



ELSEVIER

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Linear Algebra and its Applications 401 (2005) 11–27

LINEAR ALGEBRA
AND ITS
APPLICATIONS

www.elsevier.com/locate/laa

Generalized derivations restricted to Grassmann spaces and additive theory

Cristina Caldeira¹

Departamento de Matemática, Universidade de Coimbra, Apartado 3008, 3001-454 Coimbra, Portugal

Received 18 November 2002; accepted 14 April 2003

Available online 11 July 2003

Submitted by J. Queiró

Abstract

We obtain a lower bound for the degree of the minimal polynomial of generalized derivations related to the elementary symmetric functions, restricted to Grassmann spaces. That lower bound is used to obtain an additive number theory result.

© 2003 Elsevier Inc. All rights reserved.

AMS classification: 15A69

Keywords: Generalized derivations; Additive number theory

1. Introduction

Let \mathbb{F} be an arbitrary field and let p be the characteristic of \mathbb{F} in non-zero characteristic and $p = +\infty$ otherwise. Throughout this paper k and m are fixed positive integers such that $p > m \geq k$.

Let r and n be positive integers. By $\Gamma_{r,n}$ we denote the set of all maps from $\{0, 1, \dots, r-1\}$ in $\{0, 1, \dots, n-1\}$. If $\alpha \in \Gamma_{r,n}$ we use the r -tuple notation for α , that is, $\alpha = (\alpha(0), \alpha(1), \dots, \alpha(r-1))$. By $\text{Im}(\alpha)$ we denote the range of α and the *weight* of α is $w(\alpha) = \alpha(0) + \dots + \alpha(r-1)$. $Q_{r,n}$ denotes the subset of $\Gamma_{r,n}$ consisting of strictly increasing maps.

E-mail address: caldeira@mat.uc.pt (C. Caldeira).

¹ This research was done within the activities of Centro de Matemática da Universidade de Coimbra.

Let X_0, X_1, \dots, X_{m-1} be m distinct indeterminates. The k th elementary symmetric function on these indeterminates is

$$s_k(X_0, X_1, \dots, X_{m-1}) = \sum_{\omega \in Q_{k,m}} X_{\omega(0)} X_{\omega(1)} \cdots X_{\omega(m-1)}.$$

Let $A = \{a_0, a_1, \dots, a_{n-1}\}$ be a finite non-empty subset of \mathbb{F} , such that $|A| = n \geq m$, where $|A|$ denotes the cardinality of A .

By $s_k^\wedge(A)$ we denote the set

$$\{s_k(a_{\alpha(0)}, a_{\alpha(1)}, \dots, a_{\alpha(m-1)}) : \alpha \in Q_{m,n}\}.$$

For example,

$$s_1^\wedge(A) = \left\{ \sum_{i=0}^{m-1} a_{\alpha(i)} : \alpha \in Q_{m,n} \right\}$$

is the set, $\wedge^m A$, of restricted sums of m elements of A (see [1]) and

$$s_m^\wedge(A) = \left\{ \prod_{i=0}^{m-1} a_{\alpha(i)} : \alpha \in Q_{m,n} \right\}.$$

Erdős and Heilbronn conjectured that, for $\mathbb{F} = \mathbb{Z}_p$,

$$|\wedge^2 A| \geq \min\{p, 2|A| - 3\}.$$

This lower bound was established by Dias da Silva and Hamidoune in 1994 (see [1]). They proved that, for an arbitrary field,

$$|\wedge^m A| \geq \min\{p, m(|A| - m) + 1\}. \quad (1)$$

Let V be a finite dimensional vector space over \mathbb{F} such that $\dim V \geq m$. Let S_m be the symmetric group of degree m . For convenience of notation we consider the elements of S_m as permutations of elements of $\{0, 1, \dots, m-1\}$. For $\sigma \in S_m$, $P(\sigma)$ denotes the unique linear operator on the m th tensor power product of V , $\otimes^m V$, such that

$$P(\sigma)(v_0 \otimes v_1 \otimes \cdots \otimes v_{m-1}) = v_{\sigma^{-1}(0)} \otimes v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(m-1)},$$

for all $v_0, v_1, \dots, v_{m-1} \in V$.

Let ε be the alternating character on S_m . Consider the symmetrizer defined on $\otimes^m V$ by

$$T_\varepsilon = \frac{1}{m!} \sum_{\sigma \in S_m} \varepsilon(\sigma) P(\sigma)$$

and let $\wedge^m V$ denote its range ($\wedge^m V$ is the m th Grassmann space of V). For $v_0, v_1, \dots, v_{m-1} \in V$, $v_0 \wedge v_1 \wedge \cdots \wedge v_{m-1}$ denotes $T_\varepsilon(v_0 \otimes v_1 \otimes \cdots \otimes v_{m-1})$.

For g a linear operator on a vector space over \mathbb{F} , P_g denotes the minimal polynomial of g and $\deg(P_g)$ denotes its degree. The spectrum of g , i.e., the set of all eigenvalues of g in the algebraic closure of \mathbb{F} , is denoted by $\sigma(g)$.

Let f be a linear operator on V . The derivation associated with f is the linear operator on $\otimes^m V$,

$$f \otimes I_V \otimes \cdots \otimes I_V + I_V \otimes f \otimes \cdots \otimes I_V + \cdots + I_V \otimes I_V \otimes \cdots \otimes f.$$

The derivation associated with f commutes with T_ε [4, Section 3.2]. Hence, $\wedge^m V$ is an invariant subspace of the derivation associated with f . Let $D(f)$ denote the restriction of the derivation associated with f to $\wedge^m V$. Dias da Silva and Hamidoune proved (see [1]) that

$$\deg(P_{D(f)}) \geq \min\{p, m(\deg(P_f) - m) + 1\}. \tag{2}$$

Since $\sigma(D(f)) = \wedge^m \sigma(f)$, Dias da Silva and Hamidoune obtained (1) from (2), considering linear operators of simple structure.

Using the same method we are going to obtain a lower bound for the cardinality of $s_k^\wedge(A)$ that generalizes (1). We will prove that, in certain conditions, for $M \in \mathbb{N}$,

$$|s_k^\wedge(A)| \geq \min \left\{ M, \left\lfloor \frac{m(|A| - m)}{k} \right\rfloor + 1 \right\}, \tag{3}$$

where, for $x \in \mathbb{R}$, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x .

For $k = 1$ we can take $M = p$ and the lower bound given by (3) is just (1).

Suppose V_0, V_1, \dots, V_{m-1} are finite dimensional vector spaces over \mathbb{F} and, for $i = 0, 1, \dots, m - 1$, f_i is a linear operator on V_i . For $\omega \in Q_{k,m}$ let

$$\delta_\omega(f_0, f_1, \dots, f_{m-1}) = g_0 \otimes g_1 \otimes \cdots \otimes g_{m-1},$$

where

$$g_i = \begin{cases} f_i & \text{if } i \in \text{Im}(\omega) \\ I_{V_i} & \text{if } i \notin \text{Im}(\omega) \end{cases}, \quad i = 0, 1, \dots, m - 1,$$

and consider the linear operator on $V_0 \otimes V_1 \otimes \cdots \otimes V_{m-1}$

$$s_k(f_0, f_1, \dots, f_{m-1}) = \sum_{\omega \in Q_{k,m}} \delta_\omega(f_0, f_1, \dots, f_{m-1}).$$

In [2] Dias da Silva and Godinho established a lower bound for the degree of the minimal polynomial of $s_k(f_0, f_1, \dots, f_{m-1})$. They have proved that, in certain conditions,

$$\deg(P_{s_k(f_0, f_1, \dots, f_{m-1})}) \geq \min \left\{ \left\lfloor \frac{p}{k} \right\rfloor, \left\lfloor \frac{\sum_{i=0}^{m-1} \deg(P_{f_i}) - m}{k} \right\rfloor + 1 \right\}.$$

Since the mapping from $Q_{k,m}$ into the set of elements of $\Gamma_{m,2}$ with weight k , that to each $\omega \in Q_{k,m}$ assigns β defined by

$$\beta(i) = \begin{cases} 1 & \text{if } i \in \text{Im}(\omega) \\ 0 & \text{if } i \notin \text{Im}(\omega) \end{cases}, \quad i = 0, 1, \dots, m - 1,$$

is a bijection, we have that, for all $v_0 \in V_0, \dots, v_{m-1} \in V_{m-1}$,

$$\begin{aligned} s_k(f_0, f_1, \dots, f_{m-1})(v_0 \otimes v_1 \otimes \cdots \otimes v_{m-1}) \\ = \sum_{\substack{\beta \in \Gamma_{m,2} \\ w(\beta)=k}} f_0^{\beta(0)}(v_0) \otimes \cdots \otimes f_{m-1}^{\beta(m-1)}(v_{m-1}). \end{aligned}$$

Let $V_0 = V_1 = \dots = V_{m-1} = V$ and $f_0 = f_1 = \dots = f_{m-1} = f$. It is easy to prove that, for all $v_0, \dots, v_{m-1} \in V$,

$$\begin{aligned} s_k(f, f, \dots, f)(v_0 \wedge v_1 \wedge \dots \wedge v_{m-1}) \\ = \sum_{\substack{\beta \in \Gamma_{m,2} \\ w(\beta)=k}} f^{\beta(0)}(v_0) \wedge \dots \wedge f^{\beta(m-1)}(v_{m-1}). \end{aligned}$$

Therefore $\wedge^m V$ is an invariant subspace of $s_k(f, \dots, f)$. We denote by $s_k^\wedge(f)$ the restriction of $s_k(f, \dots, f)$ to $\wedge^m V$. For example,

$$s_1^\wedge(f)(v_0 \wedge v_1 \wedge \dots \wedge v_{m-1}) = \sum_{i=0}^{m-1} v_0 \wedge \dots \wedge v_{i-1} \wedge f(v_i) \wedge v_{i+1} \wedge \dots \wedge v_{m-1}$$

and

$$s_m^\wedge(f)(v_0 \wedge v_1 \wedge \dots \wedge v_{m-1}) = f(v_0) \wedge f(v_1) \wedge \dots \wedge f(v_{m-1}).$$

The linear operator $s_1^\wedge(f)$ is just the restriction of the derivation associated with f to $\wedge^m V$, $D(f)$. Following [1,2] we are going to obtain a lower bound for the degree of the minimal polynomial of $s_k^\wedge(f)$ that generalizes (2). We will prove that, in certain conditions, for $M \in \mathbb{N}$,

$$\deg(P_{s_k^\wedge(f)}) \geq \min \left\{ M, \left\lfloor \frac{m(\deg(P_f) - m)}{k} \right\rfloor + 1 \right\}. \quad (4)$$

This will be done in Section 3. In Section 4 we will show that, for some linear operators, f , we have $\sigma(s_k^\wedge(f)) = s_k^\wedge(\sigma(f))$. Using this fact, from (4) we will obtain (3). In order to do this we need to introduce some combinatorial definitions and results. This will be done in Section 2.

2. Combinatorial results

Most definitions in this section can be found in [3] or [6].

Let r be a non-negative integer. We say that $\mu = (\mu_0, \mu_1, \dots, \mu_t)$ is an *improper partition* of r if $\mu_0, \mu_1, \dots, \mu_t$ are non-negative integers and $\sum_{i=0}^t \mu_i = r$.

We say that $\lambda = (\lambda_0, \lambda_1, \dots, \lambda_t)$ is a *partition* of r if $\lambda_0 \geq \lambda_1 \geq \dots \geq \lambda_t$ are non-negative integers and $\sum_{i=0}^t \lambda_i = r$. If λ is a partition of r we write $\lambda \vdash r$. If k and t are positive integers then (k^t) denotes the partition of kt , $\underbrace{(k, k, \dots, k)}_t$.

The *length* of a partition λ , $\ell(\lambda)$, is the number of its non-zero terms and its *weight*, $w(\lambda)$, is the sum of its terms.

Let s be a positive integer. By $\mathcal{P}_{r,s}$ we denote the set of partitions of r with length at most s . We write the elements of $\mathcal{P}_{r,s}$ as s -tuples.

Consider $\lambda = (\lambda_0, \lambda_1, \dots, \lambda_t) \vdash r$. To λ there corresponds a *Young diagram*, $[\lambda]$, which consists of r boxes displayed in $\ell(\lambda)$ rows, the i th row consisting of λ_{i-1} boxes, for $i = 1, \dots, \ell(\lambda)$. The *conjugate partition* of λ is the partition of r ,

$$\lambda' = (\lambda'_0, \lambda'_1, \dots, \lambda'_{\lambda_0-1}),$$

where λ'_j is the number of boxes in the $(j + 1)$ th column of $[\lambda]$.

A *Young tableau* associated with $[\lambda]$, or λ -tableau, is obtained from $[\lambda]$ by filling in the boxes with the integers $0, 1, \dots, r - 1$ bijectively. A *generalized Young tableau* associated with $[\lambda]$, or generalized λ -tableau, is obtained from $[\lambda]$ by filling in the boxes with non-negative integers, repetitions allowed. Suppose t is the greatest integer appearing in a generalized Young tableau, Q . The *type* of Q is the improper partition of r , $\mu = (\mu_0, \mu_1, \dots, \mu_t)$ where μ_i is the number of i 's in Q . A generalized Young tableau is said to be *semistandard* if the integers are non-decreasing along each row and strictly increasing down each column. Mainly we will be interested in Young tableaux whose types are partitions.

Example 1. The generalized Young tableau, associated with $[(5, 3, 2, 1)]$,

0	0	0	1	3
1	1	2		
2	3			
4				

is semistandard and of type $(3, 3, 2, 2, 1)$.

Let λ and μ be two partitions of r . $\mathcal{F}_{\lambda, \mu}^0$ denotes the set of semistandard generalized λ -tableaux of type μ . The *Kostka number*, $K_{\lambda, \mu}$, is the cardinality of $\mathcal{F}_{\lambda, \mu}^0$. The aim of this section is to present two lemmas on Kostka numbers.

Let $v \in \mathcal{P}_{r, m}$ and $\lambda \in \mathcal{P}_{r+k, m}$. We write $v \xrightarrow[k]{} \lambda$ if there exists $\beta \in \Gamma_{m, 2}$, with weight k , such that $\lambda = v + \beta$, where the $+$ sign stands for the usual addition of m -tuples. In the next lemma we prove that, for $\lambda \vdash k(t + 1)$, the number of semistandard generalized λ' -tableaux of type (k^{t+1}) equals the number of semistandard generalized v' -tableaux of type (k^t) , when v runs over the set

$$\left\{ v \in \mathcal{P}_{kt, m} : v \xrightarrow[k]{} \lambda \right\}.$$

Lemma 1. Let t be a positive integer and suppose $\lambda \in \mathcal{P}_{k(t+1), m}$. Then

$$\sum_{\substack{v \in \mathcal{P}_{kt, m} \\ v \xrightarrow[k]{} \lambda}} K_{v', (k^t)} = K_{\lambda', (k^{t+1})}.$$

Proof. Let $v \in \mathcal{P}_{kt,m}$ and suppose $v \xrightarrow[k]{\lambda}$. There exists $\beta \in \Gamma_{m,2}$ such that $w(\beta) = k$ and $\lambda = v + \beta$.

Let Q be a generalized semistandard v' -tableau of type (k^t) . Suppose we add k new boxes filled with t to the tableau Q in the following way: for $i = 0, 1, \dots, m-1$ we add a new box at the end of column $i+1$ if and only if $\beta(i) = 1$. Since $\lambda = v + \beta$ we have

$$\begin{cases} \beta(i) = 0 \\ \beta(i+1) = 1 \end{cases} \Rightarrow v_i > v_{i+1}, \quad i = 0, 1, \dots, m-2$$

and

$$\begin{cases} \beta(i) = 1 \\ i > v'_0 = \ell(v) \end{cases} \Rightarrow \beta(v'_0) = \dots = \beta(i-1) = 1, \quad i = 0, 1, \dots, m-1.$$

Then we obtain a semistandard generalized λ' -tableau of type (k^{t+1}) . Denote by $\Psi(Q)$ this tableau. We have thus defined a mapping

$$\Psi : \dot{\bigcup}_{\substack{v \in \mathcal{P}_{kt,m} \\ v \xrightarrow[k]{\lambda}}} \mathcal{T}_{v',(k^t)}^0 \longrightarrow \mathcal{T}_{\lambda',(k^{t+1})}^0$$

$$Q \longmapsto \Psi(Q)$$

where $\dot{\bigcup}$ stands for disjoint union. It is obvious that Ψ is injective. Let us prove that it is also surjective.

Let Q_1 be a generalized semistandard λ' -tableau of type (k^{t+1}) . Consider $\beta \in \Gamma_{m,2}$ defined by $\beta(i) = 1$ if and only if in the $(i+1)$ th column of Q_1 there is a box filled with t , for $i = 0, 1, \dots, m-1$. Then the weight of β equals the number of boxes filled with t in Q_1 , which is k .

Consider the m -tuple $v = (v_0, v_1, \dots, v_{m-1})$ defined by

$$v_i = \lambda_i - \beta(i), \quad i = 0, 1, \dots, m-1.$$

For $i = 0, 1, \dots, m-1$, if $\beta(i) = 1$ then $\lambda_i > 0$. It follows that $v_i \geq 0$, for all i . Since integers increase along each row in tableau Q_1 , we have

$$(\beta(i) = 1 \wedge \lambda_i = \lambda_{i+1}) \Rightarrow \beta(i+1) = 1.$$

Then, for $i = 0, 1, \dots, m-2$,

$$v_i - v_{i+1} = (\lambda_i - \lambda_{i+1}) + (\beta(i+1) - \beta(i)) \geq 0.$$

From $w(\beta) = k$ we have also that $w(v) = w(\lambda) - w(\beta) = k(t+1) - k = kt$. Then $v \in \mathcal{P}_{kt,m}$ and $v \xrightarrow[k]{\lambda}$.

Let Q be the semistandard generalized Young tableau obtained from Q_1 by deleting the boxes filled with t . Then Q is associated with $[v']$, is of type (k^t) and $\Psi(Q) = Q_1$. \square

Consider $t \in \mathbb{N}$ and let q and r be the unique non-negative integers such that $kt = qm + r$ and $r \leq m - 1$. Define

$$\mu^{(k,t)} = (\underbrace{m, \dots, m}_q, r) \vdash kt.$$

Lemma 2. *Let t and $\mu^{(k,t)}$ be as before. Then*

$$K_{\mu^{(m-k,t)}, ((m-k)^t)} = K_{\mu^{(k,t)}, (k^t)}.$$

Proof. Suppose $kt = qm + r$, where q and r are non-negative integers and $r \leq m - 1$. Then

$$\mu^{(k,t)} = (\underbrace{m, \dots, m}_q, r) \quad \text{and} \quad \mu^{(m-k,t)} = (\underbrace{m, \dots, m}_{t-q-1}, m-r).$$

Let Q be a generalized semistandard $\mu^{(k,t)}$ -tableau of type (k^t) . For $i = 1, 2, \dots, m$ let C_i be the set of integers lying in the i th column of Q . Then

$$|C_i| = \begin{cases} q + 1 & \text{if } 1 \leq i \leq r \\ q & \text{if } r + 1 \leq i \leq m \end{cases}, \quad \text{for } i = 1, \dots, m.$$

Consider the sets defined by

$$C'_i = \{0, 1, \dots, t - 1\} \setminus C_{m-i+1}, \quad i = 1, 2, \dots, m.$$

For $i = 1, 2, \dots, m$,

$$\begin{aligned} |C'_i| &= \begin{cases} t - q & \text{if } 1 \leq i \leq m - r \\ t - q - 1 & \text{if } m - r + 1 \leq i \leq m \end{cases} \\ &= (\mu^{(m-k,t)})'_{i-1}. \end{aligned}$$

Then we can consider the generalized $\mu^{(m-k,t)}$ -tableau obtained by filling the boxes in the i th column with the elements of C'_i in an increasing way from top to bottom, for all i from 1 up to m . We denote by $\Theta_1(Q)$ this tableau. For $j \in \{0, 1, \dots, t - 1\}$,

$$j \in C'_i \Leftrightarrow j \notin C_{m-i+1}.$$

Since Q is of type (k^t) it follows that $\Theta_1(Q)$ is of type $((m - k)^t)$.

By construction, integers strictly increase down each column in $\Theta_1(Q)$. Suppose that there is at least one row along which integers do not increase. Let $s \in \{1, \dots, t - q\}$ denote the index of the first row for which this happens. There exists $i \in \{1, \dots, m - 1\}$ such that the boxes in row s , columns $i, i + 1$ are filled with a and b , respectively, and $a > b$. Then

$$|C'_i \cap \{0, 1, \dots, b\}| = s - 1 \quad \text{and} \quad |C'_{i+1} \cap \{0, 1, \dots, b\}| = s.$$

It follows that

$$|C_{m-i+1} \cap \{0, 1, \dots, b\}| = b - s + 2$$

and

$$|C_{m-i} \cap \{0, 1, \dots, b\}| = b - s + 1,$$

but this is absurd because Q is semistandard.

Thus we have defined a map $\Theta_1: \mathcal{F}_{\mu^{(k,t)}, (k^t)}^0 \longrightarrow \mathcal{F}_{\mu^{(m-k,t)}, ((m-k)^t)}^0$.

Now let Q' be a generalized semistandard $\mu^{(m-k,t)}$ -tableau of type $((m-k)^t)$. For $i = 1, \dots, m$ let C'_i be the set of integers lying in the i th column of Q' .

For $i = 1, \dots, m$ define

$$C_i = \{0, 1, \dots, t-1\} \setminus C'_{m-i+1},$$

and let $\Theta_2(Q')$ be the generalized $\mu^{(k,t)}$ -tableau obtained by filling the boxes in the i th column with the elements of C_i in a increasing way from top to bottom, for $i = 1, \dots, m$. As we have done to $\Theta_1(Q)$, it can be proved that $\Theta_2(Q')$ is semistandard and of type (k^t) .

Hence we have defined another map, $\Theta_2: \mathcal{F}_{\mu^{(m-k,t)}, ((m-k)^t)}^0 \longrightarrow \mathcal{F}_{\mu^{(k,t)}, (k^t)}^0$, such that $\Theta_2 \circ \Theta_1 = Id$ and $\Theta_1 \circ \Theta_2 = Id$. The result follows. \square

3. Main result

For a basis $\mathcal{B} = \{e_0, e_1, \dots, e_{n-1}\}$ of a finite dimensional vector space V and $v = \sum_{i=0}^{n-1} a_i e_i \in V$ the *support* of v with respect to the basis \mathcal{B} is the set

$$\text{supp}_{\mathcal{B}} v = \{e_i \in \mathcal{B} : a_i \neq 0\}.$$

Let g be a linear operator on V and let $v \in V$. The *cyclic subspace* of v associated with g is the subspace of V ,

$$\mathcal{C}_g(v) = \langle g^i(v) : i \in \mathbb{N} \cup \{0\} \rangle.$$

Recall that $\sigma(g)$ is the spectrum of g . We will use the following results

Theorem 1. *Let g be a linear operator on vector space V . Then*

$$\deg(P_g) = \max_{v \in V} \dim \mathcal{C}_g(v).$$

Theorem 2. *If g is a simple structure linear operator then*

$$|\sigma(g)| = \deg(P_g).$$

Let k, m and p be as before. Let f be a linear operator on V and let $v \in V$.

For s a non-negative integer and $v \in \mathcal{P}_{s,m}$, $\bigwedge f^v(v)$ denotes the vector

$$f^{v_{m-1}}(v) \wedge f^{v_{m-2}+1}(v) \wedge \dots \wedge f^{v_0+m-1}(v).$$

The aim of the next lemma and the next proposition is to write the image of $v \wedge f(v) \wedge \dots \wedge f^{m-1}(v)$ by $(s_k^\wedge(f))^t$ ($t \in \mathbb{N}$) as a linear expansion of vectors of the form $\bigwedge f^v(v)$.

Lemma 3. *Let $t \in \mathbb{N}$ and $v \in V$. For $\lambda \in \mathcal{P}_{kt,m}$,*

$$s_k^\wedge(f) \left(\bigwedge f^\lambda(v) \right) = \sum_{\substack{\mu \in \mathcal{P}_{k(t+1),m} \\ \lambda \xrightarrow{k} \mu}} \bigwedge f^\mu(v).$$

Proof

$$\begin{aligned} s_k^\wedge(f) \left(\bigwedge f^\lambda(v) \right) &= \sum_{\substack{\beta \in \Gamma_{m,2} \\ w(\beta) = k}} \bigwedge_{j=0}^{m-1} f^{\lambda_{m-j-1} + j + \beta(j)}(v) \\ &= \sum_{\substack{\gamma \in \Gamma_{m,2} \\ w(\gamma) = k}} \bigwedge_{j=0}^{m-1} f^{\lambda_{m-j-1} + j + \gamma(m-j-1)}(v) \\ &= \sum_{\substack{\mu \in \mathcal{P}_{k(t+1),m} \\ \lambda \xrightarrow{k} \mu}} \bigwedge_{j=0}^{m-1} f^{\mu_{m-j-1} + j}(v) \\ &= \sum_{\substack{\mu \in \mathcal{P}_{k(t+1),m} \\ \lambda \xrightarrow{k} \mu}} \bigwedge f^\mu(v). \quad \square \end{aligned}$$

Proposition 1. *Let $t \in \mathbb{N}$ and $v \in V$. Then*

$$(s_k^\wedge(f))^t (v \wedge f(v) \wedge \dots \wedge f^{m-1}(v)) = \sum_{v \in \mathcal{P}_{kt,m}} K_{v',(kt)} \bigwedge f^v(v).$$

Proof. The proof is by induction on t . For $t = 1$, and from the previous lemma, it remains to prove that, for $v \in \mathcal{P}_{k,m}$,

$$K_{v',(k)} = \begin{cases} 0 & \text{if } (0, 0, \dots, 0) \xrightarrow{k} v \\ 1 & \text{if } (0, 0, \dots, 0) \xrightarrow{k} v'. \end{cases} \tag{5}$$

Let $v \in \mathcal{P}_{k,m}$. If $k = 1$ then $v = (1, 0, \dots, 0)$ and (5) holds.

Suppose $k \geq 2$. Since $k \leq m$, if $(0, 0, \dots, 0) \xrightarrow[k]{\neq} v$ then $v_0 \geq 2$ and $K_{v',(k)} = 0$. If $(0, 0, \dots, 0) \xrightarrow[k]{\rightarrow} v$, then $v = (\underbrace{1, \dots, 1}_k, \underbrace{0, \dots, 0}_{m-k})$, $v' = (k)$ and $K_{v',(k)} = 1$.

Let $t \geq 1$ and suppose the result holds for t . Then (Lemmas 3 and 1)

$$\begin{aligned} & (s_k^\wedge(f))^{t+1}(v \wedge f(v) \wedge \dots \wedge f^{m-1}(v)) \\ &= \sum_{v \in \mathcal{P}_{kt,m}} K_{v',(k^t)} \sum_{\substack{\mu \in \mathcal{P}_{k(t+1),m} \\ v \xrightarrow[k]{\rightarrow} \mu}} \bigwedge f^\mu(v) \\ &= \sum_{\mu \in \mathcal{P}_{k(t+1),m}} \left(\sum_{\substack{v \in \mathcal{P}_{kt,m} \\ v \xrightarrow[k]{\rightarrow} \mu}} K_{v',(k^t)} \right) \bigwedge f^\mu(v) \\ &= \sum_{\mu \in \mathcal{P}_{k(t+1),m}} K_{\mu',(k^{t+1})} \bigwedge f^\mu(v). \quad \square \end{aligned}$$

Consider $t \in \mathbb{N}$ and let q and r be the unique non-negative integers such that $kt = qm + r$ and $r \leq m - 1$. Define

$$\lambda^{(k,t)} = (\underbrace{q+1, \dots, q+1}_r, \underbrace{q, \dots, q}_{m-r}) \vdash kt.$$

Then

$$(\lambda^{(k,t)})' = (\underbrace{m, \dots, m}_q, r) = \mu^{(k,t)}.$$

Proposition 2. Let f be a linear operator on V , $v \in V$ and $n = \dim \mathcal{C}_f(v)$. Suppose that $k \leq m < p$ and let $M \in \mathbb{N}$. If

$$K_{\mu^{(k,t)},(k^t)} \not\equiv 0 \pmod{p}, \quad \text{for } t = 1, \dots, M-1,$$

then

$$\dim \mathcal{C}_{s_k^\wedge(f)}(v \wedge f(v) \wedge \dots \wedge f^{m-1}(v)) \geq \min \left\{ M, \left\lfloor \frac{m(n-m)}{k} \right\rfloor + 1 \right\}.$$

Proof. From the hypothesis $\{v, f(v), \dots, f^{n-1}(v)\}$ is a basis of $\mathcal{C}_f(v)$. Then (see [4])

$$\left\{ \bigwedge_{i=0}^{m-1} f^{\alpha(i)}(v) : \alpha \in \mathcal{Q}_{m,n} \right\}$$

is a basis of $\wedge^m \mathcal{C}_f(v)$. Since the map

$$\left\{ v \in \bigcup_{s \in \mathbb{N}_0} \mathcal{P}_{s,m} : v_0 \leq n - m \right\} \rightarrow \mathcal{Q}_{m,n}$$

$$v = (v_0, v_1, \dots, v_{m-1}) \mapsto (v_{m-1}, v_{m-2} + 1, \dots, v_1 + m - 2, v_0 + m - 1)$$

is a bijection, it follows that

$$\mathcal{B} = \left\{ \bigwedge f^v(v) : v \in \bigcup_{s \in \mathbb{N}_0} \mathcal{P}_{s,m} \text{ and } v_0 \leq n - m \right\}$$

is a basis of $\wedge^m \mathcal{C}_f(v)$.

Let $t \in \left\{ 1, \dots, \min \left\{ M - 1, \left\lfloor \frac{m(n-m)}{k} \right\rfloor \right\} \right\}$.

If $r = 0$, $\lambda_0^{(k,t)} = q = \frac{kt}{m} \leq n - m$.

If $r \neq 0$, $\lambda_0^{(k,t)} = q + 1 < \frac{kt}{m} + 1 \leq n - m + 1$. Then, in both cases,

$$\bigwedge f^{\lambda^{(k,t)}}(v) \in \mathcal{B}.$$

From Proposition 1 we have

$$(s_k^\wedge(f))^t (v \wedge f(v) \wedge \dots \wedge f^{m-1}(v)) = \sum_{v \in \mathcal{P}_{kt,m}} K_{v',(kt)} \bigwedge f^v(v).$$

Let $v \in \mathcal{P}_{kt,m}$. If $v_0 \leq n - m$ then $\bigwedge f^v(v) \in \mathcal{B}$.

Suppose

$$v_0 \geq n - m + 1. \tag{6}$$

There exist mn elements in \mathbb{F} , a_{ij} , $i = 0, 1, \dots, m - 1$, $j = 0, 1, \dots, n - 1$ such that

$$f^{v_{m-i-1}+i}(v) = \sum_{j=0}^{n-1} a_{ij} f^j(v). \tag{7}$$

From (6) and (7), it follows that $\bigwedge f^v(v)$ is a linear expansion of elements in \mathcal{B} of the form $\bigwedge f^\xi(v)$, where

$$\xi \in \bigcup_{s=0}^{kt-1} \mathcal{P}_{s,m} \quad \text{and} \quad \xi_0 \leq n - m.$$

Then $(s_k^\wedge(f))^t (v \wedge f(v) \wedge \dots \wedge f^{m-1}(v))$ is a linear expansion of vectors from the family

$$\left\{ \bigwedge f^\xi(v) : \xi \in \bigcup_{s=0}^{kt} \mathcal{P}_{s,m} \text{ and } \xi_0 \leq n - m \right\}$$

and the coefficient of $\bigwedge f^{\lambda^{(k,t)}}(v)$ in this linear expansion is $K_{\mu^{(k,t)},(kt)} \not\equiv 0 \pmod{p}$.

Define $\lambda^{(k,0)} = \underbrace{(0, 0, \dots, 0)}_m$. Then

$$\begin{aligned} (s_k^\wedge(f))^0(v \wedge f(v) \wedge \dots \wedge f^{m-1}(v)) &= v \wedge f(v) \wedge \dots \wedge f^{m-1}(v) \\ &= \bigwedge f^{\lambda^{(k,0)}}(v). \end{aligned}$$

Hence we have constructed $\min \left\{ M, \left\lfloor \frac{m(n-m)}{k} \right\rfloor + 1 \right\}$ partitions,

$$\lambda^{(k,t)}, \quad t = 0, 1, \dots, \min \left\{ M - 1, \left\lfloor \frac{m(n-m)}{k} \right\rfloor \right\},$$

such that

$$\bigwedge f^{\lambda^{(k,t)}}(v) \in \text{supp}_{\mathcal{B}}(s_k^\wedge(f))^t(v \wedge f(v) \wedge \dots \wedge f^{m-1}(v))$$

and

$$\ell > t \Rightarrow \bigwedge f^{\lambda^{(k,\ell)}}(v) \notin \text{supp}_{\mathcal{B}}(s_k^\wedge(f))^t(v \wedge f(v) \wedge \dots \wedge f^{m-1}(v)),$$

for $\ell, t = 0, 1, \dots, \min \left\{ M - 1, \left\lfloor \frac{m(n-m)}{k} \right\rfloor \right\}$.

Then

$$\left\{ (s_k^\wedge(f))^t(v \wedge f(v) \wedge \dots \wedge f^{m-1}(v)) : 0 \leq t \leq \min \left\{ M - 1, \left\lfloor \frac{m(n-m)}{k} \right\rfloor \right\} \right\}$$

is a linearly independent set and the result follows. \square

Corollary 1. Let f be a linear operator on V . Suppose that $k \leq m < p$ and let $M \in \mathbb{N}$. If

$$K_{\mu^{(k,t)},(k^t)} \not\equiv 0 \pmod{p}, \quad \text{for } t = 1, \dots, M - 1,$$

then

$$\deg(P_{s_k^\wedge(f)}) \geq \min \left\{ M, \left\lfloor \frac{m(\deg(P_f) - m)}{k} \right\rfloor + 1 \right\}.$$

Proof. Let $v \in V$ be such that $\deg(P_f) = \dim \mathcal{C}_f(v)$. Since $\deg(P_{s_k^\wedge(f)})$ is the maximum of the dimensions of $s_k^\wedge(f)$ -cyclic subspaces (Theorem 1), the result follows from Proposition 2. \square

Corollary 2. Let f be a linear operator on V and suppose that $m < p$. Then

$$\deg(P_{s_m^\wedge(f)}) \geq \deg(P_f) - m + 1.$$

Proof. Since $\mu^{(m,t)} = (m^t)$, $K_{\mu^{(m,t)},(m^t)} = 1$ for all $t \in \mathbb{N}$ and the result follows from Corollary 1. \square

Corollary 3. Let f be a linear operator on V and suppose that $m < p$. For $k \in \{1, m - 1\}$,

$$\deg(P_{s_k^\wedge(f)}) \geq \min \left\{ p, \left\lfloor \frac{m(\deg(P_f) - m)}{k} \right\rfloor + 1 \right\}.$$

Proof. Let $t \in \mathbb{N}$. From Lemma 2, $K_{\mu^{(m-1,t)},((m-1)^t)} = K_{\mu^{(1,t)},(1^t)}$ and this number is the number of semistandard Young tableaux associated with $[\mu^{(1,t)}]$. It is well known (see [6]) that this number divides $t!$. Then, for $t \leq p - 1$, $K_{\mu^{(1,t)},(1^t)} \not\equiv 0 \pmod{p}$. \square

If $k = 1$ the lower bound of Corollary 3 is the lower bound obtained by Dias da Silva and Hamidoune in [1]. This lower bound is attained at least if f is of simple structure and its distinct eigenvalues are in arithmetic progression.

In the next example we show that, if p is “big enough”, for every $n \in \mathbb{N}$ there exists a linear operator f such that $\deg(P_f) = n$ and the lower bound of Corollary 1 is attained.

Example 2. Let $n \in \mathbb{N}$ and let V be an n -dimensional vector space over \mathbb{F} . Let f be a linear operator on V such that $P_f = X^n$ and suppose

$$K_{\mu^{(k,t)},(k^t)} \not\equiv 0 \pmod{p}, \quad \text{for } t = 1, \dots, \left\lfloor \frac{m(n-m)}{k} \right\rfloor.$$

There exists (see [5]) a basis $\{e_0, e_1, \dots, e_{n-1}\}$ of V such that

$$f(e_0) = 0 \quad \text{and} \quad f(e_j) = e_{j-1}, \quad j = 1, \dots, n - 1.$$

The set $\mathcal{B}_1 = \{ \bigwedge_{i=0}^{m-1} e_{\alpha(i)} : \alpha \in \mathcal{Q}_{m,n} \}$ is a basis of $\wedge^m V$.

Let $\alpha \in \mathcal{Q}_{m,n}$. Then

$$\frac{m(m-1)}{2} \leq w(\alpha) \leq \frac{(2n-m-1)m}{2}.$$

By induction on t it is easy to prove that $(s_k^\wedge(f))^t (\bigwedge_{i=0}^{m-1} e_{\alpha(i)})$ is a linear expansion of vectors of the form $\bigwedge_{i=0}^{m-1} e_{\beta(i)}$, for $\beta \in \mathcal{Q}_{m,n}$ such that $w(\beta) = w(\alpha) - kt$.

Let $b = \left\lfloor \frac{m(n-m)}{k} \right\rfloor + 1$. Suppose $\beta \in \mathcal{Q}_{m,n}$ is such that

$$\bigwedge_{i=0}^{m-1} e_{\beta(i)} \in \text{supp}_{\mathcal{B}_1} (s_k^\wedge(f))^b \left(\bigwedge_{i=0}^{m-1} e_{\alpha(i)} \right).$$

Then

$$\begin{aligned} w(\beta) &= w(\alpha) - kb, \\ &\leq \frac{(2n-m-1)m}{2} - m(n-m) - 1, \\ &= \frac{m(m-1)}{2} - 1 \end{aligned}$$

and this is a contradiction. Hence

$$(s_k^\wedge(f))^b \left(\bigwedge_{i=0}^{m-1} e_{\alpha(i)} \right) = 0, \quad \forall \alpha \in Q_{m,n}.$$

It follows that

$$\deg(P_{s_k^\wedge(f)}) \leq b = \left\lfloor \frac{m(n-m)}{k} \right\rfloor + 1$$

and, from Corollary 1, equality holds.

4. Additive theory

Let A be a finite non-empty subset of the field \mathbb{F} . In this section we obtain, from Corollary 1, a lower bound for the cardinality of $s_k^\wedge(A)$ that generalizes (1).

The purpose of next two lemmas is to show that $s_k^\wedge(A)$ is the spectrum of $s_k^\wedge(f)$ for some linear operator f .

Lemma 4. *Let $A = \{a_0, a_1, \dots, a_{n-1}\}$ be a finite non-empty subset of the field \mathbb{F} , where $n = |A|$. Suppose $k \leq m < p$. Then, for $\alpha \in Q_{m,n}$,*

$$s_k(a_{\alpha(0)}, a_{\alpha(1)}, \dots, a_{\alpha(m-1)}) = \sum_{\substack{\beta \in \Gamma_{m,2} \\ w(\beta) = k}} \prod_{i=0}^{m-1} a_{\alpha(i)}^{\beta(i)}.$$

Proof. For $\alpha \in Q_{m,n}$,

$$\begin{aligned} s_k(a_{\alpha(0)}, a_{\alpha(1)}, \dots, a_{\alpha(m-1)}) &= \sum_{\omega \in Q_{k,m}} \prod_{j=0}^{k-1} a_{(\alpha \circ \omega)(j)} \\ &= \sum_{\omega \in Q_{k,m}} \prod_{i \in \text{Im}(\omega)} a_{\alpha(i)}. \end{aligned}$$

Since the mapping from $Q_{k,m}$ into the set of elements of $\Gamma_{m,2}$ with weight k that to each $\omega \in Q_{k,m}$ assigns $\theta(\omega)$ defined by

$$\theta(\omega)(i) = \begin{cases} 1 & \text{if } i \in \text{Im}(\omega) \\ 0 & \text{if } i \notin \text{Im}(\omega) \end{cases}, \quad i = 0, 1, \dots, m-1,$$

is a bijection, we have that,

$$\begin{aligned}
 s_k(a_{\alpha(0)}, a_{\alpha(1)}, \dots, a_{\alpha(m-1)}) &= \sum_{\omega \in Q_{k,m}} \prod_{\substack{i=0 \\ \theta(\omega)(i)=1}}^{m-1} a_{\alpha(i)} \\
 &= \sum_{\substack{\beta \in \Gamma_{m,2} \\ w(\beta)=k}} \prod_{i=0}^{m-1} a_{\alpha(i)} \\
 &= \sum_{\substack{\beta \in \Gamma_{m,2} \\ w(\beta)=k}} \prod_{i=0}^{m-1} a_{\alpha(i)}^{\beta(i)}. \quad \square
 \end{aligned}$$

Lemma 5. *Let f be a simple structure linear operator on V , such that $|\sigma(f)| = n = \dim V$. Then $s_k^\wedge(f)$ is of simple structure and*

$$\sigma(s_k^\wedge(f)) = s_k^\wedge(\sigma(f)).$$

Proof. Suppose $\sigma(f) = \{a_0, a_1, \dots, a_{n-1}\}$ and let $\{e_0, e_1, \dots, e_{n-1}\}$ be a basis of V such that $f(e_i) = a_i e_i$, $i = 0, 1, \dots, n - 1$.

Then $\{\bigwedge_{i=0}^{m-1} e_{\alpha(i)} : \alpha \in Q_{m,n}\}$ is a basis of $\wedge^m V$ and, for $\alpha \in Q_{m,n}$ we have,

$$\begin{aligned}
 s_k^\wedge(f) \left(\bigwedge_{i=0}^{m-1} e_{\alpha(i)} \right) &= \sum_{\substack{\beta \in \Gamma_{m,2} \\ w(\beta)=k}} \bigwedge_{i=0}^{m-1} f^{\beta(i)}(e_{\alpha(i)}) \\
 &= \sum_{\substack{\beta \in \Gamma_{m,2} \\ w(\beta)=k}} \bigwedge_{i=0}^{m-1} (a_{\alpha(i)}^{\beta(i)} e_{\alpha(i)}) \\
 &= \left(\sum_{\substack{\beta \in \Gamma_{m,2} \\ w(\beta)=k}} \prod_{i=0}^{m-1} a_{\alpha(i)}^{\beta(i)} \right) \bigwedge_{i=0}^{m-1} e_{\alpha(i)} \\
 &= s_k(a_{\alpha(0)}, \dots, a_{\alpha(m-1)}) \bigwedge_{i=0}^{m-1} e_{\alpha(i)}.
 \end{aligned}$$

This proves the lemma. \square

Corollary 4. Let A be a finite non-empty subset of the field \mathbb{F} . Suppose $k \leq m < p$ and let $M \in \mathbb{N}$. If

$$K_{\mu^{(k,t)}, (k^t)} \not\equiv 0 \pmod{p}, \quad \text{for } t = 1, \dots, M - 1,$$

then

$$|s_k^\wedge(A)| \geq \min \left\{ M, \left\lfloor \frac{m(|A| - m)}{k} \right\rfloor + 1 \right\}.$$

Proof. Let f be a linear operator of simple structure on $\mathbb{F}^{|A|}$, such that $\sigma(f) = A$. Since the degree of the minimal polynomial of a simple structure linear operator equals the number of its distinct eigenvalues (Theorem 2), the result follows from Corollary 1 and Lemma 5. \square

From Corollaries 2 and 3 we obtain

Corollary 5. Let A be a finite non-empty subset of the field \mathbb{F} and suppose $m < p$. Then

$$|s_m^\wedge(A)| \geq |A| - m + 1.$$

Corollary 6. Let A be a finite non-empty subset of the field \mathbb{F} . Let $k \in \{1, m - 1\}$ and suppose $m < p$. Then

$$|s_k^\wedge(A)| \geq \min \left\{ p, \left\lfloor \frac{m(|A| - m)}{k} \right\rfloor + 1 \right\}.$$

If $k = 1$ the lower bound of Corollary 6 is the lower bound for $|\wedge^m A|$ obtained by Dias da Silva and Hamidoune in [1] and that lower bound is attained, at least, if A is an arithmetic progression. The lower bound of Corollary 4 is attained, at least, in the special cases of the next examples.

Example 3. If $m = |A|$, then for all $k \in \{1, \dots, m\}$,

$$|s_k^\wedge(A)| = 1 = \left\lfloor \frac{m(|A| - m)}{k} \right\rfloor + 1.$$

Example 4. Suppose $m = 3$, $k = 2$, $p > 3$ and $A = \{a_0, a_1, a_2, a_3\}$, where $a_1 = -a_0$, $a_3 = -a_2$ and $|A| = 4$.

$$s_2(X_0, X_1, X_2) = X_0X_1 + X_0X_2 + X_1X_2.$$

Since

$$Q_{3,4} = \{(0, 1, 2), (0, 1, 3), (0, 2, 3), (1, 2, 3)\},$$

the elements of $s_2^\wedge(A)$ are

$$s_2(a_0, a_1, a_2) = a_0a_1 + a_0a_2 + a_1a_2 = -a_0^2,$$

$$s_2(a_0, a_1, a_3) = a_0a_1 + a_0a_3 + a_1a_3 = -a_0^2,$$

$$s_2(a_0, a_2, a_3) = a_0a_2 + a_0a_3 + a_2a_3 = -a_2^2$$

and

$$s_2(a_1, a_2, a_3) = a_1a_2 + a_1a_3 + a_2a_3 = -a_2^2.$$

Then

$$|s_2^\wedge(A)| = 2 = \min \left\{ p, \left\lfloor \frac{3(4-3)}{2} \right\rfloor + 1 \right\}.$$

Example 5. If $k = m$, $|A| = m + 1$ and $0 \in A$, then the lower bound is attained.

Although the lower bound established in Corollary 4 generalizes (case $k = 1$) the lower bound (1), there appears to be a major difference in equality cases. If $k = 1$, for all $n \in \mathbb{N}$ satisfying $n \leq |\mathbb{F}|$, there exists $A \subseteq \mathbb{F}$ such that $|A| = n$ and

$$|s_1^\wedge(A)| = |\wedge^m A| = \min\{p, m(|A| - m) + 1\},$$

that is, such that the lower bound in Corollary 4 is attained. It is sufficient to consider a set A which is an arithmetic progression.

For $1 < k < m$ we were unable to prove a similar result.

If $k = m$ a similar result does not hold, as shown in next example.

Example 6. If $p = +\infty$, $m = k = 2$ and $|A| = 4$ then

$$|s_2^\wedge(A)| > 3 = \left\lfloor \frac{2(|A| - 2)}{2} \right\rfloor + 1.$$

References

- [1] J.A. Dias da Silva, Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. Lond. Math. Soc.* 26 (1994) 140–146.
- [2] J.A. Dias da Silva, H. Godinho, Generalized derivations and additive theory, *Linear Algebra Appl.* 342 (2002) 1–15.
- [3] G. James, A. Kerber, *The Representation Theory of the Symmetric Group*, Addison-Wesley Publishing Company, MA, 1981.
- [4] M. Marcus, *Finite Dimensional Multilinear Algebra—Parts I and II*, Marcel Dekker Inc., New York, 1973.
- [5] M. Newman, *Integral Matrices*, Academic Press, 1972.
- [6] B.E. Sagan, *The Symmetric Group: Representations Combinatorial Algorithms and Symmetric Functions*, Wadsworth & Brooks, 1991.