UNIFORM IRREDUCIBILITY AND GALOIS GROUPS OF GENERALIZED LAGUERRE POLYNOMIALS

KHAI-HOAN NGUYEN-DANG

Abstract. We prove that the generalized Laguerre polynomial $H_{n,s}$ is irreducible over $\mathbb{Q}$ and has Galois group containing A_n for every positive integer s, once n exceeds an effective absolute constant. Equivalently, every numerator and denominator in the exponential Padé table has these properties once its own degree is sufficiently large. The exceptional positive integral pairs form an effectively computable finite set. The proof combines integral traces at degenerate fibers, Padé resultants, and an energy inequality for Galois-invariant positive semidefinite forms on the roots.

hexagon:2611.00087v1

1. Introduction

A classical theorem of Schur [43] states that the exponential Taylor polynomial

$$E_n(X) = \sum_{j=0}^{n} \frac{X^j}{j!}$$

is irreducible over $\mathbb{Q}$ for every $n \geq 1$. One also can determine its Galois group: it is A_n when $4 \mid n$ and S_n otherwise [44] (see also [10]).

In fact, Schur family occurs among the generalized Laguerre polynomials. More precisely, we use the monic normalization

$$H_{n,s}(X) = \sum_{k=0}^{n} \binom{n}{k} (s)_k X^{n-k}, \qquad (s)_0 = 1, \qquad (s)_k = s(s+1)\cdots(s+k-1). \tag{1.1}$$

Here n is a nonnegative integer and s may be complex; in particular, $H_{0,s} = 1$. Our main arithmetic results concern positive integers n, s, for which $H_{n,s} \in \mathbb{Z}[X]$. It is also a generalization of Bessel polynomials (see [26]):

$$y_n(X) = \sum_{j=0}^{n} \frac{(n+j)!}{(n-j)!\, j!} \left(\frac{X}{2}\right)^j.$$

Filaseta proved y_n is irreducible over $\mathbb{Q}$ for all sufficiently large n in 1995 [21]. After that, together with Trifonov, they proved the result for every n [24].

Note that the two classical families are the specializations

$$H_{n,1}(X) = n! E_n(X), \qquad H_{n,n+1}(X) = X^n y_n(2/X). \tag{1.2}$$

The second identity uses the usual normalization of the Bessel polynomial [40, (18.34.1)]. Multiplication by a nonzero rational constant and the reciprocal substitution in (1.2) preserve irreducibility and splitting fields.

Hajir proposed extending these arithmetic properties to every positive integral pair (n, s) [29, Conjectures 1.1–1.2]. His first conjecture asserts that every $H_{n,s}$ is irreducible over $\mathbb{Q}$. His second asserts that, whenever $H_{n,s}$ is irreducible, its Galois group contains A_n. We prove both assertions

2020 *Mathematics Subject Classification.* Primary 11R09; Secondary 11C08, 11J86, 14H25, 20B15, 33C45.

Key words and phrases. Generalized Laguerre polynomial, irreducibility, Galois group, Padé approximation, Newton polygon, logarithmic energy.

ORCID: 0000-0002-6765-811X.

in all sufficiently large degrees, with an effective degree bound independent of s, and show that the remaining exceptional pairs form an effectively computable finite set.

1.1. **Uniform arithmetic.** For positive integers n, s, write $G_{n,s} = \mathrm{Gal}(H_{n,s}/\mathbb{Q})$ for the Galois group in its action on the roots. These roots are distinct, and the action is transitive exactly when $H_{n,s}$ is irreducible over $\mathbb{Q}$.

Theorem 1.1. *There is an effectively computable absolute integer N such that*

$$n \geq N, \qquad s \in \mathbb{Z}_{\geq 1} \quad \Longrightarrow \quad H_{n,s} \text{ is irreducible over } \mathbb{Q} \quad \text{and} \quad A_n \leq G_{n,s}.$$

The bound is uniform in the parameter: s may grow arbitrarily with n. Thus the theorem applies to every sequence $s = s(n)$ of positive integers. Proposition 3.21 proves irreducibility. Theorem 4.28 proves alternating containment for irreducible members, with a second effective degree bound independent of s.

Corollary 1.2. *The set of positive integral pairs (n, s) for which $H_{n,s}$ is reducible or $A_n \not\leq G_{n,s}$ is finite and effectively computable.*

For reducibility, the fixed-degree bound is explicit:

$$H_{n,s} \text{ reducible}, \quad n \geq 2 \quad \Longrightarrow \quad s < \left\lfloor \frac{n^2}{4} \right\rfloor^n. \tag{1.3}$$

For irreducible specializations with smaller Galois group, a decomposition-group criterion at infinity permits an effective application of Runge's theorem. Combining these fixed-degree results with Theorem 1.1 proves the corollary in Section 5. The exceptional set has not been enumerated, and we do not prove that it is empty. Thus the result gives uniform eventual forms of Hajir's conjectures and an effective finite reduction of their all-degree forms.

Earlier work controls complementary parts of the parameter plane. Hajir proved both conclusions for each fixed s and all sufficiently large n [29, Theorem 1.3]. Jindal–Laishram–Sarma gave the explicit sufficient condition

$$r = s - 1 \geq 2, \qquad n > \exp\left(r\left(1 + \frac{1.2762}{\log r}\right)\right),$$

and proved both conclusions in every degree for $1 \leq s \leq 61$ [32, Theorems 1.1–1.2]. The published theorem of Jindal–Nair–Shorey extends that interval to $1 \leq s \leq 93$ and proves the Galois assertion, conditional on irreducibility, for $94 \leq s \leq 101$ [33]. Jindal–Laishram studied the neighboring Bessel lines $n \leq s \leq n + 4$ [31]. In the other direction, Hajir–Wong proved that for each fixed $n \geq 5$, all but finitely many rational parameters give irreducibility and alternating containment [30, Theorem 1(a)]; the finiteness there is ineffective [29, Corollary 6.2 and the following remark]. Finiteness on each fixed row and column does not exclude infinitely many exceptional pairs with both coordinates unbounded. Theorem 1.1 excludes such pairs.

The fixed-parameter results for $L_n^{(\alpha)}$, where

$$H_{n,s}(X) = (-1)^n n! L_n^{(-n-s)}(X), \tag{1.4}$$

with $\alpha \in \mathbb{Q} \setminus \mathbb{Z}_{<0}$ have a different scope: Filaseta–Lam proved eventual irreducibility, and Hajir proved eventual alternating containment [22, Theorem 1][28, Theorem 1.1]. Here $\alpha = -n - s$ varies with the degree and is a negative integer. For the Bessel specialization, the irreducibility theorem of Filaseta–Trifonov and Grosswald's criterion give S_n in every degree [24][27, Chapter 12, Theorem 1′].

1.2. **Root geometry and the proof.** A root theorem valid for every $n \geq 2$ supplies the complex estimates in the arithmetic proof. Fix $n \geq 2$, continue a root or a conjugate pair of $H_{n,s}$ along $s > 0$, and write $q(s)$ for its modulus. Classical annular estimates for generalized Bessel polynomials locate these roots [6]. The next theorem also describes their motion.

Theorem 1.3. *For every such branch there is a unique finite, absolutely continuous, nonnegative measure μ on $[0, n-1]$ such that*

$$q(s) = s + \int_0^{n-1} \frac{s}{s+t}\, d\mu(t) \qquad (s > 0).$$

If $\xi \geq 0$ is the corresponding absolute Hermite zero, characterized by $\alpha(s) = -s + i\xi\sqrt{s} + O(1)$ as $s \to +\infty$ for the upper-half-plane root (and $\xi = 0$ for the real root), then

$$\mu([0, n-1]) = \frac{n-1}{3} + \frac{\xi^2}{6}.$$

For every integer $r \geq 1$ and every $s > 0$,

$$(-1)^{r-1} \frac{d^r}{ds^r}(q(s) - s) > 0.$$

Here the Hermite polynomials have the probabilists' normalization, specified in (2.16). Theorem 2.5, Corollary 2.6, and Proposition A.2 prove the statement and identify the exact support of each measure. In particular, $q - s$ is strictly increasing and strictly concave, and is a complete Bernstein function. Castillo obtains related complete Bernstein representations for scaled ultraspherical zeros [9]; the present representation concerns complex Laguerre roots in the range $\alpha < -n$.

Outline of the proof. The proof separates three possibilities: a rational factor, an imprimitive action on the roots, and a primitive Galois group not containing A_n. Integral traces and one energy inequality control factors and invariant partitions. Local permutations handle the remaining primitive groups.

First, a tridiagonal realization and Fan's variational principle [20] give the strict trace estimate

$$\left| \operatorname{Re} \sum_{i=1}^{d} (\alpha_i + s) \right| < d(n-d) \qquad (0 < d < n). \tag{1.5}$$

The centered trace of a rational factor is therefore an integer in a bounded interval independent of s. At $s = 0, -1, -2, -3$, at most three roots are nonzero. Reduction at these four fibers restricts the trace to finitely many subset sums. For every $n \geq 2$, a reducible member consequently has

$$\operatorname{rad}\big((s+i)(s+j)\big) < n^6 \quad \text{for some } 0 \leq i < j \leq 3.$$

Matveev's theorem [38] then gives $\log s < n^{\varepsilon}$ for every fixed $\varepsilon > 0$ and all effectively sufficiently large n. Theorem 2.12 isolates this argument for general monic families; Theorem 2.15 gives the all-degree bound, including rational parameters.

Second, we attach to a factor or an invariant partition a Galois-invariant positive semidefinite matrix Q with $Q\mathbf{1} = 0$. At a finite place, a cluster of roots contributes a nonnegative squared difference between its actual and expected occupation. The product formula compares the sum of these local contributions with complex logarithmic energy. The root-modulus representation supplies the complex bounds uniformly in s. For factors, the energy estimate and a nonzero Padé resultant give incompatible restrictions on the factor degree. The resulting contradiction proves uniform irreducibility.

For the Galois group, local permutations first exclude primitive groups not containing A_n. The partition energy and trace bounds then reduce imprimitivity to a partition into two blocks. The stabilizer of a block fixes a quadratic field. The real quadratic case is controlled by traces. In

the imaginary quadratic case, we construct integral functions whose block sums are small and whose first nonzero Laurent terms distinguish the blocks. The underlying interpolation theorem identifies a cyclic intermediate field as the obstruction to prescribing Laurent coefficients. Hermite expansions and Gaussian quadrature provide the quantitative bounds needed after specialization. The last contradiction uses a criterion for large prime valuations at nearby integers. The primitive-group step uses Burness–Guralnick [7]; this is the only input to the main theorem that uses the classification of finite simple groups.

1.3. **Consequences and related families.**

The exponential Padé table. The same question has a natural formulation in rational approximation. For $a, b \geq 0$, let $A_{a,b}/B_{a,b}$ be the Padé approximant of type $[a/b]$ to e^X, normalized by $A_{a,b}(0) = B_{a,b}(0) = 1$. Thus

$$\deg A_{a,b} = a, \qquad \deg B_{a,b} = b, \qquad B_{a,b}(X)e^X - A_{a,b}(X) = O(X^{a+b+1}).$$

Its numerator and denominator are

$$A_{a,b}(X) = \frac{b!}{(a+b)!} H_{a,b+1}(X), \qquad B_{a,b}(X) = \frac{a!}{(a+b)!} H_{b,a+1}(-X). \tag{1.6}$$

Cullinan–Scheel used these identities to study diagonal approximants and special cases of irreducibility [11]. The boundary $b = 0$ gives the exponential Taylor polynomials, and the diagonal $a = b$ gives the Bessel polynomials.

Corollary 1.4. *For the absolute constant N in Theorem 1.1, $A_{a,b}$ is irreducible over $\mathbb{Q}$ with Galois group containing A_a whenever $a \geq N$, for every $b \geq 0$. Likewise, $B_{a,b}$ is irreducible with Galois group containing A_b whenever $b \geq N$, for every $a \geq 0$.*

Proof. Apply Theorem 1.1 to (1.6). Multiplication by a nonzero rational constant and $X \mapsto -X$ preserve irreducibility and splitting fields. □

This is an equivalent form of the main theorem: the required bound depends only on the degree of the numerator or denominator being studied. It also applies to the exponential family in [41, Question 1.3 and Theorem 1.4].

The symmetric and alternating cases. Schur's discriminant formula [45, p. 54, (7)], in the present normalization, is

$$\Delta_{n,s} = (-1)^{n(n-1)/2} \prod_{j=2}^{n} j^j (s+n-j)^{j-1}. \tag{1.7}$$

Once alternating containment is known, the square class of $\Delta_{n,s}$ determines whether $G_{n,s} = A_n$ or S_n. In particular, $G_{n,s} = S_n$ when $n \equiv 2, 3 \pmod 4$ and $n \geq N$. The classification of square discriminants by Banerjee–Filaseta–Finch–Leidy [2] gives an exact description in sufficiently large degree: the alternating cases lie on the ten parameter lines

$$s \in \{1, 2, 3, 4, 5, 6, n-4, n, n+2, n+4\},$$

with the conditions in Table 1. The classification is due to the cited authors; the uniform theorem supplies alternating containment throughout the parameter range.

Other families and geometric applications. The methods also apply beyond this family. The finite-fiber criterion proves large-parameter irreducibility for the Appell family generated by $e^{Xz}(1-z)^{-s}(1-2z)^{-s}$ (Theorem 6.1). The prime-valuation criterion gives deterministic symmetric-group results for trimmed exponentials, under an irreducibility hypothesis or an explicit endpoint condition (Theorem 6.5 and Corollary 6.6). Their discriminants are nonsquare in the range of Proposition 6.4, with no upper bound on the parameter. The full conjecture of Bary-Soroker–Ben-Porath remains open [3].

Finally, the uniform theorem permits an arbitrary positive integral parameter in each degree in the root-set criterion of Bary-Soroker–Kadets [4] and in the hyperelliptic-Jacobian theorems of Zarhin [47, 48]. Together with Lombardo's product criterion [35], this gives the geometric consequences in Section 6.3. The general geometric criteria are due to these authors; our contribution is their uniform application to the present family.

Organization. Section 2 develops the root geometry and finite-fiber arithmetic. Sections 3 and 4 prove uniform irreducibility and alternating containment, respectively. Section 5 proves the effective finite reduction. Section 6 contains the applications and the remaining questions. Appendix A gives the analytic-continuation argument for the root-modulus representation; Appendix B provides the exact certificate for the Appell family.

Notation. All logarithms are natural. We normalize $v_p(p) = 1$ and fix embeddings in $\overline{\mathbb{Q}}_p$ when needed. For $m \in \mathbb{Z}_{>0}$, put $\mathrm{rad}(m) = \prod_{p\mid m} p$, $\omega(m) = \#\{p : p \mid m\}$, and let $P(m)$ be its greatest prime divisor; the values at $m = 1$ are $1, 0, 1$, respectively. An integer is y-smooth if all its prime divisors are at most y. For a reduced rational number a/b with $b > 0$, put $H(a/b) = \max\{|a|, b\}$ and $h(a/b) = \log H(a/b)$. Factors of monic integral polynomials are taken monic. A nontrivial block system has at least two blocks, each containing at least two roots; in a transitive action their sizes are equal. For a permutation g on Ω, write $\mathrm{supp}(g)$ for its support and $\mathrm{fpr}(g) = |\operatorname{Fix}(g)|/|\Omega|$. Write $\mu(G)$ for the least support size of a nonidentity element of G. A permutation is called homogeneous if all its nontrivial cycles have the same length. Every constant called effective is computable, with its dependence on fixed parameters indicated.

2. Geometry of the roots and integral traces

2.1. **Root geometry and a preliminary parameter bound.** Two estimates on the roots will be used in the arithmetic proof. After translation by s, the real part of every partial root sum is bounded independently of s. This bounds the traces of rational factors when s is integral. A lower bound of order n for $|\alpha| - s + 1$, uniform for $s \geq 1$, controls the Padé norms. We first work with real parameters and impose integrality when it is needed. Put

$$C_{n,s}(Y) = H_{n,s}(Y - s).$$

2.1.1. *Identities, root counts, and an annulus.* The exponential generating functions are

$$\sum_{n\geq 0} H_{n,s}(X)\frac{t^n}{n!} = e^{Xt}(1-t)^{-s}, \tag{2.1}$$

$$\sum_{n\geq 0} C_{n,s}(Y)\frac{t^n}{n!} = \exp\left(Yt + s\sum_{j\geq 2}\frac{t^j}{j}\right). \tag{2.2}$$

These are identities of formal power series. Coefficient comparison gives

$$H'_{n,s}(X) = nH_{n-1,s}(X), \tag{2.3}$$

$$H_{n+1,s}(X) = (X + s + n)H_{n,s}(X) - nXH_{n-1,s}(X), \tag{2.4}$$

$$XH''_{n,s}(X) - (X + n + s - 1)H'_{n,s}(X) + nH_{n,s}(X) = 0. \tag{2.5}$$

For real $s > 0$, expansion of the integrand also gives

$$H_{n,s}(X) = \frac{1}{\Gamma(s)} \int_0^\infty (X+t)^n t^{s-1} e^{-t}\, dt. \tag{2.6}$$

Thus $H_{n,s}$ has no real root in even degree. In odd degree its derivative is positive on $\mathbb{R}$ by (2.3), so it has exactly one real root, which is negative because $H_{n,s}(0) = (s)_n > 0$.

For any complex parameter, a multiple nonzero root is impossible. Indeed, if $a \neq 0$ were a root of multiplicity $r \geq 2$, the term $XH''_{n,s}$ in (2.5) would have a nonzero coefficient of $(X-a)^{r-2}$, while the other terms would have higher order. A zero root occurs precisely at $s = 0, -1, \ldots, 1-n$. Thus all roots are simple when $s > 0$.

The identity $H_{n,s}(X) = X^n y_n(2/X; s-n+1)$, in the notation of [40, (18.34.1)], relates these roots to those of generalized Bessel polynomials. Classical annular estimates for the latter were given by de Bruin, Saff, and Varga [6, Theorem 5.1]. The following matrix argument gives the bound needed here.

Lemma 2.1. *For $n \geq 2$ and real $s > 0$, every root α of $H_{n,s}$ satisfies*

$$s < |\alpha| < s + n - 1. \tag{2.7}$$

Proof. Let T be the real symmetric tridiagonal matrix with zero diagonal and adjacent entries $\sqrt{1}, \ldots, \sqrt{n-1}$, and put $D_0 = \operatorname{diag}(s, s+1, \ldots, s+n-1)$. The determinant recurrence and (2.4) give

$$H_{n,s}(z^2) = \det(z^2 I - zT + D_0).$$

Choose $z^2 = \alpha$ and a unit vector v in the corresponding kernel. Multiplication on the left by v^* gives

$$z^2 - (v^*Tv)z + v^*D_0 v = 0.$$

Both coefficients are real. Since α is not nonnegative real, z is nonreal; the other root of this scalar quadratic is therefore $\bar{z}$. Consequently

$$|\alpha| = |z|^2 = v^*D_0 v \in [s, s+n-1].$$

Equality at either endpoint would force v to be a multiple of the first or last coordinate vector. The adjacent nonzero entry of T then contradicts $(z^2 I - zT + D_0)v = 0$. Both bounds are strict. □

2.1.2. *Centered roots and integral factor traces.* After centering at $-s$, sums of roots satisfy bounds independent of s. The estimate follows from Fan's maximum principle [20, Theorem 1]; we include the matrix proof to obtain the strict inequality.

Proposition 2.2. *Let $n \geq 2$ and let $s > 0$ be real. For any d distinct roots $\alpha_1, \ldots, \alpha_d$ of $H_{n,s}$, with $0 < d < n$,*

$$\left| \operatorname{Re} \sum_{i=1}^{d} (\alpha_i + s) \right| < d(n-d).$$

In particular, if a is the root sum of a monic real factor of $C_{n,s}$ of degree d, then

$$|a| < d(n-d). \tag{2.8}$$

For positive integral s, a monic rational factor has $a \in \mathbb{Z}$. Moreover, every root α of $H_{n,s}$ satisfies

$$|\alpha + s| \leq n - 1 + 2\sqrt{(n-1)(s+n-1)}. \tag{2.9}$$

Proof. The centered polynomial is the characteristic polynomial of the tridiagonal matrix A with entries

$$\begin{aligned} A_{jj} &= 2j - n - 1 && (1 \leq j \leq n), \\ A_{j,j+1} &= j, \qquad A_{j+1,j} = -(n+s-j) && (1 \leq j < n). \end{aligned}$$

To verify this, let $P_k(X)$ be the characteristic polynomial of the leading k-by-k block of $A - sI$. Its continuant recurrence is

$$P_k = (X + n + s + 1 - 2k)P_{k-1} + (k-1)(n+s-k+1)P_{k-2},$$

with $P_0 = 1$ and $P_1 = X + n + s - 1$. Substitution into this recurrence, using Pascal's identity, verifies the explicit formula

$$P_k(X) = \sum_{j=0}^{k} \frac{k!}{j!} \binom{n+s-1-j}{k-j} X^j.$$

At $k = n$ its coefficient of X^j is $\binom{n}{j}(s)_{n-j}$, as required.

A positive diagonal similarity transforms A into $D + K$, where

$$D = \operatorname{diag}(1-n, 3-n, \ldots, n-1), \qquad K^* = -K,$$

and

$$K_{j,j+1} = \sqrt{j(n+s-j)}, \qquad K_{j+1,j} = -K_{j,j+1}.$$

Eigenvectors belonging to the selected roots span a d-dimensional invariant subspace V. If the columns of U are an orthonormal basis of V, the trace of $U^*(D+K)U$ is $\sum_i(\alpha_i + s)$. Since K is skew-Hermitian,

$$\operatorname{Re}\sum_{i=1}^{d}(\alpha_i + s) = \operatorname{tr}(U^*DU) = \sum_{j=1}^{n}(2j-n-1)w_j, \qquad 0 \le w_j \le 1, \quad \sum_{j=1}^{n} w_j = d,$$

where w_j are the diagonal entries of the orthogonal projection onto V. The minimum and maximum of this expression are the sums of the first and last d diagonal entries of D, namely $-d(n-d)$ and $d(n-d)$. Because those entries are strictly increasing, equality requires V to be the corresponding coordinate subspace. Neither subspace is invariant under $D + K$, as its boundary coupling is nonzero. This proves the first assertion and hence (2.8).

Finally, the row and column sum bounds for the operator norm give

$$\|D\| = n - 1, \qquad \|K\| \le 2 \max_{1 \le j < n} \sqrt{j(n+s-j)} \le 2\sqrt{(n-1)(s+n-1)}.$$

Each $\alpha + s$ is an eigenvalue of $D + K$, proving (2.9). If s is integral, Gauss's lemma makes every monic rational factor integral, and hence its trace is an integer. □

To turn the trace bound into a divisibility condition, we first consider a polynomial that reduces to a power of X times a linear factor. The two residue roots are allowed to coincide.

Lemma 2.3. *Let $P \in \mathbb{Z}[X]$ be monic of degree $N \ge 2$, and suppose that*

$$P(X) \equiv X^{N-1}(X - c) \pmod{M}$$

for integers $M \ge 1$ and c. Suppose a submultiset of the roots of P, counted with multiplicity, has integral sum τ, with $\tau \equiv A \pmod{M}$ and $A(A-c) \ne 0$. Then

$$M \mid \gcd(|A|, |A-c|)\,\operatorname{lcm}(|A|, |A-c|)^{N-1}. \tag{2.10}$$

Proof. Fix $p^e \| M$ and set

$$t = \min\{v_p(A), v_p(A-c)\}, \qquad b = \max\{v_p(A), v_p(A-c)\}, \qquad u = v_p(c) \ge t,$$

where $v_p(0) = +\infty$. Suppose, to obtain a contradiction, that $e > t + (N-1)b$. In particular $e > Nt$. The polynomial $p^{-Nt}P(p^tZ)$ is monic with p-integral coefficients. If $u > t$, its reduction is Z^N, so every root of P has valuation greater than t. Their selected sum does too. But in this case $v_p(A) = v_p(A-c) = t$, contrary to $\tau \equiv A \pmod{p^e}$.

If $u = t$, the reduction is $Z^{N-1}(Z-\gamma)$ with $\gamma \neq 0$. Hensel's lemma lifts the simple nonzero root to a unique root over $\mathbb{Z}_p$. Division by this linear factor leaves a polynomial reducing to Z^{N-1}. Thus exactly one root β of P has valuation t, and all other roots have valuation greater than t. Every root α is integral, and the coefficient congruence implies

$$v_p(\alpha^{N-1}(\alpha - c)) \geq e.$$

For $\alpha \neq \beta$ one has $v_p(\alpha - c) = t$, and therefore

$$v_p(\alpha) \geq \frac{e-t}{N-1} > b.$$

For β the same congruence gives

$$v_p(\beta - c) \geq e - (N-1)t > b.$$

Thus, according as the selection excludes or includes β, either $v_p(\tau) > b$ or $v_p(\tau - c) > b$. Since $e > b$, either conclusion contradicts $\tau \equiv A \pmod{p^e}$. We have proved $e \leq t + (N-1)b$, which is exactly the p-part of (2.10). □

At $s = 0$ and $s = -1$, all but at most one root of $H_{n,s}$ lie at the origin. These two specializations, together with the trace bound, give an effective restriction on the parameter of a reducible member.

Proposition 2.4. *Let $n \geq 2$ and $s \geq 1$ be integers. If a proper monic rational factor of $C_{n,s}$ has degree d and root sum a, then*

$$s \mid a^n. \tag{2.11}$$

If $a = 0$, then

$$s + 1 \mid \gcd(d, n-d)\,\mathrm{lcm}(d, n-d)^{n-1}. \tag{2.12}$$

In particular, writing $B_d = d(n-d)$ and $g = \gcd(d, n-d)$, one has

$$\begin{cases} s \leq (B_d - 1)^n, & a \neq 0, \\ s \leq B_d^{n-1} g^{2-n} - 1, & a = 0. \end{cases} \tag{2.13}$$

Consequently, reducibility of $H_{n,s}$ implies

$$s < \left\lfloor \frac{n^2}{4} \right\rfloor^n, \qquad \log s < 2n \log n. \tag{2.14}$$

Proof. The coefficient formula gives $C_{n,s}(Y) \equiv Y^n \pmod{s}$. For $p^e \| s$, every centered root has valuation at least e/n: otherwise its leading term in the polynomial equation would have strictly smaller valuation than all other terms. Its selected root sum therefore satisfies $v_p(a) \geq e/n$, proving (2.11).

At the next integral fiber,

$$H_{n,s}(X) \equiv X^{n-1}(X - n) \pmod{s+1}.$$

The uncentered root sum is $\tau = a - ds \equiv a + d \pmod{s+1}$. When $a = 0$, Lemma 2.3, with $A = d$ and $c = n$, applies because $0 < d < n$, and proves (2.12).

Since $a \in \mathbb{Z}$, (2.8) gives $|a| \leq B_d - 1$; also $\gcd(d, n-d)\,\mathrm{lcm}(d, n-d)^{n-1} = B_d^{n-1} g^{2-n}$. These observations prove (2.13). Now $B_d \leq B = \lfloor n^2/4 \rfloor$. If $a \neq 0$, then $s \leq (B-1)^n < B^n$; if $a = 0$, then $s + 1 \leq B^{n-1} \leq B^n$. The latter is impossible when $B = 1$. Thus (2.14) follows in every case. □

2.1.3. *The motion of the root moduli.* The annulus bounds the excess $|\alpha| - s$ at each parameter. Its variation with s is more rigid: every root branch has a positive integral representation. Monotonicity will then reduce the required uniform gap to the single parameter $s = 1$.

Theorem 2.5. *Fix $n \geq 2$. Continue a conjugate pair of roots of $H_{n,s}$ along $s > 0$, and let $q(s)$ be their common modulus. When n is odd, $q(s)$ may instead be the modulus of the unique real root. There is a unique finite nonnegative Borel measure μ on $[0, n-1]$ such that*

$$q(s) = s + \int_0^{n-1} \frac{s}{s+t}\, d\mu(t) \qquad (s > 0). \tag{2.15}$$

The measure is absolutely continuous. In particular, $q(s) - s$ is nondecreasing.

Appendix A proves the representation by continuation across the singular fibers and Cauchy's formula. Proposition A.2 identifies the exact support of the measure for each branch. In the standard terminology, q and $q - s$ are complete Bernstein functions. Related representations for scaled ultraspherical zeros are established in [9, Theorem 1.4].

The expansion at infinity identifies the mass of the measure. We fix the Hermite normalization used throughout the paper:

$$h_m(T) = m![u^m]e^{Tu+u^2/2} = i^{-m}\,\mathrm{He}_m(iT), \tag{2.16}$$

where He_m is the probabilists' Hermite polynomial. The centered generating function gives the scaled polynomial

$$F_n(T, v) := v^n C_{n,v^{-2}}(T/v) = n![u^n] \exp\left(Tu + \sum_{m\geq 2} \frac{v^{m-2}u^m}{m} \right). \tag{2.17}$$

The right side extends polynomially to $v = 0$, with $F_n(T, 0) = h_n(T)$. The zeros of h_n are simple and purely imaginary. Indeed, Rodrigues' formula $\mathrm{He}_n(x) = (-1)^n e^{x^2/2}(d/dx)^n e^{-x^2/2}$ and integration by parts give orthogonality for the positive Gaussian weight. Multiplication by the product of the sign-changing factors then shows that He_n has n distinct real zeros. The scaled polynomial therefore has a separate holomorphic root germ at each limiting zero.

Corollary 2.6. *Let q and μ be as in Theorem 2.5. Let $\xi \geq 0$ be the absolute value of the zero of the probabilists' Hermite polynomial He_n corresponding to this root branch. For a conjugate pair, choose the root in the upper half-plane; then the scaling is*

$$\alpha(s) = -s + i\xi\sqrt{s} + O(1) \qquad (s \longrightarrow +\infty).$$

For the real root in odd degree, take $\xi = 0$. Then

$$\mu([0, n-1]) = \lim_{s\to\infty}(q(s) - s) = \frac{n-1}{3} + \frac{\xi^2}{6}. \tag{2.18}$$

In particular, for every integer $r \geq 1$ and every $s > 0$,

$$(-1)^{r-1}\frac{d^r}{ds^r}(q(s) - s) = r! \int_0^{n-1} \frac{t}{(s+t)^{r+1}}\, d\mu(t) > 0. \tag{2.19}$$

Thus $q'(s) > 1$, $q''(s) < 0$, and the root-modulus excess is strictly increasing and strictly concave.

Proof. The polynomials in (2.16) satisfy $h_j' = jh_{j-1}$ and $h_j = Th_{j-1} + (j-1)h_{j-2}$. For $n \geq 3$, (2.17) gives

$$F_n(w, z) = h_n(w) + \frac{n(n-1)(n-2)}{3} z h_{n-3}(w) + O(z^2).$$

Let $w_0 = i\xi$ and let $w(z) = w_0 + bz + O(z^2)$ be the corresponding root germ. Since $h_n(w_0) = 0$ and $h_n'(w_0) \neq 0$, implicit differentiation gives

$$b = -\frac{(n-1)(n-2)}{3}\frac{h_{n-3}(w_0)}{h_{n-1}(w_0)}.$$

The recurrence, applied twice, yields

$$(n-1)(n-2)h_{n-3}(w_0) = (n-1+w_0^2)h_{n-1}(w_0).$$

Consequently

$$b = -\frac{n-1+w_0^2}{3} = \frac{\xi^2 - n + 1}{3}.$$

For $n = 2$, one has $F_n(w,z) = w^2 + 1$ and $\xi^2 = 1$, so the same formula holds with $b = 0$. Substituting $z = s^{-1/2}$ gives

$$\alpha(s) = -s + i\xi\sqrt{s} + \frac{\xi^2 - n + 1}{3} + O(s^{-1/2}).$$

Taking absolute values shows that

$$q(s) - s \longrightarrow -\frac{\xi^2 - n + 1}{3} + \frac{\xi^2}{2} = \frac{n-1}{3} + \frac{\xi^2}{6}.$$

This also applies to $\xi = 0$, when $q = -\alpha$. Dominated convergence in (2.15) identifies this limit with the mass of μ, proving (2.18).

Differentiation under the integral is valid on every compact subinterval of $(0,\infty)$ and gives (2.19). Its right-hand side is strictly positive: the mass in (2.18) is positive, and absolute continuity excludes an atom at 0. □

The quadratic example. For $n = 2$ the roots are $-s \pm i\sqrt{s}$, so $q(s) = \sqrt{s(s+1)}$. The representing measure is

$$d\mu(t) = \frac{1}{\pi}\sqrt{\frac{1-t}{t}}\,\mathbf{1}_{(0,1)}(t)\,dt.$$

Its mass is $1/2$, in agreement with (2.18). This example exhibits both the full support and the strict derivative signs directly.

Proposition 2.7. *Let $n \geq 2$. For every $s > 0$, distinct roots of $H_{n,s}$ cannot lie on the same nonreal ray. Label the roots in the upper half-plane, together with the real root in odd degree, by*

$$\alpha_j(s) \sim ((n-1)!s)^{1/n} e^{(2j+1)\pi i/n}, \qquad 0 \leq j \leq \lfloor (n-1)/2 \rfloor, \qquad s \downarrow 0.$$

Then the corresponding Hermite zeros in $\alpha_j(s) = -s + i\xi_j\sqrt{s} + O(1)$ satisfy

$$\xi_j > \xi_{j+1} \quad (0 \leq j < \lfloor (n-1)/2 \rfloor), \qquad \xi_{\lfloor (n-1)/2 \rfloor} \geq 0.$$

Thus the exact support endpoint $n-1-j$ in Proposition A.2 corresponds to the jth nonnegative Hermite zero in decreasing order, starting with $j = 0$.

Proof. Put $A = n + s - 1$ and $\kappa = n - A/2$. On a ray $X = \rho e^{i\theta}$, the substitution $H(X) = e^{e^{i\theta}\rho/2}\rho^{A/2}u(\rho)$ in (2.5) gives

$$u'' + \left(-\frac{e^{2i\theta}}{4} + \frac{\kappa e^{i\theta}}{\rho} - \frac{A(A+2)}{4\rho^2}\right)u = 0. \tag{2.20}$$

Suppose two roots lie at radii $\rho_1 < \rho_2$ on a nonreal ray. Proposition 2.2 gives $\rho\cos\theta < n - 1 - s = 2\kappa - 2$ at both endpoints and hence on the whole radial segment. Multiply the equation by $\overline{u}$, integrate, and take imaginary parts. The endpoint terms vanish, so

$$0 = \sin\theta \int_{\rho_1}^{\rho_2} \left(\frac{\kappa}{\rho} - \frac{\cos\theta}{2}\right)|u|^2\,d\rho,$$

although the parenthesized factor is greater than $1/\rho$. This proves separation. A nonreal branch cannot cross the real axis without meeting its conjugate, contrary to simplicity. Its initial angular order is therefore preserved for all $s > 0$. The expansion $\arg \alpha_j(s) = \pi - \xi_j/\sqrt{s} + O(s^{-1})$ then orders the Hermite limits in the opposite direction. These limits are distinct by the simple-root perturbation of (2.17), proving the strict inequalities. □

The arithmetic applications require a lower bound uniform in s. Monotonicity reduces this estimate to the exponential Taylor polynomial at $s = 1$.

Corollary 2.8. *Let $\rho_0 > 0$ be the unique solution of $\log \rho_0 + \rho_0 = -1$. For $n \geq 2$, real $s \geq 1$, and every root α of $H_{n,s}$,*

$$|\alpha| - s + 1 > \rho_0(n+1) > \frac{n+1}{4}. \tag{2.21}$$

Proof. At $s = 1$ one has $H_{n,1}(X) = n! \sum_{j=0}^{n} X^j/j!$. Taylor's integral remainder at a root α gives

$$e^{\alpha} = \frac{\alpha^{n+1}}{n!} \int_0^1 e^{t\alpha}(1-t)^n \, dt.$$

Dividing by e^{α} and taking absolute values, with $R = |\alpha|$ and $N = n + 1$, yields

$$1 \leq \frac{R^{n+1}}{n!} \int_0^1 e^{-(1-t)\Re\alpha}(1-t)^n \, dt \leq \frac{R^N e^R}{N!}.$$

Since $\log(N!) > N \log N - N$, this implies $\log(R/N) + R/N > -1$. The function $u \mapsto \log u + u$ is strictly increasing from $-\infty$ to $+\infty$, so $R > \rho_0 N$. Moreover $\log 4 > 5/4$, since $e < 3$ and $3^5 < 4^4$; hence $\rho_0 > 1/4$.

Continue the root or its conjugate pair from parameter 1 to s. Theorem 2.5 gives $q(s) - s + 1 \geq q(1) > \rho_0(n+1)$. The weaker constant $1/4$ will suffice in the quantitative arguments. □

2.2. **Finite fibers and large-parameter irreducibility.** A monic rational factor of a monic integral polynomial has an integral root sum. At a fiber where all but a bounded number of roots vanish, reduction modulo a prime restricts this sum to a subset sum of the residual roots. If the corresponding trace relation is nonzero, its size bounds the prime divisors of the parameter difference. Two such relations give a height bound by linear forms in logarithms. We formulate this argument first, then apply it to Laguerre polynomials. The Appell application is given in Section 6.1.

The arithmetic input comes from linear forms in logarithms. We record the exact estimate before deriving the bound used here.

2.2.1. *Linear forms in logarithms.* We use the following rational specialization of Matveev's theorem [38, Corollary 2.3, p. 1219]. The number of logarithms is allowed to vary; its dependence in the estimate will be needed when the prime support grows with the degree.

Lemma 2.9. *Let $a_1, \ldots, a_t$ be positive rational numbers different from 1, and let $b_1, \ldots, b_t$ be integers. Suppose that*

$$\Lambda = b_1 \log a_1 + \cdots + b_t \log a_t \neq 0.$$

Put $B = \max\{1, |b_1|, \ldots, |b_t|\}$, and choose

$$A_j \geq \max\{h(a_j), |\log a_j|, 0.16\} \qquad (1 \leq j \leq t).$$

Here $h(M/N) = \log \max\{M, N\}$ for coprime positive integers M, N. Then

$$\log|\Lambda| > -C_t A_1 \cdots A_t \log(eB), \qquad C_t = \min\left\{\frac{e}{2}\, 30^{t+3} t^{9/2},\, 2^{6t+20}\right\}. \tag{2.22}$$

Proof. For $t \geq 2$, reorder the terms so that $A_t = \max_j A_j$. The coefficient parameter in [38, (1.3)] then satisfies

$$B_{\mathrm{M}} = \max\{1, \max_j |b_j| A_j/A_t\} \leq B.$$

Corollary 2.3 of [38, p. 1219], with $D = \kappa = 1$, gives (2.22). The corollary allows dependent logarithms. For $t = 1$, write $a_1 = M/N$ in lowest terms. Since $M \neq N$, integration of $1/x$ between these positive integers gives $|\log a_1| > e^{-h(a_1)}$; this implies the displayed bound. □

2.2.2. *Nearby integers with bounded prime support.*

Lemma 2.10. *Let M, h be positive integers, and suppose*

$$R \geq e^4, \qquad \log \mathrm{rad}(M(M+h)) \leq R.$$

Put

$$T = \frac{2R}{\log R}, \qquad C_R = \frac{e}{2}\, 30^3 T^{9/2} (15 \log R)^T.$$

Then

$$\log M < \max\{2\log(2h),\ 4C_R \log(12eC_R)\}. \tag{2.23}$$

Proof. The assertion is immediate if $M = 1$ or $M \leq h$. Otherwise put $L = \log M$ and $H = \log h$. Factoring $(M+h)/M$ gives a nonzero linear form

$$0 < \Lambda = \log \frac{M+h}{M} = \sum_{\ell=1}^{t} b_\ell \log p_\ell < \frac{h}{M}, \qquad \sum_{\ell=1}^{t} \log p_\ell \leq R,$$

where the p_ℓ are distinct primes and all $b_\ell \neq 0$. Since the ℓth prime is at least $\ell + 1$,

$$R \geq \log((t+1)!) \geq t \log t - t.$$

We claim that $t \leq T$. Writing $w = \log R \geq 4$, one has

$$T(\log T - 1) - R = \frac{R}{w}(w - 2\log w + 2\log 2 - 2) > 0.$$

The expression in parentheses is positive at $w = 4$ and increasing thereafter. Monotonicity of $z(\log z - 1)$ for $z > 1$ proves the claim.

Use the first constant in Lemma 2.9, the rational case of [38, Corollary 2.3, p. 1219]:

$$\log|\Lambda| > -\frac{e}{2}\, 30^{t+3} t^{9/2} \left(\prod_{\ell=1}^{t} \log p_\ell\right) \log(eB), \qquad B = \max_\ell |b_\ell|.$$

By the arithmetic–geometric mean inequality and $t \leq T$,

$$\frac{e}{2}\, 30^{t+3} t^{9/2} \prod \log p_\ell \leq \frac{e}{2}\, 30^3 t^{9/2} (30R/t)^t \leq C_R.$$

The last inequality uses the increase of $z \log(30R/z)$ on $0 < z \leq T$; indeed $T \leq R/2$. Also, since $M \geq 2$ and $h < M$,

$$B \leq \frac{\log(M+h)}{\log 2} < 3L.$$

Consequently

$$L - H < C_R \log(3eL).$$

If $L \leq 2H$, the claimed bound follows. Otherwise $L < 2C_R \log(3eL)$. For $a, b \geq 1$ and $y > 0$, the inequality $y < a\log(by)$ implies $y < 2a\log(2ab)$ whenever $2ab \geq e$: at $y_0 = 2a\log(2ab)$ one has $a\log(by_0) \leq y_0$, and $y - a\log(by)$ increases for $y \geq y_0$. Apply this with $a = 2C_R$, $b = 3e$. It gives $L < 4C_R \log(12eC_R)$, as required. □

2.2.3. *The finite-fiber criterion.* If $R \in \mathbb{Z}[X]$ is monic of degree r, with roots $\rho_1, \dots, \rho_r$ counted with multiplicity, define its *subset-trace polynomial* by

$$\mathcal{T}_R(Z) = \prod_{J \subseteq \{1,\dots,r\}} \left(Z - \sum_{j \in J} \rho_j \right).$$

It is monic of degree 2^r and belongs to $\mathbb{Z}[Z]$: its coefficients are algebraic integers and symmetric functions of the roots. The empty subset contributes the factor Z.

Proposition 2.11. *Let $P(T,X) \in \mathbb{Z}[T,X]$ be monic of degree n in X, and let $c(T) \in \mathbb{Z}[T]$. Suppose that, at distinct integers $t_1, \dots, t_q$,*

$$P(t_i, X) = X^{n-r_i} R_i(X), \qquad 0 \le r_i \le n, \qquad R_i \in \mathbb{Z}[X] \text{ monic of degree } r_i.$$

Let $t \in \mathbb{Z} \setminus \{t_1, \dots, t_q\}$, and let a monic integral factor of $P(t,X)$ have degree d, root sum τ, and centered trace $A = \tau - dc(t)$. Then

$$\operatorname{rad}(|t - t_i|) \mid \mathcal{T}_{R_i}(A + dc(t_i)). \tag{2.24}$$

Whenever two of the integers on the right are nonzero, the radical of the product of the corresponding two parameter differences divides the absolute value of their product.

Proof. For a prime $p \mid t - t_i$, reduction modulo p takes the given factor to a monic divisor of $X^{n-r_i} R_i(X)$. Its roots, counted with multiplicity, select a submultiset of the roots of R_i together with some zero roots. Its trace is therefore a root of $\mathcal{T}_{R_i}$ modulo p. This trace is congruent to $A + dc(t_i)$, proving the divisibility prime by prime. Reduction of the symmetric definition of $\mathcal{T}_{R_i}$ is valid even when roots coalesce modulo p. □

The next theorem reduces large-parameter irreducibility to a strip bound and a condition on the subset traces of finitely many fibers.

Theorem 2.12. *Fix an integer $n_0 \ge 2$. For each integer $n \ge n_0$, let $P_n(T,X) \in \mathbb{Z}[T,X]$ be monic of degree n in X, and let $c_n(T) \in \mathbb{Z}[T]$. Suppose that there are fixed constants $C \ge 1$, $\kappa \ge 1$, and integers $q \ge 3$, $r_0 \ge 0$, with the following properties.*

(1) For every positive integer t and every complex root α of $P_n(t,X)$,

$$|\operatorname{Re}(\alpha - c_n(t))| \le C n^{\kappa}.$$

(2) There are distinct integers $t_{n,1}, \dots, t_{n,q}$ satisfying

$$|t_{n,i}| + |c_n(t_{n,i})| \le C n^{\kappa}$$

and specializations

$$P_n(t_{n,i}, X) = X^{n-r_{n,i}} R_{n,i}(X), \qquad 0 \le r_{n,i} \le \min\{n, r_0\},$$

where $R_{n,i}$ is monic of degree $r_{n,i}$ and every coefficient has absolute value at most Cn^{κ}.

(3) Put $U_{n,i} = \mathcal{T}_{R_{n,i}}$. For every integer $1 \le d \le n/2$ and every $A \in \mathbb{Z}$, at least two of

$$U_{n,i}(A + dc_n(t_{n,i})), \qquad 1 \le i \le q,$$

are nonzero.

Then, for every $\varepsilon > 0$, there is an effective $N = N(C, \kappa, q, r_0, \varepsilon, n_0)$ such that $P_n(t,X)$ is irreducible over $\mathbb{Q}$ whenever

$$n \ge N, \qquad t \in \mathbb{Z}_{>0}, \qquad \log t \ge n^{\varepsilon}.$$

The last condition says equivalently that, after omitting any one index j, the remaining shifted trace polynomials have no common integer root. A sufficient algebraic condition is

$$\gcd_{\mathbb{Q}[Z]}\{U_{n,i}(Z + dc_n(t_{n,i})) : i \neq j\} = 1 \quad \text{for every } d, j \text{ as above.} \tag{2.25}$$

The distinction is useful: the theorem only needs exclusion of integer roots, whereas a resultant can verify the stronger condition.

Proof. Suppose a monic factor has degree $1 \le d \le n/2$, and let τ be its root sum. Gauss's lemma gives $\tau \in \mathbb{Z}$, so the centered trace $A = \tau - dc_n(t)$ is integral. Because it is real, the first hypothesis bounds it by

$$|A| \le dCn^{\kappa} \le Cn^{\kappa+1}.$$

By the third hypothesis, at least two of the integers

$$U_{n,i}(A + dc_n(t_{n,i}))$$

are nonzero.

There are constants C_1, K_1, depending only on C, κ, r_0, such that the absolute value of every nonzero displayed integer is at most $C_1 n^{K_1}$. To see this directly, every root of $R_{n,i}$ has absolute value at most $1 + Cn^{\kappa}$ by Cauchy's bound. Every subset sum has absolute value at most $r_0(1 + Cn^{\kappa})$, and there are at most 2^{r_0} factors in $U_{n,i}$. Also

$$|A + dc_n(t_{n,i})| \le 2Cn^{\kappa+1}.$$

These estimates give, for example, a uniform bound

$$|U_{n,i}(A + dc_n(t_{n,i}))| \le \big(2C + r_0(1 + C)\big)^{2^{r_0}} n^{(\kappa+1)2^{r_0}}.$$

Choose indices $i \neq j$ with nonzero evaluations. For all large n, the inequality $\log t \ge n^{\varepsilon}$ gives $t > 2Cn^{\kappa}$. Therefore the two integers $t - t_{n,i}$ and $t - t_{n,j}$ are positive. Proposition 2.11 gives

$$\log \operatorname{rad}\big((t - t_{n,i})(t - t_{n,j})\big) \le 2 \log C_1 + 2K_1 \log n.$$

Their difference h lies between 1 and $2Cn^{\kappa}$, while their smaller member M satisfies $M \ge t/2$. Apply Lemma 2.10 with $R = \max\{e^4, 2 \log C_1 + 2K_1 \log n\}$. Its explicit bound gives

$$\log M \le \exp\left(O\left(\frac{\log n \, \log\log\log n}{\log\log n}\right)\right),$$

for all sufficiently large n, with effective constants depending only on the stated data. The bound is $n^{o(1)}$. In particular, $\log M < n^{\varepsilon/2}$ for all sufficiently large n. But $M \ge t/2$ gives $\log M \ge n^{\varepsilon} - \log 2 > n^{\varepsilon/2}$, a contradiction. □

Corollary 2.13. *Under the hypotheses of Theorem 2.12, suppose that, for some fixed $\delta > 0$, $P_n(t, X)$ is irreducible for every integer $1 \le t \le \exp(n^{\delta})$ once n is sufficiently large. Then $P_n(t, X)$ is irreducible for every positive integer t once n is sufficiently large.*

Proof. Apply the theorem with $\varepsilon = \delta$ to cover the complementary range. □

Scope. The geometric hypothesis is stronger than necessary: a uniform bound for the centered trace of every rational factor suffices. Likewise, one may replace $U_{n,i}$ by any integral polynomial annihilating the relevant subset traces, and may remove repeated prime factors after evaluation. The four-fiber Laguerre argument uses both refinements, giving the much smaller exponent 6 in its prime-support bound.

The same proof also permits fibers of the form

$$P_n(t_{n,i}, X) = (X - b_{n,i})^{n - r_{n,i}} R_{n,i}(X - b_{n,i}), \qquad b_{n,i} \in \mathbb{Z}.$$

One adds the bound $|b_{n,i}| \le Cn^{\kappa}$ to the hypotheses and replaces $c_n(t_{n,i})$ in every trace evaluation by $c_n(t_{n,i}) - b_{n,i}$. A degree-d factor then has trace $db_{n,i}$ plus a subset sum of the residual roots after specialization. All height and prime-support estimates are unchanged apart from their constants.

The trace condition excludes persistent factors that the other hypotheses do not detect. For example, the Appell family $n![z^n]e^{Xz}(1-z^2)^{-t}$ has a factor X for every odd n, because its coefficients have fixed parity. Its negative-integer fibers have bounded residual degree. The convolution argument in Section 6.1, applied to $H_{n,t}(X)$ and $(-1)^n H_{n,t}(-X)$, places every root in $|\operatorname{Re} X| \le 2(n-1)$, independently of t. All the trace polynomials nevertheless vanish at the trace of the factor X.

Corollary 2.14. *Assume the hypotheses of Theorem 2.12, with its strip bound valid for every real parameter $t > 0$. Suppose also that $c_n(T)$ has degree at most one and that*

$$\deg_T([X^{n-k}]P_n(T,X)) \le k \qquad (0 \le k \le n).$$

For every fixed $B \ge 0$ and $\varepsilon > 0$, there is an effective $N = N(C,\kappa,q,r_0,n_0,B,\varepsilon)$ such that $P_n(a/b,X)$ is irreducible over $\mathbb{Q}$ whenever

$$n \ge N, \qquad a,b \in \mathbb{Z}_{>0}, \qquad (a,b) = 1, \qquad b \le n^B, \qquad \log a \ge n^{\varepsilon}.$$

Proof. The coefficient-degree assumption makes

$$F(X) = b^n P_n(a/b, X/b)$$

monic and integral. If it has a monic integral factor of degree $1 \le d \le n/2$ and trace τ, put $A = \tau - dbc_n(a/b)$. The affine condition gives $A \in \mathbb{Z}$, and the real-parameter strip bound gives $|A/b| \le Cn^{\kappa+1}$. Write $e_i = \deg U_{n,i} \le 2^{r_0}$. If $p \mid a - bt_{n,i}$, then $p \nmid b$, and reduction to the fiber $t_{n,i}$ gives

$$p \mid b^{e_i} U_{n,i}(A/b + dc_n(t_{n,i})).$$

These evaluations are integers. At least two are nonzero: otherwise A/b would be a common rational root of all but one of the shifted trace polynomials. Each of those polynomials is monic and integral, so this rational root would be an integer, contrary to the trace condition.

For all sufficiently large n, the hypotheses give $a > 2Cbn^{\kappa}$, so every $a - bt_{n,i}$ is positive and at least $a/2$. The coefficient and trace estimates in the proof of Theorem 2.12 bound each nonzero evaluation by $b^{2^{r_0}} C_1 n^{K_1}$, with the same effective constants C_1, K_1. For two nonzero evaluations, the corresponding positive integers $a - bt_{n,i}$ and $a - bt_{n,j}$ therefore satisfy

$$\log \operatorname{rad}((a - bt_{n,i})(a - bt_{n,j})) \le 2\log C_1 + 2K_1 \log n + 2^{r_0+1} \log b.$$

Their positive difference is at most $2Cbn^{\kappa}$. Since $b \le n^B$, the radical bound is $O_B(\log n)$ and the logarithm of the difference is $O_B(\log n)$. Lemma 2.10 gives $\log a = n^{o_B(1)}$, effectively and uniformly in b, contradicting $\log a \ge n^{\varepsilon}$. The rational change of variable defining F preserves irreducibility. □

2.2.4. *Four degenerate Laguerre fibers.* For relatively prime positive integers a, b, put

$$F_{n,a,b}(X) = b^n H_{n,a/b}(X/b) = \sum_{k=0}^{n} \binom{n}{k} \left(\prod_{j=0}^{k-1} (a + jb) \right) X^{n-k}.$$

This polynomial is monic and integral. Its irreducibility over $\mathbb{Q}$ is equivalent to that of $H_{n,a/b}$.

Theorem 2.15. *Let $n \ge 2$, and let a, b be relatively prime positive integers. If $F_{n,a,b}$ is reducible over $\mathbb{Q}$, then there are $0 \le i < j \le 3$ such that*

$$\operatorname{rad}((a + ib)(a + jb)) < b^3 n^6.$$

Proof. For $n = 2$, the polynomial $H_{2,a/b}$ has discriminant $-4a/b < 0$, so it is irreducible and there is nothing to prove. Assume $n \geq 3$. Choose a monic integral factor of degree $1 \leq d \leq n/2$, with roots $\beta_1, \ldots, \beta_d$. Its centered trace

$$A = \sum_{\nu=1}^{d} (\beta_\nu + a)$$

is an integer. Since β_ν/b are roots of $H_{n,a/b}$, the real-parameter trace estimate in Proposition 2.2 gives

$$|A| < bd(n-d). \tag{2.26}$$

At parameters $s = 0, -1, -2, -3$, the nonzero parts of $H_{n,s}$ are

$$1, \qquad X - n, \qquad X^2 - 2nX + n(n-1), \qquad R(X),$$

where

$$R(X) = (X-n)^3 - 3n(X-n) - 2n.$$

Polynomials annihilating all subset sums of the nonzero roots are

$$\begin{aligned} T_0(Z) &= Z, \\ T_1(Z) &= Z(Z-n), \\ T_2(Z) &= Z(Z-2n)((Z-n)^2 - n), \\ T_3(Z) &= -Z(Z-3n)R(Z)R(3n-Z). \end{aligned}$$

For the last identity, the subset sums are 0, $3n$, the three roots of R, and their complements in $3n$.

If $p \mid a + ib$, then $p \nmid b$, because $\gcd(a, b) = 1$. The chosen factor reduces to a monic divisor of the fiber at $a = -ib$. Its uncentered trace is congruent to $A + ibd$ modulo p. Consequently

$$p \mid b^{\deg T_i} T_i(A/b + id). \tag{2.27}$$

The quantity on the right is an integer. The assertion remains valid in every characteristic, since roots are counted with multiplicity. Whenever A/b is integral, powers of b can be discarded from this divisibility.

First suppose $A \notin \{0, -bd, b(n-d)\}$. Taking $(i, j) = (0, 1)$ in (2.27) shows that the required radical divides the nonzero integer

$$N = A(A + bd)(A + bd - bn).$$

By (2.26),

$$|A| < bdn, \qquad |A + bd| < bdn, \qquad |A + bd - bn| < b(d+1)n,$$

and hence $|N| < b^3 n^3 d^2 (d+1) < b^3 n^6$.

For the three exceptional trace values, the following integers contain the required prime supports whenever they are nonzero:

A	(i, j)	N
$-bd$	$(0, 2)$	$d(d-2n)((d-n)^2 - n)$
0	$(1, 2)$	$2d(d-n)((2d-n)^2 - n)$
$b(n-d)$	$(0, 2)$	$(n-d)(n+d)(d^2 - n)$.

(2.28)

This follows by substitution in T_0, T_1, T_2; replacing repeated factors by one copy preserves their prime support. Every nonzero entry has absolute value less than n^4. The first entry can vanish only when $(n, d) = (4, 2)$: writing $n = m^2$ and $n - d = m$ gives $m^2 - m \leq m^2/2$, hence $m \leq 2$. At this exceptional trace $A = -2b$, use fibers 0 and 3. Their evaluations are $T_0(-2) = -2$ and $T_3(4) = -2048$, so all relevant primes divide 2. The required bound follows.

The other two entries leave only the following cases:

$$n = m^2, \quad (A, d) = \left(0, \frac{m^2 - m}{2}\right), \qquad \text{or} \qquad n = m^2, \quad (A, d) = (b(m^2 - m), m).$$

Here $m \geq 2$.

In the first case use fibers 1 and 3. Writing $d = m(m-1)/2$, direct substitution gives

$$T_1(d) = -\frac{m^2(m^2-1)}{4}$$

and

$$T_3(3d) = \frac{9m^6(m^2-1)^3(m^2-9m+16)(m^2+9m+16)}{256}.$$

Every prime divisor of either integer divides

$$N = 3m(m^2-1)(m^2-9m+16)(m^2+9m+16).$$

Neither quadratic factor vanishes at an integer: the first has discriminant 17, and the second is positive. For $m \geq 3$,

$$|m^4 - 49m^2 + 256| \leq m^4 + 49m^2 + 256 < 10m^4,$$

so $0 < |N| < 30m^7 < m^{12} = n^6$. For $m = 2$, the same integer has absolute value $1368 < 4096 = m^{12}$.

In the second case use fibers 0 and 3. Put

$$J(m) = m(m-1)(m-4) + 2.$$

Then

$$T_3(n + 2m) = 4m^6(m-1)^3(m+2)J(m).$$

The prime supports of $n - m = m(m-1)$ and this value are contained in that of

$$N = 2m(m-1)(m+2)J(m).$$

Here $J(2) = -2$ and $J(3) = -4$, while $0 < J(m) < m^3$ for $m \geq 4$. Thus $0 < |J(m)| < m^3$ for every $m \geq 2$, and $0 < |N| < 4m^6 < m^{12} = n^6$. Powers of b introduce no relevant primes. This completes the proof. □

Corollary 2.16. *For every fixed $B \geq 0$ and $\varepsilon > 0$, there is an effective integer $N(B, \varepsilon)$ such that $F_{n,a,b}$ is irreducible over $\mathbb{Q}$ whenever*

$$n \geq N(B, \varepsilon), \qquad \gcd(a, b) = 1, \qquad 1 \leq b \leq n^B, \qquad \log a \geq n^{\varepsilon}.$$

More explicitly, a reducible member with $n \geq 2$ satisfies

$$\log a < \max\{2\log(6b),\ 4C_R \log(12eC_R)\}, \qquad R = \max\{e^4,\ 3\log b + 6\log n\},$$

where C_R is defined in Lemma 2.10.

Proof. Theorem 2.15 supplies $M = a + ib \geq a$ and $h = (j-i)b \leq 3b$ to which Lemma 2.10 applies. This proves the explicit estimate. For $b \leq n^B$, write $u = \log n$. Then $R = O_B(u)$ and

$$\log C_R = \log((e/2)30^3) + \frac{9}{2}\log\frac{2R}{\log R} + \frac{2R\log(15\log R)}{\log R} = o_B(u).$$

It follows that $4C_R \log(12eC_R) = \exp(o_B(u)) = n^{o_B(1)}$, whereas $2\log(6b) = O_B(u)$. Both are eventually smaller than n^{ε}. All quantities in the explicit bound are elementary and effectively computable, so the threshold is effective. □

Positive rational parameters can give reducible polynomials. For example,

$$H_{3,1/4}(X) = \left(X + \frac{3}{4}\right)\left(X^2 + \frac{15}{16}\right), \qquad F_{3,1,4}(X) = (X+3)(X^2+15).$$

Thus the numerator and denominator conditions in the rational theorem have genuine content; positivity alone is not sufficient.

3. Uniform irreducibility

3.1. **Local arithmetic and energy.** A rational factor selects a Galois-invariant set of roots; a block system gives an invariant partition. Both restrict how roots can occupy a local cluster. We express these restrictions by positive semidefinite matrices and compare the resulting local contributions with a bound from complex root separation. The same inequality will therefore exclude factors and block systems.

We first determine the tame clusters of $H_{n,s}$ and prove the separation estimates needed at all places. The energy theorem is then stated for a general monic integral polynomial. Its applications depend on finding clusters with enough imbalance; the differential equation alone supplies only the separation bounds.

3.1.1. *Tame root clusters and inertia.* The local calculation rests on the following form of Hensel's lemma. No irreducibility assumption is needed.

Lemma 3.1. *Let $F \in \mathbb{Z}_p[X]$ be monic, and suppose $\overline{F} = X^N\overline{R}$ with $1 \le N \le \deg F$, $\overline{R}$ squarefree, and $\overline{R}(0) \neq 0$. Let A be the degree-N Hensel factor lifting X^N. Suppose $p \nmid N$ and, for an integer $e > 0$, every nonleading coefficient of A has valuation at least e, with $v_p(A(0)) = e$. Put $g = \gcd(N, e)$ and $q = N/g$. Then every root of A has valuation e/N, as does every difference between two distinct roots of A. All other roots are units, and every difference of distinct roots involving one of those roots has valuation zero. The inertia group of the splitting field over $\mathbb{Q}_p$ is cyclic of order q, with a generator of cycle type $q^g 1^{\deg F - N}$.*

Proof. Write $N = gq$ and $e = ga$, where $\gcd(a, q) = 1$. Choose a finite unramified extension $K_0/\mathbb{Q}_p$ whose residue field splits $\overline{R}$ and $Y^N + c$, where c is the reduction of $p^{-e}A(0)$, and which contains the qth roots of unity. This is possible since $p \nmid q$. If $\pi^q = p$, then $p^{-e}A(\pi^a Y)$ is integral and reduces to $Y^N + c$. That polynomial is separable because $p \nmid N$, so its roots lift to units of $K_0(\pi)$ with distinct residues. Rescaling gives the asserted valuations of the roots of A and their differences. The complementary Hensel factor splits over K_0, with distinct nonzero residues.

The splitting field is therefore contained in the tame extension $K_0(\pi)$, whose ramification index is q. Conversely, the valuation a/q of every root of A forces its root field to have ramification index divisible by q. Thus the splitting field and every such root field have ramification index exactly q. Tame inertia is cyclic, and its orbit on a root has size equal to the ramification index of that root field. Its generator consequently has g cycles of length q, while the complementary roots are fixed. □

For the Laguerre family, a prime above the degree can divide only one of the consecutive parameter nodes $s, \dots, s + n - 1$. The preceding lemma then determines the full inertia action.

Proposition 3.2. *Let $n \ge 2$ and $s \ge 1$ be integers. Let $p > n$ be prime and suppose $p \mid s + j$, where $0 \le j < n$. Set*

$$e = v_p(s + j), \qquad N = n - j, \qquad g = \gcd(N, e), \qquad q = N/g.$$

In the splitting field of $H_{n,s}$, inertia at p is cyclic of order q and has a generator of cycle type $q^g 1^j$. In particular, inertia is trivial exactly when $N \mid e$.

Proof. There is at most one node divisible by p, since the nodes lie in an interval of length n. Modulo p we have

$$H_{n,s}(X) \equiv X^N R_{n,j}(X) \pmod{p}, \qquad R_{n,j}(X) = \sum_{k=0}^{j} (-1)^k \binom{n}{k} \frac{j!}{(j-k)!} X^{j-k}.$$

The constant coefficient of $R_{n,j}$ is nonzero. Also $R_{n,j} = (-1)^j j! L_j^{(N)}$ and hence

$$X R''_{n,j} + (N + 1 - X) R'_{n,j} + j R_{n,j} = 0. \tag{3.1}$$

The residual polynomial is separable. Indeed, a repeated nonzero root, followed through successive derivatives of (3.1), would make all derivatives through order j vanish there, whereas $R_{n,j}^{(j)} = j! \neq 0$ in characteristic p. The case $j = 0$ is immediate.

Hensel factorization gives $H_{n,s} = FU$ over $\mathbb{Z}_p$, with F, U monic, $\deg F = N$, $\overline{F} = X^N$, and $\overline{U} = R_{n,j}$. Every coefficient of $H_{n,s}$ below degree N has valuation exactly e. Since $U(0)$ is a unit, induction on the coefficient index in $H_{n,s} = FU$ gives

$$v_p(F(0)) = e, \qquad v_p([X^h]F) \geq e \quad (0 < h < N).$$

Lemma 3.1 now applies and gives the stated inertia group and cycle type. Its order is one exactly when $N \mid e$. □

3.1.2. *Root separation.* A *valuation packet* is the full set of roots with a specified valuation at a fixed prime. For the Laguerre family put

$$\epsilon_p = \begin{cases} 1/(p-1), & p \leq n, \\ 0, & p > n. \end{cases}$$

The differential equation bounds the distance between distinct roots at every place. The p-adic bound determines how far a cluster can persist; the complex bound supplies disjoint disks around the roots.

Lemma 3.3. *Let $n \geq 2$ and $s \geq 1$ be integers. Any two distinct roots of $H_{n,s}$ satisfy*

$$v_p(\alpha - \beta) \leq v_p(\alpha) + \epsilon_p. \tag{3.2}$$

If $s \geq n$, they also satisfy

$$|\alpha - \beta| > \frac{1}{12}\sqrt{\frac{s}{n}}. \tag{3.3}$$

Proof. The roots are simple by Section 2.1. Fix a root α and set

$$D_k = \frac{H_{n,s}^{(k)}(\alpha)}{H'_{n,s}(\alpha)}, \qquad D_0 = 0, \quad D_1 = 1.$$

Differentiating (2.5) k times gives, for $0 \leq k \leq n-2$,

$$\alpha D_{k+2} - (\alpha + n + s - 1 - k) D_{k+1} + (n - k) D_k = 0. \tag{3.4}$$

The roots are algebraic integers. If $a = v_p(\alpha) \geq 0$, induction in this recurrence gives $v_p(D_k) \geq -(k-1)a$ for $k \geq 1$. For $v_p(z) > a + \epsilon_p$, every term after the constant term in

$$\frac{H_{n,s}(\alpha + z)}{H'_{n,s}(\alpha) z} = 1 + \sum_{k=2}^{n} \frac{D_k}{k!} z^{k-1}$$

has positive valuation. Here we use $v_p(k!) \leq (k-1)/(p-1)$ when $p \leq n$, and $v_p(k!) = 0$ when $p > n$. The displayed quotient cannot vanish, proving (3.2).

For the complex estimate put $t = n/s \le 1$. The annulus (2.7) and centered-radius estimate (2.9) imply, for $0 \le k \le n-2$,

$$\left|\frac{\alpha+n+s-1-k}{\alpha}\right| \le 2t + 2\sqrt{2t} < 5\sqrt{t}, \qquad \left|\frac{n-k}{\alpha}\right| \le t.$$

With $M = 6\sqrt{t}$ we have $5\sqrt{t}\,M + t < M^2$. The recurrence therefore gives $|D_k| \le M^{k-1}$ by induction. If $0 < |z| \le 1/(2M)$, the sum after the constant term in the same Taylor quotient has absolute value at most

$$\sum_{k\ge 2} \frac{2^{1-k}}{k!} = 2e^{1/2} - 3 < 1.$$

This proves (3.3). □

3.1.3. *An adelic energy inequality.* The local positivity and the complex estimate below are elementary logarithmic-energy arguments. Galois invariance allows their comparison by the product formula, even when the matrix entries are arbitrary real numbers. The condition $Q\mathbf{1} = 0$ means zero total charge at the complex place, and positive semidefiniteness makes every local cluster contribution nonnegative. Encoding a factor or a block system in Q gives a common form of the two arithmetic obstructions. A comparison of finite-place and complex bounds for a factor resultant is also used in Deng's preprint [12, Sections 4–5].

Theorem 3.4. *Let $F \in \mathbb{Z}[X]$ be monic and separable of degree $n \ge 2$, with nonzero roots $\alpha_1, \dots, \alpha_n$. For every prime p, fix an extension of v_p to $\overline{\mathbb{Q}}$, normalized by $v_p(p) = 1$. Suppose that numbers $\epsilon_p \ge 0$, zero for all but finitely many p, satisfy*

$$v_p(\alpha_i - \alpha_j) \le v_p(\alpha_i) + \epsilon_p \qquad (i \ne j). \tag{3.5}$$

Let $Q = (q_{ij})$ be a real symmetric positive semidefinite matrix, invariant under the Galois action on the roots, and suppose $Q\mathbf{1} = 0$. Put $\tau = \operatorname{tr} Q$ and

$$E_p(Q) = \sum_{i\ne j} q_{ij} v_p(\alpha_i - \alpha_j) + \sum_i q_{ii}(v_p(\alpha_i) + \epsilon_p).$$

Then only finitely many $E_p(Q)$ are nonzero, and

$$E_p(Q) \ge \int_0^\infty \mathbf{1}_{C_p(t)}^{\mathsf{T}} Q \mathbf{1}_{C_p(t)}\, dt \ge 0, \qquad C_p(t) = \{i : v_p(\alpha_i) \ge t\}. \tag{3.6}$$

Furthermore,

$$\sum_p E_p(Q)\log p = \sum_{i\ne j} q_{ij} \log|\alpha_i - \alpha_j| + \sum_i q_{ii}\log|\alpha_i| + \tau \sum_p \epsilon_p \log p. \tag{3.7}$$

If the closed disks of radii $\rho_i > 0$ about the complex roots are pairwise disjoint, then

$$0 \le \sum_p E_p(Q)\log p \le \sum_i q_{ii} \log\frac{|\alpha_i|}{\rho_i} + \tau \sum_p \epsilon_p \log p. \tag{3.8}$$

In particular, if $|\alpha_i| \le R$ and $\rho_i = \rho$, the upper bound is $\tau(\log(R/\rho) + \sum_p \epsilon_p \log p)$.

If, at some prime with $\epsilon_p = 0$, a set C of $N \ge 1$ roots has valuation e/N for some $e > 0$, all differences between its distinct roots have valuation e/N, and every other root and every other difference has valuation zero, call C an exact packet *at p. Then*

$$E_p(Q) = \frac{e}{N} \mathbf{1}_C^{\mathsf{T}} Q \mathbf{1}_C. \tag{3.9}$$

The theorem can also be applied after replacing each α_i by $\alpha_i - a$, for a fixed integer a with $F(a) \ne 0$, provided (3.5) is verified for the shifted roots; the correction terms may change.

Proof. Write $h_i = v_p(\alpha_i) + \epsilon_p$. At height $t > 0$ retain the indices with $h_i \geq t$ and partition them by the equivalence relation $v_p(\alpha_i - \alpha_j) \geq t$. The ultrametric inequality makes this relation transitive. Hypothesis (3.5) ensures that every distinct pair with difference valuation at least t is retained. Consequently

$$E_p(Q) = \int_0^\infty \sum_C \mathbf{1}_C^{\mathsf{T}} Q \mathbf{1}_C \, dt.$$

Every term is nonnegative. The indices with $v_p(\alpha_i) \geq t$ form one entire retained class when this set is nonempty: their pairwise differences have valuation at least t, whereas a root of smaller valuation cannot belong to that class. This proves (3.6). Finiteness follows because, outside the supports of ϵ_p, $F(0)$, and $\operatorname{Disc} F$, all valuations in the definition are zero. The packet formula is immediate from the same definition.

To apply the product formula with real matrix entries, first group the terms by Galois orbits. The entries q_{ii} are constant on each root orbit I, and the entries q_{ij} are constant on each orbit $\mathcal{O}$ of unordered pairs of distinct roots. The orbit products

$$\prod_{i \in I} \alpha_i \quad \text{and} \quad \prod_{\{i,j\} \in \mathcal{O}} (\alpha_i - \alpha_j)^2$$

are nonzero rational numbers. Apply the product formula to each one, weight the resulting identity by the corresponding real matrix entry, and sum over the orbits. The squares in the pair products account for the two ordered terms q_{ij} and q_{ji}. Adding $\tau \sum_p \epsilon_p \log p$ gives (3.7).

Decompose $Q = \sum_\nu c_\nu c_\nu^{\mathsf{T}}$ with real vectors c_ν orthogonal to $\mathbf{1}$. For one such vector c, let σ_i be normalized arclength on the circle of radius ρ_i about α_i, and put $\eta = \sum_i c_i \sigma_i$. Its logarithmic potential is the continuous, piecewise harmonic function

$$U(z) = \sum_i c_i \log \max\{\rho_i, |z - \alpha_i|\}.$$

Because $\sum_i c_i = 0$, we have $U(z) = O(|z|^{-1})$ and $\nabla U(z) = O(|z|^{-2})$ at infinity. Integration by parts on the disks and their exterior, using $\Delta U = 2\pi\eta$, gives

$$\iint \log|z - w| \, d\eta(z) \, d\eta(w) = -\frac{1}{2\pi} \int_{\mathbb{C}} |\nabla U|^2 \, dA \leq 0.$$

The radial derivative jumps by c_i/ρ_i across the ith circle, and the outer boundary term tends to zero. The mean-value property identifies the interaction between distinct circles with $\log|\alpha_i - \alpha_j|$ and the self-interaction of the ith circle with $\log \rho_i$. Summing over ν yields

$$\sum_{i \neq j} q_{ij} \log|\alpha_i - \alpha_j| + \sum_i q_{ii} \log \rho_i \leq 0.$$

Together with (3.7), this proves (3.8). Translating by an integer preserves monicity, integrality, the differences, and the Galois action. □

Lemma 3.5. *Let $n \geq 2$, $s \geq 1$ be integers and let Q satisfy the hypotheses of Theorem 3.4 for the roots of $H_{n,s}$. Use*

$$\epsilon_p = \begin{cases} 1/(p-1), & p \leq n, \\ 0, & p > n. \end{cases}$$

Then (3.6)–(3.8) *hold. If $p > n$ and $p^e \| s + j$, $0 \leq j < n$, put $N = n - j$ and let C be the set of roots of positive p-adic valuation. Then $|C| = N$ and*

$$E_p(Q) = \frac{e}{N} \mathbf{1}_C^{\mathsf{T}} Q \mathbf{1}_C. \tag{3.10}$$

If $s \geq n$, $\log n \geq 10000$, and $Q \neq 0$, then

$$\sum_p E_p(Q) \log p < \operatorname{tr}(Q) \left(\frac{1}{2} \log s + \frac{3}{2} \log n + \log 48 \right).$$

Proof. Lemma 3.3 supplies the local-separation hypothesis. The proof of Proposition 3.2 identifies the N positive-valuation roots as the tame packet of Lemma 3.1, so (3.9) gives (3.10). Finally, use $|\alpha_i| < s + n \leq 2s$ from Lemma 2.1, the disjoint disk radius $\rho = \sqrt{s/n}/24$ from Lemma 3.3, and $\sum_{p \leq n} \log p/(p-1) < \log n$ from (3.25). □

Proposition 3.6. *In the notation of Theorem 3.4, a Galois-invariant subset A of k roots, $0 < k < n$, gives the admissible rank-one matrix $Q = cc^{\mathsf{T}}$, where*

$$c_i = \begin{cases} 1 - k/n, & i \in A, \\ -k/n, & i \notin A, \end{cases} \qquad \operatorname{tr} Q = \frac{k(n-k)}{n}.$$

For an exact packet C of size N as in (3.9), putting $m = |A \cap C|$ gives

$$E_p(Q) = \frac{e}{N} \left(m - \frac{kN}{n} \right)^2.$$

A Galois-invariant partition into $a \geq 2$ blocks $B_1, \ldots, B_a$, each of size $b \geq 2$, with $n = ab$, gives the admissible projector

$$q_{ij} = \frac{\mathbf{1}_{\{i,j \text{ in the same block}\}}}{b} - \frac{1}{n}, \qquad \operatorname{tr} Q = a - 1.$$

For an exact packet and $k_\ell = |B_\ell \cap C|$,

$$E_p(Q) = \frac{e}{N} \left(\frac{1}{b} \sum_{\ell=1}^{a} k_\ell^2 - \frac{N^2}{n} \right). \tag{3.11}$$

If an inertia element of prime order $P > a$ has support exactly C, write $N = P\ell$ and $\ell = au + r$, $0 \leq r < a$. Then

$$E_p(Q) \geq \frac{eP^2 r(a-r)}{nN}. \tag{3.12}$$

When the uniform disk and modulus bounds ρ, R hold, take such packets at distinct primes. If the sum of the displayed lower bounds, each multiplied by $\log p$, exceeds $(a-1)(\log(R/\rho) + \sum_p \epsilon_p \log p)$, then that block system is impossible. Independently, if an element of prime order $P > b$ has support C, then bP must divide $|C|$.

Proof. The rank-one formula is immediate. The block matrix is the orthogonal projector onto the vectors constant on each block and orthogonal to $\mathbf{1}$, giving positive semidefiniteness, its trace, and (3.11). An element of order $P > a$ acts trivially on the a blocks. Its nontrivial cycles have length P, so every k_ℓ is divisible by P. Among nonnegative integers with sum ℓ, the sum of squares is minimized by $a - r$ entries equal to u and r entries equal to $u + 1$. Hence

$$\sum k_\ell^2 \geq P^2 \left(\frac{\ell^2}{a} + \frac{r(a-r)}{a} \right).$$

Substitution proves (3.12); summing it and using nonnegativity at all other primes proves the energy criterion. For the final divisibility assertion, any fixed block has fewer than P elements and is therefore fixed pointwise. Every moved block lies in an orbit of P blocks and contributes all its b elements to the support. □

Corollary 3.7. *Under the hypotheses of Theorem 3.4, suppose $|\alpha_i| \le R$ and the closed disks of radius $\rho > 0$ about the roots are pairwise disjoint. Put*

$$\mathcal{B} = \log(R/\rho) + \sum_p \epsilon_p \log p.$$

Let $\mathcal{P}$ be a finite set of exact packet primes, with $\epsilon_p = 0$, packet size N_p, height e_p/N_p, and all inertia orbits in the packet of a common length q_p. For $1 \le k \le \lfloor n/2 \rfloor$, define

$$\mathcal{M}_{p,k} = \{m \in \mathbb{Z} : \max(0, k-n+N_p) \le m \le \min(k, N_p), \quad q_p \mid m\}.$$

If, for every such k, either some $\mathcal{M}_{p,k}$ is empty or

$$\sum_{p\in\mathcal{P}} \frac{e_p \log p}{nN_p k(n-k)} \min_{m\in\mathcal{M}_{p,k}} (nm - kN_p)^2 > \mathcal{B}, \tag{3.13}$$

then F is irreducible over $\mathbb{Q}$. For the tame packets of Lemma 3.1, one may take $q_p = N_p/\gcd(N_p, e_p)$.

Proof. A proper rational factor has degree $k \le n/2$ after choosing the smaller complementary factor. Its root set is a union of inertia orbits, so its packet intersection has size in $\mathcal{M}_{p,k}$. Apply the factor matrix of Proposition 3.6. Dividing its local energy by $\operatorname{tr} Q = k(n-k)/n$ gives the summand on the left of (3.13). The global upper bound is $\mathcal{B}$, a contradiction. □

3.1.4. *Differential equations as a source of energy bounds.* The proof of Lemma 3.3 applies more generally to a second-order differential equation. Its leading coefficient replaces the root in the diagonal term of the energy. Since that coefficient need only be nonzero at the roots, the polynomial itself may have a zero root.

Proposition 3.8. *Let $P \in \mathbb{Z}[X]$ be monic and separable of degree $n \ge 2$, and suppose*

$$AP'' + BP' + CP = 0, \qquad A, B \in \mathbb{Z}[X],\ C \in \mathbb{Z}, \quad \deg A \le 2, \quad \deg B \le 1, \quad \gcd(A, P) = 1.$$

Write its roots as α_i, and put $\epsilon_p = 1/(p-1)$ for $p \le n$ and $\epsilon_p = 0$ otherwise. Then

$$v_p(\alpha_i - \alpha_j) \le \min\{v_p(A(\alpha_i)), v_p(A(\alpha_j))\} + \epsilon_p \quad (i \ne j).$$

For any real symmetric Galois-invariant positive semidefinite matrix Q with $Q\mathbf{1} = 0$, define

$$E_p^A(Q) = \sum_{i\ne j} q_{ij} v_p(\alpha_i - \alpha_j) + \sum_i q_{ii}(v_p(A(\alpha_i)) + \epsilon_p).$$

These energies are nonnegative, and with $\tau = \operatorname{tr} Q$,

$$\begin{aligned}\sum_p E_p^A(Q) \log p &= \sum_{i\ne j} q_{ij} \log|\alpha_i - \alpha_j| + \sum_i q_{ii} \log|A(\alpha_i)| + \tau S(n) \\ &\le \tau\big(\log(4MR) + S(n)\big), \qquad S(n) = \sum_{p\le n} \frac{\log p}{p-1},\end{aligned}$$

where $R = \max\{1, \max_i |A(\alpha_i)|\}$, $M = \max\{1, U + \sqrt{V}\}$, and

$$U = \max_{i,\, 0\le k\le n-2} \left| \frac{kA'(\alpha_i) + B(\alpha_i)}{A(\alpha_i)} \right|,$$

$$V = \max_{i,\, 0\le k\le n-2} \left| \frac{\binom{k}{2} A''(\alpha_i) + kB'(\alpha_i) + C}{A(\alpha_i)} \right|.$$

Proof. At a root α put $D_k = P^{(k)}(\alpha)/P'(\alpha)$. Differentiating the equation k times gives

$$A(\alpha)D_{k+2} + (kA'(\alpha) + B(\alpha))D_{k+1} + \left(\binom{k}{2}A''(\alpha) + kB'(\alpha) + C\right)D_k = 0,$$

with $D_0 = 0$, $D_1 = 1$. Integrality implies $v_p(D_k) \geq -(k-1)v_p(A(\alpha))$. Since $v_p(k!) \leq (k-1)\epsilon_p$ for $2 \leq k \leq n$, the quotient

$$\frac{P(\alpha + z)}{zP'(\alpha)} = 1 + \sum_{k=2}^{n} \frac{D_k}{k!} z^{k-1}$$

cannot vanish if $v_p(z) > v_p(A(\alpha)) + \epsilon_p$. Interchanging the two roots proves the local bound.

Use the cluster-integral proof of Theorem 3.4, now with diagonal heights $h_i = v_p(A(\alpha_i)) + \epsilon_p$. Each pair height is at most both diagonal heights, so the same integral gives $E_p^A(Q) \geq 0$. For each Galois orbit of roots, the product of the corresponding $A(\alpha_i)$ is a nonzero rational number. The orbit-product argument in Theorem 3.4 therefore gives the displayed global identity. Only primes dividing $\mathrm{Disc}(P)\,\mathrm{Res}(P, A)$ or at most n can contribute.

For complex separation, $M^2 \geq UM + V$ and the recurrence imply $|D_k| \leq M^{k-1}$. If $0 < |z| \leq 1/(2M)$, the nonconstant part of the Taylor quotient has absolute value at most $\sum_{k\geq 2} 2^{1-k}/k! = 2e^{1/2} - 3 < 1$. Thus the closed disks of radius $1/(4M)$ about the roots are disjoint. The circle-energy estimate in the proof of Theorem 3.4 gives $\sum_{i\neq j} q_{ij} \log|\alpha_i - \alpha_j| \leq \tau \log(4M)$. This proves the global bound. □

For Laguerre polynomials, $A(X) = X$ recovers the earlier diagonal term. The monic probabilists' Hermite polynomials satisfy $P'' - XP' + nP = 0$, so the proposition applies with $A = 1$, including in odd degree when P has the factor X. To deduce irreducibility one must still find local clusters whose energy exceeds the global bound.

3.2. **Padé norms and the prime-square obstruction.** The root-modulus gap also has an arithmetic consequence. We use the exponential Padé pair to construct a nonzero integral resultant. Its local valuations and its complex absolute value give opposite bounds, which constrain the prime divisors of a factor's constant term. A Newton-polygon obstruction then excludes factors throughout a polynomial range of parameters. The Padé connection for this family also appears in Cullinan and Scheel [11]. For positive integers K and d, put

$$T_d(K) = \sum_{p|K} \min\left\{v_p(K), \frac{d}{p-1}\right\} \log p. \tag{3.14}$$

3.2.1. *The exponential Padé pair.*

Proposition 3.9. *Let $n \geq 3$ and $s \geq 1$ be integers. If G is a monic rational factor of $H_{n,s}$ of degree $d \geq 1$, and $K = |G(0)|$, then, with ρ_0 as in Corollary 2.8,*

$$\log(\rho_0(n+1)) < \frac{T_d(K)}{d} + \frac{\omega(K)\log s}{n+1}. \tag{3.15}$$

If $s \geq n+2$, one also has

$$\frac{\log s + \log n}{2} - 2 < \frac{T_d(K)}{d} + \frac{\omega(K)\log s}{n+1}. \tag{3.16}$$

In the latter inequality, the constant 2 can be replaced by $\log 2 + 1/2$.

Proof. Gauss's lemma gives $G \in \mathbb{Z}[X]$. Set $r = s - 1$, $P(Z) = H_{n,s}(-Z)$, and $Q(Z) = H_{r,n+1}(Z)$, with the convention $H_{0,n+1} = 1$. Coefficient extraction from $(1-t)^{j-r-1}$ gives

$$\binom{n+r-j}{n} = \sum_{a=0}^{n} (-1)^a \binom{n+r-a}{n-a}\binom{j}{a}.$$

Consequently, as formal power series,

$$e^Z \frac{P(Z)}{n!} = \sum_{j\geq 0} \binom{n+r-j}{n} \frac{Z^j}{j!} = \frac{Q(Z)}{r!} + O(Z^{n+r+1}). \tag{3.17}$$

The generalized binomial coefficients in the infinite sum are integers. Those with $r+1 \leq j \leq n+r$ vanish. If $E = e^Z P/n! - Q/r!$, then

$$PE' - (P' + P)E = -\frac{PQ' - P'Q - PQ}{r!} = O(Z^{n+r}).$$

The numerator is a polynomial of degree at most $n+r$ with leading coefficient $(-1)^{n+1}$. Thus

$$PQ' - P'Q - PQ = (-1)^{n+1} Z^{n+r}. \tag{3.18}$$

Since $P(0) \neq 0$, P and Q have no common root. Write $-M_1, \ldots, -M_d$ for the roots of G.

Fix a prime p and a root with $e = v_p(M_i) > 0$; the valuation e need not be an integer. Let $s_p(r)$ denote the sum of the base-p digits of r. We claim that

$$v_p Q(M_i) \geq (n+s)e - (n+1)\min\{e, (p-1)^{-1}\} - \frac{s_p(r)}{p-1}. \tag{3.19}$$

If $e > 1/(p-1)$, the series in (3.17) converge at M_i. Because $P(M_i) = 0$, $Q(M_i)/r!$ is the negative of the tail beginning at $j = n+s$. Legendre's formula gives, for $j \geq 1$,

$$je - v_p(j!) \geq j\left(e - \frac{1}{p-1}\right) + \frac{1}{p-1}.$$

It follows that

$$v_p Q(M_i) \geq (n+s)e - \frac{n + s_p(r)}{p-1},$$

which is stronger than (3.19). If $0 < e \leq 1/(p-1)$, use the finite polynomial identity

$$Q(M_i) = r! \sum_{j=0}^{r} \binom{n+r-j}{n} \frac{M_i^j}{j!}.$$

For $0 \leq j \leq r$, $je - v_p(j!) \geq r(e - 1/(p-1))$. Hence $v_p Q(M_i) \geq re - s_p(r)/(p-1)$, which is exactly the required bound. This argument includes $r = 0$ and the convergence boundary.

We shall use the elementary digit estimate

$$p^{s_p(r)/(p-1)} \leq r + 1 = s. \tag{3.20}$$

Indeed, concavity of $\log(a+1)$ on $0 \leq a \leq p-1$ gives $p^{a/(p-1)} \leq a+1$. If a_i are the digits of r, then $\prod_i (a_i + 1) \leq r+1$: the product counts the integers whose digits are bounded by the corresponding a_i, and all of them lie in $[0, r]$.

The resultant

$$\mathcal{R} = \mathrm{Res}((-1)^d G(-Z), Q(Z)) = \prod_{i=1}^{d} Q(M_i)$$

is a nonzero integer. Both M_i and $Q(M_i)$ are algebraic integers, so their finite valuations are nonnegative. For a fixed p, $\sum_i v_p(M_i) = v_p(K)$, and

$$\sum_{i : v_p(M_i) > 0} \min\{v_p(M_i), (p-1)^{-1}\} \leq \min\{v_p(K), d/(p-1)\}.$$

For roots with zero valuation, use only $v_p Q(M_i) \geq 0$. Summing (3.19) over the remaining roots, then over $p \mid K$, and applying (3.20), yields

$$\log|\mathcal{R}| \geq (n+s)\log K - (n+1)T_d(K) - d\,\omega(K)\log s. \tag{3.21}$$

Primes not dividing K make nonnegative contributions to the left side, so omitting them preserves this inequality.

For $R = |M_i| > s$, the gamma integral gives

$$\begin{aligned} |Q(M_i)| &\le \frac{R^r}{n!} \int_0^\infty t^n e^{-t} (1 + t/R)^r \, dt \\ &\le \frac{R^{n+s}}{(R-r)^{n+1}}. \end{aligned}$$

The root gap (2.21) gives $R - r > \rho_0(n+1)$. Therefore

$$\log |\mathcal{R}| < (n+s) \log K - d(n+1) \log\bigl(\rho_0(n+1)\bigr).$$

This is strict also when $r = 0$. Comparison with (3.21) proves (3.15).

For the second inequality, the tangent line to $\log(1+x)$ at $v > 0$ gives

$$\log(1+x) \le \phi(v) + \frac{x}{1+v}, \qquad \phi(v) = \log(1+v) - \frac{v}{1+v} \le \frac{v^2}{2} \quad (x \ge 0).$$

The last bound follows by integrating $\phi'(v) = v/(1+v)^2 \le v$ from zero. Since $R > s > r$, the same gamma integral now gives

$$|Q(M_i)| < \frac{R^{n+s}}{L_v^{n+1}}, \qquad L_v = e^{-r\phi(v)/(n+1)} \left(R - \frac{r}{1+v} \right). \tag{3.22}$$

The inequality is strict because $r > 0$ and the tangent-line inequality is strict except at one integration point. Take $v = \sqrt{(n+1)/r} \le 1$, using $s \ge n+2$. Then

$$L_v > e^{-1/2} \left(1 + \frac{rv}{1+v} \right) > \frac{\sqrt{r(n+1)}}{2\sqrt{e}} \ge \frac{\sqrt{sn}}{2\sqrt{e}}.$$

The last step uses $(s-1)(n+1) \ge sn$. Multiplying (3.22) over the roots and comparing with (3.21) proves the assertion with constant $\log 2 + 1/2 < 2$. □

In the estimates below we use the weaker bound $\rho_0 > 1/4$ to keep the numerical constants simple.

3.2.2. *Prime estimates.* Write

$$\pi(x) = \#\{p \le x : p \text{ prime}\}, \qquad \vartheta(x) = \sum_{p \le x} \log p, \qquad S(x) = \sum_{p \le x} \frac{\log p}{p-1}.$$

We use the following explicit estimates:

$$|\vartheta(x) - x| \le \frac{x}{100(\log x)^2} \qquad (x > 7\,713\,133\,853), \tag{3.23}$$

$$\pi(x) \le \frac{x}{\log x - 1.1} \qquad (x > 60\,184), \tag{3.24}$$

$$S(x) < \log x \qquad (x \ge 319). \tag{3.25}$$

The first two estimates are [15, Theorem 5.2, p. 4, and Theorem 6.9, (6.6)]. For the third, Rosser and Schoenfeld [42, Theorem 6, (3.22)] prove

$$\sum_{p \le x} \frac{\log p}{p} < \log x + E + \frac{1}{2 \log x} \qquad (x \ge 319),$$

where [42, (2.8)] defines

$$E = -\gamma - \sum_p \frac{\log p}{p(p-1)}.$$

Adding the sum over $p \le x$ of $\log p/(p(p-1))$ gives

$$S(x) < \log x - \gamma + \frac{1}{2\log x} < \log x.$$

The last inequality follows, for example, from $\gamma > 1-\log 2 > 3/10$ and $\log x > 2$. Here $\gamma > 1-\log 2$ follows by writing γ as the increasing limit of $\sum_{k=1}^{N}(1/k - \log(1+1/k))$.

We shall repeatedly use the elementary comparisons

$$\frac{\log u}{u} < \frac{1}{1000}, \qquad e^u > 10^{30}u^5, \qquad e^{u/2} > 10^{25}u^4 \qquad (u \ge 10000). \tag{3.26}$$

At $u = 10000$, the logarithmic comparisons follow from $\log 10000 < 10$ and $\log 10 < 7/3$. The function $(\log u)/u$ decreases, while the logarithms of the last two ratios have derivatives $1-5/u > 0$ and $1/2 - 4/u > 0$. We also use $2/3 < \log 2 < 7/10$, $\log 13 < 3$, and $\log 52 < 4$. These elementary bounds follow from the exponential series and

$$\log 2 = 2\sum_{j\ge 0} \frac{1}{(2j+1)3^{2j+1}}.$$

The Newton-polygon arguments require lower bounds for the number of primes in intervals proportional to n. The same estimates also control the total number of primes up to n.

Lemma 3.10. *If $u = \log n \ge 10000$, then*

$$\pi(n) < \frac{1003n}{1000u}, \qquad \pi(n/\ell) - \pi(n/(4\ell)) > \frac{749n}{1000\ell u} \quad (1 \le \ell \le 13). \tag{3.27}$$

In particular, $\pi(n) < n/100$.

Proof. The estimate (3.24) gives directly

$$\pi(n) \le \frac{n}{u - 11/10} < \frac{1003n}{1000u} \qquad (u \ge 10000).$$

For $t = n/\ell$, all arguments exceed the threshold in (3.23), by (3.26), and $\log(t/4) > u - 4$. Hence

$$\vartheta(t) - \vartheta(t/4) \ge \frac{3t}{4} - \frac{5t}{400(u-4)^2} > \frac{749t}{1000}.$$

Division by $\log t \le u$ gives the second estimate. □

The Padé inequalities involve $\omega(K)$ and $T_d(K)$. Both can be estimated from an upper bound for $\log K$, which the root annulus supplies for a factor constant term.

Lemma 3.11. *Let K, d be positive integers, and suppose $\log K < X$, where $X \ge 10000$. Then*

$$\omega(K) < \frac{2X}{\log X}, \qquad \frac{T_d(K)}{d} < \log X + 1.001. \tag{3.28}$$

Proof. Put $w = \omega(K)$. Since the ith prime is at least $i+1$, $K \ge (w+1)!$. If $w \ge 1$, integration of $\log t$ gives $\log K > w\log w - w$. At $w = 2X/\log X$, this last expression exceeds X: writing $y = \log X \ge 4$, the required comparison is $y/2 - \log y + \log 2 - 1 > 0$, which holds at $y = 4$ and increases thereafter. The function $w\log w - w$ increases for $w > 1$, proving the first bound; the case $w = 0$ is immediate.

For the second bound, use $T_d(K)/d \le \sum_{p|K} \log p/(p-1)$ and split at X. The smaller primes contribute at most $S(X) < \log X$ by (3.25). The remaining contribution is at most $\log K/(X-1) < X/(X-1) < 1.001$. □

When s has polynomial size in n, the first Padé inequality already excludes small factors.

Lemma 3.12. *If $\log n \geq 10000$, $1 \leq s \leq n^3$, and $H_{n,s}$ has a proper rational factor of degree d, then*

$$d > \frac{n}{100 \log n}. \tag{3.29}$$

Proof. Let G be a monic factor of degree d, and set $u = \log n$, $t = \log(s+n)$, $X = dt$, and $K = |G(0)|$. The annulus (2.7) gives $\log K < X$, and $u < t < 3.01u$. If $d \leq n/(100u)$, then $10000 \leq u < X < n/32$. Lemma 3.11 implies

$$\frac{T_d(K)}{d} < u - 5\log 2 + 1.001 < u - 2.3.$$

As $X/\log X$ increases in this range,

$$\frac{\omega(K)\log s}{n+1} < \frac{3u}{16(u - \log 32)} < \frac{1}{5}.$$

The right side of (3.15) is less than $u - 2.1$, whereas its left side exceeds $u - \log 4 > u - 2$, a contradiction. □

3.2.3. *The prime-square obstruction.* For primes p with $\sqrt{n} < p \leq n$, the absence of a multiple of p^2 in the parameter interval forces a Newton-polygon side of slope $-1/p$. Its denominator restricts the degrees of rational factors.

Proposition 3.13. *Suppose $H_{n,s}$ has a rational factor of degree d. If a prime p satisfies $p^2 > n$ and $p \mid \binom{n}{d}$, then some integer in $[s, s+n-1]$ is divisible by p^2. Moreover, if $n \geq 5$ and $1 \leq d \leq n/2$, then*

$$\pi(n) - \pi(n-d) \leq \left\lfloor \frac{s+n-1}{(n-d+1)^2} \right\rfloor - \left\lceil \frac{s}{n^2} \right\rceil + 1. \tag{3.30}$$

Proof. Suppose that the interval contains no multiple of p^2. The asserted divisibility of $\binom{n}{d}$ requires $p \leq n$. Write $n = ap + b$ and $s - 1 = cp + t$, with $0 \leq b, t < p$ and $a < p$. For $j = \ell p + v$, $0 \leq v < p$, the coefficient of X^j has valuation

$$a - \ell + \left\lfloor \frac{t + b - v}{p} \right\rfloor + \mathbf{1}_{v>b}. \tag{3.31}$$

Indeed, the rising factorial $(s)_{n-j}$ counts multiples of p, each of valuation one, and, since $n < p^2$, $v_p\binom{n}{j} = \mathbf{1}_{v>b}$.

If $t + b < p$, the lower Newton polygon has vertices

$$(0, a), \qquad (ap, 0), \qquad (n, 0).$$

If $t + b \geq p$, put $v_0 = t + b - p < b$. Its vertices are

$$(0, a+1), \qquad (v_0 + 1, a), \qquad (ap + v_0 + 1, 0), \qquad (n, 0).$$

These assertions follow directly from (3.31); coincident vertices are omitted. In the second case the initial slope is $-1/(v_0+1)$, where $1 \leq v_0 + 1 \leq b < p$, so it is distinct from $-1/p$. The Newton polygon theorem therefore shows that exactly ap roots have valuation $1/p$, with only b other roots.

The roots selected by the rational factor form a set invariant under the local Galois group. Intersecting it with the set of roots of valuation $1/p$ again gives an invariant set. Its product belongs to $\mathbb{Q}_p^\times$, and hence has integer valuation. The number of selected roots of valuation $1/p$ must consequently be a multiple of p. Thus $d = kp + e$ with $0 \leq k \leq a$ and $0 \leq e \leq b$. The same base-p factorial valuation formula now gives $v_p\binom{n}{d} = 0$, a contradiction.

For the second assertion, every prime $p \in (n-d, n]$ satisfies $p > n/2 > \sqrt{n}$ and divides $\binom{n}{d}$. Choose an integer $k_p \geq 1$ with $s \leq k_p p^2 \leq s + n - 1$. Distinct primes have distinct multipliers: if $p < q$ had the same multiplier k, then $k(q^2 - p^2) \geq 2p + 1 > n - 1$, impossible in an interval

of length $n-1$. Every multiplier lies between $\lceil s/n^2 \rceil$ and $\lfloor (s+n-1)/(n-d+1)^2 \rfloor$, proving (3.30). □

The degree bound and the prime estimates ensure that $(n-d, n]$ contains many primes. The square-divisibility obstruction then requires more distinct multipliers than a small value of s permits.

Proposition 3.14. *If* $\log n \geq 10000$ *and*

$$1 \leq s \leq \frac{n^3}{10 \log n}, \tag{3.32}$$

then $H_{n,s}$ *is irreducible over* $\mathbb{Q}$.

Proof. If $H_{n,s}$ is reducible, choose a factor of degree $1 \leq d \leq n/2$ and put $u = \log n$. Lemma 3.12 gives $d > n/(100u)$. Both n and $n-d$ exceed the threshold of (3.23), and $\log(n-d) \geq u - \log 2$. Therefore

$$\vartheta(n) - \vartheta(n-d) > d - \frac{3n}{100u^2} > \frac{4d}{5}, \qquad \pi(n) - \pi(n-d) > \frac{4d}{5u}.$$

On the other hand, the right side of (3.30) is less than

$$\frac{6sd}{n^3} + 1 + \frac{4}{n} \leq \frac{3d}{5u} + 1 + \frac{4}{n}.$$

Here we used $n - d \geq n/2$ and

$$\frac{1}{(n-d)^2} - \frac{1}{n^2} = \frac{d(2n-d)}{n^2(n-d)^2} \leq \frac{6d}{n^3}.$$

But $d/(5u) > n/(500u^2) > 1 + 4/n$ by (3.26). This is a contradiction. □

For larger parameters, the tangent estimate in Proposition 3.9 gives a stronger restriction. The resulting degree bound depends on s only through $\log(s+n)$.

Lemma 3.15. *Suppose* $\log n \geq 10000$, $s \geq n^{5/2}$, *and* $H_{n,s}$ *has a rational factor of degree* $d \geq 1$. *Put* $A = \log(s+n)/\log n$. *Then*

$$d > \frac{n}{16A}. \tag{3.33}$$

Proof. Write $u = \log n$, suppose $d \leq n/(16A)$, and put $X = dAu$ and $K = |G(0)|$ for a monic factor G of degree d. The root annulus gives $\log K < X$, while $10000 \leq Au \leq X \leq nu/16$. Lemma 3.11 yields

$$\frac{T_d(K)}{d} < u + \log u, \qquad \omega(K) < \frac{n}{4}.$$

The estimate for $T_d(K)$ uses $\log 16 > 1.001$. To bound $\omega(K)$, apply monotonicity of $X/\log X$ and the inequality $\log(nu/16) > u/2$. Moreover $Au - 1 < \log s < Au$. Thus (3.16) would imply

$$\frac{Au+u}{2} - 3 < u + \log u + \frac{Au}{4}.$$

This is impossible: $A \geq 5/2$, and

$$u\left(\frac{A}{4} - \frac{1}{2}\right) - \log u - 3 \geq \frac{u}{8} - \log u - 3 > 0$$

by (3.26). □

3.3. **Root energy and uniform eventual irreducibility.** We apply the matrix-energy inequality to a rational factor. Its proportion of roots in a local cluster need not equal its proportion in the full root set; the square of this discrepancy contributes to the energy. The resulting degree restrictions will combine with the trace criterion to cover all parameters. Throughout this section, n, s are positive integers, $u = \log n$, and all factors are defined over $\mathbb{Q}$.

3.3.1. *The energy of a rational factor.* Suppose $H_{n,s} = GJ$, where G, J are monic rational factors and $1 \le d = \deg G \le n/2$. They are integral by Gauss's lemma. Put $x = d/n$, and use the rank-one matrix $Q = cc^{\mathsf{T}}$ with $c_i = 1 - x$ on the roots of G and $c_i = -x$ on the roots of J. Thus

$$\sum_i c_i = 0, \qquad \sum_i c_i^2 = nx(1-x). \tag{3.34}$$

At a prime p, define stopping heights and local energy by

$$h_{p,i} = v_p(\alpha_i) + \epsilon_p, \qquad E_p = \sum_{i \ne j} c_i c_j v_p(\alpha_i - \alpha_j) + \sum_i c_i^2 h_{p,i}. \tag{3.35}$$

There are only finitely many nonzero contributions: outside the primes at most n and those dividing the constant term or discriminant, all the valuations occurring here vanish.

Lemma 3.16. *Every E_p is nonnegative. If $N_p(t)$ counts all roots of valuation at least t, and $K_p(t)$ counts the selected roots of valuation at least t, then*

$$E_p \ge \int_0^\infty (K_p(t) - xN_p(t))^2 \, dt. \tag{3.36}$$

Write

$$K = |G(0)|, \qquad P = (s)_n, \qquad S(n) = \sum_{p \le n} \frac{\log p}{p-1},$$

$$C_\infty = \sum_{i \ne j} c_i c_j \log|\alpha_i - \alpha_j|.$$

Then the global energy $\mathcal{E} = \sum_p E_p \log p$ satisfies

$$\mathcal{E} = C_\infty + (1-x)^2 \log K + x^2 \log(P/K) + nx(1-x)S(n). \tag{3.37}$$

If the closed complex disks of radius ρ around the roots are pairwise disjoint, then

$$C_\infty \le -nx(1-x)\log\rho. \tag{3.38}$$

Proof. The root sets of the rational factors are Galois invariant, so $Q = cc^{\mathsf{T}}$ is invariant and has trace $nx(1-x)$. Lemma 3.5 therefore applies. On the roots of valuation at least t, the sum of the charges is $K_p(t) - xN_p(t)$, giving (3.36). The diagonal contribution to the product formula is $(1-x)^2 \log K + x^2 \log(P/K)$, which gives (3.37). The complex bound follows from the same lemma. □

The annulus and separation estimates now give an upper bound.

Lemma 3.17. *Suppose $u = \log n \ge 10000$ and a factor of degree $1 \le d \le n/2$ exists. If $s \ge n^{5/2}$, then*

$$\mathcal{E} < 3nx(1-x)\log s. \tag{3.39}$$

Proof. For $s \ge n$, apply Lemma 3.5 to $Q = cc^{\mathsf{T}}$, whose trace is $nx(1-x)$. It gives

$$\mathcal{E} < nx(1-x)\left(\frac{1}{2}\log s + \frac{3}{2}u + \log 48\right). \tag{3.40}$$

For $s \ge n^{5/2}$ this is less than (3.39). □

3.3.2. *Packets and deletion of small-prime contributions.* For $p > n$, the local calculation in Proposition 3.2 concerns a single node $s + j$. The following specialization of the packet-energy formula records both its energy and the restriction on the number of roots selected by a factor.

Lemma 3.18. *Suppose $p > n$ and $p^e \| s + j$, where $0 \le j < n$, and put $N = n - j$. Exactly N roots have valuation e/N; the other j roots are units. If a rational factor selects k of the former roots, then*

$$N \mid ke, \qquad E_p \log p = N \left(\frac{k}{N} - x \right)^2 \log(p^e). \tag{3.41}$$

Proof. The tame-packet construction in Proposition 3.2 and Lemma 3.1 gives the stated valuations and inertia orbit length $q = N/\gcd(N, e)$. A rational factor selects a union of these orbits, so $q \mid k$, equivalently $N \mid ke$. Formula (3.10), applied to $Q = cc^{\mathsf{T}}$, gives

$$E_p = \frac{e}{N}(k - xN)^2,$$

which proves the energy identity, including when $N = 1$. □

Before summing over large primes, we bound the parts of the nodes supported on small primes. For each small prime, remove its full contribution from one node of maximal valuation. The remaining product divides a factorial. Deleting those nodes altogether gives the form used below. This is the allocation argument of Erdős and Selfridge [17, Lemma 2].

Lemma 3.19. *Let $\mathcal{I} \subseteq \{0, \dots, n-1\}$ and $Y \ge 2$. Let $\mathcal{P}$ be the set of primes $p \le Y$ dividing at least one node $s + j$ with $j \in \mathcal{I}$. For each $p \in \mathcal{P}$, choose an index $j_p \in \mathcal{I}$ of maximal p-valuation. Remove the p-part only from the node assigned to p, and put*

$$R_j = \prod_{\substack{p \in \mathcal{P} \\ j \ne j_p}} p^{v_p(s+j)}.$$

Then $\prod_{j \in \mathcal{I}} R_j \mid (n-1)!$. In particular, deleting the union of the chosen indices removes at most $\pi(Y)$ nodes. If $\mathcal{J}$ is the remaining set and $S_Y(m)$ denotes the part of m supported on primes at most Y, then

$$\prod_{j \in \mathcal{J}} S_Y(s + j) \mid (n-1)!. \tag{3.42}$$

Proof. For $j \ne j_p$, maximality gives $v_p(s+j) \le v_p(j - j_p)$. The product of the distances on either side of j_p divides $j_p!(n - 1 - j_p)!$, which divides $(n-1)!$. This proves the first assertion prime by prime. Every undeleted node retains its entire Y-smooth part, giving the second. □

From now on take $Y = n$, write $S_j = S_n(s + j)$, and put $B_j = (s + j)/S_j$. Thus all primes dividing B_j are greater than n. A prime greater than n occurs at only one parameter node. Moreover, for $p^e \| B_j$,

$$e < A := \frac{\log(s + n)}{\log n}. \tag{3.43}$$

The reduced denominator of a selected fraction $q = k/(n - j)$ divides both $n - j$ and e, by (3.41).

3.3.3. *A restriction on the factor degree.* Since $e < A$, every selected fraction has reduced denominator less than A. Distinct such fractions are separated by at least A^{-2}. We choose packet widths that exclude the one possible fraction close to $x = d/n$ and then sum the resulting energy bounds.

Lemma 3.20. *Suppose $u = \log n \ge 10000$, $s \ge n^{5/2}$, and a rational factor of degree $1 \le d \le n/2$ exists. Then*

$$d < 4800 \qquad \text{or} \qquad A > (n/4800)^{1/4}. \tag{3.44}$$

Proof. Put $x = d/n$ and $\eta = \min\{x/2, 1/(4A^2)\}$. Distinct reduced fractions with denominators at most A differ by at least A^{-2}. Hence at most one lies in $(x-\eta, x+\eta)$. If present, its denominator b is at least two, since $0 < x-\eta < x+\eta < 1$. Choose the widths $\lceil n/8 \rceil \le N \le n$, omitting the multiples of b if that close fraction exists. There are at least $7n/16 - 2$ choices. Every reduced fraction whose denominator is at most A and divides one of the chosen widths N is therefore at distance at least η from x.

Apply Lemma 3.19 to the corresponding indices $j = n - N$. The bound $\pi(n) < n/100$ from (3.27) leaves more than $0.42n$ indices. Consequently

$$\sum_{j \in \mathcal{J}} \log B_j > 0.42n \log s - \log((n-1)!) > \frac{n}{50} \log s,$$

since $\log s \ge (5/2)u$ and $\log((n-1)!) < nu$. For every prime power in these B_j, (3.43) and the preceding denominator exclusion give $|k/N - x| \ge \eta$. Since $N \ge n/8$, summing the packet energies without repetition of any large prime yields

$$\mathcal{E} > \frac{n^2\eta^2}{400} \log s.$$

Comparison with (3.39) gives $n\eta^2 < 1200x(1-x)$. If $\eta = x/2$, then $d < 4800$. Otherwise $n/(16A^4) < 1200x(1-x) \le 300$, giving the other alternative. □

3.3.4. *Uniform eventual irreducibility.* For a reducible member, the four-fiber bound makes $\log s$ smaller than every fixed positive power of n once n is sufficiently large. Within that range, the Padé lower bound for the factor degree contradicts the energy dichotomy. Together these estimates give uniform eventual irreducibility.

Proposition 3.21. *There is an effective absolute integer N_0 such that $H_{n,s}$ is irreducible for every $n \ge N_0$ and every positive integer s.*

Proof. Suppose a factor of degree $1 \le d \le n/2$ exists. Corollary 2.16, with $B = 0$ and $\varepsilon = 1/8$, gives $\log s < n^{1/8}$ for all sufficiently large n. For sufficiently large n, one has $n^{5/2} \le n^3/(10 \log n)$, so Proposition 3.14 excludes $s \le n^{5/2}$. In the remaining range put $u = \log n$ and $A = \log(s+n)/u$. For all sufficiently large n,

$$A < \frac{2n^{1/8}}{u} < (n/4800)^{1/4}, \qquad d > \frac{n}{16A} > 4800,$$

where the middle degree bound is Lemma 3.15. These inequalities contradict Lemma 3.20. Every threshold used here is effective, so their maximum gives the asserted N_0. □

4. Galois groups

Assuming irreducibility, we prove that the Galois group contains A_n once n exceeds an effective absolute constant. A local criterion first excludes the primitive groups that omit A_n. For an imprimitive group, the energy estimate restricts its invariant partitions to two blocks. Integral traces handle a real quadratic block field; Laurent interpolation handles an imaginary quadratic block field. The estimates are uniform in s.

4.1. **Prime valuations in short intervals.** We begin with an arithmetic criterion for alternating containment. A short interval cannot contain many integers whose large-prime valuations are all divisible by exponents comparable to its length. Newton polygons turn this statement into a criterion for alternating containment. We apply it first to Laguerre polynomials; the trimmed-exponential application is given in Section 6.2. Sections 4.2–4.5 will place every remaining Laguerre obstruction in its parameter range.

4.1.1. *Independent nodes and simultaneous logarithms.* For a rational number a/b in lowest terms, put $H(a/b) = \max\{|a|, |b|\}$ and $h(a/b) = \log H(a/b)$. We use Loxton's estimate for simultaneous linear forms [36, Theorem 4], in the form stated by Stewart [46, Lemma 1]. Let $r \geq 2$, $1 \leq m \leq r$, and let $\beta_1, \dots, \beta_r$ be multiplicatively independent positive rational numbers. Suppose the rational matrix (b_{ij}) has rank m, and put

$$\Lambda_i = \sum_{j=1}^{r} b_{ij} \log \beta_j \qquad (1 \leq i \leq m).$$

For $A_j, B \geq 4$ with $H(\beta_j) \leq A_j$ and $H(b_{ij}) \leq B$, write $\Omega = \prod_{j=1}^{r} \log A_j$. Then

$$\max_i |\Lambda_i| > \exp\Big(-(16r)^{200r} (\Omega \log \Omega)^{1/m} \log(B\Omega)\Big). \tag{4.1}$$

The forms must retain full rank after dependent bases are removed. We ensure this by first choosing multiplicatively independent integers in the parameter interval. The following elementary version of Stewart's argument is convenient [46, Theorem 1 and Corollary 3].

Lemma 4.1. *Fix an integer $t \geq 2$, and put*

$$K_t = t\big((4(t-1))^{t-1} + 1\big).$$

Let M, s be positive integers with $s > 2M^2$. Any set of at least K_t distinct integers in $[s, s+M]$ contains t multiplicatively independent integers.

Proof. Suppose every t-element subset is dependent. Choose an integral multiplicative relation for each such subset and omit an index whose coefficient has largest absolute value. If there are k numbers, some fixed $(t-1)$-element subset is associated with at least

$$\left\lceil \frac{\binom{k}{t}}{\binom{k}{t-1}} \right\rceil = \left\lceil \frac{k-t+1}{t} \right\rceil$$

subsets. Write its elements as $a_1, \dots, a_{t-1}$. For every associated extra element z, the chosen relation has the form

$$z^{\ell} = \prod_{i=1}^{t-1} a_i^{c_i}, \qquad \ell > 0, \qquad |c_i| \leq \ell.$$

Divide each coordinate interval of $[-1, 1]^{t-1}$ into $4(t-1)$ intervals. Since $k \geq K_t$, two distinct extra elements z, z' have associated vectors satisfying

$$\left| \frac{c_i}{\ell} - \frac{c_i'}{\ell'} \right| \leq \frac{1}{2(t-1)} \qquad (1 \leq i < t).$$

Raise the quotient of the two relations to clear denominators. The identities $h(x^j) = |j| h(x)$ and $h(xy) \leq h(x) + h(y)$ then give

$$h(z/z') \leq \sum_{i=1}^{t-1} \left| \frac{c_i}{\ell} - \frac{c_i'}{\ell'} \right| h(a_i) \leq \frac{1}{2} \log(2s).$$

Here $s + M < 2s$. But $\gcd(z, z') \mid z - z'$ and $0 < |z - z'| \leq M$, so

$$h(z/z') \geq \log(s/M) > \tfrac{1}{2} \log(2s),$$

a contradiction. □

The next bound allows a fixed number of small primes to have large exponents. It will be used after assigning each small prime to one node where its valuation is maximal.

Lemma 4.2. *Fix $C \geq 1$ and integers $m \geq 2$, $R \geq 0$. There is an effectively computable constant $C_{m,R,C} > 0$ with the following property. Let $n \geq 3$ and s be positive integers, put $L = \log s$, and suppose*

$$L \geq 2\log(Cn), \qquad 2 \leq H \leq L.$$

Let $z_0, \dots, z_m$ be multiplicatively independent integers in $[s, s+Cn]$. Suppose that, for $1 \leq i \leq m$,

$$z_i = d_i x_i^{k_i} \prod_{\ell=1}^{R_i} p_{i\ell}^{e_{i\ell}},$$

where d_i, x_i, k_i are positive integers, the $p_{i\ell}$ are primes, and

$$\log d_i \leq H, \quad n/2 \leq k_i \leq n, \quad R_i \leq R, \quad p_{i\ell} \leq Cn, \quad 0 \leq e_{i\ell} \leq n.$$

Then

$$L^{1-1/m} \leq C_{m,R,C}\, H (\log n)^R \max\{1, L/n\} \big(\log(nL)\big)^{1+1/m}. \tag{4.2}$$

Proof. Use the m real forms

$$\Lambda_i = k_i \log x_i + \log d_i + \sum_{\ell=1}^{R_i} e_{i\ell} \log p_{i\ell} - \log z_0 = \log(z_i/z_0).$$

Their values are linearly independent over $\mathbb{Q}$, since a relation among them would give a multiplicative relation among $z_0, \dots, z_m$. Moreover,

$$0 < \max_i |\Lambda_i| \leq Cn/s. \tag{4.3}$$

List the positive integers occurring as bases, omitting 1 and repetitions, and choose a maximal independent subset $\beta_1, \dots, \beta_r$. There are at most $r_0 = m(R+2)+1$ original bases, and $m \leq r \leq r_0$. Every original logarithm is a rational linear combination of this basis. All original bases have logarithmic height at most $2L$: indeed $s \geq (Cn)^2$, and

$$\log x_i \leq \frac{\log(s+Cn)}{k_i} \leq \frac{4L}{n}.$$

Choose r primes for which the valuation matrix of the β_j is nonsingular. Its entries, and the entries of the valuation vector of each original base, are at most $4L$. Cramer's rule gives a common denominator $\det V$ and numerators of absolute value at most

$$D_0 = r!(4L)^r.$$

These are relations at every prime: the selected valuation vectors form a basis of the span of all original valuation vectors, and restriction to the chosen r primes is injective on that span.

After substitution, the coefficient matrix of the Λ_i still has rank m, by the independence of their values. Each entry has rational height at most $B_0 = (R+3)nD_0$, since a row has at most $R+3$ original terms and their integer coefficients have absolute value at most n. Thus

$$\log \max\{4, B_0\} \ll_{m,R} \log(nL). \tag{4.4}$$

Put $U = \max\{1, L/n\}$. We may use logarithmic height bounds H, $4U$, $2\log(Cn)$, and $2L$ for the bases d_i, x_i, $p_{i\ell}$, and z_0, respectively. Every bound exceeds $\log 4$ and hence also 1. Because the independent basis is a subset of the original list,

$$\Omega \leq 2L \left(4HU(2\log(Cn))^R\right)^m, \qquad \log \Omega \ll_{m,R,C} \log(nL). \tag{4.5}$$

Repeated bases can be assigned any one of their corresponding bounds; removing repetitions or dependent bases decreases the upper bound for the product. Applying (4.1) and using (4.4)–(4.5), we obtain

$$-\log \max_i |\Lambda_i| \ll_{m,R,C} L^{1/m} HU (\log n)^R \big(\log(nL)\big)^{1+1/m}.$$

By (4.3), the left side is at least $L - \log(Cn) \geq L/2$. This proves (4.2). □

4.1.2. *Large-prime valuations at nearby integers.* The exponent in the next theorem may vary from one integer to another and need not be prime. This flexibility is what permits one to use different Newton-polygon widths simultaneously.

Theorem 4.3. *Fix real numbers $C \geq 1$, $c > 0$, $D > 0$, and*

$$\kappa > \lfloor C/c \rfloor + 3.$$

There is an effectively computable integer $N = N(C, c, D, \kappa)$ such that the following holds. Let $n \geq N$ and $s \in \mathbb{Z}_{>0}$ satisfy

$$(\log n)^\kappa \leq \log s \leq n^D.$$

If

$$\mathcal{Z} \subseteq [s, s + \lfloor Cn \rfloor] \cap \mathbb{Z}, \qquad |\mathcal{Z}| \geq cn/\log n,$$

then, for every assignment of integers k_z with $n/2 \leq k_z \leq n$, there are $z \in \mathcal{Z}$ and a prime $p > Cn$ for which

$$k_z \nmid v_p(z).$$

Proof. Put $M = \lfloor Cn \rfloor$, $L = \log s$, and suppose instead that $k_z \mid v_p(z)$ for all $z \in \mathcal{Z}$ and all primes $p > Cn$. For every prime $p \leq M$ dividing a node, assign p to one node z_p where $v_p(z_p)$ is maximal. Reduce every valuation at a node z modulo k_z. Put the remainders at its assigned primes into separate factors and all other remainders into d_z. This gives

$$z = d_z x_z^{k_z} \prod_{p \text{ assigned to } z} p^{r_{z,p}}, \qquad 0 \leq r_{z,p} < k_z.$$

There are no remainders at primes exceeding M, since an integer prime exceeds M exactly when it exceeds Cn.

The unassigned parts satisfy

$$\prod_{z \in \mathcal{Z}} d_z \mid M!. \tag{4.6}$$

To check this at a prime $p \leq M$, consider any level $h \geq 1$. At most $\lfloor M/p^h \rfloor + 1$ integers in an interval of length M are divisible by p^h. If there is one, the chosen maximal node z_p is among them. The total valuation of the unassigned parts is therefore at most $\sum_{h \geq 1} \lfloor M/p^h \rfloor = v_p(M!)$. Reducing valuations modulo the individual k_z can only decrease this total, proving (4.6).

Set

$$R = \lfloor C/c \rfloor, \qquad \gamma = c - \frac{C}{R+1} > 0, \qquad A = \max\left\{2, \frac{4(C+1)}{\gamma}\right\}, \qquad H = A(\log n)^2.$$

For all effectively sufficiently large n, the prime estimate (3.24) and the elementary factorial bound give

$$\pi(M) \leq \left(C + \frac{\gamma(R+1)}{4}\right) \frac{n}{\log n}, \qquad \sum_z \log d_z \leq \log(M!) \leq (C+1)n \log n.$$

The number of nodes with more than R assigned primes is at most

$$\frac{\pi(M)}{R+1} \leq \left(c - \frac{3\gamma}{4}\right) \frac{n}{\log n}.$$

At most $\gamma n/(4 \log n)$ nodes have $\log d_z > H$. Consequently at least $\gamma n/(2 \log n)$ nodes remain, each with at most R separate prime factors and $\log d_z \leq H$.

Choose an integer

$$m > \max\left\{2, D, \frac{\kappa + 1}{\kappa - R - 3}\right\}.$$

Then $D/m < 1$ and

$$\kappa(1 - 1/m) > R + 3 + 1/m.$$

For sufficiently large n, there are at least K_{m+1} remaining nodes, $s > 2M^2$, $L \geq 2\log(Cn)$, and $2 \leq H \leq L$. Lemma 4.1 gives independent nodes $z_0, \ldots, z_m$. Retain the displayed factorization for $z_1, \ldots, z_m$ and use z_0 as a single base. Lemma 4.2 yields

$$L^{1-1/m} \ll_{C,c,D,\kappa} (\log n)^{R+3+1/m} \max\{1, L/n\},$$

where we used $L \leq n^D$ to bound $\log(nL)$. If $L \geq n$, this implies

$$n \ll_{C,c,D,\kappa} n^{D/m} (\log n)^{R+3+1/m},$$

which is impossible for large n because $D/m < 1$. If $L < n$, it instead implies

$$(\log n)^{\kappa(1-1/m)} \ll_{C,c,D,\kappa} (\log n)^{R+3+1/m},$$

again a contradiction by the choice of m. All constants depend only on the displayed fixed parameters. The prime estimates and logarithmic-form bound are effective, so the required threshold is effective as well. □

For every fixed $0 < \varepsilon \leq D$, the same conclusion holds in the range $n^\varepsilon \leq \log s \leq n^D$, with a threshold depending on C, c, ε, D. Indeed, choose $\kappa = \lfloor C/c \rfloor + 4$ and use $(\log n)^\kappa \leq n^\varepsilon$ for sufficiently large n.

4.1.3. *A Newton-polygon criterion.* A single edge whose slope has a sufficiently large prime denominator forces alternating containment in a transitive group [28, Theorems 2.1 and 2.2]. The preceding theorem supplies such a denominator from a collection of nearby integers.

Theorem 4.4. *Fix $C \geq 1$, $c > 0$, $D > 0$, and $\kappa > \lfloor C/c \rfloor + 3$. For all effectively sufficiently large n, the following holds. Let $s \in \mathbb{Z}_{>0}$ satisfy $(\log n)^\kappa \leq \log s \leq n^D$, and let $F \in \mathbb{Z}[X]$ be separable of degree n, with $F(0) \neq 0$. Suppose there are a set of primes*

$$\mathcal{P} \subseteq (n/2, n-3], \qquad |\mathcal{P}| \geq cn/\log n,$$

and distinct integers $j_P \in \{0, \ldots, \lfloor Cn \rfloor\}$ with the following property: whenever $p > Cn$ is prime and $e = v_p(s + j_P) > 0$ is not divisible by P, the p-adic Newton polygon of F has an edge of slope $-e/P$. For each pair (p, P), this edge condition may instead hold for $F(X + a_{p,P})$ with some integer $a_{p,P}$.

Then $\mathrm{Gal}(F/\mathbb{Q})$ contains a P-cycle for some $P \in \mathcal{P}$ and preserves no nontrivial partition into equal blocks. If F is irreducible over $\mathbb{Q}$, then

$$A_n \leq \mathrm{Gal}(F/\mathbb{Q}).$$

The threshold depends only on C, c, D, κ.

Proof. Apply Theorem 4.3 to the distinct integers $z_P = s + j_P$, with exponent $k_{z_P} = P$. It gives a prime $p > Cn$ and a width $P \in \mathcal{P}$ for which $P \nmid e = v_p(z_P)$. In particular $e > 0$. The corresponding Newton-polygon edge supplies a root of the relevant translate with p-adic valuation e/P. The translate has the same splitting field as F. Since this fraction has denominator P, the ramification index of the local splitting field, and hence the order of the global Galois group, is divisible by P. Cauchy's theorem gives an element of order P. It is a single P-cycle because $2P > n$.

A group preserving a blocks of size b, where $a, b \geq 2$ and $ab = n$, embeds in $S_b \wr S_a$. Its order divides $(b!)^a a!$, which is not divisible by $P > n/2 \geq \max\{a, b\}$. Thus no such partition exists. If F is irreducible, its root action is transitive and therefore primitive. Jordan's theorem, applied to the P-cycle with $P \leq n - 3$, gives A_n. □

Corollary 4.5. *Fix $D > 0$ and $\kappa > 5$. For all effectively sufficiently large n, the Galois group of $H_{n,s}$ preserves no nontrivial partition into equal blocks whenever*

$$(\log n)^{\kappa} \le \log s \le n^{D}.$$

If $H_{n,s}$ is irreducible in this range, then $A_n \le G_{n,s}$. These conclusions do not use the classification of finite simple groups. In particular, they hold in every range $n^{\varepsilon} \le \log s \le n^{D}$ with fixed $0 < \varepsilon \le D$, after increasing the effective threshold in terms of ε, D.

Proof. Use all primes $n/2 < P \le n-3$ and put $j_P = n-P$. Their number is at least $2n/(5\log n)$ for all effectively sufficiently large n. For $p > n$ and $e = v_p(s+j_P) > 0$, write $H_{n,s}(X) = \sum_{k=0}^{n} A_k X^k$. Then

$$A_k = \binom{n}{k}(s)_{n-k}, \qquad v_p(A_k) = \begin{cases} e, & 0 \le k < P, \\ 0, & P \le k \le n. \end{cases}$$

Indeed $s + j_P$ is the only multiple of p among $s, \dots, s+n-1$, and $p \nmid \binom{n}{k}$. The Newton polygon contains the edge from $(0, e)$ to $(P, 0)$. Theorem 4.4 applies with $C = 1$ and $c = 2/5$, since $\lfloor C/c \rfloor + 3 = 5$; separability follows from (1.7). The final assertion follows by taking $\kappa = 6$ and then $(\log n)^6 \le n^{\varepsilon}$. □

4.1.4. *Powers in dense subsets of a progression.* The preceding criterion requires an upper bound on $\log s$. We also need an estimate with no upper bound on the parameter. The following theorem, independent of the polynomial family, supplies it. The initial term may be as small as $k^{2+\varepsilon}$, and the excluded density is explicit. The argument combines Erdős's maximal-valuation deletion [16] with the determinant count of Filaseta–Laishram–Saradha [23, Lemma 3.1]. For earlier work on products after terms have been omitted, see Erdős–Turk [18, Theorem 6.1].

For $\varepsilon > 0$, define

$$a_{\varepsilon} = \min\left\{\varepsilon, \frac{3}{\sqrt{7}} - 1\right\}, \qquad \delta_{\varepsilon} = \frac{a_{\varepsilon}(1 - \frac{7}{2}a_{\varepsilon})}{6(1 + a_{\varepsilon})}.$$

Theorem 4.6. *Fix positive integers d, C with $C \ge d$, and real numbers $\varepsilon > 0$ and $0 < \delta < \delta_{\varepsilon}$. There is an effectively computable $k_0(d, C, \varepsilon, \delta)$ such that, whenever positive integers k, A satisfy*

$$k \ge k_0, \qquad A \ge k^{2+\varepsilon}, \qquad \gcd(A, d) = 1,$$

the following assertions hold simultaneously for every integer $r \ge 2$.

(i) *Fewer than $(1-\delta)k$ indices $0 \le j < k$ admit a representation*

$$A + jd = a_j x_j^r, \qquad a_j, x_j \in \mathbb{Z}_{>0}, \qquad P(a_j) \le Ck.$$

(ii) *More than δk distinct primes $p > Ck$ satisfy*

$$r \nmid v_p\left(\prod_{j=0}^{k-1}(A + jd)\right).$$

(iii) *If $I \subseteq \{0, \dots, k-1\}$ has at least $(1-\delta)k$ elements, then*

$$\prod_{j \in I}(A + jd) \ne cy^r \quad \text{for all } c, y \in \mathbb{Z}_{>0} \text{ with } P(c) \le Ck.$$

In particular, for $\varepsilon \ge 1/10$ one may take $\delta = 1/102$. The threshold is independent of A and r.

Proof. Choose fixed real numbers $a, b > 0$ such that

$$a \le \varepsilon, \qquad \frac{7}{2}a + 6b < 1, \qquad \delta < \frac{ab}{1+a}. \tag{4.7}$$

Such a choice exists by the definition of δ_{ε}: the maximum of $a(1 - \frac{7}{2}a)/(6(1+a))$ on $0 < a \le \varepsilon$ occurs at $a = a_{\varepsilon}$. All estimates below are uniform in A and in the integer $r \ge 2$.

Suppose that a set I of at least $(1-\delta)k$ indices satisfies the representation in (i). Replace each a_j by the rth-power-free part of $A+jd$. For every prime $p \le Ck$ dividing one of these terms, remove one index in I maximizing $v_p(A+jd)$. Let J be the remaining set and $m = |J|$. Then

$$m \ge (1-\delta)k - \pi(Ck) = (1-\delta-o(1))k, \qquad \prod_{j\in J} a_j \mid (k-1)!. \tag{4.8}$$

Indeed, if j_p is a removed maximizing index, then $p \nmid d$ and $v_p(A+jd) \le v_p(j-j_p)$ for every remaining j. The product of the nonzero distances from j_p, on both sides, divides $j_p!(k-1-j_p)!$, which divides $(k-1)!$. In particular,

$$v_p(a_j) \le \left\lfloor \frac{\log(k-1)}{\log p} \right\rfloor \qquad (j \in J).$$

Put $\alpha = k^a$, $\beta = k^{-b}$, and $U = \{j \in J : a_j \le \alpha k\}$. We claim that at most

$$O_d(\alpha^{7/2}\beta^{-5}) \tag{4.9}$$

primes in $[\beta k, k)$ divide two of the cofactors indexed by U. For each such prime p, select an ordered pair of distinct indices (i,j). There are at most $(\alpha/\beta)^2$ possible ordered pairs $(a_i/p, a_j/p)$. Fix such a pair (h,h') and one prime p with its associated (x_i,x_j). For any other prime q with the same cofactor pair, write its associated variables as (x_u,x_v). For sufficiently large k, all four variables lie in

$$L = (A/(\alpha k))^{1/r} \le x \le R = (2A/(\beta k))^{1/r},$$

and

$$|hx_i^r - h'x_j^r| \le d/\beta, \qquad |hx_u^r - h'x_v^r| \le d/\beta.$$

Multiplying by x_v^r and x_j^r, respectively, and subtracting gives

$$h\left|(x_ix_v)^r - (x_jx_u)^r\right| \le \frac{4dA}{\beta^2 k}.$$

Consequently

$$|x_ix_v - x_jx_u| \le \frac{4d}{r}\alpha^{2-2/r}\beta^{-2}(A/k)^{-1+2/r} \le 2d\alpha\beta^{-2}.$$

The last inequality uses $A/k \ge \alpha$ and $-1+2/r \le 0$. If $e = \gcd(x_i,x_j)$, then pe^r divides the difference of the two corresponding progression terms and is coprime to d. Thus $pe^r \le k-1$ and $e \le \beta^{-1/r}$. For a fixed integer determinant $x_ix_v - x_jx_u$, its solutions (x_u,x_v) lie on an arithmetic line whose coordinate steps are x_i/e and x_j/e. The number lying in $[L,R]^2$ is at most

$$2Re/L + 1 \le 2(2\alpha)^{1/r}\beta^{-2/r} + 1 \le 2\sqrt{2\alpha}\,\beta^{-1} + 1.$$

Since $\gcd(A,d) = 1$, each x_j is coprime to d. The variables x_j, $j \in U$, are therefore pairwise distinct: equality of two would give $x_j^r \mid i-j$, although $x_j^r \ge A/(\alpha k) \ge k > |i-j|$. Thus a pair (x_u,x_v) cannot be assigned to two different primes. Counting the cofactor pairs, determinants, and points on each line proves (4.9).

Since $b < 1/6$, every prime $p \ge \beta k$ has exponent at most one in each retained a_j. An exceptional prime from (4.9) divides at most $2/\beta$ terms; every other prime in $[\beta k, k)$ occurs at most once in the product over U. No prime at least k divides a retained cofactor. Hence

$$\begin{aligned}\sum_{j\in U} \log a_j &\le k \sum_{p \le \beta k} \frac{\log p}{p-1} + \sum_{p<k} \log p + O_d(\alpha^{7/2}\beta^{-6}\log k) \\ &\le (1-b)k\log k + o(k\log k).\end{aligned}$$

Here (4.7) makes the last error $o(k\log k)$; the effective prime estimates are those of [42, Theorems 4 and 6].

All cofactors a_j, $j \in J$, are distinct. Otherwise, for $a_i = a_j = c$,

$$d|i-j| = c|x_i^r - x_j^r| \geq rc^{1/r}A^{1-1/r} \geq 2\sqrt{A} > dk,$$

a contradiction. The uniform Stirling bound

$$\log(u!) \geq u\log k - O(k) \qquad (0 \leq u \leq k)$$

therefore shows that $|U| \leq (1-b+o(1))k$. Writing $W = J \setminus U$, we obtain $|W| \geq (b-\delta-o(1))k$, and then

$$\begin{aligned}\sum_{j\in J} \log a_j &\geq \log(|U|!) + (1+a)|W|\log k \\ &\geq \big(1+ab-(1+a)\delta - o(1)\big)k\log k.\end{aligned}$$

This contradicts (4.8), since $ab > (1+a)\delta$. This proves (i).

Every index excluded from (i) has a prime $p > Ck$ whose valuation in that term is not divisible by r. Such a prime divides no other progression term, because $p > Ck \geq dk > d|i-j|$. Choosing one for each excluded index proves (ii). The same uniqueness shows that a product as in (iii) would force every selected index to satisfy (i), a contradiction. Finally, if $\varepsilon \geq 1/10$, the choices $a = 1/10$, $b = 27/250$, and $\delta = 1/102$ satisfy (4.7): indeed, $(7/2)a + 6b = 499/500 < 1$ and $ab/(1+a) = 27/2750 > 1/102$. Every limiting estimate used above has an effective error bound, proving effectivity. □

Theorem 4.6(iii) allows a fixed positive proportion of arbitrary omissions. It does not settle the corresponding problem for unions of widely separated intervals, or the problem of powerful products: a valuation not divisible by r need not equal one.

4.2. **Local cycles and primitive groups.** We first obtain a large prime cycle when the parameter is at most cubic in the degree. For larger parameters, the local packets give elements with small support. We combine these with a progression estimate and the primitive-group theorem of Burness and Guralnick. Irreducibility is assumed only in the statements that require transitivity.

4.2.1. *A first parameter range.* For a prime close to the degree, the absence of a square multiple in the parameter interval produces the required prime cycle.

Lemma 4.7. *Let $n/2 < p < n$ be prime. If no integer in $[s, s+n-1]$ is divisible by p^2, the p-adic Newton polygon of $H_{n,s}$ has an edge of width p and slope $-1/p$. In particular, p divides $|G_{n,s}|$.*

Proof. Write $n = p + b$, with $0 \leq b < p$. The coefficient calculation (3.31), and the two polygons in the proof of Proposition 3.13, show that exactly p roots have valuation $1/p$. A corresponding local ramification index is divisible by p, hence so is the order of the global Galois group. This is the Newton-index argument of [28, Theorems 2.1 and 2.2]. □

The obstruction in the lemma is a square multiple in a short interval. Such multiples cannot occur simultaneously for all primes close to n unless s is sufficiently large.

Proposition 4.8. *There is an absolute effective integer n_{cub} such that, if $n \geq n_{\mathrm{cub}}$, $H_{n,s}$ is irreducible over $\mathbb{Q}$, and*

$$1 \leq s \leq \frac{n^3}{10\log n},$$

then $G_{n,s}$ contains A_n.

Proof. Put $u = \log n$ and

$$\mathcal{P} = \{p \text{ prime} : 9n/10 < p < n-2\}.$$

The effective prime number theorem gives

$$|\mathcal{P}| > \frac{n}{20u} \tag{4.10}$$

for all sufficiently large n. For example, this follows directly from the effective bounds for ϑ in [14, Theorem 4.2], after removing the at most three primes in the upper endpoint interval.

Suppose every $p \in \mathcal{P}$ has a square multiple $k_p p^2 \in [s, s+n-1]$. Distinct primes have distinct multipliers: if $p < q$ had the same multiplier k, then

$$k(q^2 - p^2) \geq q^2 - p^2 > 2p > n - 1,$$

which is impossible for two integers in this interval. The multipliers all lie in

$$\left[\frac{s}{n^2}, \frac{100(s+n-1)}{81n^2}\right].$$

The number of integers in this real interval is at most its length plus one. Consequently

$$|\mathcal{P}| \leq \frac{19s}{81n^2} + \frac{100}{81n} + 1 \leq \frac{19n}{810u} + \frac{100}{81n} + 1 < \frac{n}{20u}$$

for sufficiently large n, contradicting (4.10).

Choose $p \in \mathcal{P}$ for which there is no square multiple. Lemma 4.7 gives $p \mid |G_{n,s}|$. Cauchy's theorem supplies an element of order p, necessarily a single p-cycle because $2p > n$. Since irreducibility makes the root action transitive and $p > n/2$, this action is primitive. Indeed, in a nontrivial block system an order-p element either moves at least p whole blocks, requiring at least $2p$ points, or fixes every block and has its p-cycle inside one block, requiring a block of size at least $p > n/2$; both alternatives are impossible. Jordan's theorem now gives $G_{n,s} \supseteq A_n$, since $p < n-2$; equivalently, apply [28, Theorem 2.2]. Every numerical threshold used above is effective. □

4.2.2. *Small supports and Cartesian products.* The progression estimate first gives small nonidentity permutations uniformly in the parameter. No rate of decay is needed for the subsequent argument.

Proposition 4.9. *For every fixed $\delta \in (0,1)$ there is an effective n_δ such that*

$$\mu(G_{n,s}) \leq \delta n$$

whenever $n \geq n_\delta$, $s \geq 1$, and $H_{n,s}$ is irreducible.

Proof. For $s \leq n^3/(10 \log n)$, Proposition 4.8 gives $G_{n,s} \supseteq A_n$ in sufficiently large degree. A 3-cycle has support $3 \leq \delta n$ once n is large enough.

Suppose therefore that $s > n^3/(10 \log n)$, put $k = \lfloor \delta n/2 \rfloor$, and assume $\mu(G_{n,s}) > \delta n$. For each width $N = 2, 4, \ldots, 2k$ and each prime $p > n$ dividing $s + n - N$, Proposition 3.2 would give a nonidentity element of support $N \leq \delta n$ unless $N \mid v_p(s+n-N)$. Thus all these valuations are even.

The resulting nodes form a progression of length k and step 2. Divide its terms by $h = \gcd(s+n, 2)$. Its starting point and step are

$$A = \frac{s+n-2k}{h}, \qquad d = \frac{2}{h} \in \{1, 2\}, \qquad \gcd(A, d) = 1.$$

Every term is a square times an n-smooth integer. Choose a fixed integer $C \geq 4/\delta$; then $n \leq Ck$ for large n. Moreover $A \geq s/2 > n^3/(20 \log n) > k^{5/2}$ for large n. Theorem 4.6(i), with $\varepsilon = 1/2$, $\delta = 1/102$, and $r = 2$, contradicts the fact that all k indices qualify. □

The next observation relates fixed-point counts to divisors. Its strength is that it applies to the full symmetric group on each coordinate, irrespective of the smaller group acting there.

Lemma 4.10. *Let $m \geq 2$, $a \geq 2$, and $n = m^a$. In the product action of $S_m \wr S_a$ on $\{1, \dots, m\}^a$, an element fixing at least $15n/16$ points has trivial coordinate permutation. Its number of fixed points is a product $f_1 \cdots f_a$ with $15m/16 \leq f_i \leq m$. In particular it has a divisor in $(m/2, m]$.*

Proof. A cycle of $r \geq 2$ coordinates permits at most m choices for those entries of a fixed tuple, rather than m^r. A nontrivial coordinate permutation therefore has fixed-point ratio at most $1/m \leq 1/2$. In the base group the fixed-point ratio is $\prod_i (f_i/m)$. Since each factor lies in $[0, 1]$, a product at least $15/16$ forces each factor to be at least $15/16$. □

Ford's divisor estimate makes the set of possible fixed-point counts in this lemma sparse when m grows. This excludes the whole product action, including its odd-base cases.

Proposition 4.11. *For all sufficiently large n, effectively and uniformly in $s \geq 1$ with $H_{n,s}$ irreducible, the root action of $G_{n,s}$ is not permutation-isomorphic to a subgroup of $S_m \wr S_a$ in its product action, for any $m \geq 2$, $a \geq 2$, $n = m^a$.*

Proof. In this action a nontrivial coordinate permutation moves at least $(1 - 1/m)n$ points, and a nontrivial base element moves at least $2n/m$ points. Thus the minimal degree is at least $n \min\{1-1/m, 2/m\}$. Proposition 4.9 implies that $m \to \infty$ along any sequence of such exceptional actions with $n \to \infty$.

For large n, the displayed lower bound for the support exceeds 3 for every $m \geq 2$, $a \geq 2$. Thus the product action cannot contain A_n. Proposition 4.8 again permits us to assume $s > n^3/(10 \log n)$. Put $k = \lfloor n/32 \rfloor$. For a width $N \in \{2, 4, \dots, 2k\}$ set $j = n - N$. If $p > n$ divides $s + j$ and its inertia is nontrivial, that inertia has support $N \leq n/16$. Lemma 4.10 implies that j has a divisor in $(m/2, m]$.

Let $H(x, y, z)$ count the positive integers at most x with a divisor in $(y, z]$. Ford proved the uniform estimate

$$H(x, y, 2y) \ll \frac{x}{(\log y)^{\kappa} (\log \log y)^{3/2}}, \qquad 3 \leq y \leq \sqrt{x}, \quad \kappa = 1 - \frac{1 + \log \log 2}{\log 2} > 0; \tag{4.11}$$

see [25, Theorem 1(v) and Corollary 2]. Its upper bound is effective. Since $a \geq 2$, we can apply it with $x = n$ and $y = m/2$. As $m \to \infty$, the number of exceptional labels j is $o(n) = o(k)$.

At every other label all inertia at primes above n is trivial. Proposition 3.2 then shows that every such prime has valuation divisible by the even integer N. Consequently all but $o(k)$ terms of

$$s + n - 2k, \ s + n - 2k + 2, \dots, s + n - 2$$

are squares times n-smooth integers. Divide by $h = \gcd(s + n, 2)$ to obtain a progression with step $d = 1$ or 2, coprime starting point $A \geq s/2 > k^{5/2}$, and length k. For large n, $n \leq 33k$. Theorem 4.6(i), with $C = 33$, $r = 2$, $\varepsilon = 1/2$, and $\delta = 1/102$, contradicts this density. For effectivity, first use (4.11) to choose a fixed m_0 for which the exceptional proportion is smaller than $1/102$. Then apply Proposition 4.9 with a fixed positive support proportion smaller than $\min_{2 \leq m < m_0} \min\{1 - 1/m, 2/m\}$ to exclude the remaining values of m. This gives a single effective threshold. □

4.2.3. *Primitive groups.* After Cartesian products have been excluded, the primitive-group classification leaves actions of symmetric or alternating groups on subsets. Their homogeneous permutations have a simple restriction.

Lemma 4.12. *Suppose $2 \leq \ell < m/2$. In the action of S_m on the ℓ-element subsets of $\{1, \dots, m\}$, a homogeneous permutation with fixed-point ratio at least $15/16$ cannot have even nontrivial cycle length greater than two.*

Proof. Let $\sigma \in S_m$ move u letters, and let I be a uniformly chosen ℓ-element subset. Counting the contributions of the moved letters to the symmetric difference gives

$$\mathbb{E}|I \triangle \sigma(I)| = \frac{2u\ell(m-\ell)}{m(m-1)}.$$

Since the symmetric difference is at most 2ℓ and is zero on fixed subsets,

$$1 - \mathrm{fpr}(\sigma) \geq \frac{u(m-\ell)}{m(m-1)} > \frac{u}{2m}.$$

Thus $u < m/8$. In particular there are at least ℓ fixed letters. Selecting one letter from a nontrivial letter cycle of length r, together with $\ell - 1$ fixed letters, gives a subset orbit of length r. If the subset action is homogeneous of length q, every nontrivial letter cycle therefore has length q. If $q > 2$ is even, select two opposite letters from a q-cycle and $\ell - 2$ fixed letters. Their subset orbit has length $q/2 > 1$, contradicting homogeneity. □

The lemma converts odd valuations into forbidden permutations on a full progression of widths.

Proposition 4.13. *For all sufficiently large n, effectively and uniformly in $s \geq 1$ with $H_{n,s}$ irreducible, its root action is not a subgroup of the action of S_m on ℓ-element subsets with $2 \leq \ell < m/2$.*

Proof. The small-parameter case follows from Proposition 4.8, since a proper subset action has order at most $m! < |A_n|$ for sufficiently large $n = \binom{m}{\ell}$. Suppose $s > n^3/(10 \log n)$ and put $k = \lfloor n/64 \rfloor$. At a width $N = 4, 8, \ldots, 4k$, an odd valuation e at a prime $p > n$ gives inertia with

$$g = \gcd(N, e) \text{ odd}, \qquad q = N/g \equiv 0 \pmod 4.$$

The inertia is nonidentity, homogeneous, and has fixed-point ratio at least $15/16$. Lemma 4.12 excludes it. Therefore every valuation at a prime above n is even in every term of

$$s + n - 4k,\ s + n - 4k + 4, \ldots, s + n - 4.$$

Divide by $h = \gcd(s + n, 4)$. The resulting progression has step $d = 4/h \in \{1, 2, 4\}$, starting point $A = (s + n - 4k)/h$ coprime to d, and all terms squares times n-smooth integers. For large n, we have $n \leq 65k$ and $A \geq s/4 > k^{5/2}$. Apply Theorem 4.6(i) with $C = 65$, $r = 2$, $\varepsilon = 1/2$, and $\delta = 1/102$. □

We can now apply the primitive-group theorem. The inequality in that theorem is strict, so the numerical margin below also handles elements of order two.

Theorem 4.14. *For all effectively sufficiently large n and every positive integer s, if $G_{n,s}$ is primitive, then $A_n \leq G_{n,s}$.*

Proof. Primitivity includes transitivity, so $H_{n,s}$ is irreducible. By Proposition 4.9, a sufficiently large $G_{n,s}$ has a nonidentity element of support at most $n/3$. A suitable nonidentity power has prime order r and no larger support. Its fixed-point ratio is at least $2/3 > 1/\sqrt{r+1}$. Burness and Guralnick [7, Corollary 2] imply that the primitive action has the form

$$(A_m)^a \leq G_{n,s} \leq S_m \wr S_a, \qquad n = \left(\binom{m}{\ell}\right)^a, \qquad 1 \leq \ell < m/2,$$

where each coordinate is the action on ℓ-element subsets and the wreath product acts on the Cartesian product of the coordinate sets. The middle-subset action $\ell = m/2$ is imprimitive, since complementary subsets form blocks, so it does not occur here. Proposition 4.11 excludes $a \geq 2$. Proposition 4.13 excludes $\ell \geq 2$. The remaining action has $a = \ell = 1$, so $G_{n,s} \supseteq A_n$. □

4.3. **Invariant partitions.** We exclude invariant partitions in three steps. Progressions of cubes rule out blocks of size two. Linear forms in logarithms bound the parameter when both the block size and the number of blocks are at least three. The partition energy then excludes all partitions in the complementary range. Only partitions into two large blocks remain for the next section.

4.3.1. *Blocks of size two.* For blocks of size two, an odd packet cannot support inertia whose nontrivial cycles have length divisible by three.

Lemma 4.15. *There is an effective absolute integer n_0 such that, if $n \ge n_0$ and $s > n^3/(10\log n)$, then $G_{n,s}$ preserves no partition of the roots into blocks of size two.*

Proof. Suppose such a partition exists. Put $k = \lfloor n/12 \rfloor$ and use the odd widths $N_t = 3(1+2t)$, $0 \le t < k$, all smaller than $n/2$. If $p > n$ divides $s + n - N_t$ to an exponent e not divisible by 3, Proposition 3.2 gives an inertia permutation whose nontrivial cycles all have length $q = N_t/\gcd(N_t, e)$, with $3 \mid q$. A block fixed by this permutation cannot contain a moved root, since $q > 2$. Every moved block consists entirely of moved roots. Its support is therefore a union of pairs, contradicting its odd size N_t. Thus every valuation above n at these nodes is divisible by 3.

In reverse order the nodes form $A, A+6, \dots, A+6(k-1)$, with $A > s$. Put $g = \gcd(A, 6)$, $A' = A/g$, and $d = 6/g$. Then $\gcd(A', d) = 1$, and every term $A' + jd$ is a cube times an n-smooth positive integer. For all sufficiently large n, we have $n \le 13k$ and

$$A' > s/6 > \frac{n^3}{60\log n} > k^{5/2}.$$

Theorem 4.6(i), with $C = 13$, $r = 3$, $\varepsilon = 1/2$, $\delta = 1/102$, and $d \in \{1, 2, 3, 6\}$, contradicts the fact that all k terms qualify. The four possible steps give a single effective threshold. □

4.3.2. *A parameter bound for invariant partitions.* It is not necessary to discard a whole node for each small prime. Instead, assign each small prime to one node where its valuation is maximal. A pair of nodes with a common large exponent then has only a bounded number of exceptional prime factors.

Proposition 4.16. *There are effective absolute constants $C_1, n_3 > 0$ such that, whenever $n \ge n_3$ and $G_{n,s}$ preserves a partition with block size*

$$3 \le b \le n/3,$$

one has

$$\log s \le C_1 (\log n)^9.$$

Irreducibility is not required for this assertion.

Proof. Put $a = n/b$, $u = \log n$, and $L = \log s$. We may assume $L > 2u$, since otherwise the conclusion holds after increasing C_1. For every prime

$$n/3 < P \le n/2$$

use the two widths P and $2P$. They are distinct across all prime groups. Since $a, b \ge 3$ and $ab = n$, we have $\max\{a, b\} \le n/3 < P$. Thus P does not divide $(b!)^a a!$, the order of the partition stabilizer. If a prime $p > n$ occurs in either corresponding node to an exponent not divisible by P, Proposition 3.2 supplies an inertia element whose order is divisible by P, a contradiction. Therefore

$$z_{P,\ell} := s + n - \ell P = a_{P,\ell} x_{P,\ell}^P, \qquad P(a_{P,\ell}) \le n, \qquad \ell \in \{1, 2\},$$

where each $a_{P,\ell}$ is Pth-power-free.

For every prime $p \le n$ dividing at least one selected node, choose one node $z_{P,\ell}$ where $v_p(z_{P,\ell})$ is maximal, and assign p to that node. Let $\mathcal{E}_{P,\ell}$ be its assigned primes. Define

$$r_{P,\ell,p} = v_p(a_{P,\ell}) \quad (p \in \mathcal{E}_{P,\ell}), \qquad d_{P,\ell} = a_{P,\ell} \prod_{p \in \mathcal{E}_{P,\ell}} p^{-r_{P,\ell,p}}.$$

These are positive integers, and $0 \le r_{P,\ell,p} < P$. The maximal-valuation argument gives

$$\prod_{P,\ell} d_{P,\ell} \mid (n-1)!. \tag{4.12}$$

This is the allocation assertion of Lemma 3.19: the remaining cofactor at each node divides its unassigned small-prime part.

Let R be the number of prime groups. The effective prime number theorem gives

$$R = \left(\frac{1}{6} + o(1)\right)\frac{n}{u}, \qquad \pi(n) = (1+o(1))\frac{n}{u}.$$

At most $\pi(n)/7$ groups have seven or more assigned primes on their two nodes. By (4.12), at most $n/(1000u)$ groups satisfy

$$\log d_{P,1} + \log d_{P,2} > 1000u^2.$$

Since

$$\frac{1}{6} - \frac{1}{7} - \frac{1}{1000} > 0,$$

there is, for all sufficiently large n, a prime group with at most six assigned primes and

$$\log d_{P,1} + \log d_{P,2} \le 1000u^2.$$

Write its assigned primes as $p_1, \dots, p_h$, where $h \le 6$. They are distinct, because every small prime was assigned to only one node. For suitable integers c_j with $|c_j| < P$ we have

$$\frac{z_{P,1}}{z_{P,2}} = \frac{d_{P,1}}{d_{P,2}} \left(\frac{x_{P,1}}{x_{P,2}}\right)^P \prod_{j=1}^{h} p_j^{c_j}.$$

Taking real logarithms gives a nonzero linear form $\Lambda = \log(z_{P,1}/z_{P,2})$ satisfying

$$0 < |\Lambda| \le n/s.$$

The rational bases have logarithmic heights at most

$$1000u^2, \qquad \frac{\log(s+n)}{P} \le \frac{2L}{P}, \qquad u, \dots, u,$$

respectively. Omit any base equal to one and any term with zero coefficient. The number of logarithms is at most eight and all integer coefficients have modulus at most P.

If only one logarithm remains, its elementary rational-height bound gives the inequality below directly. Otherwise Matveev's theorem [38, Corollary 2.3], in degree one with coefficient bound $B^* \le P$, gives

$$L - u \le C_2 u^9 \max\left\{1, \frac{L}{P}\right\} \le C_3 u^9 \max\left\{1, \frac{L}{n}\right\}.$$

Here the factors u^2, at most six factors u, and the coefficient factor $\log(eP) = O(u)$ account for the exponent nine. The maximum also covers the case $x_{P,1} = x_{P,2}$, when that logarithm is omitted. Thus no assumption that a large-power part is nontrivial is needed.

Since $L > 2u$, after changing the absolute constant we obtain

$$L \le C_4 u^9 \max\left\{1, \frac{L}{n}\right\}.$$

For $n > 2C_4u^9$, the alternative $L \geq n$ is impossible. Hence $L < C_4u^9$, proving the assertion. The prime number theorem and the logarithmic-form estimate both have effective constants. □

In particular, for partitions whose block size and number are both at least three, it now suffices to treat a parameter range of fixed polynomial growth in $\log n$. This reduction is uniform in the number and size of the blocks. It does not by itself exclude such partitions in that remaining parameter range.

4.3.3. *The energy of a partition.* The matrix energy identity applies even when individual blocks are not defined over $\mathbb{Q}$. This is the reason to use the entire invariant partition in place of a single block.

Suppose now that the Galois group preserves a partition into a blocks of size b, where $n = ab$ and $a, b \geq 2$. Index the roots by their positions in this partition and define

$$Q_{ij} = \frac{\mathbf{1}_{\{i,j \text{ in the same block}\}}}{b} - \frac{1}{n}.$$

This is the orthogonal projection onto the block-constant vectors orthogonal to the constant vector. It has rank $a - 1$, constant diagonal $(a - 1)/n$, and is invariant under the Galois group.

Lemma 4.17. *Put $u = \log n$, $T = \log s$, and*

$$E_p = \sum_{i \neq j} Q_{ij} v_p(\alpha_i - \alpha_j) + \sum_i Q_{ii}(v_p(\alpha_i) + \epsilon_p).$$

Then $E_p \geq 0$. For $s \geq n$ and $\log n \geq 10000$,

$$\mathcal{E} := \sum_p E_p \log p < (a - 1)\left(\frac{T}{2} + \frac{3u}{2} + \log 48\right). \tag{4.13}$$

If $p > n$ divides $s + j$, set $N = n - j$ and $e = v_p(s + j)$, and let k_i count the roots of positive valuation in the ith block. Then

$$E_p = \frac{e}{N}\left(\frac{1}{b}\sum_{i=1}^{a} k_i^2 - \frac{N^2}{n}\right). \tag{4.14}$$

Proof. The displayed matrix Q is rational, positive semidefinite, and Galois invariant, and it annihilates the constant vector. Apply Lemma 3.5, with $\operatorname{tr} Q = a - 1$. It gives nonnegativity and the upper bound (4.13). For a packet C of size N, $\mathbf{1}_C^{\mathsf{T}} Q \mathbf{1}_C = b^{-1}\sum_i k_i^2 - N^2/n$. The exact packet identity (3.10) proves (4.14). □

An order-P power of a homogeneous inertia permutation has the same support. When P exceeds the number of blocks, it fixes every block and hence forces packet occupations to be multiples of P.

Lemma 4.18. *Suppose $p > n$ divides the node corresponding to a width $N = \ell P$, where P is prime and $P \nmid e = v_p(s + n - N)$. If $P > a$ and $a \nmid \ell$, then*

$$E_p \geq \frac{eP^2(a - 1)}{nN}. \tag{4.15}$$

If $P > b$ and $b \nmid N$, such a prime contribution is impossible.

Proof. The homogeneous inertia cycle length $q = N/\gcd(N, e)$ is divisible by P. Raising its generator to the power q/P gives an order-P permutation with the same support. If $P > a$, it fixes every block. Write $k_i = Pt_i$, where $\sum_i t_i = \ell$. If $\ell = ah + r$ with $0 < r < a$, minimization over integral occupations gives

$$\frac{1}{b}\sum_i k_i^2 - \frac{N^2}{n} \geq \frac{P^2 r(a - r)}{n} \geq \frac{P^2(a - 1)}{n}.$$

Equation (4.14) proves (4.15). For the last assertion, $q \geq P > b$, so a fixed block contains no moved point. The support is therefore a union of entire blocks, forcing $b \mid N$, a contradiction. □

We next choose many widths to which this occupation bound applies. Fix $\theta = 101/200$ and put $\delta = \log(1/\theta)$; thus $\delta/2 > 1/3$. For any integer $d \geq 2$, the number of widths

$$N = \ell P \leq n, \qquad P > n^{\theta} \text{ prime}, \qquad d \nmid \ell$$

is at least $(\delta(1 - 1/d) - o(1))n$, uniformly in d. Indeed, the prime $P > \sqrt{n}$ is unique, and this number equals

$$\sum_{n^{\theta} < P \leq n} \left(\left\lfloor \frac{n}{P} \right\rfloor - \left\lfloor \frac{n}{dP} \right\rfloor \right) \geq n(1 - 1/d) \sum_{n^{\theta} < P \leq n} \frac{1}{P} - \pi(n).$$

The prime reciprocal sum tends effectively to δ, and $\pi(n) = o(n)$. These are the usual effective consequences of the prime number theorem; all errors here are independent of d.

Proposition 4.19. *For all effectively sufficiently large n, if*

$$s > \frac{n^3}{10 \log n}, \qquad \frac{\log(s+n)}{\log n} < n^{101/200},$$

then $G_{n,s}$ preserves no partition into equal blocks with at least two blocks and at least two roots per block.

Proof. Suppose there are a blocks of size b. First let $a \leq n^{\theta}$. Choose the widths just counted with $d = a$. Every prime $p > n$ dividing a selected node has exponent $e < n^{\theta} < P$. Lemma 4.18 therefore gives $E_p > e(a-1)n^{2\theta-2}$.

Delete one selected node with maximal valuation for every prime at most n. At most $\pi(n)$ nodes are lost, and the product of the small-prime parts of the remaining nodes divides $(n-1)!$. This is Lemma 3.19. Consequently the logarithmic mass W of the retained prime powers with primes exceeding n satisfies

$$W \geq (\delta/2 - o(1))nT - nu \geq cnT$$

for an absolute $c > 0$. Here $T > 3u - \log(10u)$ and $\delta/2 > 1/3$. Nonnegativity of the other local energies gives $\mathcal{E} > c(a-1)n^{2\theta-1}T$, contradicting (4.13), which is less than $2(a-1)T$ in this range.

If $a > n^{\theta}$, then $b < n^{1-\theta} < n^{\theta}$. Choose the widths with $d = b$. Since $P > b$, $b \nmid \ell$ implies $b \nmid \ell P$. The last assertion of Lemma 4.18 says that every selected node has no prime divisor exceeding n. This contradicts the same lower bound $W \geq cnT$. □

4.4. **Laurent interpolation and quadratic block fields.** Let E be the splitting field of an irreducible polynomial, and suppose that its Galois group preserves a partition into two blocks. The setwise stabilizer G_B of either block has index two; its fixed field $K = E^{G_B}$ is the *quadratic block field*. Every root stabilizer is contained in G_B, so K lies in each root field. A bounded trace treats the real quadratic case. For the imaginary quadratic case, we construct integral polynomials whose block traces become small at infinity.

4.4.1. *The real quadratic case.* The centered block trace is bounded at both real embeddings. Its norm allows us to combine this bound with the fibers at 0 and -1.

Lemma 4.20. *Let $n = 2b \geq 4$ and suppose that $H_{n,s}$ is irreducible. If its Galois group preserves two blocks of size b and the corresponding quadratic field is real, then*

$$\log s < 2n \log n.$$

Proof. Let K be the quadratic block field. For one block B, put $t = \sum_{\alpha\in B}(\alpha + s)$. This is an algebraic integer in K, whose conjugate is $-t$, since all centered roots sum to zero. Both traces are real, and Proposition 2.2 gives $|t| < b^2$.

If $t \neq 0$, then $A = N_{K/\mathbb{Q}}(t) = -t^2$ is a nonzero integer with $|A| < b^4$. For $p^e \| s$, the congruence $H_{n,s}(Y - s) \equiv Y^n \pmod{s}$ implies that every centered root has valuation at least e/n, at every extension of v_p. The two conjugate traces therefore give $v_p(A) \geq 2e/n = e/b$. Thus $s \mid A^b$ and

$$\log s \leq b \log |A| < 4b \log b < 2n \log n.$$

If $t = 0$, the uncentered block trace is the integer $-bs$. The congruence $H_{n,s}(X) \equiv X^{n-1}(X - n) \pmod{s+1}$ and Lemma 2.3, applied with $A = b$ and $c = n = 2b$, give $s + 1 \mid b^n$. That lemma requires only an integral selected trace, not a rational factor. Hence $\log s < n \log b < 2n \log n$ in this case as well. □

4.4.2. *Laurent interpolation and cyclic intermediate fields.* The imaginary quadratic case requires integral polynomials whose negative odd Laurent coefficients vanish and whose first positive odd coefficient is prescribed. We first prove the required surjectivity over the ground field; we then bound denominators and coefficient sizes. The next theorem gives a general criterion for the first step. At a fiber with a common ramification index q, one may prescribe a finite string of Laurent coefficients in a chosen nonzero congruence class modulo q. The obstruction is a cyclic extension between intermediate fields of the cover.

Let k be an algebraically closed field of characteristic zero, let C be a smooth projective connected curve of genus g, and let $T : C \to \mathbb{P}^1_k$ have degree $n = qb$, where $q, b \geq 2$. Suppose

$$(T)_\infty = qE, \qquad E = Q_1 + \cdots + Q_b,$$

with distinct points Q_i. Choose formal local parameters v_i with $T = v_i^{-q}$. Write $K = k(C)$ and $F = k(T)$, and put

$$L(DE) = \{h \in K : (h) + DE \geq 0\} \cup \{0\}.$$

For a finite branch value t, let e_P be the ramification index at P above t. For $m \geq 1$ define

$$d_m = \sum_{t \text{ finite branch value}} \max_{P|t} \left\lfloor \frac{m(e_P - 1)}{e_P} \right\rfloor. \tag{4.16}$$

Theorem 4.21. *Fix $1 \leq a < q$, and put $e = q/\gcd(a, q)$. Let $D \geq 0$ be divisible by q, with $Db > 2g - 2$, and suppose*

$$\left\lceil \frac{D + q + m}{q} \right\rceil > d_m \qquad (1 \leq m \leq n - 1,\ e \nmid m). \tag{4.17}$$

If the coefficient map

$$\begin{aligned} \mathcal{J}_{D,a} : L(DE) &\longrightarrow k^{b(D/q+1)}, \\ h &\longmapsto \left([v_i^{-D+a+qj}]h\right)_{\substack{1\leq i\leq b \\ 0\leq j\leq D/q}} \end{aligned} \tag{4.18}$$

is not surjective, then there are intermediate fields

$$F \subseteq M \subsetneq L \subseteq K \quad \text{with} \quad L/M \text{ cyclic of degree } e.$$

In particular, the map is surjective if the monodromy action of T is primitive.

If B is the number of finite branch values, the choice $D = qB(n - 2)$ satisfies both numerical hypotheses, for every $1 \leq a < q$.

Proof. We first describe the obstruction to prescribing Laurent coefficients. Let V be the space of all coefficients of $v_i^{-D}, \dots, v_i^{q-1}$, for $1 \le i \le b$, and let $\mathcal{J} : L(DE) \to V$ be the full coefficient map. Its kernel is $L(-qE) = 0$. Since $Db > 2g-2$, Riemann–Roch gives

$$\dim \operatorname{coker} \mathcal{J} = b(D+q) - (Db + 1 - g) = g + qb - 1.$$

The same theorem gives $\dim H^0(C, \Omega_C(qE)) = g + qb - 1$. Each differential in this space defines a functional on V by

$$(h_i)_i \longmapsto \sum_{i=1}^{b} \operatorname{Res}_{Q_i}(h_i \omega).$$

This functional vanishes on global functions by the residue theorem. It determines ω: if it vanishes on every coefficient in V, then the Laurent coefficients of ω from degree $-q$ through degree $D-1$ vanish at every Q_i. Thus $\omega \in H^0(C, \Omega_C(-DE)) = 0$. The dimension count therefore identifies $H^0(C, \Omega_C(qE))$ with the dual of $\operatorname{coker} \mathcal{J}$.

Suppose now that $\mathcal{J}_{D,a}$ is not surjective. Extend a nonzero functional annihilating its image to V by making it zero on the other congruence classes of coefficients. The preceding identification supplies a nonzero differential $\omega \in H^0(C, \Omega_C(qE))$. Set $f = \omega/dT \in K$. At Q_i we have $dT = -q v_i^{-q-1}\, dv_i$, so $f = O(v_i)$. The coefficient restrictions on ω say that, through degree $D+q$, the expansion of f uses only exponents congruent to $-a$ modulo q. Hence, for a primitive qth root of unity ζ,

$$f(\zeta v_i) = \zeta^{-a} f(v_i) + O(v_i^{D+q+1}). \tag{4.19}$$

This is a relation between the local branches over T; it does not assert that $v_i \mapsto \zeta v_i$ extends to an automorphism of C.

Let $1 \le m \le n-1$ with $e \nmid m$. Since $f = O(v_i)$, raising (4.19) to the mth power and summing over the q local branches gives

$$\sum_{j=0}^{q-1} f(\zeta^j v_i)^m = O(v_i^{D+q+m}).$$

The sum is a series in $v_i^q = T^{-1}$. Consequently $\operatorname{Tr}_{K/F}(f^m)$ vanishes at infinity to order at least $\lceil (D+q+m)/q \rceil$.

At a finite point P of ramification index e_P, the differential ω is regular, whereas dT has order $e_P - 1$. In a local parameter with $T - T(P) = u^{e_P}$, the trace retains only powers of u divisible by e_P. Its pole order at $T(P)$ is therefore at most $\lfloor m(e_P-1)/e_P \rfloor$. Thus the total finite pole degree of $\operatorname{Tr}_{K/F}(f^m)$ is at most d_m. The cutoff hypothesis forces

$$\operatorname{Tr}_{K/F}(f^m) = 0 \qquad (1 \le m \le n-1,\ e \nmid m).$$

Since $e \mid n$, Newton's identities now show that

$$\operatorname{Norm}_{K/F}(W - f) \in F[W^e].$$

Let μ_f be the monic minimal polynomial of f over F. The norm is a power of μ_f, so both polynomials have the same set of roots. This set is stable under multiplication by the eth roots of unity. Moreover, none of its roots is zero, since $f \neq 0$. Every such orbit therefore has e elements, and taking the product over these orbits gives $\mu_f \in F[W^e]$.

Put $L = F(f)$ and $M = F(f^e)$. For each eth root of unity ξ, the map $f \mapsto \xi f$ defines an F-automorphism of L fixing M: the image satisfies the same minimal polynomial and already belongs to L. These are e distinct automorphisms, while $[L : M] \le e$ because f satisfies $W^e - f^e$ over M. Thus L/M is cyclic of degree e.

If the monodromy is primitive, K/F has no proper nontrivial intermediate field. The identity $\operatorname{Tr}_{K/F}(f) = 0$ excludes $f \in F$, so $L = K$. But $2 \le e \le q < n$ then gives $F \subsetneq M \subsetneq K$, a contradiction.

For the final assertion, note that $d_m \le B(m-1) \le B(n-2)$. Taking $D = qB(n-2)$ makes every left side in (4.17) strictly larger than $B(n-2)$. The finite ramification contribution is at most $B(n-1)$, and the contribution at infinity is $n-b$. Riemann–Hurwitz therefore gives

$$2g-2 \le B(n-1) - n - b < nB(n-2) = Db,$$

as required. □

Failure does occur for covers with a cyclic intermediate extension. On $C = \mathbb{P}^1_z$, put $U = z + z^{-1}$ and $T = U^q$. Then $n = 2q$, $E = (0) + (\infty)$, and $v = U^{-1}$ is a local parameter at both points of E. For $1 \le a < q$, the differential

$$\omega = d(U^a) = -av^{-a-1}\,dv \in H^0(C, \Omega_C(qE))$$

and the residue theorem give

$$[v_0^a]h + [v_\infty^a]h = 0 \qquad (h \in L(DE)).$$

Thus $\mathcal{J}_{D,a}$ is not surjective for any nonnegative multiple D of q. If $g_0 = \gcd(a,q)$, the intermediate extension $k(U^{g_0})/k(U^q)$ is cyclic of degree q/g_0, as predicted.

For $q = 2$ and $a = 1$, the prescribed powers are $-D+1, -D+3, \dots, -1, 1$. The condition (4.17) becomes

$$Db > 2g-2, \qquad (D+m+3)/2 > d_m \quad (m = 1, 3, \dots, n-1). \tag{4.20}$$

In this case the function f constructed in the proof satisfies

$$f(v_i) = O(v_i), \qquad f(v_i) + f(-v_i) = O(v_i^{D+4}). \tag{4.21}$$

We use this case below. The theorem asserts a necessary field obstruction to failure of interpolation; the presence of a cyclic intermediate extension alone does not imply failure.

4.4.3. *Separating branches at infinity.* Write $n = 2b \ge 4$ and $C_n(Z,S) = C_{n,S}(Z) = H_{n,S}(Z-S)$, and use h_n from (2.16). At infinity set $S = v^{-2}$. The roots have convergent expansions $Z(v,\zeta) = \zeta/v + O(1)$, indexed by the simple roots ζ of h_n, with $Z(-v,\zeta) = Z(v,-\zeta)$. Let $\mathcal{A}^- \subset \mathbb{Q}[T]/(h_n)$ denote the odd subspace, of dimension b.

We seek polynomials whose values on opposite branches have small differences at infinity. The following theorem supplies enough such polynomials to distinguish every selection of one branch from each pair. Its proof uses traces of odd powers and the generic symmetric group.

Theorem 4.22. *Let $D = 2n^2$. Consider the rational linear map from polynomials $P(Z,S)$ of Z-degree less than n and weighted degree at most D, where $\mathrm{wt}(Z) = 1$ and $\mathrm{wt}(S) = 2$, to the coefficients of the odd Laurent powers*

$$v^{-D+1}, v^{-D+3}, \dots, v^{-1}, v^1$$

in $P(Z(v,\zeta), v^{-2})$. Its target is $(\mathcal{A}^-)^{D/2+1}$, and the map is surjective.

In particular there exist b rational polynomials $P_0, \dots, P_{b-1}$ of the stated degrees for which all negative odd coefficients vanish and whose respective coefficients of v^1 are $\zeta, \zeta^3, \dots, \zeta^{2b-1}$. Terms independent of Z may be removed without changing these assertions.

Proof. Let C be the smooth completion of $C_n(Z,S) = 0$ and let E be the sum of its $b = n/2$ points at infinity. The simple Hermite roots show that $(S)_\infty = 2E$. The affine curve is smooth: its possible multiple-root fibers occur at $S = 0, -1, \dots, -(n-2)$, the repeated root is $X = Z - S = 0$, and $\partial H_{n,S}(0)/\partial S = ((S)_n)' \ne 0$ there. Its geometric group is S_n. Eisenstein at $S = 0$ gives transitivity. The $(n-1)$-cycle at $S = -1$ lies in the stabilizer of its fixed root and acts transitively on the other roots. Transitivity of the full group therefore gives double transitivity. Conjugating the transposition at $S = -(n-2)$ then gives every transposition, and hence the group is S_n.

There is one finite branch point of each index $N = 2, \dots, n$. Riemann–Hurwitz gives $g(C) = (b-1)^2$, while the pole budget of Theorem 4.21 is

$$d_m = \sum_{N=2}^{n} \left\lfloor \frac{m(N-1)}{N} \right\rfloor \leq (n-1)(m-1).$$

The choice $D = 2n^2$ satisfies both hypotheses (4.20). Apply Theorem 4.21 with $q = 2$ and $a = 1$ to obtain surjectivity on $L(DE)$.

The affine curve is smooth, so every function regular there belongs to its coordinate ring. Because C_n is monic in Z, such a function has a unique polynomial representative of Z-degree less than n. We claim that this representative lies in $L(DE)$ exactly when its weighted degree is at most D. One implication follows from the pole orders of Z and S. For the other, suppose its largest weight is $w > D$ and let $p_w(T)$ be the corresponding leading polynomial after substituting $Z = T/v$, $S = v^{-2}$. Then $\deg p_w < n$, and every exponent of p_w has the same parity as w. The absence of a pole of order w at each point of E forces p_w to vanish at one root from each opposite pair of Hermite roots. Its parity then makes it vanish at all n roots of h_n. This is impossible for a nonzero polynomial of degree less than n. Thus the intrinsic coefficient map is exactly the stated polynomial map over $\mathbb{C}$. Its matrix over the monomial basis of $\mathbb{Q}[T]/(h_n)$ has rational entries; its full rank over $\mathbb{C}$ therefore gives full rank over $\mathbb{Q}$. Prescribing the coefficient at v yields the polynomials P_j. Terms independent of Z contribute only even Laurent powers and may be removed. □

4.4.4. *Bounding the imaginary quadratic obstruction.* We need quantitative bounds for this construction. Bounds for its denominators and coefficients gives a uniform upper bound for a parameter admitting an imaginary quadratic block field.

We begin with a denominator estimate for the root expansions. The Hermite differential equation makes the estimate independent of a discriminant denominator.

Lemma 4.23. *Let F_n and h_n be as in* (2.17)*, and put $\mathcal{A} = \mathbb{Z}[T]/(h_n)$. The formal branch*

$$T(v) = T + \sum_{k\geq 1} a_k v^k \in (\mathcal{A} \otimes \mathbb{Q})[[v]], \qquad F_n(T(v), v) = 0,$$

satisfies $(3k)!a_k \in \mathcal{A}$ for every $k \geq 1$. Moreover, $(3k)![v^k]T(v)^j \in \mathcal{A}$ for every $j \geq 0$.

Proof. All quotients in this proof are first interpreted in $\mathbb{Q}[T]/(h_n)$; the simplicity of the Hermite roots makes h_n' invertible there. The specific quotients $h_n^{(r)}/h_n'$ have integral representatives. Indeed, their representatives A_r can be defined by

$$A_0 = 0, \qquad A_1 = 1, \qquad A_{r+2} = -TA_{r+1} + (n-r)A_r,$$

using the Hermite differential equation. Thus these quotients do not introduce the denominators of a general inverse of h_n'. Write $F_n(T, v) = \sum_{l\geq 0} F_l(T)v^l$. Expansion of the exponential gives

$$F_l^{(j)}(T) = \sum_{\substack{r_3, r_4, \dots \geq 0 \\ \sum_{m\geq 3}(m-2)r_m = l}} \frac{h_n^{(M+j)}(T)}{\prod_{m\geq 3} m^{r_m} r_m!}, \qquad M = \sum_{m\geq 3} m r_m \leq 3l.$$

The denominator in each summand divides $M!$, by the formula counting permutations of a specified cycle type, and hence divides $(3l)!$. Consequently

$$(3l)!\, F_l^{(j)}/h_n' \in \mathcal{A}.$$

This includes $l = 0$, using the derivative quotients above.

We prove the denominator bound by induction on k. Write $A(v) = \sum_{i\geq 1} a_i v^i$ and expand $F_n(T + A(v), v) = 0$ in the ring $\mathbb{Q}[T]/(h_n)[[v]]$. After division by h_n', the only term involving a_k is a_k itself. Every other contribution to the coefficient of v^k has the form

$$\frac{F_l^{(j)}(T)}{h_n'(T)} \prod_{i\geq 1} \frac{a_i^{r_i}}{r_i!}, \qquad j = \sum_i r_i, \qquad l + \sum_i i r_i = k,$$

and uses only coefficients already covered by the induction. Its denominator divides

$$(3l)! \prod_{i\geq 1} ((3i)!)^{r_i} \prod_{i\geq 1} r_i!.$$

This integer divides $(3k)!$: the quotient counts partitions of a labeled set of size $3k$ into one distinguished block of size $3l$ and r_i indistinguishable blocks of size $3i$ for each i. Hence $(3k)!a_k \in \mathcal{A}$. The same multinomial argument applied to $(T + A(v))^j$ proves $(3k)![v^k]T(v)^j \in \mathcal{A}$ for every $j \geq 0$. □

The following analytic estimates give a common disk for all root branches.

Lemma 4.24. *Let $n \geq 4$, $F(t, v) = F_n(t, v)$, and $h = h_n$. The roots ζ_i of h are simple and purely imaginary, satisfy $|\zeta_i| \leq 2\sqrt{n}$, and are separated by more than $1/(6\sqrt{n})$. On a neighborhood of $|v| \leq r = (1000n^2)^{-1}$, they extend to holomorphic roots $t_i(v)$ of F with $|t_i(v) - \zeta_i| \leq 2n|v|$ and $|t_i(v)| < 3\sqrt{n}$.*

Proof. The roots $\zeta_1, \ldots, \zeta_n$ of h are simple and purely imaginary, with $|\zeta_i| \leq 2\sqrt{n}$. One way to see these facts is to use the skew-symmetric tridiagonal matrix whose adjacent entries are $\sqrt{j}$ and $-\sqrt{j}$, for $1 \leq j < n$; its characteristic polynomial is h. Multiplication by i, followed by a diagonal unitary similarity, gives an irreducible real symmetric tridiagonal matrix. Its eigenvalues are simple, and its norm is at most $2\sqrt{n}$.

The equation $h'' + th' - nh = 0$ also gives

$$|\zeta_i - \zeta_j| > \frac{1}{6\sqrt{n}} \quad (i \neq j). \tag{4.22}$$

Indeed, at a root put $A_k = h^{(k)}(\zeta)/h'(\zeta)$. The recurrence $A_{k+2} = -\zeta A_{k+1} + (n-k)A_k$, with $A_0 = 0, A_1 = 1$, gives $|A_k| \leq (3\sqrt{n})^{k-1}$. For $0 < |z| \leq 1/(6\sqrt{n})$,

$$\left| \frac{h(\zeta + z)}{h'(\zeta) z} - 1 \right| \leq \sum_{k=2}^{n} \frac{2^{1-k}}{k!} < 2(e^{1/2} - 3/2) < 1,$$

so the Taylor quotient cannot vanish.

Set $r = (1000n^2)^{-1}$. The polynomial $F(t, v)$ is the characteristic polynomial of the analytic tridiagonal matrix with diagonal $v(2j - n - 1)$ and adjacent entries

$$\sqrt{j}\sqrt{1 + (n-j)v^2}, \qquad -\sqrt{j}\sqrt{1 + (n-j)v^2}.$$

Here the square roots are the branches equal to 1 at $v = 0$. For $|v| \leq r$, its distance in operator norm from the matrix at $v = 0$ is at most $2n|v|$. Applying the resolvent identity on the circles of radius $1/(18\sqrt{n})$ about the ζ_i shows that each circle contains exactly one eigenvalue. Consequently there are holomorphic branches $t_i(v)$ on $|v| \leq r$ satisfying

$$t_i(0) = \zeta_i, \qquad |t_i(v)| < 3\sqrt{n}.$$

The assertions remain valid on an open neighborhood of this closed disk, since all the preceding norm inequalities are strict.

The bound $|t_i(v) - \zeta_i| \leq 2n|v|$ also follows from the resolvent bound for the normal matrix at $v = 0$: every perturbed eigenvalue lies within the perturbation norm of its spectrum, and the disjoint disks identify the corresponding root. □

Eliminating the odd monomials. The large jet system has a triangular part which can be removed before taking determinants. This reduces the number of rows from order n^3 to order n^2 without changing the proved cutoff.

Put $n = 2b$, let $D = 2m \geq n$, and write $u = v^2$. Let $\mathcal{A} = \mathbb{Q}[T]/(h_n)$. Define the $\mathbb{Q}$-linear map $\mathcal{T}(v) : \mathcal{A} \to \mathcal{A}[[v]]$ on the monomial basis by

$$\mathcal{T}(v)(T^j) = Y(v)^j \pmod{h_n}, \qquad 0 \leq j < n,$$

where $Y(v) = vZ(v,T)$ is the Hermite-limit root series. Split $\mathcal{A} = \mathcal{A}^+ \oplus \mathcal{A}^-$ into even and odd polynomials, with bases $1, T^2, \dots, T^{2b-2}$ and $T, T^3, \dots, T^{2b-1}$. Parity gives block series

$$\mathcal{T}_{--}(v) = \mathcal{O}(u), \qquad \mathcal{T}_{-+}(v) = v\mathcal{B}(u), \qquad \mathcal{O}(0) = I.$$

Define

$$R(u) = u\mathcal{O}(u)^{-1}\mathcal{B}(u) = v\mathcal{O}(v^2)^{-1}\mathcal{T}_{-+}(v). \tag{4.23}$$

Its column corresponding to the constant polynomial is zero.

Lemma 4.25. *Consider a polynomial P with $\deg_Z P < n$ and weighted degree at most $2m$, with no term independent of Z. Write its even and odd monomials as Laurent-polynomial vectors*

$$A_i(u) = p_{2i}(u^{-1})u^{-i} \quad (1 \leq i < b), \qquad A_0 = 0,$$

and

$$B_i^{\mathrm{in}}(u) = p_{2i+1}(u^{-1})u^{-i} \quad (0 \leq i < b).$$

Thus A_i has powers $u^{-m}, \dots, u^{-i}$, whereas B_i^{in} has powers $u^{-(m-1)}, \dots, u^{-i}$. Fix a vector $y \in \mathbb{Q}^b$ in the odd monomial basis. There exists an odd part B^{in} for which the negative odd Laurent coefficients of $P(Z(v,T), v^{-2})$ vanish and its coefficient at v^1 is y if and only if

$$[u^k](R(u)A(u))_i = 0 \quad (1 - i \leq k \leq 0), \qquad [u^1](R(u)A(u))_i = y_i, \quad 0 \leq i < b. \tag{4.24}$$

When it exists, the odd part is unique and is obtained by taking the negative of the terms of $(RA)_i$ with exponents $-(m-1), \dots, -i$. The reduced system (4.24) has exactly $b(b+1)/2$ rows.

For $D = 2n^2$, this reduced map is surjective.

Proof. The odd part, in both the Laurent parameter and the Hermite variable, of the evaluated polynomial is

$$v\big(\mathcal{B}(u)A(u) + u^{-1}\mathcal{O}(u)B^{\mathrm{in}}(u)\big) = v^{-1}\mathcal{O}(u)\big(B^{\mathrm{in}}(u) + R(u)A(u)\big).$$

It equals $vy + O(v^3)$ exactly when

$$B^{\mathrm{in}}(u) + R(u)A(u) = uy + O(u^2),$$

since $\mathcal{O}(0) = I$. The series R starts at order u, so RA has no power below $u^{-(m-1)}$. The allowed coefficients of B_i^{in} cancel precisely the powers through u^{-i}; the remaining conditions are (4.24). There are $i+1$ conditions in component i, giving $b(b+1)/2$ in all.

For $D = 2n^2$, the full odd-jet map of Theorem 4.22 is surjective. Multiplication by $\mathcal{O}(u)^{-1}$ is an invertible triangular change of jet coordinates. The odd-monomial columns occupy exactly the coefficients canceled above, with unit pivots. Passing to the quotient by these columns gives the reduced map (4.24), which is therefore surjective. □

The inverse matrix in (4.23) has a uniform analytic disk. Working in a Hermite quadrature norm avoids a loss caused by the condition number of a monomial Vandermonde matrix.

Lemma 4.26. *Put $r = (1000n^2)^{-1}$. The matrix $R(u)$ is holomorphic on a neighborhood of $|u| \leq r^2$. In the norm induced by Gaussian Hermite quadrature on the even and odd polynomial spaces,*

$$\|\mathcal{O}(v^2)^{-1}\| \leq 2 \qquad (|v| \leq r).$$

In the monomial bases, its entries also satisfy

$$|R_{ij}(u)| \le \exp(6n\log n) \qquad (|u| \le r^2).$$

Moreover every coefficient of u^k in $R(u)$, in the monomial bases above, has denominator dividing $(6k-3)!$ for $k \ge 1$.

Proof. Write the Hermite roots as $\zeta_i = i\eta_i$ with $\eta_i \in \mathbb{R}$. On polynomials of degree below n, use the norm

$$\|q\|^2 = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} |q(ix)|^2 e^{-x^2/2}\, dx.$$

Gaussian quadrature at the n Hermite nodes identifies this norm with a weighted Euclidean norm on the values $q(\zeta_i)$, with positive, symmetric weights. This elementary quadrature identity follows by division by the monic Hermite polynomial and its orthogonality; the weights are positive because they are the integrals of the squares of the cardinal polynomials.

The polynomials $h_k(T)/\sqrt{k!}$ are orthonormal in this norm. Their derivative relation shows that differentiation on degree-below-n polynomials has norm at most $\sqrt{n}$, and its kth power has norm at most $n^{k/2}$.

Lemma 4.24 gives root branches $t_i(v)$ on $|v| \le r$ with

$$\delta_i(v) = t_i(v) - \zeta_i, \qquad \max_i |\delta_i(v)| \le 2n|v|.$$

Let $\mathcal{D}$ denote differentiation in node coordinates. Taylor expansion of each polynomial, which is finite here, therefore gives the operator identity on its node values

$$\mathcal{T}(v) = I + \sum_{k=1}^{n-1} \frac{\operatorname{diag}(\delta_i(v)^k)\mathcal{D}^k}{k!}.$$

It follows that

$$\|\mathcal{T}(v) - I\| \le \exp(2n^{3/2}|v|) - 1 < \tfrac{1}{2}.$$

The projection onto odd polynomials is orthogonal because the quadrature weights are symmetric. Hence the same bound holds for $\mathcal{O}(v^2) - I$, and the geometric-series inverse has norm at most two. Equation (4.23) proves the stated holomorphy of R. The same estimates give

$$\|R(u)\| \le 6n^{3/2}|u| \qquad (|u| \le r^2).$$

To pass to monomial coordinates, each input monomial has norm at most $(2n)^{n/2}$. Each coefficient of a normalized Hermite polynomial $h_k/\sqrt{k!}$ has absolute value at most $\sqrt{n!}$; therefore each monomial coefficient of an output polynomial is at most $n\sqrt{n!}$ times its norm. These estimates imply the displayed bound $\exp(6n\log n)$ for all $n \ge 4$.

By Lemma 4.23, every coefficient of v^k in $\mathcal{T}(v)$ becomes integral after multiplication by $(3k)!$. The substitution $v = w^3$ turns this into integrality of the exponential-generating coefficients. If $U(w) = \sum_{j\ge 0} U_j w^j/j!$ has integral matrix coefficients and $U_0 = I$, the coefficients of its inverse satisfy

$$V_0 = I, \qquad V_j = -\sum_{i=1}^{j} \binom{j}{i} U_i V_{j-i}.$$

They are therefore integral. Products have the same property by the binomial convolution formula. Applying these observations to the odd diagonal block gives the asserted integrality for its inverse and for its product with $\mathcal{T}_{-+}$. The coefficient of $u^k = v^{2k}$ in (4.23) is the coefficient of v^{2k-1} in $\mathcal{O}(v^2)^{-1}\mathcal{T}_{-+}(v)$, proving the denominator bound $(6k-3)!$. □

The parameter bound. We construct integral polynomials with small differences on paired branches and apply them to the two blocks.

Proposition 4.27. *Let $n = 2b \geq 4$ and $s \in \mathbb{Z}_{>0}$. If the Galois group of $H_{n,s}$ preserves two blocks of size b, and its action on these blocks defines an imaginary quadratic field, then*

$$\log s < 1000n^4 \log n.$$

Proof. Write $C(Z,S) = C_{n,S}(Z)$, put $D = 2n^2$, and use $F = F_n$, $h = h_n$ from (2.17). The generating function

$$\sum_{m\geq 0} C_m(Z,S)\frac{w^m}{m!} = \exp\left(Zw + S\sum_{j\geq 2}\frac{w^j}{j}\right)$$

shows that C has nonnegative integer coefficients, weighted degree n for weights $1, 2$, and coefficient sum $C(1,1) = n!$. In particular $F \in \mathbb{Z}[t,v]$.

We use the branches and radius r from Lemma 4.24.

We now apply the triangular elimination in Lemma 4.25, with $m = n^2$, $D = 2m$, and $u = v^2$. Write $\mathcal{T}(v)$ for the substitution matrix $t^j \mapsto t(v)^j$ in $\mathbb{Q}[t]/(h)$, split into its even and odd parts. In the notation of that lemma,

$$\mathcal{O}(u) = \mathcal{T}_{--}(v), \qquad \mathcal{R}(u) = v\mathcal{O}(u)^{-1}\mathcal{T}_{-+}(v).$$

The latter is a power series in u with zero constant term. Lemma 4.26 shows that its entries, in monomial coordinates, satisfy

$$|\mathcal{R}_{ij}(u)| \leq \exp(6n\log n) \qquad (|u| = r^2).$$

Consequently, all coefficients through degree $m+1$ have absolute value at most

$$\exp(20n^2 \log n). \tag{4.25}$$

Indeed $\log r^{-1} \leq 7\log n$, so Cauchy's inequality bounds their logarithms by $6n\log n + 14(n^2+1)\log n \leq 20n^2\log n$.

Lemma 4.26 gives the denominator bound $(6k-3)!$ for the coefficient of u^k in $\mathcal{R}$. Hence the integer

$$q = (6m+3)!$$

clears every coefficient used below and satisfies

$$\log q \leq 36n^2 \log n. \tag{4.26}$$

The reduced map in Lemma 4.25 has

$$R = b(b+1)/2 \leq n^2$$

rows. It sends the coefficients of the even monomials $Z^{2i}S^k$ of weighted degree at most D to the residual coefficients $[u^l](\mathcal{R}E)_i$ with $1 - i \leq l \leq 1$. Here $E_i(u) = u^{-i}p_{2i}(u^{-1})$ and $E_0 = 0$; this is the vector denoted by A in that lemma. It has full row rank, by Theorem 4.22 and the triangular elimination. Let J be its rational matrix. Equations (4.25) and (4.26) give

$$\max|(qJ)_{ij}| \leq \exp(60n^2\log n). \tag{4.27}$$

Choose R columns of qJ forming an invertible matrix B. For $1 \leq k \leq b$, let r_k be the row corresponding to the coefficient at u^1 in the kth odd component. Let $E^{(k)}$ be the even coefficient vector with entries

$$q\,\mathrm{adj}(B)e_{r_k}$$

on these selected columns and zero on all other columns. Its entries are integers divisible by q, and multiplication by J gives

$$JE^{(k)} = q^{-1}B(q\,\mathrm{adj}(B)e_{r_k}) = \det(B)e_{r_k}.$$

Thus every residual coefficient vanishes except the prescribed one, whose value is the same nonzero integer $c = \det(B)$ for every k. Hadamard's inequality and (4.27) bound the even coefficients by $\exp(70n^4 \log n)$.

The odd coefficients are obtained by canceling the allowed Laurent polynomial part of $\mathcal{R}E$, as in Lemma 4.25. This step introduces no denominators: each even coefficient is divisible by q, and q clears every coefficient of $\mathcal{R}$ used in the reconstruction. Indeed, the largest possible index is $m+1$, already covered by the definition $q = (6m+3)!$. The resulting odd terms also have the required degrees, since a power u^{-j} in the ith odd component corresponds to $Z^{2i+1}S^{j-i}$, with $i \le j \le m-1$.

Each reconstructed coefficient is a sum of at most $2n^3$ products of an even coefficient with an entry bounded by (4.25). We have therefore constructed integer polynomials $P_1, \dots, P_b$, of Z-degree less than n and weighted degree at most D, such that every negative odd Laurent coefficient vanishes and

$$[v^1]P_k(t(v)/v, v^{-2}) = c\, t^{2k-1}, \qquad c = \det B \in \mathbb{Z} \setminus \{0\}. \tag{4.28}$$

Their coefficients satisfy

$$H := \max_{k,j,l} |[Z^j S^l]P_k| \le \exp(80n^4 \log n). \tag{4.29}$$

Let $\rho = r/2$ and put

$$M = 2n^3 H (3\sqrt{n})^n \rho^{-D}.$$

Then

$$M \le \exp(90n^4 \log n). \tag{4.30}$$

For a branch with initial root ζ, write

$$G_{k,\zeta}(v) = \frac{1}{2}\left(P_k(t_\zeta(v)/v, v^{-2}) - P_k(t_\zeta(-v)/(-v), v^{-2})\right).$$

The parity of the equation shows that this is the odd Laurent part. Its negative powers have been canceled, so it is holomorphic at 0. On $|v| = \rho$ its absolute value is at most M. Cauchy's inequality and (4.28) therefore give, for $0 < v \le \rho/2$,

$$|G_{k,\zeta}(v)| \le 2Mv/\rho, \tag{4.31}$$

$$|G_{k,\zeta}(v) - c\zeta^{2k-1}v| \le 2Mv^3/\rho^3. \tag{4.32}$$

Suppose now that the two-block field is imaginary quadratic, and assume, for a contradiction, that $T = \log s \ge 1000n^4 \log n$. Then $v = s^{-1/2} < \rho/2$. Write the positive imaginary Hermite roots as $i\lambda_1, \dots, i\lambda_b$, where $0 < \lambda_1 < \cdots < \lambda_b$. At this specialization, complex conjugation pairs the branches starting at $i\lambda_j$ and $-i\lambda_j$ and exchanges the two blocks. Each block therefore contains exactly one root from each pair. There are signs $\epsilon_j \in \{1, -1\}$ such that the difference between the two block traces of P_k is

$$\Delta_k = 2\sum_{j=1}^{b} \epsilon_j G_{k,i\lambda_j}(v).$$

The sum of P_k over either block is fixed by the kernel of the action on the two blocks, so it belongs to the quadratic block field. It is an algebraic integer because P_k has integer coefficients and the centered roots are algebraic integers. Complex conjugation exchanges the blocks, hence $\overline{\Delta_k} = -\Delta_k$. If $\Delta_k \ne 0$, its norm is

$$N_{K/\mathbb{Q}}(\Delta_k) = -\Delta_k^2 = |\Delta_k|^2 \in \mathbb{Z}_{>0},$$

and therefore $|\Delta_k| \ge 1$. This is the arithmetic reason for constructing the polynomials with integer, rather than merely rational, coefficients.

Equations (4.30) and (4.31) imply $|\Delta_k| \le 4bMv/\rho < 1$. Thus $\Delta_k = 0$ for every k. Using (4.32) and $|c| \ge 1$ gives

$$\left|\sum_{j=1}^{b} \epsilon_j (i\lambda_j)^{2k-1}\right| \le 2bMv^2/\rho^3 \qquad (1 \le k \le b). \tag{4.33}$$

These inequalities contradict an elementary Vandermonde bound. Indeed, (4.22) implies

$$\lambda_j > \frac{1}{12\sqrt{n}}, \qquad |\lambda_i^2 - \lambda_j^2| > \frac{1}{36n} \quad (i \ne j), \qquad \lambda_j^2 \le 4n.$$

For the matrix $V_{kj} = \lambda_j^{2k-1}$, Lagrange interpolation at the points λ_j^2 therefore gives

$$\|V^{-1}\|_\infty \le 12b\sqrt{n}(180n^2)^{b-1}.$$

Since $\|\epsilon\|_\infty = 1$, at least one signed moment on the left of (4.33) has absolute value at least

$$\eta = \frac{1}{12b\sqrt{n}(180n^2)^{b-1}}.$$

But $\log \eta^{-1} \le 5n \log n$, while (4.30), $\rho^{-1} = 2000n^2$, and the assumed lower bound on T give $2bMv^2/\rho^3 < \eta$. This contradiction proves the proposition. □

4.5. **Completion of the uniform Galois theorem.** The preceding bounds reduce a possible failure of alternating containment to two blocks with $\sqrt{n} < \log s < n^5$. The nearby-node criterion excludes this last range. We then use the square-discriminant classification to determine the group.

Theorem 4.28. *There is an effectively computable absolute integer N_{Gal} such that, for every $n \ge N_{\mathrm{Gal}}$ and every positive integer s, irreducibility of $H_{n,s}$ implies $A_n \le G_{n,s}$.*

Proof. Choose an effective absolute threshold for the results used below, including Corollary 4.5 with $\kappa = 6$ and $D = 5$. Enlarge it so that

$$\max\{C_1(\log n)^9, (\log n)^6\} < \sqrt{n}, \qquad 2n \log n < 1000n^4 \log n < n^5, \qquad n^{101/200} \log n - \log 2 > \sqrt{n},$$

where C_1 is the constant in Proposition 4.16.

Suppose $H_{n,s}$ is irreducible and $G_{n,s}$ omits A_n. Proposition 4.8 gives $s > n^3/(10 \log n) > n$, and Theorem 4.14 shows that the root action is imprimitive. Choose a partition into a blocks of size b, with $ab = n$ and $a, b \ge 2$. Proposition 4.19 gives

$$\log(s + n) \ge n^{101/200} \log n,$$

so $L = \log s > \sqrt{n}$. Lemma 4.15 excludes $b = 2$. If $a \ge 3$ as well, Proposition 4.16 gives $L \le C_1(\log n)^9 < \sqrt{n}$, a contradiction. Hence $a = 2$.

The corresponding block field is quadratic. If it is real, Lemma 4.20 gives $L < 2n \log n$; if it is imaginary, Proposition 4.27 gives $L < 1000n^4 \log n$. Thus in either case

$$n^{1/2} < L < n^5,$$

contradicting Corollary 4.5. Every threshold used here is effective and independent of s. □

Proof of Theorem 1.1. Take $N = \max\{N_0, N_{\mathrm{Gal}}\}$, with N_0 from Proposition 3.21 and N_{Gal} from Theorem 4.28. For $n \ge N$, the first result gives irreducibility for every positive integer s, and the second gives alternating containment. Both constants are effective and independent of s. □

4.5.1. *An explicit description of the symmetric specializations.* The square-discriminant classification of Banerjee–Filaseta–Finch–Leidy [2, Theorem 2.1] turns uniform alternating containment into a short description of every Galois group in sufficiently large degree. The classification of alternating Laguerre specializations was further developed by Banerjee–Bera [1]. The square-discriminant families used below are those of [2]; the uniform theorem determines the symmetric group throughout their complement in the region $\alpha = -n - s$, $s > 0$.

For $k \geq 0$, define the integers

$$a_k = \frac{(2+\sqrt{3})^k + (2-\sqrt{3})^k}{2}, \quad b_k = \frac{(4+\sqrt{15})^k + (4-\sqrt{15})^k}{2}, \quad c_k = \frac{(1+\sqrt{2})^k + (1-\sqrt{2})^k}{2}.$$

Corollary 4.29. *There is an effectively computable absolute integer N_1 such that, for every $n \geq N_1$ and every positive integer s, one has $G_{n,s} = A_n$ exactly in the cases in Table 1. In all other cases $G_{n,s} = S_n$. In particular,*

$$s \notin \{1, 2, 3, 4, 5, 6, n-4, n, n+2, n+4\} \quad \Longrightarrow \quad G_{n,s} = S_n.$$

s	condition for $G_{n,s} = A_n$
1	$n \equiv 0 \pmod 4$
2	$n \equiv 1 \pmod 4$
3	$n \equiv 0 \pmod 4$ and $n+1$ is a square
4	$n \equiv 1 \pmod{24}$ and $(n+2)/3$ is a square
5	$n + 2 = a_{2k+1}$ for some $k \geq 1$
6	$n + 3 = b_{2k+1}$ for some $k \geq 1$
$n-4$	$(2n-5)/3 = c_{4k}$ for some $k \geq 1$
n	n is an odd square
$n+2$	$n \equiv 0 \pmod 4$, or $(n+1)/2$ is an odd square
$n+4$	$n + 1 = c_{2k+1}^2$ for some $k \geq 1$, or $n+3$ is an even square

TABLE 1. The negative-parameter part of the square-discriminant classification in [2, Section 2, items (v)–(vii) and (xx)–(xxx)], after imposing $\alpha = -n - s$ and taking $n \geq N_1$.

Proof. The cited classification gives thirty explicit families and an effectively computable finite exceptional set $\mathcal{A}_0$. Take N_1 larger than 10, the constant in Theorem 1.1, and every degree occurring in $\mathcal{A}_0$. Under $\alpha = -n - s < -n$, the families of unbounded degree that remain are precisely items (v)–(vii), (xx)–(xxv), and (xxviii)–(xxx) of [2, Section 2]. Substitution gives the ten rows of the table. The discriminant is nonzero for $s > 0$, and Theorem 1.1 gives $A_n \subseteq G_{n,s}$. Hence a square discriminant gives A_n, and every nonsquare discriminant gives S_n. □

5. Effective exceptional specializations

Runge's theorem gives effective specialization results when an intermediate cover has several closed points above infinity. Their number is the number of orbits of the arithmetic decomposition group on the corresponding coset space. We use this observation to turn the cycle type of geometric inertia into an effective criterion.

Proposition 5.1. *Let $K/\mathbb{Q}(T)$ be a regular finite Galois extension with group G, and let $D_\infty \leq G$ be the stabilizer of a place above $T = \infty$ in the arithmetic Galois group. Let S_f be a finite set of rational primes, and let $\mathcal{H}$ be a finite collection of proper subgroups of G. Suppose that*

$$\#(D_\infty \backslash G / H) > |S_f| + 1 \qquad (H \in \mathcal{H}).$$

Then the parameters $t \in \mathbb{Z}[S_f^{-1}]$ outside the branch locus whose specialization group is contained in a conjugate of a member of $\mathcal{H}$ form an effectively computable finite set.

A sufficient condition is $[G : H] > |D_\infty|(|S_f| + 1)$ for every $H \in \mathcal{H}$. For integral parameters, corresponding to $S_f = \varnothing$, it also suffices that for each $H \in \mathcal{H}$ some prime divides $[G : H]$ without dividing $|D_\infty|$.

Proof. Let X_H be the smooth projective curve with function field K^H. Its closed points above infinity correspond to the double cosets $D_\infty \backslash G/H$. Thus the support of the pole divisor of T has more than $|S_f| + 1$ irreducible components over $\mathbb{Q}$. Apply Runge's theorem in the form of [34, Theorem 1.2], with $S = S_f \cup \{\infty\}$, to obtain an effective finite set

$$\{P \in X_H(\mathbb{Q}) : T(P) \in \mathbb{Z}[S_f^{-1}]\}.$$

At an unramified rational parameter, the specialization group is contained in a conjugate of H precisely when it fixes a point of G/H, or equivalently when X_H has a rational point above that parameter. Taking the union over $\mathcal{H}$ proves the assertion.

Every D_∞-orbit has at most $|D_\infty|$ elements, proving the numerical sufficient condition. When $S_f = \varnothing$, the hypothesis is intransitivity. A transitive action would imply $[G : H] \mid |D_\infty|$, which proves the final test. □

Lemma 5.2. *Let $\sigma \in S_n$ have a_d cycles of length d, including a_1 fixed points, and put $m = \operatorname{ord}(\sigma)$. Then*

$$|N_{S_n}(\langle\sigma\rangle)| = \varphi(m) \prod_{d \geq 1} d^{a_d} a_d!.$$

If p is an odd prime with $n/2 < p < n$, then

$$p \nmid |N_{S_n}(\langle\sigma\rangle)| \quad \Longleftrightarrow \quad a_p = 0 \text{ and } a_1 < p.$$

Proof. The centralizer has order $\prod_d d^{a_d} a_d!$. Every automorphism $\sigma \mapsto \sigma^u$ of $\langle\sigma\rangle$ is realized by simultaneously multiplying the cyclic coordinates in each d-cycle by u mod d. The quotient of the normalizer by the centralizer therefore has order $\varphi(m)$.

We claim that $p \nmid \varphi(m)$. Otherwise either $p^2 \mid m$, or some prime $q \mid m$ satisfies $p \mid q - 1$. The first possibility requires a cycle of length at least $p^2 > n$. In the second, p is odd, so $q \geq 2p+1 > n$, whereas every prime divisor of m divides a cycle length at most n. Both are impossible. Also $p \mid d$ for a cycle length $d \leq n$ precisely when $d = p$. For $d \geq 2$ one has $a_d \leq n/2 < p$, so the only factorial that can contribute p is $a_1!$. This proves the equivalence. □

Lemma 5.3. *Let $n/2 < p \leq n - 3$ be prime. If $H \leq S_n$ is transitive and $A_n \not\leq H$, then $p \nmid |H|$ and $p \mid [S_n : H]$.*

Proof. If $p \mid |H|$, Cauchy's theorem supplies an element of order p. Since $2p > n$, this element is a single p-cycle. Any nontrivial block system has a blocks of size b, with $a, b \leq n/2 < p$. An element of order p must fix every block and then every point in each block, a contradiction. Thus H is primitive. Jordan's prime-cycle theorem [13, Theorem 3.3E], with $p \leq n - 3$, now gives $A_n \leq H$. □

Theorem 5.4. *Let $F(X, T) \in \mathbb{Q}(T)[X]$ have degree $n \geq 8$ in X and geometric Galois group S_n. Let $\sigma \in S_n$ generate inertia at infinity in its splitting field. Suppose that there is a prime*

$$n/2 < p \leq n - 3$$

such that σ has no p-cycle and has fewer than p fixed points. Then the integers t for which $F(X, t)$ is defined, has degree n, is irreducible over $\mathbb{Q}$, and has Galois group not containing A_n form an effectively computable finite set.

Proof. The arithmetic group is also S_n and the splitting field is regular. In characteristic zero the inertia group at infinity is cyclic and is normal in the arithmetic decomposition group. Consequently

$$D_\infty \le N_{S_n}(\langle\sigma\rangle).$$

Lemma 5.2 shows that $p \nmid |D_\infty|$. By Lemma 5.3, p divides the index of every transitive subgroup omitting A_n. Apply Proposition 5.1 to representatives of their finitely many conjugacy classes. The finitely many bad parameters coming from coefficient poles, degree drops, and branch points can be handled directly. □

5.1. **Effective exceptional sets for the Laguerre family.**

Corollary 5.5. *For every fixed $n \ge 5$, the positive integers s for which $H_{n,s}$ is irreducible and $A_n \not\le G_{n,s}$ form a finite, effectively computable set.*

Proof. The generic splitting field is a regular S_n-extension of $\mathbb{Q}(s)$. Indeed, the inertia permutations at $s = 0, -1, -(n-2)$ have an n-cycle, an $(n-1)$-cycle, and a transposition, respectively [30, Lemma 15]. The first two give double transitivity, and the transposition then gives S_n. At infinity, the Hermite expansions from Section 2.1 have inertia cycle type $2^{\lfloor n/2\rfloor}1^{n \bmod 2}$. For $n \ge 8$ and a prime $n/2 < p \le n-3$, this permutation has no p-cycle and has fewer than p fixed points. Such a prime exists for every $n \ge 8$: for $n \ge 51$ use Nagura's theorem [39], and for $8 \le n \le 50$ the primes $5, 7, 11, 13, 17, 23, 29$ suffice. Apply Theorem 5.4.

It remains to treat $n = 5, 6, 7$. Write σ for the inertia involution at infinity and $C_n = C_{S_n}(\sigma)$. Since σ has order two, $D_\infty \le C_n$, and

$$|C_5| = 8, \qquad |C_6| = |C_7| = 48.$$

The classification of transitive groups of these degrees [8, pp. 869–871] shows that a transitive subgroup omitting A_5 is contained in a conjugate of $\mathrm{AGL}_1(\mathbb{F}_5)$, of index 6 in S_5. In degree seven, a transitive subgroup omitting A_7 is contained in a conjugate of $\mathrm{AGL}_1(\mathbb{F}_7)$ or $\mathrm{GL}_3(\mathbb{F}_2)$, of indices 120 and 30 in S_7. None of these indices divides the corresponding $|C_n|$. Thus C_n is intransitive on each of these coset spaces, and also on the coset space of every subgroup of the listed groups.

In degree six, an imprimitive subgroup is contained in a conjugate of $S_3 \wr S_2$ or $S_2 \wr S_3$, of indices 10 and 15. These indices do not divide 48, so the same argument applies. Every primitive subgroup omitting A_6 is contained in a conjugate of $M = \mathrm{PGL}_2(\mathbb{F}_5)$, acting on $\mathbb{P}^1(\mathbb{F}_5)$. The map $z \mapsto 2/z$ in M has cycle type 2^3: it acts as $(0\ \infty)(1\ 2)(3\ 4)$. Consequently σ fixes a point of S_6/M. The action of S_6 on S_6/M is faithful, because M contains no nontrivial normal subgroup of S_6. Hence σ does not fix every point. Its fixed-point set is therefore nonempty and proper; it is C_6-invariant because C_6 centralizes σ. This proves that C_6 is intransitive on S_6/M, and therefore on S_6/H whenever H is contained in a conjugate of M.

In all three degrees, D_∞ is thus intransitive on S_n/H for every transitive subgroup H omitting A_n. Proposition 5.1 completes the proof. All positive parameters are outside the branch locus. □

The conclusion is effective in each fixed degree. The uniform Galois theorem supplies the separate bound on the degrees that can remain exceptional.

Corollary 5.6. *The positive integral pairs (n, s) for which $H_{n,s}$ is reducible or $A_n \not\le G_{n,s}$ form a finite, effectively computable set.*

Proof. There are no exceptions in degrees $n \le 4$, by [29, Theorem 6.3(i)]. Theorem 1.1 bounds every remaining exceptional degree by an effective absolute constant. In each such degree, Proposition 2.4 bounds every reducible specialization by

$$s < \left\lfloor n^2/4 \right\rfloor^n.$$

Exact factorization determines those exceptions. For the irreducible specializations, Corollary 5.5 gives a finite effective list containing every exception to alternating containment. Exact Galois-group computation determines which entries are exceptions. □

This reduces Hajir's two conjectures to an effective finite verification. It does not give a practical enumeration: the estimates obtained in the uniform proof are very large.

6. Applications and further questions

The preceding arguments have two kinds of applications. The finite-fiber and prime-valuation criteria apply to other polynomial families. The uniform Galois theorem also gives consequences for splitting fields, algebraic relations among roots, and products of hyperelliptic Jacobians.

6.1. **An Appell family with two scales.** We apply the finite-fiber criterion of Section 2.2 to a convolution of two Laguerre families. This application uses the centered root strip, but does not require the uniform Galois theorem. For an integer $c \geq 2$, define

$$P_{n,s}^{(c)}(X) = n![t^n]e^{Xt}(1-t)^{-s}(1-ct)^{-s}, \qquad P_{n,s} = P_{n,s}^{(2)}, \qquad \kappa_c = 1 + c. \tag{6.1}$$

For real $s > 0$, this is the moment polynomial $\mathbb{E}(X + Y_1 + cY_2)^n$ of two independent gamma variables of shape s and scale 1. Its coefficient of X^{n-k} is

$$\sum_{j=0}^{k} \frac{n!}{(n-k)!j!(k-j)!}(s)_j(s)_{k-j}c^{k-j}.$$

Thus $P_{n,s}^{(c)} \in \mathbb{Z}[s, X]$, and this coefficient has s-degree at most k.

Theorem 6.1. *For every $\varepsilon > 0$, there is an effective integer $N(\varepsilon)$ such that $P_{n,s}$ is irreducible over $\mathbb{Q}$ for all integers*

$$n \geq N(\varepsilon), \qquad s \geq 1, \qquad \log s \geq n^{\varepsilon}.$$

The same argument permits rational parameters and a scale that grows with the degree.

Corollary 6.2. *There is a finite effectively computable set $\mathcal{E} \subset \mathbb{Z}_{\geq 3}$ with the following property. For every $0 < \eta < 1/3472$, $B \geq 0$, and $\varepsilon > 0$, there is an effective integer $N(B, \varepsilon, \eta)$, independent of c, such that $P_{n,a/b}^{(c)}$ is irreducible over $\mathbb{Q}$ whenever*

$$n \geq N(B, \varepsilon, \eta), \qquad 2 \leq c \leq n^{\eta}, \qquad c \in \mathbb{Z} \setminus \mathcal{E},$$
$$a, b \in \mathbb{Z}_{>0}, \qquad \gcd(a, b) = 1, \qquad b \leq n^{B}, \qquad \log a \geq n^{\varepsilon}.$$

The set $\mathcal{E}$ will be defined by an explicit polynomial; we do not assert that it is empty. Since $2 \notin \mathcal{E}$, the corollary implies the theorem.

Proof of the theorem and corollary. We check the two inputs to the finite-fiber criterion: a strip bound from polynomial convolution, and trace separation at four fibers. We then make both estimates uniform in c.

Convolution and the root strip.

For monic polynomials p, q of degree n, write $q(X) = \sum_{k=0}^{n} q_k X^{n-k}$ and define

$$(p \boxplus_n q)(X) = \sum_{k=0}^{n} \frac{(n-k)!}{n!} q_k p^{(k)}(X).$$

This is Walsh's additive convolution, also called symmetric additive finite free convolution; see [37, Section 1]. We need its preservation of half-planes, including for polynomials whose coefficients are not real.

Suppose the roots of p and q lie in the closed left half-plane. The polynomials

$$\widetilde{p}(Z) = i^n p(Z/i), \qquad \widetilde{q}(Z) = i^n q(Z/i)$$

have their roots in the closed lower half-plane. Consider

$$T_{\widetilde{q}} = \sum_{k=0}^{n} \frac{(n-k)!}{n!} \widetilde{q}_k \frac{d^k}{dX^k}.$$

Its algebraic symbol is $T_{\widetilde{q}}[(X+Y)^n] = \widetilde{q}(X+Y)$, which is nonzero when both variables lie in the open upper half-plane. By [5, Theorem 4, p. 471], $T_{\widetilde{q}}\widetilde{p}$ has no root there. The output is monic, so the zero-polynomial alternative is excluded. Since

$$(\widetilde{p} \boxplus_n \widetilde{q})(Z) = i^n (p \boxplus_n q)(Z/i),$$

$p \boxplus_n q$ has its roots in the closed left half-plane. Translation covariance adds upper bounds on real parts; reflection adds lower bounds. Both covariance identities follow directly from the definition.

For formal power series f, g with constant term 1, coefficient comparison gives

$$\big(n![t^n]e^{Xt}f(t)\big) \boxplus_n \big(n![t^n]e^{Xt}g(t)\big) = n![t^n]e^{Xt}f(t)g(t).$$

Consequently

$$P_{n,s}^{(c)} = H_{n,s} \boxplus_n \big(c^n H_{n,s}(X/c)\big).$$

Proposition 2.2 and the half-plane bounds just proved show that, for every real $s > 0$ and every root α,

$$|\operatorname{Re}(\alpha + \kappa_c s)| \le \kappa_c (n-1). \tag{6.2}$$

Four fibers and the trace condition.

Introduce indeterminates N, C, and put

$$f_k(N) = N(N-1)\cdots(N-k+1), \qquad f_0(N) = 1, \qquad A_C(t) = (1-t)(1-Ct).$$

For $m = 1, 2, 3$, define

$$R_{m,C}(N, X) = \sum_{k=0}^{2m} f_k(N)[t^k]A_C(t)^m X^{2m-k}.$$

These belong to $\mathbb{Z}[N, C, X]$, and, for $n \ge 6$,

$$P_{n,0}^{(c)} = X^n, \qquad P_{n,-m}^{(c)} = X^{n-2m} R_{m,c}(n, X).$$

Let $U_{m,C}(N, Z)$ be the subset-trace polynomial of $R_{m,C}$, and put $U_{0,C}(N, Z) = Z$. The fundamental theorem of symmetric polynomials gives

$$U_{m,C} \in \mathbb{Z}[N, C, Z], \qquad \deg_Z U_{m,C} = 2^{2m}.$$

The full subset has sum $m(1+C)N$. For $m = 2, 3$, remove the empty and full subsets by putting

$$V_{m,C}(N, Z) = \frac{U_{m,C}(N, Z)}{Z(Z - m(1+C)N)}.$$

These are monic polynomials in $\mathbb{Z}[N, C, Z]$ of degrees 14 and 62. When $C = 2$, omit the subscript C from $R_{m,C}$, $U_{m,C}$, and $V_{m,C}$. For an integral factor at a positive integral parameter s, with degree d and centered trace $A = \tau + \kappa_c d s$, trace specialization gives

$$p \mid s + m \quad \Longrightarrow \quad p \mid U_{m,c}(n, A + m\kappa_c d), \qquad 0 \le m \le 3. \tag{6.3}$$

The first residual polynomial is

$$R_{1,c}(n, X) = X^2 - \kappa_c n X + cn(n-1).$$

Its discriminant $(c-1)^2 n^2 + 4cn$ is not a square for $n \ge 5$. Indeed, if it equals q^2, the integers

$$U = (c-1)^2 n + 2c, \qquad V = (c-1)q$$

satisfy $U > V \geq 0$ and $(U-V)(U+V) = 4c^2$. For positive integers with fixed product $4c^2$, their sum is at most $4c^2+1$. Hence $2U \leq 4c^2+1$, and integrality gives $U \leq 2c^2$. This would imply $n \leq 2c/(c-1) \leq 4$. It follows that the only rational roots of $U_{1,c}(n,Z)$ are 0 and $\kappa_c n$.

Thus fibers $0,1$ already give two nonzero evaluations unless the centered trace is 0, $-\kappa_c d$, or $\kappa_c(n-d)$. For these three possibilities, it is enough to eliminate the single variable d. Put $\kappa = 1+C$ and define

$$D_0(N,C) = \mathrm{Res}_D\big(V_{2,C}(N, 2\kappa D), V_{3,C}(N, 3\kappa D)\big),$$
$$D_1(N,C) = \mathrm{Res}_D\big(V_{2,C}(N, \kappa D), V_{3,C}(N, 2\kappa D)\big).$$

Both pairs have degrees $14, 62$ in D. Their leading coefficients are powers of κ times positive integers, independent of N; specializing N or a positive integer C therefore preserves these degrees. Write $\mathcal{D}_i(N) = D_i(N,2)$. The exact calculation in Appendix B gives

$$\mathcal{D}_0(11)\mathcal{D}_1(11) \neq 0. \tag{6.4}$$

It therefore proves nonvanishing of the two resultants as polynomials, rather than merely a trace calculation in one degree.

Suppose $n \geq 6$, $c \geq 2$, and $D_0(n,c)D_1(n,c) \neq 0$. For every $z \in \mathbb{Q}$ and integer $0 < d < n$, we claim that at least two of

$$U_{m,c}(n, z + m\kappa_c d), \qquad m = 0,1,2,3, \tag{6.5}$$

are nonzero. Outside the three exceptional traces above, this follows from fibers $0,1$. If $z = 0$, fiber 1 is nonzero. The empty and full subset factors in fibers $2,3$ are nonzero because $0 < d < n$, so $D_0(n,c) \neq 0$ prevents both evaluations from vanishing. If $z = -\kappa_c d$, fiber 0 is nonzero. The factors removed from fibers $2,3$ can vanish only at $d = 0$, $d = 2n$, or $d = 3n/2$, all outside $0 < d < n$. Thus $D_1(n,c) \neq 0$ again gives a second nonzero evaluation. For $z = \kappa_c(n-d)$, replace (z,d) by $(-z, n-d)$. Complementation of subsets gives

$$U_{m,c}(n, m\kappa_c n - Z) = U_{m,c}(n,Z) \quad (m \geq 1), \qquad U_{0,c}(n,-Z) = -U_{0,c}(n,Z).$$

This replacement therefore preserves which evaluations vanish and reduces the last case to the preceding one.

Uniformity in the scale.

Set

$$\mathcal{D}(N,C) = D_0(N,C)D_1(N,C), \qquad E(C) = \mathcal{D}(11,C), \qquad \mathcal{E} = \{c \in \mathbb{Z}_{\geq 2} : E(c) = 0\}.$$

By (6.4), $E(2) \neq 0$. Thus $\mathcal{E}$ is finite and effectively computable, and $\mathcal{E} \subset \mathbb{Z}_{\geq 3}$.

Put $K = \max\{1, \deg_C \mathcal{D}\}$. We have $K \leq 3472$. Indeed, put $d_m = 2^{\overline{2m}} - 2$ for $m = 2,3$. The coefficient of X^{2m-k} in $R_{m,C}$ has C-degree at most k. The coefficient of $Z^{d_m - j}$ in $V_{m,C}$ is symmetric and homogeneous of degree j in the residual roots. Giving the kth elementary symmetric function weight k therefore bounds its C-degree by j. After substituting $Z = \ell(1+C)D$, every coefficient in D has C-degree at most d_m. The bidegrees of the Sylvester resultant in its two coefficient lists now give

$$\deg_C D_i \leq 62 \cdot 14 + 14 \cdot 62 = 1736 \qquad (i = 0,1),$$

and hence $K \leq 3472$.

There is an effective absolute $C_0 \geq 1$ such that every coefficient of $\mathcal{D}(N,c)$, as a polynomial in N, is at most $C_0(1+c)^K$ in absolute value. For $c \notin \mathcal{E}$ this polynomial is nonzero; its highest nonzero coefficient is an integer of absolute value at least 1, even if its degree drops with c. Cauchy's bound puts every complex root in the disk of radius $1 + C_0(1+c)^K$. If $c \leq n^\eta$ and $0 < \eta < 1/3472$, then

$$1 + C_0(1+c)^K \leq 1 + 2^K C_0 n^{K\eta} < n$$

for all sufficiently large n, effectively in terms of η. Consequently $D_0(n,c)D_1(n,c) \neq 0$ uniformly over all permitted scales, and the trace condition holds.

To finish, apply Corollary 2.14. For each sufficiently large n, select any permitted scale $c = c(n)$ and use the family $P_n(T,X) = P_{n,T}^{(c(n))}(X)$ with center $c_n(T) = -\kappa_{c(n)}T$. The coefficient-degree condition follows from the displayed coefficient formula. Equation (6.2) gives the required real-parameter bound, since $\kappa_c(n-1) \leq 2n^{1+\eta}$. The four residual degrees are at most 6, and their coefficients are fixed polynomials in n, c. Their heights and the values $|c_n(-m)|$ are therefore bounded by a fixed power of n. Equation (6.5) supplies the trace condition. All constants are independent of the choice of $c(n)$, so the resulting threshold $N(B,\varepsilon,\eta)$ works simultaneously for every permitted scale. This proves the corollary and, with $c = 2$ and $b = 1$, the theorem. □

Further Appell families. Let $F(t) \in \mathbb{Z}[t]$ be nonconstant with $F(0) = 1$ and all zeros positive. Write $F(t) = \prod_{j=1}^{r}(1 - c_j t)$ with $c_j > 0$, and put $\mu = \sum_j c_j = -F'(0) \in \mathbb{Z}_{>0}$. For $Q_{n,s}(X) = n![t^n]e^{Xt}F(t)^{-s}$, repeated convolution gives

$$|\operatorname{Re}(\alpha + \mu s)| \leq \mu(n-1)$$

for every root and every real $s > 0$. Expanding $F(t)^{-s} = \sum_{j\geq 0}(s)_j(1-F(t))^j/j!$ shows that $Q_{n,s} \in \mathbb{Z}[s,X]$, with the coefficient of X^{n-k} of s-degree at most k: for $j \leq k \leq n$, the multiplier $n!/((n-k)!j!)$ is integral. At $s = -m$, the residual degree is rm for $n \geq rm$, and its coefficients are polynomial in n. Thus the strip and height hypotheses hold for any fixed list of negative-integer fibers. The trace condition remains to be proved for each new F.

Generic irreducibility does not settle this verification. Indeed, Eisenstein at $s = 0$ already gives absolute irreducibility of $Q_{n,s}(X)$ as a two-variable polynomial: every nonleading coefficient is divisible by s, while $[s]Q_{n,s}(0) = (n-1)!\sum_j c_j^n > 0$. The two-scale calculation above supplies the additional trace separation needed for arithmetic specializations. An all-parameter result would also require an argument in the complementary range, as in Corollary 2.13.

6.2. **A deterministic application to trimmed exponentials.** For positive integers n, u, define the monic integral polynomial

$$E_{n,u}(X) = (u+n)!\sum_{j=0}^{n}\frac{X^j}{(u+j)!} = \sum_{j=0}^{n}\left(\prod_{r=j+1}^{n}(u+r)\right)X^j. \tag{6.6}$$

Bary-Soroker and Ben-Porath [3, Conjecture 1] conjectured that every such trimmed exponential is irreducible with Galois group S_n, and suggested just before that conjecture that its discriminant is nonsquare when $u > 1$ and $n \geq 2$. They proved [3, Theorem 1] that, if $k_{\max}(x) = x^{o(1)}$ and the endpoint m is chosen uniformly from $\{1,\dots,x\}$, then with probability tending to one, $m > k_{\max}(x)$ and all $E_{n,m-n}$ with $8 \leq n \leq k_{\max}(x)$ have Galois group S_n. The preceding arithmetic criteria give a deterministic result for the discriminant, a conditional S_n theorem throughout a parameter window, and an unconditional S_n theorem under an explicit endpoint condition.

6.2.1. *Local packets and the discriminant.*

Lemma 6.3. *Let $1 \leq N \leq n$, let $p > n$ be prime, and suppose that $e = v_p(u+N) > 0$. Then $E_{n,u}$ is separable, its Newton polygon has an edge from $(0,e)$ to $(N,0)$, and*

$$v_p(\operatorname{Disc} E_{n,u}) = e(N-1). \tag{6.7}$$

Its local inertia group is cyclic, and a generator has cycle type $(N/g)^g 1^{n-N}$, where $g = \gcd(N,e)$.

Proof. Only $u+N$ among $u+1,\dots,u+n$ is divisible by p. The coefficient formula (6.6) therefore gives

$$v_p([X^j]E_{n,u}) = \begin{cases} e, & 0 \le j < N, \\ 0, & N \le j \le n. \end{cases}$$

This proves the Newton-polygon assertion. Put $m = n - N$ and $e_m(X) = \sum_{j=0}^{m} X^j/j!$. Since $u \equiv -N \pmod{p}$,

$$\overline{E}_{n,u}(X) = X^N R_m(X), \qquad R_m(X) = m! e_m(X) \in \mathbb{F}_p[X].$$

Here $R_m(0) = m! \neq 0$ and $R_m - R_m' = X^m$, so R_m is squarefree; the case $m = 0$ means $R_m = 1$. Let $A \in \mathbb{Z}_p[X]$ be the monic degree-N Hensel factor lifting X^N. The complementary factor has unit constant term. Comparison of coefficients in increasing degree shows that every nonleading coefficient of A is divisible by p^e, and that its constant coefficient has valuation exactly e. Lemma 3.1 now gives separability and the stated inertia action. It also gives valuation e/N for every difference between two roots in the packet and valuation zero for every other root difference. Taking the product of the squares of these differences gives $2\binom{N}{2}e/N = e(N-1)$ in (6.7). □

Proposition 6.4. *For each fixed $\eta > 0$, there is an effectively computable $n_0(\eta)$ such that $E_{n,u}$ is separable and has nonsquare discriminant whenever*

$$n \ge n_0(\eta), \qquad u \ge (\gcd(u,2) - 1 + \eta)n.$$

In particular, $u \ge (1+\eta)n$ suffices, and for odd u the weaker condition $u \ge \eta n$ suffices. In addition, for all effectively sufficiently large n and $u \ge n^{21/10}$, more than $\lfloor n/2 \rfloor/102$ distinct primes $p > 3\lfloor n/2 \rfloor$ have odd valuation in $\operatorname{Disc} E_{n,u}$.

Proof. Put $k = \lfloor n/2 \rfloor$, $h = \gcd(u,2)$, $A = (u+2)/h$, and $d = 2/h$. Then $d \in \{1,2\}$, $\gcd(A,d) = 1$, and

$$\prod_{j=0}^{k-1}(A + jd) = h^{-k}\prod_{j=1}^{k}(u+2j). \tag{6.8}$$

If a prime $p > n$ has odd valuation in this product, it divides exactly one node $u+N$ with N even, and $e = v_p(u+N)$ is odd. Lemma 6.3 then proves separability and gives the odd valuation $v_p(\operatorname{Disc} E_{n,u}) = e(N-1)$.

For the first assertion, set $\theta = \min(\eta,1)/4$ and $C = 2 + \theta$. Filaseta–Laishram–Saradha [23, Theorem 1.1] imply that, for fixed d, all sufficiently large k, and every A with

$$\gcd(A,d) = 1, \qquad A \ge (C - d + \theta d)k,$$

the product in (6.8) has a prime $p > Ck$ of odd valuation. Indeed, otherwise that product is by^2, with every prime divisor of b at most Ck, contrary to their effective finiteness theorem. Here $C \ge d$ and $0 < \theta < 1$, as required. If $h = 2$, our hypothesis gives

$$A \ge (1+\eta)k \ge (1+2\theta)k = (C - d + \theta d)k.$$

If $h = 1$, it gives $A \ge 2\eta k \ge 3\theta k = (C - d + \theta d)k$. Take k beyond the effective exceptional bounds for both $d = 1$ and $d = 2$, and also require $k > 1/\theta$. Then $p > Ck > n$, so the preceding local argument applies.

For the quantitative assertion, $u \ge n^{21/10}$ implies $A \ge k^{21/10}$. Apply Theorem 4.6(ii) with $C = 3$, $r = 2$, $\varepsilon = 1/10$, and $\delta = 1/102$. It gives more than $k/102$ primes $p > 3k$, each with odd valuation in (6.8). For $n \ge 5$ these primes exceed n, so each has odd discriminant valuation. □

6.2.2. *Symmetric groups in a parameter window.*

Theorem 6.5. *Fix $D > 0$ and $\kappa > 5$. There is an effectively computable $N = N(D, \kappa)$ such that, for all integers*

$$n \geq N, \qquad u \geq 1, \qquad (\log n)^{\kappa} \leq \log u \leq n^{D},$$

irreducibility of $E_{n,u}$ over $\mathbb{Q}$ implies

$$\mathrm{Gal}(E_{n,u}/\mathbb{Q}) = S_n.$$

In particular, for fixed $0 < \varepsilon \leq D$ the same conclusion holds whenever $n^{\varepsilon} \leq \log u \leq n^{D}$ and n is sufficiently large in terms of ε, D.

Proof. For each prime $n/2 < P \leq n-3$, take the node $u+P$. There are at least $2n/(5\log n)$ such primes for all effectively sufficiently large n. Lemma 6.3 supplies the required Newton edge at each prime $p > n$ dividing $u+P$. Theorem 4.4, with $s = u$, $C = 1$, $c = 2/5$, and $j_P = P$, proves alternating containment whenever $E_{n,u}$ is irreducible, since $\lfloor C/c \rfloor + 3 = 5$. For sufficiently large n, the lower bound $\log u \geq (\log n)^{\kappa}$ implies $u \geq 2n$. Proposition 6.4, with $\eta = 1$, excludes containment in A_n, and hence the group is S_n. For the final assertion take $\kappa = 6$ and use $(\log n)^6 \leq n^{\varepsilon}$ for sufficiently large n. □

Corollary 6.6. *Let n, u be positive integers. Suppose that primes $q_1, \ldots, q_t > n$, with $t \geq 1$, satisfy*

$$e_i = v_{q_i}(u+n) > 0, \qquad \gcd(n, e_1, \ldots, e_t) = 1.$$

Then $E_{n,u}$ is irreducible over $\mathbb{Q}$. If, in addition, n, u satisfy the hypotheses of Theorem 6.5, its Galois group is S_n. In particular, the endpoint condition holds if some prime $q > n$ divides $u+n$ with $\gcd(n, v_q(u+n)) = 1$, and hence whenever $u+n$ is prime.

Proof. Every nonleading coefficient in (6.6) has q_i-adic valuation e_i, while the leading coefficient is 1. Thus the Newton polygon is the segment joining $(0, e_i)$ to $(n, 0)$, and every root has valuation e_i/n. If a monic rational factor has degree d, its nonzero constant coefficient has integral q_i-adic valuation de_i/n. Consequently $n/\gcd(n, e_i)$ divides d for every i. The least common multiple of these integers is

$$\mathrm{lcm}_{1 \leq i \leq t} \frac{n}{\gcd(n, e_i)} = \frac{n}{\gcd(n, e_1, \ldots, e_t)} = n.$$

There is therefore no proper rational factor. This argument works for all positive n, u. In the stated parameter range, Theorem 6.5 gives S_n. If $u+n$ is prime, the irreducibility assertion is Eisenstein's criterion. □

For example, if $6 \mid n$ and $u+n = q_1^2 q_2^3$ for distinct primes $q_1, q_2 > n$, the two endpoint valuations together prove irreducibility, although neither is individually coprime to n. In the parameter range of the theorem the group is S_n.

Theorem 6.5 is uniform in every parameter in its window, conditional on irreducibility. Corollary 6.6 removes that condition on an explicit arithmetic subfamily. These statements do not settle the full conjecture of [3]: irreducibility outside the endpoint condition remains unproved here. The local Newton-polygon step is classical. Bary-Soroker and Ben-Porath already use an endpoint valuation-one prime for irreducibility and a full cycle, and an even-length cycle to exclude alternating groups [3, Propositions 5.1 and 5.2]. Theorem 4.3 supplies the prime valuations needed for alternating containment throughout the stated parameter window. The linear discriminant range uses [23, Theorem 1.1], while Theorem 4.6 gives a positive proportion of odd discriminant valuations in the larger-parameter range. All these conclusions are deterministic.

6.3. **Splitting fields and Jacobians.** The uniform Galois theorem has consequences for relations among selected roots and for products of hyperelliptic Jacobians. The general criteria are due to Bary-Soroker–Kadets, Zarhin, and Lombardo; here they apply with arbitrary positive integral parameters. Increase N in Theorem 1.1 so that $N \geq 5$, and write $J_{n,s}$ for the Jacobian of the smooth projective model of $Y^2 = H_{n,s}(X)$.

6.3.1. *Splitting fields of distinct degrees.*

Proposition 6.7. *Let $f_1, \dots, f_r \in \mathbb{Q}[X]$ be separable of distinct degrees $n_i \geq 5$, with Galois groups $G_i = A_{n_i}$ or S_{n_i}. Let L_i be their splitting fields, $\delta_i \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ their discriminant classes, and $\mathcal{R} = \{(e_i) \in \mathbb{F}_2^r : \prod_i \delta_i^{e_i} = 1\}$. Restriction identifies the group of the compositum with*

$$\mathrm{Gal}(L_1 \cdots L_r/\mathbb{Q}) = \left\{ (g_i) \in \prod_i G_i : \prod_i \mathrm{sgn}(g_i)^{e_i} = 1 \text{ for every } (e_i) \in \mathcal{R} \right\}.$$

If the δ_i span a space of dimension a, then $[L_1 \cdots L_r : \mathbb{Q}] = 2^a \prod_i (n_i!/2)$.

Proof. The compositum group G is a subdirect product of the G_i, so G' is a subdirect product of the pairwise nonisomorphic simple groups A_{n_i}. Goursat's lemma gives $G' = \prod_i A_{n_i}$. The sign quotient is the Galois group of $\mathbb{Q}(\sqrt{\delta_1}, \dots, \sqrt{\delta_r})$, with relation space $\mathcal{R}$. This proves both formulas. □

Thus, for distinct $n_i \geq N$ and arbitrary $s_i \geq 1$, the discriminant classes in (1.7) determine the Galois group of the compositum of the splitting fields of H_{n_i,s_i}.

6.3.2. *Algebraic relations among selected roots.* The criterion of Bary-Soroker–Kadets [4, Definition 1.6 and Theorem 1.7] extends their application with fixed Laguerre parameters as follows.

Corollary 6.8. *For any sequence of positive integers $(s_n)_{n\geq 1}$, let $\mathcal{S} = \{z \in \overline{\mathbb{Q}} : H_{n,s_n}(z) = 0 \text{ for some } n \geq 1\}$. For every $m \geq 1$ and $B \subseteq \mathcal{S}^m$, the Zariski closure of B in $\mathbb{A}^m_{\mathbb{C}}$ is a finite union of affine linear subspaces defined by equations $X_i = X_j$ $(i \neq j)$ and $X_i = c$ $(c \in \mathcal{S})$. In particular, an irreducible plane curve contains infinitely many points of $\mathcal{S}^2$ if and only if it is the diagonal, or a horizontal or vertical line through an element of $\mathcal{S}$.*

Proof. For $n \geq N$, the selected roots have degree n and Galois group A_n or S_n. There are finitely many of bounded degree; nonconjugate roots have splitting fields whose intersection has degree at most two, by Proposition 6.7. These are the hypotheses of the cited criterion. The finitely many remaining roots may be adjoined by partitioning tuples according to the coordinates taking these values. Since $\mathcal{S}$ is infinite, the plane-curve assertion follows. □

Remark 6.9. The choice of one parameter per degree matters. For any fixed $d \geq 2$, ordered root tuples for all $s \geq 1$ satisfy

$$(\textstyle\sum_i x_i)^2 - d \sum_i x_i^2 + d(d-1) \sum_i x_i = 0.$$

This proper hypersurface contains infinitely many tuples. None lies on a coordinate diagonal, and each equation $x_i = c$ holds for only finitely many parameters, since $H_{d,s}(c)$ is monic of degree d in s. Their closure therefore cannot be a finite union of the permitted proper subspaces. The corollary fails for the union over all parameters, even after any finite range of degrees is omitted.

6.3.3. *Products of Jacobians.*

Theorem 6.10. *Let K be a number field and let $f_1, \dots, f_r \in K[X]$ be separable of pairwise distinct degrees $n_i \geq 5$, with $\mathrm{Gal}(f_i/K) \supseteq A_{n_i}$. Let A_i be the Jacobian of $y^2 = f_i(x)$ and $B = \prod_i A_i^{e_i}$, where $e_i \geq 1$. Then*

$$\mathrm{End}_{\overline{K}}(A_i) = \mathbb{Z}, \qquad \mathrm{Hom}_{\overline{K}}(A_i, A_j) = 0 \ (i \neq j), \qquad \mathrm{End}_{\overline{K}}(B) \simeq \prod_i M_{e_i}(\mathbb{Z}).$$

Fix $K \hookrightarrow \mathbb{C}$ and polarization forms ψ_i on $V_i = H_1(A_i(\mathbb{C}), \mathbb{Q})$. In the diagonal action on repeated copies,

$$\mathrm{Hg}(B) = \prod_i \mathrm{Sp}(V_i, \psi_i),$$

$$\mathrm{MT}(B) = \mathcal{G} := \{(u_i) \in \prod_i \mathrm{GSp}(V_i, \psi_i) : \nu(u_1) = \cdots = \nu(u_r)\},$$

where ν is the similitude multiplier. For every prime ℓ, the algebraic monodromy group is $\mathcal{G}_{\mathbb{Q}_\ell}$ and the image has Lie algebra

$$\mathbb{Q}_\ell \,\mathrm{Id} \oplus \bigoplus_i \mathfrak{sp}(V_\ell(A_i), \psi_{i,\ell}), \qquad V_\ell(A_i) = T_\ell(A_i) \otimes \mathbb{Q}_\ell.$$

The Mumford–Tate conjecture holds for B. On B and every power of B, all rational Hodge classes and all ℓ-adic Tate classes over finite extensions of K are generated by divisor classes. In particular, the Hodge and Tate conjectures hold for these varieties.

Proof. The endomorphism and homomorphism assertions follow from [48, Theorem 1.1 and Corollary 1.4], including adjacent degrees $2g+1, 2g+2$, which have the same genus. Each individual ℓ-adic Lie algebra is symplectic plus scalars by [47, Theorem 2.6]. Lombardo's product criterion [35, Theorem 4.1] now applies: the symplectic algebras are simple, their standard modules are irreducible, and every automorphism preserves the standard module. Indeed, a proper semisimple subdirect product would identify two simple factors, yielding an intertwiner of their Tate modules after a finite extension. Faltings's homomorphism theorem [19] would contradict geometric Hom-vanishing. Thus the derived Lie algebra is the full direct sum. Polarizations force a common scalar line, and the cyclotomic character supplies that line.

The algebraic monodromy group lies in the connected group $\mathcal{G}_{\mathbb{Q}_\ell}$ and has its full Lie algebra, hence equals it. The usual inclusion of the ℓ-adic Lie algebra in the Mumford–Tate Lie algebra, together with the bound from polarizations, gives $\mathrm{MT}(B) = \mathcal{G}$ and the stated Hodge group; compare [47, proof of Theorem 9.1]. Repeated factors merely repeat the representations.

Finally, invariants of each symplectic factor are generated by pairwise contractions. In cohomology these are divisor classes, obtained from polarizations by pullback and addition between repeated copies; see [47, Theorems 8.1 and 9.1]. The same argument applies to every power. Finite extensions of K do not change the Lie algebra, so it covers all the stated Tate classes. The equality $\mathcal{G} = \mathbb{G}_m \cdot \prod_i \mathrm{Sp}(V_i)$ is algebraic and need not give the corresponding factorization of rational points. □

Corollary 6.11. *For pairwise distinct $n_i \geq N$ and arbitrary positive integers s_i, e_i, the product $\prod_i J_{n_i,s_i}^{e_i}$ satisfies every conclusion of Theorem 6.10. In particular, $J_{2g+1,s}$ and $J_{2g+2,t}$ are nonisogenous Jacobians of the same dimension for every $s, t \geq 1$ if $2g+1 \geq N$.*

Proof. Apply Theorem 1.1. □

6.4. **Further questions.** Theorem 1.1 gives a uniform eventual form of Hajir's conjectures. Corollary 5.6 reduces both all-degree conjectures to an effective finite verification. The remaining question is whether that finite exceptional set is empty. The current bounds do not make its enumeration practical. An all-degree proof needs estimates that remain useful when the degree is comparable to the constants in the local and logarithmic arguments. Equivalently, one may ask for irreducibility and alternating containment for every nonconstant numerator and denominator in the exponential Padé table.

The finite-fiber theorem suggests a broader irreducibility problem. For fixed positive integers $c_1, \ldots, c_r$, consider

$$P_{n,s}(X) = n![z^n]e^{Xz} \prod_{\nu=1}^{r} (1 - c_\nu z)^{-s}.$$

Does there exist an effective $N(c_1, \dots, c_r)$ such that $P_{n,s}$ is irreducible for every $n \geq N(c_1, \dots, c_r)$ and every positive integer s? Generic irreducibility is immediate: Eisenstein at $s = 0$ applies because

$$[s]P_{n,s}(0) = (n-1)! \sum_{\nu=1}^{r} c_\nu^n \neq 0.$$

The specialization problem needs more information. For each fixed $c \geq 2$ outside the finite set $\mathcal{E}$, Corollary 6.2 treats $P_{n,s}^{(c)}$ when $\log s \geq n^\varepsilon$, for every fixed $\varepsilon > 0$. A proof in $1 \leq s \leq \exp(n^\delta)$ for one fixed $\delta > 0$ would therefore complete the uniform argument for that scale. The Laguerre energy proof does not transfer directly: the two-scale degenerate fibers have cluster sizes $n - 2j$, so in even degree a factor of half the degree can have the same occupation ratio in every such cluster. One must break this possible balance or find a different source of arithmetic control. For three or more scales, a structural trace-separation theorem would also be preferable to a separate elimination certificate for each choice of scales.

Theorem 4.3 and its Newton-polygon consequence isolate a different question. For trimmed exponentials, the remaining irreducibility hypothesis is removed here by an endpoint valuation condition. A uniform irreducibility theorem without that condition would give the full symmetric group throughout the same logarithmic parameter range. The nonsquare-discriminant theorem already has no upper bound on u. Can its lower restriction $u \geq (\gcd(u, 2) - 1 + \eta)n$ be removed for all sufficiently large degrees? These are partial steps toward the full symmetric-group conjecture of Bary-Soroker–Ben-Porath [3]; the current argument neither proves irreducibility for every endpoint nor covers every relation between u and n. The lower bound $(\log n)^\kappa$, $\kappa > 5$, comes from the small-prime allocation and the height product in the simultaneous logarithmic estimate. Replacing it by a bound of order $\log n$ would extend this criterion to parameters of polynomial size; the present estimate does not reach that range.

Finally, Theorem 4.21 is geometric, whereas the application to quadratic subfields also uses arithmetic bounds for the interpolants. It would be useful to obtain such bounds for other covers from explicit ramification and height data. The Hermite argument here uses integral derivative identities and Gaussian quadrature, so those bounds are not supplied by the geometric theorem alone. For higher cyclic degree, one must also control all relevant embeddings and the possible effect of units; a small value at one embedding no longer gives the imaginary-quadratic contradiction used in Section 4.4.4. A quantitative interpolation theorem with a second arithmetic application would substantially extend this part of the method.

Appendix A. The root-modulus representation

We prove Theorem 2.5 by continuing the roots through the upper half of the parameter plane. At each parameter $0, -1, \dots, 1-n$, one more branch reaches the positive real axis. Keeping track of this order determines the boundary jump of the holomorphic continuation of the positive-axis modulus. Its expansion at infinity then permits Cauchy's formula to recover the representing measure.

Lemma A.1. *Let $1 - n < s < 0$ be real. Every root of $H_{n,s}$ that is not positive real has modulus less than $n + s - 1$. Two distinct nonzero roots cannot lie on the same ray except on the positive real axis.*

Proof. The matrix argument in Lemma 2.1 remains valid for the upper bound even when D_0 has negative diagonal entries. For a nonzero root x not on the positive real axis, choose $z^2 = x$ with $\Im z \neq 0$. It gives $|x| = v^* D_0 v < n + s - 1$; strictness follows from the same endpoint coupling. A zero root satisfies the bound as well.

Put $A = n + s - 1 \in (0, n-1)$ and $\kappa = n - A/2 > A/2$. The ray substitution used in Proposition 2.7 gives (2.20), which is valid for every real parameter. Suppose two roots lie on

a nonreal ray, at radii $\rho_1 < \rho_2$. Both are less than A. Multiply this equation by $\bar{u}$, integrate between the two radii, and take imaginary parts. The endpoint terms vanish, giving

$$\sin\theta \int_{\rho_1}^{\rho_2} \left(\frac{\kappa}{\rho} - \frac{\cos\theta}{2} \right) |u|^2 \, d\rho = 0.$$

The parenthesized function is strictly positive, since $\rho < A < 2\kappa$, and u is not identically zero. This is impossible. On the negative real ray the potential in the differential equation is strictly negative; the real part of the same integrated identity is then $-\int |u'|^2 + \int V|u|^2 = 0$ with $V < 0$, also impossible. □

Proof of Theorem 2.5. Continuation and boundary labels. The roots are simple and nonzero when $\Im s > 0$. Monicity bounds them on compact parameter sets, so each root continues along every path in that half-plane. Since the domain is simply connected, we obtain n single-valued, non-vanishing holomorphic root functions, each with a holomorphic logarithm. They extend locally across every real parameter outside $\{0, -1, \ldots, 1-n\}$.

We describe their boundary labels explicitly. For $0 \le m \le n-1$ put $N = n - m$. Directly from the coefficient formula,

$$H_{n,-m}(X) = X^N J_{m,n}(X), \qquad J_{m,n}(0) = (-1)^m \frac{n!}{N!}. \tag{A.1}$$

The m zeros of $J_{m,n}$ are simple and positive. Indeed,

$$J_{m,n}(X) = (-1)^m e^X X^{-N} \frac{d^m}{dX^m}(e^{-X} X^n).$$

Integration by parts shows that this monic degree-m polynomial is orthogonal to every polynomial of smaller degree for the weight $X^N e^{-X}$ on $(0, \infty)$. All boundary terms vanish. If it had fewer than m sign changes on that interval, multiplication by the product of its sign-changing linear factors would give a polynomial of smaller degree whose weighted product with $J_{m,n}$ has constant nonzero sign, contradicting orthogonality. It therefore has exactly m distinct positive roots. The assertion is vacuous when $m = 0$.

Write $s = -m + \delta$. The N roots tending to zero satisfy

$$X^N = -c_m \delta (1 + o(1)), \qquad c_m = \frac{m!(N-1)!N!}{n!} > 0. \tag{A.2}$$

To see this, balance the coefficient $J_{m,n}(0)$ of X^N against $H_{n,-m+\delta}(0) = (-1)^m m!(N-1)!\delta + O(\delta^2)$. More explicitly, with $\rho = \delta^{1/N}$, the polynomial $\rho^{-N} H_{n,-m+\rho^N}(\rho w)$ extends holomorphically to $\rho = 0$, with value $J_{m,n}(0)(w^N + c_m)$. Its roots are simple. The holomorphic implicit function theorem gives the asserted asymptotics uniformly for $0 \le \arg\delta \le \pi$, with a continuous choice of $\delta^{1/N}$. On the right of $-m$ the limiting arguments are $(2j+1)\pi/N$, $0 \le j < N$. Moving around a small upper semicircle increases each limiting argument by π/N. The last branch thus reaches the positive axis with continuous argument 2π. This branch is positive real just to the left of $-m$: writing $\delta = -r^N$ and $X = rw$ with $r > 0$, its limiting w-root is positive and simple, so the real implicit function theorem gives a positive real branch.

On $(-m, -m+1)$, $1 \le m \le n-1$, the coefficient signs in descending powers alternate through $(s)_m$ and are thereafter constant. There are exactly m variations. Descartes' rule allows at most m positive roots; near the left endpoint (A.1) supplies m such simple roots. They remain positive throughout the interval: leaving the real axis or changing sign would require a collision or a zero root. There are consequently exactly m positive roots. These are precisely the branches tending to the nonzero endpoint roots; all other branches tend to zero at the left endpoint. Indeed, any branch approaching a nonzero positive endpoint root is real and positive nearby by the implicit function theorem. A branch off the positive real axis cannot meet that axis in the interval, because

a simple real root has a unique real local continuation. By Lemma A.1, the remaining branches cannot exchange angular order.

Near $s = 0+$ label the roots $x_0, \dots, x_{n-1}$ in increasing argument order in $(0, 2\pi)$, and choose their holomorphic logarithms accordingly. For $s > 0$ these continuous arguments remain in that interval. Conjugation pairs j with $n-1-j$, first near zero and then everywhere on the positive axis by uniqueness and absence of collisions. Their arguments sum to 2π.

These observations give an induction across $0, -1, \dots, 1-n$. On $(-m, -m+1)$ put $N = n-m$ and write $\theta_r = \Im \log x_r$ for the continued arguments. Then

$$\begin{gathered} 0 < \theta_0 < \cdots < \theta_{N-1} < 2\pi, \qquad \theta_r + \theta_{N-1-r} = 2\pi \quad (0 \le r < N), \\ \theta_N = \cdots = \theta_{n-1} = 2\pi. \end{gathered} \tag{A.3}$$

Indeed, the m positive branches have argument 2π and are the labels already removed at earlier crossings. The other branches preserve their angular order by Lemma A.1. At $s = -m$, (A.2) rotates their limiting arguments from $(2r+1)\pi/N$ to $2(r+1)\pi/N$, so label $N-1$ becomes the next positive branch. After $s = 1-n$, all roots are positive with continued argument 2π. They remain so for $s < 1-n$, since no further collision or zero root is possible.

Continuing the modulus. For an original conjugate pair $j, k = n-1-j$, $j < k$, define in the upper half-plane

$$q(s) = \exp\left(\frac{\log x_j(s) + \log x_k(s) - 2\pi i}{2}\right). \tag{A.4}$$

On $s > 0$ this is positive and equals $|x_j(s)|$. The chosen logarithms specify the square root throughout the parameter domain. On the negative axis the continuous argument sum of x_j, x_k lies in $[2\pi, 4\pi]$. To verify the lower bound when both labels still lie off the positive real axis, let N be the number of remaining such labels. Conjugation gives $\theta_j + \theta_{N-1-j} = 2\pi$, while $k = n-1-j \ge N-1-j$ and angular order give $\theta_k \ge \theta_{N-1-j}$. If one or both labels have become positive, their arguments are 2π, and the bound is immediate. The upper bound follows because no individual argument exceeds 2π. Hence the boundary argument of q is in $[0, \pi]$.

For odd n, the real root has label $j = (n-1)/2$. While this label remains off the positive real axis, it lies at or above the middle of the remaining ordered labels, so its continuous argument belongs to $[\pi, 2\pi)$. Afterwards its argument is 2π. The function $q = -x_j$ therefore has the same boundary-argument property. In both cases q is holomorphic and nonvanishing in the upper half-plane, and its boundary imaginary part is nonnegative.

The expansion at infinity. Put $z = s^{-1/2}$, with $-\pi/2 \le \arg z \le 0$ for s in the closed upper half-plane. The scaled polynomial $F_n(w, z)$ in (2.17) has limiting polynomial $h_n(w)$ with simple purely imaginary zeros, as proved in Section 2.1. Each zero therefore extends to a holomorphic root germ $w_j(z)$ in a full disk about zero.

For positive z, conjugate roots have opposite limiting w-roots. The identity $F_n(-w, -z) = (-1)^n F_n(w, z)$ and uniqueness of the root germs imply $w_k(z) = -w_j(-z)$ for such a pair. The uncentered roots $x_j(z) = z^{-1} w_j(z) - z^{-2}$ consequently satisfy $x_k(z) = x_j(-z)$. Their product is an even Laurent series beginning with $z^{-4} = s^2$. Its square root that is positive for large positive s has an expansion $s + \theta + O(s^{-1})$, with $\theta \in \mathbb{R}$. For the real root in odd degree, the germ with limiting w-root zero is odd in z, and its uncentered root is itself an even Laurent series, giving the same expansion for $q = -x_j$.

The germs and the already continued functions agree on the positive axis and extend across it; the identity theorem identifies them in the exterior upper half-plane. Convergence of the full germ expansions gives, uniformly in that closed half-plane as $|s| \to \infty$,

$$q(s) = s + \theta + O(s^{-1}), \qquad \theta \in \mathbb{R}. \tag{A.5}$$

Cauchy's formula and the measure. The root functions have convergent expansions in $(s+m)^{1/N}$ at each singular parameter $-m$, by the rescaling in (A.2); the nonzero root branches are analytic

there. The function q therefore has a finite, continuous boundary value at each such point. If either root used in (A.4) vanishes, then q tends to zero. The same statement holds for the single real branch. In particular, $q(s) = O(|s|^{1/n})$ near zero in the closed upper half-plane.

The boundary values of q are real for $s > 0$ and for $s < 1 - n$; in the latter interval they are negative, by the continued arguments above. Schwarz reflection therefore gives a holomorphic function on $\mathbb{C} \setminus [1 - n, 0]$, whose two boundary values on the cut are conjugate. Put $\psi(t) = \Im q(-t + i0)$. The argument bounds already proved give $\psi \geq 0$. Also ψ is bounded on the cut, and $\psi(t) = O(t^{1/n})$ as $t \downarrow 0$.

Apply Cauchy's formula to $q(s) - s - \theta$ around the cut. The expansion (A.5) removes the large-circle integral; boundedness removes the small arcs about the finitely many singular points. The jump across the cut is $2i\psi(t)$, so

$$q(s) = s + \theta - \frac{1}{\pi} \int_0^{n-1} \frac{\psi(t)}{s + t}\, dt \qquad (s \in \mathbb{C} \setminus [1 - n, 0]). \tag{A.6}$$

Because $\psi(t)/t = O(t^{1/n-1})$ near zero, this quotient is integrable. Letting $s \downarrow 0$ and using dominated convergence gives

$$\theta = \frac{1}{\pi} \int_0^{n-1} \frac{\psi(t)}{t}\, dt.$$

Hence (2.15) holds with the finite nonnegative measure

$$d\mu(t) = \frac{\psi(t)}{\pi t}\, dt. \tag{A.7}$$

There are no endpoint atoms: the formula is obtained from the full contour, and every indentation integral tends to zero. If two finite measures on $[0, n-1]$ gave the same representation, expansion for large s would equate all their moments. Density of polynomials in $C[0, n-1]$ then makes the measures equal. Finally, the integrand $s/(s + t)$ is nondecreasing in $s > 0$, proving the stated monotonicity. □

Proposition A.2. *Fix $n \geq 2$. For $0 \leq j \leq \lfloor (n-1)/2 \rfloor$, label a root branch by*

$$\alpha_j(s) = ((n-1)!s)^{1/n} \exp\Big(\frac{(2j+1)\pi i}{n}\Big) + o(s^{1/n}) \qquad (s \downarrow 0),$$

and continue it along the positive real axis. Put $q_j(s) = |\alpha_j(s)|$ and $L_j = n-1-j$. The nonnegative measure in the representation

$$q_j(s) = s + \int \frac{s}{s + t}\, d\mu_j(t)$$

has support exactly $[0, L_j]$. It has a density that is strictly positive on $(m, m+1)$ for every integer $0 \leq m < L_j$, and zero for $t > L_j$. In particular, if

$$M_j = \frac{n-1}{3} + \frac{\xi_j^2}{6}, \qquad \alpha_j(s) = -s + i\xi_j\sqrt{s} + O(1) \quad (s \longrightarrow \infty),$$

then

$$M_j \frac{s}{s + L_j} < q_j(s) - s < M_j \qquad (s > 0). \tag{A.8}$$

For odd n and $j = (n-1)/2$, this is the real root branch, $\xi_j = 0$, and $L_j = (n-1)/2$.

Proof. On $(-m, -m+1)$, $1 \leq m \leq n-1$, put $N = n - m$ and use the continued arguments in (A.3). First suppose $j < k = n - 1 - j$. If $j, k < N$, then $k > N - 1 - j$, because $m > 0$. Thus

$$2\pi < \theta_j + \theta_k < 4\pi.$$

If $j < N \leq k$, the sum is $\theta_j + 2\pi$ and satisfies the same strict inequalities. If $N \leq j$, both arguments are 2π. The holomorphic modulus branch has continuous argument $(\theta_j + \theta_k - 2\pi)/2$.

Its boundary imaginary part is therefore strictly positive while $m \le n-1-j$, and is zero once $m \ge n-j$. These are precisely the regular negative parameters $s = -t$ with $0 < t < L_j$ and $t > L_j$, respectively.

If n is odd and $j = (n-1)/2$, the same conclusion follows from $q_j = -\alpha_j$: while $j < N$, one has $j > (N-1)/2$ and hence $\pi < \theta_j < 2\pi$; once $N \le j$, the root has argument 2π. The transition is at $t = j = L_j$.

In either case the representation obtained from Cauchy's formula is

$$d\mu_j(t) = \frac{\operatorname{Im} q_j(-t+i0)}{\pi t}\, dt.$$

The density is positive on every indicated open interval. It vanishes past L_j, and there are no atoms at the finitely many singular parameters. Consequently the support is exactly $[0, L_j]$. Integrating

$$\frac{s}{s+L_j} \le \frac{s}{s+t} \le 1$$

and using the already established mass $\mu_j([0,L_j]) = M_j$ gives the last inequalities. They are strict because the measure has positive density on $(0, L_j)$ away from finitely many points. □

Appendix B. An exact certificate for the Appell family

The two resultants $\mathcal{D}_i(N) = D_i(N,2)$ eliminate the factor degree before the degree parameter N is specialized. To prove $\mathcal{D}_0(11)\mathcal{D}_1(11) \neq 0$, we work over $\mathbb{F}_{479}$. This single exact calculation also proves that $\mathcal{D}_0, \mathcal{D}_1$ are nonzero polynomials in N. The residual polynomials at $N = 11$ are

$$R_2(11,X) = X^4 - 66X^3 + 1430X^2 - 11880X + 31680,$$
$$R_3(11,X) = X^6 - 99X^5 + 3630X^4 - 62370X^3 + 522720X^2 - 1995840X + 2661120.$$

The first polynomial has four distinct roots

$$\{72, 180, 353, 419\} \subset \mathbb{F}_{479}.$$

Its nonempty proper subsets have fourteen distinct sums, namely

$$S = \{12, 54, 72, 120, 126, 180, 192, 252, 293, 353, 365, 419, 425, 473\}.$$

These are the roots of $V_2(11, Z)$. Thus the first polynomials defining $\mathcal{D}_0(11)$ and $\mathcal{D}_1(11)$ have roots $z/6$ and $z/3$, respectively, for $z \in S$. Their companion factors take the following values; V_3 abbreviates $V_3(11,\cdot)$.

z	$V_3(3z/2)$	$V_3(2z)$
12	442	466
54	442	222
72	222	452
120	391	238
126	78	27
180	181	347
192	382	320
252	313	457
293	313	60
353	382	112
365	181	74
419	78	151
425	391	262
473	222	53

Every entry is nonzero. Each specialized pair is therefore relatively prime. The four leading coefficients are $6^{14}, 9^{62}, 3^{14}, 6^{62}$, all nonzero modulo 479; specialization consequently preserves the Sylvester resultants. This proves their required nonvanishing.

The table can be reproduced using matrices of order at most 20. Let C be the companion matrix of

$$X^6 + 380X^5 + 277X^4 + 379X^3 + 131X^2 + 153X + 275 \quad \text{over } \mathbb{F}_{479}.$$

For $1 \le k \le 5$, let $C^{[k]}$ act on $\bigwedge^k \mathbb{F}_{479}^6$ by

$$C^{[k]}(v_1 \wedge \cdots \wedge v_k) = \sum_{j=1}^{k} v_1 \wedge \cdots \wedge Cv_j \wedge \cdots \wedge v_k.$$

The eigenvalues of this additive exterior-power operator are the k-element subset sums of the eigenvalues of C. Consequently

$$V_3(11, Z) = \prod_{k=1}^{5} \det(ZI - C^{[k]}).$$

Triangularization proves the identity without a separability assumption.

References

[1] P. Banerjee and R. Bera, Classifying families of orthogonal polynomials having Galois group the alternating group, *J. Number Theory* **240** (2022), 31–49. doi:10.1016/j.jnt.2021.12.009.

[2] P. Banerjee, M. Filaseta, C. E. Finch and J. R. Leidy, On classifying Laguerre polynomials which have Galois group the alternating group, *J. Théor. Nombres Bordeaux* **25** (2013), no. 1, 1–30. doi:10.5802/jtnb.822.

[3] L. Bary-Soroker and O. Ben-Porath, On the Galois theory of generalized Laguerre polynomials and trimmed exponential, *Acta Arith.* **200** (2021), no. 2, 183–196. doi:10.4064/aa200825-7-3.

[4] L. Bary-Soroker and B. Kadets, *Generic Manin–Mumford*, preprint (2026), arXiv:2609.09354.

[5] J. Borcea and P. Brändén, Pólya–Schur master theorems for circular domains and their boundaries, *Ann. of Math. (2)* **170** (2009), 465–492. doi:10.4007/annals.2009.170.465.

[6] M. G. de Bruin, E. B. Saff, and R. S. Varga, On the zeros of generalized Bessel polynomials. I, *Indag. Math. (Proceedings)* **84** (1981), no. 1, 1–13. doi:10.1016/1385-7258(81)90013-5.

[7] T. C. Burness and R. M. Guralnick, Fixed point ratios for finite primitive groups and applications, *Adv. Math.* **411** (2022), 108778. doi:10.1016/j.aim.2022.108778.

[8] G. Butler and J. McKay, The transitive groups of degree up to eleven, *Comm. Algebra* **11** (1983), no. 8, 863–911. doi:10.1080/00927878308822884.

[9] K. Castillo, Complete Bernstein functions and scaled ultraspherical zeros, preprint (2026), arXiv:2609.19186.

[10] R. F. Coleman, On the Galois groups of the exponential Taylor polynomials, *Enseign. Math.* (2) **33** (1987), no. 3–4, 183–189. doi:10.5169/seals-87891.

[11] J. Cullinan and N. Scheel, On the arithmetic of Padé approximants to the exponential function, *J. Ramanujan Math. Soc.* **37** (2022), no. 3, 207–219. `https://www.mathjournals.org/jrms/2022-037-003/2022-037-003-001.html`.

[12] Z. Deng, A proof of the irreducibility conjecture for Legendre polynomials, preprint (2026), arXiv:2609.22336.

[13] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, vol. 163, Springer, New York, 1996. doi:10.1007/978-1-4612-0731-3.

[14] P. Dusart, Explicit estimates of some functions over primes, *Ramanujan J.* **45** (2018), no. 1, 227–251. doi:10.1007/s11139-016-9839-4.

[15] P. Dusart, Estimates of some functions over primes without R.H., preprint (2010), arXiv:1002.0442.

[16] P. Erdős, On consecutive integers, *Nieuw Arch. Wisk. (3)* **3** (1955), 124–128.

[17] P. Erdős and J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* **19** (1975), no. 2, 292–301. `https://users.renyi.hu/~p_erdos/1975-46.pdf`.

[18] P. Erdős and J. Turk, Products of integers in short intervals, *Acta Arith.* **44** (1984), no. 2, 147–174. doi:10.4064/aa-44-2-147-174.

[19] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366. doi:10.1007/BF01388432.

[20] K. Fan, On a theorem of Weyl concerning eigenvalues of linear transformations. I, *Proc. Natl. Acad. Sci. USA* **35** (1949), no. 11, 652–655. doi:10.1073/pnas.35.11.652.

[21] M. Filaseta, The irreducibility of all but finitely many Bessel polynomials, *Acta Math.* **174** (1995), no. 2, 383–397. doi:10.1007/BF02392470.
[22] M. Filaseta and T.-Y. Lam, On the irreducibility of the generalized Laguerre polynomials, *Acta Arith.* **105** (2002), no. 2, 177–182. doi:10.4064/aa105-2-4.
[23] M. Filaseta, S. Laishram, and N. Saradha, Solving $n(n+d)\cdots(n+(k-1)d) = by^2$ with $P(b) \leq Ck$, *Int. J. Number Theory* **8** (2012), 161–173. doi:10.1142/S1793042112500091.
[24] M. Filaseta and O. Trifonov, The irreducibility of the Bessel polynomials, *J. Reine Angew. Math.* **550** (2002), 125–140. doi:10.1515/crll.2002.069.
[25] K. Ford, The distribution of integers with a divisor in a given interval, *Ann. of Math. (2)* **168** (2008), no. 2, 367–433. doi:10.4007/annals.2008.168.367.
[26] E. Grosswald, On some algebraic properties of the Bessel polynomials, *Trans. Amer. Math. Soc.* **71** (1951), no. 2, 197–210. doi:10.1090/S0002-9947-1951-0053280-2.
[27] E. Grosswald, *Bessel Polynomials*, Lecture Notes in Mathematics, vol. 698, Springer, Berlin–New York, 1978. doi:10.1007/BFb0063135.
[28] F. Hajir, On the Galois group of generalized Laguerre polynomials, *J. Théor. Nombres Bordeaux* **17** (2005), 517–525. doi:10.5802/jtnb.505.
[29] F. Hajir, Algebraic properties of a family of generalized Laguerre polynomials, *Canad. J. Math.* **61** (2009), no. 3, 583–603. doi:10.4153/CJM-2009-031-6.
[30] F. Hajir and S. Wong, Specializations of one-parameter families of polynomials, *Ann. Inst. Fourier (Grenoble)* **56** (2006), no. 4, 1127–1163. doi:10.5802/aif.2208.
[31] A. Jindal and S. Laishram, Families of Laguerre polynomials with alternating group as Galois group, *J. Number Theory* **241** (2022), 387–429. doi:10.1016/j.jnt.2022.04.001.
[32] A. Jindal, S. Laishram, and R. Sarma, Irreducibility and Galois groups of generalized Laguerre polynomials $L_n^{(-1-n-r)}(x)$, *J. Number Theory* **183** (2018), 388–406. doi:10.1016/j.jnt.2017.08.003.
[33] A. Jindal, S. G. Nair, and T. N. Shorey, Extension of irreducibility results on generalized Laguerre polynomials $L_n^{(-n-s-1)}(x)$, *Publ. Math. Debrecen* **105** (2024), no. 3–4, 473–494. doi:10.5486/PMD.2024.9906.
[34] A. Levin, Variations on a theme of Runge: effective determination of integral points on certain varieties, *J. Théor. Nombres Bordeaux* **20** (2008), no. 2, 385–417. doi:10.5802/jtnb.634.
[35] D. Lombardo, On the ℓ-adic Galois representations attached to nonsimple abelian varieties, *Ann. Inst. Fourier (Grenoble)* **66** (2016), no. 3, 1217–1245. doi:10.5802/aif.3035.
[36] J. H. Loxton, Some problems involving powers of integers, *Acta Arith.* **46** (1986), no. 2, 113–123. doi:10.4064/aa-46-2-113-123.
[37] A. W. Marcus, D. A. Spielman, and N. Srivastava, Finite free convolutions of polynomials, *Probab. Theory Related Fields* **182** (2022), 807–848. doi:10.1007/s00440-021-01105-w.
[38] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. II, *Izv. Math.* **64** (2000), no. 6, 1217–1269. doi:10.1070/IM2000v064n06ABEH000314.
[39] J. Nagura, On the interval containing at least one prime number, *Proc. Japan Acad.* **28** (1952), no. 4, 177–181. doi:10.3792/pja/1195570997.
[40] NIST Digital Library of Mathematical Functions, Chapter 18, Orthogonal Polynomials, especially §§18.5, 18.7–18.8, 18.9, and 18.34. `https://dlmf.nist.gov/18` (accessed 4 November 2026).
[41] P. Rabarison, F. Pazuki, and P. Molin, Exponentielle tronquée et autres contes galoisiens, *Publ. Math. Besançon Algèbre Théor. Nombres* (2024), 105–117. doi:10.5802/pmb.57.
[42] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), no. 1, 64–94. doi:10.1215/ijm/1255631807.
[43] I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen. I, *Sitzungsber. Preuss. Akad. Wiss., Phys.-Math. Kl.* (1929), 125–136.
[44] I. Schur, Gleichungen ohne Affekt, *Sitzungsber. Preuss. Akad. Wiss., Phys.-Math. Kl.* (1930), 443–449.
[45] I. Schur, Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome, *J. Reine Angew. Math.* **165** (1931), 52–58. doi:10.1515/crll.1931.165.52.
[46] C. L. Stewart, On heights of multiplicatively dependent algebraic numbers, *Acta Arith.* **133** (2008), no. 2, 97–108. doi:10.4064/aa133-2-1.
[47] Y. G. Zarhin, Very simple 2-adic representations and hyperelliptic jacobians, *Mosc. Math. J.* **2** (2002), no. 2, 403–431. doi:10.17323/1609-4514-2002-2-2-403-431.
[48] Y. G. Zarhin, Homomorphisms of hyperelliptic Jacobians, *Proc. Steklov Inst. Math.* **241** (2003), 79–92. `https://www.mathnet.ru/eng/tm389`.