Diversity in rationally parameterized number fields

Benjamin Klahn

Abstract

Let $\mathbf{X}$ be a curve defined over $\mathbb{Q}$ and let $t \in \mathbb{Q}(\mathbf{X})$ be a non-constant rational function on $\mathbf{X}$ of degree $v \geq 2$. For every rational number a/b pick a point $P_{a/b} \in \mathbf{X}(\overline{\mathbb{Q}})$ such that $t(P_{a/b}) = a/b$. Bilu and Luca showed that there is a constant $\eta > 0$ only depending on v and the genus $\mathbf{g}$ of $\mathbf{X}$ such that for large integers N there are at least $N/(\log N)^{1-\eta}$ distinct fields among $\mathbb{Q}(P_1), \mathbb{Q}(P_2), \ldots, \mathbb{Q}(P_N)$. In this paper we obtain lower bounds on the number of distinct fields among $\mathbb{Q}(P_{a/b})$ with $1 \leq a, b \leq N$ under some assumptions on t. We show that if t has a pole of order at least 2 or if there is a rational number α such that $t - \alpha$ has a zero of order at least 2, then the set $\{\mathbb{Q}(P_{a/b}) \mid 1 \leq a, b \leq N\}$ contains $\gg \frac{N^2}{(\log N)^2}$ elements. We also obtain partial results when t does not have a pole of order at least two.

1 Introduction

Everywhere in this paper "curve" means "smooth geometrically projective algebraic curve". Furthermore, let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

1.1 Hilbert's Irreducibility Theorem

Let $\mathbf{X}$ be a curve of genus $\mathbf{g}$ and let $t \in \mathbb{Q}(\mathbf{X})$ be a non-constant rational function on $\mathbf{X}$ of degree $v \geq 2$. For a rational number $r \in \mathbb{Q}$ the absolute Galois group $G(\overline{\mathbb{Q}}|\mathbb{Q})$ acts on the the fiber $t^{-1}(r) \subset \mathbf{X}(\overline{\mathbf{Q}})$ and we call $t^{-1}(r)$ *irreducible* if the action is transitive or, equivalently, if $[\mathbb{Q}(P_r) : \mathbb{Q}] = v$ for any $P_r \in t^{-1}(r)$. Hilbert's Irreducibility Theorem, HIT, tells that for infinitely many r the fiber $t^{-1}(r)$ is irreducible. In fact, a quantitative version of HIT states that most fibers are irreducible, see Theorem 2.2 below for a more precise formulation.

Related to the question of whether fibers $t^{-1}(r)$, $r \in \mathbb{Q}$ are irreducible is how diverse the fibers are; HIT tells us that typically $[\mathbb{Q}(P_r) : \mathbb{Q}] = v$, but what happens if one adds several points, i.e. what is the degree $[\mathbb{Q}(P_{r_1}, P_{r_2}, \ldots, P_{r_m}) : \mathbb{Q}]$? Dvornicich and Zannier studied this question in [DZ] and obtained the following result.

Theorem 1.1 (Dvornicich, Zannier)**.** *Choose for every integer n a point $P_n \in t^{-1}(n)$. There exists a constant $c = c(\mathbf{g}, v) > 0$ such that for sufficiently large integers N, independent of the choice of P_n, the degree of $\mathbb{Q}(P_1, P_2, \ldots, P_N)$ is at least $e^{c\frac{N}{\log N}}$.*

From Theorem 1.1 one also obtains a lower bound on the number of distinct fields among $\mathbb{Q}(P_1), \mathbb{Q}(P_2), \ldots, \mathbb{Q}(P_N)$.

Corollary 1.2 (Dvornicich, Zannier)**.** *In the setup above there is a constant $c' = c'(\mathbf{g}, v)$ such that for sufficiently large integers N there are at least $c'\frac{N}{\log N}$ distinct number fields among $\mathbb{Q}(P_1), \mathbb{Q}(P_2), \ldots, \mathbb{Q}(P_N)$.*

From the example below, one sees that Theorem 1.1 in general is optimal, but Corollary 1.2 is not.

Example 1.3. *Consider the curve* $\mathbf{X} : YZ - X^2 = 0$ *and the rational function* $t = \frac{Y}{Z}$ *on* $\mathbf{X}$*. one finds that* $P_n = [\pm\sqrt{n} : n : 1]$ *and hence* $\mathbb{Q}(P_n) = \mathbb{Q}(\sqrt{n})$*. Therefore,*

$$\mathbb{Q}(P_1, P_2, \ldots, P_N) = \mathbb{Q}(\sqrt{p} \mid p \leq N),$$

and therefore

$$[\mathbb{Q}(P_1, P_2, \ldots, P_N) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p}) \mid p \leq N] = 2^{\pi(N)} \leq 2^{(1+\epsilon)\frac{N}{\log N}},$$

and

$$|\{\mathbb{Q}(P_n) \mid 1 \leq n \leq N\}| = |\{n \leq N \mid \mu^2(n) = 1\}| \sim \zeta(2)^{-1}N.$$

However, one could hope that in many cases the growth of the degree of $\mathbb{Q}(P_1, P_2, \ldots, P_N)$ would be exponential in N. Schintzel conjectured that imposing rather weak conditions on t would ensure exponential growth. In [DZ] and [$DZ2$] Dvornicich and Zannier obtained a partial results towards this conjecture. Their result is stated in terms of the so-called *critical values* of t.

1.2 Critical values

We say that $\alpha \in \bar{\mathbb{Q}} \cup \{\infty\}$ is a *critical value* for the rational function t on $\mathbf{X}$ if $t - \alpha \in \bar{\mathbb{Q}}(\mathbf{X})$ has a zero of multiplicity at least 2, here $t - \infty := t^{-1}$. Here the multiplicity of a zero is defined via the usual intersection multiplicity for curves. In particular, ∞ is a critical value exactly when t has pole of order at least 2. We call a critical value $\alpha \neq \infty$ a *finite* critical value. It can easily be seen that the finite critical values of t come in Galois conjugates. Furthermore, from the Riemann-Hurwitz genus formula

$$2\mathbf{g} + 2v - 2 = \sum_{P \in X(\overline{\mathbb{Q}})} (e_P - 1)$$

where e_P is the ramification index (multiplicity) of t at P we see that t has only finitely many critical values. Furthermore, since the ramification index at any point is at most v, we see that if the degree of t is at least 2, then there are at least 2 *distinct* critical values.

Schintzel conjectured the following

Conjecture 1.4 (Schintzel)**.** *In the set-up above, if either* t *has a finite critical value not belonging to* $\mathbb{Q}$ *or the extension* $\overline{\mathbb{Q}}(X)/\overline{\mathbb{Q}}(t)$ *is abelian, then there is a* $c > 0$ *such that for sufficiently large values of* N *the degree of* $\mathbb{Q}(P_1, P_2, \ldots, P_N)$ *is at least* e^{cN}*.*

Dvornicich and Zannier showed that Conjecture 1.4 holds true in the following cases:

(1) If t has a finite critical value of degree 2 or 3 over $\mathbb{Q}$,

(2) If all finite critical values of t are rational and the Galois group of the normal closeure of $\overline{\mathbb{Q}}(X)$ over $\overline{\mathbb{Q}}(t)$ is sufficiently large.

As remarked by Dvornicich and Zannier in [DZ] the conditions on t in Conjecture 1.4 are necessary; if not then by Kummer's Theory one sees that there are rational numbers $\gamma_1, \gamma_2, \ldots, \gamma_s$ and positive integers $e_1, e_2, \ldots, e_s$ such that

$$\mathbb{Q}(\mathbf{X}) \subset L(t, (t-\gamma_1)^{1/e_1}, \ldots, (t-\gamma_s)^{1/e_s})$$

where L is a number field, and hence that there is a constant $A = A(\mathbf{X}, t) > 0$ such that $\mathbb{Q}(P_1, P_2 \ldots, P_N)$ is generated by eth roots of prime numbers $p \leq AN$, where $e = \prod_{i=1}^{s} e_i$.

1.3 Diversity in integrally parameterized fields

Bilu and Luca in turn considered specifically the question of counting the number of distinct fields among $\mathbb{Q}(P_1), \mathbb{Q}(P_2), \ldots, \mathbb{Q}(P_N)$ and conjectured from Example 1.3 that there should always be $\gg N$ many distinct fields among $\mathbb{Q}(P_1), \mathbb{Q}(P_2), \ldots, \mathbb{Q}(P_N)$:

Conjecture 1.5 (Bilu, Luca)**.** *The number of distinct fields among $\mathbb{Q}(P_n)$ with $1 \leq n \leq N$ is $\gg N$.*

In [BL] They obtained the following unconditional result towards Conjecture 1.5.

Theorem 1.6 (Bilu, Luca)**.** *In the above setup, there exists a positive real number $\eta = \eta(\mathbf{g}, \mathbf{v})$ such that for sufficiently large integers N, among the number fields $\mathbb{Q}(P_1), \mathbb{Q}(P_2), \ldots, \mathbb{Q}(P_N)$ there are at least $N/(\log N)^{1-\delta}$ distinct.*

Furthermore, in [BL2] Bilu and Luca showed that Conjecture 1.5 holds true when t is of degree at least 2 and all fininite critical values of t are rational. One can notice that the only finite critical value of the degree two rational function $t = Y/Z$ in Example 1.3 is 0 and that the linearly many distinct fields among $\mathbb{Q}(P_j),\ 1 \leq j \leq N$ therefore can be obtained via Bilu and Luca's conditional result.

Finally, in [BG] Bilu and Gilbert generalized the question of diversity among fields generated by points in distinct fibers to number fields K by considering fields generated by points in fibers $P_\tau \in t^{-1}(\tau)$ where τ is an integer of K. They obtained the following result.

Theorem 1.7 (Bilu, Gilibert)**.** *Let K be a number field of degree d. In the above setup there exists constants $c = c(K, \mathbf{g}, v) > 0$ and $B_0 = B_0(K, \mathbf{X}, t) > 1$ such that for all $B > B_0$ among the number fields*

$$K(P_\tau),\ (\tau \in \mathcal{O}_K,\ H(\tau) \leq B)$$

where H is the ususal multiplicative Weil height, there are at least $cB^d/\log B$ distinct.

1.4 Our results

The goal of this paper is to complement the mentioned results by Bilu, Dvornicich, Luca and Zannier by considering the problem of counting the number of distinct fields $\mathbb{Q}(P_r)$ where we now allow rational numbers r instead of considering only integers, i.e. count how many distinct fields there are among $\mathbb{Q}(P_r)$ where r is a

rational number with numerator and denominator bounded by, say, N. Thus, for every rational number $r \in \mathbb{Q}$ fix a point $P_r \in t^{-1}(r)$ and denote

$$RP(N) := |\{\mathbb{Q}(P_{a/b}) \mid 1 \le a, b \le N\}|. \tag{1}$$

One could hope that a similar result as in Conjecture 1.5 would carry over, i.e. that for any choice of $P_r \in t^{-1}(r)$ one would have

$$RP(N) \gg N^2.$$

However, the following example shows that this cannot always be the case:

Example 1.8. *Consider again the curve* $\mathbf{X} : YZ - X^2 = 0$ *and* $t = \frac{Y}{Z}$. *Then* $\mathbb{Q}(P_{a/b}) = \mathbb{Q}(\sqrt{a/b}) = \mathbb{Q}(\sqrt{ab})$ *and one sees that*

$$RP(N) = |\{\mathbb{Q}(\sqrt{a/b}) \mid 1 \le a, b \le N\}| = |\{ab \mid 1 \le a, b \le N, \mu^2(ab) = 1\}|.$$

From the Erdös multiplication problem one sees that there is a $\delta > 0$ *such for large values of* N *the bound* $RP(N) \le \frac{N^2}{(\log N)^\delta}$ *holds. On the other hand, considering the set* $\{(p, a) \mid p \text{ prime}, a < p, \mu^2(a) = 1\}$ *one gets the trivial bound* $RP(N) \gg \frac{N^2}{\log N}$.

However, we will show that in many cases one can obtain lower bounds on $RP(N)$ not too far away from the bound $N^2/\log N$ derived in Example 1.8.

Theorem 1.9. *Suppose that* ∞ *is a critical value of* t, *then independently of the choice of* $P_{a/b} \in t^{-1}(a/b)$ *one has* $RP(N) \gg \frac{N^2}{(\log N)^2}$.

Applying a transformation one readily obtains the following result from 1.9.

Corollary 1.10. *Suppose that* t *has a rational critical value, then* $RP(N) \gg N^2/(\log N)^2$.

Example 1.11. *Let* $\mathbf{X} : Y^2Z = X^3 + AXZ^2 + BZ^3$ *be an elliptic curve over* $\mathbb{Q}$ *and let* t *be the* x *coordinate, i.e.* $t = \frac{X}{Z}$. *Then the critical values of* t *are exactly* ∞ *and the* x*-coordinates of the zeroes of the polynomial* X^3+AX+B, *each of multiplicity 2. In particular, Theorem 1.9 can be applied to show that* $|\{\mathbb{Q}(\sqrt{(a/b)^3 + A(a/b) + B}) \mid 1 \le a, b \le N\}| \gg N^2/(\log N)^2$.

We will also obtain a partial result when the critical values are not rational. This result depends on the density of pairs of integers (a, b) in a square $[1, N] \times [1, N]$ such that the values of a form $F(x, y) \in \mathbb{Z}[x, y]$ are square-free. Only sufficiently strong results are known for quadratic forms. This result is as follows.

Theorem 1.12. *Suppose that* ∞ *is not a critical value of* t, *and that* t *has exactely two distinct critical values which are Galois conjugate to each other. There is a constant* $A > 0$ *depending on* $\mathbf{X}$ *and* t *such that independentely of the choice of* $P_{a/b} \in t^{-1}(a/b)$ *one has* $RP(N) \gg \frac{N^2}{(\log N)^A}$.

2 Toolbox – distinguishing number fields

We briefly describe the tools we will apply to prove Theorem 1.9 and Theorem 1.12. The main idea is to distinguish two number fields by considering the ramifying primes of the respective fields.

Lemma 2.1. *Let $\mathbb{Q} \subset K \subset L$ be number fields.*

(i) The discriminant $\Delta_{\mathbb{Q}}(K)$ of K divides the discrriminant $\Delta_{\mathbb{Q}}(L)$ of L, i.e. if a rational prime p ramifies in K then it ramifies in L.

(ii) Let $K_* \supset K$ be the normal closeure of K. Then a rational prime p ramifies in K if and only if it ramifies in K_*. In particular, p ramifies in K if and only if it ramifies in one of the conjugate fields of K.

We will then apply Lemma 2.1 (ii) using Hilbert's Irreducebility Theorem, HIT.

Theorem 2.2 (Hilbert's Irreduciblity Theorem, (see (Z) Theorem 1.2))**.** *In the above set-up, the number of reducible fibers is bounded by*

$$\#\{(a,b) \in [1,N]^2 \mid t^{-1}(a/b) \quad \textit{is reducible}\} \leq c(v) N \log N.$$

Recall that the finite critical values of t come in Galois conjugates, hence

$$\tilde{f}(x) := \prod_{\substack{\alpha \in \bar{\mathbb{Q}} \\ \alpha \text{ critical value}}} (x - \alpha) \in \mathbb{Q}[x].$$

Normalizing $\tilde{f}$ we obtain a primitive integer polynomial f. The polynomial f is called the *critical polynomial* of t and it roughly holds the information when a rational prime ramifies in a number field $\mathbb{Q}(P_{a/b})$. This relationship has been worked out in [BG], and we state their result here.

Theorem 2.3 (Bilu, Gillibert)**.** *Let p be a sufficiently large prime number (in terms of $\mathbf{X}$ and t) and let $r \in \mathbb{Q}$.*

(i) Assume that

(1) either $\nu_p(f(r)) = 1$, or
(2) ∞ is a critical value of t and $\nu_p(r) = -1$.

Then p ramifies in $\mathbb{Q}(P_r)$ for some $P_r \in t^{-1}(r)$.

(ii) Assume that p ramifies in $\mathbb{Q}(P)$ for some $P \in t^{-1}(r)$, then

(1) either $\nu_p(f(r)) \geq 1$, or
(2) ∞ is a critical value of t and $\nu_p(r) \leq -1$.

Note that by Hilbert's irreducibility theorem ramification in $\mathbb{Q}(t^{-1}(a/b))$ means ramification in $\mathbb{Q}(P_{a/b})$ for any $P_{a/b} \in t^{-1}(a/b)$ for almost all rational numbers a/b with $1 \leq a, b \leq N$.

Remark 2.4. *From Theorem 2.3 it follows that in order to prove Corollarry 1.5 it suffices to show that for a square-free integer polynomial $f \in \mathbb{Z}[x]$ there is a constant $c > 0$ such that for N large enough there are at least cN distinct primes $p > N \log N$ such that $p \| f(n)$ for some $1 \le n \le N$. In [MR] it is shown that a positive proportion of values, $f(n)$ with $1 \le n \le N$, have a prime divisor $p \mid f(n)$ with $p > N \log N$. It would suffice to show that for a positive proportion of those large primes one would have $p \| f(n)$.*

3 Proof of Theorem 1.9

Proof of Theorem 1.9. Assume that N is a large integer, and let f be the critical polynomial of t, of degree d, say. Define the two mutually disjoint sets of primes

$$\mathcal{P}_1 := \mathcal{P}_f \cap [N/4, N/2],\ \mathcal{P}_2(f) := [N/10, N/5]$$

where $\mathcal{P}_f$ is the set of primes that divide some value of f. By the Chebotarev Density Theorem we may choose $c_1 := c_1(f) > 0$ such that

$$\min\{|\mathcal{P}_1|, |\mathcal{P}_2|\} \ge c_1 \frac{N}{\log N}.$$

In the sequel we will denote primes from $\mathcal{P}_1$ with p's and primes from $\mathcal{P}_2$ by q's.

We will consider the set of points from the fibers of the form $t^{-1}(n/p)$ where $1 \le n \le N$ and $p \in \mathcal{P}_1$.

Lemma 3.1. *Let $p \in \mathcal{P}_1$.*

(i) For any prime $q \in \mathcal{P}_2$ there is an integer $1 \le n \le N$ such that $\nu_q(f(\frac{n}{p})) = 1$

(ii) For every integer $1 \le n \le N$ there are at most d primes $q \in \mathcal{P}_2$ such that $\nu_q(f(\frac{n}{p})) \ge 1$.

(iii) There is a subset $\mathcal{N}(p) \subseteq [1, N]$ with at least $m_p = \lfloor \frac{c_1}{d} \frac{N}{\log N} \rfloor$ distinct elements $\{n_1, n_2, \dots, n_{m_p}\} \subset [1, N]$ such that there is a prime $q_1 \in \mathcal{P}_2$ with $\nu_{q_1}(f(\frac{n_1}{p})) = 1$ and such that $j \ge 2$ there is a prime $q_j \in \mathcal{P}_2$ such that $\nu_{q_j}(f(\frac{n_j}{p})) = 1$ and $\nu_{q_j}(f(\frac{n_i}{p})) = 0$ for $i < j$.

Proof of Lemma 3.1. Ad (i): Let $q \in \mathcal{P}_2$ and denote by $\rho_f(q^j)$ the number of roots of $f \bmod q^j$ in $\mathbb{Z}/q^j\mathbb{Z}$. By Hensel's lemma $\rho_f(q^j) = \rho_f(q) > 0$ for any $j \ge 1$. Since $n/p \equiv n'/p \bmod q^i$ if and only if $n \equiv n' \bmod q^i$ we see that

$$[1, N] \supset \{1 \le n \le 2q + 1 \mid \nu_q(f(\tfrac{n}{p})) \ge 1\}$$

has $2\rho_f(q)$ elements. Furthermore, since $q^2 > N$ we see that

$$[1, N] \supset \{1 \le n \le 2q + 1 \mid \nu_q(f(\tfrac{n}{p})) \ge 2\}$$

has at most $\rho_f(q)$ elements. Hence, there are at least $\rho_f(q) > 0$ integers $1 \le n \le N$ such that $\nu_q(f(\frac{n}{p})) = 1$.

Ad (ii) Write $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$, then

$$f(\tfrac{n}{p}) = \frac{a_d n^d + a_{d-1}n^{d-1}p + \cdots + a_1 np^{d-1} + a_0 p^d}{p^d}.$$

The numerator in the expression above can be bounded by MdN^d where M is the maximum absolute value of the coefficients of f. Since N was chosen large we see that there can be at most d primes, q, from $\mathcal{P}_2$ such that $\nu_q(f(\frac{n}{p})) \geq 1$ since $(N/10)^{d+1} > MdN^d$ for large enough N.

Ad (iii): Let $q_1 \in \mathcal{P}_2$, and choose an integer $n_1 \in [1, N]$ such that

$$\nu_{q_1}(f(\tfrac{n_1}{p})) = 1.$$

Furthermore, put

$$\mathcal{S}_1 := \{q \in \mathcal{P}_2 \mid \nu_q(f(\tfrac{n_1}{p})) \geq 1\}.$$

Recursively, for $i \geq 2$ choose $q_i \in \mathcal{P}_2 \setminus S_{i-1}$ and $n_i \in [1, N]$ such that

$$\nu_{q_i}(f(\tfrac{n_i}{p})) = 1.$$

Furthermore, put

$$\mathcal{S}_i := \mathcal{S}_{i-1} \cup \{q \in \mathcal{P}_2 \mid \nu_q(f(\tfrac{n_i}{p})) \geq 1\}.$$

By (ii) we then find

$$|\mathcal{S}_j| = \Big|\bigcup_{i \leq j}\{q \in \mathcal{P}_2 \mid f(\tfrac{n_i}{p}) \geq 1\}\Big| \leq \sum_{i=1}^{j} |\{q \in \mathcal{P}_2 \mid f(\tfrac{n_i}{p}) \geq 1\}| \leq jd,$$

showing that we may repeat the recursion at least

$$|\mathcal{P}_2|/d \geq \frac{c_1}{d}\frac{N}{\log N}$$

times. □

For a fixed $p \in \mathcal{P}_1$ we fix for every $n_j \in \mathcal{N}(p)$ a prime q_j with the property that $\nu_{q_j}(f(\frac{n_j}{p})) = 1$ and $\nu_{q_j}(f(\frac{n_i}{p})) = 0$ for all $i < j$. We call this the *fresh* prime of n_j and denote it by $\mathrm{Fresh}(n_j)$.

Lemma 3.2. *Let $p_1, p_2 \in \mathcal{P}_1$ be distinct primes, then*

(a) There are at most $4d$ values of $n \in [1, N]$ such that $\nu_{p_1}(f(\frac{n}{p_2})) \geq 1$ in the interval $[1, N]$.

(b) There are at most $4d^2$ primes $q \in \mathcal{P}_2$ for which there is an integer $1 \leq n \leq N$ with $\nu_q(f(\frac{n}{p_2})) \geq 1$ and $\nu_{p_1}(f(\frac{n}{p_2})) \geq 1$.

Proof of Lemma 3.2. Ad (a): For any integer $m \in [1, p_1]$ there are at most $N/p_1 \leq 4$ integers $n \in [1, N]$ such that $n/p_2 \equiv m \bmod p_1$. Since $\rho_f(p_1) \leq d$, the claim follows.

Ad (b): Similar to the proof of (ii) in Lemma 3.1 we see that each of the at most $4d$ values of $1 \leq n \leq N$ with $\nu_{p_1}(f(\frac{n}{p_2})) \geq 1$ there are at most d primes $q \in \mathcal{P}_2$ with positive q-adic valuation, thus in total at most $4d^2$ such primes. □

We now formulate the main Lemma for the proof of Theorem 1.9:

Lemma 3.3. *Let $\mathcal{A} \subset \mathcal{P}_1$. Then for every $p \in \mathcal{P}_1$ there is a subset $\mathcal{M}(\mathcal{A}, p) \subset \mathcal{N}(p)$ with*

$$|\mathcal{M}(\mathcal{A}, p)| \geq |\mathcal{N}(p)| - 4d^2|\mathcal{A}|,$$

such that for all $p' \in \mathcal{A}$ and $n_j \in \mathcal{M}(\mathcal{A}, p)$ with corresponding fresh prime q_j one has the implication

$$\Big(\nu_p(f(\tfrac{s}{p'})) \geq 1, \text{ for some } 1 \leq s \leq N\Big) \Longrightarrow \nu_{q_j}(f(\tfrac{s}{p'})) = 0 \tag{2}$$

Proof of Lemma 3.3. Let $p \in \mathcal{P}_1$. For $p' \in \mathcal{A} \subset \mathcal{P}_1$ Lemma 3.2 yields that the set

$$\mathcal{B}(p, p') := \{q \in \mathcal{P}_2 \mid \exists\ s \in [1, N] : \nu_p(f(\tfrac{s}{p'})), \nu_q(f(\tfrac{n}{p'})) \geq 1\}$$

contains at most $4d^2$ elements, and hence

$$\mathrm{Bad}(p) := \bigcup_{p' \in \mathcal{A}} \mathcal{B}(p, p')$$

satisfies

$$|\mathrm{Bad}(p)| \leq 4d^2|\mathcal{A}|.$$

Now, let

$$\mathcal{N}_B(p) = \{n \in \mathcal{N}(p) \mid \mathrm{Fresh}(n) \in \mathrm{Bad}(p)\}$$

and put

$$\mathcal{M}(\mathcal{A}, p) = \mathcal{N}(p) \setminus \mathcal{N}_B(p).$$

It is then easy to see that $\mathcal{M}(\mathcal{A}, p)$ contains at least $|\mathcal{N}(p)| - 4d^2|\mathcal{A}|$ elements and satisfies (2). □

Now, let $\mathcal{A} \subset \mathcal{P}_1$ be a set with

$$|\mathcal{A}| = \frac{c_1}{16d^3} \frac{N}{\log N}.$$

For $p \in \mathcal{A}$ one has by Lemma 3.3

$$|\mathcal{M}(\mathcal{A}, p)| \geq \frac{c_1}{3d} \frac{N}{\log N}.$$

Let

$$\mathcal{S} := \Big\{\frac{n}{p} \mid p \in \mathcal{A},\ n \in \mathcal{M}(\mathcal{A}, p)\Big\}.$$

Then

$$|\mathcal{S}| = \sum_{p \in \mathcal{A}} |(\mathcal{M}(\mathcal{A}, p))| \geq \Big(\frac{c_1}{16d^3} \frac{N}{\log N}\Big)\Big(\frac{c_1}{3d} \frac{N}{\log N}\Big) \geq c_2 \frac{N^2}{(\log N)^2},$$

for some $c_2 > 0$. Let

$$\mathcal{S}' = \Big\{\frac{a}{b} \in \mathcal{S} \mid t^{-1}(a/b) \text{ irreducible}\Big\},$$

and notice that by Hilbert's irreducibility Theorem

$$|\mathcal{S}'| \geq c_3 \frac{N^2}{(\log N)^2},$$

for some $c_3 > 0$.

We now claim that the number fields $\mathbb{Q}(P_{a/b})$ with $a/b \in \mathcal{S}'$ and any $P_{a/b} \in t^{-1}(a/b)$ are pairwise distinct. Since the fibers $t^{-1}(a/b)$ are irreducible we see by Lemma 2.1 and Theorem 2.3 that it suffices to show that for any n/p, n'/p' in $\mathcal{S}'$ one of the two statements below hold true:

- There is a prime $q \in \mathcal{P}_2$ such that $\nu_q(f(\frac{n}{p})) = 1$ and $\nu_q(f(\frac{n'}{p'})) = 0$, or
- $p \neq p'$ and $\nu_p(f(\frac{n'}{p'})) = 0$ or $\nu_{p'}(f(\frac{n}{p})) = 0$.

Thus, let n/p and n'/p' be distinct elements from $\mathcal{S}'$. If $p = p'$ we may write $n = n_j$ and $n' = n_k$ where n_j and n_k are elements from $\mathcal{M}(\mathcal{A}, p)$ and, without loss of generality $j > k$. Then by the existence of the fresh prime q_j of n_j we may take $q = \mathrm{Fresh}(n_j)$ in the first bullet above. If $p \neq p'$ and we are not in the case of the second bullet, then by the construction of $\mathcal{M}(\mathcal{A}, p)$ we may take $q = \mathrm{Fresh}(n)$. In conclusion, the sets of ramifying primes in any fields $\mathbb{Q}(P_{a/b})$ and $\mathbb{Q}(P_{a'/b'})$ with distinct a/b, a'/b' in $\mathcal{S}'$ are different, and in particular, all the fields $\mathbb{Q}(P_{a/b})$ with $\frac{a}{b} \in \mathcal{S}'$ are distinct. □

4 Proof of Corollary 1.10

Proof of Corollary 1.10. Suppose $\alpha := \frac{a_0}{b_0}$ is a critical value of t. Then

$$t^{-1}(a/b) = \tilde{t}^{-1}((\tfrac{a}{b} - \alpha)^{-1}),$$

where

$$\tilde{t} = \frac{1}{t - \alpha}$$

is a rational function on $\mathbf{X}$ which has ∞ as a critical value. Since any rational number $\frac{a'}{b'}$ with $1 \leq a', b' \leq \frac{N}{3a_0b_0}$ can be written in the form $(\frac{a}{b} - \alpha)^{-1}$ with $1 \leq a, b \leq N$ we obtain from Theorem 1.9 that

$$RP(N) \gg \frac{(N/3a_0b_0)^2}{(\log N/3a_0b_0)^2} \gg \frac{N^2}{(\log N)^2},$$

as desired. □

5 Proof of Theorem 1.12

Again, let f be the critical polynomial of t, which now by assumption is an irreducible quadratic polynomial. By Theorem 2.3 the ramification of primes in $\mathbb{Q}(P_{a/b})$ is controlled by the divisors of the numerator in

$$f(a/b) := \frac{F(a, b)}{b^2},$$

where $F(x,y) \in \mathbb{Z}[x,y]$ is an irreducible quadratic form. In [LX] it is proved that if F does not have a fixed square divisor other than 1, then

$$|\{(a,b) \in [1,N]^2 \mid \mu^2(F(a,b)) = 1\}| \sim \underbrace{\prod_p \left(1 - \frac{\rho_F(p^2)}{p^4}\right)}_{C_F} N^2,$$

and that the constant C_F is positive since the number of solutions $\rho_F(p^k)$ of

$$p^2 \mid F(a,b),\ 1 \le a,b \le N$$

can be bounded by p^{2k-2} for $k \ge 2$. In our situation we do not know apriori whether F does not have a fixed square divisor greater than one, but we can obtain a result that fits in to our framework by altering the proof of Lapkova and Xiao's result slightly. Call a prime p a *fixed square prime* of F if $p^2 \mid F(a,b)$ for all $a,b \in \mathbb{Z}$, and notice that there are at most finitely many such.

Proposition 5.1. *Let c be a constant greater than all fixed square primes of F and greater than all coeffcients of F. Then*

$$|\{(a,b) \in [1,N]^2 \mid \exists p \ge c : p \mid F(a,b),\ \forall q \ge c,\ q^2 \nmid F(a,b)\}| \sim \prod_{p \ge c} \Big(1 - \frac{\rho_F(p^2)}{p^4}\Big) N^2.$$

Proof of Proposition 5.1. We adapt the proof of Theorem 1.2 in [LX]. Let $\xi_1 = \frac{1}{4}\log N$ and $\xi_2 = N(\log N)^{1/2}$ and

$$\mathrm{S}_F(N) = \{(a,b) \in [1,N]^2 \mid \exists p \ge c : p \mid F(a,b),\ \forall q \ge c,\ q^2 \nmid F(a,b)\},$$

$$\mathrm{S}_0(N) = \{(a,b) \in [1,N]^2 \mid p \mid F(a,b) \Longrightarrow p \le c\},$$

$$\mathrm{S}_1(N) = \{(a,b) \in [1,N]^2 \mid p^2 \mid F(a,b) \Longrightarrow c \le p \text{ or } p > \xi_1\},$$

$$\mathrm{S}_2(N) = \{(a,b) \in [1,N]^2 \mid p^2 \mid F(a,b) \Longrightarrow p > \xi_1,\ \exists \xi_1 < p \le \xi_2 : p^2 \mid F(a,b)\},$$

$$\mathrm{S}_3(N) = \{(a,b) \in [1,N]^2 \mid p^2 \mid F(a,b) \Longrightarrow p > \xi_2,\ \exists p \ge \xi_2 : p^2 \mid F(a,b)\}.$$

Denote the size of $\mathcal{S}_F(N)$ and $\mathcal{S}_i(N)$ by $S_F(N)$ and $S_i(N)$, respectively. It is seen that

$$S_1(N) - S_0(N) - S_2(N) - S_3(N) \le S_F(N) \le S_1(N). \tag{3}$$

The sets $\mathcal{S}_2(N)$ and $\mathcal{S}_3(N)$ have also been considered in $[LX]$, and it is shown in their setting that both of these sets are of size $o(N^2)$. The proofs of these bounds depend only on large primes dividing values of $F(x,y)$, and the proofs can be adapted 1-to-1 to our situation to give $S_2(N), S_3(N) = o(N^2)$.

Let $B := \pi(c)$ denote the number of primes less than c and recall that

$$\#\{n \le N \mid p \mid n \Longrightarrow p \le c\} \ll (\log N)^B. \tag{4}$$

For any integer m the equation $F(a,b) = m$ obviously has at most $2N$ solutions with $1 \le a, b \le N$, hence

$$S_0(N) \le (\log N)^B(2N) = o(N^2).$$

Finally, $S_1(N)$ can be bounded in the same manner as in [LX]:

$$\begin{aligned} S_1(N) &= \sum_{\substack{h\in\mathbb{N} \\ p|h \Rightarrow c\le p\le \xi_1}} \mu(h)\rho_F(p^2)\Big(\frac{N^2}{h^4} + O\Big(\frac{N}{h^2}+1\Big)\Big) \\ &= N^2 \prod_{c\le p\le \xi_1}\Big(1-\frac{\rho_F(p^2)}{p^4}\Big) + O\Big(\sum_{h\le e^{2\xi_1}} h^{-2+\epsilon}(Nh^{-2}+1)\Big) \\ &= N^2 \prod_{p\ge c}\Big(1-\frac{\rho_F(p^2)}{p^4}\Big) + O(N^2\xi_1^{-1}) + o(N^2) \\ &\sim N^2 \prod_{p\ge c}\Big(1-\frac{\rho_F(p^2)}{p^4}\Big). \end{aligned}$$

Putting all the estimates for the different $S_i(N)$'s together in (3) we obtain the result. □

Lemma 5.2. *Let c be as in Proposition 5.1 and let $m \in \mathcal{S}_F(N)$, then*

$$|\{(a,b) \in [1,N]^2 \mid F(a,b) = m\}| \ll \log N.$$

Proof of Lemma 5.2. Write $F(x,y) = \alpha x^2 + \beta xy + \gamma y^2$ with $\alpha, \beta, \gamma \in \mathbb{Z}$. Solving the equation $F(a,b) = m$ for a we find

$$a = \frac{-\beta y \pm \sqrt{\beta^2 y^2 - 4\alpha(\gamma y^2 - m)}}{2\alpha},$$

showing that

$$\beta^2 y^2 + 4\alpha(\gamma y^2 - m) = k^2 \tag{5}$$

for some integer k. Rewriting (5) we obtain the Pell equation

$$(\beta^2 - 4\alpha\gamma)y^2 - k^2 = -4\alpha m.$$

Since F is irreducible $\beta^2 - 4\alpha\gamma$ is not a square. Since $m \in \mathcal{S}_F(N)$ m has a prime factor $p \ge c$ with multiplicity 1, and so $4\alpha m$ is not a square number since c was assumed larger than α. From the standard theory of Pellian equations, see [M], it follows that there are bounded by $\log N$ many solutions to (5) with $1 \le y \le N$, as needed. □

Proof of Theorem 1.12. Let $c > 0$ be a constant as in the formulation of Proposition 5.1. Let again $B = \pi(c)$ be the number of primes less than c, and let $A = B + 1$. Call two numbers $m, m' \in \mathcal{S}_F(N)$ *related* if $\nu_p(m) = \nu_p(m')$ for all $p \ge c$. Notice that by (4) any $m \in \mathcal{S}_F(m)$ is related to at most $(\log N)^B$ numbers from $\mathcal{S}_F(m)$. Using Lemma 5.2 we see that

$$\{F(a,b) \mid (a,b) \in [1,N]^2\}$$

consists of at least $M := N^2/(\log N)^A$ classes of related numbers. For any of these classes C of related numbers let m_C be a representative such that there is a rational number a_{m_C}/b_{m_C}, $1 \le a_{m_C}, b_{m_C} \le N$ with $F(a_{m_C}, b_{m_C}) = m$. Applying Theorem 2.3 we see that almost all the fields $\mathbb{Q}(P_{a_{m_C}/b_{m_C}})$ are distinct. □

6 Literature

- [BL] Yuri Bilu, Florian Luca, Diversity in Parametric Families of Number Fields
- [BL2] Yuri Bilu, Florian Luca, Number Fields in Fibers: The Geometrically Abelian Case with Rational Critical Values
- [BG] Yuri Bilu (With an Appendix by Jean Gillibert), Counting Number Fields in Fibers
- [MR] James Maynard, Ze'ev Rudnick, A lower bound on the least common multiple of polynomial sequences
- [LX] Kostadinka Lapkova, Stanley Yao Xiao, Density of Power-free Values of Polynomials
- [DZ] R. Dvornicich, U. Zannier, Fields containing values of algebraic functions, Annali Della Scuola Normale Superiore Di Pisa Classe di Scienze (4) 21 (1994), 421–443
- [DZ2] R. Dvornicich, U. Zannier, Fields containing values of algebraic functions II (On a conjecture of Schintzel), Acta Arith. 72 (1995), 201–210
- [M] L.J Mordell, Diophantine equations, Academic Press (1969)
- [Z] David Zywina, Hilbert's irreducibility theorem and the large sieve
- [DLS] H. Davenport, D. Lewis, A. Schintzel, Polynomials of certain special types, Acta Arithmetica 9, 107–116 (1964)
- [N] W. Narkiewicz. Elementary and analytic theory of algebraic numbers, Volume 322 of Springer Monograph. Math. Berlin: Springer 3rd edition, 2004.

Acknowledgement: The author thanks Yuri Bilu for suggesting this topic, and Christopher Frei for answering many questions.