Construction of Classes of Irreducible Bivariate Polynomials

Doru Ştefănescu

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

Abstract. We describe a method for constructing classes of bivariate polynomials which are irreducible over algebraically closed fields of characteristic zero. The constructions make use of some factorization conditions and apply to classes of polynomials that includes the generalized difference polynomials.

Keywords: Irreducible polynomials, Polynomial factorization, Algebraic algorithms.

Introduction

We consider bivariate polynomials polynomials over an algebraically closed field k of characteristic zero. It is known that the ring $k[X,Y]$ of these polynomials is a unique factorization domain. The irreducible elements in $k[X,Y]$ are the irreducible polynomials, and they play the key role in polynomial factorization.

There exist several results concerning the construction of bivariate irreducible polynomials, see [1], [5], [6], [7]. They apply for polynomials for which the leading coefficient of a variable is a nonzero constant, namely

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

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

We remind that such a polynomial is called a *generalized difference polynomial* if

$$\deg(P_i) \;<\; i\,\frac{\deg(P_n)}{n} \quad \text{for all} \quad i,\; 1 \le i \le n-1\,.$$

We consider the degree-index

$$p_Y(F) \;=\; \max\left\{\frac{\deg(P_i)}{i}\,;\, 1 \le i \le n\right\}$$

considered by Panaitopol–Ştefănescu [6]. It was proved that for particular values of $p_Y(F)$, the polynomial $F(X,Y)$ is irreducible in $k[X,Y]$, see, for example [1], [2], [3], [5], [6]. They key tool for constructing irreducible polynomials using the degree index is the consideration of the Newton polygon of a product of two polynomials, see [6]. In fact:

V.P. Gerdt et al. (Eds.): CASC 2013, LNCS 8136, pp. 393–400, 2013.

Proposition 1 (Panaitopol–Ştefănescu, 1990). *If $F = F_1F_2$ is factorization in $k[X,Y]$ and $p_Y(F) = \deg(P_n)/n$, we have*

$$p_Y(F) = p_Y(F_1) = p_Y(F_2)\,.$$

The previous result can be restated for univariate polynomials with coefficients in a valued field, see, for example [4].

In this paper, we give a method for the construction of bivariate irreducible polynomials of the form (1) for which the degree index is not equal to $\deg(P_n)/n$. Such polynomials are called *quasi–difference polynomials* (cf. [3]). More precisely, we will give factorization conditions in function of the difference between the degree index $p_Y(F)$ and $\deg(P_n)/n$.

Factorization Conditions

From now on, we consider a family of polynomials $F \in k[X,Y]$ which contains the generalized difference polynomials.

Theorem 1. *Let*

$$F(X,Y) = cY^n + \sum_{i=1}^{n} P_i(X)Y^{n-i} \in k[X,Y], c \in k \setminus \{0\}$$

for which there exists $s \in \{1,2,...,n\}$ such that the following conditions are satisfied:

(a) $\dfrac{degP_i}{i} \le \dfrac{degP_s}{s}$ *, for all* $i \in \{1,2,...,n\}$.

(b) $(degP_s, s) = 1$.

(c) $\dfrac{degP_s}{s} - \dfrac{degP_n}{n} \le \dfrac{1}{sn}$.

Then $F(X,Y)$ is irreducible in $k[X,Y]$ or has a factor whose degree with respect to Y is a multiple of s.

Proof: Let us suppose that there exists a nontrivial factorization $F = F_1F_2$ of the polynomial F. We put $m = \deg(P_n)$ and $a = \deg(P_s)$. By hypothesis (a) we have

$$P_Y(F) \;=\; \frac{a}{s}\,.$$

On the other hand, by condition (c),

$$an - sm \;\le\; 1\,.$$

If $an - sm = 0$ we have

$$P_Y(P) \;=\; \frac{m}{n}$$

and by Proposition 1 we have

$$p_Y(F) = p_Y(F_1) = p_Y(F_2)\,. \tag{2}$$

We have $an=sm$ and, by hypotheses, $(a,s)=1$, so s should divide $n=\deg_Y(F)$. On the other hand, by (2)

$$\frac{a}{s} = p_Y(F_1) = \frac{m_1}{n_1}\,,$$

where $n_1 = \deg(F_1)$, $m_1 = \deg_X F(X,0)$. Therefore,

$$an_1 = sm_1\,.$$

But $(a,s) = 1$, so s should divide $n_1 = \deg_Y(F_1)$.

We consider now the case $an - sm = 1$.

By Theorem 1 from [6], we know that $p_Y(F) = \max\{p_Y(F_1), p_Y(F_2)\}$
We observe that

$$\frac{m_1}{n_1} \le p_Y(F_1) \le p_Y(F) = \frac{a}{s}\,,$$

which gives

$$an_1 - sm_1 \ge 0\,. \tag{3}$$

We put $n_2 = \deg_Y(F_2)$ and $m_2 = \deg_X F_2(X,0)$ and we observe that

$$\frac{m_2}{n_2} = \frac{m - m_1}{n - n_1} \le p_Y(F_2) \le p_Y(F) = \frac{a}{s}.$$

We successively obtain

$$\begin{aligned} &s(m - m_1) &&\le a(n - n_1),\\ &sm - sm_1 &&\le an - an_1,\\ &(an - sm) + (sm_1 - an_1) &&\ge 0,\\ &1 + (sm_1 - an_1) &&\ge 0,\\ &an_1 - sm_1 &&\le 1\,. \end{aligned}$$

Therefore, using (3), we have $an_1 - sm_1 \in \{0,1\}$.

In the case $an_1 - sm_1 = 0$, because a and s are coprime, it follows that s divides $n_1 = \deg_Y(F_1)$, hence the conclusion.

If $an_1 - sm_1 = 1$ we successively obtain

$$\begin{aligned} &an_1 - sm_1 &&= 1,\\ &a(n - n_2) - s(m - m_2) &&= 1,\\ &(an - sm) + (sm_2 - an_2) &&= 1,\\ &1 + (sm_2 - an_2) &&= 1,\\ &sm_2 - an_2 &&= 0\,. \end{aligned}$$

From $sm_2 = an_2$ and the assumption that a and s are coprime, it follows that s divides $n_2 = \deg_Y(F_2)$.

Corollary 1. *If $s \in \{1, n-1\}$ and F has no linear factors with respect to Y, the polynomial F is irreducible in $k[X,Y]$.*

Proof. By Theorem 1, if F is not irreducible it must have a divisor of degree s with respect to Y. So $F = F_1F_2$, where one of the polynomials F_1 or F_2 has the degree 1 with respect to Y. But F has no linear factors with respect to Y. □

Corollary 2. *If $n > 3$ and $s > n/2$ the polynomial F is irreducible or has a divisor of degree s with respect to Y.*

Proof. By Theorem 1 the polynomial F is irreducible or has a divisor G of degree ds. In the second case we have

$$n > ds > d.\frac{n}{2}.$$

It follows that $d < 2$, so $d = 1$. □

Proposition 2. *Let $F(X,Y) = Y^n + \sum_{i=1}^{n} P_i(X)Y^{n-i} \in k[X,Y]$ and suppose that there exists $s \in \{1, 2, ..., n\}$ such that $(degP_s, s) = 1$, $\frac{degP_i}{i} \le \frac{degP_s}{s}$ for all $i \in \{1, 2, ..., n\}$ and*

$$\frac{degP_s}{s} - \frac{degP_n}{n} = \frac{u}{sn}, \quad \textit{where} \quad u \in \{2, 3\}.$$

Then one of the following statements is satisfied:

1. The polynomial $F(X,Y)$ is irreducible in $k[X,Y]$.

2. The polynomial F has a divisor whose degree with respect to Y is a multiple of s.

3. The polynomial F factors in a product of two polynomials such that the difference of their degrees with respect to Y is a multiple of s.

4. The polynomial F factors in a product of two polynomials such that the difference between the double of the degree of one of them and the degree of the other with respect to Y is a multiple of s.

Proof. With the notation from Theorem 1 we have

$$as - sm = 2 \quad \text{or} \quad 3.$$

The case $as - sm = 2$.

This gives

$$a(n_1 + n_2) - s(m_1 + m_2) = 2,$$

i.e.,

$$(an_1 - sm_1) + (an_2 - sm_2) = 2.$$

If $an_1 - sm_1 = 0$ or $an_1 - sm_1 = 2$ we have the conclusions from Theorem 1, i.e., in this case the polynomial $F(X,Y)$ is irreducible in $k[X,Y]$ or has a divisor of degree with respect to Y which is a multiple of s.

If

$$\begin{aligned} an_1 - sm_1 &= 1\,, \\ an_2 - sm_2 &= 1 \end{aligned}$$

we consider the solution of the Diophantine equation $ax - sy = 1$. If (x_0, y_0) is a solution, we have

$$\begin{cases} n_1 = x_0 + t_1,\; n_2 \;= x_0 + t_2 s\,, \\ n_2 = y_0 + t_1,\; m_2 = y_0 + t_2\,, \end{cases}$$

where $t_1, t_2 \in \mathbb{Z}$.

We obtain

$$\begin{aligned} n_1 - n_2 \;\; &= (t_1 - t_2)s, \\ m_1 - m_2 &= (t_1 - t_2)a\,. \end{aligned}$$

It follows that the difference of the degrees with respect to Y of the two divisors is a multiple of s.

The case $as - sm \;=\; 3$.

It follows that

$$a(n_1 + n_2) - s(m_1 + m_2) \;=\; 3\,,$$

that is

$$(an_1 - sm_1) + (an_2 - sm_2) \;=\; 3\,.$$

We have the following possibilities:

$$\begin{aligned} an_1 - sm_1 &= 0 \text{ and } an_2 - sm_2 = 3\,, \\ an_1 - sm_1 &= 1 \text{ and } an_2 - sm_2 = 2\,, \\ an_1 - sm_1 &= 2 \text{ and } an_2 - sm_2 = 1\,, \\ an_1 - sm_1 &= 3 \text{ and } an_2 - sm_2 = 0\,. \end{aligned} \tag{4}$$

It is sufficient to examinate the first two cases.

If $an_1 - sm_1 = 0$ and $an_2 - sm_2 = 3$ we have $an_1 = sm_1$, so s divides n_1, and we are in case 2 of the conclusions.

Suppose that $an_1 - sm_1 = 1$ and $an_2 - sm_2 = 2$. Substracting these relations we obtain

$$a(n_2 - n_1) + s(m_2 - m_1) = 1$$

and substracting from this the relation $an_1 - sm_1$ we finally have

$$a(n_2 - 2n_1) - s(m_2 - 2m_1) = 0\,. \tag{5}$$

Relation (5) proves that s divides $n_2 - 2n_1$, so we are in case 4 from the conclusions. □

Remark 1. Note that if $u = 2$ we have the conclusions 1, 2 or 3, while if $u = 3$ one of the statements 1, 2 or 4 is satisfied.

Applications

We use the previous results for studying factorization properties of some families of polynomials and the construct of classes of irreducible polynomials.

Example 1. Corollary 1 produces families of irreducible polynomials in $k[X,Y]$. It is sufficient to apply the following steps:

- Fix $n \geq 4$ and $s = n-1$.
- Fix the natural numbers a_1, a_2, ..., a_{n-2} and a_n.
- Compute
$$M = \max\left\{\frac{a_i}{i}\,;\, 2 \leq i \leq n, i \neq s\right\}.$$
- Compute $a = a_s \in \mathbb{N}^*$ such that
$$\frac{a}{n-1} > M \quad \text{and} \quad (a, n-1) = 1\,.$$
- Compute polynomials P_i such that $\deg(P_i) = a_i$ for all $i \in \{1, 2, \ldots, n\}$.
- Check if the polynomial $F(X,Y) = Y^n + \sum_{i=1}^{n} P_i(X)Y^{n-i}$ has linear factors with respect to Y.

If $F(X,Y)$ has no linear divisors with respect to Y conclude that it is irreducible in $k[X,Y]$.

Example 2. We consider

$$F(X,Y) = Y^n + p(X)Y^2 + q(X),$$

where $p, q \in k[X]$, $n \in \mathbb{N}$, $n \geq 4$, and 3 does not divide n.
Note that in this case $m = \deg(q)$.

We suppose that $\deg(p)$ and $n-2$ are coprime and that

$$\frac{\deg(p)}{n-2} > \frac{\deg(q)}{n}\,.$$

and we can apply Theorem 1 or Proposition 2 provided we have

$$\frac{a}{s} - \frac{m}{n} = \frac{\deg(p)}{n-2} - \frac{\deg(q)}{n} \leq \frac{3}{(n-2)n}\,.$$

Particular Case:

We consider $\deg(p) = n-1$ and $\deg(q) = n+1$. Then we have

$$\frac{a}{s} - \frac{m}{n} = \frac{n(n-1) - (n-2)(n+1)}{(n-2)n} = \frac{2}{(n-2)n}\,.$$

The hypotheses of Proposition 2 are fulfilled. We have $a = n-1$ and $s = n-2$. Indeed, $n-1$ and $n-2$ are coprime and

$$s = n - 2 \geq \frac{n}{2}\,.$$

If we are in case 2, let G be a nontrivial divisor. Then $\deg_Y(G) = k(n-2)$, with $k \geq 1$. It follows that $k = 1$, so $\deg_Y(G) = n-2$. We deduce that the other divisor of F has the Y-degree equal to 2, so F has a quadratic factor with respect to Y.

If we are in case 3, let $F = GH$ be a nontrivial factorization in $k[X,Y]$. Since $|\deg_Y(G) - \deg_Y(H)| = k(n-2)$ we have $|\deg_Y(G) - \deg_Y(H)| = n-2$. Let us suppose that $\deg_Y(G) \geq \deg_Y(H)$. We have $\deg_Y(G) - \deg_Y(H) = n-2$, hence $\deg_Y(G) = \deg_Y(H) + n - 2 \geq n-1$.

Because $\deg_Y(H) \geq 1$ we have $\deg_Y(G) = n-1$ and $\deg_Y(H) = 1$, therefore, one of the divisors of F is linear with respect to Y.

Therefore, if $\deg(p) = n-1$ and $\deg(q) = n+1$ the polynomial $F(X,Y) = Y^n + p(X)Y^2 + q(X)$ is irreducible or has a factor of degree 1 or 2 with respect to Y.

Remark 2. If, in the previous case, the polynomial $q(X)$ is square free, then $F(X,Y)$ is irreducible or has a quadratic factor with respect to Y. Indeed, if there is a linear factor $Y - r(x)$ then $r^n + pr^2 + q = 0$, so r^2 would divide q.

Example 3. The polynomial $F(X,Y) = Y^n + X^2Y^2 + X^3$ is irreducible in $\mathbb{Z}[X,Y]$ for all $n \in \mathbb{N}^*$, n is not divisible by 3.

If $n \geq 7$ we have

$$\frac{m}{n} = \frac{3}{n} > \frac{2}{n-2} = \frac{a}{s},$$

so $p_Y(F) = 3/n$ and F is a generalized difference polynomial. By hypotheses n is not a multiple of 3, by Corollary 3 from [6], the polynomial F is irreducible.

For $n < 7$ we have to check the irreducibility for $n \in \{1,2,4,5\}$. In each case, the polynomial is irreducible.

Example 4. We consider

$$F(X,Y) = Y^n + p(X)Y^3 + q(X)Y^2 + r(X), \quad \text{where} \quad p,q,r \in k[X], n \geq 5.$$

In this case, $m = \deg(r)$.

We suppose that

$$\frac{\deg(q)}{n-2} > \frac{\deg(r)}{n} = \frac{m}{n}.$$

We consider

$$\deg(p) = n-4, \quad \deg(q) = n-1, \quad \deg(r) = n+1$$

the previous conditions are satisfied. We note that we have

$$\frac{a}{s} - \frac{m}{n} = \frac{3}{sn},$$

so we can use Proposition 2.

If a factor has the degree multiple of $s = n-2$, then it has degree $n-2$. So the other factor is quadratic or the square of a linear factor.

If we are in case 4 from the conclusions, let G, H be two factors such that $\deg(G) - 3\deg(H)$ be a multiple of $s = n - 2$. This gives information on the divisors in particular cases.

In the case $n = 5$, for example, we have $\deg(G) = 3\deg(H) + 3t$ with $t \in \mathbb{N}$, so $\deg(G)$ is a multiple of 3. Therefore, $\deg(G) = 3$, and the other factor is quadratic or the square of a linear factor.

References

1. Angermüller, G.: A generalization of Ehrenfeucht's irreducibility criterion. J. Number Theory 36, 80–84 (1990)
2. Ayad, M.: Sur les polynômes f(X,Y) tels que K[f] est intégralement fermé dans K[X,Y]. Acta Arith. 105, 9–28 (2002)
3. Bhatia, S., Khanduja, S.K.: Difference polynomials and their generalizations. Mathematika 48, 293–299 (2001)
4. Bishnoi, A., Khanduja, S.K., Sudesh, K.: Some extensions and applications of the Eisenstein irreducibility criterion. Developments in Mathematics 18, 189–197 (2010)
5. Cohen, S.D., Movahhedi, A., Salinier, A.: Factorization over local fields and the irreducibility of generalized difference polynomials. Mathematika 47, 173–196 (2000)
6. Panaitopol, L., Ştefănescu, D.: On the generalized difference polynomials. Pacific J. Math. 143, 341–348 (1990)
7. Rubel, L.A., Schinzel, A., Tverberg, H.: On difference polynomials and hereditary irreducible polynomials. J. Number Theory 12, 230–235 (1980)