Canad. J. Math. Vol. **61** (3), 2009 pp. 583–603

Algebraic Properties of a Family of Generalized Laguerre Polynomials

Farshid Hajir

Abstract. We study the algebraic properties of Generalized Laguerre Polynomials for negative integral values of the parameter. For integers $r, n \geq 0$, we conjecture that $L_n^{(-1-n-r)}(x) = \sum_{j=0}^{n} \binom{n-j+r}{n-j} x^j/j!$ is a $\mathbb{Q}$-irreducible polynomial whose Galois group contains the alternating group on n letters. That this is so for $r = n$ was conjectured in the 1950's by Grosswald and proven recently by Filaseta and Trifonov. It follows from recent work of Hajir and Wong that the conjecture is true when r is large with respect to $n \geq 5$. Here we verify it in three situations: (i) when n is large with respect to r, (ii) when $r \leq 8$, and (iii) when $n \leq 4$. The main tool is the theory of p-adic Newton Polygons.

1 Background and Summary of Results

The *Generalized Laguerre Polynomial* (GLP) is a one-parameter family defined by

$$L_n^{(\alpha)}(x) = (-1)^n \sum_{j=0}^{n} \binom{n+\alpha}{n-j} \frac{(-x)^j}{j!}.$$

Here, as usual, the binomial coefficient $\binom{t}{k}$ is defined to be $t(t-1)\cdots(t-k+1)/k!$ for non-negative integers k; the inclusion of the sign $(-1)^n$ is not standard. Sometimes it is more convenient to work with the monic integral polynomial $\mathcal{L}_n^{(\alpha)}(x) = n!L_n^{(\alpha)}(x)$. The monographs by Pólya and Szegő [PZ], Szegő [Sz], and Andrews, Askey, and Roy [AAR] contain a wealth of facts about this and other families of orthogonal polynomials. We have the second order linear (hypergeometric) differential equation

$$xy'' + (\alpha + 1 - x)y' + ny = 0, \qquad y = L_n^{(\alpha)}(x),$$

as well as the difference equation

$$L_n^{(\alpha-1)}(x) - L_n^{(\alpha)}(x) = L_{n-1}^{(\alpha)}(x).$$

A quick glance at the mathematical literature makes it clear that the GLP has been extensively studied primarily because of the very important roles it plays in various branches of analysis and mathematical physics. However, not long after its appearance in the literature early in the twentieth century, it became evident, in the hands of Schur, that the GLP also enjoys algebraic properties of great interest.

Received by the editors September 5, 2006.
This work was supported by the National Science Foundation under Grant No. 0226869.
AMS subject classification: Primary: 11R09; secondary: 05E35.

For instance, in 1931, Schur [Sc2] gave a pretty formula for the discriminant of $\mathcal{L}_n^{(\alpha)}(x)$:

$$\Delta_n^{(\alpha)} = \prod_{j=2}^{n} j^j(\alpha + j)^{j-1}. \tag{1.1}$$

In [Sc1, Sc2], he showed that $L_n^{(0)}(x)$ (classical Laguerre polynomial, first studied by Abel), and $L_n^{(1)}(x)$ (derivative of classical Laguerre), are irreducible in $\mathbb{Q}[x]$ for all n; he also calculated their Galois groups.

Recently, a number of articles concentrating on the algebraic properties of the GLP have appeared, including Feit [F], Coleman [C], Gow [Go], Hajir [H1], Filaseta and Williams[FW], and Sell [S]. In all of these papers, the authors take a sequence $(\alpha_n)_n$ of rational numbers and consider the irreducibility and Galois group of $L_n^{(\alpha_n)}(x)$ over $\mathbb{Q}$. The best general such result to date is for constant sequences α_n.

***Theorem* (Filaseta–Lam/Hajir)** *Suppose α is a fixed rational number which is not a negative integer. Then for all but finitely many integers $n \geq 0$, $L_n^{(\alpha)}(x)$ is irreducible over $\mathbb{Q}$ and has Galois group containing A_n.*

It should be noted that the reducible GLP for rational values of the parameter α do exist (already infinitely many exist in degrees 2, 3, or 4, cf. Section 6). The irreducibility part of the above theorem is due to Filaseta and Lam [FL]; the supplement on the Galois group was added in [H2]. The proof of both parts is effective.

At the values of the parameter α excluded by the theorem of Filaseta and Lam (the negative integers), one finds some of the most interesting families of GLP, *e.g.,* the truncated exponential series, and the Bessel Polynomials (see below). In this paper, we consider irreducibility and Galois groups of GLP for exactly these values of the parameter α. Note that their exclusion from the theorem is quite necessary; namely, when α is a negative integer, $L_n^{(\alpha)}(x)$ is reducible for all $n \geq |\alpha|$. Indeed, writing $\alpha = -a$ with $n = a + m$, where a is an integer in $[1, n]$ we have

$$\mathcal{L}_n^{(-a)}(x) = x^a \cdot \mathcal{L}_m^{(a)}(x), \qquad \mathcal{L}_m^{(a)}(0) \neq 0.^1 \tag{1.2}$$

Given the above observation, namely that for small negative integral values of the parameter α, $L_n^{(\alpha)}(x)$ is a simple factor times a Laguerre polynomial of positive parameter, it is natural to replace the parameter α by a parameter r via the translation $\alpha = -1 - n - r$, and to consider instead

$$L_n^{\langle r \rangle}(x) := L_n^{(-1-n-r)}(x) = \sum_{j=0}^{n} \binom{n-j+r}{n-j} \frac{x^j}{j!}. \tag{1.3}$$

[1] Incidentally, the repeated roots at the origin evident in the above factorization (for $2 \leq a \leq n$ *i.e.,* $-n \leq \alpha \leq -2$) explain the presence of the factors $\alpha + j$, $j = 2, \ldots, n$, in (1.1). Their multiplicites in the discriminant (*i.e.,* $j - 1$) express the tameness of the corresponding ramified points in the extension $\mathbb{C}(\alpha) \hookrightarrow \mathbb{C}(\alpha)[x]/(L_n^{(\alpha)}(x))$ of function fields. It would be interesting to obtain a similarly conceptual explanation of the factors j^j as well.

It is also useful to note that

$$\mathcal{L}_n^{\langle r\rangle}(x) := n!L_n^{\langle r\rangle}(x) = \sum_{j=0}^{n} \binom{n}{j}(r+1)(r+2)\cdots(r+n-j)x^j, \tag{1.4}$$

is monic and has positive integer coefficients, assuming, as we do throughout the paper, that r is a non-negative integer.

The parametrization (1.3) is a natural one in some respects (in addition to being a convenient representation of the family of polynomials we wish to consider). For instance, differentiation with respect to x of $L_n^{(\alpha)}(x)$ has the effect of lowering n by 1 and raising α by 1, so in the new parametrization, differentiation leaves r fixed: $\partial_x L_n^{\langle r\rangle}(x) = L_{n-1}^{\langle r\rangle}(x)$. Indeed, the most familiar such "derivative-coherent" sequence of polynomials, namely the truncations of the exponential series, is obtained when we set $r = 0$:

$$E_n(x) := L_n^{\langle 0\rangle}(x) = \sum_{j=0}^{n} \frac{x^j}{j!}.$$

Let us review some known algebraic facts about $L_n^{\langle r\rangle}(x)$ for small $r \geq 0$. The exponential Taylor polynomials E_n were first studied by Schur. He showed that they are irreducible over $\mathbb{Q}$ [Sc1], and have Galois group A_n or S_n (over $\mathbb{Q}$) according to whether n is divisible by 4 or not [Sc2]. Coleman [C] gave a different proof of these results. For the case $r = 1$, irreducibility and the calculation of the Galois group using methods of Coleman and Schur, respectively, were established in [H1]. Moreover, in [H1], the values of n for which the splitting field of $L_n^{\langle 0\rangle}(x)$ or $L_n^{\langle 1\rangle}(x)$ can be embedded in an $\tilde{A}_n$-extension were determined using formulae of Feit [F] and a criterion of Serre [Se]. All of the above was carried out for $r = 2$ by Sell in [S]. But perhaps the best-studied family of GLP is that of Bessel Polynomials (BP) $z_n(x)$ which are simply the monic GLP with $r = n$. Namely we have

$$z_n(x) := \sum_{j=0}^{n} \frac{(2n-j)!}{j!(n-j)!}x^j = \mathcal{L}_n^{\langle n\rangle}(x).$$

Grosswald pointed out that the BPs play a distinguished role among GLPs due to certain "symmetries" which in our notation amounts to their invariance under exchange of r and n. They are arithmetically interesting as well (for example the prime 2 does not ramify in the algebra $\mathbb{Q}[x]/(z_n(x))$ despite the presence of many powers of 2 in the discriminant of z_n, cf. (1.1)). Their irreducibility was conjectured by Grosswald [Gr], who also showed that their Galois group is always the full symmetric group (assuming his conjecture). The irreducibility of all BPs was proved, first for all but finitely many n by Filaseta [F1], and later for all n by Filaseta and Trifonov [FT].

As an extension of Grosswald's conjecture, we have the following.

Conjecture 1.1 For integers $r, n \geq 0$, $L_n^{\langle r\rangle}(x)$ is irreducible over $\mathbb{Q}$.

Conjecture 1.2 For integers $r, n \geq 0$, if $L_n^{\langle r \rangle}(x)$ is irreducible over $\mathbb{Q}$, then its Galois group over $\mathbb{Q}$ contains the alternating group A_n.[2]

There is already a fair bit of evidence for this pair of conjectures. As described above, they are true for all n if $r = 0, 1, 2$ or $r = n$. In Sell [S], it was shown that $L_n^{\langle r \rangle}(x)$ is irreducible over $\mathbb{Q}$ if $\gcd(n, r!) = 1$; that is already enough to show that for each fixed r, Conjecture 1.1 is true for a positive proportion of integers $n \geq 0$ (this proportion goes to zero quickly with r however).

Our first and main result is as follows.

Theorem 1.3 *For a fixed integer $r \geq 0$, all but finitely many $L_n^{\langle r \rangle}(x)$ are irreducible over $\mathbb{Q}$ and have Galois group (over $\mathbb{Q}$) containing A_n.*

For a more precise (effective) statement, see Theorems 4.4 and 5.4. The irreducibility part of Theorem 1.3 is a companion of sorts for the Filaseta–Lam Theorem. As an illustration of the effectivness of our approach and to gather more evidence for Conjectures 1.1 and 1.2, we prove the following theorem.

Theorem 1.4 *If r is a fixed integer in the range $0 \leq r \leq 8$, then for all $n \geq 1$, $L_n^{\langle r \rangle}(x)$ is irreducible and has Galois group containing A_n over $\mathbb{Q}$.*

Investigating the irreducibility of $L_n^{\langle r \rangle}(x)$ for a fixed n and all large r has a different flavor; the methods we use here give us only a weak result (see the Remark following Theorem 2.9). In a joint work with Wong [HW], using algebro-geometric and group-theoretic techniques, we prove that given an integer $n \geq 5$, and a number field K, for all but finitely many $\alpha \in K$, $L_n^{(\alpha)}(x)$ is K-irreducible and has Galois group (over K) containing A_n. In particular, for $n \geq 5$, Conjectures 1.1 and 1.2 hold for all r large enough with respect to n.

Here, we complement the above result of [HW] by showing that Conjectures 1.1 and 1.2 hold for all $r \geq 0$ if $n \leq 4$ (Theorem 6.3). As for the possibility of verifying further cases of these conjectures, the methods used by Filaseta and Trifonov [FT] in proving the irreducibility of $L_n^{\langle r \rangle}(x)$ for $r = n$ should hopefully yield results in the middle range where $r \approx n$.

The basic strategy we use for proving irreducibility of $L_n^{\langle r \rangle}(x)$ was developed by Sell [S] for the case $r = 2$ as an extension of the proof for $r = 1$ given in [H1], which was itself an adaptation of Coleman's proof [C] for the case $r = 0$. Here is a sketch of it. We fix $r \geq 0$ and suppose g is a proper divisor in $\mathbb{Q}[x]$ of $L_n^{\langle r \rangle}(x)$. In Step 1, using a criterion of Coleman [C] formalized by Sell [S], we show that $\deg(g)$ is divisible by n_0, the largest divisor of n which is co-prime to $\binom{n+r}{r}$. Then $\deg(g)/n_0$ is at most $r!$, so is bounded since r is fixed. In Step 2, thanks to a criterion of Filaseta [F2], we eliminate this bounded number of possibilities for $\deg(g)/n_0$, giving the desired contradiction. For Filaseta's criterion to apply, we require the existence of certain auxiliary primes, and this is where we have to assume that n is large with respect to r so as to apply results from analytic number theory on the existence of primes in short intervals; these are gathered together in Section 3.

[2]Note that once we know the Galois group of a degree n polynomial f contains A_n, then it is either A_n or S_n according to whether the discriminant of f is a square or not; the latter is easily determined for our polynomials using Schur's formula (1.1).

We should point out that the Coleman and Filaseta criteria are both based on the theory of p-adic Newton polygons. Indeed, the key idea of Step 1 is the simple observation that if p is a prime divisor of n which does not divide the constant coefficient of $L_n^{\langle r\rangle}(x)$, then the p-adic Newton polygons of $L_n^{\langle r\rangle}(x)$ and E_n coincide.

For the computation of the Galois group, we use the criterion described in [H2], which was already implicit in Coleman [C] and is also based on Newton Polygons.

Finally, a bibliographic comment. In Grosswald's meticulously written treatise *Bessel Polynomials* [Gr], he considers not just the BP $z_n(x)$ but "Generalized Bessel Polynomials (GBP)" $z_n(x;a)$ and gives much information about their algebraic and analytic properties. The GBP is just a different parametrization of the GLP, as described on p. 36 of [Gr]. Therefore, even though it is not billed as such, Grosswald's book is a rich source of information about the GLP.

2 Irreducibility Criteria

For a prime p and $z \in \mathbb{Q}^*$, we write $\mathrm{ord}_p(z)$ for the p-adic valuation of z : $\mathrm{ord}_p(z) = a$, where $z = p^a m/n$ with integers m and n not divisible by p. It is convenient to put $\mathrm{ord}_p(0) = \infty$. We extend the p-adic valuation ord_p to the algebraic closure $\overline{\mathbb{Q}}_p$ of the p-adic completion $\mathbb{Q}_p$ of $\mathbb{Q}$ in the standard way, see Gouvêa [G] for example.

Our main tool is the p-adic Newton Polygon. We use three results which follow from the Main Theorem of Newton Polygons (Theorem 2.1 below); these are stated below as Corollary 2.2, Lemma 2.7, and Theorem 5.2. We review the definition of Newton Polygons below; for further details, the reader is referred to Gouvêa [G], Amice [A], Artin [Ar], and Hensel and Landsberg [HL]; the latter is, to the best of my knowledge, where the general notion of p-adic Newton Polygons originated. An excellent survey on the applications of Newton Polygons for irreducibility is Mott [M].

The *p-adic Newton Polygon* (or p-Newton polygon) $NP_p(f)$ of a polynomial $f(x) = \sum_{j=0}^{n} c_j x^j \in \mathbb{Q}[x]$ is the lower convex hull of the set of points

$$S_p(f) = \{(j, \mathrm{ord}_p(c_j)) | 0 \le j \le n\}.$$

It is the highest polygonal line passing on or below the points in $S_p(f)$. The vertices $(x_0, y_0), (x_1, y_1), \ldots, (x_r, y_r)$, *i.e.,* the points where the slope of the Newton polygon changes (including the rightmost and leftmost points) are called the *corners* of $NP_p(f)$; their x-coordinates ($0 = x_0 < x_1 < \cdots < x_r = n$) are the *breaks* of $NP_p(f)$. For the i-th edge, joining (x_{i-1}, y_{i-1}) to (x_i, y_i), we put $m_i = (y_i - y_{i-1})/(x_i - x_{i-1})$ and call this the i-th slope of $NP_p(f)$.

***Theorem 2.1* (Main Theorem of Newton Polgyons)** *Let $(x_0, y_0), (x_1, y_1), \ldots, (x_r, y_r)$ denote the successive vertices of $NP_p(f)$. Then there exist polynomials $f_1, \ldots, f_r$ in $\mathbb{Q}_p[x]$ such that*

(i) $f(x) = f_1(x) f_2(x) \cdots f_r(x)$,
(ii) *for $i = 1, \ldots, r$, the degree of f_i is $x_i - x_{i-1}$,*
(iii) *for $i = 1, \ldots, r$ and α_i any root of f_i in $\overline{\mathbb{Q}_p}$, we have* $\mathrm{ord}_p(\alpha_i) = -m_i$.

Proof See any of the references given above. ∎

***Corollary 2.2* (Coleman)** *Suppose $f \in \mathbb{Q}[x]$ and p is a prime. If an integer d divides the denominator (in lowest terms) of every slope of $NP_p(f)$, then d divides the degree of any factor $g \in \mathbb{Q}[x]$ of f.*

Proof The following proof is from Coleman [C].

Since a $\mathbb{Q}[x]$-factor of f of degree k induces a degree k $\mathbb{Q}_p[x]$-factor of f when considered as a polynomial over $\mathbb{Q}_p$, and since every $\mathbb{Q}_p[x]$-polynomial is a product of irreducible ones, it suffices to prove that every $\mathbb{Q}_p[x]$-irreducible divisor g of f has degree divisible by d. Letting α be a root in $\overline{\mathbb{Q}_p}$ of such a polynomial g, the rational number $-\mathrm{ord}_p(\alpha)$, by virtue of being one of the slopes of $NP_p(f)$ (thanks to Theorem 2.1), has denominator divisible by d. Thus, d divides the index of ramification of the extension $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$, a divisor of the degree of this extension (cf. [G, Proposition 5.4.2]), which is precisely the degree of g. ∎

Remark. This corollary has in fact appeared a number of times in the literature, see Mott [M] and the references therein. For example, Dumas [D] was certainly already aware of it in 1906 and used it in various examples, though to the best of my knowledge he did not state it formally.

In [C], Coleman computed the Newton Polygon of $E_n(x)$ at an arbitrary prime p; this computation was facilitated by part (i) of the following Lemma, which is a classical fact due to Legendre.

Lemma 2.3 *Suppose m, r are non-negative integers, and p is a prime.*

(i) *If we write m in base p as*

$$m = a_0 + a_1 p + \cdots + a_t p^t, \qquad 0 \le a_i \le p-1,$$

then

$$\mathrm{ord}_p(m!) = \frac{m - \sigma_p(m)}{p-1},$$

where $\sigma_p(m) = a_0 + a_1 + \cdots + a_t$ is the sum of the base p digits of m.

(ii) *Let $b = \binom{m+r}{r}$, where m, r are non-negative integers. For any prime p, $\mathrm{ord}_p(b)$ is the number of carries in the base p addition of m and r.*

Proof For (i), see, for example, Hasse [Ha, Ch. 17, no. 3, p. 263]. For (ii), we apply (i) to $b = (m+r)!/(m!r!)$ to find

$$\mathrm{ord}_p \binom{m+r}{r} = \frac{\sigma_p(m) + \sigma_p(r) - \sigma_p(m+r)}{p-1}.$$

The latter expression is precisely the number of carries in the base p addition of m and r. ∎

Given an integer $n \ge 1$ and a prime p, we will define $s+1$ integers $0 = k_0 < k_1 < \cdots < k_s = n$ (where s is the number of non-zero p-adic digits of n) called the pivotal indices associated to (n, p) as follows. Let us write n in base p recording only the non-zero digits, namely

$$n = b_1 p^{e_1} + b_2 p^{e_2} + \cdots + b_s p^{e_s}, \qquad 0 < b_1, \ldots, b_s < p, \qquad e_1 > e_2 > \cdots > e_s \ge 0.$$

The *pivotal indices associated to* (n, p) are the partial sums

$$k_i = b_1 p^{e_1} + b_2 p^{e_2} + \cdots + b_i p^{e_i}, \qquad i = 0, \ldots, s. \tag{2.1}$$

Note that $k_0 = 0$ and $k_s = n$. This definition is motivated by Coleman's calculation of $NP_p(E_n)$ (see Lemma 2.5 below). We will also see that a fundamental fact about the GLP $L_n^{\langle r \rangle}(x)$ for $r \geq 0$ is that its p-Newton polygons lies on or above $NP_p(E_n)$. To explain this, we introduce some more terminology.

Definition 2.4 Suppose $f(x) = \sum_{j=0}^{n} a_j \frac{x^j}{j!} \in \mathbb{Q}[x]$ and p is a prime number. Following Pólya and Szegő, we say f is *p-Hurwitz integral* if $\mathrm{ord}_p(a_j) \geq 0$ for $j = 0, \ldots, n$. We call it *Hurwitz integral* if it is p-Hurwitz integral for all primes p, *i.e.,* if the Hurwitz coefficients a_j are integral. We say that f is *p-Coleman integral* if f is a p-Hurwitz integral and additionally $\mathrm{ord}_p(a_{k_i}) = 0$ for $i = 0, \ldots, s$, with k_i as defined in (2.1), *i.e.,* the Hurwitz coefficients are all p-integral and the pivotal ones are *p-units*.

This definition is motivated by the following Lemma.

Lemma 2.5 *If $f \in \mathbb{Q}[x]$ is p-Coleman integral of degree n, then*

(i) $NP_p(f) = NP_p(E_n)$;
(ii) *the breaks of $NP_p(f)$ are precisely the pivotal indices associated to (n, p);*
(iii) *the slopes of $NP_p(f)$ all have denominator divisible by $p^{\mathrm{ord}_p(n)}$.*

Proof We know from Coleman [C] that the breaks of $NP_p(E_n)$ are the pivotal points associated to (n, p). Since f is p-Hurwitz integral, $NP_p(f)$ lies on or above $NP_p(E_n)$. On the other hand, by definition, the corners of $NP_p(E_n)$ lie on $NP_p(f)$, so $NP_p(f) = NP_p(E_n)$. Assertion (iii) follows from (i) and (ii) together with (2.1), because, using Lemma 2.3, the slopes of $NP_p(E_n)$ are calculated to be

$$\begin{aligned} m_i &= \frac{\mathrm{ord}_p(1/k_i!) - \mathrm{ord}_p(1/k_{i-1}!)}{k_i - k_{i-1}} \\ &= -\frac{k_i - \sigma_p(k_i) - k_{i-1} + \sigma_p(k_{i-1})}{(p-1)(k_i - k_{i-1})} \\ &= -\frac{b_i p^{e_i} - b_i}{b_i p^{e_i}(p-1)} = -\frac{p^{e_i} - 1}{p^{e_i}(p-1)}. \end{aligned}$$

■

Our proof of Theorem 1.3 rests on the following two irreducibility criteria.

Lemma 2.6 **(Coleman Criterion)** *Suppose $f \in \mathbb{Q}[x]$ has degree n and p is a prime number. If f is p-Coleman integral, then $p^{\mathrm{ord}_p(n)}$ divides the degree of any factor $g \in \mathbb{Q}[x]$ of f. If f is p-Coleman integral for all primes p dividing n, then f is irreducible in $\mathbb{Q}[x]$.*

Proof This is essentially Theorem 1.7 of Sell [S]. By Lemma 2.5, the slopes of $NP_p(f)$ all have denominators divisible by $p^{\mathrm{ord}_p(n)}$. Now apply Corollary 2.2. ■

Example The classical Laguerre polynomial

$$L_n^{(0)}(x) = \sum_{j=0}^{n} \binom{n}{j} \frac{x^j}{j!}$$

is p-Coleman integral for every prime p. To show this, we simply note that for $j = k_i \in \{k_0, k_1, \ldots, k_s\}$, the base p expansions of $j = b_1 p^{e_1} + \cdots + b_i p^{e_i}$ and $n - j = b_{i+1} p^{e_{i+1}} + \cdots + b_s p^{e_s}$ are completely "disjoint" so there is no carry in the base p addition of these numbers, which, by Lemma 2.3, implies that $\mathrm{ord}_p(\binom{n}{j}) = 0$ for such j. Thus, by Lemma 2.5, $NP_p(L_n^{(0)}(x)) = NP_p(L_n^{\langle 0 \rangle}(x))$ for all primes p, and by Lemma 2.6, we get another proof of the irreducibility of $L_n^{(0)}(x)$.

An immediate consequence of Theorem 2.1 is that the Newton Polygon of the product of two polynomials is formed by the concatenation, in ascending slope, of their edges (*i.e.,* is their Minkowski sum). This fact played an important role in Dumas' work. It can also be used to prove the following criterion due to Filaseta (see [F2] for the proof, but note that the convention for Newton Polygons in that paper differs slightly from ours).

Lemma 2.7 **(Filaseta Criterion)** *Suppose*

$$f(x) = \sum_{j=0}^{n} b_j \frac{x^j}{j!} \in \mathbb{Q}[x]$$

is Hurwitz-integral and $|b_0| = 1$. *Let* k *be a positive integer* $\leq n/2$. *Suppose there exists a prime* $p \geq k+1$ *such that*

$$\mathrm{ord}_p(n(n-1)\cdots(n-k+1)) > \mathrm{ord}_p(b_n).$$

Then $f(x)$ *cannot have a factor of degree* k *in* $\mathbb{Q}[x]$.

We now give the key calculation allowing the application of the Coleman Criterion to our family of polynomials.

Lemma 2.8 (i) *If* p *is a prime divisor of* n, *then* $L_n^{\langle r \rangle}(x)$ *is* p*-Coleman integral if and only if* $\binom{n+r}{r} \not\equiv 0 \bmod p$.

(ii) *If* $\mathrm{ord}_p(n) > \mathrm{ord}_p(r!)$, *then* $L_n^{\langle r \rangle}(x)$ *is* p*-Coleman integral.*

Proof From (1.3), we recall that

$$L_n^{\langle r \rangle}(x) = \sum_{j=0}^{n} a_j \frac{x^j}{j!}, \qquad a_j = \binom{n-j+r}{n-j},$$

is clearly Hurwitz integral. If $p | \binom{n+r}{r}$, then $\mathrm{ord}_p(a_{k_0}) > 0$ because by (2.1), $k_0 = 0$ and $a_0 = \binom{n+r}{r}$. In that case, therefore, $L_n^{\langle r \rangle}(x)$ is not p-Coleman integral. On the other hand, suppose p does not divide $\binom{n+r}{r}$. Then, by Part (ii) of Lemma 2.3, there

is no carry in the base p addition of $n = b_1 p^{e_1} + \cdots + b_s p^{e_s}$ and r. Recalling the definition of k_i, we see that for $0 \le i \le s$, there cannot be a carry in the addition of $(n - k_i)$ and r because the base p expansion of $n - k_i$ is simply a truncation of that of n, *i.e.*, $n - k_i = b_{i+1} p^{e_{i+1}} + \cdots + b_s p^{e_s}$. Thus, $\mathrm{ord}_p(a_0) = 0$ implies that $\mathrm{ord}_p(a_j) = 0$ for $j \in \{k_0, k_1, \cdots, k_s\}$, *i.e.*, that $L_n^{\langle r \rangle}(x)$ is p-Coleman integral, completing the proof of (i).

From the definition of a_0, we have $a_0 \equiv 1 \bmod p^{\mathrm{ord}_p(n) - \mathrm{ord}_p(r!)}$, so (ii) follows from (i). ∎

Theorem 2.9 (i) *If* $\gcd(n, \binom{n+r}{r}) = 1$, *then* $L_n^{\langle r \rangle}(x)$ *is irreducible over* $\mathbb{Q}$.
(ii) *If* $\gcd(n, r!) = 1$, *then* $L_n^{\langle r \rangle}(x)$ *is irreducible over* $\mathbb{Q}$.

Proof If n is coprime to $\binom{n+r}{r}$, $L_n^{\langle r \rangle}(x)$ is p-Coleman integral for every prime divisor p of n by Lemma 2.8, so it is irreducible over $\mathbb{Q}$ by the Coleman Criterion 2.6. Part (ii), which was first obtained by Sell [S], follows from (i) since $\gcd(n, r!) = 1$ implies $\gcd(n, \binom{n+r}{r}) = 1$. ∎

Remark. Fix a positive integer n. It is not difficult to show that the positive integers r for which there exists a prime $p > n$ satisfying $\mathrm{ord}_p(r+1) = 1$ has density one. For each such r, (1.4) implies that $\mathcal{L}_n^{\langle r \rangle}(x)$ and hence $L_n^{\langle r \rangle}(x)$, is p-Eisenstein and hence irreducible. Thus for a fixed n, there is an easy proof of irreducibility for a density 1 subset of integers r.

3 Primes in Short Intervals

For the proof of Theorem 1.3, we will need to establish the existence of primes of appropriate size, namely primes for which the Newton polygon of $L_n^{\langle r \rangle}(x)$ precludes the existence of factors of certain degrees. We will state two such results here, to be used in the next section.

The first is a well-known consequence of the Prime Number Theorem, generalizing Chebyshev's theorem on the existence of a prime in $(n, 2n)$. For lack of a suitable reference with an explicit constant, a proof is supplied.

Theorem 3.1 *Given* $h \ge 2$, *there exists a constant* $C(h)$ *such that whenever* $N > C(h)$, *the interval* $[N(1 - 1/h), N]$ *contains a prime. We may take* $C(h) = e^{h+1/2}(1 - 1/h)^{-h}$.

Proof We have from Rosser and Schoenfeld [RS], that

$$\pi(x) > \frac{x}{\log x - 0.5} \qquad \text{for } 67 \le x,$$

$$\pi(x) < \frac{x}{\log x - 1.5} \qquad \text{for } e^{1.5} < x.$$

Since $h \ge 2$, the first inequality applies for $x = N$ and the second one applies for $x = N - N/h$, assuming only $N \ge 67$. We then have

$$\pi(N) - \pi(N - N/h) > \frac{N}{\log N - 0.5} - \frac{N - N/h}{\log N + \log(1 - 1/h) - 1.5}.$$

Combining the fractions, the right hand side is positive if and only if

$$\log N > 1/2 + h - h\log(1 - 1/h),$$

proving the lemma for $N \geq 67$. Note that from $(1 - 1/h)^{-h} > e$, one obtains that $C(h) > e^{4.5} > 67$ for $h \geq 3$; thus we only need to consider $h = 2$. We have $C(2) = 4e^{2.5} > 48$. For $N \in [48, 67]$, one easily checks by hand that the lemma holds. ∎

For Galois group computations in Section 5, we record the following.

Corollary 3.2 *If $n + r \geq 48$ and $n \geq 8 + 5r/3$, then there exists a prime p in the interval $(n + r)/2 < p < n - 2$.*

Proof The condition $n \geq 8 + 5r/3$ is equivalent to $(n + r)/2 \leq 4(n - 3)/5$. We suppose first that $n \geq 750$ and put $N = n - 2.5 > 747 > C(5)$; applying Theorem 3.1 with $h = 5$, we deduce that there exists a prime $p \in [4N/5, N]$. Thus we have

$$\frac{n+r}{2} \leq \frac{4}{5}(n-3) < \frac{4}{5}(n-2.5) \leq p \leq n - 2.5 < n - 2,$$

proving the Corollary for $n \geq 750$. The assumptions $n + r \geq 48$ and $n \geq 8 + 5r/3$ imply that $n \geq 33$. For $33 \leq n \leq 749$, one verifies directly the existence of a prime in the range $(4(n - 3)/5, n - 2)$. ∎

For the proof of Theorem 1.4, we will use the following result from Harborth and Kemnitz [HK], which is a combination of Theorem 3.1 together with a finite but long computation.

Theorem 3.3 **(Harborth-Kemnitz)** *If $n \geq 48683$, then the interval $(n, 1.001n]$ contains a prime.*

4 Irreducibility of $L_n^{\langle r \rangle}(x)$ for Large n

We fix $r \geq 0$, and write $n = n_0 n_1 = n_2 n_3$, where

$$n_1 = \prod_{p \mid \gcd(n, \binom{n+r}{r})} p^{\mathrm{ord}_p(n)}, \qquad n_3 = \prod_{\substack{p \mid n \\ \mathrm{ord}_p(n) \leq \mathrm{ord}_p(r!)}} p^{\mathrm{ord}_p(n)}.$$

Note that the n_0 is the largest divisor of n which is coprime to $\binom{n+r}{r}$. We also have $n_2 | n_0$ (see the proof of Lemma 2.8), so $n_1 | n_3 | \gcd(n, r!)$. Consequently,

$$n_1 \leq r!, \tag{4.1}$$

which is a somewhat crude estimate. To improve it slightly, recall from Lemma 2.3 that a prime p divides $\binom{n+r}{n}$ if and only if there is a carry in the base p addition of n and r. Thus, if $n \equiv 0 \pmod{p^a}$, and $r < p^a$, then p does not divide $\binom{n+r}{n}$ so p

does not divide n_1; for example, primes exceeding r do not divide n_1. Therefore, for a given fixed r, we have

$$n_1 \leq \prod_{\substack{p|r! \\ \mathrm{ord}_p(n) \leq \log_p(r)}} p^{\mathrm{ord}_p(n)} \leq \prod_{p|r!} p^{\lfloor \log_p(r) \rfloor}. \tag{4.2}$$

Let us note if $r \geq 4$ is fixed, $\lfloor \log_2(r) \rfloor < \mathrm{ord}_2(r!)$. To see this, let $t = \lfloor \log_2(r) \rfloor$ and observe that

$$\mathrm{ord}_2(r!) = \lfloor r/2 \rfloor + \lfloor r/2^2 \rfloor + \lfloor r/2^3 \rfloor + \cdots + \lfloor r/2^t \rfloor$$

is a sum of $t \geq 2$ strictly decreasing positive integers, proving the claim. It follows that

$$\text{If } r \geq 4, \text{ then } n_1 \leq r!/2. \tag{4.3}$$

We will not need it, but we remark that, more generally, for any prime p satisfying $p \leq r/2$, $\lfloor \log_p(r) \rfloor < \mathrm{ord}_p(r!)$.

Lemma 4.1 *If there is a prime p satisfying $\max(\frac{n+r}{2}, n - n_0) < p \leq n$, then $L_n^{\langle r \rangle}(x)$ is irreducible over $\mathbb{Q}$.*

Proof By Lemmas 2.8 and 2.6, every $\mathbb{Q}[x]$-factor of $L_n^{\langle r \rangle}(x)$ has degree divisible by n_0. If $n_1 = 1$, then $n = n_0$ and we are done, so we assume $n_1 > 1$ and proceed by contradiction. We suppose $L_n^{\langle r \rangle}(x)$ has a $\mathbb{Q}[x]$-factor of positive degree $k \leq n/2$. We know that $k \in \{n_0, 2n_0, 3n_0, \ldots, (n_1 - 1)n_0\}$. To eliminate these possibilities, we apply the Filaseta Criterion. Since the latter requires the constant coefficient to be 1, we renormalize our polynomial by setting

$$f(x) = a_0^{-1} L_n^{\langle r \rangle}(a_0 x) = \sum_{j=0}^{n} b_j \frac{x^j}{j!}$$

with integral Hurwitz coefficients $b_j = a_0^{j-1} a_j$, where $a_0 = \binom{n+r}{r}$. Note that $b_0 = 1$ and $b_n = a_0^{n-1}$. Of course, the factorization over $\mathbb{Q}$ of $f(x)$ mirrors exactly that of $L_n^{\langle r \rangle}(x)$. With the hypotheses on p, we have $p \geq k + 1$ (since $k \leq n/2$). Moreover, $p \geq n - k + 1$ since $k \geq n_0$. Finally, $p \nmid b_n = a_0^{n-1}$ since $(n + r)/2 < p < n + 1$. Applying the Filaseta Criterion 2.7 to $f(x)$, we find it does not have a factor of degree k, hence neither does $L_n^{\langle r \rangle}(x)$, giving the desired contradiction. ∎

Definition 4.2 For an integer $r \geq 0$, we define

$$B(r) = \begin{cases} 48 & r = 0, 1, 2, 3 \\ e^{r!+1/2}(1 - 1/r!)^{-r!} & r \geq 4. \end{cases}$$

Lemma 4.3 *Given $r \geq 0$, for every integer $n > B(r)$, there exists a prime p satisfying*

$$\max\left(\frac{n+r}{2}, n - n_0\right) < p \leq n,$$

where n_0 is the largest divisor of n coprime to $\binom{n+r}{r}$.

Proof First let us assume $r \geq 4$; we note that $B(r) > r(r!)/(r! - 2)$. Thus, $n > B(r)$ implies $r < n\left(1 - \frac{2}{r!}\right)$. Adding n to both sides of the latter inequality and dividing by 2, we find $\frac{n+r}{2} < n\left(1 - \frac{1}{r!}\right)$. Next, since $r \geq 4$, by (4.3), $n_1 \leq r!/2$, so $n - n_0 = n - n/n_1 \leq n(1 - 2/h) < n(1 - 1/h)$ with $h = r!$. We have shown that $\max((n + r)/2, n - n_0) < n(1 - 1/h)$. On the other hand, $n > e^{h+1/2}(1 - 1/h)^{-h}$, hence by Theorem 3.1, there exists a prime p satisfying $\max((n + r)/2, n - n_0) < n(1 - 1/h) \leq p \leq n$.

Now let us assume $0 \leq r \leq 3$ and $n \geq 48$. For $r \in [0, 3]$, by (4.1), $n_1 \leq 3!$ so $n - n_0 \leq 5n/6$. On the other hand, $(n + r)/2 \leq (n + 3)/2 \leq 5n/6$, thus $\max((n + r)/2, n - n_0) \leq 5n/6$. By applying Theorem 3.1 with $h = 7$, we find $[6n/7, n] \subset (5n/6, n]$ contains a prime for $n > 5320$, and then by a direct check for $48 \leq n \leq 5320$, we find that $(5n/6, n]$ contains a prime for all $n \geq 48$. This completes the proof of the lemma. ∎

Combining the above lemmata gives the proof of the first part of Theorem 1.3. More precisely, we have proved the following.

Theorem 4.4 *For $r \geq 0$, if $n > B(r)$, then $L_n^{\langle r \rangle}(x)$ is irreducible over $\mathbb{Q}$.*

5 Galois Groups

We begin by recalling a simple criterion based on ramification (as measured by the Newton polygon) for an irreducible polynomial to have a "large" Galois group.

Definition 5.1 Given $f \in \mathbb{Q}[x]$, let $\mathcal{N}_f$, called the *Newton Index* of f, be the least common multiple of the denominators (in lowest terms) of all slopes of $NP_p(f)$ as p ranges over all primes.

To see that $\mathcal{N}_f$ is effectively computable, first note that 0 is defined to have denominator 1, so slope 0 segments of $NP_p(f)$ do not contribute to $\mathcal{N}_f$. On the other hand, for p large enough, all coefficients of f have p-adic valuation 0, so $NP_p(f)$ consists of a single slope 0 segment. For a monic polynomial $f \in \mathbb{Z}[x]$, for example, the Newton Index requires merely the computation of $NP_p(f)$ for the prime divisors p of its constant coefficient. Note also that $\mathcal{N}_f$ divides the least common multiple of the first n positive integers, where $n = \deg(f)$.

The following result from [H2] can be quite useful for calculating the Galois group of polynomials which have many ramified primes in their splitting field.

Theorem 5.2 *Given an irreducible polynomial $f \in \mathbb{Q}[x]$, $\mathcal{N}_f$ divides the order of the Galois group of f. Moreover, if $\mathcal{N}_f$ has a prime divisor q in the range $n/2 < q < n - 2$, where n is the degree of f, then the Galois group of f contains A_n. In that case, the Galois group of f is A_n if the discriminant of f is a rational square, and S_n otherwise.*

Example If $f(x) = L_5^{\langle 3\rangle}(x)$, then f is irreducible over $\mathbb{Q}$ by Lemma 2.8. An easy calculation shows $\mathcal{N}_f = 60$; indeed we need only consider $p = 2, 3, 5, 7$, for which $NP_p(f)$ has slopes whose denominators are divisible by, repectively, $4, 3, 5$ and 2. Thus, the Galois group of f has order divisible by 60. Since the discriminant of f is not a square (by (1.1) or (5.1) below), the Galois group of f is S_5.

Lemma 5.3 *Suppose p is a prime in the interval $(n + r)/2 < p \leq n$. Then the p-Newton polygon of $L_n^{\langle r\rangle}(x)$ has $-1/p$ as a slope. In particular, $p|\mathcal{N}_{L_n^{\langle r\rangle}(x)}$.*

Proof Under the assumptions, it is an easy exercise to calculate the p-Newton polygon of $L_n^{\langle r\rangle}(x)$ directly from (1.3); instead, we use the tools we have developed to get the result. According to Lemma 2.5, the corners of $NP_p(E_n)$ have x-coordinates 0, p, and n (simply 0 and n if $p = n$ of course), so it has $-1/p$ as a slope. Writing $L_n^{\langle r\rangle}(x) = \sum_{j=0}^{n} a_j x^j/j!$, one checks easily that $\mathrm{ord}_p(a_0) = \mathrm{ord}_p(a_p) = 0$, and we always have $\mathrm{ord}_p(a_n) = 0$ since $a_n = 1$. Since $NP_p(L_n^{\langle r\rangle})$ lies on or above $NP_p(E_n)$, and they agree at the corners of the latter, they must coincide. ∎

Theorem 5.4 *Let $r \geq 0$ be an integer.*

(i) *If there exists a prime p satisfying $(n + r)/2 < p < n - 2$, and if $L_n^{\langle r\rangle}(x)$ is irreducible over $\mathbb{Q}$, then its Galois group over $\mathbb{Q}$ contains A_n.*

(ii) *If $n \geq \max(48 - r, 8 + 5r/3)$, and if $L_n^{\langle r\rangle}(x)$ is irreducible over $\mathbb{Q}$, then its Galois group over $\mathbb{Q}$ contains A_n.*

(iii) *For $n > B(r)$, with $B(r)$ given in Definition 4.2, the Galois group of $L_n^{\langle r\rangle}(x)$ over $\mathbb{Q}$ contains A_n.*

Proof For (i) and (ii), we apply Corollary 3.2 in combination with Theorem 5.2 and Lemma 5.3. For (iii), first suppose $0 \leq r \leq 3$ and $n > B(r) = 48$. Then, the interval $((n+3)/2, n-2)$ contains a prime; we can verify this by applying Theorem 3.1 with $N = n - 3$ and $h = 3$ which proves it for $n \geq 114$, then we check the remaining $n \in [48, 114]$ by hand. When we combine (i) with Theorem 4.4, we obtain (iii) for $r \leq 3$. Now suppose $r \geq 4$. We have $B(r) > \max(48 - r, 8 + 5r/3)$, so we can apply (ii) in tandem with Theorem 4.4 to complete the proof. ∎

We have thus completed the proof of Theorem 1.3. We remark that Schur's original method [Sc2, Satz A], which was used in [H1] for the case $r = 1$, would yield a proof of Theorem 5.4 as well.

Remark. By plugging $\alpha = -1 - n - r$ into Schur's formula (1.1), the discriminant of $n!L_n^{\langle r\rangle}(x)$ is seen to be

$$\Delta_n^{\langle r\rangle} = (-1)^{n(n-1)/2} \prod_{j=1}^{n-1} (j+1)^{j+1}(r+j)^{n-j}. \tag{5.1}$$

In particular, $\Delta_n^{\langle r\rangle} < 0$, for $n \equiv 2, 3 \pmod 4$ (recall our blanket assumption $r \geq 0$). For these values of n, therefore, we know that the Galois group of $L_n^{\langle r\rangle}(x)$ is not contained in A_n. If we fix $n > 5, n \equiv 0, 1 \pmod 4$, then by (5.1), the Galois group of $L_n^{\langle r\rangle}(x)$ is contained in A_n if and only if r is the x-coordinate of an integral point on a (fixed) smooth curve of genus at least 1, of which there are only finitely many

by Siegel's theorem. Thus, Conjecture 1.2 would imply that, for fixed n, the Galois group of $L_n^{\langle r\rangle}(x)$ is S_n except for a (small) finite number of integers $r \geq 0$.

Similarly, for fixed r, the proportion of n for which $\Delta_n^{\langle r\rangle}$ is a square can be large if r is small (as we have already seen for $r = 0, 1, 2$). Filaseta has pointed out that this is not so for large r. Specifically, one can check that for $r = 3$, $\Delta_n^{\langle r\rangle}$ is a square if and only if $n \equiv 1 \pmod 4$ and $n+2$ is 3 times a square; for $r = 4, 5$, the n for which $\Delta_n^{\langle r\rangle}$ is a square occur in Fibonacci-type recurrences, namely, for $r = 4$, $n \equiv 0 \bmod 4$, and $2n + 4 = \epsilon_3^j + \epsilon_3^{-j}$ for some j, and similarly for $r = 5$, $n \equiv 1 \bmod 4$ and $2n+6 = \epsilon_{15}^j + \epsilon_{15}^{-j}$ for some j. Here $\epsilon_3 = 2+\sqrt{3}$, $\epsilon_{15} = 4+\sqrt{15}$ are the fundamental units of $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{15})$ respectively. For fixed $r \geq 6$, if $n \equiv (r+1)^2 \bmod 4$, then for n large enough, $\Delta_n^{\langle r\rangle}$ cannot be a square because its p-valuation must be 1 for some prime $p \in ((n+r)/2, n+r)$. On the other hand, if $n \equiv r^2 \bmod 4$, then integers n for which $\Delta_n^{\langle r\rangle}$ is a square correspond to integral points on a smooth curve $y^2 = c_r(x+2)\cdots(x+2\lfloor r/2\rfloor)$ of positive genus (for some easily determined non-zero constant c_r); there are, therefore, only finitely many such n by Siegel's theorem.

6 Properties of $L_n^{\langle r\rangle}(x)$ for $n \leq 4$

In this section, as well as the next, we establish more evidence for Conjectures 1.1 and 1.2 of a somewhat complementary nature to Theorem 1.3. Namely, we fix n and consider those $\alpha \in \mathbb{Q}$ for which $L_n^{(\alpha)}(x)$ is irreducible over $\mathbb{Q}$. This point of view has a rather different flavor. For arbitrary n, the methods of this paper allowed us to get only a weak result in this direction (see the Remark following Theorem 2.9). If $n \geq 5$, a much more fruitful, algebro-geometric, point of view, adopted in [HW], is to consider the covering of curves $\mathcal{X}_1 \to \mathbb{P}^1$ given by the projection-to-y map, where $\mathcal{X}_1 \colon \mathcal{L}_n^{(y)}(x) = 0$ is the projective curve defined by the n-th degree GLP. The Galois closure of this cover, call it $\mathcal{X}'$, has monodromy group S_n (by Schur's result that $\mathcal{L}_n^{(0)}(x)$ has Galois group S_n). By estimating from below the genus of $\mathcal{X}_1$ and other quotients of $\mathcal{X}'$, the following theorem was proved in [HW].

***Theorem 6.1* (Hajir-Wong)** *Suppose an integer $n \geq 5$ and a number field K are fixed. There is a finite subset $\mathcal{E}(n, K) \subset K$ such that for $\alpha \in K - \mathcal{E}(n, K)$, we have*

(i) *$L_n^{(\alpha)}(x)$ is irreducible over K, and*
(ii) *the Galois group of $L_n^{(\alpha)}(x)$ contains A_n if $5 \leq n \leq 9$, and is the full symmetric group if $n \geq 10$.*

Applying the theorem with $K = \mathbb{Q}$, we have the following nice complement to the main theorem 1.3 of this paper.

Corollary 6.2 *For each $n \geq 5$, there is a bound C_n such that Conjectures* 1.1 *and* 1.2 *hold for the pair (n, r) whenever $r \geq C_n$.*

Remark. The constant C_n in the above corollary is ineffective since the proof of the theorem preceding it rests on Faltings' theorem on finitude of rational points on curves of genus at least 2. For the corollary, we could apply Siegel's theorem on

integral points instead, but this does not resolve the effectivity issue either since for $n \geq 5$, the relevant curves have genus greater than 1.

For $n \leq 4$, on the other hand, GLP admitting proper factors over $\mathbb{Q}$ turn out to be plentiful, as such factors correspond to rational points on certain curves of genus 0 or 1. In this section, we calculate the (very few) integral points on these curves effectively, thereby establishing Conjectures 1.1 and 1.2 for $n \leq 4$ and all $r \geq 0$. We summarize the results in the following theorem. During the proof, we will give parametrizations for all $\alpha \in \mathbb{Q}$, $n \leq 4$, for which $L_n^{(\alpha)}(x)$ is $\mathbb{Q}$-reducible. We also parametrize, for $n = 4$, an infinite family of specializations which are reducible but have exceptional Galois group D_4.

Theorem 6.3 (i) *If $n \leq 4$ and $r \geq 0$, then $L_n^{\langle r \rangle}(x)$ is irreducible over $\mathbb{Q}$ and has Galois group containing A_n. If $n \leq 3$, this Galois group is in fact the full symmetric group S_n.*

(ii) *For each $n \in \{2, 3, 4\}$, there exist infinitely many rational numbers α such that $L_n^{(\alpha)}(x)$ is reducible over $\mathbb{Q}$.*

(iii) *There are infinitely many rational numbers α for which $L_4^{(\alpha)}(x)$ is irreducible over $\mathbb{Q}$ with Galois group* not *containing A_4.*

Proof To prove irreducibility of $L_n^{\langle r \rangle}(x)$ for a fixed n, and arbitrary $r \geq 0$, the techniques we have used so far (the existence of ramification at primes dividing $n!$) would have to be modifed, because for suitable r, not all primes less than n ramify in the splitting field of $L_n^{\langle r \rangle}(x)$ over $\mathbb{Q}$. We can take a more direct approach and give elementary arguments for proving (i). Then we go back and study rational points on certain curves which correspond to the exceptional specializations over $\mathbb{Q}$ of $L_n^{(\alpha)}(x)$, proving (ii) and (iii). My original arguments for proving (i) also relied on the study of these rational points. The simpler arguments given here were kindly provided by the referee.

For $n = 2$, the sign in the discriminant formula (5.1) is already enough to show the irreducibility of all $L_n^{\langle r \rangle}(x)$ for $n = 2$, and, similarly, (1.1) shows that $L_2^{(\alpha)}(x)$ is reducible exactly when $\alpha + 2$ is a rational square. Finally, (5.1) also shows that $L_3^{\langle r \rangle}(x)$ does not have Galois group A_3.

Now suppose $n = 3$. Let $s = r + 1$ and put

$$f(x) := 3! L_3^{\langle r \rangle}(x - r - 1) = x^3 + 3sx + 2s.$$

We need to show that $f(x)$ is irreducible over $\mathbb{Q}$. It suffices to show that f does not vanish on $\mathbb{Z}$. Suppose $f(m) = 0$ for some integer m. Then,

$$s = \frac{-m^3}{3m + 2} \geq 1.$$

The inequality $f(0) = 2s \geq 2$ implies $m \neq 0$. On the other hand, for non-zero integers m, the quantity $-m^3/(3m + 2)$ is negative. Thus, f has no root in $\mathbb{Z}$ and is therefore irreducible.

Moreover, we see immediately that $L_3^{(\alpha)}(x)$ is reducible over $\mathbb{Q}$ for infinitely many rational numbers α, and that this is so exactly for those of the form

$$\alpha = \frac{m^3 - 9m - 6}{3m + 2}, \qquad m \in \mathbb{Q}.$$

For $n = 4$, we consider linear factors and quadratic factors separately. We start by simplifying the model via killing the trace term as before, *i.e.,* we reparametrize with $s = r + 1$ again and define

$$g(x, s) := 4! L_4^{\langle s-1 \rangle}(x - s) = x^4 + 6sx^2 + 8sx + 3s^2 + 6s.$$

Suppose for some integer $s \geq 1$, $g(x, s)$ has an integer root $x = m$. We first note that $m \neq -1$ since $g(-1, s) = 3s^2 + 4s + 1 > 1$ for $s > 0$. If $m \geq 0$, $g(m, s)$ is a sum of positive integers and hence does not vanish. Thus, $m \leq -2$, which implies that $m(3m + 4) > 0$ so that $g(m, s) = m^4 + 2sm(3m + 4) + 3s^2 + 6s > 0$, giving a contradiction. Thus, if $s \geq 1$, $g(x, s)$ has no linear factors.

Before treating the quadratic factors, let us study the specializations $s \in \mathbb{Q}$ for which $L_4^{\langle s-1 \rangle}(x)$ has a linear factor. A $\mathbb{Q}$-linear factor $(x - x_0)$ of $g(x, s_0)$ for a rational number s_0 corresponds exactly to a (finite) rational point (x_0, s_0) on the curve $\mathcal{X}_1 : g(x, s) = 0$. It is easy to see that this curve has genus 1, so is elliptic ($(0, 0)$ is on it). Upon using the Cayley–Hermite formula, (implemented in Maple 7 for example), to put $\mathcal{X}_1$ in Weierstrass form, we find it is birational to the minimal Weierstrass model $384H2 : Y^2 = X^3 + X^2 - 25X + 119$, of conductor $384 = 2^7 \cdot 3$, where

$$x = 6\frac{4X + Y + 28}{X^2 - 22X - 95}, \qquad s = -216\frac{X^2 + 10X + 8Y + 129}{X^4 - 44X^3 + 294X^2 + 4180X + 9025}.$$

Here we are using the notation from Cremona's table (available, for instance, in a very usable format at [PRT]), from which we learn that this elliptic curve has an infinite Mordell–Weil group over $\mathbb{Q}$, generated by the point $P_1 = (-1, 12)$ of infinite order and the 2-torsion point $P_0 = (-7, 0)$. This completes the proof of (b). By the usual height arguments, it is not difficult to show that the only integral points on $g(x, s) = 0$ are

$$(0, 0), (0, -2), (3, -1), (4, -2), (-1, -1), (-2, -2), (-3, -3), (3, -27), (-3, -9).$$

All but the last two of these correspond to the trivial factorizations (see (1.2)). This verifies again that for $n = 4$ and integers $r \geq 0$, $L_n^{\langle r \rangle}(x)$ does not have a linear factor over $\mathbb{Q}$ (but it also shows that this is the case for $r \leq -11$). Note the exceptional factorization for $s = -9, -27$, *i.e.,* $r = -10, -28$, corresponds to the factors $x - 6$ and $x - 30$ in $L_4^{(5)}(x)$ and $L_4^{(23)}(x)$ respectively.

The quadratic factors of $L_4^{\langle r \rangle}(x)$ are also parametrized by a curve ($\mathcal{X}_2$ let us call it), for which we can find a model by writing

$$g(x, s) = x^4 + 6sx^2 + 8sx + 3s^2 + 6s = (x^2 + Ax + B)(x^2 - Ax + C)$$

and equating coefficients. A simple elimination of the resulting equations gives us the curve $\mathcal{X}_2 : h(A^2, s) = 0$, where

$$h(z, s) := z^3 + 12sz^2 + 24s(s-1)z - 64s^2$$

is the cubic resolvent of $g(x, s)$.

To complete the proof of (i), we note that $A \neq 0$, since the coefficient of x in $g(x, s)$ does not vanish. On the other hand, $g(x, s) \equiv x^4$ or $x^4 + 1 \bmod 2$, hence $A \equiv 0 \bmod 2$. Taking $z = A^2 \geq 4$, we find $24z > 64$ and $12z^2 > 24z$ so that

$$h(A^2, s) = z^3 + (12z^2 - 24z)s + (24z - 64)s^2 > 0,$$

giving the desired contradiction. This completes the proof of Conjecture 1.1 for $n \leq 4$.

To find all $s \in \mathbb{Q}$ for which $L_4^{\langle s-1 \rangle}(x)$ has a quadratic factor, one checks that $\mathcal{X}_2$ also has genus 1 and is birational to $384H1 : Y^2 = X^3 + X^2 - 35X + 69$ via

$$A = \frac{-6Y}{X^2 + 4X - 23}, \qquad s = \frac{-27(X-3)^2}{(2X-5)(X^2+4X-23)}.$$

Thus, $\mathcal{X}_1$ and $\mathcal{X}_2$ in fact form an isogeny class of order 2. (Note in passing that, with respect to the projection-to-s map, the fiber product $\mathcal{X}' = \mathcal{X}_1 \times_{\mathbb{P}^1} \mathcal{X}_2$ is the minimal Galois cover of either.) In particular, $\mathcal{X}_2$ also has rank 1, with a Mordell–Weil group generated by $P_1 = (1, 6)$ together with 2-torsion point $(3, 0)$. We find the integral points on this curve correspond exactly to the previously known trivial factorizations, namely $(0, 0), (\pm 2, -2), (\pm 2, -1), (\pm 4, -2)$.

Turning to the Galois group over $\mathbb{Q}$ of $g(x, s)$, we know that it contains A_4 if and only if the cubic resolvent $h(z, s)$ does not have a rational root, *i.e,*. if and only if the curve $\mathcal{Y}_2 : h(z, s) = 0$, over which $\mathcal{X}_2$ is a double cover, does not have a $\mathbb{Q}$-rational point. Considering $h(z, s)$ as a quadratic in s with discriminant $(4z)^2(3z^2 - 20z + 36)$, we see that the integral (or rational) points on $\mathcal{Y}_2$ correspond the integral (rational) points on the conic $w^2 = 3z^2 - 20z + 36$. This already suffices to prove (iii), and one can give an explicit formula

$$s = \frac{z(12 - 6z \pm \sqrt{3z^2 - 20z + 36})}{8(3z - 8)}, \qquad (3z - 10)^2 - 3w^2 = -8,$$

for rational values of the parameter s at which $L_4^{\langle s-1 \rangle}(x)$ has dihedral Galois group D_4 (hence is not contained in A_4); it is clear that the values of s, w, and z can be parametrized by the trace of powers of the fundamental unit of $\mathbb{Z}[\sqrt{3}]$. If s is restricted to the integers, then by Gauss's Lemma, z and w are also integers, and one again shows that $s = 0, -1, -2$ give the only integral points on the model $\mathcal{Y}_2$; we omit the details. This completes the proof of Conjecture 1.2 for $n \leq 4$, as well as that of the theorem. ∎

Remark. The Galois group of $L_4^{\langle 4 \rangle}(x)$ is A_4 for infinitely many integers r, namely exactly those expressible as $r = -2 + \sqrt{12k^2 + 1}$, with $k \in \mathbb{Z}$ (these can be parametrized by the trace of powers of the fundamental unit of $\mathbb{Z}[\sqrt{3}]$).

7 Proof of Theorem 1.4

Now we want to prove Conjectures 1.1 and 1.2 for arbitrary n and small r.

Proof of Theorem 1.4. As mentioned earlier, the cases $r = 0, 1, 2$ have already appeared in the literature, missing only the calculation of a few Galois groups for small n. Since it is no extra work, we give a uniform proof here for all $0 \leq r \leq 8$. By Theorem 5.4(iii), this has been reduced to a finite calculation, but the bound given there is prohibitively large, since $B(8)$ is greater than $2 \cdot 10^{17511}$.

We claim that for $r \leq 8$ and all $n \geq 1$, $n_1 \leq 840$. This follows immediately from (4.2).

Thus, for $0 \leq r \leq 8$ and $n \geq 9$, we have $n - n_0 = n(1 - 1/n_1) \leq (839/840)n$. By Theorem 3.3, the interval $(839n/840, n]$ contains a prime for $n \geq 48742$ (note that $1/839 = 0.00119\ldots > 0.001$; one checks easily then that we can replace 48742 by 44350 if we wish). For $0 \leq r \leq 8$, $n \geq 9$, we have $(n + r)/2 \leq 839n/840$; we have therefore shown that for $0 \leq r \leq 8$, $n \geq 48742$, there exists a prime p in the range $\max((n + r)/2, n - n_0) < p \leq n$. This proves the irreducibility of $L_n^{\langle r \rangle}(x)$ for $n \geq 48742$ by Lemma 4.1.

Now we need to handle the small degrees. By Theorem 6.3, we can take $n \geq 5$. Using PARI [B], for each pair (n, r) in the box $5 \leq n \leq 48741$, $0 \leq r \leq 8$, we calculated n_0 and checked (i) whether $n = n_0$, and (ii) whether the smallest prime exceeding $\max((n + r)/2, n - n_0)$ is at most n (PARI is equipped with a table of primes). If (i) holds, then $L_n^{\langle r \rangle}(x)$ is irreducible by Theorem 2.9, and if (ii) holds, then $L_n^{\langle r \rangle}(x)$ is irreducible by Lemma 4.1. It took PARI only a few seconds to verify that among these 438631 pairs (r, n), only 20 cases remain (listed in Table 1) where neither Lemma 4.1 nor Theorem 2.9 applies. Using PARI's `polisirreducible` routine we verified that for these remaining pairs, $L_n^{\langle r \rangle}(x)$ is irreducible.

In order to supply a more tangible certificate of irreducibility, we list in Table 1, with one exception, a prime ℓ such that the reduction $L_n^{\langle r \rangle}(x)$ is irreducible in $\mathbb{F}_\ell[x]$.

The very last entry in the table is interesting. Although $L_{120}^{\langle 8 \rangle}$ is not p-Coleman integral for any prime divisor p of 120, one checks that all slopes of its p-Newton polygon are divisible by p for $p = 3$ and $p = 5$. By Corollary 2.2, 15 divides the degree of any irreducible factor of $L_{120}^{\langle 8 \rangle}$. Thus, even though $n_0 = 1$, we can apply Lemma 4.1 with $n_0 = 15$ and $p = 107$ to get the irreducibility of $L_{120}^{\langle 8 \rangle}$.

Now let us turn to the computation of the Galois group. Again, we need only consider $n \geq 5$. When $n < 8$, $(n/2, n - 2)$ does not contain a prime, so we cannot apply Jordan's criterion. For the 24 polynomials $L_n^{\langle r \rangle}(x)$ with $0 \leq r \leq 8$ and $5 \leq n \leq 7$, we used the PARI routine `polgalois` to verify that the Galois group contains A_n.

Now suppose $n \geq 8$ and $r \leq 8$. By Theorem 5.4(ii), we are done if $n \geq 49$. Of the remaining pairs (r, n), when $((n + r)/2, n - 2)$ contains a prime, we apply Theorem 5.4(i). There remain 47 cases, listed in Table 2. In these 47 cases, since $n \geq 8$, there exists a prime in the interval $(n/2, n - 2)$, labelled q in Table 2. We check in each case that $NP_q(L_n^{\langle r \rangle}(x))$ has at least one slope with denominator q, then apply Theorem 5.2. Thus, in all cases, the Galois group of $L_n^{\langle r \rangle}(x)$ contains A_n. ∎

r	n	ℓ	r	n	ℓ	r	n	ℓ
3	6	13	6	20	311	8	8	29
4	6	29	7	6	47	8	10	137
5	6	23	7	10	47	8	12	173
5	20	149	7	12	47	8	24	191
6	6	31	7	20	271	8	42	113
6	10	17	7	42	79	8	120	613
6	12	29	8	6	17			

Table 1

r	n	q	r	n	q	r	n	q
1	9	5	4	13	7	7	11	7
1	13	7	5	8	5	7	12	7
2	8	5	5	9	5	7	13	7
2	9	5	5	10	7	7	15	11
2	12	7	5	11	7	7	19	11
2	13	7	5	12	7	8	8	5
3	8	5	5	13	7	8	9	5
3	9	5	6	8	5	8	10	7
3	11	7	6	9	5	8	11	7
3	12	7	6	10	7	8	12	7
3	13	7	6	11	7	8	13	7
4	8	5	6	12	7	8	14	11
4	9	5	6	13	7	8	15	11
4	10	7	7	8	5	8	18	11
4	11	7	7	9	5	8	19	11
4	12	7	7	10	7			

Table 2

8 A Question

Given $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Q}[x]$, let us say $g(x) = \sum_{j=0}^{n} a_j b_j x^j$ is an *admissible modification* of $f(x)$ if $b_j \in \mathbb{Z}$ for all $0 \leq j \leq n$ and $b_0 = \pm 1, b_n = 1$. We could also allow $b_n = -1$, but since multiplication by -1 is harmless when it comes to irreducibility and Galois groups, we can dispense with it.

Already in Schur's original treatment of $E_n(x) = L_n^{\langle 0 \rangle}(x)$, he proved not just the irreducibility of E_n but also of all its admissible modifications. In [FT], Filaseta and Trifonov prove the irreducibility of all admissible modifications of the Bessel polynomials $z_n(x) = n! L_n^{\langle n \rangle}(x)$. Also, the Filaseta–Lam theorem quoted in the introduction was in fact proved for all admissible modifications of $L_n^{(\alpha)}(x)$ for n large enough with respect to α. These results, combined with Conjecture 1.1 suggest the following question.

Question 8.1 For which pairs of non-negative integers (r, n) is it true that every admissible modification of $L_n^{\langle r \rangle}(x)$ is irreducible over $\mathbb{Q}$?

The particular strategy developed in this paper would not appear to be suitable for answering this question, but the techniques of [FT] and [FL], suitably altered, would hopefully apply.

Some experimentation reveals that there are exceptions already for $n = 2$. Indeed, suppose $r = 4m^2 - 1$ and the modifying coefficients (b_0, b_1, b_2) are $(-1, m, 1)$. The resulting admissible modification of $2L_2^{\langle r \rangle}(x)$ is

$$x^2 + 8m^3x - 4m^2(4m^2 + 1) = (x - 2m)(x + 2m + 8m^3).$$

If one does not allow the modification of the constant coefficient, then it is not hard to show that the resulting admissible modifications of $L_2^{\langle r \rangle}(x)$ are always irreducible over $\mathbb{Q}$. Moreover, a PARI calculation for $n = 3$ and $r \leq 100$, with modification coefficients (b_0, b_1, b_2, b_3) satisfying $|b_0| = 1$, $b_3 = 1$, $|b_1|, |b_2| \leq 100$ turned up only irreducible polynomials (more than 2 million of them).

Acknowledgments I would like to thank Professors Filaseta and Wong for their helpful remarks. I am grateful to the anonymous referee for a very careful reading of the paper and numerous corrections to and simplifications of the arguments.

References

[A] Y. Amice, *Les nombres p-adiques.* Collection SUP: Le Mathématicien 14, Presses Universitaires de France, Paris, 1975.

[AAR] G. E. Andrews, R. Askey, and R. Roy, *Special functions.* Encyclopedia of Mathematics and its Applications 71, Cambridge University Press, Cambridge, 1999.

[Ar] E. Artin, *Algebraic numbers and algebraic functions.* Gordon and Breach Science Publishers, New York-London-Paris, 1967.

[B] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, GP-PARI 2.0.12, http://pari.math.u-bordeaux.fr

[C] R. F. Coleman, *On the Galois groups of the exponential Taylor polynomials.* Enseign. Math. (2) **33**(1987), no. 3-4, 183–189.

[D] G. Dumas, *Sur quelques cas d'irréducibilité des polynomes à coefficients rationnels.* J. de Math. Pures et Appl. **2**(1906), 191–258.

[F] W. Feit, *$\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over number fields.* J. Algebra **104**(1986), no. 2, 231–260.

[F1] M. Filaseta, *On the irreducibility of all but finitely many Bessel polynomials.* Acta Math. **174**(1995), no. 2, 383–397.

[F2] ———, *A generalization of an irreducibility theorem of I. Schur.* In: Analytic number theory 1, Progr. Math. 138, Birkhäuser Boston, Boston, MA, 1996, pp. 371–396.

[FL] M. Filaseta and T.-Y. Lam, *On the irreducibility of the generalized Laguerre polynomials.* Acta Arith. **105**(2002), no. 2, 177–182.

[FT] M. Filaseta and O. Trifonov, *The irreducibility of the Bessel polynomials.* J. Reine Angew. Math. **550**(2002), 125–140.

[FW] M. Filaseta and R. L. Williams, Jr., *On the irreducibility of a certain class of Laguerre polynomials.* J. Number Theory **100**(2003), no. 2, 229–250.

[G] F. Q. Gouvêa, *p-adic numbers. An introduction.* Second edition, Springer-Verlag, Berlin, 1997.

[Go] R. Gow, *Some generalized Laguerre polynomials whose Galois groups are the Alternating groups.* J. Number Theory **31**(1989), no. 2, 201–207.

[Gr] E. Grosswald, *Bessel polynomials.* Lecture Notes in Mathematics 698, Springer, Berlin, 1978.

[H1] F. Hajir, *Some $\tilde{A}_n$-extensions obtained from generalized Laguerre polynomials.* J. Number Theory **50**(1995), no. 2, 206–212.

[H2] ———, *On the Galois group of generalized Laguerre Polynomials.* J. Théor. Nombres Bordeaux **17**(2005), no. 2, 517–525.
[HW] F. Hajir and S. Wong, *Specializations of one-parameter families of polynomials.* Ann. Inst. Fourier (Grenoble) **56**(2006), no. 4, 1127–163.
[HK] H. Harborth and A. Kemnitz, *Calculations for Bertrand's postulate.* Math. Mag. **54**(1981), no. 1, 33–34.
[Ha] H. Hasse, *Number theory.* Classics in Mathematics, Springer-Verlag, Berlin, 2002.
[HL] K. Hensel and G. Landsberg, *Theorie der algebraischen Funktionen einer Variabeln und ihre Anwendung auf algebraische Kurven und Abelsche Integrale.* Chelsea Publishing Co., New York, 1965.
[M] J. L. Mott, *Eisenstein-type irreducibility criteria.* In: Zero-dimensional commutative rings, Lecture Notes in Pure and Appl. Math. 171, Dekker, New York, 1995, pp. 307–329.
[PRT] A. Pacetti, F. Rodriguez-Villegas, and G. Tornaria, *Computational Number Theory Tables and Computations*, http://www.ma.utexas.edu/users/tornaria/cnt/.
[PZ] G. Pólya and G. Szegő, *Problems and theorems in analysis. Vol. II. Theory of functions, zeros, polynomials, determinants, number theory, geometry.* Die Grundlehren der Mathematischen Wissenschaften 216, Springer-Verlag, New York, 1976.
[RS] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers.* Illinois J. Math. **6**(1962), 64–94.
[Sc1] I. Schur, *Gleichungen Ohne Affekt.* In: Gesammelte Abhandlungen. Band III, Springer-Verlag, Berlin, 1973, pp. 191-197.
[Sc2] I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome.* In: Gesammelte Abhandlungen. Band III, Springer-Verlag, Berlin-New York, 1973, pp. 227–233.
[S] E. A. Sell, *On a certain family of generalized Laguerre polynomials.* J. Number Theory **107**(2004), no. 2, 266–281.
[Se] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$. Comment. Math. Helv. **59**(1984), no. 4, 651–676.
[Sz] G. Szegő, *Orthogonal polynomials.* Fourth edition, American Mathematical Society, Providence, RI, 1975.

Department of Mathematics & Statistics, University of Massachusetts, Amherst, Amherst MA 01003, USA
e-mail: hajir@math.umass.edu