Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

ELA

A NEW PARALLEL POLYNOMIAL DIVISION BY A SEPARABLE POLYNOMIAL VIA HERMITE INTERPOLATION WITH APPLICATIONS*

ARISTIDES I. KECHRINIOTIS†, KONSTANTINOS K. DELIBASIS‡, CHRISTOS TSONOS§, AND NICHOLAS PETROPOULOS§

Abstract. A new parallel division of polynomials by a common separable divisor over a perfect field is presented and this is done by expressing the remainders as derivatives of a unique polynomial. In order to get this result, a novel variant expression of the classical Lagrange–Sylvester Hermite interpolating polynomial has been utilised, although any known variant may be used. The above findings are utilized to obtain a number of new identities involving polynomial derivatives, including a closed formula for the semi–simple part of the Jordan decomposition of a matrix.

Key words. Euclidean polynomial division, Hermite interpolation, Semisimple part of a matrix.

AMS subject classifications. 12Y05, 15A21, 11C08, 65F30.

1. Introduction.

The Hermite interpolation of total degree is described in the following theorem [1]:

THEOREM 1.1. *Given n distinct elements $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ in a perfect field $\mathbb{K}$, positive integers m_i, $i = 0, \ldots, n-1$, and $a_{ij} \in \mathbb{K}$ for $0 \le i \le n-1$, $0 \le j \le m_i - 1$, then there exists one and only one polynomial $r \in \mathbb{K}[x]$ of degree less than $\sum_{i=0}^{n-1} m_i$, such that*

$$r^{(j)}(\lambda_i) = a_{ij}, \quad 0 \le j \le m_i - 1,\ 0 \le i \le n-1\,. \tag{1.1}$$

This polynomial r is explicitly given by,

$$\begin{aligned} r(x) = \sum_{i=0}^{n-1} \sum_{j=0}^{m_i-1} \sum_{k=0}^{m_i-j-1} a_{ij} \frac{1}{j!} \frac{1}{k!} \left[\frac{(x-\lambda_i)^{m_i}}{\Omega(x)} \right]^{(k)}_{x=x_i} \\ \times \frac{\Omega(x)}{(x-\lambda_i)^{m_i-j-k}}\,, \end{aligned}$$

*Received by the editors on March 2, 2012. Accepted for publication on August 18, 2012. Handling Editor: Bryan L. Shader.

†Department of Informatics, Technological Educational Institute of Lamia, 35100 Lamia, Greece (kechrin@teilam.gr).

‡Department of Computer Science and Biomedical Informatics, University of Central Greece, Lamia 35100, Greece (kdelibasis@yahoo.com).

§Department of Electronics, Technological Educational Institute of Lamia, 35100 Lamia, Greece (tsonos@teilam.gr, nicholas@teilam.gr).

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

where

$$\Omega(x) = \prod_{i=0}^{n-1} (x-\lambda_i)^{m_i}\,,$$

and $r^{(k)}(a)$ *is the* $k-th$ *derivative of* r *at* a.

The applications of Hermite interpolation to numerical analysis are well known. A number of forms of the interpolating polynomial $r(x)$ have been reported in the literature, which require calculation of derivatives of rational polynomial functions (e.g., [1]), or recursive calculation of the coefficients a_{ij} of Theorem 1.1 (e.g., [8]). We propose a closed form expression of the interpolating polynomial r of the univariate Hermite interpolation which is a variation of the classical Lagrange–Sylvester formula, as presented in [11]. The expression in [11] involves less computational load than the proposed Hermite interpolating polynomial except in the special case of very small values of m_j.

We utilise the Hermite interpolating polynomial to show the main result of this work, the parallel polynomial division by a separable polynomial.

Let us note that the remainder $r \in \mathbb{K}[x]$ of the Euclidean division of any polynomial $P \in \mathbb{K}[x]$ of degree n by a separable polynomial $Q \in \mathbb{K}[x]$ of degree m, where $n \geq m$, can be calculated in closed form using the Langrange interpolation formula as following:

$$r(x) = \sum_{i=1}^{m} P(\lambda_i) \prod_{j=1 j\neq i}^{m} \frac{(x-\lambda_j)}{(\lambda_i - \lambda_j)}\,,$$

where $\lambda_1, \ldots, \lambda_m$ are the roots of Q in the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. In this work, we extend this simplified idea of polynomial remainder calculation by Langrange interpolation, to achieve a polynomial division by a common separable divisor, using the proposed closed form of the interpolating polynomial r of the univariate Hermite interpolation, although any expression of r may be utilized.

Furthermore, the above results will be used to obtain a number of new identities involving polynomial derivatives, as well as a closed form expression of the semisimple part of the Jordan decomposition of an algebraic element in an arbitrary algebra. These results however are independent from the selected expression of the Hermite interpolating polynomial.

The rest of the paper is organized as follows. In Section 2, we present a new closed form for Hermite interpolation. In Section 3, we present a new parallel division of polynomials by a common separable divisor over a perfect field, by expressing the remainders as derivatives of a unique polynomial. In Section 4, the main result

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

ELA

of Section 3 is applied to obtain a number of new identities involving polynomial derivatives, as well as a new closed form expression of the semisimple part of the Jordan decomposition of an algebraic element in an arbitrary algebra.

2. A new closed form for Hermite interpolation. Let $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ be distinct elements in a perfect field $\mathbb{K}$ and $m_0, m_1, \ldots, m_{n-1}$ be positive integers. Let us denote by L_k the polynomials given by

$$L_k(x) = \prod_{\substack{i=0 \\ i\neq k}}^{n-1} \frac{(x-\lambda_i)^{m_i}}{(\lambda_k - \lambda_i)^{m_i}} \in \mathbb{K}[x]\,. \tag{2.1}$$

Furthermore, we denote by Λ_k, $0 \le k \le n-1$, the $m_k \times m_k$ lower triangular matrices $[l_{ij}] \in \mathbb{K}^{m_k \times m_k}$, $0 \le i, j \le m_k - 1$, given by

$$l_{ij} := \begin{cases} \binom{i}{j} (L_k)^{(i-j)}(\lambda_k) & \text{if} \quad 0 \le j \le i \le m_k - 1 \\ 0 & \text{if} \quad 0 \le i < j \le m_k - 1 \end{cases},$$

where $(L_k)^{(i-j)}(\lambda_k)$ is the derivative of order $(i-j)$ of the polynomial $L_k(x)$ at λ_k. Thus, Λ_k has the following representation

$$\begin{bmatrix} \binom{0}{0} L_k(\lambda_k) & 0 & \cdots & 0 \\ \binom{1}{0} (L_k)^{(1)}(\lambda_k) & \binom{1}{1} L_k(\lambda_k) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m_k-1}{0} (L_k)^{(m_k-1)}(\lambda_k) & \binom{m_k-1}{1} (L_k)^{(m_k-2)}(\lambda_k) & \cdots & \binom{m_k-1}{m_k-1} L_k(\lambda_k) \end{bmatrix}. \tag{2.2}$$

For our purpose the following technical lemmas are required:

Lemma 2.1. *The matrices Λ_k, $0 \le k \le n-1$, are invertible with $\Lambda_k^{-1} = \sum_{i=0}^{m_k-1} (I_{m_k} - \Lambda_k)^i$, where I_{m_k} is the $m_k \times m_k$ unit matrix.*

Proof. Clearly, for $0 \le k \le n-1$ holds $L_k(\lambda_k) = 1$. Therefore, all matrices Λ_k, $0 \le k \le n-1$ are invertible and lower unitriangular. Thus, $(I_{m_k} - \Lambda_k)^{m_k} = 0$ and consequently $\Lambda_k \sum_{i=0}^{m_k-1} (I_{m_k} - \Lambda_k)^i = I_{m_k}$. ∎

Using Leibnitz's rule for derivatives, we easily get the following lemma:

Lemma 2.2. *For $0 \le i, s \le m_k - 1$ and $0 \le j, t \le n-1$, the following holds:*

$$\left(\frac{(x-\lambda_t)^s}{s!} L_t(x)\right)^{(i)} \Big|_{x=\lambda_j} = \begin{cases} 0 & \textit{if} \quad t \ne j \\ 0 & \textit{if} \quad t = j \textit{ and } i < s \\ \binom{i}{s} (L_j)^{(i-s)}(\lambda_j) & \textit{if} \quad t = j \textit{ and } s \le i \end{cases}. \tag{2.3}$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

ELA

Our proposed form of Hermite interpolation can now be presented in the following theorem.

THEOREM 2.3. *Given n distinct elements $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ in a perfect field $\mathbb{K}$, positive integers m_i, $i = 0, \ldots, n-1$, and $a_{ij} \in \mathbb{K}$ for $0 \le j \le n-1,\ 0 \le i \le m_j - 1$. Then there exists one and only one polynomial $r \in \mathbb{K}[x]$ of degree less than $\sum_{i=0}^{n-1} m_i$, such that*

$$r^{(i)}(\lambda_j) = a_{ij},\ \ 0 \le j \le n-1,\ 0 \le i \le m_j - 1. \tag{2.4}$$

This polynomial r is explicitly given by,

$$\begin{aligned} r &= \sum_{j=0}^{n-1} X_j \Lambda_j^{-1} A_j \qquad (2.5) \\ &= \sum_{j=0}^{n-1} \sum_{k=0}^{m_j-1} X_j (I_{m_j} - \Lambda_j)^k A_j, \end{aligned}$$

where the matrices X_j and A_j are given by

$$X_j = \left[\begin{array}{cccc} L_j(x) & \frac{(x-\lambda_j)}{1!} L_j(x) & \cdots & \frac{(x-\lambda_j)^{m_j-1}}{(m_j-1)!} L_j(x) \end{array}\right],$$

and

$$A_j = \left[\begin{array}{cccc} a_{0j} & a_{ij} & \cdots & a_{m_j-1j} \end{array}\right]^T.$$

Proof. It can be observed that (2.5) can be equivalently written in the following form:

$$r(x) = \sum_{j=0}^{n-1} \sum_{i=0}^{m_j-1} c_{ij} \frac{(x-\lambda_j)^i}{i!} L_j(x) \ \in\ \mathbb{K}[x]\,,$$

where

$$\begin{bmatrix} c_{0j} \\ c_{1j} \\ \vdots \\ c_{m_j-1j} \end{bmatrix} = \Lambda_j^{-1} \begin{bmatrix} a_{0j} \\ a_{1j} \\ \vdots \\ a_{m_j-1j} \end{bmatrix}, \quad 0 \le j \le n-1\,. \tag{2.6}$$

Now, by calculating the derivative of order i of the polynomial r at λ_j and using (2.3) in Lemma 2.2, we obtain

$$r^{(i)}(\lambda_j) = \sum_{k=0}^{i} c_{kj} \binom{i}{k} (L_j)^{(i-k)}(\lambda_j)\,, \tag{2.7}$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

for all $0 \leq j \leq n-1$, $0 \leq i \leq m-1$. Taking into consideration the definition of Λ_j in (2.2), the system of equations (2.7) can be rewritten in the following matrix form

$$\begin{bmatrix} r(\lambda_j) \\ r'(\lambda_j) \\ \vdots \\ r^{(m_j-1)}(\lambda_j) \end{bmatrix} = \Lambda_j \begin{bmatrix} c_{0j} \\ c_{1j} \\ \vdots \\ c_{m_j-1j} \end{bmatrix}, \quad 0 \leq j \leq n-1\,. \tag{2.8}$$

By substituting (2.6) in (2.8), we get

$$\begin{bmatrix} r(\lambda_j) \\ r'(\lambda_j) \\ \vdots \\ r^{(m_j-1)}(\lambda_j) \end{bmatrix} = \begin{bmatrix} a_{0j} \\ a_{1j} \\ \vdots \\ a_{m_j-1j} \end{bmatrix}.$$

Hence, we derive that $r^{(i)}(\lambda_j) = a_{ij}$, $0 \leq j \leq n-1, 0 \leq i \leq m_j - 1$. The second equality of (2.5) is obtained by Lemma 2.1.

Moreover, it can be easily confirmed that any polynomial $(x-\lambda_j)^i L_j(x)$, $0 \leq j \leq n-1$, $0 \leq i \leq m_j - 1$ has degree less than $\sum_{i=0}^{n-1} m_i$, and since r is a $\mathbb{K}$–linear combination of these polynomials, we conclude that the degree of r is less than $\sum_{i=0}^{n-1} m_i$. □

REMARK 2.4. The inversion of matrices Λ_j in Theorem 2.3 may be performed by any efficient numerical technique, replacing the last expression in (2.1).

3. Division of polynomials by a separable polynomial. At this point we are ready to present the following generalization of Euclidean polynomial division by a separable divisor, based on Theorem 2.3.

THEOREM 3.1. *Let $g \in \mathbb{K}[x]$ be a separable polynomial and $\lambda_0, \ldots, \lambda_{n-1}$ be the roots of g in the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. Then for any polynomials $f_0, f_1, \ldots, f_{m-1} \in \mathbb{K}[x]$, there exists unique $r \in \mathbb{K}[x]$ of degree less than mn and unique polynomials $q_0, q_1, \ldots, q_{m-1} \in \mathbb{K}[x]$ such that*

$$f_i = r^{(i)} + gq_i, \quad 0 \leq i \leq m-1\,.$$

This result is optimal, in the sense that if $m \geq 1$ and g is inseparable, then this result is not true. The polynomial r is given by

$$r(x) = \sum_{j=0}^{n-1} X_j \Lambda_j^{-1} A_j \in \mathbb{K}[x]\,,$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

where

$$X_j = \begin{bmatrix} L_j(x) & \frac{(x-\lambda_j)}{1!}L_j(x) & \cdots & \frac{(x-\lambda_j)^{m-1}}{(m-1)!}L_j(x) \end{bmatrix},$$
$$A_j = \begin{bmatrix} f_0(\lambda_j) & f_1(\lambda_j) & \cdots & f_{m-1}(\lambda_j) \end{bmatrix}^T$$

and L_j, Λ_j *are respectively as in (2.1), (2.2) by* $m_0 = m_1 = \cdots = m_{n-1} = m$.

Proof. Let k be the dimension of the field $\mathbb{K}(\lambda_0, \ldots, \lambda_{n-1})$ as vector space over $\mathbb{K}$, that is,

$$k = [\mathbb{K}(\lambda_0, \ldots, \lambda_{n-1}), \mathbb{K}]\,. \tag{3.1}$$

Then there exist $\tau_1, \ldots, \tau_{k-1}$ in $\mathbb{K}(\lambda_0, \ldots, \lambda_{n-1})$ such that $\{1, \tau_1, \ldots, \tau_{k-1}\}$ is a basis of $\mathbb{K}(\lambda_0, \ldots, \lambda_{n-1})$ as a vector space over $\mathbb{K}$.

Now, using Theorem 2.3 by $m_0 = m_1 = \cdots = m_{n-1} = m$, we have that there is unique polynomial $\widehat{r} \in \mathbb{K}(\lambda_0, \ldots, \lambda_{n-1})[x]$ given by (2.5) for $m_0 = m_1 = \cdots = m_{n-1} = m$ having degree less than mn such that

$$(\widehat{r})^{(i)}(\lambda_j) = f_i(\lambda_j)\,, \tag{3.2}$$

for all $0 \leq i \leq m-1, 0 \leq j \leq n-1$. Therefore, there exist polynomials $\widehat{q}_i \in \mathbb{K}(\lambda_0, \ldots, \lambda_{n-1})[x]$, $0 \leq i \leq m-1$, such that

$$\widehat{r}^{(i)} = f_i + g\widehat{q}_i\,. \tag{3.3}$$

Moreover, by (3.1) we have that the dimension of $\mathbb{K}(\lambda_0, \ldots, \lambda_{n-1})[x]$ as free module over $\mathbb{K}[x]$ is k and $\{1, \tau_1, \ldots, \tau_{k-1}\}$ is a basis of $\mathbb{K}(\lambda_0, \ldots, \lambda_{n-1})[x]$ over $\mathbb{K}[x]$. Therefore, the polynomials $\widehat{r}, \widehat{q}_i \in \mathbb{K}(\lambda_0, \ldots, \lambda_{n-1})[x]$ can be uniquely written in the following form:

$$\widehat{r} = r + \sum_{s=1}^{n-1} \tau_s r_s\,, \tag{3.4}$$

and

$$\widehat{q}_i = q_i + \sum_{s=1}^{n-1} \tau_s q_{si}, \quad 0 \leq i \leq m-1\,, \tag{3.5}$$

where r, r_s, q_i, $q_{si} \in \mathbb{K}[x]$, with $\deg r$, $\deg r_i < mn$.

Setting (3.4) and (3.5) in (3.3), we get

$$r^{(i)} = f_i + gq_i \tag{3.6}$$

for all $0 \leq i \leq m-1$.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

ELA

Now from (3.6) we clearly get that r satisfies the identities (3.2), and since the polynomial of degree less than mn satisfying the identities (3.2) is unique, we conclude that $r = \widehat{r}$.

Finally, suppose that Theorem 3.1 is true for one polynomial $g \in \mathbb{K}[x]$ having a root $\lambda \in \overline{\mathbb{K}}$ of multiplicity > 1. Then there exists a polynomial g_0 in $\overline{\mathbb{K}}[x]$ such that

$$g(x) = (x-\lambda)^2 g_0(x)\,.$$

Applying Theorem 3.1 for g and $f_0 = f_1 = 1$, we obtain

$$r(x) = 1 + (x-\lambda)^2 g_0(x) q_0(x) \tag{3.7}$$

and

$$r^{(1)}(x) = 1 + (x-\lambda)^2 g_0(x) q_1(x) \tag{3.8}$$

for some r, q_0, $q_1 \in \overline{\mathbb{K}}[x]$.

Differentiating (3.7), and setting $x = \lambda$ in the resulting identity, as well as in (3.8), we respectively get the contradiction

$$r^{(1)}(\lambda) = 0 \;\text{ and }\; r^{(1)}(\lambda) = 1. \quad \square$$

4. Applications of Theorem 3.1. Firstly, we will use Theorem 3.1 to give a closed formula for the semi–simple part of the well known Jordan decomposition, (e.g., [2, 4, 7]) of an algebraic element A of an algebra $\mathbf{A}$ over a perfect field $\mathbb{K}$ into a semisimple S_A and a nilpotent part. A proof of the existence of S_A that is presented in the book of Hoffman and Kunze [4], is based on Newton's method and yields direct methods for computations. An algorithm, which is essentially based on these ideas, is given by Levelt [6]. The algorithm of Bourgoyne and Cushman [3] is faster, because higher derivatives are used. In [9], D. Schmidt has used Newton's method to construct the semi–simple part of the Jordan decomposition of an algebraic element in an arbitrary algebra, showing quadratic convergence of the algorithm. Another approach uses the partial fractions decomposition of the reciprocal of the minimal polynomial [5, 10, 11]. An explicit construction of the spectral decomposition of a matrix using Hermite interpolation is reported in [11], which requires the use of Taylor coefficients of the reciprocal of the matrix minimal polynomial.

In this work, we also obtain a new closed formula for the semi–simple part S_A of the Jordan decomposition of an algebraic element A in an arbitrary algebra, using our proposed polynomial division by a common separable divisor. The proposed closed formula requires only evaluation of the derivatives of the basic Hermite–like interpolation polynomials that are associated with the eigenvalues of A, up to the

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

maximum algebraic multiplicity of the roots of the minimal polynomial of A, as well as matrix multiplication operations. It has to be noted however that the semi–simple part S_A of A is obtained using a polynomial of higher degree than the one used in [11]. In order to obtain the expression for S_A we need the following lemma.

LEMMA 4.1. *Let $g \in \mathbb{K}[x]$ be a separable polynomial and $\lambda_0, \dots, \lambda_{n-1}$ are the roots of g in $\overline{\mathbb{K}}$. Let $f \in \mathbb{K}[x,y]$ be a polynomial of two variables and m be a positive integer. Then there exists unique $r \in \mathbb{K}[x]$ of degree less than mn such that*

$$f(x,y) = r(x+y) \mod I,$$

where $I \subset \mathbb{K}[x,y]$ is the ideal generated from the polynomials $g(x)$, y^m. Further, the polynomial r is given by

$$r(x) = \sum_{j=0}^{n-1} X_j \Lambda_j^{-1} A_j \in \mathbb{K}[x], \tag{4.1}$$

where the matrices X_j, A_j are given by

$$X_j = \left[\begin{array}{cccc} L_j(x) & \frac{(x-\lambda_j)}{1!} L_j(x) & \cdots & \frac{(x-\lambda_j)^{m-1}}{(m-1)!} L_j(x) \end{array} \right],$$
$$A_j = \left[\begin{array}{cccc} f(\lambda_j, 0) & \frac{\partial}{\partial y} f(\lambda_j, 0) & \cdots & \frac{\partial^{m-1}}{\partial y^{m-1}} f(\lambda_j, 0) \end{array} \right]^T,$$

and L_j, Λ_j are as in (2.1), (2.2) by $m_0 = m_1 = \cdots = m_{n-1} = m$

Proof. The polynomial f can be rewritten in the form

$$f(x,y) = \sum_{i=0}^{m-1} \frac{1}{i!} \frac{\partial^i}{\partial y^i} f(x,0) y^i + y^m h(x,y), \tag{4.2}$$

for some $h \in \mathbb{K}[x,y]$.

Furthermore, according to Theorem 3.1 there exists unique polynomial $r \in \mathbb{K}[x]$ of degree less than mn, given by (4.1), such that:

$$\frac{\partial^i}{\partial y^i} f(x,0) = r^{(i)}(x) \mod g(x), \ \ 0 \le i \le m-1, \tag{4.3}$$

Combining (4.2) with (4.3), we get

$$f(x,y) = \sum_{i=0}^{m-1} \frac{r^{(i)}(x)}{i!} y^i \mod I. \tag{4.4}$$

Furthermore, by using the Taylor formula, we have:

$$\sum_{i=0}^{m-1} \frac{r^{(i)}(x)}{i!} y^i = r(x+y) \mod y^m. \tag{4.5}$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

Substituting (4.5) in (4.4) completes the proof. $\square$

Now we will use Theorem 3.1 to give a closed formula for the semi–simple part of the Jordan decomposition of an algebraic number of an algebra $\mathbf{A}$ over a perfect field $\mathbb{K}$.

Let $p \in \mathbb{K}[x]$ be the minimal polynomial of an algebraic element A of an algebra $\mathbf{A}$ over $\mathbb{K}$ with unit 1. Let λ_i, $i = 0, 1, \ldots, n-1$ be the distinct roots of p in $\overline{\mathbb{K}}$, and let k_i, $i = 1, 2, \ldots, n-1$ be their respective multiplicities. We denote $\widehat{p}(x) := \prod_{i=0}^{n-1}(x - \lambda_i)$ and $m(p) := \max\{k_0, \ldots, k_{n-1}\}$.

Proposition 4.2. *The semi–simple part S_A of the Jordan decomposition of A is given by $S_A = r(A)$, where $r(x)$ is the polynomial*

$$r(x) = \sum_{j=0}^{n-1} X_j \Lambda_j^{-1} A_j \in \mathbb{K}[x], \tag{4.6}$$

where

$$X_j = \begin{bmatrix} L_j(x) & \frac{(x-\lambda_j)}{1!} L_j(x) & \cdots & \frac{(x-\lambda_j)^{m-1}}{(m-1)!} L_j(x) \end{bmatrix},$$
$$A_j = \begin{bmatrix} \lambda_j & 0 & \cdots & 0 \end{bmatrix}^T,$$

and L_j, Λ_j are as in (2.1), (2.2) by $m_0 = m_1 = \cdots = m_{n-1} = m(p)$.

Proof. Since S_A is the semi–simple part of A and N_A is the nilpotent part of A, the minimal polynomials of S_A and N_A are respectively $\widehat{p}(x)$ and $x^{m(p)}$. So we have $\widehat{p}(S_A) = 0$ and $N_A^{m(p)} = 0$. Now if we apply Lemma 4.1 by choosing $f(x, y) = x$, $g(x) = \widehat{p}(x)$ and $m = m(p)$, and taking into account that $f(x, 0) = x$, and $\frac{\partial^i}{\partial y^i} f(x, 0) = 0$ for $1 \le i \le m-1$ we have that for the polynomial r given by (4.6) holds:

$$x = r(x + y) \mod I, \tag{4.7}$$

where I is the ideal generated from the polynomials $\widehat{p}(x)$ and $y^{m(p)}$. Finally setting $x = S_A$ and $y = N_A$ in (4.7) we get $S_A = r(S_A + N_A) = r(A)$. $\square$

The next result of this section is the generalization of Theorem 3.1, which is expressed in the following theorem.

Theorem 4.3. *Let $g \in \mathbb{K}[x]$ be separable of degree n. Let $\Pi \in (\mathbb{K}[x])^{m \times m}$ such that $\det(\Pi) \neq 0$. Then, for any polynomials $f_0, f_1, \ldots, f_{m-1} \in \mathbb{K}[x]$, there exists a unique polynomial $r \in \mathbb{K}[x]$ of degree less than mn, such that*

$$\Pi \begin{bmatrix} r \\ r' \\ \vdots \\ r^{(m-1)} \end{bmatrix} = E \begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{m-1} \end{bmatrix} \mod g,$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

where $E := \gcd(g,\ \det(\Pi))$.

Proof. We start from

$$\Pi\widetilde{\Pi} = \widetilde{\Pi}\Pi = \det(\Pi) I_m, \tag{4.8}$$

where $\widetilde{\Pi}$ is the adjugate of Π and I_m is the $m \times m$ unit matrix.

Moreover, since $E = \gcd(g, \det(\Pi))$ one has that there exist $H, G \in \mathbb{K}[x]$ such that

$$H \det(\Pi) + Gg = E\,. \tag{4.9}$$

Combining (4.8) with (4.9), we get

$$H\Pi\widetilde{\Pi} = (E - gG) I_m\,. \tag{4.10}$$

Now, according to Theorem 3.1, there exists a unique $r \in \mathbb{K}[x]$ of degree less than mn such that

$$\begin{bmatrix} r \\ r' \\ \vdots \\ r^{(m-1)} \end{bmatrix} = H\widetilde{\Pi} \begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{m-1} \end{bmatrix} \mod g\,. \tag{4.11}$$

Multiplying (4.11) from the left by Π and setting (4.10) in the resulting identity we get the conclusion. ☐

Remark 4.4. Choosing $\Pi = I_m$ in Theorem 4.3, we get Theorem 3.1. Therefore, Theorem 4.3 can be regarded as a generalization of Theorem 3.1.

Now we will apply Theorem 4.3 to produce some formulas for polynomials involving derivatives.

Corollary 4.5. *Let* $g, g_0, g_1, \ldots, g_{m-1} \in \mathbb{K}[x]$ *be polynomials. Assume that* g *is separable and that*

$$(g_i, g) = 1, \quad 0 \le i \le m-1\,.$$

Then, for any $f_0, f_1, \ldots, f_{m-1} \in \mathbb{K}[x]$*, there exists unique* $r \in \mathbb{K}[x]$ *of degree less than* mn *such that*

$$g_i r^{(i)} = f_i \mod g, \quad 0 \le i \le m-1\,.$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

Proof. Applying Theorem 4.3 by

$$\Pi := \begin{bmatrix} g_0 & 0 & \cdots & 0 \\ 0 & g_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{m-1} \end{bmatrix},$$

and afterwards using that $E = \gcd(g, \det(\Pi) = \prod_{i=0}^{m-1} g_i) = 1$, we directly get the conclusion. ∎

Corollary 4.6. *Let g, $g_0, g_1, \ldots, g_{m-1} \in \mathbb{K}[x]$ be as in Corollary 4.5. Then, for any $f_0, f_1, \ldots, f_{m-1} \in \mathbb{K}[x]$, there exists unique r of degree less than mn such that*

$$(g_i r)^{(i)} = f_i \mod g, \;\; 0 \leq i \leq m-1\,.$$

Proof. Let $\Pi \in (\mathbb{K}[x])^{m\times m}$ be the matrix defined by

$$\Pi = \begin{bmatrix} g_0 & 0 & \cdots & 0 \\ \binom{1}{0} g_1^{(1)} & \binom{1}{1} g_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m-1}{0} g_{m-1}^{(m-1)} & \binom{m-1}{1} g_{m-1}^{(m-2)} & \cdots & \binom{m-1}{m-1} g_{m-1}^{(0)} \end{bmatrix}. \tag{4.12}$$

From the assumptions

$$(g_i, g) = 1, \;\; 0 \leq i \leq m-1,$$

we have

$$(\det(\Pi), g) = 1\,. \tag{4.13}$$

Applying Theorem 4.3 for Π, as given in (4.12), using (4.13) and Leibnitz's rule, we get the conclusion. ∎

REFERENCES

[1] I.S. Berezin and N.P. Zhidkov. *Computing Methods* (Chapter 8, Section 9, translated from Russian). Pergamon, 1973.
[2] N. Bourbaki. *Elements de Mathematique; Algebre* (Chapter 7, Section 5). Hermann, Paris, 1958.
[3] N. Burgoyne and R. Cushman. The decomposition of a linear mapping. *Linear Algebra Appl.*, 8:515–519, 1974.
[4] K. Hoffman and R. Kunze. *Linear Algebra*, second edition (Chapter 7, Section 7). Prentice-Hall, Englewood Cliffs, NJ, 1971 .

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 23, pp. 770-781, August 2012

[5] P.F. Hsieh, M. Kohno, and Y. Sibuya. Construction of a fundamental matrix solution at a singular point of the first kind by means of the SN decomposition of matrices. *Linear Algebra Appl.*, 239:29–76, 1996.

[6] A.H.M. Levelt. *The Semi-Simple Part of a Matrix.* Algoritmen In De Algebra, A Seminar on Algebraic Algorithms, University of Nijmegen, Nijmegen, 1993.

[7] T. Mulders. *Computation of Normal Forms for Matrices.* Algoritmen In De Algebra, A Seminar on Algebraic Algorithms, University of Nijmegen, Nijmegen, 1993.

[8] R. Sakai and P. Vertesi. Hermite-Fejer interpolations of higher order. III. *Studia Sci. Math. Hungar.*, 28:87–97, 1993.

[9] D. Schmidt. Construction of the Jordan decomposition by means of Newton's method. *Linear Algebra Appl.* 314:75–89, 2000.

[10] G. Sobczyk. The generalized spectral decomposition of a linear operator. *College Math. J.*, 28:27–38, 1997.

[11] L. Verde-Star. Interpolation approach to the spectral resolution of square matrices. *L' Enseignement Mathematique*, 52:239–253, 2006.