Journal of Number Theory **72**, 153–173 (1998)
Article No. NT982269

A Pollard Type Result for Restricted Sums

Cristina Caldeira*

Departamento de Matemática, Universidade de Coimbra, 3000 Coimbra, Portugal

and

J. A. Dias da Silva†

Centro de Álgebra da Universidade de Lisboa, Av Gama Pinto 2, 1699 Lisboa Codex, Portugal

Communicated by Alan C. Woods

Received August 9, 1996; revised December 16, 1997

Let $\mathbb{F}$ be an arbitrary field. Let p be the characteristic of $\mathbb{F}$ in case of finite characteristic and ∞ if $\mathbb{F}$ has characteristic 0. Let A be a finite subset of $\mathbb{F}$. By $\bigwedge^2 A$ we denote the set $\{a+b \mid a, b \in A \text{ and } a \neq b\}$. For $c \in \bigwedge^2 A$, let $\nu_c^{(R)}$ be one-half of the cardinality of the set of pairs (a, b) satisfying $a \neq b$ and $a+b=c$. Denote by $\mu_i^{(R)}$ the cardinality of the set $\{c \in \bigwedge^2 A \mid \nu_c^{(R)} \geqslant i\}$. We prove that, for $t=1, ..., \lfloor |A|/2 \rfloor$, $\sum_{i=1}^{t} \mu_i^{(R)} \geqslant t \min\{p, 2(|A|-t)-1\}$. For $\mathbb{F}=\mathbb{Z}_p$ and $t=1$ we get the Erdős–Heilbronn conjecture, first proved by J. A. Dias da Silva and Y. O. Hamidoune (*Bull. London Math. Soc.* **26**, 1994, 140–146).

1. INTRODUCTION

Let $\mathbb{F}$ be an arbitrary field. Let p be the characteristic of $\mathbb{F}$ in case of finite characteristic and ∞ if $\mathbb{F}$ has characteristic 0. Given $b \in \mathbb{R}$ we write $\lceil b \rceil$ ($\lfloor b \rfloor$) for the smallest integer greater than or equal to b (the greatest integer less than or equal to b). For $a \in \mathbb{N}$ let $[1, a]$ denote the set $\{x \in \mathbb{N}: 1 \leqslant x \leqslant a\}$. Let A and B be nonempty finite subsets of $\mathbb{F}$. By $A+B$ we denote the set of elements $a+b$ with $a \in A$ and $b \in B$. For each element $c \in \mathbb{F}$, let $\nu_c(A, B)$ be the cardinality of the set of pairs (a, b) such that $a+b=c$. Let i be a positive integer. We denote by $\mu_i(A, B)$, or briefly

* This research was done within the activities of "Centro de Matemática da Universidade de Coimbra" and partially supported by PRAXIS project "Álgebra e Matemáticas Discretas."

† This research was done within the activities of "Centro de Álgebra da Universidade de Lisboa" and partially supported by PRAXIS project "Álgebra e Matemáticas Discretas."

0022-314X/98 $25.00

by μ_i, the cardinality of the set of the elements $c \in A+B$ for which $v_c(A, B)$ is greater than or equal to i.

Let X be a set. We denote by $|X|$ the cardinality of X. If $|X|=k$ we say that X is a k-set. In [1] we prove the following theorem:

1.1. THEOREM. *Let A and B be finite nonempty subsets of $\mathbb{F}$. Then for $t=1, 2, ..., \min\{|A|, |B|\}$ we have*

$$\sum_{i=1}^{t} \mu_i \geqslant t \min\{p, |A|+|B|-t\}.$$

This result is an extension to an arbitrary field of a theorem proved by Pollard [4, 5], for $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number. Notice that the case where $t=1$ is the well known Cauchy–Davenport Theorem.

In this paper we prove, for restricted sums, an analogue of Theorem 1.1. Let A be a finite subset of $\mathbb{F}$. We denote by $\bigwedge^2 A$ the set

$$\{a+b \mid a, b \in A \text{ and } a \neq b\}.$$

For $c \in \bigwedge^2 A$, let $v_c^{(R)}$ be one-half of the cardinality of the set of pairs (a, b) satisfying $a \neq b$ and $a+b=c$. Denote by $\mu_i^{(R)}$ the cardinality of the set

$$\{c \in \textstyle\bigwedge^2 A \mid v_c^{(R)} \geqslant i\}.$$

We prove that, for $t=1, ..., \lfloor |A|/2 \rfloor$,

$$\sum_{i=1}^{t} \mu_i^{(R)} \geqslant t \min\{p, 2(|A|-t)-1\}. \tag{1}$$

This lower bound is tight and the equality in (1) is attained when A is an arithmetic progression.

For $\mathbb{F} = \mathbb{Z}_p$ and $t=1$ we get the Erdős–Heilbronn conjecture [3], first proved in [2].

2. COMBINATORIAL BACKGROUND

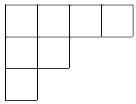
A sequence of integers $\lambda = (\lambda_1, ..., \lambda_t)$ will be called a *partition* if $0 \leqslant \lambda_1 \leqslant \cdots \leqslant \lambda_t$. We say that λ is a partition of k if

$$\sum_{i=1}^{t} \lambda_i = k.$$

The length of the partition λ is the number of its nonzero terms. Let s be a positive integer. The set of the partitions of k of length at most s is denoted by $\mathscr{P}_{k,s}$. Let μ be a partition of k and let λ be a partition of $k+1$. We write $\mu \to \lambda$ if there exists j such that $\lambda_i = \mu_i + \delta_{ij}$ for all i, where δ_{ij} is the Kronecker symbol.

To each partition $\lambda = (\lambda_1, ..., \lambda_t)$ of k there corresponds a Young Diagram, $[\lambda]$, which consists of k boxes in t rows starting in the same column, where the ith row consists of λ_{t-i+1} boxes, $1 \leqslant i \leqslant t$.

EXAMPLE. Let $k = 7$ and $\lambda = (1, 2, 4)$. Then

$[\lambda] =$ 

The box that lies in ith row and jth column of $[\lambda]$ is called the (i, j)-*box* of $[\lambda]$. The (i, j)-*hook* of $[\lambda]$, $H^{\lambda}_{i,j}$, is the collection of boxes consisting of the (i, j)-box along with the boxes of the same row to the right and the boxes of the same column under it. The number of boxes of $H^{\lambda}_{i,j}$ is denoted by $h^{\lambda}_{i,j}$. For a partition of k of length t, $\lambda = (\lambda_1, ..., \lambda_t)$, let

$$P(\lambda) = \prod_{i=1}^{t} \prod_{j=1}^{\lambda_{t-i+1}} h^{\lambda}_{i,j}.$$

In [2] the following result is established:

2.2. PROPOSITION. *Let* $\lambda \in \mathscr{P}_{k+1,s}$. *Then*

$$\sum_{\substack{\mu \in \mathscr{P}_{k,s} \\ \mu \to \lambda}} \frac{1}{P(\mu)} = \frac{k+1}{P(\lambda)}.$$

Using this proposition it is easy to see that, if λ is a partition of k, then $k!/P(\lambda)$ is an integer. The next result is easy to prove, so its proof will be left to the reader.

2.3. PROPOSITION. *For* $\mu = (\mu_1, \mu_2)$ *we have*

$$P(\mu) = \frac{(\mu_2 + 1)!\, \mu_1!}{\mu_2 - \mu_1 + 1}.$$

3. AUXILIARY RESULTS

Let $\mathbb{F}$ be an arbitrary field and denote by $\overline{\mathbb{F}}$ the algebraic closure of $\mathbb{F}$. Let $V \neq \{0\}$ be an m-dimensional vector space over the field $\mathbb{F}$ and let f be a linear operator on V. We use P_f to denote the minimal polynomial of f and $\alpha_{f,1} \mid \cdots \mid \alpha_{f,m} = P_f$ to denote the invariant factors of f (so that each $\alpha_{f,i}$ divides all subsequent polynomials $\alpha_{f,i+1}, ..., \alpha_{f,m}$). For every $v \in V$, $\mathscr{C}_f(v)$ is the f-cyclic space of v, i.e.,

$$\mathscr{C}_f(v) = \langle f^i(v) \colon i \in \mathbb{Z}^+ \rangle,$$

where $\langle X \rangle$ denotes the linear span of X and $\mathbb{Z}^+$ denotes the set of nonnegative integers. We use $\sigma(f)$ to denote the spectrum of f, i.e., $\sigma(f)$ is the family of the m roots of the characteristic polynomial of f in $\overline{\mathbb{F}}$. Let i be a positive integer. We denote by $m_i(f)$ the number of distinct roots of the characteristic polynomial of f with algebraic multiplicity greater than or equal to i. Notice that $m_1(f)$ is the number of distinct eigenvalues of f and for a diagonal linear operator f,

$$m_i(f) = \deg(\alpha_{f,m-i+1}), \qquad i = 1, ..., m.$$

3.4. Definition. Let $a = (a_1, ..., a_n)$ and $b = (b_1, ..., b_n)$ be two sequences of nonnegative integers. Denote by $(\bar{a}_1, ..., \bar{a}_n)$ and $(\bar{b}_1, ..., \bar{b}_n)$ the reordering, in a nonincreasing way, of a and b, respectively. We say that a *weakly dominates* b and we write

$$a \sqsupseteq b$$

if

$$\sum_{i=1}^{k} \bar{a}_i \geqslant \sum_{i=1}^{k} \bar{b}_i, \qquad k = 1, ..., n.$$

If $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ we say that a *dominates* b and we write $a \succcurlyeq b$.

In [1] the following result was proved:

3.5. Lemma. *Let V be a finite dimensional vector space over the field $\mathbb{F}$ of dimension m. Let f be a linear operator on V. Let $s_1, ..., s_t$ be positive integers. If there exist $v_1, ..., v_t \in V$ such that*

$$\bigcup_{i=1}^{t} \{v_i, f(v_i), f^2(v_i), ..., f^{s_i-1}(v_i)\}$$

is a linearly independent $(s_1 + \cdots + s_t)$*-set then*

$$(s_1, ..., s_t) \sqsubseteq (\deg(\alpha_{f,m}), ..., \deg(\alpha_{f,m-t+1})).$$

For the benefit of the reader we reproduce here the proof of this lemma. For this we need some definitions and results.

3.6. DEFINITION. Let $v_1, ..., v_t \in V$ and let f be a linear operator on V. The subspace

$$\mathscr{C}_f(v_1, ..., v_t) = \langle f^j(v_i) \colon j \in \mathbb{Z}^+, i = 1, ..., t \rangle$$

will be called the *generalized f-cyclic subspace associated to* $v_1, ..., v_t$. We say that the pair $((v_1, ..., v_t), f)$, or the generalized f-cyclic subspace $\mathscr{C}_f(v_1, ..., v_t)$, is *completely controllable* if

$$\mathscr{C}_f(v_1, ..., v_t) = V.$$

3.7. DEFINITION. Let f be a linear operator on V and let $v_1, ..., v_t \in V$. A basis, $\mathscr{B}$, of $\mathscr{C}_f(v_1, ..., v_t)$ selected from

$$\{f^j(v_i) \colon j \in \mathbb{Z}^+, i = 1, ..., t\}$$

is *nice* if, for $0 \leqslant i \leqslant k-1$, $f^i(v_j) \in \mathscr{B}$ provided that $f^k(v_j) \in \mathscr{B}$.

Let

$$\mathscr{B} = \bigcup_{i=1}^{t} \{v_i, f(v_i), f^2(v_i), ..., f^{r_i - 1}(v_i)\}$$

be a nice basis of $\mathscr{C}_f(v_1, ..., v_t)$. We say that the nonnegative integers $r_1, ..., r_t$ are *indices of* $\mathscr{B}$.

Let $v_1, ..., v_t \in V$. If

$$\mathscr{I} = \bigcup_{i=1}^{t} \{v_i, f(v_i), f^2(v_i), ..., f^{s_i - 1}(v_i)\}$$

is a linearly independent $(s_1 + \cdots + s_t)$-set, we say that $\mathscr{I}$ is a $((v_1, ..., v_t), f)$-*nice independent set* and we call the nonnegative integers $s_1, ..., s_t$ *indices of* $\mathscr{I}$.

Notice that it is possible to associate more than one list of indices to a $((v_1, ..., v_t), f)$-nice independent set. For instance if v_1, v_2, v_3 are linearly independent vectors of V and $f(v_1) = v_2$,

$$\mathscr{I} = \{v_1, v_2, v_3\} = \{v_1, f(v_1), v_3\}$$

is a $((v_1, v_2, v_3), f)$-nice independent set and both $(1, 1, 1)$ and $(2, 0, 1)$ are lists of indices of $\mathscr{I}$.

In [6], the following result is proved.

3.8. PROPOSITION. *Let A be an $\ell \times \ell$ matrix and let $\alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_\ell$ be its invariants factors. Let m be a positive integer satisfying $m > \ell$. Let $\gamma_1, ..., \gamma_m$ be monic polynomials over $\mathbb{F}$ such that $\deg(\gamma_1 \cdots \gamma_m) = m$ and $\gamma_1 \mid \cdots \mid \gamma_m$. Then there exist $C \in \mathbb{F}^{(m-\ell)\times \ell}$ and $D \in \mathbb{F}^{(m-\ell)\times(m-\ell)}$ such that the $m \times m$ matrix*

$$\begin{bmatrix} A & 0 \\ C & D \end{bmatrix}$$

has invariant factors $\gamma_1, ..., \gamma_m$, if and only if

$$\gamma_i \mid \alpha_i \mid \gamma_{i+m-\ell}, \qquad i = 1, ..., \ell.$$

The next theorem is proved in [8, Corollary 2.2].

3.9. THEOREM. *Let V be an m-dimensional vector space over the field $\mathbb{F}$. Let f be a linear operator on V and let $r_1, ..., r_t$ be positive integers. Then there exist linearly independent vectors $v_1, ..., v_t$, such that $\mathscr{C}_f(v_1, ..., v_t)$ is completely controllable, and a nice basis of $\mathscr{C}_f(v_1, ..., v_t)$ with indices $r_1, ..., r_t$ if and only if the following conditions hold:*

$$\alpha_{f,i} = 1, \qquad i = 1, ..., m - t,$$

and

$$(r_1, ..., r_t) \preccurlyeq (\deg(\alpha_{f,m}), ..., \deg(\alpha_{f,m-t+1})).$$

The next theorem is proved in [1] and states a necessary condition for the existence of nice bases with prescribed indices when the constraint of complete controllability is skipped.

3.10. THEOREM. *Let V be an m-dimensional vector space over the field $\mathbb{F}$ and let f be a linear operator on V. Let $r_1, ..., r_t$ be positive integers. If there exist linearly independent vectors $v_1, ..., v_t$ and a nice basis of $\mathscr{C}_f(v_1, ..., v_t)$ with indices $r_1, ..., r_t$, then*

$$(r_1, ..., r_t) \sqsubseteq (\deg(\alpha_{f,m}), ..., \deg(\alpha_{f,m-t+1})).$$

Proof. Let $U = \mathscr{C}_f(v_1, ..., v_t)$ and let $\ell = \dim(U)$. As usual, let $f_{|U}$ denote the restriction of f to U. Clearly, $\mathscr{C}_{f|U}(v_1, ..., v_t)$ is completely controllable and from Theorem 3.9 we have

$$(r_1, ..., r_t) \preccurlyeq (\deg(\alpha_{f_{|U}, \ell}), ..., \deg(\alpha_{f_{|U}, \ell - t + 1})). \tag{2}$$

By the transposed version of Proposition 3.8 we know that

$$\alpha_{f, i} \mid \alpha_{f_{|U}, i} \mid \alpha_{f, i+m-\ell}, \qquad i = 1, ..., \ell.$$

Therefore

$$\alpha_{f_{|U}, \ell} \alpha_{f_{|U}, \ell - 1} \cdots \alpha_{f_{|U}, \ell - j} \mid \alpha_{f, m} \alpha_{f, m-1} \cdots \alpha_{f, m-j}, \qquad j = 0, ..., \ell - 1. \tag{3}$$

Taking degrees in (3) we have

$$\sum_{i=0}^{j} \deg(\alpha_{f_{|U}, \ell - i}) \leqslant \sum_{i=0}^{j} \deg(\alpha_{f, m-i}), \qquad j = 0, ..., \ell - 1. \tag{4}$$

Since $v_1, ..., v_t \in U$ are linearly independent vectors we have $t \leqslant \dim(U) = \ell$. Therefore, from (4) and (2) we get

$$(r_1, ..., r_t) \sqsubseteq (\deg(\alpha_{f, m}), ..., \deg(\alpha_{f, m-t+1})). \quad \blacksquare$$

Proof of Lemma 3.5. Let $s_1, ..., s_t$ be positive integers and suppose that

$$\bigcup_{i=1}^{t} \{v_i, f(v_i), f^2(v_i), ..., f^{s_i - 1}(v_i)\}$$

is a linearly independent $(s_1 + \cdots + s_t)$-set. In order to use Theorem 3.10, we complete this set to a nice basis of $\mathscr{C}_f(v_1, ..., v_t)$. For each $q \in \{1, ..., t\}$, let r_q be the positive integer such that

$$\left(\bigcup_{j=1}^{q} \{v_j, f(v_j), ..., f^{r_j - 1}(v_j)\}\right) \cup \left(\bigcup_{i=q+1}^{t} \{v_i, f(v_i), f^2(v_i), ..., f^{s_i - 1}(v_i)\}\right)$$

is a linearly independent $(r_1 + \cdots + r_q + s_{q+1} + \cdots + s_t)$-set and

$$f^{r_q}(v_q) \in \left\langle \left(\bigcup_{j=1}^{q} \{v_j, f(v_j), ..., f^{r_j - 1}(v_j)\}\right) \cup \left(\bigcup_{i=q+1}^{t} \{v_i, f(v_i), f^2(v_i), ..., f^{s_i - 1}(v_i)\}\right)\right\rangle.$$

It is obvious, from the definitions, that

$$f\left(\left\langle \bigcup_{i=1}^{t} \{v_i, ..., f^{r_i-1}(v_i)\} \right\rangle\right) \subseteq \left\langle \bigcup_{i=1}^{t} \{v_i, ..., f^{r_i-1}(v_i)\} \right\rangle. \tag{5}$$

We now show that

$$\bigcup_{i=1}^{t} \{v_i, ..., f^{r_i-1}(v_i)\}$$

is a maximal linearly independent set contained in $\mathscr{C}_f(v_1, ..., v_t)$. Assume, for a contradiction, that for some $i \in \{1, ..., t\}$ and some $r \in \mathbb{N}$,

$$f^r(v_i) \notin \left\langle \bigcup_{i=1}^{t} \{v_i, ..., f^{r_i-1}(v_i)\} \right\rangle. \tag{6}$$

Without loss of generality we can suppose that r is the smallest integer with this property. Then

$$f^{r-1}(v_i) \in \left\langle \bigcup_{i=1}^{t} \{v_i, ..., f^{r_i-1}(v_i)\} \right\rangle$$

and

$$f^r(v_i) \in f\left(\left\langle \bigcup_{i=1}^{t} \{v_i, ..., f^{r_i-1}(v_i)\} \right\rangle\right).$$

Using (5) we get

$$f^r(v_i) \in \left\langle \bigcup_{i=1}^{t} \{v_i, ..., f^{r_i-1}(v_i)\} \right\rangle,$$

which contradicts (6).

By Theorem 3.10 we conclude that

$$(r_1, ..., r_t) \sqsubseteq (\deg(\alpha_{f,m}), ..., \deg(\alpha_{f,m-t+1})).$$

But, since by construction, we have $s_i \leqslant r_i$, $i = 1, ..., t$, we get from the former inequalities

$$(s_1, ..., s_t) \sqsubseteq (\deg(\alpha_{f,m}), ..., \deg(\alpha_{f,m-t+1})). \quad \blacksquare$$

Let $\bigwedge^2 V$ be the second exterior power of V. Let f be a linear operator on V. We denote by $D(f)$ the induced operator on $\bigwedge^2 V$, defined by

$$D(f)(v_1 \wedge v_2) = f(v_1) \wedge v_2 + v_1 \wedge f(v_2), \qquad v_1, v_2 \in V.$$

3.11. Proposition. *Given a finite subset $A \subseteq \mathbb{F}$, let V be a vector space over $\mathbb{F}$ of dimension $|A|$. Let f be a linear operator on V with spectrum $\sigma(f) = A$. Then*

$$m_i(D(f)) = \mu_i^{(R)}, \qquad i \in \mathbb{N}.$$

Proof. Suppose $A = \{a_1, ..., a_n\}$. It is easily derived from the definitions that the spectrum of $D(f)$ is the family

$$(a_j + a_k)_{1 \leqslant j < k \leqslant n}.$$

Then for $i \in \mathbb{N}$ we have

$$\begin{aligned} m_i(D(f)) &= |\{x \in \textstyle\bigwedge^2 A \colon |\{(j, k) \colon 1 \leqslant j < k \leqslant n \text{ and } a_j + a_k = x\}| \geqslant i\}| \\ &= \mu_i^{(R)}. \quad \blacksquare \end{aligned}$$

Let f be a linear operator on V and let $v \in V$ be such that $n = \dim \mathscr{C}_f(v) \geqslant 2$.

3.12. Definition. Let $x \in \bigwedge^2 \mathscr{C}_f(v)$. We define the *weight of* x as the maximal element of the set

$$\{i + j \colon x \text{ has a nonzero coefficient of } f^i(v) \wedge f^j(v)\}.$$

The following results will allow us to evaluate the weight of $D(f)^k\,(f^{j-1}(v) \wedge f^j(v))$.

3.13. Lemma. *For every $k \in \mathbb{Z}^+$ and $j \in \mathbb{N}$*

$$D(f)^k\,(f^{j-1}(v) \wedge f^j(v)) = \sum_{\lambda \in \mathscr{P}_{k,2}} \frac{k!}{P(\lambda)}\, f^{\lambda_1 + j - 1}(v) \wedge f^{\lambda_2 + j}(v).$$

Proof. We use induction on k. For $k = 0$ the result is trivial. Observe now that, for $\lambda \in \mathscr{P}_{k,2}$,

$$D(f)(f^{\lambda_1 + j - 1}(v) \wedge f^{\lambda_2 + j}(v)) = \sum_{\substack{\beta \in \mathscr{P}_{k+1,2} \\ \lambda \to \beta}} f^{\beta_1 + j - 1}(v) \wedge f^{\beta_2 + j}(v). \tag{7}$$

We have now, using the induction hypothesis,

$$
\begin{aligned}
D(f)^{k+1}&\,(f^{j-1}(v) \wedge f^{j}(v)) \\
&= \sum_{\lambda \in \mathscr{P}_{k,2}} \frac{k!}{P(\lambda)} \sum_{\substack{\beta \in \mathscr{P}_{k+1,2} \\ \lambda \to \beta}} f^{\beta_1+j-1}(v) \wedge f^{\beta_2+j}(v) \\
&= \sum_{\beta \in \mathscr{P}_{k+1,2}} \left(\sum_{\substack{\lambda \in \mathscr{P}_{k,2} \\ \lambda \to \beta}} \frac{k!}{P(\lambda)} \right) f^{\beta_1+j-1}(v) \wedge f^{\beta_2+j}(v) \\
&= \sum_{\beta \in \mathscr{P}_{k+1,2}} \frac{(k+1)!}{P(\beta)} f^{\beta_1+j-1}(v) \wedge f^{\beta_2+j}(v).
\end{aligned}
$$

The last equality follows from Proposition 2.2. ∎

3.14. Lemma. *For $k \in \mathbb{Z}^+$ and $j \in \mathbb{N}$ there exists a family of elements of $\mathbb{F}$, $(b_\nu)_{\substack{0 \leqslant \nu_1 \leqslant \nu_2 \leqslant n-2 \\ \nu_1+\nu_2 \leqslant k+2j-3}}$, such that*

$$
D(f)^{k}\,(f^{j-1}(v) \wedge f^{j}(v)) = \sum_{\substack{\lambda \in \mathscr{P}_{k,2} \\ \lambda_2 \leqslant n-j-1}} \frac{k!}{P(\lambda)} f^{\lambda_1+j-1}(v) \wedge f^{\lambda_2+j}(v)
$$

$$
+ \sum_{\substack{0 \leqslant \nu_1 \leqslant \nu_2 \leqslant n-2 \\ \nu_1+\nu_2 \leqslant k+2j-3}} b_\nu f^{\nu_1}(v) \wedge f^{\nu_2+1}(v).
$$

Proof. We use Lemma 3.13 and isolate the terms $f^{\lambda_1+j-1}(v) \wedge f^{\lambda_2+j}(v)$ with $\lambda_2 + j \geqslant n$. Clearly, each of these terms can be written as a linear combination of $f^{\nu_1}(v) \wedge f^{\nu_2}(v)$, where $0 \leqslant \nu_1 < \nu_2 \leqslant n-1$ and $\nu_1+\nu_2 \leqslant (\lambda_1+j-1)+(\lambda_2+j)-1 = k+2j-2$. The result follows. ∎

3.15. Theorem. *For $j \in \mathbb{N}$ and $0 \leqslant k \leqslant \min\{p-1, 2n-2j-2\}$, the weight of*

$$
D(f)^{k}\,(f^{j-1}(v) \wedge f^{j}(v))
$$

is $k+2j-1$.

Proof. Clearly the weight does not exceed $k+2j-1$. On the other hand, let $\lambda = (\lfloor k/2 \rfloor, \lceil k/2 \rceil) \in \mathscr{P}_{k,2}$. Since $k \leqslant 2n-2j-2$ we have $\lambda_2 \leqslant n-j-1$. We now use Lemma 3.14 and notice, that the coefficient $k!/P(\lambda)$ is not 0 in $\mathbb{F}$ as $k < p$. ∎

3.16. LEMMA. *Let $\mathbb{F}$ and p be as usual. Let $a, b, k \in \mathbb{Z}^+$ satisfy $b+2k \leqslant a < p$. Then the $(k+1)\times(k+1)$ matrix over $\mathbb{F}$, $C(a, b, k) = [c_{ij}]$ where*

$$c_{ij} = \begin{cases} \dfrac{(a-i+1)!\,(b+i-1)!}{(a-i-j+2)!\,(b+i-j)!} & \text{if} \quad b+i-j \geqslant 0 \\ 0 & \text{if} \quad b+i-j < 0, \end{cases}$$

is invertible.

Proof. We proceed by induction on k. If $k=0$ we have

$$C(a, b, 0) = [1].$$

Assume now that $k \geqslant 1$. Let J be the $(k+1)\times(k+1)$ matrix, with the $(i+1, i)$ entries, $i = 1, ..., k$, equal to 1, and the remaining entries equal to 0. We have

$$(I_{k+1} - J)\, C(a, b, k) = \left[\begin{array}{c|ccc} 1 & c_{12} & \cdots & c_{1,k+1} \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right],$$

where $B = (b_{ij})$ is the $k \times k$ matrix whose (i, j)-entry is $b_{ij} = -c_{i,j+1} + c_{i+1,j+1}$, $i, j = 1, ..., k$.

If $b+i-j<0$ both $c_{i,j+1}$ and $c_{i+1,j+1}$ are zero. Then $b_{ij}=0$.

If $b+i-j=0$ then $c_{i,j+1}=0$ and

$$\begin{aligned} b_{ij} &= c_{i+1,j+1} \\ &= \frac{(a-i)!\,(b+i)!}{(a-i-j)!\,(b+i-j)!} \\ &= \frac{(a-i)!\,(b+i-1)!\; j(a-i-j+1)}{(a-i-j+1)!\,(b+i-j)!} \\ &= \frac{(a-i)!\,(b+i-1)!\; j(a-b-2i+1)}{(a-i-j+1)!\,(b+i-j)!}. \end{aligned}$$

For the third equality we have used the fact that $(b+i)! = j(b+i-1)!$ and we have multiplied both the numerator and the denominator by $a-i-j+1 = a-b-2i+1 > 0$. If $b+i-j > 0$ we have

$$b_{ij} = \frac{(a-i)!\,(b+i-1)!}{(a-i-j+1)!\,(b+i-j)!}$$

$$\times\left[-(a-i+1)(b+i-j)+(b+i)(a-i-j+1)\right]$$

$$= \frac{(a-i)!\,(b+i-1)!\; j(a-b-2i+1)}{(a-i-j+1)!\,(b+i-j)!}.$$

Then there exist two invertible matrices P and Q such that $PBQ = C(a-1, b, k-1)$. Therefore using the induction hypothesis, we conclude that $C(a, b, k)$ is invertible. ∎

4. MAIN RESULTS

4.17. *Notation.* Let A be a finite subset of the field $\mathbb{F}$. Recall that if i is a positive integer, $\mu_i^{(R)}$ is the cardinality of the set

$$\{x \in \wedge^2 A\colon \nu_x^{(R)} \geqslant i\}.$$

It is easy to see that $\mu_i^{(R)} = 0$ for $i > |A|/2$.

4.18. THEOREM. *Let V be a nonzero m-dimensional vector space over the field $\mathbb{F}$. Let f be a linear operator on V with minimal polynomial P_f and assume that* $\deg(P_f) \geqslant 2$ *and* $1 \leqslant t \leqslant \lfloor \deg(P_f)/2 \rfloor$. *Then we have*

$$\sum_{i=1}^{t} \deg(\alpha_{D(f),\binom{m}{2}-i+1}) \geqslant t \min\{p, 2(\deg(P_f)-t)-1\}.$$

4.19. COROLLARY. *Let A be a finite subset of the field $\mathbb{F}$ and $1 \leqslant t \leqslant \lfloor |A|/2 \rfloor$. Assume that $|A| \geqslant 2$. Then we have*

$$\sum_{i=1}^{t} \mu_i^{(R)} \geqslant t \min\{p, 2(|A|-t)-1\}.$$

Proof of Corollary 4.19. Let $n=|A|$ and let f be a diagonal linear operator on $\mathbb{F}^n$ whose spectrum is A. Then $D(f)$ is diagonal with spectrum $\bigwedge^2 A$. Using Proposition 3.11 we obtain

$$\sum_{i=1}^{t} \mu_i^{(R)} = \sum_{i=1}^{t} \deg(\alpha_{D(f), \binom{n}{2}-i+1}), \qquad t=1, 2, ..., \binom{n}{2}.$$

Then using Theorem 4.18 we conclude that, for $1 \leqslant t \leqslant \lfloor n/2 \rfloor$,

$$\sum_{i=1}^{t} \mu_i^{(R)} \geqslant t \min\{p, 2(n-t)-1\}. \quad \blacksquare$$

Remark. If x is an integer, denote by $\bar{x}$ the canonical image of x in $\mathbb{F}$. Suppose that $A \subseteq \mathbb{F}$ is an arithmetic progression with $|A| \geqslant 3$. Then $p \geqslant |A| \geqslant 3$.

Let $A' = \{\bar{0}, \bar{1}, ..., \overline{|A|-1}\}$. For $\bar{x} \in \bigwedge^2 A'$, let $\hat{v}_{\bar{x}}^{(R)}$ be one-half of the cardinality of the set of pairs $(\bar{a}, \bar{b}) \in A' \times A'$ satisfying $\bar{a} \neq \bar{b}$ and : $\bar{a}+\bar{b}=\bar{x}$. Denote by $\hat{\mu}_i^{(R)}$ the cardinality of the set

$$\{\bar{x} \in \textstyle\bigwedge^2 A' \mid \hat{v}_{\bar{x}}^{(R)} \geqslant i\}.$$

It is easy to see that

$$\mu_i^{(R)} = \hat{\mu}_i^{(R)}, \qquad i \in \mathbb{N}.$$

For $\bar{x} \in \bigwedge^2 A' = \{\bar{1}, ..., \overline{\min\{p, 2\,|A|-3\}}\}$ we have:

If $p \leqslant 2\,|A|-4$ then

$$\hat{v}_{\bar{x}}^{(R)} = \begin{cases} |A| - \dfrac{p+1}{2} & \text{if } \bar{x} \in \{\bar{1}, ..., \overline{2\,|A|-p-3}\} \\ \left\lceil \dfrac{x}{2} \right\rceil & \text{if } \bar{x} \in \{\overline{2\,|A|-p-2}, ..., \overline{|A|-1}\} \\ |A| - \left\lfloor \dfrac{x}{2} \right\rfloor - 1 & \text{if } \bar{x} \in \{\overline{|A|}, ..., \bar{p}\}. \end{cases}$$

If $p \geqslant 2\,|A|-3$ then

$$\hat{v}_{\bar{x}}^{(R)} = \begin{cases} \left\lceil \dfrac{x}{2} \right\rceil & \text{if } \bar{x} \in \{\bar{1}, ..., \overline{|A|-1}\} \\ |A| - \left\lfloor \dfrac{x}{2} \right\rfloor - 1 & \text{if } \bar{x} \in \{\overline{|A|}, ..., \overline{2\,|A|-3}\} \end{cases}.$$

Then, for $i=1, ..., \lfloor |A|/2 \rfloor$, we have

$$\begin{aligned}
\mu_i^{(R)} &= \hat{\mu}_i^{(R)} \\
&= |\{\bar{x} \in \wedge^2 A' : \hat{v}_{\bar{x}}^{(R)} \geqslant i\}| \\
&= \begin{cases} p & \text{if} \quad 1 \leqslant i \leqslant |A| - \dfrac{p+1}{2} \\ 2\,|A| - 4i + 1 & \text{if} \quad \max\left\{1, |A| - \dfrac{p-1}{2}\right\} \leqslant i \leqslant \left\lfloor \dfrac{|A|}{2} \right\rfloor. \end{cases}
\end{aligned}$$

It follows that, for $t=1, 2, ..., \lfloor |A|/2 \rfloor$,

$$\sum_{i=1}^{t} \mu_i^{(R)} = \begin{cases} tp & \text{if} \quad t \leqslant |A| - \dfrac{p+1}{2} \\ t(2\,|A| - 2t - 1) & \text{if} \quad t \geqslant \max\left\{1, |A| - \dfrac{p-1}{2}\right\} \end{cases}$$

and thus equality holds in Corollary 4.19.

5. PROOF OF THEOREM 4.18

Let $v \in V$ be such that $\dim \mathscr{C}_f(v) = \deg(P_f) = n \geqslant 2$. Let $\mathscr{B}$ be the basis of $\wedge^2 \mathscr{C}_f(v)$ defined by

$$\begin{aligned}
\mathscr{B} &= \{ f^{\lambda_1}(v) \wedge f^{\lambda_2+1}(v) : 0 \leqslant \lambda_1 \leqslant \lambda_2 \leqslant n-2 \} \\
&= \left\{ f^{\lambda_1}(v) \wedge f^{\lambda_2+1}(v) : \lambda = (\lambda_1, \lambda_2) \in \bigcup_{s \in \mathbb{Z}^+} \mathscr{P}_{s,2} \text{ and } \lambda_2 \leqslant n-2 \right\}.
\end{aligned}$$

Let $1 \leqslant t \leqslant \lfloor n/2 \rfloor$. For $k \in \mathbb{Z}^+$ and $1 \leqslant j \leqslant t$ define

$$z_{k,j} = D^k(f)(f^{j-1}(v) \wedge f^j(v)).$$

Let $u = t \min\{p, 2n-2t-1\}$. We shall prove that

$$\mathscr{C} = \{ z_{k,j} : 1 \leqslant j \leqslant t, 0 \leqslant k \leqslant \min\{p-1, 2n-2t-2\} \}$$

is a linear independent u-set and use Lemma 3.5 to conclude that

$$(\deg(\alpha_{D(f), \binom{m}{2}}), \deg(\alpha_{D(f), \binom{m}{2}-1}), ..., \deg(\alpha_{D(f), \binom{m}{2}-t+1}))$$

weakly dominates the t-tuple

$$(\min\{p, 2n-2t-1\}, ..., \min\{p, 2n-2t-1\}),$$

thereby obtaining the result.

In order to prove that $\mathscr{C}$ is a linearly independent set we split it into several linearly independent and pairwise disjoint subsets and prove that the linear span of $\mathscr{C}$ is the direct sum of the linear spans of those subsets. These subsets will be obtained by grouping together the elements of $\mathscr{C}$ with the same weight.

From Theorem 3.15 it is easy to see that the maximum weight of the vectors of $\mathscr{C}$ is

$$M_t = \min\{p+2t-2, 2n-3\}.$$

For $r=1, ..., M_t$ let $\mathscr{S}_r$ be the index set of the subset of the elements of $\mathscr{C}$ of weight r. That is,

$$\begin{aligned}\mathscr{S}_r = \{&(k, j) \in \mathbb{Z}^+ \times \mathbb{N}\colon 1 \leqslant j \leqslant t, 0 \leqslant k \leqslant \min\{p-1, 2n-2t-2\}\\ &\text{and } k+2j-1=r\}\\ = \{&(r-2j+1, j) \in \mathbb{Z}^+ \times \mathbb{N}\colon a_r \leqslant j \leqslant b_r\},\end{aligned}$$

where

$$a_r = \max\left\{1, \left\lceil \frac{r-p}{2} \right\rceil + 1, \left\lceil \frac{r+1}{2} \right\rceil - n + t + 1\right\}$$

and

$$b_r = \min\left\{t, \left\lfloor \frac{r+1}{2} \right\rfloor\right\}$$

We have

$$\mathscr{C} = \dot{\bigcup_{r=1}^{M_t}} \{z_{k,j}\colon (k, j) \in \mathscr{S}_r\}. \tag{8}$$

Claim 1. *For any fixed $r \in [1, M_t]$, the set $\{z_{k,j}\colon (k, j) \in \mathscr{S}_r\}$ is linearly independent.*

Proof. Let $q_r = |\mathscr{S}_r| = b_r - a_r + 1$. We denote by $\mathscr{B}_r$ the set of those elements of $\mathscr{B}$ with weight r:

$$\mathscr{B}_r = \left\{ f^i(v) \wedge f^{r-i}(v) \colon \max\{0, r-n+1\} \leqslant i \leqslant \left\lfloor \frac{r-1}{2} \right\rfloor \right\}.$$

Let π_r be the projection of $\bigwedge^2 \mathscr{C}_f(v)$ onto $\langle \mathscr{B}_r \rangle$, along $\bigoplus_{s=1, s \neq r}^{2n-3} \langle \mathscr{B}_s \rangle$.

Let $(k, j) \in \mathscr{S}_r$. From Lemma 3.14 we have

$$\pi_r(z_{k,j}) = \sum_{\substack{\lambda \in \mathscr{P}_{k,2} \\ \lambda_2 \leqslant n-j-1}} \frac{k!}{P(\lambda)} f^{\lambda_1 + j - 1}(v) \wedge f^{\lambda_2 + j}(v). \tag{9}$$

We order the elements of $\{\pi_r(z_{k,j}) : (k, j) \in \mathscr{S}_r\}$ by writing

$$y_j = \pi_r(z_{r-2j-2a_r+3,\, j+a_r-1}), \qquad j = 1, 2, ..., q_r.$$

To prove Claim 1 it is sufficient to prove

Claim 1′. *$\{y_1, ..., y_{q_r}\}$ is linearly independent.*

Proof. Let

$$\left\{ \theta_j \colon \max\{0, r-n+1\} \leqslant j \leqslant \left\lfloor \frac{r-1}{2} \right\rfloor \right\}$$

be the dual basis of $\mathscr{B}_r$; i.e., θ_j are linear functions on $\bigwedge^2 \mathscr{C}_f(v)$, satisfying

$$\theta_j(f^i(v) \wedge f^{r-i}(v)) = \delta_{ij}, \qquad \max\{0, r-n+1\} \leqslant i, j \leqslant \left\lfloor \frac{r-1}{2} \right\rfloor,$$

where δ_{ij} is the Kronecker symbol.

We prove that the $|\mathscr{B}_r| \times q_r$ matrix of the coefficients of $y_1, ..., y_{q_r}$ with respect to the basis $\mathscr{B}_r$, that is,

$$[\theta_i(y_j)]_{\substack{i=1, ..., |\mathscr{B}_r| \\ j=1, ..., q_r}},$$

has an invertible $q_r \times q_r$ submatrix, to conclude that $\{y_1, ..., y_{q_r}\}$ is linearly independent.

We consider two cases.

Case 1. $a_r \geqslant r-n+2$. For all $i \in \{1, 2, ..., q_r\}$ we have

$$\max\{0, r-n+1\} \leqslant a_r - 1 \leqslant i + a_r - 2 \leqslant b_r - 1 \leqslant \left\lfloor \frac{r-1}{2} \right\rfloor,$$

so we can consider $X_i = \theta_{i+a_r-2}$.

From (9) it follows that

$$\begin{aligned} X_i(y_j) &= \theta_{i+a_r-2}(\pi_r(z_{r-2j-2a_r+3,\, j+a_r-1})) \\ &= \sum_{\substack{\lambda \in \mathscr{P}_{r-2j-2a_r+3,\,2} \\ \lambda_2 \leqslant n-j-a_r}} \frac{(r-2j-2a_r+3)!}{P(\lambda)} \\ &\quad \times \theta_{i+a_r-2}(f^{\lambda_1+j+a_r-2}(v) \wedge f^{\lambda_2+j+a_r-1}(v)) \\ &= \sum_{\substack{\lambda \in \mathscr{P}_{r-2j-2a_r+3,\,2} \\ \lambda_2 \leqslant n-j-a_r}} \frac{(r-2j-2a_r+3)!}{P(\lambda)} \delta_{\lambda_1,\, i-j}, \end{aligned} \tag{10}$$

for $1 \leqslant i, j \leqslant q_r$.

If $i < j$, then all $\delta_{\lambda_1,\, i-j}$ at the right vanish and $X_i(y_j) = 0$.

Suppose $i \geqslant j$. Then

$$2a_r + 2i \leqslant 2a_r + 2q_r.$$

Bearing in mind that $q_r = b_r - a_r + 1$ we have

$$2a_r + 2i \leqslant 2b_r + 2.$$

Since $b_r = \min\{t, \lfloor (r+1)/2 \rfloor\}$, we get from the former equality

$$2a_r + 2i \leqslant 2\left\lfloor \frac{r+1}{2} \right\rfloor + 2 \leqslant r+3.$$

Then $2i \leqslant r - 2a_r + 3$ and

$$i - j = 2i - (i+j) \leqslant r - i - j - 2a_r + 3 \leqslant n - a_r - j.$$

Thus, if $i \geqslant j$ then for $\lambda_1 = i - j$, $\lambda_2 = r - i - j - 2a_r + 3$ we have $(\lambda_1, \lambda_2) \in \mathscr{P}_{r-2j-2a_r+3,\,2}$. Next, from the assumption $a_r \geqslant r-n+2$ we get $\lambda_2 = r - i - j - 2a_r + 3 \leqslant n - a_r - j$, and hence by (10) we have

$$X_i(y_j) = \frac{(r-2j-2a_r+3)!}{P((\lambda_1, \lambda_2))}.$$

It follows that $[X_i(y_j)]_{i,\, j=1,2,\ldots,q_r}$ is a triangular matrix with the elements on the principal diagonal equal to 1, and so $\{y_1, \ldots, y_{q_r}\}$ is linearly independent.

Case 2. $a_r \leqslant r-n+1$. In this case $r-n+1 \geqslant a_r \geqslant 1$ and then

$$\mathscr{B}_r = \left\{ f^i(v) \wedge f^{r-i}(v) \colon r-n+1 \leqslant i \leqslant \left\lfloor \frac{r-1}{2} \right\rfloor \right\}.$$

Observe that since, by definition we have $q_r = b_r - a_r + 1$, we get

$$q_r \leqslant t - \left(\left\lceil \frac{r+1}{2} \right\rceil - n + t + 1 \right) + 1.$$

Therefore

$$q_r + r - n \leqslant \left\lfloor \frac{r-1}{2} \right\rfloor,$$

and so we can define $X_i = \theta_{i+r-n}$, $i = 1, 2, \ldots, q_r$.

For $i, j = 1, 2, \ldots, q_r$,

$$\begin{aligned} X_i(y_j) &= \theta_{i+r-n}(\pi_r(z_{r-2j-2a_r+3,\, j+a_r-1})) \\ &= \sum_{\substack{\lambda \in \mathscr{P}_{r-2j-2a_r+3,\, 2} \\ \lambda_2 \leqslant n-j-a_r}} \frac{(r-2j-2a_r+3)!}{P(\lambda)} \\ &\qquad \times \theta_{i+r-n}(f^{\lambda_1+j+a_r-2}(v) \wedge f^{\lambda_2+j+a_r-1}(v)) \\ &= \sum_{\substack{\lambda \in \mathscr{P}_{r-2j-2a_r+3,\, 2} \\ \lambda_2 \leqslant n-j-a_r}} \frac{(r-2j-2a_r+3)!}{P(\lambda)} \delta_{\lambda_1,\, i-j-a_r+r-n+2}. \end{aligned} \tag{11}$$

If $i-j-a_r+r-n+2 < 0$, then all $\delta_{\lambda_1,\, i-j-a_r+r-n+2}$ vanish and $X_i(y_j) = 0$.

Suppose $i-j-a_r+r-n+2 \geqslant 0$. Since $i \geqslant 1$, we have $n-i-j-a_r+1 \leqslant n-j-a_r$. Also, from $i \leqslant q_r$ we get

$$\begin{aligned} 2i &\leqslant 2b_r - 2a_r + 2 \\ &\leqslant 2t - 2\left(\left\lceil \frac{r+1}{2} \right\rceil - n + t + 1 \right) + 2 \\ &\leqslant -2\left\lceil \frac{r+1}{2} \right\rceil + 2n \\ &\leqslant -r - 1 + 2n, \end{aligned}$$

and thus

$$i-j-a_r+r-n+2 \leqslant n-i-j-a_r+1.$$

Then, for $\lambda_1=i-j-a_r+r-n+2$, $\lambda_2=n-i-j-a_r+1$ we have $(\lambda_1, \lambda_2) \in \mathscr{P}_{r-2j-2a_r+3,\,2}$. Clearly $\lambda_2 \leqslant n-a_r-j$ and by (11) we have

$$X_i(y_j)=\frac{(r-2j-2a_r+3)!}{P((\lambda_1, \lambda_2))}.$$

Using Proposition 2.3 we conclude that

$$X_i(y_j)=\begin{cases} 0 & \text{if } \; i-j-a_r+r-n+2<0 \\ \dfrac{(r-2j-2a_r+3)!\,(2n-2i-r)}{(n-i-j-a_r+2)!\,(i-j-a_r+r-n+2)!} & \\ \qquad \text{if } \; i-j-a_r+r-n+2 \geqslant 0. & \end{cases}$$

Then there exist two invertible matrices P and Q such that $P[X_i(y_j)]_{i,\,j=1,\,\ldots,\,q_r}$ $Q=C(n-a_r, r-n-a_r+2, q_r-1)$.

Next we verify that the conditions for application of Lemma 3.16 to the matrix $C(n-a_r, r-n-a_r+2, q_r-1)$ are fulfilled.

From $r \leqslant M_t \leqslant 2n-3$ and $t \leqslant n/2$ we have

$$\left\lceil \frac{r-p}{2} \right\rceil +1 \leqslant \frac{r-p}{2}+1 \leqslant n-\frac{p-1}{2}<n$$

and

$$\left\lceil \frac{r+1}{2} \right\rceil -n+t+1 \leqslant t<n.$$

Then, by the definition of a_r we get $a_r<n$, that is, $n-a_r \geqslant 1$.

From the assumption $a_r \leqslant r-n+1$ we get $r-n-a_r+2 \geqslant 1$.

From the definitions of a_r, b_r, and q_r we have

$$2q_r-2 \leqslant 2t-2\left(\left\lceil \frac{r+1}{2} \right\rceil -n+t+1\right) \leqslant 2n-r-2,$$

and thus $(r-n-a_r+2)+2(q_r-1) \leqslant n-a_r$. Also, from the definition of a_r we have $p \geqslant r-2a_r+2$. Since $r \geqslant a_r+n-1$ it follows that $p \geqslant n-a_r+1$.

Thus we can apply Lemma 3.16 and conclude that $C(n-a_r, r-n-a_r+2,$ $q_r-1)$ is an invertible matrix. Then also $[X_i(y_j)]_{i,\,j=1,\,\ldots,\,q_r}$ is invertible and $\{y_1, \ldots, y_{q_r}\}$ is linearly independent.

From (8) we have

$$\langle \mathscr{C} \rangle = \sum_{r=1}^{M_t} \langle z_{kj} \colon (k, j) \in \mathscr{S}_r \rangle. \tag{12}$$

This proves Claims 1′ and 1.

Next we prove that the sum in (12) is direct. Suppose

$$\sum_{r=1}^{M_t} \sum_{(k,j) \in \mathscr{S}_r} u_{k,j} z_{k,j} = 0.$$

Then

$$\sum_{r=1}^{M_t} \sum_{(k,j) \in \mathscr{S}_r} u_{k,j} \pi_{M_t}(z_{k,j}) = 0. \tag{13}$$

For $(k, j) \notin \mathscr{S}_{M_t}$ the vector $z_{k,j}$ has weight $k + 2j - 1 < M_t$ and thus $\pi_{M_t}(z_{k,j}) = 0$. Then, by (13) we have

$$\sum_{(k,j) \in \mathscr{S}_{M_t}} u_{k,j} \pi_{M_t}(z_{k,j}) = 0.$$

From Claim 1′ it follows that $u_{k,j} = 0$, for all $(k, j) \in \mathscr{S}_{M_t}$.

If we repeat this procedure with π_s, $s = M_t - 1, M_t - 2, ..., 1$, we conclude that

$$u_{k,j} = 0, \qquad (k, j) \in \mathscr{S}_r, \qquad r = 1, ..., M_t.$$

Then the sum in (12) is direct and $\mathscr{C}$ is linearly independent, which proves Theorem 4.18. ∎

REFERENCES

1. C. Caldeira and J. A. Dias da Silva, The invariant polynomials degrees of the Kronecker sum of two linear operators and additive theory, preprint.
2. J. A. Dias da Silva and Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994), 140–146.
3. P. Erdős and R. L. Graham, "Old and New Problems and results in Combinatorial Number Theory," L'Enseignement Mathématique, Genève, 1980.
4. M. B. Nathanson, "Additive Number Theory: Inverse Problems and the geometry of Sumsets," Springer-Verlag, New York/Berlin, 1996.

5. J. M. Pollard, A generalization of the theorem of Cauchy and Davenport, *J. London Math. Soc.* **8** (1974), 460–462.
6. I. Zaballa, Matrices with prescribed rows and invariant factors, *Linear Algebra Appl.* **87** (1987), 113–146.
7. I. Zaballa, Interlacing inequalities and control theory, *Linear Algebra Appl.* **101** (1988), 9–31.
8. I. Zaballa, Controllability and Hermite indices of matrix pairs, preprint.