ISSN 0965-5425, Computational Mathematics and Mathematical Physics, 2020, Vol. 60, No. 1, pp. 128–133. © Pleiades Publishing, Ltd., 2020.

# Computational Aspects of Irreducible Polynomials

**D. Ştefănescu**

*Department of Theoretical Physics and Mathematics University of Bucharest, Bucharest, 050107 Romania*

*e-mail: doru.stefanescu@gmail.com*

Received July 31, 2019; revised August 15, 2019; accepted September 18, 2019

**Abstract**—We present results on testing the computation of bounds for polynomial divisors and give estimates for their heights. There are also given results on the irreducibility of polynomials and some methods for constructing irreducible polynomials. They are based on properties of Newton's polygon.

Finally we give applications to the irreducibility of univariate polynomials

$$F(X) = \sum_{i=0}^{d} a_i X^{d-i}$$

over a discrete valuation domain. We give applications to bivariate polynomials.

**Keywords:** computer polynomial algebra, polynomial divisors, irreducible polynomials

**DOI:** 10.1134/S0965542520010133

## 1. INTRODUCTION

A main problem in polynomial algebra is to decide if a polynomial over a unique factorization domain is irreducible. There exist many results that give sufficient conditions for the irreducibility, the so called *irreducible polynomials*. On the other hand the irreducibility can be decided using algorithms for polynomial factorization.

We shall discuss computational problems concerning irreducible polynomials. We shall first present results on the computation of sizes of polynomial divisors. In the second part we present irreducible criteria that use properties of Newton's polygon.

## 2. POLYNOMIAL DIVISORS

We know that any univariate polynomial over a unique factorization domain can be uniquely decomposed in a product of irreducible polynomials. In particular, any univariate polynomial over the integers is a product of irreducible polynomials.

The classical methods invented by Newton and Kronecker give algorithmic methods for the factorization of univariate polynomials over the integers. They implicitely give also criteria for establishing if a polynomial is irreducible. Modern and more efficient methods were developed at the end of the 20th century, using reduction to the factorization over finite fields and suitable lifting methods.

I. Newton described in *Arithmetica Universalis* a device for computing the polynomial divisors of univariate divisors over the integers, see the section *De inventione divisorum*. His method is based on properties of finite differences and polynomial interpolation through finite differences. The method of Newton was improved by N. Bernoulli and F.T. Schubert (see [13]).

We consider a nonconstant reducible univariate polynomial $P$ with integer coefficients and a divisor $Q$ over the integers. We obtain new bounds for the coefficients of $Q$ in function of the degree and of the coefficients of $P$. These bounds are obtained using an inequality of Beauzamy and the multiplication by a suitable linear factor.

Let $P$ be a nonconstant univariate polynomial with integer coefficients. If $Q$ is a nontrivial divisor of $P$ over $\mathbb{Z}$ we are interested to give bounds for the absolute values of its coefficients in function of the coefficients and the degree of $P$. Such bounds are relevant in polynomial factorization and are expressed in function of the measure, the quadratic norm, the Bombieri norm and other polynomial sizes.

We refine an inequality of Beauzamy using the multiplication of the polynomial $P$ by a suitable linear factor.

## 3. APPLICATIONS TO POLYNOMIAL FACTORIZATION

We obtain upper bounds for the size of polynomial factors of an univariate polynomial with integer coefficients.

Let $P(X) = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]\backslash\mathbb{Z}$. By a result of B. Beauzamy [2], if $Q$ is a nontrivial divisor of $P$ in $\mathbb{Z}[X]$ one has

$$\mathrm{H}(Q) \le l_d \sqrt{D}, \tag{1}$$

where

$$l_d = \frac{3^{3/4}\cdot 3^{d/2}}{2\sqrt{\pi d}}, \qquad D = [P]_2^2 = \sum_{i=0}^{d} \frac{a_i^2}{\binom{d}{i}}.$$

Note that $[P]_2$ is the Bombieri's norm of the polynomial $P$.

We first need an inequality similar to (1). Our inequality depends on a real parameter $\alpha$ and suitable choices of it allows us to deduce refinements for the height of polynomial divisors of integer polynomials.

**Theorem 1.** *Let $Q$ be a nontrivial divisor of $P$ in $\mathbb{Z}[X]$, $d = \deg(P) \ge 2$. We have*

$$H(Q) \le \frac{1}{\big||\alpha|-1\big|} \frac{3^{3/4}\cdot 3^{\frac{d+1}{2}}}{2\sqrt{\pi(d+1)}} [(X-\alpha)P]_2$$

*for all $\alpha \in \mathbb{R}\backslash\{-1, 0, 1\}$.*

**Proof.** Suppose $P = QR$ is a nontrivial factorization of $P$ in $\mathbb{Z}[X]$. This gives the factorization

$$F = \big((X-\alpha)Q\big)\, R \tag{2}$$

of $F = (X-\alpha)P$ in $\mathbb{C}[X]$. We put $n = \deg(Q)$.

Let us remind a useful inequality of B. Beauzamy, E. Bombieri, P. Enflo and H. Montgomery [1]:

If $G$ and $H$ are nonconstant polynomials over $\mathbb{C}$ of degrees $m$ and $l$ respectively we have

$$\sqrt{\frac{(m+l)!}{m!l!}}[GH]_2 \ge [G]_2[H]_2.$$

By (2) this gives

$$[F]_2 \ge \sqrt{\frac{(n+1)!(d-n)!}{(d+1)!}}[(X-\alpha)Q]_2[R]_2.$$

Since the coefficients of $R$ are integers we have, as in the proof of (1), $[R]_2 \ge \sqrt{2}$. It follows that

$$[(X-\alpha)Q]_2 \le \sqrt{\frac{1}{2}\binom{d+1}{n+1}}[F]_2.$$

Let $(X-\alpha)Q = \sum_{j=0}^{n+1} v_j X^j$. We observe that

$$\frac{|v_j|^2}{\binom{n+1}{j}} \le [(X-\alpha)Q]_2^2 \le \frac{1}{2}\binom{d+1}{n+1}[F]_2^2,$$

so

$$|v_j| \le \sqrt{\frac{1}{2}\binom{d+1}{n+1}\binom{n+1}{j}}[F]_2.$$

On the other hand

$$\frac{1}{2}\binom{d+1}{n+1}\binom{n+1}{j} = \frac{(d+1)!}{2(d-n)!(n+1-j)!j!}$$

and $(d-n)+(n+1-j)+j=d+1$. Therefore, as in [1],

$$\sqrt{\frac{1}{2}\binom{d+1}{n+1}\binom{n+1}{j}} \le \frac{3^{3/4}\cdot 3^{\frac{d+1}{2}}}{2\sqrt{(d+1)\pi}} = l_{d+1},$$

which gives

$$\mathrm{H}\big((X-\alpha)Q\big) \le l_{d+1}[F]_2. \tag{3}$$

By the inequality of M. Mignotte [10] we have

$$\big\|\alpha\big|-1\big|\,\mathrm{H}(Q) \le \mathrm{H}\big((X-\alpha)Q\big).$$

So (3) gives

$$\mathrm{H}(Q) \le \frac{1}{\big\|\alpha\big|-1\big|}\,l_{d+1}[F]_2.$$

**Remark.** It is not possible to obtain the previous result applying directly the inequality (1) because the polynomial $(X-\alpha)P(X)$ has no integer coefficients, an essential condition in the theorem of B. Beauzamy [2].

### *3.1. Some Examples*

We consider first the polynomials studied in [1] and [11]:

$$F1 = x^8 + x^6 + 10x^4 + 10x^3 + 8x^2 + 2x + 8,$$

$$F2 = x^{15} + 30x^{14} + 5x^{13} + 2x^2 + 5x + 2,$$

$$F3 = 904050x^7 + 1479450x^6 - 2336817x^5 - 3403088x^4 + 2021847x^3 + 1477766x^2 - 1006566x + 170694,$$

$$F4 = x^{18} + 9x^{17} + 45x^{16} + 126x^{15} + 189x^{14} + 27x^{13} - 540x^{12} - 1215x^{11} + 1377x^{10} + 15444x^9 + 46899x^8 + 90153x^7 + 133893x^6 + 125388x^5 + 29160x^4 - 32076x^3 + 26244x^2 - 8748x + 2916.$$

The polynomial $F_5$ was considered by P.S. Wang [17] and M. Mignotte–P. Glesser [11]. Let $F_5 = a_1a_2a_3a_4$ where

$$a1 = 8192x^{10} + 20480x^9 + 58368x^8 - 161792x^7 + 198656x^6 + 199680x^5 - 414848x^4 - 4160x^3 + 171816x^2 - 48556x + 469,$$

$$a2 = 8192x^{10} + 12288x^9 + 66560x^8 - 22528x^7 - 138240x^6 + 572928x^5 - 90496x^4 - 356032x^3 + 113032x^2 + 23420x - 8179, \ cr,$$

$$a3 = 4096x^{10} + 8192x^9 + 1600x^8 - 20608x^7 + 20032x^6 + 87360x^5 - 105904x^4 + 18544x^3 + 11888x^2 - 3416x + 1,$$

$$a4 = 4096x^{10} + 8192x^9 - 3008x^8 - 30848x^7 + 21056x^6 + 146496x^5 - 221360x^4 + 1232x^3 + 144464x^2 - 78488x + 11993.$$

We denote by $B_1(P)$ the bound of Beauzamy (1) and by $B_2(P)$ our bound in Theorem 1.

**Table 1**

| $P$ | $F_1$ | $F_2$ | $F_3$ | $F_4$ | $F_5$ |
|---|---|---|---|---|---|
| $B_1(P)$ | 155.2 | 5145.1 | 16531988.3 | 13962915.8 | $3.8\times10^{2992}$ |
| $B_2(P)$ | 97.9 | 3832.4 | 15948685.5 | 8730942.5 | $5.8\times10^{2990}$ |

Note that, for convenient values of the parameter $\alpha$, we have $B_1(F_5)/B_2(F_5) = 64.49$.

However, as in [2], we have the bad polynomials $(1+X)^d$ and $X^d - 1$. If we take, for example, $P(X) = X^d - 1$, we obtain

$$B_1(P)/B_2(P) = \sqrt{\frac{2(d+1)^3}{2d(d+2)}} > 1 \quad \text{for all} \quad d \geq 1.$$

## 4. NEWTON'S POLYGON AND IRREDUCIBILITY CRITERIA

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.

Let $F(X) = \sum_{i=0}^{d} a_i X^{d-i} \in A[X]$, where $(A, v)$ is a discrete valuation domain.

The *Newton polygon* $N(F)$ of the polynomial $F$ is the lower convex hull of the set $\{(d-i,\ v(a_i));\ a_i \neq 0\}$. 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 [8] has studied the relationship between the Newton indices of two polynomials and the index of their product in 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 $F_1F_2$ 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.

**Proposition 2.** *If $F_1, F_2 \in A[X] \backslash A$ then $e(F_1F_2) = \max\big(e(F_1), e(F_2)\big)$.*

### *4.1. Irreducibility Tests*

We consider polynomials $F(X) = \sum_{i=0}^{d} a_i X^{d-i} \in A[X]$ for which the Newton index could be attained for an index $s \neq d$ and for which $v(a_0)$ could be nonzero. We have given in [16] the following results:

**Theorem 3.** *Let $(A, v)$ be a discrete valuation domain, and let $F(X) = a_0X^d + a_1X^{d-1} + \ldots + a_{d-1}X + a_d \in A[X]$, 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* $i \in \{1, 2, \ldots, d\}$, $i \neq s$,

(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 $s$.*

**Theorem 4.** *Let $(A, v)$ be a discrete valuation domain, and let $F(X) = a_0X^d + a_1X^{d-1} + \ldots + a_{d-1}X + a_d \in A[X]$, 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* $i \in \{1, 2, \ldots, d\}$, $i \neq s$;

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

One of the oldest irreducibility criterion for univariate polynomials with coefficients in a valuation domain was given by G. Dumas [8] as a valuation approach to Schönemann–Eisenstein's criterion for polynomials with integer coefficients ([15] and [9]).

**Theorem 5 (G. Dumas).** *Let $F(X) = \sum_{i=0}^{d} a_i X^{d-i}$ be a polynomial over a discrete valuation domain $A$, with valued field $(K, v)$. If the following conditions are fulfilled*

(i) $v(a_0) = 0$,

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

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

*then the polynomial $F(X)$ is irreducible in $K[X]$.*

**Remark.** We observe that Theorems 3 and 4 consider conditions that are not satisfied by Theorem 5 of G. Dumas.

With the notations in Theorem 3, one has the following result.

**Corollary 6.** *If $d \geq 4$ and $s > d/2$, then the polynomial $F$ is either irreducible, or has a divisor of degree $s$.*

**Proof.** 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.

### *4.2. Examples*

(1) Let $F(X) = X^d + p^d X^2 + p^{d-2}(p-1)X + p^{d-1} \in \mathbb{Z}[X]$, with $d \geq 3$ and $p$ a prime number, and let us consider the usual $p$-adic value on $\mathbb{Z}$, denoted by $v$. Since

$$\frac{v(a_{d-1})}{d-1} = \frac{d-2}{d-1} < \frac{d}{d-2} = \frac{v(a_{d-2})}{d-2}$$

and

$$\frac{v(a_{d-1})}{d-1} = \frac{d-2}{d-1} < \frac{d-1}{d} = \frac{v(a_d)}{d},$$

we may take $s = d-1$, and since $sv(a_d) - dv(a_s) = (d-1)^2 - d(d-2) = 1$, we conclude by Theorem 3 that $F$ is either irreducible, or has a factor of degree $d-1$, and hence also a linear factor. On the other hand, one may easily check that $F$ has no integer solutions, and hence is an irreducible polynomial.

(2) Let $F(X, Y) = Y^d + q(X)Y + r(X) \in \mathbb{Z}[X, Y]$, where $q, r \in \mathbb{Z}[X]$ with $\deg(q) = \deg(r) = 1$. Using now the discrete valuation on $\mathbb{Z}[X]$ given by $v(h) = -\deg(h)$ for $h \in \mathbb{Z}[X]$, we see that

$$\frac{v(q)}{d-1} = \frac{-1}{d-1} < \frac{-1}{d} = \frac{v(r)}{d},$$

so with the notation in Theorem 3 we have $s = d-1$. On the other hand, using the same notation we observe that

$$sv(a_d) - dv(a_s) = (d-1)v(r) - dv(q) = 1.$$

It follows that $F$ is either irreducible in $\mathbb{Z}[X, Y]$, or has a linear factor with respect to $Y$.

(3) Let $K$ be a field of characteristic zero, $d \geq 4$ an integer, and let

$$F(X, Y) = Y^d + (X^{d-2} + X + 1)Y^2 + (X^d + X + 1)Y + X^{d+1} + X^2 + 1 \in K[X, Y].$$

We represent the polynomial $F$ as

$$F(X, Y) = Y^d + a_{d-2}(X)Y^2 + a_{d-1}(X)Y + a_d(X)$$

with $a_{d-2}(X) = X^{d-2} + X + 1$, $a_{d-1}(X) = X^d + X + 1$ and $a_d(X) = X^{d+1} + X^2 + 1$. Using now the discrete valuation on $K[X]$ given by $v(h) = -\deg(h)$ for $h \in K[X]$, we observe that

$$\frac{v(a_{d-2})}{d-2} = -1, \quad \frac{v(a_{d-1})}{d-1} = -\frac{d}{d-1} \quad \text{and} \quad \frac{v(a_d)}{d} = -\frac{d+1}{d}.$$

Therefore $\frac{v(a_{d-1})}{d-1} < \frac{v(a_{d-2})}{d-2}$ and $\frac{v(a_{d-1})}{d-1} < \frac{v(a_d)}{d}$, so we may take $s = d-1$, and since $sv(a_d) - dv(a_s) = 1$, we conclude by Theorem 3 that $F$ is either irreducible in $K[X, Y]$, or has a factor whose degree with respect to $Y$ is a multiple of $d-1$, that is $F$ is either irreducible, or has a linear factor in $Y$.

## CONCLUSIONS

We have obtained a refinement of a theorem of B. Beauzamy about the size of polynomial divisors. We have also obtained new irreducibility criteria based on the study of Newton's polygon.

## REFERENCES


1. E. Beauzamy, P. Bombieri, and H. Enflo, "Montgomery: Products of polynomials in many variables," J. Number Theory **36**, 219–245 (1990).
2. B. Beauzamy, "Products of polynomials and a priori estimates for coefficients in polynomial decompositions: A sharp result," J. Symb. Comput. **13**, 463–472 (1992).
3. S. Bhatia and S. K. Khanduja, "Difference polynomials and their generalizations," Mathematika **48**, 293–299 (2001).
4. A. Bishnoi, S. K. Khanduja, and K. Sudesh, "Some extensions and applications of the Eisenstein irreducibility criterion," Dev. Math. **18**, 189–197 (2010).
5. N. C. Bonciocat, "On an irreducibility criterion of Perron for multivariate polynomials," Bull. Math. Soc. Sci. Math. Roum. **53** (101), 213–217 (2010).
6. N. C. Bonciocat, "Schönemann–Eisenstein–Dumas-type irreducibility conditions that use arbitrarily many prime numbers," Commun. Algebra **43**, 3102–3122 (2015).
7. N. C. Bonciocat, Y. Bugeaud, M. Cipu, and M. Mignotte, "Irreducibility criteria for sums of two relatively prime polynomials," Int. J. Number Theory **9**, 1529–1539 (2013).
8. G. Dumas, "Sur quelques cas d'irréducibilité des polynômes à coefficients rationnels," J. Math. Pures Appl. **12**, 191–258 (1906).
9. G. Eisenstein, "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).
10. M. Mignotte, "An inequality on the greatest roots of a polynomial," Elem. Math. **46**, 86–87 (1991).
11. M. Mignotte and P. Glesser, "On the smallest divisor of a polynomial," J. Symb. Comput. **17**, 277–282 (1994).
12. M. Mignotte, D. Ştefănescu, *Polynomials—An Algorithmic Approach* (Springer-Verlag, 1999).
13. M. Mignotte and D. Ştefănescu, "La première mèthode gènèrale de factorisation des polynômes: Autour d'un mḿoire de F. T. Schubert," Rev. d'Hist. Math. **7**, 101–123 (2001).
14. L. Panaitopol and D. Ştefănescu, "On the generalized difference polynomials," Pac. J. Math. **143**, 341–348 (1990).
15. T. Schönemann, "Von denjenigen Moduln, welche Potenzen von Primzahlen sind," J. Reine Angew. Math. **32**, 93–105 (1846).
16. D. Ştefănescu, "Applications of the Newton index to the construction of irreducible polynomials," in *CASC'2014, Lecture Notes in Computer Science*, Ed. by V. Gerdt, W. Koepf, W. Mayr, and E. Vorozhtsov (Springer, Berlin, 2014), Vol. 8660, pp. 460–471.
17. P. S. Wang, "Parallel univariate polynomial factorization on shared–memory multiprocessors," *Proceedings of ISSAC'90* (1990), pp. 145–151.
18. S. H. Weintraub, "A mild generalization of Eisenstein's criterion, Proc. Am. Math. Soc. **141**, 1159–1160 (2013).