# Critical polynomials related to generalized derivations

J.A. Dias da Silva[*]
Departamento de Matemática-CELC
Universidade de Lisboa
Av Gama Pinto 2
1649-003 Lisboa
Portugal

Hemar Godinho[†]
Departamento of Matemática
Universidade de Brasília
70919-900 Brasília
Brasil

## 1 Introduction

In this paper we further investigate cyclic spaces of generalized derivations related to the elementary symmetric functions. There are important correlations between these derivations and problems in additive number theory, as described in details in our previous paper [2]. Before presenting the problem addressed here, some definitions are necessary.

Let $m, k \in \mathbb{N}$ such that $k \leq m$. Denote by $Q_{k,m}$ the set of all strictly increasing mappings from $\{1, \cdots, k\}$ into $\{1, \cdots, m\}$ and let $X_1, \ldots, X_m$ be $m$ distinct indeterminates. The $k$th elementary symmetric function on the indeterminates $X_1, \ldots, X_m$ may be written as

$$s_{k,m}(X_1, \ldots, X_m) = \sum_{\omega \in Q_{k,m}} X_{\omega(1)} \cdot X_{\omega(2)} \cdots X_{\omega(k)}.$$

Let $V$ be an $n$-dimensional vector space over the field $\mathbb{F}$. Let $L(V, V)$ be the $\mathbb{F}$-algebra of linear operators on $V$ and let $T \in L(V, V)$. We denote by

[*] This research was done within the activities of the Centro de Estruturas Lineares e Combinatórias and was partially supported by Fundação para a Ciência e Tecnologia and "Programa Ciência, Tecnologia e Inovação do Quadro Comunitário de Apoio"

[†] This paper started while the second author was enjoying the hospitality of the Universidade de Lisboa. This work was partially supported by CAPES/Brasil, CNPq/Brasil and FAP-DF/Brasil

$\otimes^m V = V \otimes \cdots \otimes V$ the $m$th-tensor power of $V$ (the tensor product of $m$ copies of $V$). If $T$ is a linear operator, we denote by $P_T$ the minimal polynomial of $T$, and by $I$ the identity linear operator on $V$.

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

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

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

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

where

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

We denote by $s_{k,m}(\mathbb{X})$ the element of $\otimes^m \mathbb{Z}[X] = \mathbb{Z}[X] \otimes \cdots \otimes \mathbb{Z}[X]$ defined as

$$s_{k,m}(\mathbb{X}) := \sum_{\omega \in Q_{k,m}} \delta_\omega(X, \ldots, X).$$

Let us denote by $s_{k,m}(\mathbb{T})$ the linear operator on $\otimes^m V$

$$s_{k,m}(\mathbb{T}) := \sum_{\omega \in Q_{k,m}} \delta_\omega(T, \ldots, T).$$

Let $p$ be the characteristic of the field $\mathbb{F}$. Then $p$ is a prime number if the characteristic is finite, or let $p = \infty$, otherwise. In [2] the authors discussed the existence of a lower bound for the degree of the minimal polynomial of $s_{k,m}(\mathbb{T})$, proving, among other results, one that contains, as a particular case, the following theorem:

**Theorem 1.1** *Let $m, k$ be positive integers and $k \leq m$. Let $T \in L(V, V)$ and $n$ be the degree of $P_T$. Then*

$$deg(P_{s_{k,m}(\mathbb{T})}) \geq \left\lfloor \frac{m(n-1)}{k} \right\rfloor + 1, \tag{1}$$

*for $p$ sufficiently large.*

From [2, prop. 2.1], a trivial bound can be obtained to the sizes of the primes $p$, that is $p \geq b^\ell$, where

$$b = \binom{m}{k} \quad \text{and} \quad \ell = \left\lfloor \frac{m(n-1)}{k} \right\rfloor.$$

But in general it seems to be a very difficult problem to describe precisely for which $p$'s the theorem is not valid. It is a problem related to the number of (0,1)-matrices with prescribed row sum vector and column sum vector. The hypothesis "$p$ sufficiently large" can be lifted in the spacial cases of $k = 1$ and $k = m - 1$, giving the following result:

**Theorem 1.2** *Let $m, k$ be positive integers and $k \leq m$. Let $T \in L(V,V)$ and $n$ be the degree of $P_T$. Then*

*(i)* $deg(P_{s_{1,m}(\mathbb{T})}) \geq \min\{p,\ m(n-1)+1\}$.

*(ii)* $deg(P_{s_{m-1,m}(\mathbb{T})}) \geq \min\{p, \left\lfloor \frac{m(n-1)}{m-1} \right\rfloor + 1\}$.

Our goal is to present some results on the structure of operators $T$, for which the degree of the minimal polynomial of $s_{k,m}(\mathbb{T})$ is small. The techniques involved come from Linear Algebra and Combinatorics, and their use for the purpose of describing these polynomials seems to be new.

We say that an operator $T \in L(V,V)$ is *critical* if (see (1))

$$deg(P_{s_{k,m}(\mathbb{T})}) = \left\lfloor \frac{m(n-1)}{k} \right\rfloor + 1.$$

And we will call the minimal polynomial $P_T$ a *critical polynomial* if $T$ is a critical operator. We are now in position to state our main result.

**Theorem 1.3 (Main Theorem)** *Let $m, k$ be positive integers and $k \leq m$. Assume that $m(n-1) \equiv k-1 \pmod{k}$, and $p$ is sufficiently large. If $P_T$ is a critical polynomial of degree $n$ then*

$$P_T(X) = X^n - \sum_{i=1}^{r} A_{n-ik} X^{n-ik},$$

*where* $r = \left\lfloor \frac{n}{k} \right\rfloor$.

It is important to observe that for every $k, m \in \mathbb{N}$, $1 \leq k \leq m$, the polynomials of the form $X^n$ are critical. It is also interesting to mentioned that, for $k = m$, one can prove that the polynomials,

$$P_i(X) = X^n - A_{n-ik} X^{n-ik},$$

for $i = 1, \ldots, r$, are all critical. These proofs and some other examples are presented at the final sections of this paper.

To prove the theorem above, we will study the powers of the operator $s_{k,m}(\mathbb{T})$, and find conditions for the set

$$\{I, s_{k,m}(\mathbb{T}), \ldots, s_{k,m}(\mathbb{T})^{\ell+1}\}$$

to be linearly dependent.

## 2 Multilinear Algebra

Denote by $1_{\mathbb{F}}$ the identity of $\mathbb{F}$. Consider the $\mathbb{Z}$-algebra homomorphism $\phi$ from $\mathbb{Z}$ into $\mathbb{F}$ satisfying $\phi(n) = \underbrace{1_{\mathbb{F}} + 1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}_{n \text{ times}}$ for all $n \in \mathbb{N}$. Denote also by $\phi$ the canonical extension of $\phi$ from $\mathbb{Z}[X]$ into $\mathbb{F}[X]$ satisfying

$$aX^m \longmapsto \phi(a)X^m, \quad m \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}, a \in \mathbb{Z}.$$

Then

$$\Phi = \phi \otimes \phi \otimes \cdots \otimes \phi$$

is a $\mathbb{Z}$-algebra homomorphism from $\otimes^m \mathbb{Z}[X]$ into $\otimes^m \mathbb{F}[X]$.

It is well known that

$$\mathcal{E} = \{X^{s_1} \otimes \cdots \otimes X^{s_m} \mid s_i \in \mathbb{N}_0,\ i = 1, \ldots, m\}$$

is a basis of the free $\mathbb{Z}$-module, $\otimes^m \mathbb{Z}[X]$ and,

$$\mathcal{E}_{\mathbb{F}} = \{X^{s_1} \otimes \cdots \otimes X^{s_m} \mid s_i \in \mathbb{N}_0,\ i = 1, \ldots, m\}$$

is a basis of the vector space $\otimes^m \mathbb{F}[X]$, over $\mathbb{F}$. Hence, if

$$z = \sum_{(s_1,\ldots,s_m)} c_{(s_1,\ldots,s_m)} X^{s_1} \otimes \cdots \otimes X^{s_m} \in \otimes^m \mathbb{Z}[X]$$

is the expression of $z$ as linear combination of the elements of $\mathcal{E}$ then

$$\Phi(z) = \sum_{(s_1,\ldots,s_m)} \phi(c_{(s_1,\ldots,s_m)}) X^{s_1} \otimes \cdots \otimes X^{s_m}$$

is the expression of $\Phi(z)$ as linear combination of the elements of $\mathcal{E}_{\mathbb{F}}$.

Denote by $\Gamma_{m,\mathbb{N}_0}$ the set of all mappings from $\{1, \cdots, m\}$ into $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. We will identify the mapping $\alpha \in \Gamma_{m,\mathbb{N}_0}$ with the $m$-tuple $(\alpha(1), \cdots, \alpha(m))$. Using Theorem 2.3 of [2] we can easily derive the following theorem.

**Theorem 2.1** *Let $k$ and $m$ be as before and $t$ be a positive integer. Then*

$$(s_{k,m}(\mathbb{X}))^t = \sum_{(s_1,\ldots,s_m) \in \Lambda_{m,\mathbb{N}_0}(t)} C_{(s_1,\ldots,s_m)} X^{s_1} \otimes \cdots \otimes X^{s_m},$$

*where*

$$\Lambda_{m,\mathbb{N}_0}(t) = \{(s_1, \ldots, s_m) \in \Gamma_{m,\mathbb{N}_0} \mid \sum_{i=1}^{m} s_i = kt \ \text{ and } \ s_i \leq t, \ \text{for } 1 \leq i \leq m\},$$

*and $C_{(s_1,\ldots,s_m)}$ is equal to the image by $\phi$ of the number of $(0,1)$-matrices of type $m \times t$ with row sum vector equal to $(s_1, \ldots, s_m)$ and whose column sum vector is equal to $(k, \ldots, k)$.*

**Definition 2.1** *Let $W$ be a vector space over the field $\mathbb{F}$. Let $\mathcal{E} = \{e_i \mid i \in I\}$ be a basis of $W$. We say that $e_i$ $\mathcal{E}$-occurs in $w \in W$ if the coefficient of $e_i$ in the expansion of $w$ as a linear combination of the elements of $\mathcal{E}$ is different from zero.*

**Corollary 2.1** *Let $(s_1, \ldots, s_m) \in \Gamma_{m,\mathbb{N}_0}$ and let $(s_1', \ldots, s_m')$ be a permutation of $(s_1, \ldots, s_m)$. If the term $X^{s_1} \otimes \cdots \otimes X^{s_m}$ does $\mathcal{E}_{\mathbb{F}}$-occur in the expression of $(s_{k,m}(\mathbb{X})^t$ then all the terms $X^{s_1'} \otimes \cdots \otimes X^{s_m'}$ also $\mathcal{E}_{\mathbb{F}}$-occur in $(s_{k,m}(\mathbb{X})^t$ and with the same coefficient.*

It is easy to see that the mapping from $\Gamma_{m,\mathbb{N}_0}$ into $\mathcal{E}_{\mathbb{F}}$

$$S = (s_1, \cdots, s_m) \longleftrightarrow X^{s_1} \otimes \cdots \otimes X^{s_m}$$

is a bijection. Then we will identify $S$ with $X^{s_1} \otimes \cdots \otimes X^{s_m}$. For $S' = (s_1', \cdots, s_m')$, we may define $S + S'$ to be the addition

$$X^{s_1} \otimes \cdots \otimes X^{s_m} + X^{s_1'} \otimes \cdots \otimes X^{s_m'}. \tag{2}$$

Consider the action of $\mathsf{Sym}(m)$, the full symmetric group of degree $m$, on $\Gamma_{m,\mathbb{N}_0}$, $(\sigma, S) \to S\sigma^{-1}$. Denote be $\mathcal{O}_S$ the orbit of $S$ by this action. We define for $S = (s_1, \cdots, s_m)$,

$$((S)) = ((s_1, \cdots, s_m)) := \sum_{S' \in \mathcal{O}_S} S'. \tag{3}$$

Before continuing, we would like to open a parenthesis to define a linear operator on $\otimes^m V$ that will play a important role in the sequel. Let $\sigma \in \mathsf{Sym}(m)$, and denote by $\mathcal{P}_V(\sigma)$ the linear operator on $\otimes^m V$ satisfying, for every $v_1, \ldots, v_m \in V$ (see [3, p. 72]),

$$\mathcal{P}_V(\sigma)(v_1 \otimes \cdots \otimes v_m) = v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(m)}.$$

These linear operators are related with the $m$-th powers of the linear mappings as follows.

**Proposition 2.1** *Let $V$ and $W$ be vector spaces over $\mathbb{F}$. Let $D$ be a linear mapping form $V$ into $W$. Then the linear mapping $D \otimes \cdots \otimes D$ from $\otimes^m V$ into $\otimes^m W$ satisfies the following equality*

$$\mathcal{P}_W(\sigma)(D \otimes \cdots \otimes D) = (D \otimes \cdots \otimes D)\mathcal{P}_V(\sigma), \tag{4}$$

*for every $\sigma \in \mathsf{Sym}(m)$*

**Proof**: For $v_1, \ldots, v_m \in V$ we have

$$\begin{aligned}(D \otimes \cdots \otimes D)\mathcal{P}_V(\sigma)(v_1 \otimes \cdots \otimes v_m) &= D(v_{\sigma^{-1}(1)}) \otimes \cdots \otimes D(v_{\sigma^{-1}(m)}) \\ &= \mathcal{P}_W(\sigma)(D(v_1) \otimes \cdots \otimes D(v_m)) \\ &= \mathcal{P}_W(\sigma)(D \otimes \cdots \otimes D)(v_1 \otimes \cdots \otimes v_m).\end{aligned}$$

Since the decomposable tensors $v_1 \otimes \cdots \otimes v_m$ span the tensor product $\otimes^m V$, we get the equality (4). ■

**Remarks 2.1** *(i) Let $S = (s_1, \ldots, s_m) \in \Gamma_{m,\mathbb{N}_0}$, and define $G_S$ to be the* **stabilizer** *of $S$ by the action above described. Then (see (3))*

$$\begin{aligned} \sum_{\sigma \in \mathsf{Sym}(m)} S\sigma^{-1} &= |G_S| \sum_{S \in \mathcal{O}_S} S' \\ &= |G_S|((s_1, \ldots, s_m)). \end{aligned} \tag{5}$$

*(ii) Observe that if $S = (s_1, \ldots, s_m) \in \Gamma_{m,\mathbb{N}_0}$, and considering the former identification, we have*

$$S\sigma^{-1} = \mathcal{P}_{\mathbb{F}[X]}(\sigma)(X^{s_1} \otimes \ldots \otimes X^{s_m}).$$

*Therefore, bearing in mind (5), we have*

$$((s_1, \ldots, s_m)) = \frac{1}{|G_S|} \left( \sum_{\sigma \in \mathsf{Sym}(m)} \mathcal{P}_{\mathbb{F}[X]}(\sigma) \right) (X^{s_1} \otimes \ldots \otimes X^{s_m}). \tag{6}$$

*(iii) If $S' = (s'_1, \ldots, s'_m) \in \mathcal{O}_S$ then*

$$((s'_1, \ldots, s'_m)) = ((s_1, \ldots, s_m))$$

*and for every $S = (s_1, \ldots, s_m) \in \Gamma_{m,\mathbb{N}_0}$, there is one and only one* **decreasing** *$m$-tuple in $\mathcal{O}_S$ (i.e. a* **partition** *of $\sum s_i$).*

Suppose that $S = (s_1, \cdots, s_m)$ has coefficient $C_S$ in the expansion of $(s_{k,m}(\mathbb{X}))^t$ as a linear combination of the elements of $\mathcal{E}_{\mathbb{F}}$. Then we can rewrite theorem 2.1 as

$$(s_{k,m}(\mathbb{X}))^t = \sum_{S \in \Lambda_{m,\mathbb{N}_0}(t)} C_S(s_1, \ldots, s_m). \tag{7}$$

Let $\Pi$ be the set of partitions $S = (s_1, \cdots, s_m)$ of $kt$ satisfying $s_i \leq t$, for $i = 1, \ldots, m$,

$$\Pi = \{(s_1, \ldots, s_m) \in \Lambda_{m,\mathbb{N}_0}(t)) \mid t \geq s_1 \geq s_2 \geq \cdots \geq s_m\}.$$

Grouping the right hand side of the equality (7) by the orbits of the action of $\mathsf{Sym}(m)$ on $\Gamma_{m,\mathbb{N}_0}$ we have, by theorem 2.1 (observe that, if $S \in \Lambda_{m,\mathbb{N}_0}(t)$ then $\mathcal{O}_S \subset \Lambda_{m,\mathbb{N}_0}(t)$),

$$(s_{k,m}(\mathbb{X}))^t = \sum_{S \in \Pi} \sum_{S' \in \mathcal{O}_S} C_{S'}(s'_1, \ldots, s'_m).$$

Now using corollary 2.1 we have

$$(s_{k,m}(\mathbb{X}))^t = \sum_{S \in \Pi} C_S \sum_{S' \in \mathcal{O}_S} S'.$$

Therefore, we may write the expansion of $(s_{k,m}(\mathbb{X}))^t$ in (7) as (see theorem 2.1)

**Lemma 2.1** *We have*

$$(s_{k,m}(\mathbb{X}))^t = \sum_{S\in\Pi} \mathcal{C}_S((s_1, \cdots, s_m)). \tag{8}$$

From this we can easily see that $s_{k,m}(\mathbb{X})^t$ belongs to the subspace of the vector space $\otimes^m \mathbb{F}[X]$, spanned by the linearly independent set

$$((\mathcal{E}_{\mathbb{F}})) \; = \; \{ \; ((s_1, \ldots, s_m)) \; \mid \; (s_1, \ldots, s_m) \; \in \; \Pi \;\; \}.$$

## 2.1 The Algebra $L(V, V)$

Let $T$ be a linear operator on $V$ whose minimal polynomial has degree $n$ and $\langle T\rangle$ be the cyclic subalgebra of $L(V, V)$ spanned by $T$ over $\mathbb{F}$. Consider the basis of $\otimes^m\langle T\rangle$

$$\mathcal{B} = \{T^{b_1} \otimes T^{b_2} \otimes \cdots \otimes T^{b_m} \;\mid\; 0 \le b_i \le n-1,\; i = 1, \ldots, m\}.$$

Denote by $\Gamma_{m,n}$ the subset of $\Gamma_{m,\mathbb{N}_0}$ of all mappings from $\{1, \cdots, m\}$ into $\{0, 1, \cdots, n-1\}$. In this setting and for convenience of the exposition we will denote the $m$-tuple of $\alpha$ of $\Gamma_{m,n}$ by $[\alpha(1), \ldots, \alpha(m)]$ or briefly by $[\alpha]$. It is easy to see that the correspondence

$$[b_1, \ldots, b_m] \to T^{b_1} \otimes T^{b_2} \otimes \cdots \otimes T^{b_m}$$

is a bijection from $\Gamma_{m,n}$ onto $\mathcal{B}$. As before we will identify $[b_1, \ldots, b_m]$ with $T^{b_1} \otimes \cdots \otimes T^{b_m}$ and give the meaning that follows from this identification to the sum of $m$-tuples of $\Gamma_{m,n}$ (see (2)).

We consider defined the action $(\sigma, B) \to B\sigma^{-1}$ of $\mathsf{Sym}(m)$ on $\Gamma_{m,n}$. Let $B = [b_1, \ldots, b_m] \in \Gamma_{m,n}$, and let us use the notation (following the analogy with $((s_1, \cdots, s_m))$ )

$$[[B]] = [[b_1, \cdots, b_m]] := \sum_{[b'_1,\ldots,b'_m]\in\mathcal{O}_{[b_1,\ldots,b_m]}} [b'_1, \ldots, b'_m]$$

to describe the sum of the elements of the *orbit* of the element $[b_1, \cdots, b_m]$ of the basis $\mathcal{B}$.

**Remarks 2.2** *(i) Let $B = [b_1, \ldots, b_m] \in \Gamma_{m,n}$, and define $G_B$ to be the* **stabilizer** *of $B$ by the action above described. Then*

$$\begin{aligned}\sum_{\sigma\in\mathsf{Sym}(m)} B\sigma^{-1} &= \sum_{\sigma\in\mathsf{Sym}(m)} [b_{\sigma(1)}, \ldots, b_{\sigma(m)}] \\ &= |G_B| \sum_{[b'_1,\ldots,b'_m]\in\mathcal{O}_{[b_1,\ldots,b_m]}} [b'_1, \ldots, b'_m] \\ &= |G_B|[[b_1, \ldots, b_m]].\end{aligned} \tag{9}$$

*(ii) Observe that if $B = [b_1, \ldots, b_m]$ (considering the former identification) we obtain*

$$B\sigma^{-1} = \mathcal{P}_{<T>}(\sigma)(T^{b_1} \otimes \ldots \otimes T^{b_m}),$$

*where $\langle T \rangle$ denotes the subalgebra of $L(V,V)$ spanned by $T$.*

*Using the item (i) above we get*

$$[[b_1, \ldots, b_m]] = \frac{1}{|G_B|} \left( \sum_{\sigma \in \mathsf{Sym}(m)} \mathcal{P}_{<T>}(\sigma) \right) (T^{b_1} \otimes \ldots \otimes T^{b_m}). \qquad (10)$$

*(iii) Again using the identification we can rewrite the basis $\mathcal{B}$ as*

$$\mathcal{B} = \{[b_1, \ldots, b_m] \;\mid\; 0 \le b_i \le n-1, \;\; i = 1, \ldots, m\}.$$

*Therefore,*

$$[[\mathcal{B}]] = \{[[b_1, \ldots, b_m]] \;\mid\; 0 \le b_i \le n-1, \;\; i = 1, \ldots, m\}.$$

*is a linearly independent set of $\otimes^m L(V,V)$.*

*(iv) From the definition of $[[b_1, \ldots, b_m]]$, we can see that*

$$[b'_1, \ldots, b'_m] \in \mathcal{O}_B \iff [[b'_1, \ldots, b'_m]] = [[b_1, \ldots, b_m]].$$

Let $\psi$ be the homomorphism from $\mathbb{F}[X]$ into $\langle T \rangle$, defined by $\psi(f(x)) = f(T)$. Then $\Psi := \psi \otimes \cdots \otimes \psi$ is the algebra homomorphism form $\otimes^m \mathbb{F}[X]$ into $\otimes^m \langle T \rangle$ satisfying

$$\Psi(X_1^{e_1} \otimes \cdots \otimes X_m^{e_m}) = T^{e_1} \otimes \cdots \otimes T^{e_m}.$$

If $z \in \otimes^m \mathbb{F}[X]$ we say that the image of $z$ by $\Psi$ is obtained by replacing $X$ by $T$ and we use the notation $z_{X=T}$ for the image $\Psi(z)$, in particular

$$(X_1^{e_1} \otimes \cdots \otimes X_m^{e_m})_{X=T} := \Psi(X_1^{e_1} \otimes \cdots \otimes X_m^{e_m}) = T^{e_1} \otimes \cdots \otimes T^{e_m}. \qquad (11)$$

Suppose that the minimal polynomial of $T$ is

$$X^n - A_{n-1}X^{n-1} - \cdots - A_1 X - A_0 I.$$

Then we have

$$T^n = A_{n-1}T^{n-1} + \cdots + A_1 T + A_0 I. \qquad (12)$$

For each $j \in \mathbb{N}_0$, let $A_{n-1}^{(j)}, \ldots, A_0^{(j)}$ be the elements of $\mathbb{F}$ such that

$$T^{n+j} = A_{n-1}^{(j)} T^{n-1} + \cdots + A_1^{(j)} T + A_0^{(j)} I, \qquad (13)$$

assuming $A_j^{(0)} = A_j$ for $j = 0, 1, \cdots, n-1$ (see (12).

In the next lemma we give a complete description of how the image by $\Psi$ of the elements $((s_1, \cdots, s_m))$ can be written in terms of the elements $[[b_1, \cdots, b_m]]$.

**Lemma 2.2** *Assume $p$ is large enough. Let $S = (s_1, \cdots, s_m)$ be a partition belonging to $\Pi$;*

*(i) If $s_1 \geq n$, take $d = \max\{ j \mid s_j \geq n \}$. Then $((s_1, \cdots, s_m))_{X=T}$ is equal to*

$$\sum_{0 \leq b_1, \ldots, b_d \leq n-1} q_{b_1,\ldots,b_d} A_{b_1}^{(s_1-n)} \ldots A_{b_d}^{(s_d-n)} [[b_1, \ldots, b_d, s_{d+1}, \ldots, s_m]] \quad (14)$$

*where*

$$q_{b_1,\ldots,b_d} = \frac{|G_{[b_1,\ldots,b_d,s_{d+1},\ldots,s_m]}|}{|G_S|}$$

*is a non-zero element of the prime field of $\mathbb{F}$.*

*(ii) If $s_1 \leq n-1$ then*

$$((s_1, \cdots, s_m))_{X=T} = [[s_1, \ldots, s_m]]. \quad (15)$$

**Proof**: Since the item (ii) above is an immediate consequence of the definitions, let us assume that $s_1 \geq n$. Writing $d = \max\{ j \mid s_j \geq n \}$, we have

$$s_1 \geq s_2 \geq \cdots \geq s_d \geq \ n \ > s_{d+1} \geq \cdots \geq s_m. \quad (16)$$

Using (6) and (11) we have

$$\begin{aligned} ((s_1, \ldots, s_m))_{X=T} &= \Psi\left(\frac{1}{|G_S|}(\sum_{\sigma \in \mathsf{Sym}(m)} \mathcal{P}_{\mathbb{F}[X]}(\sigma)\right)(X^{s_1} \otimes \cdots \otimes X^{s_m}) \\ &= \frac{1}{|G_S|}\Psi\left(\sum_{\sigma \in \mathsf{Sym}(m)} \mathcal{P}_{\mathbb{F}[X]}(\sigma)\right)(X^{s_1} \otimes \cdots \otimes X^{s_m}). \end{aligned}$$

Using proposition 2.1 we obtain, from the previous equalities,

$$\begin{aligned} ((s_1, \ldots, s_m))_{X=T} &= \frac{1}{|G_S|}\left(\sum_{\sigma \in \mathsf{Sym}(m)} \mathcal{P}_{\langle T \rangle}(\sigma)\right)\Psi(X^{s_1} \otimes \cdots \otimes X^{s_m}) \\ &= \frac{1}{|G_S|}\left(\sum_{\sigma \in \mathsf{Sym}(m)} \mathcal{P}_{\langle T \rangle}(\sigma)\right) T^{s_1} \otimes \cdots \otimes T^{s_m}. \end{aligned}$$

Bearing in mind (13) and (16) we get from the previous equalities that $((s_1, \ldots, s_m))_{X=T}$ equals to

$$\frac{1}{|G_S|}\left(\sum_{\sigma \in \mathsf{Sym}(m)} \mathcal{P}_{\langle T \rangle}(\sigma)\right)(\sum_{i=0}^{n-1} A_i^{(s_1-n)} T^i) \otimes \cdots \otimes (\sum_{i=0}^{n-1} A_i^{(s_d-n)} T^i) \otimes T^{s_{d+1}} \otimes \cdots \otimes T^{s_m}.$$

Now, by multilinearity, we get $((s_1,\ldots,s_m))_{X=T}$ equals to

$$= \frac{1}{|G_S|}\left(\sum_{\sigma\in\mathsf{Sym}(m)} \mathcal{P}_{\langle T\rangle}(\sigma)\right)\sum_{0\le b_1,\ldots,b_d\le n-1} A_{b_1}^{(s_1-n)}\cdots A_{b_d}^{(s_d-n)}(\otimes^B T)$$

$$= \frac{1}{|G_S|}\sum_{0\le b_1,\ldots,b_d\le n-1} A_{b_1}^{(s_1-n)}\cdots A_{b_d}^{(s_d-n)}\left(\sum_{\sigma\in\mathsf{Sym}(m)} \mathcal{P}_{\langle T\rangle}(\sigma)\right)(\otimes^B T)$$

where $\otimes^B T = T^{b_1}\otimes\cdots\otimes T^{b_d}\otimes T^{s_{d+1}}\otimes\cdots\otimes T^{s_m}$. From (10) follows that $((s_1,\ldots,s_m))_{X=T}$ is equal to

$$\frac{1}{|G_S|}\sum_{0\le b_1,\ldots,b_d\le n-1} A_{b_1}^{(s_1-n)}\cdots A_{b_d}^{(s_d-n)}|G_{[b_1,\ldots,b_d,s_{d+1},\ldots,s_m]}|[[b_1,\ldots,b_d,s_{d+1},\ldots,s_m]].$$

Defining

$$q_{b_1,\ldots,b_d} = \frac{|G_{[b_1,\ldots,b_d,s_{d+1},\ldots,s_m]}|}{|G_S|},$$

we see that the coefficients $q_{b_1,\ldots,b_d}$ are quotients of integers numbers (factors of $m!$), hence they belong to the prime field of $\mathbb{F}$. The hypothesis of $p$ large enough guarantees that all coefficients $q_{b_1,\ldots,b_d}$ are nonzero, completing the proof. ■

It follows from (8)

$$\begin{aligned}(s_{k,m}(\mathbb{T}))^t &= \Psi((s_{k,m}(\mathbb{X}))^t)\\ &= \sum_{S\in\Pi} C_S((s_1,\ldots,s_m))_{X=T}.\end{aligned}\tag{17}$$

An immediate consequence is that $(s_{k,m}(\mathbb{T}))^t$ belongs to the subspace spanned by $[[\mathcal{B}]]$, that is

**Lemma 2.3**

$$(s_{k,m}(\mathbb{T}))^t = \sum_{[[b_1,\ldots,b_m]]\in[[\mathcal{B}]]} H_{[[b_1,\ldots,b_m]]}[[b_1,\ldots,b_m]],$$

*with* $H_{[[b_1,\ldots,b_m]]}\in\mathbb{F}$.

**Definition 2.2** *Let* $S=(s_1,\cdots,s_m)$*, be a partition and let* $[[b_1,\ldots,b_m]]\in[[\mathcal{B}]]$.

*(i) We say that* $((s_1,\cdots,s_m))$ *is an* **ascendent** *of* $[[b_1,\ldots,b_m]]$*, if the following conditions hold:*

*(a) For some* $t$*,* $((s_1,\ldots,s_m))$ $((\mathcal{E}_{\mathbb{F}}))$*-occurs in* $s_{k,m}(\mathbb{X})^t$*, i.e.*

$$s_1+\cdots+s_m = kt \quad \text{and} \quad s_i\le t,\ i=1,\ldots,m.$$

*In this case we will say that* $((s_1,\ldots,s_m))$ *is at* **level** $t$*.*

*(b)* $[[b_1, \cdots, b_m]]$ $[[\mathcal{B}]]$*-occurs in* $((s_1, \cdots, s_m))_{X=T}$.

*(ii) An element* $((s_1, \cdots, s_m))$ *is said to have* **weight** $w$ *if* $\sum s_j = w$.

**Remark 2.1** *Let* $d = \max\{j \,|\, s_j \geq n\}$*, and assume that* $((s_1, \cdots, s_m))$ *is an ascendent of* $[[b_1, \cdots, b_m]]$*. Then by lemma 2.2 and remark 2.2(iv), there exists a* $\sigma \in \mathsf{Sym}(m)$ *such that*

$$[b_{\sigma(1)}, \cdots, b_{\sigma(m)}] = [b'_1, \cdots, b'_d, s_{d+1}, \ldots, s_m].$$

*The coordinates* $b_{\sigma(1)}, \cdots, b_{\sigma(d)}$ *will be called* **generated coordinates of** $[[b_1, \cdots, b_m]]$ **with respect to** $((s_1, \cdots, s_m))$.

# 3 Powers of T

Bearing in mind (12) and (13) we have for all $j \in \mathbb{N}_0$,

$$T^{n+j+1} = \sum_{i=0}^{n-1} (A_i A_{n-1}^{(j)} + A_{i-1}^{(j)}) T^i,$$

where we make the convention $A_{-1}^{(j)} = 0$. And immediately we have for $j \in \mathbb{N}_0$

$$A_{n-i}^{(j)} = A_{n-i} A_{n-1}^{(j-1)} + A_{n-i-1}^{(j-1)}, \tag{18}$$

for $i = 1, \cdots, n$.

**Lemma 3.1** *The following relations between the coefficients hold*

$$A_{n-t}^{(l)} = \sum_{j=1}^{l} A_{n-1}^{(l-j)} A_{n-t-j+1} + A_{n-t-l}, \quad l \in \mathbb{N}, \ t = 1, \ldots, n.$$

*where* $A_r = 0$ *if* $r < 0$ *and* $A_i^{(0)} = A_i$, $i = 0, \ldots, n-1$.

**Proof**: (Induction on $l$). The case $l = 1$ and $t = 1, \cdots, n$ follows directly from (18). So assume this is true for all $s \leq l$. By (18) we have

$$A_{n-t}^{(l+1)} = A_{n-t} A_{n-1}^{(l)} + A_{n-t-1}^{(l)},$$

and by induction hypothesis

$$A_{n-t-1}^{(l)} = \sum_{j=1}^{l} A_{n-1}^{(l-j)} A_{n-t-j} + A_{n-t-l-1},$$

which gives

$$\begin{aligned}
A_{n-t}^{(l+1)} &= A_{n-t}A_{n-1}^{(l)} + A_{n-t-1}^{(l)} \\
&= A_{n-t}A_{n-1}^{(l)} + \sum_{j=1}^{l} A_{n-1}^{(l-j)} A_{n-t-j} + A_{n-t-1-l} \\
&= A_{n-t}A_{n-1}^{(l)} + \sum_{j=2}^{l+1} A_{n-1}^{(l+1-j)} A_{n-t-j+1} + A_{n-t-(l+1)} \\
&= \sum_{j=1}^{l+1} A_{n-1}^{(l+1-j)} A_{n-t-j+1} + A_{n-t-(l+1)}.
\end{aligned}$$

■

**Corollary 3.1** *In particular*

$$A_{n-1}^{(l)} = A_{n-1}(A_{n-1}^{(l-1)} + A_{n-l}) + \sum_{j=2}^{l-1} A_{n-1}^{(l-j)} A_{n-j} + A_{n-l-1}$$

**Theorem 3.1** *Let $s \in \mathbb{N}$, such that $s = qk + r$, with $1 \leq r \leq k-1$. Suppose that*

$$A_{n-t} = 0, \quad \forall t \in \{1, \cdots, s\} \quad \textit{and} \quad t \not\equiv 0 \,(\text{mod } k).$$

*Then*

$$A_{n-1}^{(l)} = 0 \;\; \textit{for} \;\; 0 \leq l \leq s-1, \quad l \not\equiv k-1 \;(\text{mod } k), \tag{19}$$

*and, for $v = 1, \ldots, q$,*

$$A_{n-1}^{(vk-1)} = \sum_{i=1}^{v-1} A_{n-1}^{((v-i)k-1)} A_{n-ik} \; + \; A_{n-vk}. \tag{20}$$

**Proof**: (Induction on $q$). If $q = 0$ then $s = r \leq k-1$. So, from corollary 3.1 above follows that $A_{n-1}^{(l)} = 0$ for $l \leq r-1$.

Now suppose $q = 1$, then $s = k + r$ and

$$A_{n-1} = \cdots = A_{n-k+1} = A_{n-k-1} = \cdots = A_{n-s} = 0. \tag{21}$$

From lemma 3.1 we have

$$A_{n-1}^{(l)} = \sum_{\substack{j=1 \\ k \not| j}}^{l} A_{n-1}^{(l-j)} A_{n-j} \; + A_{n-1}^{(l-k)} A_{n-k} \; + A_{n-l-1}. \tag{22}$$

Assuming $l \leq s-1$ we have

$$l - k \leq (s-1) - k \leq r - 1 \leq k - 2.$$

Then we can use the case $q = 0$ above to have $A_{n-1}^{(l-k)} = 0$. Replacing (21) and $A_{n-1}^{(l-k)} = 0$ in (22) gives

$$A_{n-1}^{(l)} = A_{n-(l+1)} = \begin{cases} 0 & \text{if} \quad l \neq k-1 \\ A_{n-k} & \text{if} \quad l = k-1, \end{cases}$$

proving the theorem also for the case $q = 1$.

Let us assume that the theorem is true for all $q \leq u$ and let $s = (u+1)k + r$. Again, from corollary 3.1, follows that

$$A_{n-1}^{(l)} = \sum_{\substack{j=1 \\ k \not| j}}^{l} A_{n-1}^{(l-j)} A_{n-j} \; + \sum_{i=1}^{u+1} A_{n-1}^{(l-ik)} A_{n-ik} \; + A_{n-l-1}.$$

Assuming $l \leq s-1$ we have

$$l - ik \leq (u+1)k + r - ik = (u+1-i)k + r \leq uk + r,$$

thus, using the induction hypothesis, either (19) or (20) holds for $A_{n-1}^{(l-ik)}$, that is

$$A_{n-1}^{(l-ik)} = \begin{cases} 0 & \text{if} \quad l - ik \not\equiv k-1 \pmod{k} \\ A_{n-1}^{(t_i k-1)} & \text{if} \quad l - ik \equiv k-1 \pmod{k}. \end{cases}$$

It is important to observe that if $l - ik \equiv k-1 \pmod{k}$ for some $i$, then $l - ik \equiv k-1 \pmod{k}$ for all $i$, and $l \equiv k-1 \pmod{k}$.

Hence, for $l \leq s-1$, we must have (together with the hypothesis) either

$$A_{n-1}^{(l)} = 0 \;\text{ if }\; l \not\equiv k-1 \pmod{k}$$

or

$$A_{n-1}^{(vk-1)} = \sum_{i=1}^{v-1} A_{n-1}^{((v-i)k-1)} A_{n-ik} \; + \; A_{n-vk}$$

if $l = vk-1$ (i.e. $l \equiv k-1 \pmod{k}$), concluding this proof. ■

# 4 Genealogy of $B_j$

Let us start by recalling our assumptions that $k, m, n \in \mathbb{N}$, $2 \leq k \leq m$, $V$ is a vector space over $\mathbb{F}$, and $T \in L(V, V)$, a linear operator. We are denoting by $P_T$ is its minimum polynomial, and $n = \deg(P_T)$. Hence $\{I, T, \ldots, T^{n-1}\}$ is a linearly independent set over the field $\mathbb{F}$, and, as before, write

$$T^n = A_{n-1}T^{n-1} + \cdots + A_1 T + A_0 I.$$

Let

$$\ell = \left\lfloor \frac{m(n-1)}{k} \right\rfloor. \tag{23}$$

In [2, thm.3.5], the authors proved that the set

$$\{I, s_{k,m}(\mathbb{T}), \cdots, s_{k,m}(\mathbb{T})^{\ell}\} \tag{24}$$

is linearly independent over $\mathbb{F}$, provided $p$ is large enough.

Here we are interested in finding conditions to the extended set

$$\mathbb{S} = \{I, s_{k,m}(\mathbb{T}), \ldots, s_{k,m}(\mathbb{T})^{\ell+1}\} \tag{25}$$

to be linearly independent over $\mathbb{F}$, or equivalently, conditions when this set is linearly dependent over $\mathbb{F}$. In general this seems to be a difficult problem and here, and in what follows we will be assuming the extra hypothesis

$$m(n-1) \equiv k-1 \pmod{k}.$$

This, together with (23), gives that

$$k\ell = m(n-1) - k + 1. \tag{26}$$

The main strategy is the determination of the list of ascendents of some special elements of the basis $\mathcal{B}$, in order to find conditions for $s_{k,m}(\mathbb{T})^{\ell+1}$ not to be written as a linear combination of the smaller powers of $s_{k,m}(\mathbb{T})$.

**Definition 4.1** *For $j = 0, \ldots, n-1$, let us define*

$$B_j = [n-1, \cdots, n-1, n-1-j],$$

*and the sum of its coordinates to be $\delta_j$ which is equal to $m(n-1) - j$.*

Clearly $B_j$ is an element of the basis $\mathcal{B}$.

Next we present, without proof, two basic and immediate propositions that will be useful later in the text.

**Proposition 4.1** *Assume that*

$$\{I, s_{k,m}(\mathbb{T}), \cdots, s_{k,m}(\mathbb{T})^{\ell}\}$$

*is linearly independent and that $B = [[b_1, \ldots, b_m]]$ $[[\mathcal{B}]]$-occurs in $s_{k,m}(\mathbb{T})^{\ell+1}$ and does not $[[\mathcal{B}]]$-occur in $s_{k,m}(\mathbb{T})^t$ for any $t = 0, \ldots, \ell$. Then $\mathbb{S}$ is linearly independent.*

**Proposition 4.2** *Let $[[b_1, \ldots, b_m]] \in [[\mathcal{B}]]$ and $\delta = \sum_{j=1}^{m} b_j$. Assume that $((s_1, \ldots, s_m))$ is an ascendent of $[[b_1, \ldots, b_m]]$ such that $b_{i_j}$ are generated coordinates, for every $j = 1, \ldots, d$. Then the weight of $((s_1, \ldots, s_m))$ is $\delta + \sum_{j=1}^{d}(s_j - b_{i_j})$ (see definition 2.2 and remark 2.1).*

The following lemmas give information on the ascendents of

$$[[B_j]] = [[n-1, \cdots, n-1, n-1-j]],\ j = 0, \ldots, n-1.$$

**Lemma 4.1** *Let $j \in \{0,\ldots,n-1\}$, $j \not\equiv (k-1)\ (mod\, k)$. If $((s_1,\ldots,s_m))$ is an ascendent of $[[B_j]]$, then $s_1 \geq n$.*

**Proof:** It follows from the hypothesis that $j = qk + r$ with $r \leq k-2$. By proposition 4.2, definition 4.1 and (26) we have

$$\sum_{i=1}^{m} s_i \geq \delta_j = k(\ell + 1 - q) - (r+1).$$

Since $\sum_{i=1}^{m} s_i$ is a multiple of $k$ (see definition 2.2) and $1 \leq r+1 \leq k-1$, we have

$$\sum_{i=1}^{m} s_i > \delta_j. \tag{27}$$

If $s_1 \leq n-1$, then lemma 2.2(ii) tells us that

$$((s_1,\ldots,s_m))_{X=T} = [[b_1,\ldots,b_m]] = [[B_j]],$$

in particular,

$$\sum_{i=1}^{m} s_i = \delta_j$$

contradicting inequality (27). ■

**Lemma 4.2** *Assume that p is large enough. Let $j \not\equiv k-1\ (mod\, k)$. Then,*

$$((S_{sp})) = ((n, n-1, \cdots, n-1))$$

*is the only ascendent of $B_j$ at level at most $(\ell+1)$, for which $n-1-j$ is a generated coordinate of $[[B_j]]$ for $j = 0,1,\ldots,n-1$. Moreover*

$$((n, n-1,\ldots,n-1))_{X=T} = \sum_{j=0}^{n-1} q_j\, A_{n-1-j}\, [[B_j]], \tag{28}$$

*where the $q_j$'s are nonzero elements of $\mathbb{F}$, $j = 0,\ldots,n-1$.*

**Proof**: The formula (28) follows from (14). Now let $((s_1,\ldots,s_m))$ be an ascendent of $[[B_j]]$ satisfying the requirements of the hypothesis. Hence lemma 4.1 tells us that $s_1 \geq n$. By proposition 4.2

$$\begin{aligned} \textstyle\sum_{i=1}^{m} s_i &= (m(n-1)-j) + (s_1 - (n-j-1)) + \textstyle\sum_{j=2}^{d}(s_j - n - 1) \\ &= m(n-1) + \textstyle\sum_{j=1}^{d}(s_j - n - 1). \end{aligned}$$

Since we are assuming that $((s_1,\ldots,s_m))$ is at level at most $(\ell+1)$ (see definition 2.2), we have

$$\sum_{i=1}^{m} s_i = m(n-1) + \sum_{j=1}^{d}(s_j - (n-1)) \ \leq\ k(\ell+1) = m(n-1)+1.$$

The last equality follows from (26). Thus, since $s_1 \geq n$, we must have $d = 1$ and $s_1 = n$. ■

From now on we start a list of results that give necessary conditions for the set $\mathbb{S}$ to be linearly independent.

**Lemma 4.3** *The set* $\mathbb{S} = \{I, s_{k,m}(\mathbb{T}), \cdots, s_{k,m}(\mathbb{T})^{\ell+1}\}$ *is linearly independent if* $A_{n-1} \neq 0$, *provided* $p$ *is large enough.*

**Proof:** Assume that $((s_1, \ldots, s_m))$ is an ascendent of $B_0$ (see definition 4.1) at level at most $(\ell + 1)$. By lemma 4.1 we must have $s_1 \geq n$. Therefore $n - 1$ is a generated coordinate of $[[B_0]]$ with respect to $((s_1, \ldots, s_m))$. Now, by lemma 4.2 we have that $((s_1, \ldots, s_m)) = ((S_{sp}))$ and, from (14) and (28),

$$((S_{sp}))_{X=T} = \frac{|G_{B_0}|}{|G_{S_{sp}}|} A_{n-1} [[B_0]] + \sum_{j=1}^{n-1} q_j A_{n-1-j} [[B_j]]. \tag{29}$$

From (17) we have

$$(s_{k,m}(\mathbb{T}))^t = C_{S_{sp}}((S_{sp}))_{X=T} + \sum_{S \neq S_{sp}} C_S((s_1, \ldots, s_m))_{X=T} \tag{30}$$

Since $((S_{sp}))$ is the only ascendent of $[[B_0]]$ at level $(\ell + 1)$, we can use (29) and (30) having that

$$(s_{k,m}(\mathbb{T}))^{\ell+1} = C_{S_{sp}} \frac{|G_{B_0}|}{|G_{S_{sp}}|} A_{n-1}[[B_0]] + \mathcal{R}$$

where $\mathcal{R} \in \langle [[B]] \mid [[B]] \in [[\mathcal{B}]] - [[B_0]] \rangle$. It is very simple to see that $|G_{B_0}| = m!$ and $|G_{S_{sp}}| = (m-1)!$, hence

$$(s_{k,m}(\mathbb{T}))^{\ell+1} = m\, C_{S_{sp}} A_{n-1}[[B_0]] + \mathcal{R}.$$

The hypothesis of $p$ large enough guarantees that $m\, C_{S_{sp}} \neq 0$, thus $[[B_0]]$ $[[\mathcal{B}]]$-occurs in $s_{k,m}(\mathbb{T})^{\ell+1}$ if $A_{n-1} \neq 0$. On the other hand $[[B_0]]$ does not have any ascendent at levels $0, 1, \ldots, \ell$. Therefore it cannot $[[\mathcal{B}]]$-occur in $s_{k,m}(\mathbb{T})^t$ for $t = 0, 1, \ldots, \ell$. Now the result follows from proposition 4.1. ■

**Theorem 4.1** *Suppose* $k \leq m$, *and* $m(n-1) \equiv (k-1)$ *(mod* $k$*). Then, for* $p$ *large enough, if the set*

$$\mathbb{S} = \{I, s_{k,m}(\mathbb{T}), \cdots, s_{k,m}(\mathbb{T})^{\ell+1}\}$$

*is linearly dependent then* $A_{n-s} = 0$, *for all* $s$ *satisfying* $1 \leq s \leq n, \quad s \not\equiv 0 \pmod{k}$.

**Proof**: Consider the following property:
**Property** $P = P_w$: *If* $\mathbb{S}$ *is linearly dependent then*

$$A_{n-t} = 0, \quad t \not\equiv 0 \pmod{k} \text{ and } 1 \leq t \leq w.$$

The theorem is equivalent to the statement that $P_w$ is true for $w \in \{1, \ldots, n\}$. We are going to prove this last statement by induction on $w$.

The case $w = 1$ was treated in lemma 4.3. So assume (induction hypothesis), property $P_{w-1}$ is true.

Observe that if $w \equiv 0 \pmod{k}$ then

$$\{t \,|\, t \not\equiv 0 \pmod{k} \quad \text{and} \quad t \leq w\} = \{t \,|\, t \not\equiv 0 \pmod{k} \quad \text{and} \quad t \leq w-1\}.$$

Then, by induction hypothesis,

$$A_{n-t} = 0, \;\; t \not\equiv 0 \pmod{k} \quad \text{and } 1 \leq t \leq w,$$

and $P_w$ holds.

Now assume that $w \not\equiv 0 \pmod{k}$, and let $r = w - 1$. Observe that if $P_{r+1}$ is not true then $A_{n-r-1} \neq 0$. We are going to prove that if $A_{n-r-1} \neq 0$ then there are ascendents of $[[B_r]]$ only at level $\ell + 1$, and they are $((S_{sp}))$ and $((S_r)) = ((n+r, n-1, \ldots, n-1, n-r-1))$. This will lead to the linear independence of $\mathbb{S}$, contradicting the hypothesis.

Suppose that $((S)) = ((s_1, \ldots, s_m))$ is an ascendent of $[[B_r]]$ at one of the levels $0, 1, \ldots, \ell + 1$. By lemma 4.1 we have $s_1 \geq n$. Let $d = \max\{j \,|\, s_j \geq n\}$.

If the coordinate $(n - r - 1)$ of $B_r$ is a generated coordinate with respect to $((S))$ then, by lemma 4.2, $((S)) = ((S_{sp}))$. So assume that $n - r - 1$ is not a generated coordinate of $[[B_r]]$ with respect to $((S))$. Hence (see remark 2.1)

$$((S)) = ((s_1, \ldots, s_d, n-1, \ldots, n-1, n-r-1)). \tag{31}$$

Let

$$l_i = s_i - n, \quad i = 1, \ldots, d.$$

We will finish the proof by considering the following three cases:

**(A)** $l_i \equiv k - 1 \pmod{k}, \quad i = 1, \ldots, d.$

**(B)** There exists an $i \leq d$ such that $l_i \leq r - 1$ and $l_i \not\equiv k - 1 \pmod{k}$.

**(C)** There exists an $i \leq d$ such that $l_i \geq r$ and $l_i \not\equiv k - 1 \pmod{k}$.

Assume (A) holds. So

$$l_i + 1 = v_i k, \quad i = 1, \ldots, d \tag{32}$$

for some nonnegative integers $v_1, \ldots, v_d$.

By definition of $((s_1, \ldots, s_m))$, $(s_1, \ldots, s_m)$ is a partition of $uk$, for some nonnegative integer $u$. Then using (31)

$$uk = \sum_{i=1}^{m} s_i = \sum_{i=1}^{d} (l_i + 1) + m(n-1) - r.$$

Using equalities (32) we get from the previous equalities

$$uk = (\sum_{i=1}^{d} v_i)k + m(n-1) - r.$$

Now (26) implies that $k(\ell+1) = m(n-1)+1$, therefore

$$r = (\sum_{i=1}^{d} v_i)k + k(\ell+1) - 1 - uk.$$

Thus $r+1 \equiv 0 \pmod{k}$. A contradiction, since we are assuming $w = r+1 \not\equiv 0 \pmod{k}$.

Assume that (B) holds. The induction hypothesis says that

$$A_{n-t} = 0, \;\; t \not\equiv 0 \pmod{k} \quad \text{and} \quad 1 \le t \le r.$$

Then, from theorem 3.1, we get

$$A_{n-1}^{(l)} = 0, \;\; \text{for } \; 0 \le l \le r-1, \;\; l \not\equiv (k-1) \pmod{k}. \tag{33}$$

Using the assumptions of case (B), we obtain, from the previous equalities

$$A_{n-1}^{(l_i)} = 0$$

for some $i \le d$. Therefore, from (14), we see that $((S))$ cannot be an ascendent of $[[B_r]]$ (see definition 2.2 of ascendent). A contradiction.

Hence, if $(n-r-1)$ is not a generated coordinate of $[[B_r]]$ with respect to $((S))$, we must have that case (C) holds, that is,

$$l_i \ge r \quad \text{and} \quad l_i \not\equiv (k-1) \pmod{k}, \tag{34}$$

for some $i \le d$.

Then, using (31) we have (since we are assuming that $((S))$ is at one of the levels $0, 1, \ldots, \ell+1$)

$$k(\ell+1) \ge \sum_{i=1}^{m} s_i \ge (\sum_{j=1}^{d}(l_j+1)) + m(n-1) - r.$$

Therefore, using (34), we obtain

$$k(\ell+1) \ge (\sum_{j \ne i} l_j + 1) + (m(n-1)+1) + (l_i - r).$$

Since $m(n-1)+1 = k(\ell+1)$, we must have $\sum_{j \ne i} l_j + 1 = 0$ and $l_i = r$. Thus $d = 1$, $s_1 = n+r$ and

$$((S_r)) = ((n+r, n-1, \ldots, n-1, n-r-1)).$$

Hence we have proved that there are only ascendents of $[[B_r]]$ at level $\ell+1$ and they are

$$((S_{sp})) \quad \text{and} \quad ((S_r)).$$

From (14) we have

$$((S_{sp}))_{X=T} = q_1 A_{n-r-1}[[B_r]] + \mathcal{R}_1 \tag{35}$$

and

$$((S_r))_{X=T} = q_2 A_{n-1}^{(r)}[[B_r]] + \mathcal{R}_2 \tag{36}$$

with $\mathcal{R}_1$, $\mathcal{R}_2 \in \langle [[B]] \mid [[B]] \in [[\mathcal{B}]] - \{[[B_r]]\}\rangle$, and

$$q_1 = \frac{|G_{B_r}|}{|G_{S_{sp}}|}, \quad q_2 = \frac{|G_{B_r}|}{|G_{S_r}|}.$$

A simple calculation gives

$$|G_{S_r}| = (m-2)!, \ \ |G_{S_{sp}}| = (m-1)! \quad \text{and} \quad |G_{B_r}| = (m-1)!.$$

Hence $q_1 = 1$ and $q_2 = (m-1)$. As we have seen, (33) follows from the induction hypothesis and theorem 3.1. And this, together with corollary 3.1 give that

$$A_{n-1}^{(r)} = A_{n-r-1}.$$

Therefore (see (17))

$$\begin{aligned} s_{k,m}(\mathbb{T})^{\ell+1} &= \sum_{S\in\Pi} C_S((s_1,\ldots,s_m))_{X=T} \\ &= C_{S_{sp}}((S_{sp}))_{X=T} + C_{S_r}((S_r))_{X=T} + \sum_{S\neq S_{sp},S_r} C_S((s_1,\ldots,s_m))_{X=T}. \end{aligned}$$

Since $[[B_r]]$ has only $((S_r))$ and $((S_{sp}))$ as ascendents, and substituting (35) and (36) above, one has

$$s_{k,m}(\mathbb{T})^{\ell+1} = (C_{S_{sp}} + (m-1)C_{S_r})A_{n-r-1}[[B_r]] + \mathcal{R}_3$$

where $\mathcal{R}_3 \in \langle [[B]] \mid [[B]] \in [[\mathcal{B}]] - \{[[B_r]]\}\rangle$. Hence, for $p$ large enough, $(C_{S_{sp}} + (m-1)C_{S_r}) \neq 0$ (in fact, for $p \geq m\binom{m}{k}^{\ell}$). Thus, if $A_{n-r-1} \neq 0$, then $[[B_r]]$ $[[\mathcal{B}]]$-occurs in $s_{k,m}(\mathbb{T})^{\ell+1}$. And since $[[B_r]]$ has only ascendents at level $\ell+1$, it does not $[[\mathcal{B}]]$-occur in $s_{k,m}(\mathbb{T})^t$ for $t \leq \ell$. Then, by proposition 4.1, if $A_{n-r-1} \neq 0$ then $\mathbb{S}$ is linearly independent. ■.

**Theorem 4.2 (Main Theorem)** *Let $m, k$ be positive integers and $k \leq m$. Assume that $m(n-1) \equiv k-1 \pmod{k}$, and $p$ is sufficiently large. If $P_T$ is a critical polynomial of degree $n$ then*

$$P_T(X) = X^n - \sum_{i=1}^{r} A_{n-ik}X^{n-ik},$$

*where $r = \left\lfloor \frac{n}{k} \right\rfloor$.*

**Proof:** Now observe that if $\mathbb{S} = \{I, s_{k,m}(\mathbb{T}), \cdots, s_{k,m}(\mathbb{T})^{\ell+1}\}$ is linearly dependent then

$$\deg(P_{s_{k,m}(\mathbb{T})}) \leq \ell + 1.$$

Since we have proved that (see (24))

$$\deg(P_{s_{k,m}(\mathbb{T})}) \geq \ell + 1,$$

we must have that

$$\text{“}\mathbb{S} \text{ linearly dependent over } \mathbb{F} \iff \deg(P_{s_{k,m}(\mathbb{T})}) = \ell + 1.\text{”} \tag{37}$$

Now the conclusion of this proof follows from the theorem 4.1 above. ■

# 5 Examples

Here we are going to present some examples of critical polynomials, for special values of $k$ and $m$.

## 5.1 The case $P_T = X^n$

Assume $p$ large enough. By Theorem 2.1, for any nonnegative integer $t$ there exist a family of nonnegative integers $(\mathcal{C}_S)_{S \in \Lambda_{m,\mathbb{N}_0(t)}}$ such that

$$(s_{k,m}(\mathbb{X}))^t = \sum_{(s_1,\ldots,s_m) \in \Lambda_{m,\mathbb{N}_0}(t)} C_{(s_1,\ldots,s_m)} X^{s_1} \otimes \cdots \otimes X^{s_m}.$$

Let $T$ be a linear operator on $V$ with minimal polynomial $P_T = X^n$. Since for $t \geq \ell + 1$ we have

$$s_1 + \cdots + s_m \geq k(\ell + 1) \geq m(n-1) + 1, \quad \forall S = (s_1, \ldots, s_m) \in \Lambda_{m,\mathbb{N}_0(t)}.$$

Then, for $S = (s_1, \ldots, s_m) \in \Lambda_{m,\mathbb{N}_0(t)}$, there exists $i \in \{1, \ldots, m\}$ such that

$$s_i \geq n.$$

Therefore $\deg P_{s_{k,m}(\mathbb{T})} \leq \ell + 1$. Using now Theorem 1.1 we conclude that

$$\deg(P_{s_{k,m}(\mathbb{T})}) = \ell + 1.$$

## 5.2 The case k=m

Let us assume that $k = m$, and prove (as stated in the introduction) that the polynomials

$$P_i(X) = X^n - A_{n-ik} X^{n-ik}$$

are all critical. Let $T_i \in L(V, V)$ such that $P_{T_i}(X) = P_i(X)$. Observe that, for $t \geq 0$,

$$S_{k,k}(\mathbb{X})^t = ((t, \cdots, t)).$$

Therefore

$$\begin{array}{lcl} ((0,\ldots,0))_{X=T_i} & = & [[0,\ldots,0]] \\ ((1,\ldots,1))_{X=T_i} & = & [[1,\ldots,1]] \\ & \vdots & \\ ((n-1,\ldots,n-1))_{X=T_i} & = & [[n-1,\ldots,n-1]] \\ ((n,\ldots,n))_{X=T_i} & = & A^k_{n-ik}[[n-ik,\ldots,n-ik]]. \end{array}$$

Hence, it follows at once that

$$\mathbb{S} = \{I, s_{k,m}(\mathbb{T}_i), \cdots, s_{k,m}(\mathbb{T}_i)^n\}$$

is linearly dependent over $\mathbb{F}$. But since

$$\ell = \left\lfloor \frac{m(n-1)}{k} \right\rfloor = n-1,$$

this proves that the degree of $P_{s_{k,m}(\mathbb{T}_i)}(X)$ is $\ell + 1$, for $i = 0, 1, \ldots, \lfloor \frac{n}{k} \rfloor$ (see (37)). ■

### 5.3 The case k=n=2

**Lemma 5.1** *Let $k = 2$ and suppose $P_T(X) = X^2 - a^2$. Then, for any $m \in \mathbb{N}$, $m \geq 2$, and $p$ sufficiently large, the set*

$$\mathbb{S} = \{I, s_{k,m}(\mathbb{T}), \cdots, s_{k,m}(\mathbb{T})^{\ell+1}\}$$

*is linearly dependent over $\mathbb{F}$.*

**Proof**: From the hypothesis we have that $n = 2$ and, for $s \geq 1$,

$$T^s = \begin{cases} a^s I & \text{if } s \text{ is even} \\ a^{s-1}T & \text{if } s \text{ is odd.} \end{cases} \tag{38}$$

Let us define

$$d_{2t} = [\underbrace{1, \cdots, 1}_{2t \text{ times}}, 0, \cdots, 0, ]$$

an element of the basis $\mathcal{B}$ (see remark 2.2(iii)).

Suppose that $((s_1, \cdots, s_m))$ $((\mathcal{E}_{\mathbb{F}}))$-occurs in the expansion of $s_{2,m}(\mathbb{X})^t$ (see (8)), then we must have $\sum s_j = 2t$, hence the number of odd entries $s_j$ is even. Therefore, from (38) we get (see (14) with $n = 2$)

$$((s_1, \cdots, s_m))_{X=T} = \mathcal{K}\,[[d_r]]$$

with $\mathcal{K} \in \mathbb{F}$ and where $r$ is the number of odd entries $s_j$. But this implies that, for any $t$

$$s_{2,m}(\mathbb{T})^t \ \in \ \langle [[d_0]], [[d_2]] \cdots, [[d_{2\ell}]] \rangle \ \text{ for } \ \ell = \left\lfloor \frac{m}{2} \right\rfloor \quad \text{(see (23))}.$$

And from this follows the result of this lemma.

**Corollary 5.1** $P_T(X) = X^2 - a^2$ *is a critical polynomial, for any* $m \geq 2$.

### 5.4 The Case: k=2 and m=n=3

Since we are now assuming $k = 2$ and $m = n = 3$, we have

$$\ell = \left\lfloor \frac{m(n-1)}{k} \right\rfloor = 3.$$

Let us write

$$T^3 = A_2 T^2 + A_1 T + A_0 I,$$

hence

$$T^4 = (A_2^2 + A_1) T^2 + (A_2 A_1 + A_0) T + A_2 A_0 I.$$

From (8), we have for every $t$

$$(s_{2,3}(\mathbb{X}))^t = \sum_{S \in \Pi} C_S \left( (s_1, s_2, s_3) \right)$$

where $\Pi$ is the set of all partitions of $2t$, having $s_j \leq t$, and $C_S$ is the number of (0,1)-matrices of type $3 \times t$, with row sum vector equal to $(s_1, s_2, s_3)$, whose column sums are equal to 2 (see theorem 2.1). For this particular case, this number can be easily calculated, and we refer the reader to [2, cor.1, prop.2.3] to have

$$C_S = \frac{t!}{(t - s_1)!(t - s_2)!(t - s_3)!}.$$

Now we can explicitly write the expression $(s_{2,3}(\mathbb{X}))^t$ for $1 \leq t \leq \ell + 1 = 4$

$$\begin{array}{lcl} (s_{2,3}(\mathbb{X}))^0 & = & ((0,0,0)) \\ (s_{2,3}(\mathbb{X}))^1 & = & ((1,1,0)) \\ (s_{2,3}(\mathbb{X}))^2 & = & ((2,2,0)) + 2\,((2,1,1)) \\ (s_{2,3}(\mathbb{X}))^3 & = & ((3,3,0)) + 3\,((3,2,1)) + 6\,((2,2,2)) \\ (s_{2,3}(\mathbb{X}))^4 & = & ((4,4,0)) + 4\,((4,3,1)) + 6\,((4,2,2)) + 12\,((3,3,2)) \end{array} \tag{39}$$

A simple use of lemma 2.2 (or via a tour of force) we have

$$((0,0,0))_{X=T} = \quad [[0,0,0]]$$

$$((1,1,0))_{X=T} = \quad [[1,1,0]]$$

$$((2,2,0))_{X=T} = \quad [[2,2,0]]$$

$$((2,1,1))_{X=T} = \quad [[2,1,1]]$$

$$((2,2,2))_{X=T} = \quad [[2,2,2]]$$

$$\begin{aligned} ((3,3,0))_{X=T} = \quad & A_2A_1[[2,1,0]] + 2A_2A_0[[2,0,0]] + 2A_1A_0[[1,0,0]] \\ & +A_1^2[[1,1,0]] + 3A_0^2[[0,0,0]] + A_2^2[[2,2,0]] \end{aligned}$$

$$((3,2,1))_{X=T} \quad = 2A_2[[2,2,1]] + A_0[[2,1,0]] + 2A_1[[2,1,1]]$$

$$\begin{aligned} ((4,4,0))_{X=T} = \quad & (A_2^2 + A_1)^2[[2,2,0]] \\ & +(A_2^2 + A_1)(A_2A_1 + A_0)[[2,1,0]] \\ & +2(A_2^2 + A_1)A_2A_0[[2,0,0]] \\ & +2(A_2A_1 + A_0)A_2A_0[[1,0,0]] \\ & +(A_2A_1 + A_0)^2[[1,1,0]] + 3A_0^2A_2^2[[0,0,0]] \end{aligned} \tag{40}$$

$$\begin{aligned} ((4,3,1))_{X=T} = \quad & 2A_2(A_2^2 + A_1)[[2,2,1]] + A_0(2A_2^2 + A_1)[[2,1,0]] \\ & +2A_2A_0^2[[1,0,0]] + 6(A_1A_2 + A_0)A_1[[1,1,1]] \\ & +2(2A_2^2A_1 + A_1^2 + A_2A_0)[[2,1,1]] \\ & +2(2A_0A_1A_2 + A_0^2)[[1,1,0]] \end{aligned}$$

$$\begin{aligned} ((3,3,2))_{X=T} = \quad & 3A_2^2[[2,2,2]] + 2A_2A_1[[2,2,1]] + A_1A_0[[2,1,0]] \\ & +A_0^2[[2,0,0]] + 2A_0A_2[[2,2,0]] \\ & +A_1^2[[2,1,1]] \end{aligned}$$

$$\begin{aligned} ((4,2,2))_{X=T} = \quad & 3(A_2^2 + A_1)\,[[2,2,2]] + (A_2A_1 + A_0)[[2,2,1]] \\ & +A_0A_2[[2,2,0]]. \\ & +A_1^2[[2,1,1]] \end{aligned}$$

$$\begin{aligned} ((4,2,2))_{X=T} = \quad & 3(A_2^2 + A_1)\,[[2,2,2]] + (A_2A_1 + A_0)[[2,2,1]] \\ & +A_0A_2[[2,2,0]]. \end{aligned}$$

In order to continue this investigation we need a closer look at list (40) of possible ascendents at the levels 1,2,3,4, of the elements

$$[[1,0,0]],\ [[1,1,1]],\ [[2,0,0]],\ [[2,1,0]],\ [[2,2,1]],\ [[2,2,2]].$$

There are only 6 possible ascendents at the list (40) above, thus from inspection we can make a list of possible ascendents for the group above:

| | | |
|---|---|---|
| $[[1,0,0]]$ | possible ascendents: | $((3,3,0))$, $((4,4,0))$, $((4,3,1))$; |
| $[[1,1,1]]$ | possible ascendents: | $((4,3,1))$; |
| $[[2,0,0]]$ | possible ascendents: | $((3,3,0))$, $((4,4,0))$, $((3,3,2))$; |
| $[[2,1,0]]$ | possible ascendents: | $((3,3,0))$, $((4,4,0))$, $((4,3,1))$, $((3,2,1))$, $((3,3,2))$; |
| $[[2,2,1]]$ | possible ascendents: | $((3,2,1))$, $((4,3,1))$, $((4,2,2))$, $((3,3,2))$; |
| $[[2,2,2]]$ | possible ascendents: | $((4,2,2))$, $((3,3,2))$, $((2,2,2))$. |

**Lemma 5.2** *For $p \geq 5$, the set*

$$\mathbb{S} = \{I, s_{2,3}(\mathbb{T}), (s_{2,3}(\mathbb{T}))^2, (s_{2,3}(\mathbb{T}))^3, (s_{2,3}(\mathbb{T}))^4\}$$

*is linearly independent if $A_1(A_2A_1 + A_0) \neq 0$.*

**Proof**: Looking at (40) we can see that $[[1,1,1]]$ has only one ascendent, $((4,3,1))$, and it is at level 4. From (39) and (40) it follows that

$$(s_{2,3}(\mathbb{T}))^4 = 24\, A_1(A_2A_1 + A_0)\,[[1,1,1]] + \mathcal{R}$$

with $\mathcal{R} \in \langle [[B]] \mid [[B]] \in [[\mathcal{B}]] - \{[[1,1,1]]\}\rangle$. Hence $[[1,1,1]]$ $[[\mathcal{B}]]$-occurs in $(s_{2,3}(\mathbb{T}))^4$ if $A_1(A_2A_1 + A_0) \neq 0$, since we are assuming $p \geq 5$. The conclusion of the lemma follows now from proposition 4.1. ■

**Lemma 5.3** *Suppose $p \geq 7$ and $A_2A_1 + A_0 = 0$. If $A_0 \cdot A_1 \cdot A_2 \neq 0$ then the set $\mathbb{S}$ is linearly independent.*

**Proof**: Let $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$, and suppose we can write:

$$(s_{2,3}(\mathbb{T}))^4 = \sum_{i=0}^{3} \alpha_i\ (s_{2,3}(\mathbb{T}))^i.$$

In particular, looking at (39) and (40), we have that $[[2,1,0]]$, $[[2,2,2]]$ and $[[2,2,1]]$ $[[\mathcal{B}]]$-occur only at levels 3 and 4. Therefore (since $A_2A_1 + A_0 = 0$)

$$\begin{aligned}\alpha_3(A_2A_1 + A_0 + 2A_0)\,[[2,1,0]] = (4A_0(2A_2^2 + A_1) + 12A_1A_0)\,[[2,1,0]] &\implies\\ 2A_0\alpha_3 = 16A_0A_1 + 8A_0A_2^2 &\implies\\ \alpha_3 = 8A_1 + 4A_2^2,&\end{aligned}$$

$$\begin{aligned}6\alpha_3\,[[2,2,2]] = (36A_2^2 + 18(A_2^2 + A_1))\,[[2,2,2]] &\implies\\ \alpha_3 = 9A_2^2 + 3A_1.&\end{aligned}$$

From these two equations we have

$$A_2^2 = A_1 \quad \text{and } \alpha_3 = 12A_1. \tag{41}$$

Now

$$\begin{aligned}6\alpha_3\, A_2\,[[2,2,1]] = (24A_2A_1 + 8A_2(A_2^2 + A_1))\,[[2,2,1]] &\implies\\ 3\alpha_3 = 4A_2^2 + 16A_1.&\end{aligned}$$

Replacing $A_2^2 = A_1$ in the equation above we have $3\alpha_3 = 20A_1$, which implies $16A_1 = 0$, by (41). This is a contradiction for $p \geq 7$ and $A_1 \neq 0$, hence the set $\mathbb{S}$ must be linearly independent. ■

**Lemma 5.4** *If $p > 23$, $T^3 \neq 0$ and $A_1 = 0$ then the set $\mathbb{S}$ is linearly independent.*

**Proof**: With this hypothesis applied to (40) we see that the element $[[1, 0, 0]]$ only appears at level 4 with coefficient $10A_2A_0^2$ (see (39) also). If $A_2 = 0$, then the term $[2, 0, 0]$ will only occur at level 4 with coefficient $12A_0^2$. Since we can not have $A_2 = A_1 = A_0 = 0$ (for $T^3 \neq 0$), the set $\mathbb{S}$ must be linearly independent. Now suppose $A_0 = 0$ and $A_2 \neq 0$. As in the proof of the previous lemma, let us try to write $(s_{2,3}(\mathbb{T}))^4$ as a linear combination of the smaller powers. If it happens (with the hypothesis of $A_1 = 0$) we must have

$$\begin{gathered} 6\alpha_3\,[[2, 2, 2]] = (36A_2^2 + 18A_2^2)\,[[2, 2, 2]] \implies \\ \alpha_3 = 9A_2^2, \end{gathered}$$

and

$$\begin{gathered} 6\alpha_3\,A_2\,[[2, 2, 1]] = 8A_2^3\,[[2, 2, 1]] \implies \\ 3\alpha_3 = 4A_2^2. \end{gathered}$$

But this implies that $23A_2 = 0$, a contradiction. Hence the set $\mathbb{S}$ is linearly independent.

■

**Lemma 5.5** *Suppose $p \geq 7$ and zero is not a double root of $P_T(X)$. If $A_1 = 0$ then the set $\mathbb{S}$ is linearly independent.*

**Proof**: From the proof of lemma 5.4 above, the hypothesis $A_1 = 0$ implies that if $10A_2A_0^2 \neq 0$ then $\mathbb{S}$ is linearly independent. Furthermore, the condition $A_2 = 0$ also gives that $\mathbb{S}$ is linearly independent. So assume $A_0 = 0$. But this, together with $A_1 = 0$, tell us that $P_T(X) = X^3 - A_2X^2$, which has zero as a double root contradicting the hypothesis. Hence we must have $A_2.A_0 \neq 0$, which gives that the set $\mathbb{S}$ is linearly independent.

■

**Lemma 5.6** *If $p \geq 5$ and $A_2 = A_0 = 0$ then the set $\mathbb{S}$ is linearly* **dependent***.*

**Proof**: With these hypothesis we can easily calculate:

$$\begin{aligned} &((3, 3, 0))_{X=T} = A_1^2[[1, 1, 0]] && ((3, 2, 1))_{X=T} = 2\,A_1\,[[2, 1, 1]] \\ &((4, 4, 0))_{X=T} = A_1^2[[2, 2, 0]] && ((4, 3, 1))_{X=T} = 2A_1^2[[2, 1, 1]] \\ &((3, 3, 2))_{X=T} = A_1^2[[2, 1, 1]] && ((4, 2, 2))_{X=T} = 3A_1\,[[2, 2, 2]]. \end{aligned}$$

Now we can write (see (39)), for $p \geq 5$:

$$\begin{aligned} (s_{2,3}(\mathbb{T}))^4 &= A_1^2[[2, 2, 0]] + 20A_1^2[[2, 1, 1]] + 18A_1[[2, 2, 2]] \\ (s_{2,3}(\mathbb{T}))^3 &= A_1^2[[1, 1, 0]] + 6A_1[[2, 1, 1]] + 6[[2, 2, 2]]. \end{aligned}$$

Hence we can write

$$(s_{2,3}(\mathbb{T}))^4 = 3A_1(s_{2,3}(\mathbb{T}))^3 + A_1^2(s_{2,3}(\mathbb{T}))^2 - 3A_1^3(s_{2,3}(\mathbb{T}))^1,$$

which gives the result. ■

**Theorem 5.1** *Suppose that either*

**(i)** $p > 23$ *or*

**(ii)** $p \geq 7$ *and zero is not a double root of* $P_T(X)$*.*

*Then the set*

$$\mathbb{S} = \{I, s_{2,3}(\mathbb{T}), (s_{2,3}(\mathbb{T}))^2, (s_{2,3}(\mathbb{T}))^3, (s_{2,3}(\mathbb{T}))^4\}$$

*is linearly dependent if and only if* $A_2 = A_0 = 0$*.*

**Proof**: If $A_2 = A_0 = 0$ then the lemma 5.6 tells us that $\mathbb{S}$ is linearly dependent. Conversely, suppose $\mathbb{S}$ is linearly dependent. Then we must have $A_1 \neq 0$, otherwise lemma 5.5, together with the hypothesis would prove that the set $\mathbb{S}$ is linearly independent. But now lemma 5.2 shows that $A_2A_1 + A_0 = 0$. If $A_2.A_0 \neq 0$, then lemma 5.3 would prove that $\mathbb{S}$ is linearly independent. Hence we must have $A_2A_1 + A_0 = 0$ and either $A_2 = 0$ or $A_0 = 0$. But this implies $A_2 = A_0 = 0$ as desired.

■

**Corollary 5.2** *Assuming the same conditions as in the theorem above, the polynomial* $P_T(X) = X^3 - A_2X^2 - A_1X - A_0$ *is critical if and only if* $A_2 = A_0 = 0$*.*

■

# References

[1] Peter J. Cameron, *Permutation Groups*, Cambridge University Press Cambridge (1999).

[2] J.A. Dias da Silva and H. Godinho, *Generalized Derivations and Additive Theory.* Linear Algebra and its Applications, **342**, (2002), 1-15.

[3] Marvin Marcus, *Finite Dimensional Multilinear Algebra-Part I*, Marcel Dekker Inc, (1973).