Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Linear Algebra and its Applications 420 (2007) 117–123

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

Generalized derivations and additive theory II [☆]

J.A. Dias da Silva [a,*], Hemar Godinho [b]

[a] *Departamento de Matemática, Faculdade de Ciências da Universidade de Lisboa, Campo Grande, Edifício C6, Piso 2, P-1749-016 Lisboa, Portugal*

[b] *Departamento de Matemática, Universidade de Brasília, 70919-900 Brasília, Brazil*

Received 30 March 2006; accepted 23 June 2006
Available online 28 August 2006
Submitted by R.A. Brualdi

Abstract

We return to the theme of generalized derivations related to symmetric functions to correct the hypothesis of one of the main theorems of our first paper, so that all cases are now properly covered.

AMS classification: 15A69; 11P99

Keywords: Additive number theory; Generalized derivations

1. Preliminaries

Let $\mathbb{F}$ be an arbitrary field of characteristic p. In [1] we estimated the cardinality of the range of elementary symmetric polynomials defined on the Cartesian product of certain finite sets. The statement of the main results of [1], Theorems 5 and 6 are not correct and needs an extra constraint to guarantee the correctness of the proofs. We are going to present new versions of those results with the new proofs. The wrong argument of the proofs in [1] concerns the existence of ρ_t satisfying equalities (4) and (5) of [1].

[☆] The research of the first author was done within the activities of the Centro de Estruturas Lineares e Combinatórias and supported by project POCTI-ISFL-1-1431. The second author was partially supported by a grant from CNPq-Brazil.

[*] Corresponding author. Tel.: +351 21 750 0296; fax: +351 21 750 0072.

E-mail addresses: perdigao@hermite.cii.fc.ul.pt (J.A. Dias da Silva), hemar@unb.br (H. Godinho).

0024-3795/$ - see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2006.06.019

We use $Q_{k,m}$ to denote the subset of the strictly increasing maps from $\{1,\ldots,k\}$ into $\{1,\ldots,m\}$. We write $s_k(X_1,\ldots,X_m)$ to mean the elementary symmetric polynomial of degree k in the indeterminates $X_1,\ldots,X_m$, i.e.

$$s_k(X_1,\ldots,X_m)=\sum_{\omega\in Q_{k,m}} X_{\omega(1)}\cdots X_{\omega(k)}.$$

Let $A_1,\ldots,A_m$ be nonempty finite subsets of the field $\mathbb{F}$. In [1] a lower bound was found for the cardinality of the set

$$s_k(A_1,\ldots,A_m):=\{s_k(a_1,\ldots,a_m)\colon (a_1,\ldots,a_m)\in A_1\times\cdots\times A_m\}.$$

An answer for this problem was obtained after we translated it to the Linear Algebra setting and studied the degree of the minimal polynomial of the linear operator $s_k(T_1,\ldots,T_m)$ defined as follows:

Definition 1.1. Let T_i be a linear operator on a finite dimensional vector space V_i over $\mathbb{F}$, $i=1,\ldots,m$. For $\omega\in Q_{k,m}$, let $\delta_\omega(T_1,\ldots,T_m)=S_1\otimes\cdots\otimes S_m$ with $S_i=I$ if $i\notin \operatorname{Im}(\omega)$ and $S_i=T_i$ if $i\in\operatorname{Im}(\omega)$. The linear operator $s_k(T_1,\ldots,T_m)$ on $V_1\otimes\cdots\otimes V_m$ is defined as the sum of the operators $\delta_\omega(T_1,\ldots,T_m)$

$$s_k(T_1,\ldots,T_m):=\sum_{\omega\in Q_{k,m}}\delta_\omega(T_1,\ldots,T_m).$$

This linear operator is related with the elements

$$D_{k,\mathbb{Z}}(X_1,\ldots,X_m):=\sum_{\omega\in Q_{k,m}}\delta_\omega(X_1\otimes\cdots\otimes X_m)$$

of the $\mathbb{Z}$-algebra $\mathbb{Z}[X_1]\otimes\cdots\otimes\mathbb{Z}[X_m]$ and

$$D_{k,\mathbb{F}}(X_1,\ldots,X_m):=\sum_{\omega\in Q_{k,m}}\delta_\omega(X_1\otimes\cdots\otimes X_m)$$

of the $\mathbb{F}$-algebra $\mathbb{F}[X_1]\otimes\cdots\otimes\mathbb{F}[X_m]$. To handle these elements we have to consider the basis $\mathscr{E}_\mathbb{Z}$ of $\mathbb{Z}[X_1]\otimes\cdots\otimes\mathbb{Z}[X_m]$ induced by the bases $\left\{X_i^j\colon j\in\mathbb{N}_0\right\}$, $i=1,\ldots,m$ and the basis $\mathscr{E}_\mathbb{F}$ of $\mathbb{F}[X_1]\otimes\cdots\otimes\mathbb{F}[X_m]$ induced by the bases $\left\{X_i^j\colon j\in\mathbb{N}_0\right\}$, $i=1,\ldots,m$.

Terminology. Let A be a commutative ring with identity and M a free A-module. Let $\mathscr{V}$ be a basis of M. Given $m\in M$

$$m=\sum_{v\in\mathscr{V}} a_v v$$

we call *support* of m on $\mathscr{V}$ to the subset of $\mathscr{V}$

$$\operatorname{supp}_{\mathscr{V}}(m):=\{v\in\mathscr{V}\colon a_v\neq 0\}.$$

Let $v\in\mathscr{V}$. We say that v, *$\mathscr{V}$-occurs* in m if $v\in\operatorname{supp}_{\mathscr{V}}(m)$.

The following results were proved in [1].

Theorem 1.2. *The element $X_1^{s_1}\otimes\cdots\otimes X_m^{s_m}$, $\mathscr{E}_\mathbb{Z}$-occurs in $D_{k,\mathbb{Z}}(X_1,\ldots,X_m)^t$ if and only if $s_1+\cdots+s_k=kt$ and $s_i\leqslant t$, $i=1,\ldots,m$.*

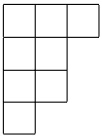
Corollary 1.3. *Let*

$$D_{k,\mathbb{Z}}(X_1,\ldots,X_m)^t = \sum_{\substack{(s_1,\ldots,s_m)\in\mathbb{N}_0^m\\ s_1+\cdots+s_m=kt\\ s_i\leqslant t, i=1,\ldots,m}} \mathscr{C}_{(s_1,\ldots,s_m)} X_1^{s_1}\otimes\cdots\otimes X_m^{s_m}$$

with $\mathscr{C}_{(s_1,\ldots,s_n)}\in\mathbb{N}$. *Then*

$$\operatorname{supp}_{\mathscr{E}_{\mathbb{F}}}\left(D_{k,\mathbb{F}}(X_1,\ldots,X_m)^t\right) = \left\{(s_1,\ldots,s_m):\ \begin{array}{c} s_1+\cdots+s_m=kt,\\ s_i\leqslant t,\ i=1,\ldots,m,\\ \text{and } p\nmid\mathscr{C}_{(s_1,\ldots,s_n)}\end{array}\right\}.$$

A partition of $N\in\mathbb{N}$ is a decreasing sequence of nonnegative integers whose terms sum up to N. We identify partitions that differ only by a string of zeros. Using this identification we represent (when convenient) any partition by a N-tuple. We use the notation $a^{(h)}$ for the finite sequence of length h with all terms equal a, i.e. $a^{(h)} := \underbrace{(a,\ldots,a)}_{h\text{ times}}$. To each partition $\lambda=(\lambda_1,\ldots,\lambda_t)$ of N we associate a Young diagram $[\lambda]$ with N boxes arranged in t left justified rows with row i having λ_i boxes, $i=1,\ldots,t$. For example the partition $(3,2,2,1)$ has Young diagram

$[\lambda] =$ 

Let $\lambda=(\lambda_1,\ldots,\lambda_N)$ be a partition of N. For $j\in\mathbb{N}$ define $\tilde{\lambda}_j$ to be the cardinality of $\{i\colon\lambda_i\geqslant j\}$. Then the sequence $\tilde{\lambda}=(\tilde{\lambda}_1,\ldots,\tilde{\lambda}_N)$ is a partition of N called the *conjugate partition* of λ. It is easy to see that $\tilde{\lambda}_j$ is the number of boxes of the jth column of $[\lambda]$. Counting, by rows, the boxes of the first t columns of $[\lambda]$ we get that for $t\in\mathbb{N}$

$$\begin{aligned}\tilde{\lambda}_1+\cdots+\tilde{\lambda}_t &= \text{number of boxes in the first } t \text{ columns of } [\lambda]\\ &= \min\{\lambda_1,t\}+\cdots+\min\{\lambda_N,t\}. \end{aligned}\tag{1.1}$$

Given two partitions of N, $\rho=(\rho_1,\ldots,\rho_N)$ and $\gamma=(\gamma_1,\ldots,\gamma_N)$ we say that ρ *dominates* γ and we write $\rho\succeq\gamma$ if

$$\rho_1+\cdots+\rho_i\geqslant\gamma_1+\cdots+\gamma_i,\quad i=1,\ldots,N.$$

2. Correcting the main result

Let V be a finite dimensional vector space over $\mathbb{F}$ and let T be a linear operator on V. Let $d=\deg(P_T)$, where P_T denotes the minimal polynomial of T. It is well known that $\{I,T,T^2,\ldots,T^{d-1}\}$ is a basis of the cyclic $\mathbb{F}$-subalgebra of $L(V,V)$ generated by $\{T\}$. We write $\langle T\rangle$ to denote this cyclic subalgebra.

Let $l_i=\deg(P_{T_i})$, $i=1,\ldots,m$. The set

$$\mathscr{B}=\left\{T_1^{e_1}\otimes\cdots\otimes T_m^{e_m}\colon 0\leqslant e_j\leqslant l_j-1 \text{ for } j=1,2,\ldots,m\right\}$$

is the basis of $\langle T_1\rangle\otimes\langle T_2\rangle\otimes\cdots\otimes\langle T_m\rangle$ induced by the bases $\left\{I,T_i,\ldots,T_i^{l_i-1}\right\}$, $i=1,\ldots,m$.

If ψ_i the evaluation map $f(X_i) \to f(T_i)$ from $\mathbb{F}[X_i]$ into $\langle T_i \rangle$, then

$$\begin{aligned} s_k(T_1, \dots, T_m)^t &= \psi_1 \otimes \cdots \otimes \psi_m \left(D_{k,\mathbb{F}}(X_1, \dots, X_m)^t\right) \\ &= \sum_{(s_1,\dots,s_m) \in \operatorname{supp}_{\mathscr{E}_{\mathbb{F}}}(D_{k,\mathbb{F}}(X_1,\dots,X_m)^t)} \mathscr{C}_{(s_1,\dots,s_m)} T_1^{s_1} \otimes \cdots \otimes T_m^{s_m}. \end{aligned} \tag{2.1}$$

Notation. Given m positive integers $a_1, \dots, a_m$ we write $\ell(k, a_1, \dots, a_m)$ to denote the integer

$$\ell(k, a_1, \dots, a_m) := \left\lfloor \frac{a_1 + \cdots + a_m - m}{k} \right\rfloor + 1$$

and $r(k, a_1, \dots, a_m)$ to denote the integer

$$r(k, a_1, \dots, a_m) := (a_1 + \cdots + a_m - m) - (\ell(k, a_1, \dots, a_m) - 1)k.$$

From now on assume $l_1 \geqslant \cdots \geqslant l_m \geqslant 1, \ell = \ell(k, l_1, \dots, l_m), r = r(k, l_1, \dots, l_m)$ and write $\lambda = (\lambda_1, \dots, \lambda_m) = (l_1 - 1, l_2 - 1, \dots, l_m - 1)$.

For $0 \leqslant t \leqslant \ell - 1$, set

$$l_i' := \min\{t + 1, l_i\}, \quad i = 1, \dots, m. \tag{2.2}$$

For $t = 1, \dots, \ell - 1$ let

$$\boldsymbol{E}_t = \left\{ j \in \{1, \dots, m\}\colon (l_1' - 1) + \cdots + (l_j' - 1) \geqslant kt \right\}.$$

Proposition 2.1. *Let $\ell = \ell(k, l_1, \dots, l_m)$ and $r = r(k, l_1, \dots, l_m)$. The set $\boldsymbol{E}_t$ is a nonempty subset of $\{1, \dots, m\}$ for every $t \in \{1, \dots, \ell - 1\}$ if and only if*

$$(l_1 - 1, \dots, l_m - 1) \preceq \left(\ell + r - 1, (\ell - 1)^{(k-1)}\right).$$

Proof. Assuming that $\lambda = (l_1 - 1, \dots, l_m - 1) \preceq \left(\ell + r - 1, (\ell - 1)^{(k-1)}\right)$, we are going to prove that $m \in \boldsymbol{E}_t$. From this hypothesis it follows that

$$\tilde{\lambda} = (\tilde{\lambda}_1, \dots, \tilde{\lambda}_m) \succeq \left(k^{(l-1)}, 1^{(r)}\right). \tag{2.3}$$

Then for $t = 1, \dots, \ell - 1$

$$\tilde{\lambda}_1 + \cdots + \tilde{\lambda}_t \geqslant kt.$$

Using (1.1) we have for, $1 \leqslant t \leqslant \ell - 1$,

$$\min\{(l_1 - 1), t\} + \cdots + \min\{(l_m - 1), t\} \geqslant kt.$$

Now using the definition of l_i' we rewrite the former inequality as follows:

$$\sum_{i=1}^{m} (l_i' - 1) \geqslant kt.$$

Therefore, $m \in \boldsymbol{E}_t$.

Conversely assume that for $t \in \{1, \dots, \ell - 1\}$, $\boldsymbol{E}_t \neq \emptyset$. Then,

$$\sum_{i=1}^{m} (l_i' - 1) \geqslant kt, \quad t = 1, \dots, \ell - 1.$$

Again, using Eqs. (1.1) and (2.2), we get

$$\min\{(l_1-1),t\}+\cdots+\min\{(l_m-1),t\}\geqslant kt.$$

Then

$$\tilde{\lambda}_1+\cdots+\tilde{\lambda}_t\geqslant kt,\quad t=1,\ldots,\ell-1. \tag{2.4}$$

Since (1^r) is the minimum of the partitions of r by the order of domination, we get from (2.4)

$$(\tilde{\lambda}_1,\ldots,\tilde{\lambda}_m)\succeq\left(k^{(\ell-1)},1^{(r)}\right).$$

Now

$$(l_1-1,\ldots,l_m-1)\preceq\left(\ell+r-1,(\ell-1)^{(k-1)}\right)$$

follows, by conjugation. □

In [1] the following is proved:

Lemma 2.2. *If $T_1^{s_1}\otimes\cdots\otimes T_m^{s_m}$ satisfies the conditions*

(i) $s_1+\cdots+s_m=kt$;
(ii) $s_i\leqslant\min\{l_i-1,t\}$, $i=1,\ldots,m$;
(iii) $p\not|\mathscr{C}_{(s_1,\ldots,s_m)}$,

then $T_1^{s_1}\otimes\cdots\otimes T_m^{s_m}\in\mathscr{B}$ and it $\mathscr{B}$-occurs in $(s_k(T_1,\ldots,T_m))^t$.

Until the end of this section let $\ell=\ell(k,l_1,\ldots,l_m)$, and $r=r(k,l_1,\ldots,l_m)$.

The next lemma shows that under the constraints listed in Proposition 2.1 there is a m-tuple $(s_1,\ldots,s_m)$ satisfying requirements conditions (i) and (ii) presented in the lemma above.

Lemma 2.3. *Assume that $((l_1-1),\ldots,(l_m-1))\preceq\left(\ell+r-1,(\ell-1)^{(k-1)}\right)$. Then for every $t\in\{1,\ldots,\ell-1\}$ there exists $\theta_t\in\mathbb{N}_0^m$ satisfying conditions* (i) *and* (ii) *of Lemma 2.2.*

Proof. For any $t\in\{1,\ldots,\ell-1\}$ let $\rho_t=\min E_t$. Define for $i=1,\ldots,m$ and $t=0,\ldots,\ell-1$

$$\theta_{t,i}=\begin{cases}l_i'-1 & \text{if } 1\leqslant i\leqslant\rho_t-1;\\ kt-(l_1'+\cdots+l_{\rho_t-1}'-(\rho_t-1)) & \text{if } i=\rho_t;\\ 0 & \text{if } i>\rho_t.\end{cases}$$

Then

(i) $\theta_{t,1}+\cdots+\theta_{t,m}=kt$;
(ii) $\theta_{t,i}\leqslant l_i'-1=\min\{l_i-1,t\}$, $i=1,\ldots,\ell-1$. □

Denote by $\theta_t(k,l_1,\ldots,l_m)$ (briefly by θ_t) the mapping constructed by the procedure described in the proof of the previous lemma.

Theorem 2.4. *Assume that $((l_1-1),\ldots,(l_m-1))\preceq\left(\ell+r-1,(\ell-1)^{(k-1)}\right)$. Let $0\leqslant s\leqslant\ell-1$. If p does not divide $\mathscr{C}_{\theta_t}$ for $t=1,\ldots,s$ then the degree of the minimal polynomial of $s_k(T_1,\ldots,T_m)$ is greater than or equal to $s+1$.*

Proof. Bearing in mind Lemmas 2.2 and 2.3 we see, since p does not divide $\mathscr{C}_{\theta_t}$ for every $t \in \{1, \ldots, \ell - 1\}$, that $\theta_t \in \operatorname{supp}_{\mathscr{B}}\big(s_k(T_1, \ldots, T_m)^t\big)$. On the other hand from Corollary 1.3 and equality (2.1) we conclude that $\theta_t \notin \operatorname{supp}_{\mathscr{B}}\big(s_k(T_1, \ldots, T_m)^{t-1}\big)$. Then

$$\theta_t \in \operatorname{supp}_{\mathscr{B}}\left(s_k(T_1, \ldots, T_m)^t\right) \backslash \operatorname{supp}_{\mathscr{B}}\left(s_k(T_1, \ldots, T_m)^{t-1}\right).$$

One can easily see that this implies that

$$I, s_k(T_1, \ldots, T_m), \ldots, s_k(T_1, \ldots, T_m)^s$$

are linearly independent linear operators of $V_1 \otimes \cdots \otimes V_m$. Therefore,

$$\deg(P_{s_k(T_1,\ldots,T_m)}) \geqslant s + 1. \qquad \square$$

Corollary 2.5. *Assume that* $((l_1 - 1), \ldots, (l_m - 1)) \preceq \left(\ell + r - 1, (\ell - 1)^{(k-1)}\right)$. *If either* $\mathbb{F}$ *is of characteristic zero or* p *is big enough then*

$$\deg P_{s_k(T_1,\ldots,T_m)} \geqslant \left\lfloor \frac{\deg(P_{T_1}) + \cdots + \deg(P_{T_m}) - m}{k} \right\rfloor + 1.$$

Corollary 2.6. *Assume that either* $\mathbb{F}$ *is of characteristic zero or* p *is big enough. If* T *be a linear operator on a nonzero finite dimensional vector space* V *over* $\mathbb{F}$ *then*

$$\deg\left(P_{s_k(T,\ldots,T)}\right) \geqslant \left\lfloor \frac{m(\deg(P_T) - 1)}{k} \right\rfloor + 1.$$

3. Additive theory results

Throughout this section k, m are positive integers with $k \leqslant m$. Let $A_1, \ldots, A_m$ be finite nonempty subsets of a field $\mathbb{F}$ and suppose, without loss of generality, that

$$|A_1| \geqslant |A_2| \geqslant \cdots \geqslant |A_m|.$$

Let $\ell = \ell(k, |A_1|, \ldots, |A_m|)$, $r = r(k, |A_1|, \ldots, |A_m|)$ and let $\theta_t = \theta_t(k, |A_1|, \ldots, |A_m|)$. Using the arguments of the proof of Theorem 4.6 of [1] we obtain from Theorem 2.4 the following result:

Theorem 3.1. *Assume that* p *does not divide* $\mathscr{C}_{\theta_t}$, $t = 1, \ldots, \ell - 1$, *and*

$$(|A_1| - 1, \ldots, |A_m| - 1) \preceq \left(\ell + r - 1, (\ell - 1)^{(k-1)}\right).$$

Then

$$|s_k(A_1, \ldots, A_m)| \geqslant \left\lfloor \frac{|A_1| + |A_2| + \cdots + |A_m| - m}{k} \right\rfloor + 1.$$

Corollary 3.2. *Assume that* $((|A_1| - 1), \ldots, (|A_m| - 1)) \preceq \left(\ell + r - 1, (\ell - 1)^{(k-1)}\right)$. *If either* $\mathbb{F}$ *is of characteristic zero or* p *is big enough then*

$$|s_k(A_1, \ldots, A_m)| \geqslant \left\lfloor \frac{|A_1| + |A_2| + \cdots + |A_m| - m}{k} \right\rfloor + 1.$$

Corollary 3.3. *Assume that either $\mathbb{F}$ is of characteristic zero or p is big enough. If A be a finite nonempty subset of $\mathbb{F}$. Then*

$$|s_k(A, \dots, A)| \geqslant \left\lfloor \frac{m(|A|-1)}{k} \right\rfloor + 1.$$

Acknowledgments

The authors wish to thank Teresa Antunes Rosa for pointing out an inaccuracy on the proof of Theorem 5 of [1].

Reference

[1] J.A. Dias da Silva, Hemar Godinho, Generalized derivations and additive theory, Linear Algebra Appl. 342 (2002) 1–15.