NORTH-HOLLAND

An Elementary Proof of Barnett's Theorem About the Greatest Common Divisor of Several Univariate Polynomials

Laureano González-Vega*
Departamento de Matemáticas, Estadística y Computación
Facultad de Ciencias
Universidad de Cantabria
Santander, Spain

ABSTRACT

This articule provides a new proof of Barnett's theorem giving the degree of the greatest common divisor of several univariate polynomials with coefficients in a field in terms of the rank of a well-defined matrix. The new proof is elementary and self-contained (no use of Jordan form or invariant factors), and it is based on some easy to state properties of subresultants. Moreover this proof allows one to generalize Barnett's results to the case when the considered polynomials have their coefficients in an integral domain.

1. INTRODUCTION

Let $\mathbb{F}$ be a field, and $\{A(x), B_1(x), \ldots, B_t(x)\}$ a family of polynomials in $\mathbb{F}[x]$ with $A(x)$ monic and $n = \deg A(x) > \deg B_j(x)$ for every $j \in \{1, \ldots, t\}$. Barnett's theorem (see [1] or [2]) assures that the degree of the greatest common divisor of $A(x), B_1(x), \ldots, B_t(x)$ verifies

$$\deg \gcd(A(x), B_1(x), \ldots, B_t(x))$$

$$= n - \operatorname{rank}(B_1(\Delta_A), B_2(\Delta_A), \ldots, B_t(\Delta_A)),$$

* Partially supported by CICyT PB 92/0498/C02/01, Esprit/Bra 6846 (PoSSo) and Caja Cantabria. E-mail: gvega@matsuml.unican.es.

LINEAR ALGEBRA AND ITS APPLICATIONS 247:185–202 (1996)

655 Avenue of the Americas, New York, NY 10010
0024-3795/96/$15.00
SSDI 0024-3795(95)00099-D

where Δ_A is the companion matrix for A:

$$\Delta_A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & \cdots & 0 & -a_{n-2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix},$$

and $B_j(\Delta_A)$ denotes the evaluation of the polynomial $B_j(x)$ in the matrix Δ_A. Moreover, some linear algebra on the matrix giving the degree of the greatest common divisor provides the coefficients of a greatest common divisor in $\mathbb{F}[x]$ for the polynomials $A(x), B_1(x), \ldots, B_t(x)$.

Two proofs are presented in [2] for the result concerning the degree of the greatest common divisor: the first one used the Jordan form of Δ_A, and the second one is based on a theorem introduced in [3] concerning the degree of the greatest common divisor of two invariant factors for two regular polynomial matrices. This paper is devoted to present a new proof of Barnett's theorem which is more elementary than the proofs in [2] in that it is self-contained and is based on a few elementary facts in linear algebra and some easy to prove properties concerning polynomial determinants and subresultants. Moreover our proof allows us to generalize Barnett's results to the case where the considered polynomials have their coefficients in an integral domain.

The paper is divided in three parts. The first one is devoted to presenting the concepts of polynomial determinant and subresultant and their relation with the Euclidean remainders of two polynomials. The second one introduces the new proof of Barnett's theorem (considering polynomials with coefficients in an integral domain) using only some elementary facts in linear algebra together with a result presented in the previous section relating subresultants and Euclidean remainders. Finally, the last section shows how the technique introduced to prove Barnett's theorem can be also used to get the greatest common divisor of the considered polynomials as presented in [2].

2. POLYNOMIAL DETERMINANTS, SUBRESULTANTS, AND EUCLIDEAN REMAINDERS

Let $\mathbb{D}$ be an integral domain. The concept of polynomial determinant associated to a matrix with entries in $\mathbb{D}$ provides one of the ways to define subresultants.

DEFINITION 2.1. Let Δ be an $m \times n$ matrix with $m \leqslant n$. The determinant polynomial of Δ, **detpol**(Δ), is defined as

$$\mathbf{detpol}(\Delta) = \sum_{k=0}^{n-m} (\det \Delta_k)\, x^{n-m-k},$$

where Δ_k is the square submatrix of Δ consisting of the first $m-1$ columns and the $(k+m)$th column.

If the matrix Δ is square, then **detpol**(Δ) = det Δ. The coefficients of the usual matrices whose **detpol** is going to be computed will be the coefficients of some polynomials. This motivates the following definition, whose first part generalizes the usual definition of Sylvester matrix.

DEFINITION 2.2. Let A, B be polynomials in $\mathbb{D}[x]$, and $p, q \in \mathbb{N}$ with deg $A \leqslant p$ and deg $B \leqslant q$:

$$A = \sum_{k=0}^{p} a_k x^{p-k}, \qquad B = \sum_{k=0}^{q} b_k x^{q-k}.$$

If $i \in \{0, \ldots, \inf(p, q) - 1\}$, then the Sylvester matrix of index i associated to A, p, B, and q is

$$\mathbf{Sylv}_i(A, p, B, q) = \overbrace{\begin{pmatrix} a_0 & \cdots & a_p & & \\ & \ddots & & \ddots & \\ & & a_0 & \cdots & a_p \\ b_0 & \cdots & b_q & & \\ & \ddots & & \ddots & \\ & & b_0 & \cdots & b_q \end{pmatrix}}^{p+q-i} \begin{matrix} \\ \\ q-i \\ \\ p-i \\ \\ \end{matrix}$$

In these conditions the subresultant polynomial of index i is defined as

$$\mathbf{Sres}_i(A, p, B, q) = \mathbf{detpol}(\mathbf{Sylv}_i(A, p, B, q)).$$

It is a general fact that the subresultant polynomials associated to A and B are very close to the polynomials appearing in the sequence of Euclidean

remainders associated to A and B. We only shall be involved with a particular case of this property, and the general case can be found in [11] or [13]. The next notion to be introduced is the pseudoremainder of two polynomials.

DEFINITION 2.3. Let A, B be polynomials in $\mathbb{D}[x]$ with respective degrees p and q. The pseudoremainder of A and B is defined as

$$\operatorname{Prem}(A, B) = \begin{cases} \operatorname{Rem}\left(\operatorname{lcof}(B)^{p-q+1} A, B\right) & \text{if } p \geqslant q, \\ A & \text{otherwise,} \end{cases}$$

where Rem denotes the Euclidean remainder.

It is clear, in the conditions of the previous definition, that if $p \geqslant q$ then

$$\operatorname{Prem}(A, B) = \operatorname{lcof}(B)^{p-q+1} \operatorname{Rem}(A, B).$$

The only needed fact about the connection between polynomial determinants and Euclidean remainders is the following proposition. More details about this connection between Euclidean remainders and determinants can be found in [9].

PROPOSITION 2.4. *Let A, U be polynomials in $\mathbb{D}[x]$ with respective degrees n, γ with $\gamma \leqslant n-1$ and $a_0 = \operatorname{lcof}(A)$. For every polynomial $T \in \mathbb{D}[x]$ with degree k the following equalities hold:*

$$\begin{aligned} \mathbf{Sres}_{n-1}(TU, n+k-1, A, n) &= (-1)^k a_0^k \operatorname{Rem}(TU, A) \\ &= (-1)^k a_0^{n-\gamma-1} \operatorname{Prem}(TU, A) \end{aligned}$$

Proof. It is enough to remark that the steps in the algorithm computing the Euclidean remainder of TU and A carry the matrices whose determinants are going to be computed to a diagonal form (for more details see [11]). ∎

3. THE NEW PROOF OF BARNETT'S THEOREM

Let $\mathbb{D}$ be an integral domain and $\mathbb{F}$ its quotient field.

DEFINITION 3.1. Let $A(x)$ be the following polynomial in $\mathbb{D}[x]$:

$$A(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

with $a_0 \neq 0$. The generalized companion matrix associated to $A(x)$ is defined as:

$$\Delta_A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n \\ a_0 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & a_0 & \cdots & 0 & -a_{n-2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & a_0 & -a_1 \end{pmatrix}.$$

The next proposition introduces the formula to compute the degree of the greatest common divisor of two polynomials in $\mathbb{D}[x]$ that will be generalized to an arbitrary number of polynomials.

PROPOSITION 3.2. *Let A and B be polynomials in* $\mathbb{D}[x]$:

$$A(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n, \qquad B(x) = b_1 x^{n-1} + \cdots + b_{n-1} x + b_n$$

with $a_0 \neq 0$ *and* $\deg B(x) \leqslant n - 1$. *Defining*

$$\tilde{B}(x) = a_0^{\deg B} B\left(\frac{x}{a_0}\right),$$

then

$$\deg \gcd(A(x), B(x)) = n - \operatorname{rank} \tilde{B}(\Delta_A),$$

where Δ_A *is the generalized companion matrix associated to* $A(x)$.

Proof. Let $\mathbb{F}_n[x]$ be the $\mathbb{F}$-vectorial space of polynomials with degree strictly smaller than n. Identifying every polynomial in $\mathbb{F}_n[x]$ with the vector of its coefficients:

$$U(x) = u_1 x^{n-1} + \cdots + u_n \leftrightarrow \begin{pmatrix} u_n \\ \vdots \\ u_1 \end{pmatrix},$$

the matrix Δ_A will be regarded as the matrix associated to the linear mapping

$$\Delta_A : \mathbb{F}_n[x] \to \mathbb{F}_n[x],$$
$$U(x) \mapsto \Delta_A \cdot U(x).$$

An easy computation gives the following expression for the linear mapping Δ_A:

$$\Delta_A \cdot U(x) = a_0 x U(x) - u_1 A(x),$$

providing the basic fact needed to prove for every $k \geqslant 0$ the following equality:

$$\Delta_A^k \cdot U(x) = (-1)^k \mathbf{detpol}\left(\begin{matrix} u_1 & u_2 & \cdots & u_n & \overbrace{\qquad\qquad}^{k} & \\ a_0 & a_1 & \cdots & a_{n-1} & a_n & \\ & \ddots & \ddots & & \ddots & \ddots \\ & & a_0 & a_1 & \cdots & a_{n-1} \quad a_n \end{matrix}\right)\Bigg\}k$$

$$= (-1)^k \mathbf{Sres}_{n-1}(x^k U(x),\ n + k - 1,\ 4(x),\ n)$$

$$\overset{2.4}{=} a_0^k \mathrm{Rem}(x^k U(x),\ A(x)).$$

Using this equality the polynomial meaning of the linear mapping $\tilde{B}(\Delta_A)$ ($\gamma = \deg B$) can be derived:

$$\begin{aligned} \tilde{B}(\Delta_A) \cdot U(x) &= \sum_{k=0}^{\gamma} b_{\gamma-k} a_0^{\gamma-k} \Delta_A^k \cdot U(x) \\ &= \sum_{k=0}^{\gamma} b_{\gamma-k} a_0^{\gamma-k} a_0^k \,\mathrm{Rem}(x^k U(x),\ A(x)) \\ &= a_0^{\gamma} \sum_{k=0}^{\gamma} b_{\gamma-k} \,\mathrm{Rem}(x^k U(x),\ A(x)) \\ &= a_0^{\gamma} \,\mathrm{Rem}\left(\sum_{k=0}^{\gamma} b_{\gamma-k} x^k U(x),\ A(x)\right) \\ &= a_0^{\gamma} \,\mathrm{Rem}(B(x)U(x),\ A(x)). \end{aligned}$$

If $D(x) \in \mathbb{F}_n[x]$ is the greatest common divisor of $A(x)$ and $B(x)$ with $\deg D(x) = k$, then the set in $\mathbb{F}_n[x]$ defined by

$$\mathscr{P} = \{F(x) \in \mathbb{F}_n[x] : D(x) \mid F(x)\}$$

is a subspace in $\mathbb{F}_n[x]$ with $\dim_{\mathbb{F}}(\mathscr{P}) = n - k$. The proof of the proposition is finished by showing that the subspace $\mathscr{P}$ if precisely the image of $\tilde{B}(\Delta_A)$: $\mathrm{Im}(\tilde{B}(\Delta_A))$.

The formula obtained for the linear mapping $\tilde{B}(\Delta_A)$

$$\tilde{B}(\Delta_A) \cdot U(x) = a_0^{\gamma} \operatorname{Rem}(B(x)U(x), A(x)),$$

gives immediately that $\mathrm{Im}(\tilde{B}(\Delta_A)) \subseteq \mathscr{P}$.

Let $H(x)$ be a polynomial in $\mathscr{P}$, and $G(x) = H(x)/D(x)$. As $D(x)$ is the greatest common divisor of $A(x)$ and $B(x)$, then there exist $\alpha(x)$ and $\beta(x)$ in $\mathbb{F}[x]$ verifying

$$D(x) = \alpha(x)A(x) + \beta(x)B(x).$$

Defining $W(x) = \beta(x)G(x)$ and multiplying the last equality by $G(x)$, we obtain [note that $\deg H(x) < n$]

$$H(x) = \operatorname{Rem}(B(x)W(x), A(x)).$$

Clearly the $U(x)$ looked for must be defined as

$$U(x) = \frac{\operatorname{Rem}(W(x), A(x))}{a_0^{\gamma}} \in \mathbb{F}_n[x],$$

whence

$$\tilde{B}(\Delta_A) \cdot U(x) = H(x).$$

This allows us to conclude that $\mathrm{Im}(\tilde{B}(\Delta_A)) = \mathscr{P}$ and

$$n - k = \dim_{\mathbb{F}} \mathscr{P} = \dim_{\mathbb{F}} \mathrm{Im}\left(\tilde{B}(\Delta_A)\right) = \operatorname{rank} \tilde{B}(\Delta_A),$$

whence

$$\deg \gcd(A(x), B(x)) = n - \operatorname{rank} \tilde{B}(\Delta_A),$$

as desired. ■

A proof of Proposition 3.2 for the monic case can be found in [16] following similar lines to the ones used here. Also, References [16] and [5] contain the proof that the determinant of the matrix $\tilde{B}(\Delta_A)$ agrees with the

resultant of A and B (in the monic case). The first proof of this proposition seems to be the one appearing in [15], and other proofs can be found in [1], [2], [4], and [12] using some properties of invariant factors.

The proof of the theorem for the general case will depend on the following two lemmas. The first one provides a useful interpretation for the sum of the kernels of a finite number of linear mappings defined by means of polynomials evaluated in the same matrix.

LEMMA 3.3. *Let $B_1(x), \ldots, B_t(x)$ be arbitrary nonzero polynomials in $\mathbb{F}[x]$, and $B(x)$ their least common multiple. Then for any square matrix Δ over $\mathbb{F}$,*

$$\ker B(\Delta) = \sum_{i=1}^{t} \ker B_i(\Delta).$$

Proof. It is straightforward. See [14, Theorem 6.1.1].

The second lemma gives an expression concerning the degree of the greatest common divisor of a finite family of polynomials in $\mathbb{D}[x]$.

LEMMA 3.4. *Let $A(x), B_1(x), \ldots, B_t(x)$ be arbitrary nonzero polynomials in $\mathbb{D}[x]$. Denoting $\mathscr{B} = \{B_1(x), \ldots, B_t(x)\}$, then*

$$\deg \gcd(A, B_1, \ldots, B_t) = (-1)^{t+1} \deg \gcd(A, \operatorname{lcm}(\mathscr{B})) + (-1)^t \sum_{k=1}^{t-1} (-1)^{k+1} \sum_{L \in \binom{\mathscr{B}}{k}} \deg \gcd(A, L),$$

where $\binom{\mathscr{B}}{k}$ denotes the family of subsets in $\mathscr{B}$ and k elements, and lcm *the least common multiple.*

Proof. In order to avoid an exponential growth in the number of superscripts and subscripts, the proof is sketched only for the case $t = 3$. The general case is treated exactly in the same way.

Let $\alpha_1(x), \ldots, \alpha_m(x)$ be the irreducible factors appearing in the factorization in $\mathbb{F}[x]$ for the polynomials $A(x)$, $B_1(x)$, $B_2(x)$, and $B_3(x)$:

$$A(x) = \alpha_1^{\epsilon_1} \cdots \alpha_m^{\epsilon_m}, \quad B_1(x) = \alpha_1^{\delta_1} \cdots \alpha_m^{\delta_m}, \qquad \epsilon_i \geqslant 0, \quad \delta_i \geqslant 0,$$

$$B_2(x) = \alpha_1^{\tau_1} \cdots \alpha_m^{\tau_m}, \quad B_3(x) = \alpha_1^{\sigma_1} \cdots \alpha_m^{\sigma_m}, \qquad \tau_i \geqslant 0, \quad \sigma_i \geqslant 0.$$

This allows us to express the degrees of the polynomials appearing in the formula in terms of the nonnegative integers ϵ_i, δ_i, τ_i, and σ_i in the following way:

$$\deg \gcd(A, B_1, B_2, B_3) = \sum_{i=1}^{m} \min(\epsilon_i, \delta_i, \tau_i, \sigma_i),$$

$$\deg \gcd(A, B_1) = \sum_{i=1}^{m} \min(\epsilon_i, \delta_i),$$

$$\deg \gcd(A, B_2) = \sum_{i=1}^{m} \min(\epsilon_i, \tau_i),$$

$$\deg \gcd(A, B_3) = \sum_{i=1}^{m} \min(\epsilon_i, \sigma_i),$$

$$\deg \gcd(A, B_1, B_2) = \sum_{i=1}^{m} \min(\epsilon_i, \delta_i, \tau_i),$$

$$\deg \gcd(A, B_1, B_3) = \sum_{i=1}^{m} \min(\epsilon_i, \delta_i, \sigma_i),$$

$$\deg \gcd(A, B_2, B_3) = \sum_{i=1}^{m} \min(\epsilon_i, \tau_i, \sigma_i),$$

$$\deg \gcd(A, \operatorname{lcm}(B_1, B_2, B_3)) = \sum_{i=1}^{m} \min(\epsilon_i, \max(\delta_i, \tau_i, \sigma_i)).$$

As for arbitrary ϵ, δ, τ, and σ the equality

$$\begin{aligned}\min(\epsilon, \delta, \tau, \sigma) = &-\min(\epsilon, \delta) - \min(\epsilon, \tau) - \min(\epsilon, \sigma) \\ &+ \min(\epsilon, \delta, \tau) + \min(\epsilon, \delta, \sigma) + \min(\epsilon, \tau, \sigma) \\ &+ \min(\epsilon, \max(\delta, \tau, \sigma))\end{aligned}$$

is always true, this gives directly the proof for the lemma when $t = 3$.

Finally, the next theorem provides the proof of Barnett's theorem for a finite family of polynomials in $\mathbb{D}[x]$.

THEOREM 3.5 (BARNETT'S THEOREM). *Let us consider the following polynomials in* $\mathbb{D}[x]$:

$$A(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n,$$

$$B_j(x) = b_{j,1} x^{n-1} + \cdots + b_{j,n-1} x + b_{j,n}, j \in \{1, \ldots, t\},$$

with $a_0 \neq 0$ *and* $\deg B_j(x) \leqslant n - 1$ *for every* j *in* $\{1, \ldots, t\}$. *Defining for every* j *in* $\{1, \ldots, t\}$ *the polynomial in* $\mathbb{D}[x]$

$$\tilde{B}_j(x) = a_0^{\deg B_j} B_j\left(\frac{x}{a_0}\right),$$

then the degree of the greatest common divisor of $A(x), B_1(x), \ldots, B_t(x)$ *can be computed by means of the following formula*:

$$\deg \gcd(A(x), B_1(x), \ldots, B_t(x)) = n - \operatorname{rank} \mathscr{B}_A(B_1, \ldots, B_t),$$

where

$$\mathscr{B}_A(B_1, \ldots, B_t) = \begin{pmatrix} \tilde{B}_1(\Delta_A) \\ \tilde{B}_2(\Delta_A) \\ \vdots \\ \tilde{B}_t(\Delta_A) \end{pmatrix}$$

with Δ_A *the generalized companion matrix associated to* $A(x)$.

Proof. The theorem will be proved by induction on t. Proposition 3.2 gives the proof of the theorem when $t = 1$, and it will be assumed the result is true for every set of polynomials with cardinality strictly smaller then t.

For every $k \in \{1, \ldots, t\}$, let Φ_k be the linear mapping induced by the matrix $\tilde{B}_k(\Delta_A)$:

$$\Phi_k : \mathbb{F}_n[x] \to \mathbb{F}_n[x],$$

$$U(x) \mapsto \tilde{B}_k(\Delta_A) \cdot U(x).$$

Next we consider the linear mapping

$$\Phi = \bigoplus_{j=1}^{t} \Phi_j : \mathbb{F}_n[x] \to \mathbb{F}_n[x] \times \overset{t}{\cdots} \times \mathbb{F}_n[x],$$

$$U(x) \mapsto \begin{pmatrix} \Phi_1(U(x)) \\ \vdots \\ \Phi_t(U(x)) \end{pmatrix},$$

whose matrix with respect to the basis for $\mathbb{F}_n[x]$ provided by the powers of x is

$$\mathcal{M}(\Phi) = \mathcal{B}_A(B_1, \ldots, B_t)$$

and whose kernel is the intersection of the $\ker \Phi_k$'s. The inductive hypothesis can be rewritten in terms of the linear mappings Φ_j in the following way:

$$\forall L \subset \{1, \ldots, t\} \qquad \deg \gcd\big(A, \{B_j : j \in L\}\big)$$

$$= n - \dim_{\mathbb{F}} \operatorname{Im}\Big(\bigoplus_{j \in L} \Phi_j\Big) = \dim_{\mathbb{F}} \bigcap_{j \in L} \ker \Phi_j.$$

Defining $\mathcal{B} = \{B_1, \ldots, B_t\}$, $\tilde{\mathcal{B}} = \{\tilde{B}_1, \ldots, \tilde{B}_t\}$, R as the least common multiple of the polynomials in $\mathcal{B}$, and $[t-1] = \{1, \ldots, t-1\}$, the combination of the previous results allows us to obtain

$$n - \operatorname{rank} \mathcal{M}(\Phi) = \dim_{\mathbb{F}} \ker \Phi = \dim_{\mathbb{F}} \bigcap_{k=1}^{t} \ker \Phi_k$$

$$= (-1)^{t+1} \dim_{\mathbb{F}} \sum_{k=1}^{t} \ker \Phi_k$$

$$+ (-1)^t \sum_{k=1}^{t-1} (-1)^{k+1} \sum_{L \subseteq \binom{[t-1]}{k}} \dim_{\mathbb{F}} \bigcap_{j \in L} \ker \Phi_j$$

$$\overset{3.3}{=} (-1)^{t+1} \dim_{\mathbb{F}} \ker \operatorname{lcm}(\tilde{\mathcal{B}})(\Delta_A)$$

$$+ (-1)^t \sum_{k=1}^{t-1} (-1)^{k+1} \sum_{L \subseteq \binom{[t-1]}{k}} \dim_{\mathbb{F}} \bigcap_{j \in L} \ker \Phi_j$$

$$= (-1)^{t+1} \dim_{\mathbb{F}} \ker \tilde{R}(\Delta_A)$$

$$+ (-1)^t \sum_{k=1}^{t-1} (-1)^{k+1} \sum_{L \subseteq \binom{[t-1]}{k}} \dim_{\mathbb{F}} \bigcap_{j \in L} \ker \Phi_j$$

$$\overset{3.2}{=} (-1)^{t+1} \deg \gcd(A, \operatorname{lcm}(\mathscr{B}))$$

$$+ (-1)^t \sum_{k=1}^{t-1} (-1)^{k+1} \sum_{L \subseteq \binom{[t-1]}{k}} \dim_{\mathbb{F}} \bigcap_{j \in L} \ker \Phi_j$$

$$= (-1)^{t+1} \deg \gcd(A, \operatorname{lcm}(\mathscr{B}))$$

$$+ (-1)^t \sum_{k=1}^{t-1} (-1)^{k+1} \sum_{L \subseteq \binom{[t-1]}{k}} \deg \gcd\big(A, \{B_j : j \in L\}\big)$$

$$\overset{3.4}{=} \deg \gcd(A, B_1, \ldots, B_t),$$

which is the desired formula.

In the monic case, the relationship of the matrix $\mathscr{B}_A(B_1, \ldots, B_t)$ with a generalized resultant for more than two polynomials is in [6].

4. THE COMPUTATION OF THE GREATEST COMMON DIVISOR OF SEVERAL UNIVARIATE POLYNOMIALS

In this section, we study how to compute the coefficients of a greatest common divisor of the polynomials $A(x), B_1(x), \ldots, B_t(x)$ in $\mathbb{D}[x]$ with $\mathbb{D}$ an integral domain, using the matrix $\mathscr{B}_A(B_1, \ldots, B_t)$ defined in Theorem 3.5. The first proposition provides information about the linearly independent columns in such a matrix. Again the difference from the proofs in [1], [2], [7], and [8] is the use of Euclidean remainders and subresultants.

PROPOSITION 4.1. *Let us consider the following polynomials in* $\mathbb{D}[x]$:

$$A(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n,$$

$$B_j(x) = b_{j,1} x^{n-1} + \cdots + b_{j,n-1} x + b_{j,n}, \quad j \in \{1, \ldots, t\},$$

with $a_0 \neq 0$ *and* $\deg B_j(x) \leqslant n-1$ *for every* j *in* $\{1, \ldots, t\}$. *Let* k *be the degree of the greatest common divisor for the polynomials* $A(x), B_1(x), \ldots, B_t(x)$, *and* $\rho_1, \ldots, \rho_n$ *the columns of the matrix* $\mathscr{B}_A(B_1, \ldots, B_t)$. *Then the columns* $\rho_1, \ldots, \rho_{n-k}$ *are linearly independent and every* ρ_j *with* $j > n-k$ *can be expressed as a linear combination of* $\rho_1, \ldots, \rho_{n-k}$.

Proof. Let $D(x)$ be a greatest common divisor for $A(x)$, $B_1(x)$, $\ldots, B_t(x)$ in $\mathbb{D}[x]$:

$$D(x) = d_0 x^k + \cdots + d_{k-1}x + d_k, \qquad d_0 \neq 0.$$

In the proof of Proposition 3.2 was given a polynomial description of the matrix Δ_A^j in terms of several well-defined Euclidean remainders:

$$\Delta_A^j \cdot U(x) = a_0^j \operatorname{Rem}\big(x^j U(x),\, A(x)\big).$$

This implies directly that

$$\tilde{D}(x) = a_0^k D\left(\frac{x}{a_0}\right) \quad \Rightarrow \quad \tilde{D}(\Delta_A) \cdot U(x) = a_0^k \operatorname{Rem}\big(D(x)U(x),\, A(x)\big).$$

Applying this last formula over the polynomials $1, x, \ldots, x^{n-k-1}$, we obtain for the matrix $\tilde{D}(\Delta_A)$ the following structure:

$$\tilde{D}(\Delta_A) = a_0^k \begin{pmatrix} 1 & x & & & x^{n-k} & & x^n \\ d_k & & & & \bullet & \cdots & \bullet \\ d_{k-1} & d_k & & & \bullet & \cdots & \bullet \\ \vdots & \vdots & \ddots & & \vdots & & \vdots \\ d_0 & d_1 & & d_k & \bullet & \cdots & \bullet \\ & d_0 & & d_{k-1} & \bullet & \cdots & \bullet \\ & & \ddots & \vdots & \vdots & & \vdots \\ & & & d_0 & \bullet & \cdots & \bullet \end{pmatrix} \begin{matrix} 1 \\ x \\ \\ \\ \\ \\ x^n \end{matrix} \qquad (*)$$

Moreover, using Proposition 3.2, we have

$$n - \operatorname{rank} \tilde{D}(\Delta_A) = \deg \gcd(A(x), D(x)) = \deg D(x) = k,$$

whence

$$\operatorname{rank} \tilde{D}(\Delta_A) = n - k,$$

and denoting by $\sigma_1, \ldots, \sigma_n$ the columns in $\tilde{D}(\Delta_A)$, the last equality and the structure of $\tilde{D}(\Delta_A)$ allow us to conclude that the vectors $\sigma_1, \ldots, \sigma_{n-k}$ are linearly independent and every σ_i with $n - k + 1 \leqslant i \leqslant n$ can be expressed as a linear combination of the $\sigma_1, \ldots, \sigma_{n-k}$.

Next we consider for every j in $\{1, \ldots, t\}$ the polynomial $\beta_j(x)$ in $\mathbb{F}[x]$ verifying

$$B_j(x) = \beta_j(x) D(x) \quad \text{and thus} \quad \tilde{B}_j(x) = \tilde{\beta}_j(x) \tilde{D}(x).$$

The evaluation in Δ_A of these polynomial expressions provides the following equality:

$$\begin{pmatrix} \tilde{B}_1(\Delta_A) \\ \vdots \\ \tilde{B}_t(\Delta_A) \end{pmatrix} = \begin{pmatrix} \tilde{\beta}_1(\Delta_A) \\ \vdots \\ \tilde{\beta}_t(\Delta_A) \end{pmatrix} \cdot \tilde{D}(\Delta_A),$$

whence

$$\forall i \in \{1, \ldots, n\} \qquad \rho_i = \begin{pmatrix} \tilde{\beta}_1(\Delta_A) \\ \vdots \\ \tilde{\beta}_t(\Delta_A) \end{pmatrix} \cdot \sigma_i. \qquad (**)$$

The definition of the polynomials $\beta_i(x)$ implies that

$$\gcd(A(x), \beta_1(x), \ldots, \beta_t(x)) = 1,$$

and, applying Theorem 3.5, it is obtained that

$$\operatorname{rank} \begin{pmatrix} \tilde{\beta}_1(\Delta_A) \\ \vdots \\ \tilde{\beta}_t(\Delta_A) \end{pmatrix} = n. \qquad (***)$$

The equations in $(**)$ relating every ρ_i with σ_i, the full rank condition in $(***)$, and the fact that $\sigma_1, \ldots, \sigma_{n-k}$ are linearly independent allow us to conclude that $\rho_1, \ldots, \rho_{n-k}$ are also linearly independent. The fact that the rank of the matrix whose columns are the ρ_i's is equal to $n - k$ finishes the proof.

The next theorem shows how to use the columns of the matrix giving the degree of the greatest common divisor to obtain its coefficients.

THEOREM 4.2. *Let us consider the following polynomials in* $\mathbb{D}[x]$:

$$A(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n,$$
$$B_j(x) = b_{j,1} x^{n-1} + \cdots + b_{j,n-1} x + b_{j,n}, \quad j \in \{1, \ldots, t\},$$

with $a_0 \neq 0$ *and* $\deg B_j(x) \leqslant n - 1$ *for every* j *in* $\{1, \ldots, t\}$. *Let* $D(x)$ *be a greatest common divisor for the polynomials* $A(x), B_1(x), \ldots, B_t(x)$:

$$D(x) = d_0 x^k + d_1 x^{k-1} + \cdots + d_{k-1} x + d_k, \qquad d_0 \neq 0,$$

and $\rho_1, \ldots, \rho_n$ *the columns of the matrix* $\mathscr{B}_A(B_1, \ldots, B_t)$. *If for every* i *in* $\{1, \ldots, k\}$

$$\rho_{n-k+i} = \sum_{j=1}^{n-k} h_{i,j} \rho_j, \qquad h_{i,j} \in \mathbb{F},$$

then

$$a_0 \begin{pmatrix} d_0 \\ d_1 \\ d_2 \\ \vdots \\ d_k \end{pmatrix} = d_0 \begin{pmatrix} a_0 & & & & \\ a_1 & a_0 & & & \\ a_2 & a_1 & a_0 & & \\ \vdots & \vdots & \vdots & \ddots & \\ a_k & a_{k-1} & a_{k-2} & \cdots & a_0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ h_{1,n-k} \\ h_{2,n-k} \\ \vdots \\ h_{k,n-k} \end{pmatrix}.$$

Proof. Proposition 4.1 assures the existence of the scalars $h_{i,j}$ verifying the conditions imposed. Let us consider the matrix $\tilde{D}(\Delta_A)$ and its columns $\sigma_1, \ldots, \sigma_n$. The equalities

$$\forall i \in \{1, \ldots, n\} \qquad \rho_i = \begin{pmatrix} \tilde{\beta}_1(\Delta_A) \\ \vdots \\ \tilde{\beta}_t(\Delta_A) \end{pmatrix} \cdot \sigma_i \quad \text{with} \quad \operatorname{rank} \begin{pmatrix} \tilde{\beta}_1(\Delta_A) \\ \vdots \\ \tilde{\beta}_t(\Delta_A) \end{pmatrix} = n,$$

shown in the proof of Proposition 4.1, allow us to conclude

$$\sigma_{n-k+i} = \sum_{j=1}^{n-k} h_{i,j}\sigma_j \qquad \forall i \in \{1,\dots,k\}.$$

Moreover the structure of the matrix $\tilde{D}(\Delta_A)$ shown in the proof of Proposition 4.1 [see (*)] gives for every σ_j with $1 \leqslant j \leqslant n-k$ the following expression:

$$\sigma_j = \left(\overbrace{0,\dots,0}^{j-1}, a_0^k d_k, \dots, a_0^k d_0, \overbrace{0,\dots,0}^{n-k-j}\right).$$

Replacing this expression for σ_j in the equations relating every σ_{n-k+i} $(1 \leqslant i \leqslant k)$ with $\sigma_1, \dots, \sigma_{n-k}$, it is obtained that if z_i is the last coordinate of σ_{n-k+i}, then

$$z_i = a_0^k d_0 h_{i,n-k}, \qquad 1 \leqslant i \leqslant k.$$

As every σ_{n-k+i} is the expression, in the usual basis of $\mathbb{F}_n[x]$, of

$$\tilde{D}(\Delta_A) \cdot x^{n-k+i-1},$$

then z_i is the coefficient of x^{n-1} in that polynomial. But the use of the expression for $\tilde{D}(\Delta_A)$ derived in the proof of Proposition 3.2 together with Proposition 2.4 allows us to write

$$\begin{aligned}\tilde{D}(\Delta_A) \cdot x^{n-k+i-1} &= a_0^k \operatorname{Rem}\big(D(x)x^{n-k+i-1}, A(x)\big)\\ &\overset{2.4}{=} (-1)^k \mathbf{Sres}_{n-1}\big(D(x)x^{n-k+i-1}, n+k-1, A(x), n\big)\\ &= (-1)^i a_0^{k-i} \mathbf{Sres}_{n-1}\big(D(x)x^{i-1}, n+i-1, A(x), n\big)\end{aligned}$$

and to obtain the following expression for every z_i:

$$a_0^k d_0 h_{i,n-k} = z_i = (-1)^i a_0^{k-i} \begin{vmatrix} d_0 & \cdots & \cdots & d_{i-1} & d_i \\ a_0 & \cdots & \cdots & a_{i-1} & a_i \\ & \ddots & & \vdots & \vdots \\ & & \ddots & \vdots & \vdots \\ & & & a_0 & a_1 \end{vmatrix}, \quad 1 \leqslant i \leqslant k. \qquad (\triangle)$$

This equality is the key that will allow us to derive the looked-for matricial equality relating the d_i's with the $h_{i,n-k}$'s. The proof will be made by induction on i, and for the sake of simplicity we define $h_{0,n-k} = 1$. The equalities for d_0 and d_1 are clear from the definition of $h_{0,n-k}$ and ($\triangle$). Now it is assumed that the result has been proved for $d_0, \ldots, d_i$:

$$a_0 d_u = d_0 \sum_{v=0}^{u} a_v h_{u-v,n-k}. \qquad (\triangle\triangle)$$

Applying ($\triangle$) for $i+1$ and ($\triangle\triangle$) to every d_u ($0 \leqslant u \leqslant i$), we obtain

$$a_0^k d_0 h_{i+1,n-k}$$

$$= (-1)^{i+1} d_0 a_0^{k-i-2} \begin{vmatrix} a_0 h_{0,n-k} & \cdots & \cdots & \sum_{v=0}^{i} a_{i-v} h_{v,n-k} & d_{i+1} \\ a_0 & \cdots & \cdots & a_i & a_{i+1} \\ & \ddots & & \vdots & \vdots \\ & & \ddots & \vdots & \vdots \\ & & & a_0 & a_1 \end{vmatrix}$$

$$= (-1)^{i+1} d_0 a_0^{k-i-2} \begin{vmatrix} 0 & \cdots & \cdots & 0 & d_{i+1} - \sum_{v=0}^{i} a_{i-v+1} h_{v,n-k} \\ a_0 & \cdots & \cdots & a_i & a_{i+1} \\ & \ddots & & \vdots & \vdots \\ & & \ddots & \vdots & \vdots \\ & & & a_0 & a_1 \end{vmatrix}$$

$$= d_0 a_0^{k-1} \left(d_{i+1} - \sum_{v=0}^{i} a_{i-v+1} h_{v,n-k} \right),$$

giving directly

$$a_0 d_{i+1} = d_0 \sum_{v=0}^{i+1} a_v h_{i-v+1,n-k},$$

as desired. ■

Clearly the last theorem provides a method to determine the coefficients of the greatest common divisor once the $h_{i,n-k}$'s have been computed. The complexity of the algorithm presented in this section to compute the greatest common divisor of several univariate polynomials has been studied in [10].

REFERENCES

1 S. Barnett, *Polynomials and Linear Control Systems*, Marcel Dekker, New York, 1983.

2 S. Barnett, Greatest common divisor of several polynomials, *Proc. Cambridge Philos. Soc.* 70:263–268 (1971).

3 S. Barnett, Degrees of greatest common divisors of invariant factors of two regular polynomial matrices, *Proc. Cambridge Philos. Soc.* 66:241–245 (1970).

4 S. Barnett, Greatest common divisor of two polynomials, *Linear Algebra Appl.* 3:7–9 (1970).

5 S. Barnett, *Matrices in Control Theory*, Van Nostrand Reinhold, London, 1971.

6 S. Barnett, Greatest common divisors for generalized Sylvester resultant matrices, *Linear and Multilinear Algebra* 8:271–279 (1980).

7 S. Barnett, Division of generalized polynomials using the comrade matrix, *Linear Algebra Appl.* 60:159–175 (1984).

8 S. Barnett, *Matrices: Methods and Applications*, Oxford U.P. 1990.

9 S. Barnett, Euclidean remainders for generalized polynomials, *Linear Algebra Appl.* 99:111–122 (1988).

10 L. González-Vega, On the complexity of computing the greatest common divisor of several univariate polynomials, in Latin'95: Theoretical Informatics, Lecture Notes in Comput. Sci. 911, Springer-Verlag, 1995, pp. 332–345.

11 L. González-Vega, H. Lombardi, T. Recio, and M. F. Roy, Specialisation de la suite de Sturm et sous-resultants, *Inform. Theorique Appl.* 24(6):561–588 (1990).

12 R. E. Kalman, Some computational problems and methods related to invariant factors and control theory, in *Computational Problems in Abstract Algebra* (J. Leech, Ed.), Pergamon, 1970, pp. 393–398.

13 R. Loos, Generalized polynomial remainder sequences, in *Computer Algebra, Comnputing Supplementum* 4, Springer-Verlag, 1982, pp. 115–138.

14 P. Lancaster and M. Tismenetsky, *The Theory of Matrices*, Comput. Sci. Appl. Math., Academic, 1985.

15 C. C. MacDuffee, Some applications of matrices in the theory of equations, *Amer. Math. Monthly* 57:154–161 (1950).

16 M. Mignotte, *Mathematics for Computer Algebra*, Universitext, Springer-Verlag, 1992.

Received 26 August 1994; final manuscript accepted 20 January 1995