ELSEVIER Linear Algebra and its Applications 342 (2002) 1–15

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

Generalized derivations and additive theory

J.A. Dias da Silva [a,*,1], Hemar Godinho [b,2]

[a] *Departamento de Matemática-CELC, Universidade de Lisboa, Av Gama Pinto 2, 1649-003 Lisboa, Portugal*

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

Received 20 April 2000; accepted 23 May 2001

Submitted by R.A. Brualdi

Abstract

In this paper we investigate cyclic spaces of generalized derivations related to the symmetric functions, and its relation with a generalization of the Cauchy–Davenport Theorem. © 2002 Elsevier Science Inc. All rights reserved.

Keywords: Additive number theory; Generalized derivations

1. Introduction

A classical approach to the study of the structure of a linear operator has been through the understanding of its associated cyclic subspace. During the decade of the 1980s, an interesting element was added to this theory, and some problems were solved with results from Additive Number Theory (e.g. [13]). More recently, a two-way path was established and results on Linear Algebra were used to solve problems in Additive Theory, and the value of these methods was tested with the proof of a longstanding conjecture of Erdös–Heilbronn (see [6]). In the last years other papers appeared presenting results on Linear Algebra also with significance in Additive Theory [3–5,7].

[*] Corresponding author.

[1] This research was done within the activities of “Centro de Estruturas Lineares e Combinatórias” and partially supported by PRAXIS XXI project “Álgebra e Matemáticas Discretas”.

[2] This paper was written while the author was visiting the Universidade de Lisboa partially supported by a grant from CAPES-Brasília/Brazil.

PII: S0024-3795(01)00406-2

In this paper we are going to investigate cyclic spaces of generalized derivations related to the symmetric functions, and its relation with a generalization of the Cauchy–Davenport Theorem.

Let $\mathbb{F}$ be an arbitrary field of characteristic p, a prime number, if it is of finite characteristic or $p = \infty$ otherwise. If $b \in \mathbb{R}$, denote by $\lfloor b \rfloor$ the greatest integer less than or equal to b. Let r and $n_1, n_2, \ldots, n_r, n$ be positive integers. We denote by $\Gamma_{(n_1,\ldots,n_r)}$ the set of all mappings α from $\{1, \ldots, r\}$ into $\mathbb{N}$ satisfying $\alpha(i) \leqslant n_i$, $i = 1, \ldots, r$. We abbreviate to $\Gamma_{r,n}$ the notation $\Gamma_{(\underbrace{n, \ldots, n}_{r \text{ times}})}$. The set $Q_{r,s}$ is the subset of $\Gamma_{r,s}$ of the strictly increasing mappings from $\{1, \ldots, r\}$ into $\{1, \ldots, s\}$. Let $m \in \mathbb{N}$ and let $k \in \mathbb{N}$ such that $k \leqslant m$. Let $X_1, \ldots, X_m$ be m distinct indeterminates. The kth elementary symmetric function on the indeterminates $X_1, \ldots, X_m$

$$\sum_{\omega \in Q_{k,m}} X_{\omega(1)} \cdot X_{\omega(2)} \cdots X_{\omega(k)}$$

will be denoted by $s_k(X_1, \ldots, X_m)$ or by s_k (if there is no ambiguity to avoid), $k = 1, \ldots, m$.

Let $A_1, \ldots, A_m$ be finite subsets of $\mathbb{F}$. We denote by

$$s_k(A_1, \ldots, A_m)$$

the set

$$s_k(A_1, \ldots, A_m) := \left\{ s_k(b_1, \ldots, b_m) : (b_1, \ldots, b_m) \in A_1 \times A_2 \times \cdots \times A_m \right\}.$$

Let V_i be a finite dimensional vector space of dimension n_i over the field $\mathbb{F}$. Let $L(V_i, V_i)$ be the $\mathbb{F}$-algebra of linear operators on V_i. We denote by $V_1 \otimes V_2 \otimes \cdots \otimes V_m$ the tensor product of $V_1, \ldots, V_m$. If T is a linear operator, we denote by P_T the minimal polynomial of T, by $\sigma(T)$ the spectrum of T (the n-tuple of characteristic roots of T in $\overline{\mathbb{F}}$, the algebraic closure of $\mathbb{F}$) and by I the identity linear operator.

Let $\mathscr{A}_1, \ldots, \mathscr{A}_m$ be algebras over a commutative ring, and take $a_i \in \mathscr{A}_i$ for $i = 1, \ldots, m$. Let us denote by

$$\Delta_i = \left\{ \omega \in Q_{k,m} \mid i \in \operatorname{Im}(\omega) \right\}.$$

Now, for $\omega \in Q_{k,m}$, define the map δ_ω from $\mathscr{A}_1 \times \cdots \times \mathscr{A}_m$ to $\mathscr{A}_1 \otimes \cdots \otimes \mathscr{A}_m$ by

$$\delta_\omega(a_1, \ldots, a_m) = u_1 \otimes u_2 \otimes \cdots \otimes u_m$$

where

$$u_i = \begin{cases} a_i & \text{if } \omega \in \Delta_i, \\ 1_{\mathscr{A}_i} & \text{otherwise.} \end{cases}$$

Consider $T_i \in L(V_i, V_i)$ $(1 \leqslant i \leqslant m)$ linear operators and denote by $s_k(T_1, \ldots, T_m)$ the linear operator on $V_1 \otimes \cdots \otimes V_m$

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

Theorem 1. *Let T_i be a linear operator on V_i and let $(\lambda_{i,1}, \ldots, \lambda_{i,n_i})$ be the spectrum of T_i, $i = 1, \ldots, m$. Then the spectrum of $s_k(T_1, \ldots, T_m)$ is*

$$(s_k(\lambda_{1,\alpha(1)}, \ldots, \lambda_{m,\alpha(m)}))_{\alpha\in\Gamma_{m,n}}.$$

Proof. This proof follows along the lines of Theorem 2.4 in [11, p. 233]. Let $T_i \in L(V_i, V_i)$ be a linear operator and $S_i \in L(V_i, V_i)$ be invertible, $i=1, \ldots, m$. Using the elementary properties of the tensor product of linear operators we can easily see that

$$\begin{aligned} &S_1 \otimes \cdots S_m(s_k(T_1, \ldots, T_m))S_1^{-1} \otimes \cdots \otimes S_m^{-1}) \\ &\quad = s_k(S_1T_1S_1^{-1}, \ldots, S_mT_mS_m^{-1}). \end{aligned}$$

Then, considering V_i over $\overline{\mathbb{F}}$, $i = 1, \ldots, m$, and making, if necessary, an extension of the field of scalars, we can always assume that T_i is an upper triangular linear operator with respect to the basis $(e_{i1}, \ldots, e_{in_i})$ of V_i, $i = 1, \ldots, m$. Let $T_{i,\omega} = I$ if $\omega \notin \Delta_i$ and $T_{i,\omega} = T_i$ if $\omega \in \Delta_i$. Then considering, ordered lexicographically, in $V_1 \otimes \cdots \otimes V_m$, the basis $(e^{\otimes}_{\alpha}) = (e_{1,\alpha(1)} \otimes \cdots \otimes e_{m,\alpha(m)})_{\alpha\in\Gamma_{m,(n_1,\ldots,n_m)}}$ induced by the bases $(e_{i1}, \ldots, e_{in_i})_{i=1,\ldots,m}$ we have

$$\begin{aligned} s_k(T_1, \ldots, T_m)(e^{\otimes}_{\alpha}) &= \sum_{\omega\in Q_{k,m}} \delta_{\omega}(T_1, \ldots, T_m)(e^{\otimes}_{\alpha}) \\ &= \sum_{\omega\in Q_{k,m}} T_{1,\omega}(e_{1,\alpha(1)}) \otimes \cdots \otimes T_{m,\omega}(e_{m,\alpha(m)}). \end{aligned}$$

We are assuming T_i to be an upper triangular operator, so

$$T_i(e_{ij}) = \lambda_{ij}e_{ij} + u_{ij},$$

where $u_{ij} \in \langle e_{i1}, \ldots, e_{i,j-1}\rangle$ (the subspace of V_i spanned by $\{e_{i1}, \ldots, e_{i,j-1}\}$), $i = 1, \ldots, n$. Thus from the former equality we get

$$\begin{aligned} &s_k(T_1, \ldots, T_m)(e^{\otimes}_{\alpha}) \\ &\quad = \sum_{\omega\in Q_{k,m}} e_{1\alpha(1)} \otimes \cdots \otimes \left(\lambda_{\omega(1),\alpha(\omega(1))}e_{\omega(1)\alpha(\omega(1))} + u_{\omega(1)\alpha(\omega(1))}\right) \\ &\qquad \otimes \cdots \otimes \left(\lambda_{\omega(k)\alpha(\omega(k))}e_{\omega(k)\alpha(\omega(k))} + u_{\omega(k)\alpha(\omega(k))}\right) \otimes \cdots \otimes e_{m,\alpha(m)} \\ &\quad = \left(\sum_{\omega\in Q_{k,m}} \prod_{t=1}^{k} \lambda_{\omega(t)\alpha(\omega(t))}\right) e^{\otimes}_{\alpha} + R_{\alpha}, \end{aligned}$$

by multilinearity.

Since $u_{ij} \in \langle e_{i1}, \ldots, e_{i,j-1}\rangle$, the tensors of the form $e^{\otimes}_{\beta}$, $\beta \in \Gamma_{m,n}$, that are present in R_{α}, have the property $\beta(t) \leqslant \alpha(t)$, $t = 1, \ldots, m$. Since $\beta \neq \alpha$, for at least one j we must have that $\beta(\omega(j)) < \alpha(\omega(j))$. Therefore $\beta < \alpha$ (by the lexicographic order) and the matrix of $s_k(T_1, \ldots, T_m)$ is upper triangular with respect to the basis $(e^{\otimes}_{\alpha})_{\alpha\in\Gamma_{(n_1,\ldots,n_m)}}$.

The entry (α, α) of that matrix is then

$$\sum_{\omega\in Q_{k,m}} \prod_{t=1}^{k} \lambda_{\omega(t),\alpha(\omega(t))} = s_k\big(\lambda_{1,\alpha(1)}, \ldots, \lambda_{m,\alpha(m)}\big). \qquad \square$$

Corollary 1. *Let $A_i = \{\lambda_{i,1}, \ldots, \lambda_{i,n_i}\}$ be a subset of $\mathbb{F}$, $i = 1, \ldots, m$. Let T_i be a diagonal linear operator on an n_i-dimensional space V_i such that $\sigma(T_i) = (\lambda_{i,1}, \ldots, \lambda_{i,n})$. Then the set of eigenvalues of $s_k(T_1, \ldots, T_m)$ is $s_k(A_1, \ldots, A_m)$. Therefore*

$$|\sigma(s_k(T_1, \ldots, T_m))| = |s_k(A_1, \ldots, A_m)|.$$

Our goal is to present lower bounds for the degree of the minimal polynomial of $s_k(T_1, \ldots, T_m)$ and for the cardinality of $s_k(A_1, \ldots, A_m)$.

2. Auxiliary results

Let $X_1, \ldots, X_m$ be indeterminates and consider the basis

$$E_i = \left\{X_i^m \mid m \in \mathbb{N}_0\right\}$$

of $\mathbb{Z}[X_i]$, $i = 1, \ldots, m$. Now consider the basis $\mathbb{E}$ in $\mathbb{Z}[X_1] \otimes \cdots \otimes \mathbb{Z}[X_m]$, induced by the bases $E_1, \ldots, E_m$.

Given $X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m} \in \mathbb{E}$ we call *degree* of $X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m}$ to the integer $s_1 + \cdots + s_m$.

Proposition 1. *Let Δ_i as before and $b = \binom{m}{k}$. Writing $\mathbb{X} = (X_1, \ldots, X_m)$, we have in $\mathbb{Z}[X_1] \otimes \cdots \otimes \mathbb{Z}[X_m]$, for $t \in \mathbb{N}$,*

$$\left(\sum_{\omega\in Q_{k,m}} \delta_\omega(\mathbb{X})\right)^t = \sum_{\substack{(n_{\omega_1},\ldots,n_{\omega_b})\in\mathbb{N}^b \\ n_{\omega_1}+\cdots+n_{\omega_b}=t}} \frac{t!}{n_{\omega_1}!n_{\omega_2}!\cdots n_{\omega_b}!} \times X_1^{\sum_{\omega\in\Delta_1} n_\omega} \otimes \cdots \otimes X_m^{\sum_{\omega\in\Delta_m} n_\omega}.$$

Proof. It is well known that if A is a commutative ring and $a_1, \ldots, a_b$ are elements of A, we have

$$(a_1 + a_2 + \cdots + a_b)^t = \sum_{\substack{(m_1,\ldots,m_b)\in\mathbb{N}_0^b \\ m_1+m_2+\cdots+m_b=t}} \frac{t!}{m_1!m_2!\cdots m_b!} a_1^{m_1} \cdot a_2^{m_2} \cdots a_b^{m_b}.$$

If we consider the tensor algebra $\mathbb{Z}[X_1] \otimes \cdots \otimes \mathbb{Z}[X_m]$, we have

$$
\begin{aligned}
&\left(\sum_{\omega\in Q_{k,m}} \delta_\omega(\mathbb{X})\right)^t \\
&\quad = \sum_{\substack{(n_{\omega_1},\ldots,n_{\omega_b})\in\mathbb{N}_0^b \\ n_{\omega_1}+n_{\omega_2}+\cdots+n_{\omega_b}=t}} \frac{t!}{n_{\omega_1}!n_{\omega_2}!\cdots n_{\omega_b}!}\delta_{\omega_1}(\mathbb{X})^{n_{\omega_1}}\cdots\delta_{\omega_b}(\mathbb{X})^{n_{\omega_b}} \\
&\quad = \sum_{\substack{(n_{\omega_1},\ldots,n_{\omega_b})\in\mathbb{N}_0^b \\ n_{\omega_1}+\cdots+n_{\omega_b}=t}} \frac{t!}{n_{\omega_1}!n_{\omega_2}!\cdots n_{\omega_b}!} X_1^{\sum_{\omega\in\Delta_1} n_\omega}\otimes\cdots\otimes X_m^{\sum_{\omega\in\Delta_m} n_\omega}. \qquad \square
\end{aligned}
$$

Let N be a positive integer. A nonincreasing sequence of nonnegative integers $R=(r_1,\ldots,r_t)$ is a *partition* of N if $r_1+\cdots+r_m=N$. Identifying partitions of N that differ only by a string of zeros, we can then represent (when convenient) any partition of N by an N-tuple.

Let us define the *conjugate partition* R of N to be the partition R' of N, $R'=(r'_1,r'_2,\ldots,r'_N)$, such that

$$r'_i=|\{j\in\{1,\ldots,N\}:r_j\geqslant i\}|,\quad i=1,\ldots,N.$$

Given two partitions of N, $R=(r_1,\ldots,r_N)$ and $S=(s_1,\ldots,s_N)$ we say that R *dominates* S and we write $R\succeq S$ if

$$r_1+\cdots+r_i\geqslant s_1+\cdots+s_i,\quad i=1,\ldots,N.$$

The following result can be found in [9, Lemma 1.4.11]:

$$R\succeq S \;\Leftrightarrow\; S'\succeq R'.$$

If $S=(s_1,\ldots,s_N)$ is a sequence of nonnegative integers, define the *partition* $\overline{S}=(\overline{s}_1,\ldots,\overline{s}_m)$ to be the reordering of $(s_1,\ldots,s_m)$ such that

$$\overline{s}_1\geqslant\overline{s}_2\geqslant\cdots\geqslant\overline{s}_m.$$

The Gale–Ryser theorem [2] is useful in the sequel:

Theorem 2 (Gale and Ryser). *Let*

$$S=(s_1,s_2,\ldots,s_m)\quad \textit{and}\quad R=(r_1,r_2,\ldots,r_t)$$

be nonnegative integral vectors. Assume that $s_1\geqslant s_2\geqslant\cdots\geqslant s_m$ *and* $r_1\geqslant r_2\cdots\geqslant r_t$. *Assume that* $s_i\leqslant t$, $i=1,\ldots,m$. *Then there exists an* $m\times t$ $(0,1)$*-matrix with row sum vector S and column sum vector R if and only if* $R\preceq S'$.

Below we give a condition for an element $X_1^{s_1}\otimes X_2^{s_2}\otimes\cdots\otimes X_m^{s_m}$, belonging to the basis $\mathbb{E}$ of $\mathbb{Z}[X_1]\otimes\cdots\otimes\mathbb{Z}[X_m]$, to occur in the expression of $\left(\sum_{\omega\in Q_{k,m}}\delta_\omega(\mathbb{X})\right)^t$ referred in Proposition 1.

Let $\mathbb{N}_0$ be the set of nonnegative integers.

Proposition 2. *Let k, m and b be as before and t be a positive integer. Let $S = (s_1, \ldots, s_m)$ be a sequence of nonnegative integers such that*

$$s_1 + \cdots + s_m = kt.$$

Then the system in the variables $(x_{\omega_1}, \ldots, x_{\omega_b})$

$$\sum_{\omega \in \Delta_i} x_\omega = s_i, \quad i = 1, \ldots, m, \tag{1}$$

is solvable in $\mathbb{N}_0$ if and only if

$$s_i \leqslant t, \quad i = 1, \ldots, m. \tag{2}$$

Proof. Let $\omega \in Q_{k,m}$.We are going to denote by $\square_\omega = (c_{i1}^{(\omega)})$ the (0, 1)-matrix of type $m \times 1$ over $\mathbb{F}$, where

$$c_{i1}^{(\omega)} = \begin{cases} 1 & \text{if } i \in \operatorname{Im}(\omega) \text{ (i.e. } \omega \in \Delta_i\text{)}, \\ 0 & \text{otherwise.} \end{cases}$$

Let us start by writing the system (2.1) in the matricial form

$$\left[\square_{\omega_1} \square_{\omega_2} \cdots \square_{\omega_b}\right] \mathscr{X} = \mathscr{S},$$

where the coefficient matrix is a (0, 1)-matrix of type $m \times b$, $\mathscr{X}$ is the column matrix of the indeterminates x_{w_j}'s and $\mathscr{S}$ is the column matrix of the s_j's, which is equivalent to

$$x_{w_1} \square_{\omega_1} + x_{w_2} \square_{\omega_2} + \cdots + x_{w_b} \square_{\omega_b} = \mathscr{S}. \tag{3}$$

If $(q_{\omega_1}, \ldots, q_{\omega_b})$ is a solution of (2.1), then we can construct the following (0, 1)-matrix

$$\mathscr{M} = \begin{bmatrix} \underbrace{\square_{\omega_1} \cdots \square_{\omega_1}}_{q_{\omega_1}} \underbrace{\square_{\omega_2} \cdots \square_{\omega_2}}_{q_{\omega_2}} \cdots \underbrace{\square_{\omega_b} \cdots \square_{\omega_b}}_{q_{\omega_b}} \end{bmatrix}$$

with vector row sum $(s_1, \ldots, s_m)$ (this follows from (2.3)). By assumption $s_1 + \cdots + s_m = kt$, and thus the matrix above has exactly kt entries equal to 1. Now each of its columns $\square_{\omega_j}$ has m lines and k entries equal to 1. Therefore $\mathscr{M}$ is an $m \times t$ matrix (in particular, $\sum q_{\omega_j} = t$).

Then since $\mathscr{M}$ has t columns inequalities (2) hold.

Suppose that inequalities (2) hold. Then we have

$$(\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_m) \preceq (\underbrace{t, t, \ldots, t}_{k \text{ times}}).$$

Using Gale and Ryser theorem, we can conclude that there exists a (0, 1)-matrix, $\mathscr{M}$, of type $m \times t$ such that the sum of each column is k and the sum of row i is s_i,

$i = 1, \ldots, m$. Therefore, for each column C_i of $\mathscr{M}$ there exists an $\omega \in Q_{k,m}$ such that $C_i = \mathbb{I}_\omega$. Denote by q_ω the number of columns of $\mathscr{M}$ equal to $\mathbb{I}_\omega$. It is now easy to conclude that $(q_{\omega_1}, q_{\omega_2}, \ldots, q_{\omega_b})$ is a solution of (1). □

Using the arguments of the former proof we can conclude the following theorem.

Theorem 3.

(a) *Let k, m and b be as before and t be a positive integer. Let $\mathscr{S} = (s_1, \ldots, s_m)$ be a sequence of nonnegative integers such that $s_1 + \cdots + s_m = kt$.*
Then, the element $X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m}$ of the basis $\mathbb{E}$ occurs in the expansion of

$$\left(\sum_{\omega \in Q_{k,m}} \delta_\omega(X_1, \ldots, X_m) \right)^t$$

if and only if the sequence $\mathscr{S}$ satisfies

$$s_i \leqslant t, \quad i = 1, \ldots, m.$$

(b) *If the term $X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m}$ does occur, its coefficient is equal to the number of* (0, 1)*-matrices of type $m \times t$ with row sums equal to $(s_1, \ldots, s_m)$ whose column sums are equal to k.*

Proof. Statement (a) is an immediate consequence of Propositions 1 and 2. So now we concentrate on (b).

Let

$$Q_{k,m} = \{\omega_1, \ldots, \omega_b\}.$$

It is easy to see that

$$\left(\sum_{\omega \in Q_{k,m}} \delta_\omega(\mathbb{X}) \right)^t = \sum_{\alpha \in \Gamma_{t,b}} \delta_{\omega_{\alpha(1)}}(X_1, \ldots, X_m) \cdots \delta_{\omega_{\alpha(t)}}(X_1, \ldots, X_m).$$

Let $\alpha \in \Gamma_{t,b}$. Define

$$\begin{aligned} \Delta_{\alpha,i} &= \left\{ j \in \{1, \ldots, t\} \mid i \in \operatorname{Im}(\omega_{\alpha(j)}) \right\}, \\ \mathscr{G} &= \left\{ \alpha \in \Gamma_{t,b} \mid S = (|\Delta_{\alpha,1}|, |\Delta_{\alpha,2}|, \ldots, |\Delta_{\alpha,m}|) = (s_1, \ldots, s_m) \right\}, \end{aligned}$$

and

$$M_t(S; k) = \text{The set of all } (0, 1) - \text{matrices of type } m \times t \text{ with row sum vector } S \text{ and column sum vector } (\underbrace{k, \ldots, k}_{t \text{ times}}).$$

Then, since

$$\delta_{\omega_{\alpha(1)}}(\mathbb{X})\cdots\delta_{\omega_{\alpha(t)}}(\mathbb{X}) = X_1^{|\Delta_{\alpha,1}|}\otimes X_2^{|\Delta_{\alpha,2}|}\otimes\cdots\otimes X_m^{|\Delta_{\alpha,m}|},$$

the coefficient of $X_1^{s_1}\otimes X_2^{s_2}\otimes\cdots\otimes X_m^{s_m}$ in the expansion of $\left(\sum_{\omega\in Q_{k,m}}\delta_\omega(\mathbb{X})\right)^t$ is equal to $|\mathcal{G}|$.

From now on, assume $S=(s_1,\ldots,s_m)$ and define

$$\begin{aligned}\Lambda : \mathcal{G} &\longrightarrow M_t(S;k)\\ \alpha &\longmapsto \Lambda(\alpha),\end{aligned}$$

where

$$\Lambda(\alpha) = \left[\mathbb{1}_{\omega_{\alpha(1)}}\mathbb{1}_{\omega_{\alpha(2)}}\cdots\mathbb{1}_{\omega_{\alpha(t)}}\right],$$

with $\mathbb{1}_{\omega_i} = (c_{i1}^{(\omega_i)})$ as defined in the proof of the previous proposition.

This map Λ is well defined for the sum of the ith line of $\Lambda(\alpha)$ which is equal to

$$\sum_{j=1}^{t} c_{i1}^{(\omega_{\alpha(j)})} = |\{j \mid \omega_{\alpha(j)}\in\Delta_i\}| = |\{j \mid i\in\operatorname{Im}(\omega_{\alpha(j)})\}| = |\Delta_{\alpha,i}|,$$

and each $\mathbb{1}_{\omega_i}$ has exactly k entries equal to 1.

To conclude this proof, we need to show that Λ is a bijection. If $\alpha,\beta\in\mathcal{G}$ and, for some j, $\alpha(j)\neq\beta(j)$, then $\mathbb{1}_{\omega_{\alpha(j)}}\neq\mathbb{1}_{\omega_{\beta(j)}}$. So Λ is 1–1.

Now take $B=[C_1,\ldots,C_t]\in M_t(S;k)$. Since the sum of each column C_j is equal to k, there exists a unique ω_i such that $C_j=\mathbb{1}_{\omega_i}$. Now it is easy to define α such that $B=[\mathbb{1}_{\omega_{\alpha(1)}}\cdots\mathbb{1}_{\omega_{\alpha(t)}}]$. □

Theorem 4. *Suppose that the term $X_1^{s_1}\otimes X_2^{s_2}\otimes\cdots\otimes X_m^{s_m}\in\mathbb{E}$ occurs with a coefficient $\mathcal{C}_s$ in the expansion of*

$$\left(\sum_{\omega\in Q_{k,m}}\delta_\omega(\mathbb{X})\right)^t.$$

Then $X_1^{t-s_1}\otimes X_2^{t-s_2}\otimes\cdots\otimes X_m^{t-s_m}\in\mathbb{E}$ occurs with the same coefficient $\mathcal{C}_s$ in the expansion of

$$\left(\sum_{\omega\in Q_{m-k,m}}\delta_\omega(\mathbb{X})\right)^t.$$

Proof. Using Propositions 1 and 2 we see that $X_1^{s_1}\otimes X_2^{s_2}\otimes\cdots\otimes X_m^{s_m}$ occurs in $\left(\sum_{\omega\in Q_{k,m}}\delta_\omega(\mathbb{X})\right)^t$ if and only if $X_1^{t-s_1}\otimes X_2^{t-s_2}\otimes\cdots\otimes X_m^{t-s_m}$ occurs in $\left(\sum_{\omega\in Q_{m-k,m}}\delta_\omega(\mathbb{X})\right)^t$. Using Theorem 3 we can see that it is enough to prove that if $S=(s_1,\ldots,s_m)$,

$$|M_t(S,k)| = |M_t((t-s_1,\ldots,t-s_m),m-k)|$$

to conclude the proof.

Given a (0, 1)-matrix $A=(a_{ij})$ denote by $\overline{A}=(\overline{a}_{ij})$ the (0, 1)-matrix of the same type than A such that $\overline{a}_{ij}=1-a_{ij}$. It is easy to see that if $A\in M_t(S,k)$, then $\overline{A}\in M_t((t-s_1,\ldots,t-s_m),m-k)$.

Since the mapping from $M_t(S,k)$ into $M_t((t-s_1,\ldots,t-s_m),m-k)$, $A\to\overline{A}$, is an involution ($\overline{\overline{A}}=A$), then it is bijective and the theorem follows. □

For some special values of k, it is possible to determine explicitly the coefficient of $X_1^{s_1}\otimes X_2^{s_2}\otimes\cdots\otimes X_m^{s_m}$. These special cases are treated in the following proposition.

Proposition 3. *Suppose that the term $X_1^{s_1}\otimes X_2^{s_2}\otimes\cdots\otimes X_m^{s_m}\in\mathbb{E}$ occurs with a coefficient $\mathscr{C}_s$ in the expansion of*

$$\left(\sum_{\omega\in Q_{k,m}}\delta_\omega(\mathbb{X})\right)^t.$$

Then,

(a) *if $k=1$, we have*

$$\mathscr{C}_s=\frac{t!}{s_1!s_2!\cdots s_m!},$$

(b) *if $k=m-1$, we have*

$$\mathscr{C}_s=\frac{t!}{(t-s_1)!(t-s_2)!\cdots(t-s_m)!}.$$

Proof. For $k=1$ we have $Q_{1,m}=\{\omega_1,\omega_2,\ldots,\omega_m\}$ and $\Delta_i=\{\omega_i\}$. Hence (see Proposition 1) there is only one solution for the system

$$\sum_{\omega\in\Delta_i}n_\omega=s_i\quad(i=1,\ldots,m)$$

that is, the solution $n_{\omega_i}=s_i$, which gives the result (a) above.

Case (b) follows from (a) and Theorem 4. □

Corollary 2. *With the same notations presented in the proof of Theorem* 3, *we have*

(a) $|M_t(S;1)|=\frac{t!}{s_1!s_2!\cdots s_m!}$,

(b) $|M_t(S;m-1)|=\frac{t!}{(t-s_1)!(t-s_2)!\cdots(t-s_m)!}$.

So far we have established results in the $\mathbb{Z}$-algebra $\mathbb{Z}[X_1]\otimes\cdots\otimes\mathbb{Z}[X_m]$. Next we present a relation between this $\mathbb{Z}$-algebra and the $\mathbb{F}$-algebra $\mathbb{F}[X_1]\otimes\cdots\otimes\mathbb{F}[X_m]$, and how to interpret the previous results in this new algebra.

Let $E_{\mathbb{F}}$ be the basis of $\mathbb{F}[X_1]\otimes\cdots\otimes\mathbb{F}[X_m]$ induced by the bases

$$\{X_i^n \mid n\in\mathbb{N}_0\}$$

of $\mathbb{F}[X_i]$, $i = 1, \ldots, m$. Given $X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m} \in E_{\mathbb{F}}$ we call *degree* of $X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m}$ to the integer $s_1 + \cdots + s_m$.

Denote by $1_{\mathbb{F}}$ the identity of $\mathbb{F}$. Consider the $\mathbb{Z}$-algebra homomorphism ϕ from $\mathbb{Z}$ into $\mathbb{F}$ defined by

$$n \longmapsto \underbrace{1_{\mathbb{F}} + 1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}_{n \text{ times}}.$$

Let ϕ_i be its canonical extension from $\mathbb{Z}[X_i]$ into $\mathbb{F}[X_i]$

$$aX_i^m \longmapsto \phi(a)X_i^m.$$

Then

$$\Phi = \phi_1 \otimes \phi_2 \otimes \cdots \otimes \phi_m$$

is a $\mathbb{Z}$-algebra homomorphism [1, p. A.III.34] from $\mathbb{Z}[X_1] \otimes \cdots \otimes \mathbb{Z}[X_m]$ into $\mathbb{F}[X_1] \otimes \cdots \otimes \mathbb{F}[X_m]$.

Let us define

$$D_{k,m}(X_1, \ldots, X_m) = \Phi\left(\sum_{\omega \in Q_{k,m}} \delta_\omega(X_1, \ldots, X_m)\right).$$

The next lemma summarizes the important properties of $D_{k,m}(X_1, \ldots, X_m)$, and is a straightforward consequence of its definition.

Lemma 1. *The following equalities hold*:

(i) $\Phi(a_S\, X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m}) = \phi(a_S)\, X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m}$.

(ii) $\Phi\left(\left(\sum_{\omega \in Q_{k,m}} \delta_\omega(X_1, \ldots, X_m)\right)^t\right) = D_{k,m}(X_1, \ldots, X_m)^t$.

(iii) *Let $S = (s_1, \ldots, s_m)$ be a sequence of nonnegative integers satisfying $s_1 + s_2 + \cdots + s_m = kt$. If $\mathscr{C}_S$ is the coefficient of $X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m}$ in the expression of $\left(\sum_{\omega \in Q_{k,m}} \delta_\omega(X_1, \ldots, X_m)\right)^t$ as linear combination of the elements of $\mathbb{E}$, then $\phi(\mathscr{C}_S)$ is the coefficient of $X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m}$ in the expression of $D_{k,m}(X_1, \ldots, X_m)^t$ as linear combination of the elements of $E_{\mathbb{F}}$.*

3. The cyclic subspace $\langle s_k(T_1, \ldots, T_m)^t \rangle$

It is well known that if $\{I, T_i, T_i^2, \ldots, T_i^{l_i - 1}\}$ is a basis of the cyclic $\mathbb{F}$-subalgebra $\langle T_i \rangle$ of $L(V_i, V_i)$, $i = 1, \ldots, m$, then $l_i = \deg P_{T_i}$ and

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

is a basis of $\langle T_1 \rangle \otimes \langle T_2 \rangle \otimes \cdots \otimes \langle T_m \rangle$. If $Z = T_1^{e_1} \otimes \cdots \otimes T_m^{e_m} \in \mathscr{B}$, we say that $\sum_{i=1}^m e_i$ is the weight of Z. Define ℓ to be

$$\ell = \left\lfloor \frac{l_1 + l_2 + \cdots + l_m - m}{k} \right\rfloor + 1.$$

Let t be an integer less than or equal to $\ell - 1$, and $l_i' = \min\{t+1, l_i\}$, $i = 1, \ldots, m$. Let ρ_t be the integer satisfying

$$(l_1' - 1) + \cdots + (l_{\rho_t - 1}' - 1) < kt \tag{4}$$

and

$$(l_1' - 1) + \cdots + (l_{\rho_t}' - 1) \geqslant kt. \tag{5}$$

Define $(\theta_{t,1}, \ldots, \theta_{t,m})$ as a m-tuple of nonnegative integers such that

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

Let us define $h_{k,t}$ to be the number of (0, 1) matrices with row sums equal to $(\theta_{t,1}, \ldots, \theta_{t,m})$, and whose column sums are equal to k for $t = 0, 1, \ldots, \ell - 1$.

Now define

$$z_t = X_1^{\theta_{t,1}} \otimes X_2^{\theta_{t,2}} \otimes \cdots \otimes X_m^{\theta_{t,m}}$$

and

$$Z_t = T_1^{\theta_{t,1}} \otimes T_2^{\theta_{t,2}} \otimes \cdots \otimes T^{\theta_{t,m}}, \quad t = 0, \ldots, \ell - 1.$$

Our purpose is to decide if Z_t belongs to the support of $s_k(T_1, \ldots, T_m)$ and get, from this, information on the linear independence of families of type

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

Lemma 2. *Z_t is an element of $\mathscr{B}$ of weight kt for every $t = 1, \ldots, \ell - 1$.*

Proof. Let us start by pointing out that the weight of Z_t is $\theta_{t,1} + \theta_{t,2} + \cdots + \theta_{t,m} = kt$. By construction we have $\theta_{t,i} \leqslant l_i - 1$ and the lemma follows. □

Lemma 3. *The element Z_t occurs in the expression of $s_k(T_1, \ldots, T_m)^t$ as a linear combination of $\mathscr{B}$ with $\phi(h_{k,t})$ as its coefficient.*

Proof. Let $\mathscr{A} = \langle T_1 \rangle \otimes \langle T_2 \rangle \otimes \cdots \otimes \langle T_m \rangle$ (the subalgebra of $L(V_1, V_1) \otimes \cdots \otimes L(V_m, V_m)$). Let ψ be $\mathbb{F}$-algebra homomorphism from $\mathbb{F}[X_1] \otimes \cdots \otimes \mathbb{F}[X_m]$ into $\mathscr{A}$, obtained by

$$X_1^{e_1} \otimes \cdots \otimes X_m^{e_m} \longmapsto T_1^{e_1} \otimes \cdots \otimes T_m^{e_m}$$

(cf. [10, p. 98]). Let $\mathscr{H}_t$ be the set of elements of $E_{\mathbb{F}}$ of degree t and $\mathscr{W}_t$ the elements of $\mathscr{B}$ of weight t. Let $L = (l_1 - 1, \ldots, l_m - 1)$, and denote by Υ_L the set of all elements $X_1^{s_1} \otimes X_2^{s_2} \otimes \cdots \otimes X_m^{s_m}$ of $E_{\mathbb{F}}$ satisfying $s_i \leqslant l_i - 1$, $i = 1, \ldots, m$. The following can be easily obtained:

(a) $s_k(T_1, \ldots, T_m)^t = \psi\left(D_{k,m}(X_1, \ldots, X_m)^t\right)$,
(b) if $z \in \mathscr{H}_t \cap \Upsilon_L$, then $\psi(z) \in \mathscr{W}_t$,
(c) if $z \in \mathscr{H}_t \cap (E_{\mathbb{F}} \backslash \Upsilon_L)$, then $\psi(z) \in \bigcup_{i=0}^{t-1} \mathscr{W}_i$.

Let $M = \underbrace{(t, \ldots, t)}_{m \text{ times}}$. Bearing in mind Theorem 3 and Lemma 1 we know that

$$(D_{k,m}(X_1, \ldots, X_m))^t = \sum_{z \in \mathscr{H}_{kt} \cap \Upsilon_M} \phi\left(\mathscr{C}_z\right) z, \tag{6}$$

with $0 \neq \mathscr{C}_z \in \mathbb{N}$.

Using (a), (b) and (c) we get

$$\begin{aligned} s_k(T_1, \ldots, T_m)^t &= \psi\left(D_{k,m}(X_1, \ldots, X_m)^t\right) \\ &= \psi\left(\sum_{z \in \mathscr{H}_{kt} \cap \Upsilon_L} \phi(\mathscr{C}_z) z + \sum_{z \in \mathscr{H}_{kt} \cap (\Upsilon_M \backslash \Upsilon_L)} \phi(\mathscr{C}_z) z\right) \\ &= \sum_{z \in \mathscr{H}_{kt} \cap \Upsilon_L} \phi(\mathscr{C}_z)\psi(z) + \sum_{z \in \mathscr{H}_{kt} \cap (\Upsilon_M \backslash \Upsilon_L)} \phi(\mathscr{C}_z)\psi(z). \end{aligned}$$

If we define $Z = \psi(z)$, we get from these equalities the following:

$$s_k(T_1, \ldots, T_m)^t = \sum_{Z \in \mathscr{W}_{kt}} \phi(\mathscr{C}_z) Z + Y, \tag{7}$$

where Y is a linear combination of elements of $\mathscr{B}$ of weight less than t.

By construction, $z_t \in \mathscr{H}_{kt} \cap \Upsilon_M$, hence it occurs in $D_{k,m}(X_1, \ldots, X_m)^t$ with the coefficient $\phi(h_{k,m})$ (see (6)). Therefore $Z_t = \psi(z_t)$ occurs in $s_k(T_1, \ldots, T_m)^t$ with the same coefficient (see (7)), concluding this proof. □

Theorem 5. *Let $0 \leqslant s \leqslant \ell - 1$. If p (the characteristic of $\mathbb{F}$) does not divide $h_{k,t}$ for $t = 0, \ldots, s$, then the degree of the minimal polynomial of $s_k(T_1, \ldots, T_m)$ is greater than or equal to $s + 1$.*

Proof. From the hypothesis we have that the coefficient $\phi(h_{k,t})$ is different from zero. Since every element of $\mathscr{B}$ that occurs in $s_k(T_1, \ldots, T_m)$ has weight less than or equal to kt, we can deduce, from Lemmas 2 and 3, that for every $t \leqslant s$ the support of $s_k(T_1, \ldots, T_m)$ contains an element $Z_t \in \mathscr{B}$ that does not belong to the support of any other power (less than t) of $s_k(T_1, \ldots, T_m)$.

Hence we have that

$$I, s_k(T_1, \ldots, T_m), s_k(T_1, \ldots, T_m)^2, \ldots, s_k(T_1, \ldots, T_m)^s$$

are linearly independent in $L(V_1 \otimes V_2 \otimes \cdots \otimes V_m, V_1 \otimes V_2 \otimes \cdots \otimes V_m)$. Therefore the degree of the minimal polynomial of $s_k(T_1, \ldots, T_m)$ is greater than or equal to $s + 1$. □

Corollary 3. *Let $d_{k,m}$ be the degree of the minimal polynomial of $s_k(T_1, \ldots, T_m)$. Then,*

(1) $d_{1,m} \geqslant \min\left\{p, \deg P_{T_1} + \deg P_{T_2} + \cdots + \deg P_{T_m} - m + 1\right\}.$

(2) $d_{m-1,m} \geqslant \min\left\{p, \left\lfloor \frac{\deg P_{T_1} + \deg P_{T_2} + \cdots + \deg P_{T_m} - m}{m-1} \right\rfloor + 1\right\}.$

Proof. Using the same type of arguments that have been used in the proof of Theorem 5 and bearing in mind Proposition 3 where the coefficients for these special cases are explicitly calculated, we conclude the corollary. □

Proposition 4. *If $h_{t,k} \mid (kt)!$, $t = 0, \ldots, \ell - 1$, then the degree of the minimal polynomial of $s_k(T_1, \ldots, T_m)$ is greater than or equal to*

$$\min\left\{\left\lfloor \frac{p}{k} \right\rfloor, \left\lfloor \frac{\deg P_{T_1} + \deg P_{T_2} + \cdots + \deg P_{T_m} - m}{k} \right\rfloor + 1\right\}.$$

Proof. Observe that if $t < \lfloor p/k \rfloor$, we have $kt < p$ therefore $p \not| (kt)!$ Thus, by hypothesis, p does not divide $h_{k,t}$ for $t = 0, \ldots, \min\{\lfloor p/k \rfloor, \lfloor \ell \rfloor\}$. Now apply Theorem 5. □

Lemma 4. *Let*

$$\ell' = \left\lfloor \frac{\deg P_{T_1} + \deg P_{T_2} + \cdots + \deg P_{T_m} - m}{m-k} \right\rfloor + 1.$$

If $h_{j,k} \mid (kj)!$, $j = 0, \ldots, \ell - 1$, then $h_{j,m-k} \mid (kj)!$, $j = 0, \ldots, \ell' - 1$.

Proof. This is a consequence of Theorem 4. □

Remark. There are reasons to think that the conditions of Proposition 4 hold or at least happen very often. Although there are several results (e.g. [8,12]) on the number of (0, 1)-matrices $m \times n$ with prescribed row and column sums (for instance in [8, p. 204 Ex. 19] a formula is obtained that expresses this number in terms of the so called Kostka numbers), the authors were unable to characterize the cases where the conditions of Proposition 4 are implemented using this formula.

4. Additive results

We are now in a position to present lower bounds for the cardinality of the set

$$|s_k(A_1, \ldots, A_m)|.$$

These lower bounds are pointing to a generalization of the Cauchy–Davenport Theorem, which in our notation can be written as

$$\begin{aligned}|A_1 + \cdots + A_m| &= |s_1(A_1, \ldots, A_m)| \\ &\geqslant \min\left\{p, |A_1| + |A_2| + \cdots + |A_m| - m + 1\right\}.\end{aligned}$$

For the following results, we are assuming all the notations and definitions presented in Section 3.

Theorem 6. *Let m, k be positive integers and $k \leqslant m$. Assume that p does not divide $h_{k,t}$ for $t = 0, \ldots, \ell - 1$. Let $A_1, \ldots, A_m$ be finite subsets of $\mathbb{F}$. Then*

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

Proof. Assume that $|A_i| = l_i, i = 1, \ldots, m$. Let T_i be a diagonal linear operator on a vector space V_i of dimension l_i over $\mathbb{F}$, whose set of eigenvalues is $A_i, i = 1, \ldots, m$. We know from Corollary 1 that

$$|\sigma(s_k(T_1, \ldots, T_m))| = |s_k(A_1, \ldots, A_m)|.$$

Since $s_k(T_1, \ldots, T_m)$ is diagonal (see Theorem 1),

$$\deg(P_{s_k(T_1,\ldots,T_m)}) = |\sigma(s_k(T_1, \ldots, T_m))| = |s_k(A_1, \ldots, A_m)|.$$

Therefore, by Theorem 5, we conclude that

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

Theorem 7. *Let m, k be positive integers and $k \leqslant m$. Assume that $h_{j,k} \mid (kj)!$, $j = 0, \ldots, \ell - 1$. Let $A_1, \ldots, A_m$ be finite subsets of $\mathbb{F}$. Then*

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

Proof. The proof can be carried out by using Proposition 4 and arguments similar to the ones used in Theorem 6. □

The following result presents a generalization of the Cauchy–Davenport theorem for the symmetric polynomial $s_{m-1}(X_1, \ldots, X_m)$ applied on the family of sets $A_1, \ldots, A_m$. The first inequality follows also immediately from Cauchy–Davenport by an induction argument.

Theorem 8. *Let m be a positive integer. Let $A_1, \ldots, A_m$ be finite subsets of $\mathbb{F}$. Then*

$$|A_1 + \cdots + A_m| \geqslant \min\left\{p, |A_1| + |A_2| + \cdots + |A_m| - (m - 1)\right\}.$$

and

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

Proof. The proof is a consequence of Corollary 2, using arguments similar to the ones presented in Theorem 6. □

Acknowledgements

The authors thank Richard Brualdi for his comments on the question of finding the number of (0, 1)-matrices, and for providing Ref. [12].

References

[1] N. Bourbaki, Éléments de Mathématique, Algèbre Chapitres 1 à 3, Hermann, Paris, 1970.

[2] R.A. Brualdi, H.J. Ryser, Combinatorial Matrix Theory, Cambridge University Press, Cambridge, 1991.

[3] C. Caldeira, Critical pairs of matrices for the degree of the minimal polynomial of the Kronecker sum, Linear and Multilinear Algebra 42 (1997) 72–88.

[4] C. Caldeira, J.A. Dias da Silva, A pollard type result for restricted sums, J. Number Theory 72 (1998) 153–173.

[5] C. Caldeira, J.A. Dias da Silva, The invariant polynomials degrees of the Kronecker sum of two linear operators and additive theory (preprint).

[6] J.A. Dias da Silva, Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, Bull. London Math. Soc. 26 (1994) 140–146.

[7] J.A. Dias da Silva, Y.O. Hamidoune, A note on the minimal polynomial of the Kronecker sum of two linear operators, Linear Algebra Appl. 141 (1990) 283–287.

[8] W. Fulton, Young Tableaux, London Mathematical Society, Student Texts, Cambridge University Press, Cambridge, 1997.

[9] G. James, A. Kerber, The Representation Theory of the Symmetric Group, Encyclopedia of Mathematics and its Applications, Addison-Wesley, Reading MA, 1981.

[10] S. Lang, Algebra, third ed., Addison-Wesley, Reading, MA, 1993.

[11] M. Marcus, Finite Dimensional Multilinear Algebra, Part 1, Marcel Dekker, New York, 1973.

[12] B.D. McKay, Asymptotics for 0–1 Matrices with Prescribed Line Sums Enumeration and Design (Waterloo, Ont., 1982), Academic Press, Toronto, Ont., 1984, pp. 225–238.

[13] R. Spiegler, An application of group theory to matrices and to ordinary differential equations, Linear Algebra Appl. 44 (1982) 143–151.