)) \asymp t^{-2h_j + 3/2}. \tag{4}$$

The transformation of the two close roots gives

$$\left|\frac{1}{\eta_j - a_j} - \frac{1}{\zeta_j - a_j}\right| = \frac{|\eta_j - \zeta_j|}{|\eta_j - a_j|\,|\zeta_j - a_j|} \asymp t^{-2q_j}|\eta_j - \zeta_j|.$$

Comparing this with (4) for j and $j+1$ yields $h_{j+1} = h_j + q_j$. Since every $q_j \geq 1$, we have $h_j \to \infty$. Thus the root separation exponent of the jth family is

$$2 - \frac{3}{2h_j} \longrightarrow 2.$$

By the preceding observation, all integral specializations $G_j(t, X)$ are irreducible over $\mathbb{Q}$, so $e^{\mathrm{poly}}_{\mathrm{irr}}(3) \geq 2$. Mahler's bound gives the reverse inequality, and also $e^{\mathrm{poly}}(3) \leq 2$. □

The same construction recovers the family in [17, Remark 4.1, p. 17]. Put

$$R_0(T, X) = -G(3T, 3X) = -243X^3 + 108TX^2 + 2.$$

A direct continued fraction calculation gives the first four polynomial parts

$$\frac{4}{9}T, \qquad 24T^2, \qquad \frac{2}{9}T, \qquad 32T^2.$$

Applying (3) successively with these four polynomials, and normalizing to primitive integer coefficients at each step, gives exactly

$$\begin{aligned} R_4(T, X) = {} & (-45056T^6 - 17280T^3 - 243)X^3 + (8192T^7 + 1536T^4 - 378T)X^2 \\ & + (512T^5 + 156T^2)X + 8T^3 + 2, \end{aligned}$$

which is the family from [17, Remark 4.1, p. 17]. For every integer t, the polynomial $R_4(t, X)$ is Eisenstein at 2. Here $h = 7$. The proof of Theorem 2.1, applied to this scaled sequence, gives the exponent $25/14$. The next polynomial part is $2T/11$, so the following family has $h = 8$ and exponent $29/16 > 25/14$.

3 Quartic polynomials

3.1 An irreducible family

We first give an explicit family. Consider

$$\begin{aligned} Q(T, X) = {} & (729T^4 - 611T^2 + 128)X^4 \\ & + (-1436T^3 + 602T)X^3 \\ & + (625T^4 + 184T^2 + 109)X^2 \\ & + (-1250T^3 + 524T)X + (625T^2 - 1). \end{aligned}$$

Its height satisfies

$$H(Q(t, X)) \sim 729t^4. \tag{5}$$

A direct calculation gives the discriminant

$$\mathrm{Disc}_X\, Q = -2^8 3^{12}\left((25T^2 + 5)^3 + 3^7\right). \tag{6}$$

In particular, its degree in T is 6.

Proposition 3.1. *As the positive integer t tends to infinity,*

$$\operatorname{sep}(Q(t,X)) \asymp t^{-9}.$$

Moreover, $Q(t,X)$ is irreducible whenever 5 divides t. Consequently,

$$e_{\mathrm{irr}}^{\mathrm{poly}}(4) \geq \frac{9}{4} \qquad \textit{and} \qquad e_{\mathrm{irr}}(4) \geq \frac{9}{4}.$$

Proof. Coefficientwise as $t \to \infty$,

$$t^{-4}Q(t,X) \longrightarrow 729X^4 + 625X^2 = X^2(729X^2 + 625).$$

Label the roots of $Q(t,X)$ so that $\alpha_1(t), \alpha_2(t) \to 0$, $\alpha_3(t) \to 25i/27$, and $\alpha_4(t) \to -25i/27$. Continuity of roots, counted with multiplicity, shows that every root difference except $\alpha_1(t) - \alpha_2(t)$ tends to a nonzero limit. The leading coefficient of $Q(t,X)$ is of order t^4, while (6) is of order t^6. The product formula for the discriminant (see e.g. [4, Appendix A]) therefore gives

$$|\alpha_1(t) - \alpha_2(t)|^2 \asymp t^{6-24} = t^{-18}.$$

Hence $\operatorname{sep}(Q(t,X)) \asymp t^{-9}$. Together with (5), this gives the exponent $9/4$.

If 5 divides t, reduction modulo 5 gives

$$Q(t,X) \equiv 3X^4 + 4X^2 + 4 \pmod 5.$$

Multiplying by 2, it is enough to consider $X^4 + 3X^2 + 3$. This polynomial has no root in $\mathbb{F}_5$. If it were a product of two quadratics, we could write

$$X^4 + 3X^2 + 3 = (X^2 + uX + v)(X^2 - uX + w).$$

The coefficient of X gives $u(w - v) = 0$. If $u = 0$, then v and w would be roots of $Y^2 - 3Y + 3$, whose discriminant 2 is not a square modulo 5. If $v = w$, then $v^2 = 3$, again impossible modulo 5. Hence the reduction is irreducible, and so is $Q(t,X)$. □

3.2 Reducible families

We now construct reducible polynomially parametrized quartic families F_m, $m \geq 1$, whose root separation exponents tend to $5/2$. The form of the underlying polynomial identity was motivated by polynomial constructions related to Hall's conjecture, especially by Dujella's construction [9, Theorem 1].

Define

$$S_0 = 1, \qquad S_1 = T, \qquad S_{n+1} = TS_n + S_{n-1}, \qquad n \geq 1. \tag{7}$$

Each S_n is monic of degree n and contains only powers of T of the same parity as n. The recurrence gives the Cassini-type identity

$$S_m^2 - TS_mS_{m-1} - S_{m-1}^2 = (-1)^m, \qquad m \geq 1, \tag{8}$$

and the addition formula

$$S_{r+s} = S_rS_s + S_{r-1}S_{s-1}, \qquad r, s \geq 1.$$

We shall use the following polynomial identity. By (8), its right-hand side becomes constant after the specialization $u = S_m$, $v = S_{m-1}$.

Lemma 3.2. *For indeterminates T, u, v, put*

$$N = u^2 - Tuv - v^2,$$

and define

$$\begin{aligned} a &= (T+2)u + (2-T)v, \\ b &= 3(2-T)u + (T^2 - 3T - 2)v, \\ c &= (T^2 - 3T - 2)u + 3(T^2 + T + 2)v, \\ d &= (T^2 + T + 2)u + (2 - 3T - T^3)v, \end{aligned}$$

and

$$\begin{aligned} p &= 3u^2 v - 3Tuv^2 + (T^2+1)v^3 + Nu, \\ q &= u^3 + 3uv^2 - Tv^3 - Nv. \end{aligned}$$

Then

$$-ap^3 + bp^2 q - cpq^2 + dq^3 = 8N^5.$$

Proof. A direct expansion of the left-hand side gives $8(u^2 - Tuv - v^2)^5 = 8N^5$. □

Fix $m \geq 1$ and put

$$u = S_m(T), \qquad v = S_{m-1}(T).$$

Equation (8) gives $N = (-1)^m$. The recurrence and the addition formula give

$$S_{2m} = u^2 + v^2, \qquad S_{2m-1} = 2uv - Tv^2,$$

and then

$$\begin{aligned} S_{3m-1} &= 3u^2 v - 3Tuv^2 + (T^2+1)v^3, \\ S_{3m} &= u^3 + 3uv^2 - Tv^3. \end{aligned}$$

Consequently, the specializations of p and q are

$$p_m = S_{3m-1} + (-1)^m S_m, \qquad q_m = S_{3m} - (-1)^m S_{m-1}. \tag{9}$$

Let a_m, b_m, c_m, d_m denote the corresponding specializations of a, b, c, d, and define

$$\begin{aligned} K_m(T, X) &= -a_m X^3 + b_m X^2 - c_m X + d_m, \\ L_m(T, X) &= q_m X - p_m, \\ F_m(T, X) &= K_m(T, X) L_m(T, X). \end{aligned} \tag{10}$$

Theorem 3.3. *For every $m \geq 1$, we have*

$$\mathrm{Res}_X(L_m, K_m) = q_m^3 K_m(T, p_m/q_m) = 8(-1)^m. \tag{11}$$

As positive integers t tend to infinity,

$$H(F_m(t, X)) = t^{4m+2}(1 + O(t^{-1})), \tag{12}$$

and

$$\mathrm{sep}(F_m(t, X)) = 8t^{-(10m+2)}(1 + O(t^{-1})). \tag{13}$$

Moreover, $K_m(t, X)$ is irreducible over $\mathbb{Q}$ for every integer $t \equiv 0 \pmod 3$. The root separation exponent of F_m is

$$e(F_m) = \frac{10m+2}{4m+2} = \frac{5m+1}{2m+1} = \frac{5}{2} - \frac{3}{4m+2}. \tag{14}$$

Proof. Lemma 3.2 and (8) give

$$q_m^3 K_m(T, p_m/q_m) = 8(-1)^m.$$

Since $L_m = q_m X - p_m$, the left-hand side is $\mathrm{Res}_X(L_m, K_m)$, which proves (11).

In d_m, the terms of degree $m+2$ cancel, leaving degree $m+1$ and leading coefficient 1. The degrees and leading coefficients are therefore

	a_m	b_m	c_m	d_m	p_m	q_m
$\deg_T$	$m+1$	$m+1$	$m+2$	$m+1$	$3m-1$	$3m$
lc_T	1	-2	1	1	1	1

.

The coefficient of X^2 in F_m is $-b_m p_m - c_m q_m$ and has leading term $-T^{4m+2}$, whereas every other coefficient has degree at most $4m+1$. This proves (12).

Put

$$\beta_m = \frac{p_m}{q_m} \in \mathbb{Q}(T).$$

Since p_m and q_m are monic of degrees $3m-1$ and $3m$, respectively,

$$\beta_m(t) = t^{-1} + O(t^{-2}).$$

Uniformly for $0 \le Y \le 2$, the preceding degree calculations give

$$t^{-(m+1)} K_m(t, Y/t) = 1 - Y + O(t^{-1}),$$

and

$$t^{-(m+2)} \frac{\partial K_m}{\partial X}(t, Y/t) = -1 + O(t^{-1}).$$

It follows that, for all sufficiently large t, the polynomial $K_m(t, X)$ is strictly decreasing on $[0, 2/t]$ and has a unique root $\alpha_m(t)$ in $(0, 2/t)$. Moreover,

$$\alpha_m(t) = t^{-1} + O(t^{-2}),$$

and $\beta_m(t)$ also belongs to $(0, 2/t)$.

For later use, regard $\beta_m \in \mathbb{Q}(T)$ as an element of $\mathbb{Q}((T^{-1}))$. The same degree calculations give

$$\frac{\partial K_m}{\partial X}(T, \beta_m) = -T^{m+2}(1 + O(T^{-1})). \tag{15}$$

Equation (11) gives

$$K_m(T, \beta_m) = \frac{8(-1)^m}{q_m^3} = 8(-1)^m T^{-9m}(1 + O(T^{-1})).$$

Returning to the specialization $T = t$, the mean value theorem applied between $\alpha_m(t)$ and $\beta_m(t)$, together with the uniform derivative estimate on $[0, 2/t]$, gives

$$|\alpha_m(t) - \beta_m(t)| = 8t^{-(10m+2)}(1 + O(t^{-1})).$$

It remains to locate the other two roots of $K_m(t, X)$. Coefficientwise as $t \to \infty$,

$$t^{-(m+5/2)} K_m(t, t^{1/2} X) \longrightarrow -X(X^2 + 1).$$

The roots of the limiting polynomial are simple. Since $t^{-1/2}\alpha_m(t) \to 0$, continuity of roots shows that the other two roots of $K_m(t, X)$ are

$$t^{1/2}(i + o(1)) \qquad \text{and} \qquad t^{1/2}(-i + o(1)).$$

Every distance involving either of these roots is of order $t^{1/2}$. Since $\beta_m(t)$ is the root of $L_m(t, X)$, the preceding estimate for $|\alpha_m(t) - \beta_m(t)|$ proves (13).

We finally prove the irreducibility assertion. If $t \equiv 0 \pmod 3$, the recurrence (7) gives

$$S_{2j}(t) \equiv 1, \qquad S_{2j+1}(t) \equiv 0 \pmod 3, \qquad j \geq 0.$$

Therefore

$$K_m(t, X) \equiv \begin{cases} X^3 + 2X + 2, & m \text{ even}, \\ X^3 + X^2 + 2, & m \text{ odd} \end{cases} \pmod 3.$$

A direct check shows that neither cubic has a root in $\mathbb{F}_3$. Hence both are irreducible over $\mathbb{F}_3$, and $K_m(t, X)$ is irreducible over $\mathbb{Q}$. Formula (14) now follows from (12) and (13). □

By (14), F_m improves on the root separation exponent 7/3 obtained by Bugeaud and Dujella [6, Theorem 1] precisely when $m \geq 5$.

Corollary 3.4. *We have*

$$e_{\mathrm{red}}^{\mathrm{poly}}(4) \geq \frac{5}{2} \qquad \textit{and} \qquad e_{\mathrm{red}}(4) \geq \frac{5}{2}.$$

Proof. Since every F_m is reducible, Theorem 3.3 and the definitions give

$$e_{\mathrm{red}}(4) \geq e_{\mathrm{red}}^{\mathrm{poly}}(4) \geq \sup_{m \geq 1} e(F_m) = \frac{5}{2}.$$ □

The unrestricted lower bound in Corollary 3.4 was already obtained in [18, Theorem 1] from a Pell-type sequence. The present construction refines this result by establishing the same lower bound within the class of polynomially parametrized families, since $\sup_{m \geq 1} e(F_m) = 5/2$.

3.3 A universal upper bound

The following theorem gives a universal upper bound for the root separation exponent of polynomially parametrized quartic families.

Theorem 3.5. *Let*

$$F(T, X) = a(T)X^4 + b(T)X^3 + c(T)X^2 + d(T)X + e(T) \in \mathbb{Z}[T, X]$$

be of degree 4 in X and separable over $\mathbb{Q}(T)$. Let $h \geq 1$ be the largest degree in T of its coefficients. Put

$$I = 12ae - 3bd + c^2$$

and

$$J = 72ace + 9bcd - 27ad^2 - 27b^2e - 2c^3.$$

Define

$$\mu = \max\left\{\frac{\deg I}{2}, \frac{\deg J}{3}\right\},$$

where a zero polynomial is omitted from the maximum. If $\mu > 0$, then for all sufficiently large positive t,

$$\mathrm{sep}(F(t, X)) \gg t^{-h-3\mu/2+1/2}.$$

If $\mu = 0$, then for all sufficiently large positive t,

$$\mathrm{sep}(F(t, X)) \gg t^{-h}.$$

In either case,

$$\mathrm{sep}(F(t, X)) \gg t^{-(5h-1)/2}.$$

Proof. Let Δ be the discriminant of F with respect to X. The polynomials I and J defined above are the classical invariants of the binary quartic obtained by homogenizing F with respect to X [7, Section 4.1.1, equations (15)–(17)]. They satisfy

$$27\Delta = 4I^3 - J^2. \tag{16}$$

Since Δ is nonzero, at least one of I and J is nonzero. Thus μ is well defined. We also have $\mu \le h$.

For a fixed sufficiently large t, label the roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ so that $|\alpha_1 - \alpha_2| = \operatorname{sep}(F(t, X))$. In the identities below, I, J and Δ also denote their values at t. Set

$$u = a(t)(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4),$$

$$v = a(t)(\alpha_1 - \alpha_3)(\alpha_4 - \alpha_2), \qquad w = a(t)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3).$$

Direct expansion gives

$$u+v+w = 0, \qquad I = \frac{u^2 + v^2 + w^2}{2}, \qquad J = (u-v)(v-w)(w-u), \qquad \Delta = (uvw)^2. \tag{17}$$

By the definition of μ,

$$|I(t)| \ll t^{2\mu} \qquad \text{and} \qquad |J(t)| \ll t^{3\mu}.$$

Identity (16) therefore gives

$$|\Delta(t)| \ll t^{6\mu}.$$

It follows from $\Delta = (uvw)^2$ that $|uvw| \ll t^{3\mu}$. The numbers u, v, w are the roots of $x^3 - Ix - uvw$. Hence, for each $z \in \{u, v, w\}$,

$$|z|^3 \le |I||z| + |uvw| \le 2\max\{|I||z|, |uvw|\}.$$

Therefore

$$\max\{|u|, |v|, |w|\} \ll \max\{|I|^{1/2}, |uvw|^{1/3}\} \ll t^{\mu}. \tag{18}$$

Since every coefficient of F has degree at most h in T and $|a(t)| \asymp t^{\deg a}$, Cauchy's root bound gives

$$|\alpha_i| \le 1 + \frac{\max\{|b(t)|, |c(t)|, |d(t)|, |e(t)|\}}{|a(t)|} \ll 1 + t^{h - \deg a} \ll t^{h - \deg a}.$$

Therefore

$$|a(t)(\alpha_i - \alpha_j)| \ll t^h$$

for every i, j. In particular,

$$|u| \ll t^h \operatorname{sep}(F(t, X)).$$

Together with (18) and $\Delta = (uvw)^2$, this yields

$$|\Delta(t)| \ll t^{2h+4\mu} \operatorname{sep}(F(t, X))^2. \tag{19}$$

Suppose first that $\mu = 0$. Then I and J are constant, so (16) shows that Δ is a nonzero constant. Equation (19) therefore gives

$$\operatorname{sep}(F(t, X)) \gg t^{-h}.$$

Assume now that $\mu > 0$. We claim that

$$\deg \Delta \geq \mu + 1. \tag{20}$$

This is the special case of Davenport's inequality [8] needed here. Since $\mu > 0$, its definition gives $\mu \geq 1/3$. If either I or J is zero, (16) gives

$$\deg \Delta = 6\mu \geq \mu + 1.$$

Assume that both are nonzero. If $3 \deg I \neq 2 \deg J$, there is no cancellation between the leading terms in (16). Hence $\deg \Delta = 6\mu \geq \mu + 1$. It remains to consider the case $\deg I = 2\mu$ and $\deg J = 3\mu$. If $2IJ' - 3I'J \neq 0$, differentiating (16) gives

$$4I^2(2IJ' - 3I'J) = 54J'\Delta - 27J\Delta'.$$

Here primes denote differentiation with respect to T. The left-hand side has degree at least 4μ, while the right-hand side has degree at most $3\mu + \deg \Delta - 1$. Hence (20) follows. If $2IJ' - 3I'J = 0$, then J^2/I^3 is constant. Since $\Delta \neq 0$, (16) gives $\deg \Delta = 6\mu$, which again proves (20).

Since $\Delta(T)$ is a nonzero polynomial, $|\Delta(t)| \gg t^{\deg \Delta}$. Combining this with (19) and (20),

$$\operatorname{sep}(F(t, X)) \gg t^{-h-2\mu+(\mu+1)/2} = t^{-h-3\mu/2+1/2}.$$

Since $\mu \leq h$, it follows that

$$\operatorname{sep}(F(t, X)) \gg t^{-(5h-1)/2}.$$

The same estimate follows from the bound obtained when $\mu = 0$. □

Corollary 3.6. *We have*

$$e_{\mathrm{red}}^{\mathrm{poly}}(4) = e^{\mathrm{poly}}(4) = \frac{5}{2}$$

and

$$\frac{9}{4} \leq e_{\mathrm{irr}}^{\mathrm{poly}}(4) \leq \frac{5}{2}.$$

Proof. For a fixed family as in Theorem 3.5, we have $H(F(t, X)) \asymp t^h$. The theorem therefore gives

$$e(F) \leq \frac{5}{2} - \frac{1}{2h} < \frac{5}{2}.$$

In particular, no fixed polynomially parametrized quartic family attains the supremum $5/2$. Corollary 3.4 gives the lower bound $e_{\mathrm{red}}^{\mathrm{poly}}(4) \geq 5/2$, while Proposition 3.1 gives $e_{\mathrm{irr}}^{\mathrm{poly}}(4) \geq 9/4$. The remaining inequalities follow from the definitions. □

3.4 A conditional upper bound

Hall's conjecture [14], in the standard ϵ-form stated, for example, in [9, p. 397], asserts that for every $\epsilon > 0$,

$$|x^3 - y^2| \gg_\epsilon x^{1/2-\epsilon}$$

for all positive integers x and y satisfying $x^3 \neq y^2$.

The conditional equality $e_{\mathrm{red}}(4) = 5/2$ was proved in [18, Theorem 1] by combining the reduction to cubic rational approximation with Badziahin's estimate. The following argument applies to every separable quartic.

Theorem 3.7. *Assume Hall's conjecture. Let $P = aX^4 + bX^3 + cX^2 + dX + e \in \mathbb{Z}[X]$ be a separable quartic, let $H = H(P)$, and put*

$$I = 12ae - 3bd + c^2, \qquad J = 72ace + 9bcd - 27ad^2 - 27b^2e - 2c^3.$$

Then, for every $\epsilon > 0$,

$$\operatorname{sep}(P) \gg_\epsilon H^{-1} \max\{1, |I|^{1/2}, |J|^{1/3}\}^{-3/2-\epsilon} \gg_\epsilon H^{-5/2-\epsilon}.$$

Consequently,

$$e_{\mathrm{red}}(4) = e(4) = \frac{5}{2}.$$

Proof. Fix $\epsilon > 0$. Let Δ be the discriminant of P and put

$$B = \max\{1, |I|^{1/2}, |J|^{1/3}\}.$$

We first claim that Hall's conjecture gives

$$|\Delta| \gg_\epsilon B^{1-2\epsilon}. \tag{21}$$

If $I \le 0$, identity (16) gives the stronger bound $|\Delta| \gg B^6$. Suppose that $I > 0$. If one of the two nonnegative quantities $4I^3$ and J^2 is at least twice the other, the same stronger bound follows. In the remaining case

$$|I|^{1/2} \asymp |J|^{1/3} \asymp B.$$

In particular, $J \neq 0$. Apply Hall's conjecture to the positive integers

$$x = 4I, \qquad y = 4|J|.$$

Since P is separable, $\Delta \neq 0$, and hence $x^3 \neq y^2$. We have

$$x^3 - y^2 = 16(4I^3 - J^2) = 432\Delta,$$

and $x \asymp B^2$. Hall's conjecture therefore gives (21).

Label the roots $\alpha_1, \dots, \alpha_4$ of P so that $|\alpha_1 - \alpha_2| = \operatorname{sep}(P)$ and define u, v, w by the same formulas as in the proof of Theorem 3.5. Then the identities in (17) hold. Cauchy's root bound gives

$$|a\alpha_i| \le |a| + H \le 2H$$

for every i. Hence

$$|u| \ll H \operatorname{sep}(P).$$

By the definition of B and (16),

$$|\Delta| \ll B^6, \qquad |uvw| = |\Delta|^{1/2} \ll B^3.$$

For each $z \in \{u, v, w\}$, the equation $z^3 = Iz + uvw$ gives

$$|z|^3 \le |I||z| + |uvw| \ll B^2|z| + B^3,$$

and therefore $|u|, |v|, |w| \ll B$. Using these estimates in $\Delta = (uvw)^2$, we obtain

$$|\Delta| \ll H^2 B^4 \operatorname{sep}(P)^2.$$

Together with (21), this gives

$$B^{1-2\epsilon} \ll_\epsilon H^2 B^4 \operatorname{sep}(P)^2,$$

and hence

$$\operatorname{sep}(P) \gg_\epsilon H^{-1} B^{-3/2-\epsilon}.$$

Since $I \ll H^2$ and $J \ll H^3$, we have $B \ll H$. Hence

$$\operatorname{sep}(P) \gg_\epsilon H^{-5/2-\epsilon}.$$

Thus $e(4) \le 5/2$. Corollary 3.4 gives the reverse inequality and gives it within the reducible class. □

3.5 Cubic approximation over a function field

The reducible families constructed above also yield a sharp result on rational approximation to cubic Laurent series. In this subsection, let

$$\mathbb{K} = \mathbb{Q}((T^{-1}))$$

with the non-Archimedean absolute value extending

$$\left|\frac{P}{Q}\right| = 2^{\deg P - \deg Q}, \qquad 0 \neq P, Q \in \mathbb{Q}[T].$$

The height $H(\xi)$ of an element ξ of $\mathbb{K}$ algebraic over $\mathbb{Q}(T)$ is the maximum absolute value of the coefficients of a primitive polynomial in $\mathbb{Q}[T][X]$ associated with the minimal polynomial of ξ over $\mathbb{Q}(T)$. If $r = P/Q$ with coprime $P, Q \in \mathbb{Q}[T]$, then $H(r) = \max\{|P|, |Q|\}$.

Following Badziahin [1, Section 6], let $D_{3,1}(\mathbb{K})$ be the set of pairs $(u, v) \in \mathbb{R}^2_{>0}$ for which there is a constant $c = c(u, v) > 0$ such that

$$|\xi - r| > cH(\xi)^{-u} H(r)^{-v} \tag{22}$$

for every $\xi \in \mathbb{K}$ of degree 3 over $\mathbb{Q}(T)$ and every $r \in \mathbb{Q}(T)$.

Liouville's inequality gives $(1, 3) \in D_{3,1}(\mathbb{K})$. Badziahin proved that $(4, 2) \in D_{3,1}(\mathbb{K})$ and that, for every $2 \le v \le 3$, the set $D_{3,1}(\mathbb{K})$ contains a point of the form (u, v) [1, Theorem 5]. His example shows that $(u, 2) \in D_{3,1}(\mathbb{K})$ is possible only if $u \ge 3$ [1, Section 6, (22) and the discussion following it]. He asked for the minimum such u and for the shape of the set when $2 < v < 3$ [1, Section 6, penultimate paragraph].

The following proposition answers both questions for $\mathbb{K} = \mathbb{Q}((T^{-1}))$ by determining $D_{3,1}(\mathbb{K})$ in the strip $2 \le v \le 3$.

Proposition 3.8. *For $\mathbb{K} = \mathbb{Q}((T^{-1}))$ we have*

$$D_{3,1}(\mathbb{K}) \cap \{(u, v) \mid 2 \le v \le 3\} = \{(u, v) \mid 2 \le v \le 3,\ u + 3v \ge 10\}.$$

In particular,

$$\min\{u \mid (u, 2) \in D_{3,1}(\mathbb{K})\} = 4.$$

Proof. With definitions given in (9) and (10), and properties obtained in the proof of Theorem 3.3, we see that the coefficients of $T^{-(m+2)} K_m(T, X)$, as well as $\beta_m = p_m/q_m$, have absolute value at most 1. Equations (11) and (15) give

$$\left|T^{-(m+2)} K_m(T, \beta_m)\right| = 2^{-(10m+2)}, \qquad \left|T^{-(m+2)} \frac{\partial K_m}{\partial X}(T, \beta_m)\right| = 1.$$

The first of these numbers is smaller than the square of the second. The strong form of Hensel's lemma [20, Chapter 2, Section 1.5, Hensel's Lemma, pp. 80–82] therefore gives a root $\alpha_m \in \mathbb{K}$ of $K_m(T, X)$ satisfying

$$|\alpha_m - \beta_m| = \frac{\left|T^{-(m+2)} K_m(T, \beta_m)\right|}{\left|T^{-(m+2)} \dfrac{\partial K_m}{\partial X}(T, \beta_m)\right|} = 2^{-(10m+2)}.$$

Theorem 3.3 provides infinitely many irreducible specializations of K_m. Hence K_m is irreducible over $\mathbb{Q}(T)$, since a factorization over $\mathbb{Q}(T)$, after clearing denominators, would specialize to a nontrivial factorization for all but finitely many integers t. Thus α_m has degree 3.

Any nonconstant common divisor of the coefficients of K_m, or of p_m and q_m, would divide the nonzero constant in (11). Thus K_m is primitive and p_m and q_m are coprime in $\mathbb{Q}[T]$. Together with the degree calculations in the proof of Theorem 3.3, this gives

$$H(\alpha_m) = 2^{m+2}, \qquad H(\beta_m) = 2^{3m}, \qquad |\alpha_m - \beta_m| = 2^{-(10m+2)}.$$

If $(u, v) \in D_{3,1}(\mathbb{K})$, inequality (22), with the same constant c for every m, gives

$$2^{-(10m+2)} > c\, 2^{-u(m+2)-3mv}.$$

Equivalently,

$$(u + 3v - 10)m + 2u - 2 > \log_2 c.$$

Letting m tend to infinity gives

$$u + 3v \geq 10.$$

For the converse, let $2 \leq v \leq 3$. The numbers $3 - v$ and $v - 2$ are nonnegative and have sum 1. Taking the weighted geometric mean of the inequalities at $(4, 2)$ and $(1, 3)$ gives the inequality at

$$(3 - v)(4, 2) + (v - 2)(1, 3) = (10 - 3v, v).$$

Since $H(\xi) \geq 1$, replacing $10 - 3v$ by a larger value of u can only decrease the right-hand side of (22). It follows that $(u, v) \in D_{3,1}(\mathbb{K})$ for every $u \geq 10 - 3v$. □

4 p-adic root separation

The polynomial families used in the real setting also give new bounds for p-adic root separation.

Theorem 4.1. *For every prime p, we have*

$$e_{\mathrm{irr}}(3, p) = e(3, p) = 2, \qquad e_{\mathrm{irr}}(4, p) \geq \frac{9}{4},$$

and

$$\frac{5}{2} \leq e_{\mathrm{red}}(4, p) \leq e(4, p) \leq 3.$$

Proof. We obtain integer polynomials by substituting $T = p^{-k}$ in our polynomial families and clearing denominators. In each case, the highest-degree terms in T determine the Newton polygons, whereas nonzero constant terms determine the Archimedean heights.

For a polynomial $\sum c_i X^i$, the coefficient point with abscissa i has ordinate $-\log_p |c_i|_p$. A segment of slope s and horizontal length r accounts for exactly r roots in $\overline{\mathbb{Q}}_p$, counted with multiplicity, of absolute value p^s [13, Theorem 6.4.7].

We first treat cubics using families from Section 2. Start with $G(T, X) = 9X^3 - 4TX^2 - 2$ and put

$$G_{p,k}(X) = p^k G(p^{-k}, X) = 9p^k X^3 - 4X^2 - 2p^k.$$

For odd p this polynomial is Eisenstein at 2. If $p = 2$ and $k \equiv 2 \pmod 4$, its reduction modulo 5 is $X^3 + X^2 + 2$. This cubic has no zero in $\mathbb{F}_5$ and is irreducible. Thus $G_{p,k}$ is irreducible for infinitely many k for every prime p.

For fixed $j \geq 0$, put

$$G_{j,p,k}(X) = p^{h_j k} G_j(p^{-k}, X) \in \mathbb{Z}[X].$$

The proof of Theorem 2.1 shows that the coefficient of X^2 in G_j has degree h_j, the coefficient of X^3 has degree $h_j - q_j$, and the other two coefficients have degree at most h_j. After multiplication by $p^{h_j k}$, a coefficient of degree d in T gives a point of ordinate $(h_j - d)k + O(1)$. Hence the coefficient point with abscissa 2 has ordinate $O(1)$, the point with abscissa 3 has ordinate $q_j k + O(1)$, and the remaining coefficient points have ordinates bounded below independently of k. Since $q_j \geq 1$, for all sufficiently large k the point with abscissa 2 lies strictly below every line joining the point with abscissa 3 to a coefficient point with abscissa 0 or 1. Hence the final segment of the Newton polygon joins the points with abscissas 2 and 3 and has slope $q_j k + O(1)$, while all preceding slopes are bounded above independently of k. It follows that one root of $G_{j,p,k}$ has absolute value $\asymp p^{q_j k}$, while the other two have absolute values bounded independently of k. The distance from this root to either of the other two is therefore $\asymp p^{q_j k}$.

The leading coefficient of $G_{j,p,k}$ has absolute value $\asymp p^{-q_j k}$. Moreover, $\operatorname{Disc}_X G_j$ is a nonzero rational multiple of $\operatorname{Disc}_X G$ and has degree 3 in T. Since multiplying a cubic polynomial by $p^{h_j k}$ multiplies its discriminant by $p^{4h_j k}$, we have

$$|\operatorname{Disc}_X G_{j,p,k}|_p \asymp p^{-(4h_j - 3)k}.$$

In the product formula for the discriminant, the fourth power of the leading coefficient contributes a factor $\asymp p^{-4q_j k}$, while the two distances involving the root of absolute value $\asymp p^{q_j k}$ contribute $\asymp p^{4q_j k}$ after squaring. These factors cancel, and the distance between the other two roots is

$$\asymp p^{-(2h_j - 3/2)k}.$$

This is the root separation of $G_{j,p,k}$ for all sufficiently large k.

The discriminant of G_j has a nonzero constant term, so at least one coefficient of G_j has a nonzero constant term. Consequently,

$$H(G_{j,p,k}) \asymp p^{h_j k}.$$

The linear fractional transformations preserve irreducibility over $\mathbb{Q}$ after specialization, so $G_{j,p,k}$ is irreducible along the same infinite subsequence of k as $G_{p,k}$. For every fixed j, letting k tend to infinity gives

$$e_{\mathrm{irr}}(3, p) \geq 2 - \frac{3}{2h_j}.$$

Since $h_j \to \infty$, we obtain $e_{\mathrm{irr}}(3, p) \geq 2$. The general bound from [19, Lemma 2.3, p. 17] gives $e(3, p) \leq 2$.

We next treat the irreducible quartic family obtained from the one in Section 3.1. Define

$$Q_{p,k}(X) = p^{4k} Q(p^{-k}, X).$$

Then $H(Q_{p,k}) \asymp p^{4k}$, and (6) gives

$$\operatorname{Disc} Q_{p,k} = -2^8 3^{12} p^{18k} \left((25 + 5p^{2k})^3 + 3^7 p^{6k} \right). \tag{23}$$

If $p \neq 5$, the factor in parentheses in (23) converges p-adically to the unit 25^3. If $p = 5$, this factor is 5^6 times a 5-adic unit for all sufficiently large k. Hence its p-adic absolute value is bounded above and below by positive constants depending only on p, and

$$|\operatorname{Disc} Q_{p,k}|_p \asymp p^{-18k}.$$

The coefficient points of $Q_{p,k}$ have the form

$$(0, 2k + O(1)), \quad (1, k + O(1)), \quad (2, O(1)), \quad (3, k + O(1)), \quad (4, O(1)).$$

Its Newton polygon therefore gives two roots of absolute value $\asymp p^{-k}$ and two roots of absolute value $\asymp 1$. Moreover, $Q_{p,k}$ converges coefficientwise in $\mathbb{Q}_p[X]$ to

$$X^2(729X^2 + 625) = X^2((27X)^2 + 25^2).$$

The two nonzero roots of this polynomial are simple. Applying the Hensel's lemma over a finite extension of $\mathbb{Q}_p$ containing them [20, Chapter 2, Section 1.5, Hensel's Lemma, pp. 80–82] shows that all five distances involving at least one of the two roots of $Q_{p,k}$ of absolute value $\asymp 1$ are $\asymp 1$. The leading coefficient of $Q_{p,k}$ also has absolute value $\asymp 1$. The product formula for the discriminant therefore gives

$$\operatorname{sep}_p(Q_{p,k}) \asymp p^{-9k}.$$

We verify irreducibility along an infinite subsequence. If $p \neq 5$, choose infinitely many k with $p^k \equiv 1 \pmod 5$. Then

$$Q_{p,k}(X) \equiv X^4 + X^3 + 3X^2 + 4X + 4 \pmod 5$$

and

$$\gcd(X^4 + X^3 + 3X^2 + 4X + 4, X^{25} - X) = 1 \quad \text{in } \mathbb{F}_5[X].$$

If $p = 5$, take positive integers $k \equiv 0 \pmod 5$. Since $5^k \equiv 1 \pmod{11}$, multiplication by 3 gives

$$3Q_{5,k}(X) \equiv X^4 + 6X^3 + 4X^2 + 2 \pmod{11}$$

and

$$\gcd(X^4 + 6X^3 + 4X^2 + 2, X^{121} - X) = 1 \quad \text{in } \mathbb{F}_{11}[X].$$

The polynomial $X^{q^2} - X$ is the product of the monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide 2 [15, Theorem 3.20]. A reducible quartic has a factor of degree 1 or 2. The two gcd calculations therefore prove irreducibility. We have proved $e_{\text{irr}}(4, p) \geq 9/4$.

Finally, consider the reducible families from Section 3.2. Fix $m \geq 1$ and define

$$F_{m,p,k}(X) = p^{(4m+2)k} F_m(p^{-k}, X).$$

The degree calculations in the proof of Theorem 3.3 show that every coefficient of F_m has degree at most $4m + 2$ in T. Hence $F_{m,p,k} \in \mathbb{Z}[X]$. Moreover,

$$p^{-(4m+2)k} F_{m,p,k}(X) = F_m(p^{-k}, X) \longrightarrow F_m(0, X)$$

coefficientwise with respect to the usual absolute value. The constant resultant identity (11), evaluated at $T = 0$, shows that $F_m(0, X) \neq 0$. Therefore

$$H(F_{m,p,k}) \asymp p^{(4m+2)k}.$$

The coefficients of K_m have degree at most $m + 2$ in T, so

$$p^{(m+2)k} K_m(p^{-k}, X) \in \mathbb{Z}[X] \subseteq \mathbb{Z}_p[X].$$

Since p_m and q_m are monic of degrees $3m - 1$ and $3m$, respectively, their leading terms dominate p-adically at $T = p^{-k}$. Thus

$$|p_m(p^{-k})|_p = p^{(3m-1)k}, \qquad |q_m(p^{-k})|_p = p^{3mk}, \qquad |\beta_m(p^{-k})|_p = p^{-k}.$$

In particular, $\beta_m(p^{-k}) \in \mathbb{Z}_p$. Equations (11) and (15), the latter regarded as a Laurent expansion at infinity, give, for all sufficiently large k,

$$\left| p^{(m+2)k} K_m(p^{-k}, \beta_m(p^{-k})) \right|_p = |8|_p \, p^{-(10m+2)k}$$

and

$$\left| p^{(m+2)k} \frac{\partial K_m}{\partial X}(p^{-k}, \beta_m(p^{-k})) \right|_p = 1.$$

The first absolute value is then smaller than the square of the second. The strong form of Hensel's lemma [20], applied to the normalized polynomial at $\beta_m(p^{-k})$, gives a root $\alpha_{m,p,k} \in \mathbb{Z}_p$ of $K_m(p^{-k}, X)$ satisfying

$$|\alpha_{m,p,k} - \beta_m(p^{-k})|_p = \left| \frac{K_m(p^{-k}, \beta_m(p^{-k}))}{\dfrac{\partial K_m}{\partial X}(p^{-k}, \beta_m(p^{-k}))} \right|_p \asymp p^{-(10m+2)k}.$$

The polynomial K_m is irreducible over $\mathbb{Q}(T)$ and hence separable, while L_m is linear and their resultant is nonzero. Thus $F_m = K_m L_m$ is separable over $\mathbb{Q}(T)$, so $\mathrm{Disc}_X F_m(T, X)$ is a nonzero polynomial in T. Since F_m has degree 4 in X, the leading coefficient of $F_m(T, X)$ with respect to X is also a nonzero polynomial in T. Neither of these two polynomials can vanish at $T = p^{-k}$ for more than finitely many k. Hence $F_{m,p,k}$ is a separable quartic for all sufficiently large k. For such k, $\beta_m(p^{-k})$ is the root of $L_m(p^{-k}, X)$, whereas $\alpha_{m,p,k}$ is a root of $K_m(p^{-k}, X)$, these roots are distinct by (11). Consequently,

$$\mathrm{sep}_p(F_{m,p,k}) \leq |\alpha_{m,p,k} - \beta_m(p^{-k})|_p \asymp p^{-(10m+2)k}.$$

The polynomials $F_{m,p,k}$ are reducible by construction. Letting k tend to infinity and using the height estimate gives, for every fixed $m \geq 1$,

$$e_{\mathrm{red}}(4, p) \geq \frac{10m + 2}{4m + 2}.$$

Letting m tend to infinity gives $e_{\mathrm{red}}(4, p) \geq 5/2$. The upper bound $e(4, p) \leq 3$ follows again from [19, Lemma 2.3, p. 17]. □

We conclude with the matching upper bound conditional on the *abc* conjecture.

Theorem 4.2. *Assume the abc conjecture. Then, for every prime p,*

$$e_{\mathrm{red}}(4, p) = e(4, p) = \frac{5}{2}.$$

Proof. Fix a prime p. We use the *abc* conjecture in the form stated in [3, Section 12.2, p. 402].

We first note the following consequence. If $A, B \in \mathbb{Z}$, $C = A^3 - B^2 \neq 0$, and $p^2 \nmid A$ or $p^3 \nmid B$, then, for every $\epsilon > 0$,

$$|C|_p^{-1} \ll_{p,\epsilon} \max\{1, |A|^{1/2}, |B|^{1/3}\}^{5+\epsilon}.$$

If $AB = 0$, this is immediate. Indeed, if $A = 0$, then $p^3 \nmid B$ and $C = -B^2$, while if $B = 0$, then $p^2 \nmid A$ and $C = A^3$. In either case, $|C|_p^{-1} \leq p^4$.

Suppose that $AB \neq 0$ and put

$$M = \max\{1, |A|^{1/2}, |B|^{1/3}\}, \qquad g = \gcd(|A|^3, |B|^2).$$

The assumption on A and B implies that the highest power of p dividing g is at most p^4. The integers A^3/g, $-B^2/g$, C/g are pairwise coprime, and the maximum of their absolute values is at least M^6/g. Every prime divisor of $|A|^3/g$ divides A, and every prime divisor of $|B|^2/g$ divides B, while every nonzero integer n satisfies $\mathrm{rad}(|n|) \leq p|n||n|_p$, where $\mathrm{rad}(n)$ denotes the product of the distinct prime divisors of a nonzero integer n. Since $g \mid C$ and $|g|_p^{-1} \leq p^4$, it follows that

$$\mathrm{rad}\left(\frac{|C|}{g}\right) \leq p^5 \frac{|C||C|_p}{g}.$$

Therefore

$$\mathrm{rad}\left(\frac{|A|^3|B|^2|C|}{g^3}\right) \leq p^5 \frac{|A||B||C|\,|C|_p}{g} \ll_p \frac{M^{11}|C|_p}{g},$$

where we used $|A| \leq M^2$, $|B| \leq M^3$, and $|C| \leq 2M^6$. After changing signs and rearranging if necessary, the *abc* conjecture gives, for every $\eta > 0$,

$$\frac{M^6}{g} \ll_{p,\eta} \left(\frac{M^{11}|C|_p}{g}\right)^{1+\eta}.$$

Consequently,

$$|C|_p^{-(1+\eta)} \ll_{p,\eta} M^{5+11\eta} g^{-\eta} \leq M^{5+11\eta},$$

and hence

$$|C|_p^{-1} \ll_{p,\eta} M^{5+6\eta/(1+\eta)}.$$

Choosing $\eta > 0$ so that $6\eta/(1+\eta) \leq \epsilon$ proves the claimed consequence.

Now let

$$P = aX^4 + bX^3 + cX^2 + dX + e \in \mathbb{Z}[X]$$

be separable, put $H = H(P)$ and $\delta = \mathrm{sep}_p(P)$, let I, J be its classical invariants defined as in Theorems 3.5 and 3.7, and let Δ be its discriminant. Let λ be the largest power of p such that

$$\lambda^2 \mid 4I, \qquad \lambda^3 \mid 4J.$$

Since $\Delta \neq 0$, by (16), the integers I, J are not both zero, so λ is well defined. Put

$$A = \frac{4I}{\lambda^2}, \qquad B = \frac{4J}{\lambda^3}, \qquad C = A^3 - B^2 = \frac{432\Delta}{\lambda^6}.$$

The separability of P gives $C \neq 0$, while the maximality of λ gives $p^2 \nmid A$ or $p^3 \nmid B$. Thus the preceding consequence applies to A, B. The bounds $|I| \ll H^2$ and $|J| \ll H^3$ imply $\lambda \ll H$ and hence

$$\max\{1, |A|^{1/2}, |B|^{1/3}\} \ll \frac{H}{\lambda}.$$

Label the roots of P so that $|\alpha_1 - \alpha_2|_p = \delta$ and define u, v, w by the same formulas as in the proof of Theorem 3.5. Since $a\alpha_i$ is an algebraic integer for every i, we have

$$|u|_p = |\alpha_1 - \alpha_2|_p |a(\alpha_3 - \alpha_4)|_p \leq \delta.$$

The integrality of A and C gives

$$\max\{|I|_p^{1/2}, |\Delta|_p^{1/6}\} \ll_p \lambda^{-1}.$$

As in the proof of Theorem 3.5, each $z \in \{u, v, w\}$ satisfies $z^3 = Iz + uvw$, and $\Delta = (uvw)^2$. The ultrametric inequality therefore gives

$$|z|_p \leq \max\{|I|_p^{1/2}, |uvw|_p^{1/3}\} = \max\{|I|_p^{1/2}, |\Delta|_p^{1/6}\} \ll_p \lambda^{-1}.$$

It follows that

$$|\Delta|_p \ll_p \delta^2 \lambda^{-4}$$

and consequently

$$\delta \gg_p \lambda^2 |\Delta|_p^{1/2} \asymp_p \lambda^{-1} |C|_p^{1/2}.$$

Applying the preceding consequence with 2ϵ in place of ϵ, we obtain

$$\delta \gg_{p,\epsilon} \lambda^{-1} \left(\frac{H}{\lambda}\right)^{-5/2-\epsilon} = H^{-5/2-\epsilon} \lambda^{3/2+\epsilon} \geq H^{-5/2-\epsilon}.$$

Since $\epsilon > 0$ is arbitrary, this proves $e(4, p) \leq 5/2$. Together with Theorem 4.1, this proves the theorem. □

Unconditionally, the exact values of $e_{\mathrm{irr}}(4, p)$, $e_{\mathrm{red}}(4, p)$, and $e(4, p)$ remain open. Under the *abc* conjecture, Theorem 4.2 determines the latter two, while for the irreducible exponent Theorems 4.1 and 4.2 give only

$$\frac{9}{4} \leq e_{\mathrm{irr}}(4, p) \leq \frac{5}{2}.$$

Funding. The author was supported by the Croatian Science Foundation under the project no. IP-2022-10-5008 (TEBAG). The author acknowledges support from the project "Implementation of cutting-edge research and its application as part of the Scientific Center of Excellence for Quantum and Complex Systems, and Representations of Lie Algebras", Grant No. PK.1.1.10.0004, co-financed by the European Union through the European Regional Development Fund - Competitiveness and Cohesion Programme 2021-2027. This research was funded by the European Union's NextGenerationEU through the National Recovery and Resilience Plan 2021-2026 Institutional grant of University of Zagreb Faculty of Science (IK IA 1.1.3. Impact4Math).

References

[1] D. Badziahin, *Distance between cubics and rationals*, Results Math. **81** (2026), article 58. doi:10.1007/s00025-026-02616-5.

[2] V. Beresnevich and B. Dixon, *p-adic root separation and the discriminant of integer polynomials*, preprint, arXiv:2504.03851v2 (2026). doi:10.48550/arXiv.2504.03851.

[3] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monographs **4**, Cambridge University Press, Cambridge, 2006. doi:10.1017/CBO9780511542879.

[4] Y. Bugeaud, *Approximation by Algebraic Numbers*, Cambridge Tracts in Mathematics **160**, Cambridge University Press, Cambridge, 2004. doi:10.1017/CBO9780511542886.

[5] Y. Bugeaud and A. Dujella, *Root separation for irreducible integer polynomials*, Bull. Lond. Math. Soc. **43** (2011), 1239–1244. doi:10.1112/blms/bdr085.

[6] Y. Bugeaud and A. Dujella, *Root separation for reducible integer polynomials*, Acta Arith. **162** (2014), 393–403. doi:10.4064/aa162-4-6.

[7] J. E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 62–92. doi:10.1112/S1461157000000073.

[8] H. Davenport, *On* $f^3(t) - g^2(t)$, Norske Vid. Selsk. Forh. (Trondheim) **38** (1965), 86–87. MR0186621.

[9] A. Dujella, *On Hall's conjecture*, Acta Arith. **147** (2011), 397–402. doi:10.4064/aa147-4-5.

[10] A. Dujella and T. Pejković, *Root separation for reducible monic quartics*, Rend. Semin. Mat. Univ. Padova **126** (2011), 63–72. doi:10.4171/RSMUP/126-4.

[11] J.-H. Evertse, *Distances between the conjugates of an algebraic number*, Publ. Math. Debrecen **65** (2004), 323–340. doi:10.5486/PMD.2004.3313.

[12] G. Fischer, *Plane Algebraic Curves*, Student Mathematical Library **15**, American Mathematical Society, Providence, RI, 2001. doi:10.1090/stml/015.

[13] F. Q. Gouvêa, *p-adic Numbers. An Introduction*, 2nd ed., Springer, Berlin, 1997. doi:10.1007/978-3-642-59058-0.

[14] M. Hall, Jr., *The Diophantine equation* $x^3 - y^2 = k$, in A. O. L. Atkin and B. J. Birch (eds.), *Computers in Number Theory*, Academic Press, London, 1971, 173–198. MR0323705.

[15] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge University Press, Cambridge, 1997. doi:10.1017/CBO9780511525926.

[16] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262. doi:10.1307/mmj/1028999140.

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

[18] T. Pejković, *Root separation for reducible integer polynomials of degrees four and five*, preprint, 2026. author's preprint.

[19] T. Pejković, *Polynomial root separation and applications*, PhD thesis, Université de Strasbourg, Strasbourg, 2012. HAL tel-00656877.

[20] A. M. Robert, *A Course in p-adic Analysis*, Graduate Texts in Mathematics **198**, Springer, New York, 2000. doi:10.1007/978-1-4757-3254-2.

[21] A. Schönhage, *Polynomial root separation examples*, J. Symbolic Comput. **41** (2006), 1080–1090. doi:10.1016/j.jsc.2006.06.003.

[22] A. J. van der Poorten, *Formal power series and their continued fraction expansion*, in J. P. Buhler (ed.), *Algorithmic Number Theory*, ANTS-III, Lecture Notes in Comput. Sci. **1423**, Springer, Berlin, 1998, 358–371. doi:10.1007/BFb0054875.

Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address: pejkovic@math.hr