Applications of the Newton Index to the Construction of Irreducible Polynomials

Doru Ştefănescu

University of Bucharest, Romania
stef@rms.unibuc.ro

Abstract. We use properties of the Newton index associated to a polynomial with coefficients in a discrete valuation domain for generating classes of irreducible polynomials. We obtain factorization properties similar to the case of bivariate polynomials and we give new applications to the construction of families of irreducible polynomials over various discrete valuation domains. The examples are obtained using the package `gp-pari`.

1 Introduction

The construction of classes of irreducible polynomials is based on some few irreducibility criteria or is the result of factorization algorithms. One of the devices used for obtaining irreducibility criteria is to associate properly to a polynomial a Newton polygon and to deduce from the properties of the polygon useful information concerning the irreducibility. This was done by G. Dumas [10] in his extension of the irreducibility criteria of T. Schönemann [16] and G. Eisenstein [11]. In fact Dumas considered the product of two univariate polynomials F_1 and F_2 with integer coefficients and studied the relations among the slopes of the Newton polygons of the polynomials F_1, F_2 and their product $F = F_1F_2$.

The Newton polygon method was subsequently used by various authors for the study of the irreducibily of the polynomials. Recently such results were obtained by A. Bishnoi–S. K. Khanduja–K. Sudesh [3], C. N. Bonciocat [7], C. N. Bonciocat–Y. Bugeaud–M. Cipu–M. Mignotte [8], D. Ştefănescu [17], [18] and S. H. Weintraub [20].

The Newton polygon was initially defined for bivariate polynomials. Another approach is to associate a Newton polygon to a univariate polynomial with the coefficients in a discrete valuation domain. However, the irreducibility criterion of G. Dumas [10] makes use of Newton polygons of univariate polynomials over the integers and of the valuation defined by powers of a prime p. This result was improved by O. Ore [13]. This idea was used by many authors, recently the irreducibility over valued fields was considered by A. Bishnoi–S. K. Khanduja–K. Sudesh [3], A. I. Bonciocat–C. N. Bonciocat [4], [5], C. N. Bonciocat [6], [9], and A. Zaharescu [19]. On the other hand, the Newton polygon was used by L. Panaitopol–D. Ştefănescu [14] for obtaining irreducibility criteria for bivariate

V.P. Gerdt et al. (Eds.): CASC Workshop 2014, LNCS 8660, pp. 460–471, 2014.

polynomials. The Newton polyhedra were considered by A. Lipkovski [12] for the study of absolute irreducibility of multivariate polynomials.

In this paper we consider properties of the Newton index for obtaining information on the factorization of a univariate polynomial with the coefficients in a discrete valuation field. A related method was first used by the author in [17], in the case of bivariate polynomials. However, the results cannot be applied directly to polynomials with coefficients in a valuation domain, so we restate Theorem 1 from [17] in this context, as Theorem 1. The Theorem 2 gives more information on the factorization of a general univariate polynomial over a discrete valuation domain. These results will be used for generating families of irreducible polynomials. In particular, we construct new classes of univariate irreducible polynomials over the integers and over fields of formal power series. Other applications are given to bivariate irreducible polynomials over algebraically closed fields of characteristic zero.

2 On the Newton Index

We consider a univariate polynomial $F(X) = \sum_{i=0}^{d} a_i X^{d-i}$ with coefficients in a discrete valuation domain (A, v). We remind that the Newton polygon $N(F)$ of the polynomial $F(X) = \sum_{i=0}^{d} a_i X^{d-i}$ is the lower convex hull of the set $\{(d-i, v(a_i))\,;\, a_i \neq 0\}$. The slopes of the Newton polygon are the slopes of some line segment. We note that the slope of the line joining the points $(d, v(a_0))$ and $(d-i, v(a_i))$ is $\dfrac{v(a_0) - v(a_i)}{i}$. The *Newton index* $e(F)$ of the polynomial F is the largest slope $e(F)$ of these lines. More precisely,

$$e(F) \;=\; \max_{1 \leq i \leq d} \frac{v(a_0) - v(a_i)}{i}\,.$$

G. Dumas [10] studied the relationship between the Newton indices of two polynomials and the index of their product. He considered the case of univariate integer polynomials with the valuation defined by powers of a prime p. If F_1 and F_2 are such polynomials, he established that the Newton polygon of the product $F_1 F_2$ can be obtained by translating the edges of the polygons $N(F_1)$ and $N(F_2)$ in such a way that they compose a convex polygonal path with the slopes of the edges ordered increasingly. The proof of Dumas is based only on properties of the Newton polygons and it remains true for the case of arbitrary discrete valuations. From the result of Dumas we obtain:

Proposition 1. *If* $F_1\,, F_2 \in A[X] \setminus A$ *then*

$$e(F_1 F_2) \;=\; \max\left(e(F_1), e(F_2)\right)\,.$$

In the case of bivariate polynomials Proposition 1 gives a relation between the degree indices of two polynomials and the degree index of their product. We remind that, in [17], to a bivariate polynomial $F(X,Y) = \sum_{i=0}^{d} P_i(X) Y^{d-i}$ we associated the degree-index

$$P_Y(F) \;=\; \max_{1 \leq i \leq d} \frac{\deg(P_i) - \deg(P_0)}{i}\,.$$

It was used for obtaining irreducibility criteria for bivariate generalized difference polynomials and their extensions by L. Panaitopol–D. Ştefănescu [14]. Among other generalizations of irreducibility tests on generalized difference polynomials we mention those of G. Angermüller [1], S. Bhatia–S. K. Khanduja [2], and A. Bishnoi–S. K. Khanduja–K. Sudesh [3], D. Ştefănescu [17] and [18].

The oldest polynomial irreducibility criterion that applies to a general family of polynomials was obtained by T. Schönemann [16] in 1846. A particular case is Eisenstein's criterion [11] published in 1850. G. Dumas [10] noted that Eisenstein's criterion is related to properties of the Newton polygon and obtained a generalization of the Schönemann–Eisenstein criterion. We remind its valuation approach:

Lemma 1 (G. Dumas, 1906). *Let $F(X) = \sum_{i=0}^{d} a_i X^{d-i} \in A[X]$ be a polynomial over a discrete valuation domain A, with the valuation field (K, v). If the following conditions*

i) $v(a_0) = 0$,

ii) $\frac{v(a_d)}{d} < \frac{v(a_i)}{i}$ *for all* $i \in \{1, 2, \ldots, d-1\}$,

iii) $\gcd(v(a_d), d) = 1$,

are satisfied, the polynomial $F(X)$ is irreducible in $K[X]$.

Remark 1. The condition ii) in Lemma 1 means that the Newton index of the polynomial F is $e(F) = -v(a_d)/d$.

Remark 2. We consider now a generalized difference polynomial $F(X, Y) \in k[X, Y]$, where k is a field,

$$F(X, Y) = cY^d + \sum_{i=1}^{d} P_i(X) Y^{d-i},$$

with $c \in k \setminus \{0\}$, $\in \mathbb{N}^*$, $P_i(X) \in k[X]$ and

$$\frac{\deg(P_i)}{i} < \frac{\deg(P_d)}{d} \quad \text{for all} \quad i,\ 1 \le i \le d-1. \tag{1}$$

Putting, for a polynomial $P \in k[X]$, $v(P) = -\deg(P)$, we observe that $k[X, Y]$ can be organized as a discrete valuation domain. The relation (1) becomes exactly the condition ii) from Theorem 1. Because $v(c) = 0$ the Theorem of Dumas 1 states that the generalized difference polynomial $F(X, Y)$ is irreducible if $(\deg(P_d), d) = 1$. This proves a result established, using a different method, by G. Angermüller in [1].

We will look at factorization properties of univariate polynomials over a discrete valuation domain for which the hypotheses in Theorem 1 are not satisfied.

3 Factorization Conditions

Let (A, v) be a discrete valuation domain and $F(X) = \sum_{i=0}^{d} a_i X^{d-i} \in A[X]$. We will consider the case in which the Newton index could be attained for an index $s \neq d$ and for which $v(a_0)$ could be nonzero.

Theorem 1. *Let (A, v) be a discrete valuation domain, and let*

$$F(X) = a_0X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d \in A[X]\,,$$

with $a_0a_d \neq 0$ and $d \geq 2$. We assume that there exists an index $s \in \{1, 2, \ldots, d\}$ such that

(a) $\dfrac{v(a_0) - v(a_s)}{s} > \dfrac{v(a_0) - v(a_i)}{i}$ *for* $i \in \{1, 2, ..., d\}, i \neq s$,

(b) $\dfrac{v(a_0) - v(a_s)}{s} - \dfrac{v(a_0) - v(a_d)}{d} = \dfrac{1}{ds}$,

(c) $\gcd(v(a_0) - v(a_s), s) = 1$.

Then the polynomial F is either irreducible in $A[X]$, or has a factor whose degree is a multiple of s.

Proof. The proof follows the same lines as that of Theorem 5 in [18], using valuations instead of degrees. We suppose that there exists a nontrivial factorization $F = F_1F_2$ in $A[X]$. We have $d = \deg(F)$ and we put

$$d_1 = \deg(F_1)\,, \quad d_2 = \deg(F_2)\,.$$

We suppose that

$$F_1(X) = \sum_{i=0}^{d_1} a_{1i}X^{d_1-i}\,, \quad F_2(X) = \sum_{i=0}^{d_2} a_{2i}X^{d_2-i}\,.$$

We observe that $a_d = a_{1d_1}a_{2d_2}$ and, $a_0 = a_{10}a_20$.

Then we put

$$c = v(a_0) - v(a_s)\,, \quad m = v(a_0) - v(a_d)\,.$$

$$m_1 = v(a_{10}) - v(a_{1d_1})\,, \quad m_2 = v(a_{20}) - v(a_{2d_2})\,.$$

We observe that

$$d = d_1 + d_2\,, \quad m = m_1 + m_2\,.$$

¿From the condition (b) we obtain

$$cd - sm = 1\,. \tag{2}$$

By Proposition 1 we have $e(F) = \max\{e(F_1), e(F_2)\}$ and, by the hypothesis (a), it follows that

$$\frac{c}{s} = \frac{v(a_0) - v(a_s)}{s} = e(F) \geq e(F_1) \geq \frac{v(a_{10}) - v(a_{1d_1})}{d_1} = \frac{m_1}{d_1}\,,$$

which gives

$$\frac{c}{s} - \frac{m_1}{d_1} \geq 0\,,$$

so

$$cd_1 - sm_1 \geq 0\,.$$

Because $e(F) \geq e(F_2)$ we also have

$$cd_2 - sm_2 \geq 0\,.$$

But we have

$$1 = cd - sm = (cd_1 - sm_1) + (cd_2 - sm_2)\,,$$

so one of the positive integers $cd_1 - sm_1$ and $cd_2 - sm_2$ must be 0.

Suppose, for example, that we have $cd - sm_1 = 0$. So $cd = sm_1$. But, by the condition (c), the integers c and s are coprime. Therefore, s must divide d. If $cd - sm_2 = 0$ we obtain that s must divide m_2. So, if the polynomial F is reducible, the degree of one of its divisors must be a multiple of s. □

Corollary 1. *In the conditions of Theorem 1, if $d \geq 3$ and $s > d/2$, then the polynomial F is either irreducible, or has a divisor of degree s.*

Proof. By Theorem 1 the polynomial F is irreducible or it has a factor of degree a multiple of s. If F would have a factor of degree ks, with $k \geq 2$, then we would obtain

$$d \;>\; ks \;>\; k\,\frac{d}{2} \;\geq\; d\,,$$

a contradiction. Therefore, $k = 1$ or F is irreducible. □

If the difference between the numbers in the left-hand side in condition (b) in Theorem 1 is larger than $\frac{1}{ds}$ we can also say something about the possible divisors of F. More precisely, we have the following result:

Theorem 2. *Let (A, v) be a discrete valuation domain, and let*

$$F(X) = a_0X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d \in A[X]\,,$$

with $a_0a_d \neq 0$ and $d \geq 2$. We assume that there exists an index $s \in \{1, 2, \ldots, d\}$ such that

(a) $\dfrac{v(a_0) - v(a_s)}{s} > \dfrac{v(a_0) - v(a_i)}{i}$ *for $i \in \{1, 2, ..., d\}, i \neq s$;*

(b) $\dfrac{v(a_0) - v(a_s)}{s} - \dfrac{v(a_0) - v(a_d)}{d} = \dfrac{u}{ds}$, *with $u \geq 2$;*

(c) $\gcd(v(a_0) - v(a_s), s) = 1$.

Then one of the following conditions is satisfied:

i. The polynomial F is irreducible in $A[X]$.

ii. The polynomial F has a divisor whose degree is a multiple of s.

iii. The polynomial F admits a factorization $F = F_1F_2$ and s divides $\beta\, d_1 - \alpha\, d_2$, for some $\alpha, \beta \in \{1, 2, \ldots, u-1\}$, where $d_1 = \deg(F_1)$, $d_2 = \deg(F_2)$.

Proof. We use the same notation as in the proof of Theorem 1. We obtain the relation

$$cd - sm \;=\; u\,. \tag{3}$$

We have $cd_1 - sm_1 \geq 0\,,\; cd_2 - sm_2 \geq 0$ and

$$(cd_1 - sm_1) + (cd_2 - sm_2) \;=\; u\,. \tag{4}$$

We look to the possible values of $cd_1 - sm_1$.

If $cd_1 - sm_1 = 0$ as in Theorem 1 we deduce that the degree of a divisor of the polynomial F must be divisible by s.

If $cd_1 - sm_1 = 1$ we have $cd_2 - sm_2 = u - 1$ and we obtain

$$c\,(d_2 - (u-1)d_1)) \;=\; (m_2 - (u-1)m_1)\;,$$

therefore s divides $d_2 - (u-1)d_1$.

In general, we suppose that

$$\begin{aligned} cd_1 - sm_1 &= \alpha\,,\\ cd_2 - sm_2 &= \beta\,, \end{aligned} \tag{5}$$

with $\alpha + \beta \;=\; u$.

From the relations (5) we obtain

$$c(\,\beta\, d_1 - \,\alpha\, d_2) \;=\; s(\,\beta\, m_1 - \,\alpha\, m_2)\,.$$

But s and c are coprime, so s should divide $\beta\, d_1 - \,\alpha\, d_2$. Therefore, the case iii is satisfied. □

4 Applications

We consider univariate polynomials over particular discrete valuation domains (the p–adic numbers, the integers, the formal power series) and bivariate polynomials with coefficients in an algebraically closed field of characteristic zero.

Theorems and 1 and 2 are suitable for constructing families of irreducible polynomials over $A[X]$, where $A = (A, v)$ is a discrete valuation domain. Given a nonconstant polynomial $F(X) = a_0X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d \in A[X]$, with $a_0a_d \neq 0\,,\; d \geq 2$ the method is summarized in the following steps:

- Compute the valuations $v(a_0)$, $v(a_1)$, …, $v(a_d)$.
- Compute the Newton index $e(F) = \max_{1\leq i\leq d}\{(v(a_0) - v(a_i))\,/i\}$ and the index s for which $e(F) = (v(a_0) - v(a_s))\,/s$.
- Compute $\gcd\,(v(a_0) - v(a_s))$.
- If $\gcd\,(v(a_0) - v(a_s)) \neq 1$, the irreducibility of the polynomial cannot be tested by this method.
- If $s = d$ we conclude that F is irreducible by the argument in the Theorem of Dumas.

– If $s \neq d$ we compute u such that

$$e(F) - \frac{v(a_0) - v(a_d)}{d} = \frac{u}{sd}\,.$$

– If $u \notin \{1, 2, \ldots, d-1\}$, the irreducibility cannot be tested by this method.
– If $u = 1$ we apply Theorem 1.
– If $u \in \{2, \ldots, d-1\}$ we apply Theorem 2.

Using the package `gp-pari` we computed the Newton indices and we found couples of numbers (s, u) that satisfy the hypotheses in Theorems 1 or 2.

4.1 Univariate Polynomials over p–adic Numbers

Let $r \in \mathbb{Z}_p$ be a p–adic number, $r = p^n \sum_{i=0}^{\infty} a_i p^i$, $a_i \in \{0, 1, \ldots, p-1\}$, $a_0 \neq 0$.. We define a discrete valuation by $v(r) = n$.

Example 1. Let $F(X) = X^d + aX^2 + bX + c \in \mathbb{Z}_p[X]$. Suppose that $d \geq 2$ and $v(a) = d$, $v(b) = d-2$, $v(c) = d-1$. We have

$$\frac{v(1) - v(a)}{d-2} = \frac{-d}{d-2} < 0\,,$$

$$\frac{v(1) - v(b)}{d-1} = \frac{1}{d-1} - 1\,,$$

$$\frac{v(1) - v(c)}{d} = \frac{1}{d} - 1\,.$$

It follows that $e(F) = \frac{v(1)-v(b)}{d-1}$ and

$$e(F) - \frac{v(1) - v(c)}{d} = \frac{1}{d(d-1)}\,.$$

We have $s = d-1$ and, by Theorem 1, we conclude that F is either irreducible, or has a factor of degree $d-1$, and hence also a linear factor. Therefore, if F has no p–adic roots it is irreducible over $\mathbb{Z}_p[X]$.

4.2 Univariate Polynomials over Formal Power Series

Let k be an algebraically closed field of characteristic zero. If $f(X) = \sum_{i=0}^{\infty} a_i X^i$ is a formal power series from $k[[X]]$ we put $v(f) = \mathrm{ord}(f) := \min_i\{i; a_i \neq 0\}$.

Example 2. Let $F(Y) = XY^d + f(X)Y^{d-1} + g(X)Y^2 + Y + h(x) \in k[[X]][Y]$, with $d \geq 3$,

$$\begin{aligned} f(X) &= X^d + X^{d+1} + \ldots + X^{d+n} + \ldots)\,,\\ g(X) &= X^{d-2} + X^{d-1} + X^d\,,\\ h(X) &= X^{d+1}(1 - X + X^2 - X^3 + \cdots)\,. \end{aligned}$$

We have $\frac{v(X)-v(f)}{1} = 1-d$, $\frac{v(X)-v(g)}{d-2} = \frac{3-d}{d-2}$, $\frac{v(X)-v(1)}{d-1} = \frac{1}{d-1}$, $\frac{v(1)-v(h)}{d} = -1$. Therefore, $e(F) = \frac{v(1)-v(1)}{d-1} = \frac{1}{d-1}$ and we have $s = d-1$. We have by Theorem 1 that F is either irreducible in $K[X,Y]$, or has a factor whose degree is a multiple of $d-1$. Hence F is either irreducible, or has a linear factor.

4.3 Univariate Polynomials over the Integers

We suppose that $F(X) \in \mathbb{Z}[X] \setminus \mathbb{Z}$ and we consider the valuation given by the power with respect to a prime ≥ 2.

Example 3. Let $F(X) = (p^2+p+1)X^d + X^3 + p^{d-2}(p+1)X + p^d$, with $d \geq 4$ and p a prime. We have

$$v(a_0) = 0\,, \quad v(a_{d-3}) = 0\,, \quad v(a_{d-1}) = d-2\,, \quad v(a_d) = d\,.$$

$$e(F) = \max\left\{\frac{-d+2}{d-1}, -1\right\} = \frac{-d+2}{d-1} = \frac{v(a_0)-v(a_{d-1})}{d-1}\,,$$

so we can apply Theorem 1. We have $s = d-1$ and $\gcd\left(v(a_0)-v(a_{d-1}), s\right) = \gcd(d-2, d-1) = 1$.

Therefore, the polynomial F is irreducible or has a divisor of degree $s = d-1$. In this case, it should have also a linear divisor, so an integer root. Such roots should be of the form $-p^t$, with $t \in \{0, 1, \ldots, p^d\}$, and this can be checked for particular values of d and t.

4.4 Bivariate Polynomials

Let k be an algebraically closed field of characteristic zero and suppose that F is a bivariate polynomial from $k[X,Y]$. We suppose that it has the representation

$$F(X,Y) \;=\; P_0(X)Y^d + P_1(X)Y^{d-1} + \ldots + P_{d-1}(X)Y + P_d(X)\,,$$

where $P_i \in k[X]$, $P_0 \neq 0$.

For $P \in k[X]$ we put $v(P) = -\deg(P)$, and this defines a discrete valuation on $A := k[X]$. Because

$$v(P_0) - v(P_i) = \deg(P_i) - \deg(P_0)$$

the Newton index of the polynomial $F(X,Y) \in A[Y]$ becomes

$$e(F) \;=\; \max_{1 \leq i \leq d}\left\{\frac{\deg(P_i)-\deg(P_0)}{i}\right\}\,,$$

which is exactly the degree index considered bu L. Panaitopol–D. Ştefănescu in [14]. The results within Section 3 have, therefore, polynomial approaches. For example, by Theorem 1 we obtain:

Corollary 2 (D. Ştefănescu [18]). *Let k be an algebraically closed field of characteristic zero and let*

$$F(X,Y) = P_0(X)Y^d + P_1(X)Y^{d-1} + \ldots + P_{d-1}(X)Y + P_d(X)\,, \quad P_0\,P_d \neq 0\,.$$

If there exists an index $s \in \{1,2,\ldots,d\}$ such that the following conditions are satisfied

(a) $\dfrac{\deg(P_i) - \deg(P_0)}{i} < \dfrac{\deg(P_s) - \deg(P_0)}{s}$ *for* $i \in \{1,2,...,d\}, i \neq s$;

(b) $\dfrac{\deg(P_s) - \deg(P_0)}{s} - \dfrac{\deg(P_d) - \deg(P_0)}{d} = \dfrac{1}{ds}\,.$

(c) $\gcd(\deg(P_s) - \deg(P_0), s) = 1$

the polynomial F is either irreducible in $A[X]$, or has a factor whose degree is a multiple of s.

Example 4. Let $F(X,Y) = X^mY^d + XY^{d-1} + XY^{d-2} + Y^2 + p(X)Y + q(X)$ with $\deg(p) = \deg(q) = m+1$, $m \geq 1$, $d \geq 5$ and $q(0) \neq 0$. We have

$$\begin{aligned}
\frac{\deg(P_1) - \deg(P_0)}{1} &= \frac{1-m}{1}\,,\\
\frac{\deg(P_2) - \deg(P_0)}{1} &= \frac{1-m}{2}\,,\\
\frac{\deg(P_{d-2}) - \deg(P_0)}{d-2} &= \frac{-2}{d-3}\,,\\
\frac{\deg(P_{d-1}) - \deg(P_0)}{d-1} &= \frac{1}{d-1}\,,\\
\frac{\deg(P_d) - \deg(P_0)}{d} &= \frac{1}{d}\,.
\end{aligned}$$

We then apply Theorem 1 and obtain that the polynomial F is either irreducible or it has a divisor of degree $d-1$ with respect to Y. Therefore, F is irreducible or has a linear divisor with respect to Y.

Example 5. Let $F(X,Y) = (X^3+1)Y^d + X^2Y^{d-1} + (X^{d-2}+X+1)Y^3 - XY + X^{d+1} + 1$. We have

$$\begin{aligned}
\frac{\deg(P_1) - \deg(P_0)}{1} &= \frac{0-3}{1} = -3\,,\\
\frac{\deg(P_{d-3}) - \deg(P_0)}{d-3} &= \frac{d-2}{d-3} > 1\,,\\
\frac{\deg(P_{d-1}) - \deg(P_0)}{d-1} &= \frac{1-3}{d-1} = -\frac{2}{d-1}\,,\\
\frac{\deg(P_d) - \deg(P_0)}{d} &= \frac{4-3}{d} = \frac{1}{d}\,.
\end{aligned}$$

It follows that the Newton index is $e(F) = \frac{d-2}{d-3}$. We have $s = d-3$, $(d-2, d-3) = 1$ and

$$\frac{\deg(P_{d-3}) - \deg(P_0)}{d-3} - \frac{\deg(P_d) - \deg(P_0)}{d} = \frac{d-2}{d-3} - \frac{d+1}{d} = \frac{3}{d(d-3)}.$$

So we can apply Theorem 2. We have the following possibilities.

i. The polynomial F is irreducible in $k[X, Y]$.

ii. The polynomial F has a divisor whose degree with respect to Y is a multiple of $d-3$. Therefore, there exists a divisor of degree 3 with respect to Y.

iii. There exists a nontrivial factorization $F = F_1 F_2$ such that $d-3$ divides $\beta d_1 - \alpha d_2$, where $d_1 = \deg(F_1)$, $d_2 = \deg(F_2)$ and $\alpha, \beta \in \{1, 2, 3\}$. If we look at the proofs of Theorems 1 and 2 we can compute α and β.

In fact, from the relations

$$\begin{aligned} cd_1 - sm_1 &= 1, \\ cd_2 - sm_2 &= 2 \end{aligned}$$

we obtain $c(d_2 - 2d_1) = s(m_2 - 2m_1)$, so s must divide $d_2 - 2d_1$.

For our example we deduce that $d_2 - 2d_1$ must be divisible by 3. For particular values of d this condition is not satisfied. For example, for $d = 5$, we have $(d_2, d_1) \in \{(1,4), (2,3), (3,2), (4,1)\}$, so the cases to be considered are

$$\begin{aligned} 1 - 2 \cdot 4 &= -7, \\ 2 - 2 \cdot 3 &= -4, \\ 3 - 2 \cdot 2 &= -1, \\ 4 - 2 \cdot 1 &= 2, \end{aligned}$$

and none of them is a multiple of 3.

Example 6. Let $F(X, Y) = p(X)Y^d + Y^{d-1} + q(X)Y^2 + r(X)$, with $\deg(p) = m \geq 1$, $\deg(q) = d + m - 1$, $\deg(r) = d + m + 1$, $d \geq 5$. We have

$$\begin{aligned} \frac{\deg(P_1) - \deg(P_0)}{1} &= \frac{0 - m}{1} &&= -m, \\ \frac{\deg(P_{d-2}) - \deg(P_0)}{d-2} &= \frac{d + m - 1 - m}{d-2} &&= -\frac{d-1}{d-2}, \\ \frac{\deg(P_d) - \deg(P_0)}{d} &= \frac{d + m - 2 - m}{d} &&= \frac{d+1}{d}. \end{aligned}$$

We obtain $e(F) = \frac{d-1}{d-2}$ and $d-1$ and $d-2$ are coprime. On the other hand,

$$e(F) - \frac{\deg(r)}{d} = \frac{d-1}{d-2} - \frac{d+1}{d} = \frac{2}{d(d-2)}$$

and we can apply Theorem 2. There are three possible cases:

i. The polynomial F is irreducible in $k[X, Y]$.

ii. The polynomial F has a divisor whose degree with respect to Y is a multiple of $d-2$. So this divisor is od degree $d-2$ with respect to Y. Therefore F could have a quadratic divisor with respect to Y.

iii. There exists a factorization $F = F_1F_2$ and the difference of their degrees is a multiple of $d-2$. If we suppose $1 \leq d_1 \leq d_2 \leq d-1$ we obtain $0 \leq d_2-d_1 \leq d-2$. It follows that we have

$$d_1 = d_2 \quad \text{or} \quad d_2 - d_1 = d - 2\,.$$

The last condition is satisfied only if $d_1 = 1$ and $d_2 = d-1$.

We conclude that the polynomial F is irreducible if it does not have quadratic divisors with respect to Y and satisfies one of the two conditions:

a. Its degree d is odd.

b. It does not have linear divisors with respect to Y.

5 Conclusion

In this paper we proposed a method for the construction of univariate irreducible polynomials over discrete valuation domains. We proved that our approach extends basic results on the irreducibility of univariate polynomials over the integers and on bivariate polynomials over an algebraically closed field. The method has applications also to polynomials in other discrete valuation domains. It requires the computation of families of numbers that satisfy some conditions. The use of computer packages allows us to obtain new classes of irreducible polynomials.

Future work will be done for applying these techniques for the construction of multivariate irreducible polynomials.

Acknowledgement. The author is grateful to the anonymous referees for valuable comments and suggestions.

References

1. Angermüller, G.: A generalization of Ehrenfeucht's irreducibility criterion. J. Number Theory 36, 80–84 (1990)
2. Bhatia, S., Khanduja, S.K.: Difference polynomials and their generalizations. Mathematika 48, 293–299 (2001)
3. Bishnoi, A., Khanduja, S.K., Sudesh, K.: Some extensions and applications of the Eisenstein irreducibility criterion. Developments in Mathematics 18, 189–197 (2010)
4. Bonciocat, A.I., Bonciocat, N.C.: Some classes of irreducible polynomials. Acta Arith. 123, 349–360 (2006)

5. Bonciocat, N.C.: A Capelli type theorem for multiplicative convolutions of polynomials. Math. Nachr. 281, 1240–1253 (2008)
6. Bonciocat, N.C.: On an irreducibility criterion of Perron for multivariate polynomials. Bull. Math. Soc. Sci. Math. Roumanie 53(101), 213–217 (2010)
7. Bonciocat, N.C.: Schönemann-Eisenstein-Dumas-type irreducibility conditions that use arbitrarily many prime numbers. arXiv:1304.0874v1
8. Bonciocat, N.C., Bugeaud, Y., Cipu, M., Mignotte, M.: Irreducibility criteria for sums of two relatively prime polynomials. Int. J. Number Theory 9, 1529–1539 (2013)
9. Bonciocat, N.C., Zaharescu, A.: Irreducible multivariate polynomials obtained from polynomials in fewer variables. J. Pure Appl. Algebra 212, 2338–2343 (2008)
10. Dumas, G.: Sur quelques cas d'irréducibilité des polynômes à coefficients rationnels. Journal de Math. Pures et Appl. 12, 191–258 (1906)
11. Eisenstein, G.: Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt. J. Reine Angew. Math. 39, 160–182 (1850)
12. Lipkovski, A.: Newton Polyhedra and Irreducibility. Math. Z. 199, 119–128 (1988)
13. Ore, O.: Zur Theorie der Eisensteinschen Gleichungen. Math. Z. 20, 267–279 (1924)
14. Panaitopol, L.D., Ştefănescu, D.: On the generalized difference polynomials. Pacific J. Math. 143, 341–348 (1990)
15. Rubel, L.A., Schinzel, A., Tverberg, H.: On difference polynomials and hereditary irreducible polynomials. J. Number Theory 12, 230–235 (1980)
16. Schönemann, T.: Von denjenigen Moduln, welche Potenzen von Primzahlen sind. J. Reine Angew. Math. 32, 93–105 (1846)
17. Ştefănescu, D.: Construction of classes of irreducible bivariate polynomials. In: Gerdt, V.P., Koepf, W., Mayr, E.W., Vorozhtsov, E.V. (eds.) CASC 2013. LNCS, vol. 8136, pp. 393–400. Springer, Heidelberg (2013)
18. Ştefănescu, D.: On the irreducibility of bivariate polynomials. Bull. Math. Soc. Sci. Math. Roumanie 56(104), 377–384 (2013)
19. Zaharescu, A.: Residual transcendental extentions of valuations, irreducible polynomials and trace series over p–adic fields. Bull. Math. Soc. Sci. Math. Roumanie 56(104), 125–131 (2013)
20. Weintraub, S.H.: A mild generalization of Eisenstein's criterion. Proc. Amer. Math. Soc. 141, 1159–1160 (2013)