AN IRREDUCIBILITY LEMMA

MICHAEL R. BUSH AND FARSHID HAJIR

1. Introduction

Let K be a field, equipped with a normalized discrete valuation v. We let K_v be the completion of K with respect to v, and fix an algebraic closure $\overline{K_v}$, to which we extend v. For a non-zero degree n polynomial $f = \sum_{i=0}^{n} a_i x^i \in K_v[x]$, the *$v$-adic Newton polygon of f*, $NP_v(f)$ is defined to be the lower convex hull in the x, y-plane of the set of points

$$(j, v(a_j)), \qquad j = 0, 1, \ldots, n.$$

It is composed of a finite number of line segments whose slopes are increasing from left to right. By the *length* of such a segment, we mean the length of its projection onto the x-axis. The endpoints of the segments are called the *corners* of $NP_v(f)$; their x-coordinates are called the *breaks*. If $f(x)$ vanishes to order $k > 0$ at $x = 0$, then by convention, we think of the left-most segment as one of slope $-\infty$ and length k. In summary, if $NP_v(f)$ has $r + 1$ corners (x_0, y_0), (x_1, y_1),..., (x_r, y_r), (listed from left to right so that $x_0 = 0$ and $x_r = n$), then the ith segment of $NP_v(f)$ has length $x_i - x_{i-1}$ and slope

$$m_i = \frac{y_i - y_{i-1}}{x_i - x_{i-1}}.$$

The fundamental fact about v-adic Newton Polygons is that, in the above notation, for $i = 1, 2, \ldots, r$, f has precisely $x_i - x_{i-1}$ roots in $\overline{K_v}$ of valuation $-m_i$. (See [7] or [3] for example). An immediate corollary of the fundamental theorem, which is frequently just as useful, is that the Newton Polygon of a product of two polynomials is their *Minkowski sum*, i.e. the polygon one obtains by concatenating their segments together according to increasing slope.

In this brief note, we give a simple result (Lemma 2.5) which can be handy for proving certain polynomials are irreducible, or at least for putting constraints on the degrees of their possible factors. One can interpret our lemma as a generalization of the well-known Eisenstein Criterion. By way of illustration, we apply the lemma to prove the irreducibility of a certain family of hypergeometric polynomials.

2. The Lemma

Before stating the lemma, let us make some definitions.

Definition 2.1. For $f \in K_v[x]$, let $\lambda_v(f) \geq 0$ be the length of the slope 0 segment of $NP_v(f)$; if none of the slopes is 0, $\lambda_v(f) = 0$. We call $\lambda_v(f)$ the *flatness* of f with respect to v. We define $\mu_v(f) = \max_{1 \leq i \leq r} |m_i|$ where $m_1, \ldots, m_r$ are the slopes of $NP_v(f)$ and call it the *steepness* of f with respect to v. We say that $NP_v(f)$ is *non-trivial* if $\mu_v(f) \neq 0$. Define

$$\ell_v(f) := \{i \in [0, n] \cap \mathbb{Z} \mid v(a_i) = \min_{0 \leq j \leq n} v(a_j)\}.$$

Hajir's research is supported by the National Science Foundation under Grant No. 0226869.

We call a degree n polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in K_v[x]$ is called *v-Eisenstein* if $v(a_n) = 0$, $v(a_0) = 1$, and $v(a_i) \geq 1$ for $1 \leq i \leq n-1$.

Remark 2.2. i) By the fundamental theorem of Newton polygons, $\lambda_v(f)$ counts how many of the roots of f in $\overline{K_v}$ are v-adic units. We also note that $\min \ell_v(f)$ and $\max \ell_v(f)$ are the left and right endpoints of the slope 0 segment of $NP_v(f)$ (or of the unique lowest point on $NP_v(f)$ if none of the slopes is 0). Thus,

$$\lambda_v(f) = \max \ell_v(f) - \min \ell_v(f).$$

ii) The Newton polygon $NP_v(f)$ is non-trivial if and only if $\lambda_v(f) < \deg(f)$.

iii) If, as above, the slopes of $NP_v(f)$ are listed in increasing order from left to right as $m_1 < m_2 < \cdots < m_r$, then $\mu_v(f) = \max(|m_1|, |m_r|)$ is either the absolute value of the left-most slope or the right-most slope, whichever is greater.

iv) If $\mu_v(f) > 0$, i.e. if $NP_v(f)$ is non-trivial, then $\mu_v(f) \geq \deg(f)^{-1}$, because the least non-zero "rise" for one of its segments is 1 and the greatest "run" is $\deg(f)$.

v) The inequality $\mu_v(f) \geq \deg(f)^{-1}$ is an equality if and only if f (or a constant multiple of it) is v-Eisenstein.

Definition 2.3. A polynomial $\tilde{f}(x) = \sum_{i=0}^{n} \tilde{a}_i x^i \in K[x]$ is called a *v-admissible deformation of* $f(x) = \sum_{i=0}^{n} a_i x^i$ if

- $v(\tilde{a}_i) \geq v(a_i)$ for all $0 \leq i \leq n$,
- for $i = 0, n$ and for some integer $i \in \ell_v(f)$, $v(\tilde{a}_i) = v(a_i)$.

Remark 2.4. For a v-admissible deformation $\tilde{f}$ of f, $NP_v(\tilde{f})$ and $NP_v(f)$ are either both trivial or both non-trivial. If $\tilde{f}$ is a v-admissible deformation of f, then $\ell_v(f) \cap \ell_v(\tilde{f})$ is not empty, which implies that $\lambda_v(\tilde{f}) \leq \lambda_v(f)$. It is even easier to see that $\mu_v(\tilde{f}) \leq \mu_v(f)$. Thus, a v-admissible deformation renders the v-Newton Polygon no flatter and no steeper.

Very roughly speaking, the following result shows that a polynomial whose Newton polygon is not too flat nor too steep cannot have too many factors.

Lemma 2.5. *Suppose $f \in K_v[x]$ has non-trivial $NP_v(f)$. If $\tilde{f}$ is any v-admissible modification of f, and $g \in K_v[x]$ is a divisor of $\tilde{f}$, then* $\deg(g) \notin (\lambda_v(f), \mu_v(f)^{-1})$, *i.e.* $\deg(g)$ *does not belong to the open (possibly empty) interval indicated.*

Proof. By Remark 2.4, it suffices to prove the Lemma for $\tilde{f} = f$. Suppose $f = gh$ with $g, h \in K_v[x]$ and let $d = \deg(g)$. We must show that if $d > \lambda_v(f)$, then $d \geq \mu_v(f)^{-1}$. The assumption $d > \lambda_v(f)$ implies that g has a root $\alpha \in \overline{K_v}$ with $|v(\alpha)| > 0$. In particular, $\mu_v(g) > 0$, which implies that $\mu_v(g) \geq d^{-1}$. Thus, $\mu_v(f) \geq \mu_v(g) \geq d^{-1}$, which gives $d \geq \mu_v(f)^{-1}$ as desired. □

Remark 2.6. We recover the Eisenstein criterion easily from the Lemma, for if f is v-Eisenstein, $NP_v(f)$ has a unique slope, namely $1/n$, so $\lambda_v(f) = 0$ and $\mu_v(f) = 1/n$; thus for any $g \in K_v[x]$ dividing f, the Lemma ensures that $\deg(g) \in \{0, n\}$, which means that f is irreducible over K_v, hence also over K. Note that v-admissible modifications of a v-Eisenstein polynomial is v-Eisenstein.

Let us now specialize Lemma 2.5 to a polynomial $f \in K_v[x]$ which is both monic and v-integral, for in that case it takes a more concrete form, as we now explain. Let us suppose that f is v-monic and v-integral, i.e. $f(x) = \sum_{i=0}^{n} a_i x^i$ with $v(a_i) \geq 0$ for all i and $v(a_n) = 0$.

Then $\max \ell_v(f) = n$ clearly, so $\lambda_v(f) = n - \min\{0 \le j \le n \mid v(a_j) = 0\}$. Thus, if $v(a_j) > 0$ for $0 \le j \le n-u-1$, then $\lambda_v(f) \le u$. Moreover, $\mu_v(f)$ is the absolute value of the left-most slope of $NP_v(f)$. We thus obtain

Corollary 2.7. *Suppose $f(x) = \sum_{i=0}^{n} a_i x^i \in K_v[x]$ is v-monic and v-integral, and satisfies $v(a_j) > 0$ for $0 \le j \le n-u-1$. If the left-most slope of $NP_v(f)$ is $-\mu$, then no v-admissible deformation of f admits factor in $K_v[x]$ with degree belonging to (u, μ^{-1}).*

For $K = \mathbb{Q}$ and v the valuation attached to some prime p, this Corollary is precisely Lemma 2 of [1], which has been used quite effectively by Filaseta and his collaborators to demonstrate the irreducibility of many families of polynomials.

Since any polynomial can be made monic and integral by a simple change of variables which does not effect irreducibility, one may wonder whether we can dispense with Lemma 2.5 and rely only on the more concrete Corollary 2.7. Note, however, that if $NP_v(f)$ has positive as well as negative slopes, which can happen quite easily if f is not monic or not v-integral, then Lemma 2.5 can yield much more information than Corollary 2.5 alone. This is because a rescaling change of variables, while it does not change the lengths of the segments of the Newton polygon, does alter the slopes radically, as we will now see.

Given an arbitrary $f = \sum_{i=0}^{n} a_i x^i \in K_v[x]$, we choose some $c \in K_v$ which will clear the denominator, i.e. such that $v(ca_i) \ge 0$ for all i, then we obtain a monic v-integral polynomial by putting

$$\begin{aligned} \hat{f}(x) &:= c^n a_n^{n-1} f(\frac{x}{ca_n}) \\ &= x^n + ca_{n-1}x^{n-1} + c^2 a_n a_{n-2} x^{n-2} + \cdots + c^n a_n^{n-1} a_0. \end{aligned}$$

It is easy to see that $NP_v(\hat{f})$ has the same breaks as $NP_v(f)$, but if the slopes of $NP_v(f)$ are $m_1, \ldots, m_r$, then the slopes of $NP_v(\hat{f})$ are

$$\hat{m}_i = m_i + v(ca_n), \qquad i = 1, \ldots, r.$$

One can see this directly from the definition of the Newton polygon, or one can use the fundamental theorem together with the fact that the roots of $\hat{f}(x)$ are simply those of $f(x)$ scaled by the multiplication factor ca_n. Thus, for example, if we apply Lemma 2.5 to the non-monic polynomial $f_m(x) := px^{2m} + x^{m+1} + x^{m-1} + p$, with $m \ge 2$, we find that if $f_m(x)$ is not irreducible over $\mathbb{Q}$ then it must have a $\mathbb{Q}$-rational factor of degree in the set $\{1, 2, m-1, m\}$. If we consider the monic version $\hat{f}_m(x) = p^{2m-1} f_m(x/p) = x^{2m} + p^{m-2}x^{m+1} + p^m x^{m-1} + p^{2m}$, however, the Newton Polygon at p has slopes $-m/(m-1), -1, -(m-2)/(m-1)$ so Corollary 2.7 tells us nothing.

3. Application to a family of Jacobi Polynomials

In this section, we would like to illustrate the utility of Lemma 2.5 with an example we draw from a family of hypergeometric polynomials. In so doing, we wish to have a family of polynomials whose irreducibility can be ascertained by several applications of Lemma 2.5, but which requires the full strength of the Lemma; for this we have chosen a family whose NP has positive as well as negative slopes.

Let us recall the Jacobi Polynomial

$$P_n^{(\alpha,\beta)}(x) := J_n^{(\alpha,\beta)} \left(\frac{x-1}{2} \right),$$

where

$$J_n^{(\alpha,\beta)}(x) := \sum_{j=0}^{n} \binom{n+\alpha}{n-j}\binom{n+\alpha+\beta+j}{j} x^j.$$

On putting $r = -1-n-\alpha$ and $s = n+\alpha+\beta$, we have another parametrization which is often more convenient, viz.

$$\begin{aligned} J_n^{\langle r,s\rangle}(x) &:= J_n^{(-1-n-r,\, r+s+1)}(x) \\ &= (-1)^n \sum_{j=0}^{n} \binom{r+n-j}{n-j}\binom{s+j}{j}(-x)^j. \end{aligned}$$

Based on a numerical experiment, it appears that for integral $r \in [0,n]$, the polynomials

$$F_n^{\langle r\rangle}(x) := J_n^{\langle r,n-r\rangle}(x)$$

are always irreducible over $\mathbb{Q}$. Indeed, with the aid of Pari-gp's `polisirreducible` function [4] we have verified that this is the case for $n \in [3,506]$. Note that since

$$J_n^{\langle s,r\rangle}(x) = (-1)^n x^n J_n^{\langle r,s\rangle}(x^{-1}),$$

one only needs to check irreducibility for $r \in [0, \lfloor n/2 \rfloor]$.

For individual examples irreducibility can often be shown by selecting a suitable prime and applying Eisenstein's criterion to $F_n^{\langle r\rangle}(x)$ or a suitable shift $F_n^{\langle r\rangle}(ax+b)$. For instance when $n = p-1$ with p an odd prime and $r = 0$ then $F_n^{\langle r\rangle}(x)$ is Eisenstein with respect to p (see Lemma 3.2 below). This approach will not suffice in all cases. For example, it is possible to find values of n and r for which the extension of $\mathbb{Q}$ defined by $F_n^{\langle r\rangle}(x)$ is not totally ramified at *any* prime (eg. $(r,n) = (0,7)$ and $([1,2,3,4],10)$).

With the help of Lemma 2.5, we now prove the main result of this section.

Proposition 3.1. *If $p = 2k+1$ is an odd prime, then $F_{2k}^{\langle k\rangle}(x)$ and $F_{2k}^{\langle k-1\rangle}(x)$ are irreducible over $\mathbb{Q}$ of degree $2k$.*

We first determine the Newton Polygon at p of $F_{2k}^{\langle r\rangle}(x)$.

Lemma 3.2. *If $p = 2k+1$ and r is an integer in $[1,k]$ then $NP_p(F_{2k}^{\langle r\rangle}(x))$ consists of an edge of slope $-1/r$ and one of slope $1/s$ where $s = 2k-r$. When $r = 0$ there is one edge of slope $1/2k$ and $F_{2k}^{\langle 0\rangle}(x)$ is p-Eisenstein.*

Proof. If we let c_j be the absolute value of the coefficient of x^j in $F_{2k}^{\langle r\rangle}(x)$ then we have

$$c_j = \binom{r+2k-j}{2k-j}\binom{2k-r+j}{j} = \frac{(2k+r-j)!(2k-r+j)!}{r!j!(2k-j)!(2k-r)!}.$$

Since $0 \le r \le k$ and $0 \le j \le 2k$ it is clear that p never divides the denominator of c_j. It also follows that $-2k \le r-j \le k$ from which one can deduce the inequalities $0 \le 2k+r-j \le 3k$ and $k \le 2k-r+j \le 4k$.

Let v be the valuation associated to the prime p. If $r-j \ge 1$ or $r-j \le -1$ then p divides exactly one of the factorials appearing in the numerator of c_j with exponent 1. It follows that in these cases $v(c_j) = 1$. In the remaining case $j = r$ we see that p does not divide the numerator so that $v(c_r) = 0$. The statements regarding the Newton polygon now follow easily. □

Combining Lemma 3.2 and Lemma 2.5, we see that the only possible degrees for a non-trivial rational factor are $k-1$, k or $k+1$ for $F_{2k}^{\langle k-1\rangle}(x)$, and k for $F_{2k}^{\langle k\rangle}(x)$. To rule these out we determine the Newton Polygons of both polynomials at an auxiliary prime ℓ. We first describe some general congruences that hold *mod* ℓ for the coefficients of the shifted polynomial $F_n^{\langle r\rangle}(x+1)$.

Lemma 3.3. *Let $a(n,r,j)$ be the coefficient of x^j in the polynomial $F_n^{\langle r\rangle}(x+1)$, i.e.*

$$F_n^{\langle r\rangle}(x+1)=\sum_{j=0}^{n}\sum_{t=0}^{n-j}(-1)^t\binom{2n-r-t}{n-t}\binom{n-t}{j}\binom{r+t}{t}x^j.$$

If ℓ is an odd prime satisfying $n>\ell>\max(r,n-r)$ then $a(n,r,j)\equiv 0$ mod ℓ for $0\le j<\ell$.

Proof. If we let $s=n-r$ and

$$c_t=(-1)^t\binom{s+n-t}{n-t}\binom{n-t}{j}\binom{r+t}{t}$$

then $a(n,r,j)=\sum_{t=0}^{n-j}c_t$. We now verify the following assertions from which the statement in the lemma follows easily:

(a) $c_t+c_{\ell+t}\equiv 0 \bmod \ell$ for $0\le t\le n-(\ell+j)$.
(b) $c_t\equiv 0 \bmod \ell$ for $\max(0,n-(\ell+j)+1)\le t\le \min(\ell-1,n-j)$.

First we rewrite c_t by expanding the binomial coefficients in the formula above

$$c_t=\frac{(-1)^t}{r!s!j!}\left[\frac{(s+n-t)!}{(n-t-j)!}\frac{(r+t)!}{t!}\right].$$

Observe that $r!s!j!\not\equiv 0 \bmod \ell$. Part (a) now follows easily when one compares c_t and $c_{\ell+t} \bmod \ell$.

To prove (b) we consider two cases separately: $\ell\le r+t$ and $\ell>r+t$.

(i) By assumption $t\le\min(\ell-1,n-j)\le\ell-1$ which implies that $1+t\le\ell$. If $\ell\le r+t$ then ℓ must divide $(r+t)!/t!$ and hence c_t.
(ii) Suppose now that $\ell>r+t$ and let $r+t=\ell-a$ where $a\ge 1$. First note that $\ell\le n+s-t$. This inequality follows since after the substitution $t=\ell-a-r$ one sees that it is equivalent to $2\ell\le 2n+a$. By assumption $t\ge\max(0,n-(\ell+j)+1)\ge n-(\ell+j)+1$ which implies that $n-(t+j)+1\le\ell$. Thus ℓ divides $(s+n-t)!/(n-(t+j))!$ and hence c_t.

□

Lemma 3.4. *Let $p=2k+1$ and let ℓ be a prime in the interval $((3k+1)/2,2k)$, then the Newton polygons $NP_\ell(F_{2k}^{\langle k-1\rangle}(x+1))$ and $NP_\ell(F_{2k}^{\langle k\rangle}(x+1))$ each have a side of slope m with m satisfying the inequality $-1/\ell\le m<0$. There is at most one other side of slope 0 and length at most $2k-l$.*

Proof. Let v be the valuation associated to the prime ℓ. By Lemma 3.3 we see that $v(a(2k,k-1,j))\ge 1$ and $v(a(2k,k,j))\ge 1$ for $0\le j<\ell$. We now derive identities for the coefficients $a(2k,k-1,0)$ and $a(2k,k,0)$, from which it will follow that $v(a(2k,k-1,0))=a(2k,k,0)=1$.

Let $G_k(x) = \sum_{t \geq k} \binom{t}{k} x^{t-k}$, then $a(2k, k-m, 0)$ is equal to the coefficient of x^{2k} in $G_{k+m}(x)G_{k-m}(-x)$. But $G_k(x) = \frac{1}{(1-x)^{k+1}}$ so this is also the coefficient of x^{2k} in

$$\frac{1}{(1-x)^{k+m+1}} * \frac{1}{(1+x)^{k-m+1}} = \frac{(1+x)^{2m}}{(1-x^2)^{k+m+1}} = (1+x)^{2m} G_{k+m}(x^2).$$

Thus we have $a(2k, k-1, 0) = \binom{2k+1}{k+1} + \binom{2k}{k+1} = \frac{3k+1}{k+1}\binom{2k}{k}$, and $a(2k, k, 0) = \binom{2k}{k}$.
(The authors would like to thank Bruce Reznick for supplying the approach used in verifying these identities.) Since $\ell \in ((3k+1)/2, 2k)$ it divides $(2k)!$ exactly once and it does not divide $3k+1$. Hence $v(a(2k, k-1, 0)) = v(a(2k, k, 0)) = 1$ as required.

It now follows that the first side of each Newton polygon has slope m with $-1/\ell \leq m < 0$. The leading coefficients satisfy $a(2k, k-1, 2k) = \binom{3k+1}{2k}$ and $a(2k, k, 2k) = \binom{3k}{2k}$. Thus the restrictions on ℓ imply that $v(a(2k, k-1, 2k)) = v(a(2k, k, 2k)) = 0$ and both Newton polygons can have at most one other side with slope 0 and length at most $2k - l$.. □

Proof of Proposition 3.1. Suppose that $g \in \mathbb{Q}[x]$ is a non-trivial divisor of $F_{2k}^{\langle k-1 \rangle}(x)$. By Lemma 3.2 we have $\deg(g) \in \{k-1, k, k+1\}$. If there exists a prime ℓ in the interval $((3k+1)/2, 2k)$ then an application of Lemma 3.4 shows that $\deg(g) \notin (2k-\ell, \ell)$ thus contradicting the previous assertion. It follows that no such divisor g can exist and so $F_{2k}^{\langle k-1 \rangle}(x)$ must be irreducible.

To complete the proof we must verify the existence of such a prime ℓ. In fact this is guaranteed by various existing results in the literature. For instance in [5] (pg 143) one finds a proof that if $r \geq 29$ then there always exists a prime ℓ with $r < \ell \leq \frac{5}{4}r$. This guarantees the existence of ℓ in our situation once $p \geq 41$. For $p < 41$ the irreducibility can be verified on a case by case basis. See also Theorem 3.1 in [2] for a more general result on primes in intervals and further references to the literature.

Exactly the same argument can be applied to show that $F_{2k}^{\langle k \rangle}(x)$ is irreducible over $\mathbb{Q}$. □

References

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

[2] F. Hajir, *Algebraic properties of a family of generalized Laguerre polynomials*, preprint, 2005.

[3] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften **322**. Springer-Verlag, Berlin, 1999.

[4] PARI/GP, version `2.1.6`, Bordeaux, 2004. See `http://pari.math.u-bordeaux.fr/`.

[5] I. Schur, *Gesammelte Abhandlungen*, Band III. (German). Springer-Verlag, Berlin-New York, 1973.

[6] G, Szegö, *Orthogonal polynomials*, Fourth edition. American Mathematical Society, Colloquium Publications, Vol. XXIII. American Mathematical Society, Providence, R.I., 1975.

[7] E. Weiss, *Algebraic number theory*, Reprint of the 1963 original. Dover Publications, Inc., Mineola, NY, 1998.