Construction of Classes of Irreducible Bivariate Polynomials

Doru Ştefănescu
University of Bucharest

CASC 2013

Outline

- Generalized difference polynomials
- Factorization conditions
- Irreducibility tests
- Applications

Bivariate polynomials

We consider an algebraically closed field k of characteristic zero and the ring $k[X, Y]$ of bivariate polynomials over k.

There exist several results concerning the construction of bivariate irreducible polynomials. 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 $c \in k \setminus \{0\}, \in \mathbb{N}^*, P_i(X) \in k[X]$.

Generalized difference polynomials

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

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

- We consider the degree-index

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

see Panaitopol–Ştefănescu (1990).

Generalized difference polynomials (contd.)

- For special values of $p_Y(F)$, Angermüller (1990), Panaitopol–Ştefănescu (1990), Cohen–Movahhedi–Salinier (2000), Bhatia–Khanduja (2001), Ayad (2002) proved that the polynomial $F(X,Y)$ is irreducible in $k[X,Y]$.
- They key tool for constructing irreducible polynomials using the degree index is the consideration of the Newton polygon of a product of two polynomials. In fact, we have:

A theorem of Panaitopol–Ştefănescu

Proposition (Panaitopol–Ştefănescu, 1990)

If $F = F_1 F_2$ *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 Bishnoi–Khanduja–Sudesh (2010).

A class of quasi–difference polynomials

Our purpose is to 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 not generalized difference polynomials but belong to the family of *quasi–difference polynomials*, see Bhatia-Khanduja (2001).

We will give factorization conditions in function of the difference between the degree index $p_Y(F)$ and $\deg(P_n)/n$.

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

Factorization conditions

Theorem

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.

Irreducibility tests

Corollary

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

Corollary

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

Irreducibility tests (contd.)

Proposition

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*
$(degP_s, s) = 1$,
$$\frac{degP_i}{i} \leq \frac{degP_s}{s} \ \text{for all} \ i \in \{1,2,...,n\}$$
and
$$\frac{degP_s}{s} - \frac{degP_n}{n} = \frac{u}{sn} \ \text{where} \ u \in \{2,3\}.$$
Then one of the following statements is satisfied:

Irreducibility tests (contd.)

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.

Irreducibility tests (contd.)

Remark: 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.

Construction of irreducible polynomials

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

Corollary 2 produces families of irreducible polynomials in $k[X, Y]$. It is sufficient to apply the following steps:

Examples

- Fix $n \geq 4$ and $s = n - 1$.
- Fix the natural numbers $a_1, a_2, \ldots, a_{n-2}$ 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 $\frac{a}{n-1} > M$ and $(a, n-1) = 1$.
- 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 $k[X,Y]$.

An example

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 cases

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

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

Particular cases (contd.)

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.

Particular cases (contd.)

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 $\deg_Y(G) = \deg_Y(H) + n - 2 \geq n - 1$.

Particular cases (contd.)

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.

Particular cases (contd.)

Remark: 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.

Particular cases (contd.)

Example

The polynomial $F(X,Y) = Y^n + X^2Y^2 + X^3$ is irreducible in $\mathbb{Z}[X,Y]$ for all $n \in \mathbb{N}^*$, with n 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 the paper Panaitopol–Ştefănescu (1990), 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.

Another application

We consider $F(X,Y) = Y^n + p(X)Y^3 + q(X)Y^2 + r(X)$, where $p, q, r \in k[X]$, $n \geq 5$. In this case, $m = \deg(r)$.
We suppose that

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

and we consider

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

Another application (contd.)

so 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.

Another application (contd.)

If we are in case 4 from the conclusions, let G, H be two factors such that $\deg(G) - 3\deg(H)$ is 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.

Some references

- Angermüller, G.: A generalization of Ehrenfeucht's irreducibility criterion. J. Number Theory 36, 80–84 (1990)
- 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)
- Bhatia, S., Khanduja, S.K.: Difference polynomials and their generalizations. Mathematika 48, 293–299 (2001)

Some references

- Bishnoi, A., Khanduja, S.K., Sudesh, K.: Some extensions and applications of the Eisenstein irreducibility criterion. Developments in Mathematics 18, 189–197 (2010)
- Cohen, S.D., Movahhedi, A., Salinier, A.: Factorization over local fields and the irreducibility of generalized difference polynomials. Mathematika 47, 173–196 (2000)

Some references

Panaitopol, L., Ştefănescu, D.: On the generalized difference polynomials. Pacific J. Math. 143, 341–348 (1990)

Rubel, L.A., Schinzel, A., Tverberg, H.: On difference polynomials and hereditary irreducible polynomials. J. Number Theory 12, 230–235 (1980)

Thanks

$\ddot\smile$ MANY THANKS FOR YOUR ATTENTION !