ROOT SEPARATION FOR POLYNOMIALS OVER $\mathbb{F}_q[T]$

Abstract. We study the minimum distance between distinct roots of a separable polynomial of degree $d \geq 2$ over $\mathbb{F}_q[T]$, with respect to the absolute value $|T| = q$. For reducible polynomials of height H, the exponent $d-1$ in the lower bound $H^{-(d-1)}$ is best possible in every degree. In characteristic two we construct absolutely irreducible polynomials that attain this bound at every height q^N, $N \geq 1$. In odd characteristic p, the exponent $d-1$ is best possible for absolutely irreducible polynomials whenever $d-1 = p^a m$ with $p \nmid m$ and $m \mid p^a - 1$. The separation exponents for irreducible and absolutely irreducible polynomials coincide for every q and d.

hexagon:2611.00692v1

Use of artificial intelligence. The research was carried out under human direction from the choice of topic and research questions to the selection of results for the paper. OpenAI's ChatGPT 6.2 Astra developed the constructions and proofs and drafted the manuscript. Anthropic's Claude Fable 5.2 reviewed the manuscript, checked examples, and suggested improvements to the proofs and to the comparison with known results. The human review did not include an independent check of every proof.

1. Introduction

How close can two distinct roots of an integer polynomial of given degree and height be? For a separable integer polynomial of degree d and height H, Mahler [9] gave a lower bound of order $H^{-(d-1)}$ for the distance between any two distinct roots. In the other direction, Bugeaud and Dujella [3, Theorem 1] constructed, for each $d \geq 4$, reducible integer polynomials of arbitrarily large height H with two roots at distance $\ll_d H^{-(2d-1)/3}$. We refer to Bugeaud and Mignotte [5] for a survey.

Here we consider polynomials with coefficients in $k[T]$, where $k = \mathbb{F}_q$ is the finite field with q elements. Write p for the characteristic of k and put $K = k(T)$. For nonzero $a, b \in k[T]$ set $|a/b| = q^{\deg a - \deg b}$. The completion of K for this absolute value is the field of Laurent series $K_\infty = k((T^{-1}))$. We extend this absolute value to an algebraic closure of K_∞ and write $v = -\log_q |\cdot|$.

Throughout the paper, $F = \sum_{i=0}^{d} a_i X^i \in k[T][X]$ is a primitive separable polynomial of degree $d \geq 2$ in X, with roots $x_1, \ldots, x_d$. Thus the coefficients a_i have no common factor of positive degree. We define its height $H(F)$ and its separation $\operatorname{sep}(F)$ by

$$h(F) = \max_i \deg_T a_i, \quad H(F) = q^{h(F)},$$
$$\operatorname{sep}(F) = \min_{i<j} |x_i - x_j|, \quad s(F) = -\log_q \operatorname{sep}(F).$$

Here $h(F)$ is the logarithmic height of F, and $\deg 0 = -\infty$. For $u = a/b$ with coprime polynomials $a, b \in k[T]$ and $b \neq 0$, put $h(u) = \max(\deg a, \deg b)$ and $H(u) = q^{h(u)}$.

For fixed q and d, we define the separation exponent by

$$E_q(d) = \limsup_{h(F)\to\infty} \frac{s(F)}{h(F)}.$$

2020 *Mathematics Subject Classification.* Primary 11C08; Secondary 11J61, 11T55.

Key words and phrases. Root separation, polynomial height, function fields of positive characteristic, Diophantine approximation.

Tomislav Pejković proposed the topic and guided the research presented in this paper. Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia (pejkovic@math.hr).

We write $E_{q,\mathrm{red}}(d)$, $E_{q,\mathrm{irr}}(d)$ and $E_{q,\mathrm{abs}}(d)$ when F ranges over the reducible, irreducible and absolutely irreducible polynomials, respectively. The first two classes are defined over K. We say that F is absolutely irreducible if it remains irreducible over $\bar{k}(T)$, where $\bar{k}$ is an algebraic closure of k. Since F is primitive, this is equivalent to irreducibility in $\bar{k}[T, X]$.

The discriminant gives

$$\mathrm{sep}(F) \geq H(F)^{-(d-1)}. \tag{1}$$

In particular, $E_q(d) \leq d-1$. To compare $\mathrm{sep}(F)$ with the right-hand side of (1), we write $\Delta(F) = (d-1)h(F) - s(F)$ for the loss in this bound. Thus $\mathrm{sep}(F) = q^{\Delta(F)} H(F)^{-(d-1)}$. Along any sequence with $h(F) \to \infty$, the quotient $s(F)/h(F)$ tends to $d-1$ if and only if $\Delta(F) = o(h(F))$.

Theorem 1.1. *Let $n = d-1 \geq 1$. Over every finite field k there are polynomials F of arbitrarily large logarithmic height h with $\Delta(F) \ll_d \sqrt{h}$. We may take $F = LG$, where L is linear and G is absolutely irreducible of degree n. In particular,*

$$E_{q,\mathrm{red}}(d) = E_q(d) = d-1.$$

Every reducible F of logarithmic height $h \geq n-1$ satisfies $\Delta(F) \geq n-1$. Equality holds for infinitely many values of h if and only if $p \nmid n$ or n is a power of p. In all other cases $\Delta(F) \geq 2(n-1)$ for all sufficiently large h.

For $n \geq 2$, the equality $E_{q,\mathrm{red}}(n+1) = n$ also follows from a theorem of Badziahin [1, Theorem 5]. Given $0 < \varepsilon < 1$, he proves that the product $|\alpha - u|(H(\alpha)H(u))^{n-\varepsilon}$ can be arbitrarily small for $u \in K$ and $\alpha \in K_\infty$ of degree n over K. Here $H(\alpha)$ is the height of the primitive polynomial $P \in k[T][X]$ associated with the minimal polynomial of α over K. To see that α is separable, suppose that $P_X = 0$. Differentiating $P(T, \alpha) = 0$ with respect to T gives $P_T(T, \alpha) = 0$. Hence P divides P_T in $k[T][X]$ by Gauss's lemma, and comparison of degrees in T gives $P_T = 0$. Since k is perfect, P would be a pth power. This contradicts its irreducibility. Multiplying P by the primitive linear polynomial with root u gives a reducible polynomial of height $H(\alpha)H(u)$. These heights are unbounded, since there are only finitely many polynomials of bounded degree and height over $k[T]$. Letting ε tend to zero gives the required equality.

The proof of Theorem 1.1 gives explicit bounds for $\Delta(F)$. For $p \nmid n$ we use an example of Osgood [11, 2]. For n a power of p we use a lacunary power series as in Mahler's construction [8]. In both cases the factor of degree n is fixed. In the construction for the remaining degrees both factors vary.

When can Δ stay bounded as the height tends to infinity? For reducible polynomials of degree $n+1$, this happens precisely when some finite group of fractional linear transformations of the projective line over $\bar{k}$ has an orbit of size n. In those degrees the factor of degree n can be kept fixed. In every other degree all reducible polynomials of sufficiently large logarithmic height satisfy $\Delta \gg_n \sqrt{h}$, and the construction of Theorem 1.1 shows that this order is best possible. Theorem 7.1 gives the list of degrees. For example, when $d = 29$ and $p = 7$, every reducible F of sufficiently large height satisfies $28h - s(F) \gg \sqrt{h}$, and there are polynomials of arbitrarily large height for which $28h - s(F) \ll \sqrt{h}$.

Theorem 1.2. *Let $d \geq 2$. In characteristic two, for every integer $N \geq 1$ there is an absolutely irreducible polynomial of degree d and height q^N for which equality holds in (1). For $d \geq 3$ the polynomial can be chosen monic in X. In particular, $E_{q,\mathrm{abs}}(d) = d-1$.*

In odd characteristic write $d-1 = p^a m$ with $a \geq 0$ and $p \nmid m$. If $m \mid p^a - 1$, there are absolutely irreducible polynomials F of degree d and arbitrarily large logarithmic height h satisfying $\Delta(F) \ll_d \sqrt{h}$. Hence $E_{q,\mathrm{abs}}(d) = d-1$ in this case as well.

If $p \nmid d-1$, then $a = 0$ and the condition $m \mid p^a - 1$ always holds. If d is also odd, Section 5.1 gives the stronger estimate $\Delta(F) = O_d(1)$ along a sequence of unbounded heights. For an example with $p \mid d-1$, take $d = 11$ and $p = 5$. The construction in odd characteristic uses the identity $|x^{p^j} - y^{p^j}| = |x-y|^{p^j}$. Starting with two conjugate roots near a critical point, we take their p^jth powers and make a linear change of variable. We estimate the height of the resulting polynomial. By (1), the minimal polynomial of either transformed root over $\bar{k}(T)$ must then have degree d.

For every q and d, Section 5 gives $E_{q,\mathrm{abs}}(d) \geq d-8$. We obtain the stronger lower bound $d-4$ if $p \neq 3$ and $d-2$ if d is odd or divisible by four. In Section 6 we fix a divisor $c > 1$ of d and consider irreducible polynomials for which $K(x)$, with x a root, has constant field $\mathbb{F}_{q^c}$. For this class the exponent is $2d/c^2$. It follows that $E_{q,\mathrm{irr}}(d) = E_{q,\mathrm{abs}}(d)$ for all q and d.

2. Reducible polynomials

2.1. **Estimates from the discriminant and the resultant.** The Gauss norm of a polynomial over a non-Archimedean valued field is the maximum of the absolute values of its coefficients. It is multiplicative. Indeed, after dividing each factor by a coefficient of maximal absolute value, both factors have nonzero reduction modulo the maximal ideal, and so does their product. In particular, $h(AB) = h(A) + h(B)$. For $F = a_d \prod_i (X - x_i)$, put $M_i = \max(1, |x_i|)$. Then $H(F) = |a_d| \prod_i M_i$. Choose two roots at distance $\mathrm{sep}(F)$. For every other pair use $|x_i - x_j| \leq M_i M_j$ in the formula for the discriminant. Since $\operatorname{Disc} F$ is a nonzero polynomial in T, we obtain

$$\mathrm{sep}(F) \geq |\operatorname{Disc} F|^{1/2} H(F)^{-(d-1)} \geq H(F)^{-(d-1)}.$$

For irreducible polynomials see also Ooto [10, Lemma 3.3]. Applying the same argument to the resultant of two coprime polynomials A, B of degrees i, j, respectively, gives

$$v(x-y) \leq jh(A) + ih(B) - \deg_T \operatorname{Res}_X(A,B) \tag{2}$$

for every root x of A and every root y of B.

2.2. **A lower bound for Δ and examples of equality.** Let W be reducible of degree $n+1$. For $n = 1$, (1) gives $\Delta(W) \geq 0$. Suppose that $n \geq 2$. If $s(W) \leq (n-1)h(W)$, then $\Delta(W) \geq h(W)$. Otherwise, two roots at distance $\mathrm{sep}(W)$ must belong to different irreducible factors by (1). If both factors had degree at most $n-1$, (2) would give $s(W) \leq (n-1)h(W)$. Thus one factor has degree n and the other is linear. Applying (2) to them gives

$$W(X) = F(X)(bX - a), \qquad \Delta(W) \geq (n-1)h(F) + \deg_T \operatorname{Res}_X(F, bX-a), \tag{3}$$

where F is irreducible of degree n and $a, b \in k[T]$ are coprime. If $h(F) = 0$, each root of F is a constant outside k. Its distance from a/b is at least one, since a/b has residue in k whenever $|a/b| \leq 1$. This contradicts $s(W) > (n-1)h(W)$, so $h(F) \geq 1$. We conclude that $\Delta(W) \geq n-1$ whenever $h(W) \geq n-1$.

Suppose first that $p \nmid n$. Let r run through the powers of p congruent to 1 modulo n, and put $j = (r-1)/n$. Take $F = TX^n - (T+1)$ and $u = T^j/(T+1)^j$. Then $(T+1)^{nj} F(u) = -1$, so $v(F(u)/T) = r$. The reduction of F/T modulo T^{-1} is $X^n - 1$, which has n simple roots. Since u reduces to 1, exactly one root x of F satisfies $v(x-u) > 0$, and for this root $v(x-u) = r$. The product $F(X)((T+1)^j X - T^j)$ therefore has logarithmic height $j+1$ and $\Delta = n-1$. Eisenstein's criterion at $T+1$ shows that F is absolutely irreducible.

Next suppose that $n = P = p^e$ with $e \geq 1$, and take $F = X^P + TX - 1$. It is separable since $F_X = T$. As a polynomial in T it is linear with coprime coefficients X and $X^P - 1$,

so it is absolutely irreducible. Put $B_j = (P^j - 1)/(P - 1)$ and

$$\alpha = \sum_{i \geq 1} (-1)^{i-1} T^{-B_i}, \qquad u_j = \sum_{i=1}^{j} (-1)^{i-1} T^{-B_i}.$$

The recurrence $B_{i+1} = PB_i + 1$ gives $T\alpha = 1 - \alpha^P$, so $F(\alpha) = 0$. Moreover, $h(u_j) = B_j$ and $v(\alpha - u_j) = PB_j + 1$. The difference z between any two distinct roots of F satisfies $z^{P-1} = -T$, whence $|z| > 1$. Thus the product $W_j = F(X)T^{B_j}(X - u_j)$ has logarithmic height $B_j + 1$ and satisfies $s(W_j) = PB_j + 1$. It follows that $\Delta(W_j) = P - 1$.

2.3. **A construction for the remaining degrees.** Suppose that $n = mP$, where $P > 1$ is a power of p, $m > 1$ and $p \nmid m$. We construct a polynomial $Q(Z, X)$ of degree n in X and a polynomial $V(Z)$ such that $Q(Z, V(Z))$ has a zero of high order at $Z = 1$. Take arbitrarily large powers $R = P^t > n$ with $R \equiv 1 \pmod{m}$. Put $M = (R - 1)/m$ and

$$V(Z) = \sum_{i=0}^{t-1} Z^{MP^i}.$$

Then $V^P - V + Z^M = Z^{MR}$. Raising both sides to the mth power and multiplying by Z^R gives

$$Q(Z, X) = Z^R(X^P - X + Z^M)^m - 1, \qquad Q(Z, V(Z)) = Z^{R^2} - 1 = (Z - 1)^{R^2}.$$

Write $D = \deg_Z Q = 2R - 1$ and $E = \deg V = MR/P$. As a polynomial in X, Q has leading coefficient Z^R and constant term $Z^{2R-1} - 1$, so it is primitive. The polynomial $Q(1, X) = (X^P - X + 1)^m - 1$ has n simple roots, one of which is $V(1)$. By Hensel's lemma there is a unique root x of Q in $\bar{k}[[Z - 1]]$ with $x(1) = V(1)$. The factorization of $Q(Z, V(Z))$ shows that $x - V$ has a zero of order R^2 at $Z = 1$, since the leading coefficient of Q and the other factors are units there.

We now prove that Q is absolutely irreducible. Since $V(1)$ is a simple root of $Q(1, X)$, exactly one irreducible factor C of Q over $\bar{k}[Z, X]$ vanishes at $(1, V(1))$, and it occurs only once. It follows that $C(Z, V(Z))$ is divisible by $(Z - 1)^{R^2}$. Now $R + nE = R^2$ and $E = (R - 1)R/n > R - 1$, so

$$D + (n - 1)E = R^2 + R - 1 - E < R^2.$$

Since $\deg_Z C(Z, V(Z)) \leq D + E \deg_X C$, we must have $\deg_X C = n$. Primitivity now gives the desired irreducibility.

In the product $Q(Z, X)(X - V(Z))$ substitute $Z = 1 + T^{-1}$ and multiply by T^{D+E} to clear denominators. Denote the resulting polynomial by W. Its coefficients have no common zero in $\bar{k}$. Indeed, any common zero $T_0 \neq 0$ would give a common zero $1 + T_0^{-1}$ of the coefficients of the original product, which is primitive. At $T = 0$, W is the nonzero coefficient of Z^{D+E} in that product. Thus W is primitive. Its logarithmic height is $D + E$ because $Q(1, X)(X - V(1)) \neq 0$. The roots of Q have distinct residues at $Z = 1$, and exactly one agrees with V to order R^2. Hence

$$s(W) = R^2, \qquad \Delta(W) = n(D + E) - R^2 = (2n - 1)R - n.$$

In particular, $h(W) \geq R^2/n$ and $\Delta(W) \ll_d \sqrt{h(W)}$.

2.4. **A necessary condition for equality.**

Completion of the proof of Theorem 1.1. Suppose that $p \mid n$, that n is not a power of p, and that $\Delta(W) < 2(n - 1)$ for a sequence of reducible polynomials W of degree $n + 1$ with $h(W) \to \infty$. For all sufficiently large $h(W)$, (3) gives $W = F(X)(bX - a)$ with $h(F) = 1$ and $\deg_T \operatorname{Res}_X(F, bX - a) < n - 1$. As k is finite, only finitely many

polynomials F can occur. Passing to a subsequence, we may therefore assume that F is fixed. The reduced fractions a/b take infinitely many values, whereas the nonzero resultants $S_{a,b}(T) = \mathrm{Res}_X(F, bX - a)$ range over a finite set.

Write $F(T, X) = C(X)T + D(X)$ with C, D coprime, and put $f = -D/C$. Then f is a separable rational function of degree n. We shall show that the cross-ratio of any four distinct roots of $f(X) = T$ belongs to $\bar{k}$. For each of the fractions a/b consider the rational function

$$g_{a,b}(X) = b(f(X))X - a(f(X)).$$

It is nonzero, since $X = a(f(X))/b(f(X))$ would imply $\deg f = 1$. Every finite pole of $g_{a,b}$ is a pole of f. If x is a finite zero of $g_{a,b}$ and $f(x)$ is finite, then x is a common root of $F(f(x), Y)$ and $b(f(x))Y - a(f(x))$. Hence $S_{a,b}(f(x)) = 0$. There are only finitely many such values $f(x)$, and each has only finitely many preimages. Thus the numerators and denominators of all the $g_{a,b}$ have their irreducible factors in a fixed finite set.

Fix a power $R = p^j$. There are only finitely many ways to choose, modulo R, the exponents of these irreducible factors in $g_{a,b}$. Since every constant in k has an Rth root in k, there are two distinct fractions $a/b, c/d_0$ for which $g_{a,b}/g_{c,d_0}$ is an Rth power in $k(X)$. Evaluating at each root x_i of $f(X) = T$, we find that

$$\frac{b(T)x_i - a(T)}{d_0(T)x_i - c(T)}$$

is an Rth power in the splitting field L of F. Fractional linear transformations preserve cross-ratios. Thus the cross-ratio of any four distinct roots of F belongs to L^R for every $R = p^j$. If $z \in L$ is transcendental over k, then $[L : k(z)]$ is finite. If also $z = u^R$ for some $u \in L$, then $[k(u) : k(z)] = R$, so $R \leq [L : k(z)]$. Consequently every cross-ratio belongs to $\bar{k}$. By Lemma 2.1, applied over $\bar{k}$, n must be a power of p, a contradiction. □

For a related criterion in the rational approximation of algebraic Laurent series, see Voloch [13]. Lasjaunias and de Mathan [7, Lemma 3.2] give a proof of Voloch's lemma.

Lemma 2.1. *Let k_0 be an algebraically closed field of characteristic p and let $f \in k_0(X)$ be a separable rational function of degree n divisible by p. If the cross-ratio of any four distinct roots of $f(X) = T$ belongs to k_0, then n is a power of p.*

Proof. Write $n = mP$, where P is the largest power of p dividing n, and suppose that $m > 1$. Then $n \geq 6$. Let v_0 be a valuation of the splitting field of $f(X) = T$ that is trivial on k_0. Since k_0 is infinite, a fractional linear transformation over k_0 makes the reductions of all the roots finite. If x_1, x_2 have the same reduction and x_3, x_4 both reduce to other points, then

$$v_0\left(\frac{(x_1 - x_2)(x_3 - x_4)}{(x_1 - x_3)(x_2 - x_4)}\right) > 0.$$

Indeed, the numerator vanishes upon reduction and the denominator is a unit. This is impossible because the cross-ratio is a nonzero constant. Thus, if two roots have the same reduction, at least $n-1$ roots have that reduction. Since fractional linear transformations preserve cross-ratios, this conclusion also holds after a change of coordinates over an extension field.

We apply this observation to the fibers of f. Factor the homogeneous equation of a fiber into linear forms and normalize each form to have Gauss norm one. The scalar multiplying their product is a unit, since the homogeneous numerator and denominator of f have no common zero. Reduction therefore gives the roots of the specialized equation with their multiplicities. Hence each ramified fiber consists either of a single point of multiplicity n or of two points of multiplicities $n - 1$ and 1.

We claim that f is totally ramified at some point. Otherwise every ramification index greater than one would equal $n-1$, which is prime to p. Write $f = A/B$ in lowest terms and homogenize $A'B - AB'$ to degree $2n-2$. The zeros of this form are the critical points of f. At a point of ramification index e prime to p, differentiation in local coordinates shows that the form vanishes to order $e-1$. Thus every zero would have multiplicity $n-2$, forcing $n-2$ to divide $2n-2$. This is impossible for $n \geq 6$.

Choose coordinates on the source and target so that a totally ramified point and its image are both zero. The numerator has a zero of order n at 0, so $f(X) = aX^n/B(X)$ with $aB(0) \neq 0$. Substituting $T = t^n$ and $X = tY$ gives

$$aY^n - B(tY) = 0.$$

The leading coefficient is a unit at $t = 0$. The reduction $aY^n - B(0)$ has m distinct roots, each of multiplicity P. Thus exactly P of the roots reduce to each of these points. Since $1 < P < n-1$, this contradicts the conclusion of the first paragraph. □

3. Equality in characteristic two

Proof of Theorem 1.2 in characteristic two. Fix $N \geq 1$. For $d = 2$, take $G = T^N X^2 + X + 1$. Its reciprocal polynomial $T^N + X^2 + X$, regarded as a polynomial in T over $\bar{k}[X]$, is irreducible by Eisenstein's criterion at X. Thus G is absolutely irreducible, and its two roots differ by T^{-N}.

For $d \geq 3$, we construct a monic polynomial F whose reciprocal attains equality in (1). Write $\ell = d-2$, let e be the least even integer greater than or equal to ℓ, and put

$$A = (X+1)^{e-\ell}, \qquad B = \frac{X^e + X}{A}, \qquad F = B(X)(X^2 + T^N) + A(X).$$

Since $X^e + X$ has derivative one and vanishes at both 0 and 1, the polynomials A and B are coprime. The polynomial B is monic and squarefree of degree ℓ, with $B(0) = 0$ and $A(0) = 1$. Thus F and $G = X^d F(1/X)$ are both monic of degree d and logarithmic height N. As a polynomial in Z over $\bar{k}[X]$, $(BX^2 + A)Z^N + B$ is primitive and satisfies Eisenstein's criterion at X. Substituting $Z = 1/T$ and clearing denominators gives F, so F and G are both absolutely irreducible.

Reducing $T^{-N}F$ modulo T^{-1} gives B. By Hensel's lemma, each of the ℓ simple roots of B lifts to a unique root of F of absolute value at most one. Every such root reduces to a root of B. The remaining two roots x_1, x_2 satisfy $|x_i| > 1$ and $x_i^2 + T^N = A(x_i)/B(x_i)$. Since A and B are monic and $\deg A \leq \deg B$, the right-hand side has absolute value at most one. Hence $|x_1| = |x_2| = R$, where $R = q^{N/2}$.

In characteristic two we have $BF' - B'F = (AB)' = 1$, so F is separable and $|F'(x_1)| = |B(x_1)|^{-1} = R^{-\ell}$. Each of the ℓ roots of absolute value at most one is at distance R from x_1. Since F is monic, the identity $F'(x_1) = \prod_{x \neq x_1}(x_1 - x)$ gives $R^\ell |x_1 - x_2| = R^{-\ell}$. The distance between the corresponding roots of G is therefore $R^{-2\ell-2} = q^{-(d-1)N}$, as required. □

4. Absolutely irreducible polynomials in odd characteristic

In odd characteristic we can strengthen (1) for absolutely irreducible polynomials of logarithmic height at least two.

Proposition 4.1. *Let F be a separable absolutely irreducible polynomial of degree $d \geq 2$ and logarithmic height $h \geq 2$. If p is odd, then*

$$s(F) \leq (d-1)(h-1) + \tfrac{1}{2}, \qquad \textit{or equivalently} \qquad \Delta(F) \geq d - \tfrac{3}{2}.$$

Proof. Put $t = 1/T$. Choose $a \in \bar{k}$ different from the residue of every root x_i of F for which $|x_i| \le 1$. Then $|x_i - a| = M_i = \max(1, |x_i|)$ for every i. The roots $y_i = 1/(x_i - a)$ of the polynomial

$$G(t, Y) = t^h Y^d F(1/t, a + 1/Y)$$

all have absolute value at most one. Moreover, $\deg_t G \le h$, and its leading coefficient as a polynomial in Y is nonzero at $t = 0$ because $|F(T, a)| = H(F)$. Substituting $|y_i - y_j| = |x_i - x_j|/(M_i M_j)$ in the formula for the discriminant gives

$$\sum_{i<j} v(y_i - y_j) = (d-1)h - \tfrac{1}{2} \deg_T \operatorname{Disc} F \le (d-1)h.$$

Let $m = (d-1)(h-1) + 1$ and suppose that $s(F) > m - \frac{1}{2}$. As $h \ge 2$, we have $2s(F) > (d-1)h$. At least one pair satisfies $v(y_i - y_j) \ge s(F)$, since $M_i M_j \ge 1$. All terms in the sum above are nonnegative, so there is exactly one such pair, say y_1, y_2. Every automorphism of the splitting field of G over $\bar{k}((t))$ preserves the set $\{y_1, y_2\}$. Hence $b = (y_1 + y_2)/2$ belongs to $\bar{k}[[t]]$ and $(y_1 - y_2)^2$ belongs to $\bar{k}((t))$. In particular $2v(y_1 - y_2)$ is an integer greater than $2m - 1$. It follows that $v(y_i - b) \ge m$ for $i = 1, 2$.

We now choose a nonzero polynomial $Q \in \bar{k}[t, Y]$ of degree at most $h - 1$ in t and at most $d-1$ in Y. The condition $Q(t, b) \equiv 0 \pmod{t^m}$ gives at most m homogeneous linear equations in the hd coefficients of Q. Choose $h + d - 3$ distinct nonzero elements $c \in \bar{k}$ at which the leading coefficient of G in Y does not vanish. For each c, choose a root z of $G(c, Y)$ and impose the additional equation $Q(c, z) = 0$. Since $m + h + d - 3 = hd - 1$, the system has a nonzero solution.

The resultant $D(t) = \operatorname{Res}_Y(G, Q)$ is nonzero since G is irreducible over $\bar{k}(t)$ and $\deg_Y Q < d$. Its degree is at most $d(h-1) + (d-1)h$. On the other hand, $v(Q(t, y_i)) \ge m$ for $i = 1, 2$, since $v(y_i - b) \ge m$ and $Q(t, b) \equiv 0 \pmod{t^m}$. The product formula for the resultant now gives a zero of order at least $2m$ at $t = 0$. Also $D(c) = 0$ at each of the $h + d - 3$ points chosen above. Thus

$$\deg D \ge 2m + h + d - 3 = d(h-1) + (d-1)h + 1,$$

a contradiction. □

For every $d \ge 3$, equality in Proposition 4.1 is attained at $h = 2$ by a polynomial monic in X. To see this, put

$$g_0(z) = 1 + z, \qquad g_{i+1}(z) = 1 + \frac{z^2}{g_i(z)}, \qquad T = z^{-2} + g_{d-3}(z), \qquad y = z^2.$$

Write $g_i = A_i/B_i$ in lowest terms. The recursion replaces (A_i, B_i) by $(A_i + z^2 B_i, A_i)$. The two polynomials remain coprime, have constant term one and have degrees $i+1, i$ at step i. Write $T = P(z)/Q(z)$ in lowest terms. Since $\deg P = d$ and $\deg Q = d-1$, the equation $P(z) - TQ(z) = 0$ shows that z is integral over $k[T]$. Moreover, $g_0(z) - g_0(-z) = 2z$, and each step multiplies this difference by $-z^2/(g_i(z) g_i(-z))$. Hence, for $g = g_{d-3}$,

$$\operatorname{ord}_{z=0}\big(g(z) - g(-z)\big) = 2d - 5.$$

In particular $T(z) \ne T(-z)$, so $k(T, y) = k(z)$, also after extending the constants to $\bar{k}$. The monic minimal polynomial of y over $k(T)$ therefore belongs to $k[T][X]$, is absolutely irreducible and has degree d in X. Its degree in T is $[k(z) : k(z^2)] = 2$. It is separable since the pole of T at zero has order two.

Put $w = T^{-1/2}$. Substituting $z = wZ$ gives $Z^2 = 1 + w^2 Z^2 g(wZ)$. Its roots $1, -1$ modulo w are simple and lift to roots $Z_+, Z_- \in \bar{k}[[w]]$. Put $z_\pm = wZ_\pm$. Since g is regular

at zero, $v(g(z_-) - g(-z_+)) \geq v(z_- + z_+)$. On the other hand,

$$v\big(g(z_+) - g(z_-)\big) = v\left(\frac{z_+^2 - z_-^2}{z_+^2 z_-^2}\right) = v(z_+ + z_-) - \tfrac{3}{2}.$$

The last quantity is therefore also $v(g(z_+) - g(-z_+)) = (2d-5)/2$. It follows that $v(z_+^2 - z_-^2) = d - \frac{1}{2}$, as required.

For quadratics equality holds at every logarithmic height $h \geq 2$, and for cubics it holds at arbitrarily large heights. For the quadratic example, let $h \geq 1$ and take $\delta \in \{0,1\}$ with $\delta \equiv h \pmod 2$. The polynomial

$$(T^h - T^{1-\delta})X^2 - 2T^{(h+\delta)/2}X + T^\delta$$

is primitive. Its discriminant $4T$ is not a square in $\bar{k}(T)$, so the polynomial is absolutely irreducible. Since its leading coefficient has degree h, the quadratic formula gives $s = h - \frac{1}{2}$. This also proves Theorem 1.2 for $d = 2$.

For the cubic example we use the continued fraction of a root, as in Schönhage's construction over the integers (see Bugeaud and Mignotte [5, Section 6]). As a polynomial in T, the cubic $X^3 + TX - 1$ is linear with relatively prime coefficients X and $X^3 - 1$, so it is absolutely irreducible. With $t = 1/T$, Hensel's lemma applied to $tX^3 + X - t$ gives a root $\alpha \in K_\infty$ with $|\alpha| = q^{-1}$. The other two roots β, γ of the cubic satisfy $\beta + \gamma = -\alpha$ and $\beta\gamma = T + \alpha^2$. It follows that $|\beta| = |\gamma| = q^{1/2}$ and, since $p \neq 2$, that $|\beta - \gamma| = q^{1/2}$.

Let A'/B' and A/B be two consecutive convergents of the continued fraction of α, with $n = \deg B \geq 1$. By Ooto [10, Lemma 4.1], $AB' - A'B \in k^\times$, $|B\alpha - A| < q^{-n}$ and $|B'\alpha - A'| = q^{-n}$. Since the determinant is a unit, the substitution $y = (B'x - A')/(Bx - A)$ preserves primitivity and absolute irreducibility. Up to a factor in $k^\times$, the resulting cubic is the product of the three linear factors $(Bx - A)Y - (B'x - A')$ for $x = \alpha, \beta, \gamma$. Their Gauss norms are q^{-n}, $q^{n+1/2}$ and $q^{n+1/2}$, respectively. The cubic therefore has logarithmic height $n + 1$, and the distance between the images of β and γ is

$$\frac{|\beta - \gamma|}{|B\beta - A|\,|B\gamma - A|} = q^{-2n-1/2}.$$

Proposition 4.1 now gives $s = 2n + \frac{1}{2}$ and $\Delta = \frac{3}{2}$. Since α is irrational, the degrees of the denominators of its convergents tend to infinity.

We shall approximate an element of a quadratic extension of $k(T)$ by rational functions in $k(T)$. We use the following elementary observation. If an involution interchanges z and z' and sends w to $1/w$, then it fixes

$$y = \frac{zw + z'}{w + 1}.$$

When $z \neq z'$, we can solve for w to obtain $w = (z' - y)/(y - z)$.

Lemma 4.2. *Let k be a field of odd characteristic p, let σ be an indeterminate and put $T = \sigma + \sigma^{-1}$. For $g \in k(\sigma)$ write $g^*(\sigma) = g(\sigma^{-1})$, and let ord_0 denote the order at $\sigma = 0$. Suppose that $g \neq g^*$. For every power r of p, the rational function*

$$B_r(g) = \frac{g - \sigma^r g^*}{1 - \sigma^r}$$

belongs to $k(T)$ and satisfies

$$h(B_r(g)) \leq r/2 + O_g(1), \qquad \operatorname{ord}_0(B_r(g) - g) = r + \operatorname{ord}_0(g - g^*).$$

For all sufficiently large powers r of p, there is also a rational function $V_r \in k(T)$ with a simple pole at $T = 2$ such that

$$h(V_r) \leq r/2 + O_g(1), \qquad \operatorname{ord}_0(V_r - g) = r + O_g(1).$$

Proof. Take $z = g^*$, $z' = g$ and $w = -\sigma^r$ in the observation above. Then $B_r(g)$ is fixed by $\sigma \mapsto \sigma^{-1}$ and hence belongs to $k(T)$. Clearing the denominators of g and g^* shows that $B_r(g)$ has degree at most $r + O_g(1)$ in σ. Its degree in σ is twice its height as a rational function of T, since T has degree two in σ. The formula for the order at zero follows from $B_r(g) - g = \sigma^r(g - g^*)/(1 - \sigma^r)$.

To obtain the pole at $T = 2$, put $G = 1/(T-2)$, $w = 1/(g-G)$ and $V_r = G + 1/B_r(w)$. We have $w \neq w^*$ and $h(V_r) \leq h(G) + h(B_r(w)) \leq r/2 + O_g(1)$. For large r, $B_r(w)$ and w have the same order at zero. Thus $V_r - g = (w - B_r(w))/(wB_r(w))$ has order $r + O_g(1)$ at zero. At $\sigma = 1$ the denominator of $B_r(w)$ is $(1-\sigma)^r$. For large r the order of its numerator $w - w^* + (1-\sigma)^r w^*$ equals that of $w - w^*$. Hence $1/B_r(w)$ vanishes at $T = 2$, and V_r has a simple pole there. □

Suppose now that p is odd. Put $n = d - 1$ and let P be the largest power of p dividing n. Thus $P = 1$ when $p \nmid n$. Write $n = mP$ and suppose that $n \geq 2$ and $m \mid P - 1$. The proof starts with a polynomial of degree $n + 1$ whose reduction has precisely one double root. The two roots reducing to it are conjugate over the Laurent series field $\bar{k}((\sigma))$. We use their Rth powers, where R is a power of p, to construct a polynomial over $k(T)$. The distance between the resulting roots will rule out every proper factor containing them.

Proof of Theorem 1.2 in odd characteristic. Put $L(X) = X$ if $P = 1$ and $L(X) = X^P - X$ otherwise. Its derivative $\epsilon = L'$ is 1 or -1, respectively. The polynomial L is additive and satisfies

$$L(bY) = bD_{b^m}(Y), \qquad D_U(Y) = \begin{cases} Y, & P = 1, \\ U^{(P-1)/m}Y^P - Y, & P > 1. \end{cases}$$

For $P > 1$ the exponent of U is an integer by hypothesis.

A critical point of a rational function. Put $u = L(x)$ and consider the rational function of degree $n + 1$

$$f(x) = x + \frac{au}{u^m - 1}.$$

We choose a so that we can describe a zero of f' explicitly. If $w = u^m - 1 \neq 0$, the equation $f'(x) = 0$ becomes $w^2 = \epsilon a\{m + (m-1)w\}$. Completing the square gives

$$\left(\frac{2m}{w} + m - 1\right)^2 = (m-1)^2 + \frac{4m\epsilon}{a}.$$

In the notation of Lemma 4.2, let $z = \sigma - \sigma^{-1}$. Since $z^* = -z$ and $z^2 = T^2 - 4$, we may take

$$a = \frac{4m\epsilon}{z^2 - (m-1)^2} \in k(T), \qquad w = \frac{2m}{z - (m-1)}.$$

At $\sigma = 0$ we have $v(\sigma) = 1$, since $1/T = \sigma/(1 + \sigma^2)$. In particular $v(w) = 1$. Modulo σ, the equation $L(x)^m = 1 + w$ has only simple roots. By Hensel's lemma it has a root x_* in $\mathcal{O} = \bar{k}[[\sigma]]$. Put $t_* = f(x_*)$. Then

$$J = L(t_*)^m = (1 + w)\{1 + D_{1+w}(a/w)\}^m \in k(\sigma).$$

Since $\epsilon a/w = w/(m + (m-1)w)$, the expansion at $w = 0$ gives $D_{1+w}(a/w) = w/m + O(w^2)$ and hence $J = 1 + 2w + O(w^2)$. Under $\sigma \mapsto \sigma^{-1}$, the function w becomes $-mw/(m + (m-1)w) = -w + O(w^2)$. It follows that $v(J - J^*) = 1$.

Two conjugate roots. For $P > 1$ take $R = P^j$ and let j tend to infinity. For $P = 1$ let R run through the powers of p congruent to one modulo m. Put $\beta = B_R(J)$. Lemma 4.2 gives

$$h(\beta) \leq R/2 + O_n(1), \qquad v(\beta - J) = R + 1.$$

Write $L^m(X) = L(X)^m$. Since $(L^m)'(t_*)$ is a unit, Hensel's lemma gives $t \in \mathcal{O}$ with $L(t)^m = \beta$ and $v(t - t_*) = R + 1$. On clearing denominators in $f(X) = t$, we obtain the monic polynomial

$$N_t(X) = (X - t)(L(X)^m - 1) + aL(X).$$

As $v(a/w) > 0$, we have $t \equiv t_* \equiv x_* \pmod{\sigma}$. Thus N_t reduces to $(X - \bar{x}_*)(L(X)^m - 1)$, which has $n - 1$ simple roots and a double root at $\bar{x}_*$. The simple roots lift to roots in $\mathcal{O}$. Dividing out their linear factors and substituting $X = x_* + Z$, we obtain

$$N_t(x_* + Z) = U(Z)(Z^2 + c_1 Z + c_0), \qquad U \in \mathcal{O}[Z], \quad U(0) \in \mathcal{O}^\times, \quad c_0, c_1 \in \mathcal{O}.$$

Since $f(x_*) = t_*$ and $f'(x_*) = 0$, we have $N_{t_*}(x_*) = N'_{t_*}(x_*) = 0$. It follows that

$$N_t(x_*) = -(t - t_*)w, \qquad N'_t(x_*) = -(t - t_*)(L^m)'(x_*).$$

Evaluating the factorization and its derivative at zero gives $v(c_0) = R+2$ and $v(c_1) \geq R+1$. Consequently $v(c_1^2 - 4c_0) = R + 2$. This is odd, so the quadratic factor is irreducible over $\bar{k}((\sigma))$. The corresponding roots x_1, x_2 of N_t satisfy $v(x_1 - x_2) = (R+2)/2$, and all $n+1$ roots of N_t are distinct.

An equation over $k(T)$. Put $b = L(t)$, so that $b^m = \beta$ is a unit. For each root x of N_t, put $Y = (x^R - t)/b$. Then $L(x^R) = b(1 + D_\beta(Y))$ and $(x - t)^R = b(Y - C)$, where $C = (t^R - t)/b$. If $P = 1$, then $C = \beta^{(R-1)/m} - 1$. If $P > 1$, raising $t^P - t = b$ to the powers $1, P, \ldots, P^{j-1}$ and adding gives $C = \sum_{i=0}^{j-1} \beta^{(P^i-1)/m}$. In either case C is a polynomial in β of degree at most $(R/P - 1)/m$. Raise $N_t(x) = 0$ to the Rth power and divide by b to obtain

$$(Y - C)\big\{\beta(1 + D_\beta(Y))^m - 1\big\} + a^R(1 + D_\beta(Y)) = 0.$$

This equation has degree $n+1$ over $k(T)$. Its roots are distinct because $x \mapsto x^R$ is injective. Let $F \in k[T][Y]$ be the primitive polynomial obtained by clearing denominators. The coefficients on the left are polynomials in β and a of degrees at most $P + (R/P - 1)/m$ and R, respectively. It follows that

$$h(F) \leq \big(P + (R/P - 1)/m\big)h(\beta) + Rh(a) \leq \frac{R^2}{2n} + O_n(R).$$

The two roots $Y_i = (x_i^R - t)/b$, $i = 1, 2$, are conjugate over $\bar{k}((\sigma))$. They are therefore roots of the same irreducible factor A of F over $\bar{k}(T)$, taken primitive over $\bar{k}[T]$. Since b is a unit, $v(Y_1 - Y_2) = R(R + 2)/2$. If $\deg_Y A \leq n$, applying (1) to A gives

$$R(R + 2)/2 \leq (n - 1)h(A) \leq (n - 1)h(F) \leq (n - 1)R^2/(2n) + O_n(R),$$

which is impossible for large R. Thus F is absolutely irreducible. Applying (1) to F gives $nh(F) \geq R(R + 2)/2$. Combining the two estimates for $h(F)$ gives $h(F) \asymp_n R^2$ and $\Delta(F) \leq nh(F) - R(R + 2)/2 \ll_n R \ll_n \sqrt{h(F)}$. □

5. Lower bounds in all degrees

We give a lower bound for the separation exponent in every degree. For odd degrees we also estimate the separation at finite height.

Theorem 5.1. *For every finite field $k = \mathbb{F}_q$ of characteristic p and every $d \geq 2$,*

$$E_{q,\mathrm{abs}}(d) \geq \begin{cases} d - 2, & d \text{ odd or } 4 \mid d, \\ d - 4, & d \equiv 2 \pmod 4,\ p \neq 3, \\ d - 8, & d \equiv 2 \pmod 4,\ p = 3. \end{cases}$$

If d and p are odd, put $j = 1$ when $p \nmid d - 1$ and $j = 2$ otherwise. There are absolutely irreducible polynomials F of degree d and arbitrarily large logarithmic height h for which $s(F) \geq (d - j)h - O_d(1)$.

Theorem 1.2 proves the assertion about the exponent if $p = 2$ or $p \nmid d-1$. We first prove the estimate for odd d and p.

5.1. **Odd degrees.** Suppose that $d \geq 3$ and p are odd. Take $j = 1$ if $p \nmid d-1$ and $j = 2$ otherwise, and put $\nu = d - j$. Then $p \nmid j\nu$ and $\gcd(d, 2\nu) = 1$. We shall use a rational function f of degree d with a simple critical point. The two roots of $f(X) = t$ near this point will give the required estimate $s(F) \geq \nu h(F) - O_d(1)$.

Let $c = \nu/j$ in $\mathbb{F}_p$ and put $A = (1+c)^2$, $B = (1-c)^2$. We choose a nonsquare $\lambda \in \mathbb{F}_p$ for which $(1-\lambda)(A - B\lambda)$ is also a nonsquare. To see that such a choice is possible, put $N = (p-1)/2$. For every nonsquare v, both $1 - v$ and $A - Bv$ are nonzero, since A and B are squares and $A - B = 4c \neq 0$. If their product were always a square, then

$$P(X) = (A - BX)^N - (1 - X)^N$$

would vanish at all roots of $X^N + 1$. As $\deg P \leq N$, it would be a constant multiple of $X^N + 1$. At least one of A, B is a nonzero square, so either the constant coefficient or the coefficient of X^N in P is zero. This would give $P = 0$, whereas $P(1) = (4c)^N \neq 0$.

Put $u = x^\nu$, $\rho(u) = (u - \lambda)/(1 - u)$ and

$$t = f(x) = x^j \rho(u), \qquad z = t^\nu, \qquad D = \lambda^d, \qquad W = u + \lambda/u, \qquad U = z + D/z.$$

The involution $u \mapsto \lambda/u$ sends ρ to λ/ρ and $z = u^j \rho^\nu$ to D/z. Thus U belongs to the fixed field $k(W)$. Its degree in W is d, since z has degree d in u and both $u \mapsto W$ and $z \mapsto U$ have degree two. Away from the zeros and poles of f, the equation $f'(x) = 0$ becomes

$$(u - \lambda)(1 - u) + cu(1 - \lambda) = 0.$$

Its discriminant is $(1-\lambda)(A - B\lambda)$, so its two roots u_0 and λ/u_0 are conjugate over $\mathbb{F}_p$. Neither is 0, 1 or λ. Write $z_0 = u_0^j \rho(u_0)^\nu$. Then $z_0^p = D/z_0$ and $U_0 = z_0 + D/z_0$ belongs to $\mathbb{F}_p$. If $z_0^2 = D$, we would have $z_0^p = z_0$, making D a square in $\mathbb{F}_p$. Since d is odd, $D = \lambda^d$ is a nonsquare. We therefore have $z_0^2 \neq D$. Take $T = 1/(U - U_0)$.

Choose $1 \leq b \leq 2\nu$ with $db \equiv 1 \pmod{2\nu}$, and let r run through the powers of p congruent to 1 modulo 2ν. Put

$$e = \lambda^{(r-db)/(2\nu)}, \qquad w = \frac{x^r}{et^b}, \qquad y = \frac{zw + D/z}{w + 1}.$$

Since $d \equiv j \pmod{\nu}$, we have $w = e^{-1} u^{(r-jb)/\nu} \rho(u)^{-b}$. Its product with its image under $u \mapsto \lambda/u$ is $\lambda^{(r-db)/\nu}/e^2 = 1$. Thus the involution fixes y, and $y \in k(W)$.

Over $\bar{k}(t)$ the elements y and x^r are related by a fractional linear transformation. They generate $\bar{k}(x)$ over $\bar{k}(t)$, since $\bar{k}(x)/\bar{k}(t)$ is separable and x is purely inseparable over $\bar{k}(t, x^r)$. Thus y has degree d over $\bar{k}(t)$ and at least d over $\bar{k}(T)$. As $[k(W) : k(T)] = d$, we have $k(T, y) = k(W)$, and the same equality holds over $\bar{k}$. The primitive polynomial $F(T, Y)$ associated with the minimal polynomial of y is therefore absolutely irreducible. It is separable in Y since both $f(x)$ and $U = t^\nu + D/t^\nu$ have nonzero derivative. Moreover,

$$h(F) = \deg_T F = [k(W) : k(y)] = \deg_W y.$$

After substituting $t = f(x)$, the coefficients of the fractional linear transformation from x^r to y and of its inverse have degrees in x bounded in terms of d. Hence $\deg_x y = r + O_d(1)$. Since $\deg_x W = 2\nu$, we obtain $h(F) = (r + O_d(1))/(2\nu)$.

Choose x_0 with $x_0^\nu = u_0$ and set $t_0 = f(x_0)$. The derivative of $U = t^\nu + D/t^\nu$ at t_0 is nonzero, since $p \nmid \nu$ and $z_0^2 \neq D$. Consequently $v(t - t_0) = v(U - U_0) = 1$ at $t = t_0$. The simple root u_0 of the critical equation gives a simple zero of f' at x_0. Thus $f(X) - t_0 = (X - x_0)^2 g(X)$ with $g(x_0) \neq 0$. As p is odd, g has a square root in $\bar{k}[[X - x_0]]$. The local parameter $(X - x_0)\sqrt{g(X)}$ takes the values $\pm\sqrt{t - t_0}$ at the two roots reducing

to x_0. Their difference has valuation $1/2$. At $t = t_0$ the fractional linear transformation from x^r to y has regular coefficients and its determinant is a unit, since $t_0 \neq 0$ and $z_0^2 \neq D$. At the common residue of the two rth powers, either this transformation or its reciprocal has a unit denominator. In that coordinate the difference of the two images has valuation $r/2$. Replacing F by its reciprocal polynomial if necessary preserves its height and gives $s(F) \geq r/2 \geq \nu h(F) - O_d(1)$.

For example, $27 \leq E_{7^a,\mathrm{abs}}(29) \leq 28$ for every $a \geq 1$. Whether $E_{7^a,\mathrm{abs}}(29) = 28$ remains open.

5.2. **A construction for even degrees.** Suppose that $d = 2\ell + b$, where $\ell, b \geq 1$, $\gcd(\ell, b) = 1$ and $p \nmid 2b\ell$. We shall construct absolutely irreducible polynomials F of degree d and arbitrarily large logarithmic height h for which

$$s(F) \geq 2\ell h - O_{q,d}(\sqrt{h}). \tag{4}$$

If $p \mid d$, then $p \nmid d-1$, and Theorem 1.2 gives the same estimate with $d-1$ in place of 2ℓ. Since $d - 1 \geq 2\ell$, we may assume that $p \nmid d$. The construction uses two properties of a rational function f. Near a simple critical point of f, the equation $f(x) = t$ has two roots close to each other when t is close to the critical value. At $T = 2$, Eisenstein's criterion will give an irreducible equation of degree d.

As in Lemma 4.2, write $T = \sigma + \sigma^{-1}$. Put

$$z = \frac{1+\sigma}{1-\sigma}, \qquad a = \frac{bd}{(b-\ell)^2 - z^2}.$$

We have $z^2 = (T+2)/(T-2)$, so $a \in k(T)$ has a simple zero at $T = 2$. The substitution $\sigma \mapsto \sigma^{-1}$ sends z to $-z$. Set

$$u = x^\ell, \qquad A = u^2 - 2au + a, \qquad B = au^2 - 2au + 1, \qquad t = f(x) = x^b A/B.$$

The two quadratics have the same nonzero discriminant $4a(a-1)$. They have no common zero. Indeed, $A - B = (1-a)(u^2-1)$, whereas $A(1)$ and $A(-1)$ are both nonzero. Since $B(0) = 1$, it follows that $\deg f = d$. The identity $B(u) = u^2 A(1/u)$ explains our choice of A and B. Write

$$W = u + u^{-1}, \qquad \xi = t^\ell = u^b (A/B)^\ell, \qquad V = \xi + \xi^{-1}.$$

Under $u \mapsto u^{-1}$, the function ξ goes to ξ^{-1}, so $V = \Phi(W)$ for some rational function Φ over $k(T)$. The maps $x \mapsto W$ and $t \mapsto V$ both have degree 2ℓ. Taking degrees in $V = \Phi(W)$ therefore gives $\deg \Phi = d$.

At a point where f is finite and nonzero, the equation $f'(x) = 0$ reduces to $bAB + \ell u(A'B - AB') = 0$, with derivatives of A and B taken with respect to u. Divide by u^2 and complete the square to obtain

$$[bW - (b-\ell)a - b - \ell]^2 = (a-1)^2\big((b-\ell)^2 - bd/a\big).$$

The two solutions are $W_\pm = ((b-\ell)a + b + \ell \pm (a-1)z)/b$. Their images under Φ are $J(z) = \Phi(W_+) \in k(z) = k(\sigma)$ and $J(-z) = \Phi(W_-)$, since $\sigma \mapsto \sigma^{-1}$ interchanges W_+ and W_-. To apply Lemma 4.2, we must show that $J(z) \neq J(-z)$. At $z = \infty$ we have $a = -bd/z^2 + O(z^{-4})$. Of the two solutions of $u + u^{-1} = W_+$, the one with a pole at $z = \infty$ has the expansion $u = -z/b + (b+\ell)/b + O(z^{-1})$. Hence

$$A/u^2 = 1 + O(z^{-3}), \qquad B = -\frac{2\ell}{b}\big(1 - d/z + O(z^{-2})\big).$$

Using $\xi = u^b(A/B)^\ell$ in $J = \xi + \xi^{-1}$ gives

$$J(z) = Cz^d\big(1 - bd/z + O(z^{-2})\big), \qquad C = (-1/b)^d(-2\ell/b)^{-\ell} \neq 0.$$

If d is odd, the coefficient of z^d changes sign under $z \mapsto -z$. If d is even, the nonzero coefficient of z^{d-1} changes sign. Thus $J(z) \neq J(-z)$. The only possible branch values of the maps $x \mapsto W$ and $t \mapsto V$ are $2, -2, \infty$. As elements of $k(z)$, W_+ and J are nonconstant and hence distinct from these values. Since W_+ is a simple root of the equation for W, each x_0 lying over W_+ is a simple critical point of f.

Let r run through the sufficiently large powers of p congruent to 1 modulo ℓ. By Lemma 4.2, there exists $V_r \in k(T)$ with a simple pole at $T = 2$ such that $h(V_r) \leq r/2 + O(1)$ and $v(V_r - J) = r + O(1)$ at $\sigma = 0$. We first work over $K_2 = \bar{k}((T-2))$. Hensel's lemma, applied to $V_r^{-1}\eta^2 - \eta + V_r^{-1}$ at $\eta = 0$, gives a solution of $\eta + \eta^{-1} = V_r$ with a simple zero at $T = 2$. By Eisenstein's criterion, a root t of $t^\ell = \eta$ is a uniformizer of $K_2(t)$. The monic polynomial $x^b A - tB$ of degree d is Eisenstein at t. Indeed, a is divisible by t, and the constant term is $-t$. This polynomial is separable, since it is irreducible and $p \nmid d$.

Choose $1 \leq j \leq \ell$ with $bj \equiv 1 \pmod{\ell}$, and put

$$w = x^r/t^j = u^{(r-bj)/\ell}(A/B)^{-j}, \qquad y = (\xi w + \xi^{-1})/(w+1).$$

Replacing u by u^{-1} replaces both w and ξ by their inverses and leaves y fixed. Thus y is a rational function of W over $k(T)$. For the value of t just chosen, y is an invertible fractional linear transformation of x^r, since $V_r \neq \pm 2, \infty$. As $K_2(t,x)/K_2(t)$ is separable, x^r generates this extension, and so does y. It follows that y has degree at least d over $\bar{k}(T)$. On the other hand, $y \in k(T, W)$ and $\Phi(W) = V_r$, so its degree over $k(T)$ is at most d. Consequently its primitive polynomial $F(T, Y)$ over $k[T]$ is separable and absolutely irreducible of degree d in Y.

To estimate $h(F)$, first regard W as an indeterminate and write $y = R(W)$. The fractional linear transformation from x^r to y and its inverse have coefficients of bounded degree in x, since $t = f(x)$ is fixed. Hence $\deg_x y = r + O(1)$, and $\deg_x W = 2\ell$ gives $\deg_W R = (r + O(1))/(2\ell)$. The degree of R in T is bounded independently of r. Indeed, extending the coefficient field $k(W)$ to $k(x)$ preserves the degree in T, and in the expression for y in terms of x only $t = f(x)$ depends on T. Clear denominators in $Y = R(W)$ and $\Phi(W) = V_r$. The resulting polynomials have degrees $O(1)$ and at most $h(V_r) + O(1)$ in T, respectively. Their resultant with respect to W is divisible by F. For polynomials P, Q, the determinant of the Sylvester matrix gives $\deg_T \operatorname{Res}_W(P, Q) \leq (\deg_W P)(\deg_T Q) + (\deg_W Q)(\deg_T P)$. Here the degrees in W are $(r + O(1))/(2\ell)$ and d, whence

$$h(F) \leq \frac{r + O(1)}{2\ell}(h(V_r) + O(1)) + O(1) \leq \frac{r^2}{4\ell} + O(r).$$

We now work at $\sigma = 0$. Fix a critical point x_0 above W_+ and put $t_0 = f(x_0)$. Since $t \mapsto V = t^\ell + t^{-\ell}$ is unramified at t_0, the equation $t_r^\ell + t_r^{-\ell} = V_r$ has a solution with $v(t_r - t_0) = r + O(1)$ for all sufficiently large r. In the local coordinate $Z = x - x_0$ we have $f(x) - t_0 = cZ^2(1 + O(Z))$, with $c \neq 0$. Since p is odd, $1 + O(Z)$ has an analytic square root near zero. Thus $f(x) = t_r$ has two roots x_1, x_2 tending to x_0 with $v(x_1 - x_2) = r/2 + O(1)$.

For finite a, b, write $[a, b] = |a - b|/(\max(1, |a|)\max(1, |b|))$ for their chordal distance. Since x_0 is finite and independent of r, we have $[x_1, x_2] = q^{-r/2+O(1)}$ and hence $[x_1^r, x_2^r] = [x_1, x_2]^r = q^{-r^2/2+O(r)}$. At $t = t_r$ the fractional linear transformation from x^r to y has matrix $M(t_r)$, where $M(t) = \left(\begin{smallmatrix} t^\ell & t^{j-\ell} \\ 1 & t^j \end{smallmatrix}\right)$. Since $t_0 \neq 0, \infty$ and $t_0^{2\ell} \neq 1$, the limit $M(t_0)$ is invertible. Thus $M(t_r)$ and its inverse have bounded entries. The chordal distance between the two images is therefore $q^{-r^2/2+O(r)}$. The two images are roots of F. Indeed, the equation $\Phi(W) = V_r$ is irreducible over $k(T)$ because $k(T, W)$ contains $k(T, y)$ of degree d. Its roots therefore give conjugate values of y. Replacing F by its reciprocal if necessary, we may assume that both roots have absolute value at most one, whence

$s(F) \geq r^2/2 - O(r)$. It follows from (1) that $h(F) \gg r^2$. Together with the upper bound for $h(F)$ this proves (4).

For even d it remains to consider odd p dividing $d-1$, since Theorem 1.2 covers the other cases. For $4 \mid d$ take $b = 2$. For $d \equiv 2 \pmod 4$ take $b = 4$ if $p \geq 5$ and $b = 8$ if $p = 3$. In the last case $d \geq 10$. In each case $\ell = (d-b)/2$ is odd and $2\ell \equiv 1 - b \not\equiv 0 \pmod p$. Substitution in (4) gives the bounds in Theorem 5.1 for even d.

6. The constant field

Let x be a root of a separable irreducible polynomial F of degree d. The full constant field of $K(x)$ is $K(x) \cap \bar{k} = \mathbb{F}_{q^c}$ for some divisor c of d. We denote this field by k_c. The polynomial F is absolutely irreducible if and only if $c = 1$.

Theorem 6.1. *If $c > 1$, then*

$$s(F) \leq \frac{2d}{c^2}\, h(F).$$

For each divisor $c > 1$ of d and each integer $N \geq 1$, there is such a polynomial of logarithmic height cN for which equality holds. Hence the separation exponent for irreducible polynomials of degree d that factor over $\bar{k}(T)$ is $2d/\ell^2$, where ℓ is the least prime divisor of d.

Proof. Write $r = d/c$. The minimal polynomial of x over $k_c(T)$ has degree r and remains irreducible over $\bar{k}(T)$. To see this, let $\alpha \in \bar{k}$. The minimal polynomial of α over $K(x)$ has all its roots in $\bar{k}$, so its coefficients belong to $K(x) \cap \bar{k} = k_c$. Thus $[K(x,\alpha) : K(x)] = [k_c(\alpha) : k_c]$. By the tower law, x has degree r over $k_c(\alpha)(T)$, and $\bar{k}(T)$ is the union of these fields.

Up to a constant factor, F is the product of c absolutely irreducible polynomials of degree r in $k_c[T][X]$. Indeed, the Frobenius automorphism of k_c/k permutes the monic irreducible factors transitively, since F is irreducible over K. Their primitive representatives have the same logarithmic height, which by multiplicativity of the Gauss norm is $h(F)/c$. For distinct roots u_1, u_2 of the same factor, inequality (1) gives $v(u_1 - u_2) \leq (r-1)h(F)/c$. If u_1, u_2 are roots of two different factors, (2) gives $v(u_1 - u_2) \leq 2rh(F)/c$. This proves the upper bound.

To obtain equality, we adapt a construction of Bugeaud and Mignotte [4, (3.1)] for integer polynomials. Choose $\gamma \in k_c$ of degree c over k, put $a = T^N$, and set

$$G_\eta(X) = X^r + (1 + \eta X^{r-1})(1 - aX), \qquad F_N = \prod_{i=0}^{c-1} G_{\gamma^{q^i}}.$$

For each conjugate η of γ, write $G_\eta = A - T^N B$, where $B = X(1 + \eta X^{r-1})$ and $A = X^r + 1 + \eta X^{r-1}$. The polynomial B has a simple zero at 0, whereas $A(0) \neq 0$. This also holds for $r = 1$, since $\eta \notin k$. At each nonzero root of B we have $A = X^r \neq 0$. Hence A and B are coprime, and Eisenstein's criterion at X shows that $AZ^N - B$ is irreducible in $\bar{k}[X, Z]$. Replacing Z by $1/T$ and clearing denominators shows that G_η is absolutely irreducible. For distinct conjugates η, θ, the difference $G_\theta - G_\eta = (\theta - \eta)X^{r-1}(1 - aX)$ is nonzero, while $G_\eta(1/a) = G_\theta(1/a) = a^{-r}$. Thus no two factors are scalar multiples of one another. Frobenius permutes the c factors transitively, so F_N is irreducible over K. Each factor has logarithmic height N, whence $h(F_N) = cN$.

For $\eta \neq \theta$, the formula for $G_\theta - G_\eta$, together with $a^r G_\eta(1/a) = 1$ and, for $r > 1$, $G_\eta(0) = 1$, gives $\mathrm{Res}_X(G_\eta, G_\theta) = (\theta - \eta)^r$. To find the distance between the closest roots, reduce $a^{-1}G_\eta$ modulo T^{-1}. Its reduction $-X(1 + \eta X^{r-1})$ has degree r and a simple root at 0. In particular, the leading coefficient of G_η has absolute value $|a|$, and all its roots have absolute value at most one. By Hensel's lemma it has a unique root x_η with $|x_\eta| < 1$.

This root is simple, so G_η is separable. The c absolutely irreducible factors of F_N therefore show, by the first part of the proof, that the full constant field is k_c.

For $\eta \neq \theta$, the only common root of the two reductions is 0. It follows that $|u - v| = 1$ for every pair of roots u of G_η and v of G_θ, except for (x_η, x_θ). Taking absolute values in the product formula for the resultant gives $1 = |a|^{2r}|x_\eta - x_\theta|$. Thus $s(F_N) = 2rN$. □

We can now compare the two exponents $E_{q,\mathrm{irr}}(d)$ and $E_{q,\mathrm{abs}}(d)$. For $c > 1$ the preceding theorem gives an exponent at most $d/2$. By Theorem 5.1, $E_{q,\mathrm{abs}}(d) \geq d - 8 \geq d/2$ for $d \geq 16$, and $E_{q,\mathrm{abs}}(d) \geq d - 2 \geq d/2$ for $d \geq 4$ odd or divisible by four. For the remaining degrees $2, 3, 6, 10, 14$, the integer $d - 1$ is either 1 or a prime power, so Theorem 1.2 gives $E_{q,\mathrm{abs}}(d) = d - 1$. Hence $E_{q,\mathrm{irr}}(d) = E_{q,\mathrm{abs}}(d)$ for every q and d.

7. When the loss is bounded

Theorem 7.1. *Let $k = \mathbb{F}_q$ have characteristic p, and let $n \geq 1$. There are reducible polynomials of degree $n+1$ with unbounded height and bounded Δ if and only if n satisfies at least one of the following conditions. In the list, P denotes a positive power of p.*

1. *$p \nmid n$.*
2. *$n = Pm$ for some $m \mid P - 1$.*
3. *$p = 2$ and $n \equiv 2 \pmod 4$.*
4. *$n = P(P^2 - 1)$ or $n = P(P^2 - 1)/\gcd(2, P - 1)$.*
5. *$p = 3$ and $n = 60$.*

In each case the polynomials can be taken to be products of a linear factor and a fixed absolutely irreducible factor of degree n. For every other n there is a constant $c_n > 0$ such that $\Delta(F) \geq c_n\sqrt{h(F)}$ for every reducible F of degree $n + 1$ and sufficiently large logarithmic height.

Theorem 1.1 covers $p \nmid n$, so we may assume that $p \mid n$. Suppose that W is reducible of degree $n + 1$ and that $s(W) > (n - 1)h(W)$. By (3), a closest pair consists of a root α of an irreducible factor F of degree n and the root $u = a/b$ of the remaining linear factor. Put $B = h(F)$ and $r = b^n F(a/b)$. Then

$$h(W) = B + h(u), \qquad (n - 1)B + \deg r \leq \Delta(W). \tag{5}$$

Each conjugate of α over K_∞ is just as close to u. Two distinct conjugates would therefore violate (1) for F, since $s(W) > (n - 1)B$. Thus $\alpha \in K_\infty$. The monic irreducible factor of F over $\bar{k}(T)$ having root α is fixed by the automorphism that raises the constants to their qth powers and fixes T, since it fixes the Laurent series α. It follows that F is absolutely irreducible.

Suppose that $n \geq 4$ and that the cross-ratio of any four distinct roots of F lies in $\bar{k}$. A fractional linear transformation M sending three roots to $0, 1, \infty$ then takes every root to a point of $\mathbb{P}^1(\bar{k})$. For every automorphism τ of the splitting field over $\bar{k}(T)$, the transformation $M\tau(M)^{-1}$ permutes these n points. Its coefficients can be taken in $\bar{k}$, since the images of three points determine it. These transformations form a finite group, because they induce the permutations $M(x) \mapsto M(\tau x)$ on these points. The action is transitive by absolute irreducibility. Thus n is the size of an orbit of a finite subgroup of $\mathrm{PGL}_2(\bar{k})$.

7.1. **The possible orbit sizes.** We determine the orbit sizes divisible by p, using the classical count of fixed points of fractional linear transformations (see Faber [6, Sections 5–6]). Let G be a finite subgroup of $\mathrm{PGL}_2(\bar{k})$ of order g divisible by p. Let P be the order of a Sylow p-subgroup and a the number of such subgroups. A nonidentity projectivity has two fixed points, except when it has order p, in which case it has one. A Sylow

p-subgroup fixes the unique fixed point of any central element of order p. Sending this point to infinity identifies the subgroup with a group of translations. The translations in the full stabilizer form its unique Sylow p-subgroup. Thus the a fixed points of the Sylow subgroups are distinct and form one orbit. A Sylow subgroup acts freely on the other $a-1$ points, so $a = 1 + tP$ for some $t \geq 0$. Its fixed point has stabilizer of order Pm, where $m \mid P-1$, since each nonidentity multiplier permutes the $P-1$ nonzero translation parameters without fixing any of them. In particular $g = aPm$.

An orbit of size b accounts for $g - b$ pairs (x, γ) with $1 \neq \gamma \in G$ and $\gamma x = x$. There are $a(P-1)$ elements of order p. After subtracting the $g - a$ pairs from the orbit of the Sylow fixed points, the number of pairs left is

$$2g - 2 - a(P-1) - (g-a) = g - 2 - a(P-2).$$

Each further orbit of size less than g accounts for at least $g/2$ pairs. There is consequently at most one such orbit, and its size, if it exists, is $b = 2 + a(P-2)$. For $t = 0$ the only possible sizes are $1, P, g$. For $t > 0$ the remaining count is at least $2a - 2 > 0$. Since $b = P(1 + t(P-2))$ divides g, we have

$$1 + t(P-2) \mid (1+tP)m.$$

The two factors $1 + t(P-2)$ and $1 + tP$ have greatest common divisor dividing 2. Hence $1+t(P-2) \leq 2m \leq 2(P-1)$. For $P \geq 3$ this leaves $t = 1, 2$ and the additional possibility $P = t = 3$. For $t = 2$ the greatest common divisor is one, whereas $2P - 3 > m$. For $t = 1$ we get $m = P - 1$ or, for odd P, $m = (P-1)/2$. The possible sizes divisible by p are then g and $P(P-1)$. If $P = t = 3$, then $m = 2$, $g = 60$ and $b = 12 = |\mathrm{PSL}_2(\mathbb{F}_3)|$. Finally, $P = 2$ gives $m = 1$, $g = 2(1 + 2t)$ and $b = 2$. This gives all the possibilities in Theorem 7.1.

Each size on the list occurs as the order of a group stable under the qth-power map on coefficients. For $p \nmid n$, take the rotations $z \mapsto uz$ with $u^n = 1$. For $n = Pm$ take the maps $z \mapsto uz + v$ with $u^m = 1$ and $v \in \mathbb{F}_P$. For $p = 2$ and $n \equiv 2 \pmod 4$ take the maps $z \mapsto uz$ with $u^{n/2} = 1$ together with $z \mapsto 1/z$. The two orders $P(P^2-1)$ and $P(P^2-1)/\gcd(2, P-1)$ are those of $\mathrm{PGL}_2(\mathbb{F}_P)$ and $\mathrm{PSL}_2(\mathbb{F}_P)$.

For $p = 3$ and $n = 60$ there is a small explicit example. Take $\eta^2 = \eta + 1$ in $\mathbb{F}_9$. Label ∞ by the pair 45 and the nine finite points by the pairs in the table.

	z	$z+1$	$z+2$
$z = 0$	12	23	13
$z = \eta$	25	35	15
$z = -\eta$	14	24	34

On these labels $z \mapsto z + 1$, $z \mapsto \eta^2/z$ and $z \mapsto z^3$ act as (123), (14)(25) and (45), respectively. The first two generate A_5. Indeed, their product has order five, so the subgroup they generate has order divisible by 30, and A_5 has no subgroup of index two since it is generated by 3-cycles. The cubing map therefore normalizes the group of sixty projectivities.

7.2. **Examples with a fixed factor.** For each n on the list with $p \mid n$, take one of the groups G of order n constructed above. The coefficients of $\prod_{\gamma \in G}(Y - \gamma(z))$ lie in $k(z)$ and generate a field $k(J)$ by Lüroth's theorem. The polynomial gives $\deg_z J \leq n$, while the n automorphisms over $\bar{k}(J)$ give the reverse inequality. The fibers of J are the G-orbits. The fixed-point count shows that at most two of them have fewer than n points. Thus some point of $\mathbb{P}^1(k)$ has a fiber Ω of size n, even for $q = 2$. Changing the coordinate on the target over k, take T with pole at this fiber. It has degree n in z and a simple pole at each point of Ω.

Choose a power Q of q for which the points of Ω and the matrices of G are defined over $\mathbb{F}_Q$. The transformation

$$M_z(X) = \frac{(X - z^Q)(z^{Q^2} - z)}{(X - z)(z^{Q^2} - z^Q)}$$

sends z, z^Q, z^{Q^2} to $\infty, 0, 1$. Hence $M_{\gamma z}(\gamma X) = M_z(X)$ for $\gamma \in G$. Fix a finite $c \in \Omega$ and put $\alpha = M_z(c)$. Its conjugates over $\bar{k}(T)$ are the n distinct values $M_z(c')$, $c' \in \Omega$. Since the qth-power map on the constants permutes Ω, their monic polynomial lies in $k(T)[X]$. Let $F \in k[T][X]$ be its primitive representative.

For $R = Q^j$, $j \geq 3$, the function $u = M_z(z^R)$ is invariant under G and belongs to $k(z)$, so $u \in k(T)$. Its expression gives $nh(u) = \deg_z u \leq R + Q^2$. At $z = c$ the difference

$$u - \alpha = \frac{(z^{Q^2} - z)(z^Q - z)(z^R - c)}{(z^{Q^2} - z^Q)(z^R - z)(c - z)}$$

has order $R - Q$. Since T has a simple pole there, $v(u - \alpha) = R - Q$. The limit α therefore belongs to K_∞ by completeness. The heights $h(u)$ are unbounded because α has degree $n > 1$. Multiplying F by the primitive linear polynomial with root u gives polynomials of unbounded height with $\Delta \leq nh(F) + Q^2 + Q$.

For example, $n = 6$ occurs on the list in characteristics two and three. In both cases the Laurent series α has degree six and irrationality exponent six. Indeed, $v(\alpha - u) \geq 6h(u) - O(1)$, and Liouville's inequality gives the reverse bound for the exponent. Bugeaud singled out these two cases in his discussion of a question of Mahler [2, Problem 1.1 and p. 193].

7.3. **A lower bound outside the list.** If n lies outside the list, then $n \geq 4$. The argument at the beginning of this section shows that whenever $s(W) > (n - 1)h(W)$, four roots of F in (5) have a nonconstant cross-ratio. For a fixed algebraic Laurent series, Voloch related rational approximation to the cross-ratios of its conjugates [13, 7]. Here we need an estimate uniform in the factor F.

Lemma 7.2. *Let $F \in k[T][X]$ be separable of degree $n \geq 4$, and suppose that four of its roots have a cross-ratio outside $\bar{k}$. Put $B = h(F)$. For coprime $a, b \in k[T]$ with $b \neq 0$ and $r = b^n F(a/b) \neq 0$, we have*

$$h(a/b) \ll_n (B + 1)(B + 1 + \deg r).$$

Proof. Let L be the field generated by the four roots $x_1, \ldots, x_4$ over $\bar{k}(T)$ and put $D = [L : \bar{k}(T)] \leq n^4$. For $x \in L$ write $h_L(x)$ for the degree of its pole divisor. Each x_i satisfies $h_L(x_i) \leq DB$. Indeed, if f_n is the leading coefficient of F, the homogeneous coordinates $[f_n x_i : f_n]$ are integral at every finite place. At a place of ramification index e above infinity, each coordinate has pole order at most eB. For $f_n x_i$ this follows from its monic equation, whose coefficient in degree $n - j$ has degree at most jB in T.

The genus g of L satisfies $g \ll_n B + 1$. To see this, choose a linear combination z of the x_i over $\bar{k}$ that separates the D embeddings of L over $\bar{k}(T)$. Then $L = \bar{k}(T, z)$ and $h_L(z) \leq 4DB$. For every $l \geq 0$ the $D(l + 1)$ functions $T^i z^j$ with $0 \leq i \leq l$ and $0 \leq j < D$ are linearly independent. Their pole divisors are bounded by $l(T)_\infty + (D - 1)(z)_\infty$. For sufficiently large l, the Riemann–Roch formula gives $D(l+1) \leq lD + (D-1)h_L(z) + 1 - g$, as required [12, Theorem 1.5.17].

Let M send x_1, x_2, x_3 to $0, \infty, 1$ and put $\gamma = M(x_4) \notin \bar{k}$. Write $u = a/b$. Both $M(u)$ and $M(u)/\gamma$ are finite and nonzero. Let Q be the largest power of p for which they are both Qth powers in L. Their quotient γ is also a Qth power, so $Q \leq h_L(\gamma)$. Every

constant in $\bar{k}$ is a p^jth power for every $j \geq 1$. Thus one of the two values has the form V^Q with $V \notin L^p$. The cross-ratio formula

$$M(X) = \frac{(X - x_1)(x_3 - x_2)}{(X - x_2)(x_3 - x_1)}$$

gives $h_L(\gamma) \ll_n B$ and $Dh(u) = h_L(u) \leq Qh_L(V) + O_n(B)$. For the latter bound apply the inverse of M or M/γ to V^Q. Its matrix entries, up to a common scalar, are polynomials of bounded degree in the four roots, so applying the matrix in homogeneous coordinates increases the height by at most $O_n(B)$.

Let S be the places of L above infinity and above the zeros of $f_n \operatorname{Disc}(F) r$. Then $|S| \ll_n 1 + B + \deg r$. Outside S the four roots have distinct finite reductions, and $[a : b]$ reduces to none of them. Both transformations M and M/γ take three of the four reduced roots to $0, 1, \infty$, so all places above these three values of V lie in S. The map defined by V is separable, since $V \notin L^p$. Put $m = h_L(V)$. At a point of ramification index e the different exponent is at least $e - 1$. The three fibers thus contribute at least $3m - |S|$ to the degree of the different, which is $2g - 2 + 2m$ by the Riemann–Hurwitz formula [12, Theorem 3.4.13]. Hence $h_L(V) \leq 2g - 2 + |S|$. The bounds for Q and g give the assertion. □

We now finish the proof of Theorem 7.1. If $s(W) \leq (n-1)h(W)$, then $\Delta(W) \geq h(W)$. Otherwise, Lemma 7.2 and (5) give

$$h(W) = B + h(a/b) \ll_n (1 + \Delta(W))^2.$$

Thus $\Delta(W) \gg_n \sqrt{h(W)}$ for every sufficiently large $h(W)$. The families in Theorem 1.1 attain this order.

Funding. T. P. acknowledges support from the Croatian Science Foundation under project IP-2022-10-5008 (TEBAG). He also 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 under the Competitiveness and Cohesion Programme 2021–2027. This research was funded by the European Union through NextGenerationEU under the National Recovery and Resilience Plan 2021–2026 (institutional grant of the Faculty of Science, University of Zagreb, 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] Y. Bugeaud, On simultaneous approximation in fields of power series, Bull. Math. Soc. Sci. Math. Roumanie **65(113)** (2022), 191–202.

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

[4] Y. Bugeaud and M. Mignotte, On the distance between roots of integer polynomials, Proc. Edinb. Math. Soc. **47** (2004), 553–556. doi:10.1017/S0013091503000257.

[5] Y. Bugeaud and M. Mignotte, Polynomial root separation, Int. J. Number Theory **6** (2010), 587–602. doi:10.1142/S1793042110003083.

[6] X. Faber, Finite p-irregular subgroups of $\mathrm{PGL}_2(k)$, La Matematica **2** (2023), 479–522. doi:10.1007/s44007-023-00051-4.

[7] A. Lasjaunias and B. de Mathan, Differential equations and Diophantine approximation in positive characteristic, Monatsh. Math. **128** (1999), 1–6. doi:10.1007/PL00010080.

[8] K. Mahler, On a theorem of Liouville in fields of positive characteristic, Canad. J. Math. **1** (1949), 397–400. doi:10.4153/CJM-1949-035-0.

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

[10] T. Ooto, Quadratic approximation in $\mathbb{F}_q((T^{-1}))$, Osaka J. Math. **54** (2017), 129–156. doi:10.18910/61892.
[11] C. F. Osgood, Effective bounds on the "Diophantine approximation" of algebraic functions over fields of arbitrary characteristic and applications to differential equations, Indag. Math. **37** (1975), 105–119. doi:10.1016/1385-7258(75)90023-2.
[12] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd ed., Graduate Texts in Mathematics, vol. 254, Springer, Berlin, 2009. doi:10.1007/978-3-540-76878-4.
[13] J. F. Voloch, Diophantine approximation in characteristic p, Monatsh. Math. **119** (1995), 321–325. doi:10.1007/BF01293591.