INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UMI®

A GENERAL

POLLARD TYPE RESULT FOR RESTRICTED SUMS

by

ABDELLATIF BELLAHNID

A dissertation submitted to the graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy.The city university of New York

2000

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

12/21/99
Date

Melvyn B. Nathanson
chair of Examining committee

12/21/99
Date

Executive officer

Melvyn B. Nathanson

Burton Randol

Carlos Moreno

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

A GENERAL POLLARD TYPE RESULT

FOR RESTRICTED SUMS

by

ABDELLATIF BELLAHNID

Advisor: Professor Melvyn B. Nathanson

Let F be an arbitrary field. Let p be the characteristic of F in the case of finite characteristic and ∞ if F has characteristic 0. Let A and B be nonempty finite subsets of F. For $c \in F$, let $\nu_c(A,B)$ be the cardinality of the set of pairs (a,b) such that $a+b=c$, and $\mu_i(A,B)$ the cardinality of the set of elements $c \in A+B$ for which $\nu_c(A,B)$ is greater than or equal to i.

In [6] Caldiera and Dias Da Silva proved the following theorem:

Theorem 1 *Let A and B be finite nonempty subsets of F.*

Then for $t = 1, 2, \ldots, \min\{p, |A|+|B|\}$ we have

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

This result is an extension to an arbitrary field of a theorem proved by Pollard, for $F = Z_p = Z/pZ$, where p is a prime number. Notice that the case where $t=1$ is well known as Cauchy-Davenport Theorem.

In [2] Caldiera and Dias Da Silva proved the following results, for restricted sums. as an analogue of Theorem1.

Let A be a finite subset of F. We denote by $\Lambda^2 A$ the set

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

For $c \in \Lambda^2 A$, let

$$\nu_c^{(2)} = \frac{1}{2}|\{(a,b) \in A^2,\ a \neq b \text{ and } a+b=c\}|$$

and

$$\mu_i^{(2)} = |\{c \in \Lambda^2 A \mid \nu_c^{(2)} \geq i\}|.$$

Then, for $t = 1, \ldots, \lfloor |A|/2 \rfloor$.

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

This lower bound is tight and the equality is attained when A is an arithmetic progression.

For $F = Z_p$ and $t = 1$ we get the Erdos-Heilbronn conjecture.

In this paper I generalize this result to the restricted sum $\Lambda^h A$ for $2 \leq h \leq |A| \leq p$.

Acknowledgements

First and foremost, I would like to thank my advisor, Professor Melvyn B. Nathanson, for his consistent support and encouragement. It was a uniquely rewarding personal and educational experience to be part of his highly qualified research group. Under his guidance, I was introduced to a wealth of material that ultimately led to this dissertation. His constant enthusiasm, integrity and creativity will continue to be a model for me in the future. I would like to express my deep gratitude to Professor Carlos Morino and Professor Burton Randol, for being committee members of my thesis. I owe tremendous debt of gratitude to my family, my wife, Leila, and my son, Yassine, for their love, devotion, and understanding during this difficult time.

Contents

0.1 Introduction 1

1 Combinatorial Background **3**

1.1 The Classical Multinomial Ballot Numbers 3

1.2 The Strict Multinomial Ballot Numbers 5

2 Matrices Controllability and Invariant Factors **18**

2.1 Invariant Factors 18

2.2 Controllability and Indices 21

3 Main Results **31**

Bibliography **45**

0.1 Introduction

Let F be an arbitrary field. Let p be the characteristic of F in case of finite characteristic and ∞ if F has characteristic 0. Given $b \in R$ 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 $a \in N$ let $[1, a]$ denote the set $\{x \in N : 1 \leq x \leq a\}$.

Let A be a finite subset of F. We denote by $\Lambda^h A$ the set

$$\{a_1 + \cdots + a_h \mid a_i \in A \,.\, a_i \neq a_j \text{ for } i \neq j\}$$

For $c \in \Lambda^h A$. Let $\nu_c^{(h)}$ be the cardinality of the set of all h-tuples $(a_1, \ldots, a_h)$ of distinct elements of A such that $a_1 + \cdots + a_h = c$ without counting the permutations of the elements of the h-tuple. Then

$$\nu_c^{(h)} = \frac{1}{h!}|\{(a_1, \ldots, a_h) \in A^h,\ a_i \neq a_j\ i \neq j,\ a_1 + \cdots + a_h = c\}|$$

Denote by $\mu_i^{(h)}$ the cardinality of the set $\{c \in \Lambda^h A \ : \ \nu_c^{(h)} \geq i\}$

In this paper I prove the following Theorem which is a generalization of the Theorem proved in [2] for $h = 2$ by Caldiera and Dias Da Silva.

Theorem 0.1 *Let A be a finite subset of the field F. If*

$$2 \leq h \leq |A| \leq p,$$

then for all integers t such that

$$1 \leq t \leq \min\left(\left\lfloor \binom{|A|}{h-1}/h \right\rfloor, |A| - h + 1\right)$$

we have

$$\sum_{i=1}^{t} \mu_i^{(h)} \geq t \ min\left(p, h(|A| - t + 1) - h^2 + 1\right)$$

we get the Erdos-Heilbronn conjecture in the general case for $F = Z_p$ and $t = 1$

$$\mu_1^{(h)} = |\Lambda^h A| \geq \min\left(p, h|A| - h^2 + 1\right)$$

Chapter 1

Combinatorial Background

1.1 The Classical Multinomial Ballot Numbers

The standard basis for R^h is the set of vectors $\{\epsilon_1, \ldots, \epsilon_h\}$. where

$$\begin{aligned} \epsilon_1 &= (1.0.0.0.\ldots.0) \\ \epsilon_2 &= (0.1.0.0.\ldots.0) \\ &\vdots \\ \epsilon_h &= (0.0.0.\ldots.0.1). \end{aligned}$$

The lattice Z^h is the subgroup of R^h generated by the set $\{\epsilon_1, \ldots, \epsilon_h\}$. so Z^h is the set of vectors in R^h with integral coordinates. Let

$$a = (a_0, a_1, \ldots, a_{h-1}) \in Z^h$$

and

$$b = (b_0, b_1, \ldots, b_{h-1}) \in Z^h.$$

A path in Z^h is a finite sequence of lattice points

$$a = \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_m = b$$

such that

$$\mathbf{v}_j - \mathbf{v}_{j-1} \in \{e_1, \ldots, e_h\}$$

for $j = 1, \ldots, m$. Let $\mathbf{v}_{j-1}$, $\mathbf{v}_j$ be the successive points on a path. We call this a step in the direction ϵ_i if

$$\mathbf{v}_j = \mathbf{v}_{j-1} + \epsilon_i.$$

The vector a is called nonnegative vector if $a_i \geq 0$ for $i = 0, 1, \ldots, h-1$. We write

$$a \leq b$$

If $b - a$ is a nonnegative vector.

Let $P(a, b)$ denote the number of paths from a to b. The path function $P(a, b)$ is translation invariant in the sense that

$$P(a + c, b + c) = P(a, b)$$

for all $a, b, c \in Z^h$. In particular,

$$P(a, b) = P(0, b - a).$$

The path function satisfies the boundary conditions

$$P(a, a) = 1,$$

and

$$P(a, b) > 0 \text{ if and only if } a \leq b.$$

If $a = \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_m = b$ is a path with $m \geq 1$, then

$$\mathbf{v}_{m-1} = b - e_i$$

for some $i = 1, \ldots, h$, and there is a unique path from $b - e_i$ to b. It follows that the path counting function $P(a, b)$ also satisfies the difference equation

$$P(a, b) = \sum_{i=1}^{h} P(a, b - e_i).$$

Let $a \leq b$. For $i = 0, 1, \ldots, h-1$, every path from a to b contains exactly $b_i - a_i$ steps in the direction e_{i+1}. Let

$$m = \sum_{i=0}^{h-1} (b_i - a_i).$$

Every path from a to b has exactly m steps, and the number of different paths is the multinomial coefficient

$$P(a, b) = \frac{\left(\sum_{i=0}^{h-1} (b_i - a_i)\right)!}{\prod_{i=0}^{h-1} (b_i - a_i)!} = \frac{m!}{\prod_{i=0}^{h-1} (b_i - a_i)!}.$$

1.2 The Strict Multinomial Ballot Numbers

Let $h \geq 2$. Suppose that there are h candidates in an election. The candidates will be labeled by the integers $0, 1, \ldots, h-1$. If m_0 votes have already been cast, and if candidate i has received a_i votes, then

$$m_0 = a_0 + a_1 + \cdots + a_{h-1}.$$

We shall call

$$\mathbf{v}_0 = a = (a_0, a_1, \ldots, a_{h-1})$$

the initial ballot vector. Suppose that there are m remaining voters, each of whom has one vote, and these votes will be cast sequentially. Let $v_{i,k}$ denote the number of votes that candidate i has received after k additional votes have been cast. We represent the distribution of votes at step k

$$\mathbf{v}_k = (v_{0,k}, v_{1,k}, \ldots, v_{h-1,k}).$$

Then

$$v_{0,k} + v_{1,k} + \cdots + v_{h-1,k} = k + m_0$$

for $k = 0, 1, \ldots, m$,. Let

$$\mathbf{v}_m = b = (b_0, b_1, \ldots, b_{h-1})$$

be the final ballot vector. It follows immediately from the definition of the ballot vectors that

$$\mathbf{v}_k - \mathbf{v}_{k-1} \in \{e_1, \ldots, e_h\}$$

for $k = 1, \ldots, m$, and so

$$a = \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_m = b$$

is a path in Z^h from a to b. Therefore, the number of distinct sequences of m votes that can lead from the initial ballot vector a to the final ballot vector b is the multinomial coefficient

$$\frac{\left(\sum_{i=0}^{h-1}(b_i - a_i)\right)!}{\prod_{i=0}^{h-1}(b_i - a_i)!} = \frac{m!}{\prod_{i=0}^{h-1}(b_i - a_i)!}.$$

Let $\mathbf{v} = (v_1, \ldots, v_h)$ and $\mathbf{w} = (w_1, \ldots, w_h)$ be vectors in R^h. The vector $\mathbf{v}$ will be called increasing if

$$v_1 \leq v_2 \leq \cdots \leq v_h$$

and strictly increasing if

$$v_1 < v_2 < \cdots < v_h.$$

Now suppose that the initial ballot vector is

$$a = (0, 0, 0, \ldots, 0)$$

and that the final ballot vector is

$$b = (b_0, b_1, \ldots, b_{h-1}).$$

Let

$$m = b_0 + b_1 + \cdots + b_{h-1}.$$

Let $B(b_0, b_1, \ldots, b_{h-1})$ denote the number of ways that m votes can be cast so that all the k^{th} ballot vectors are nonnegative and increasing. This is the classical h-dimensional ballot number. Observe

$$B(0, 0, \ldots, 0) = 1.$$

and that

$$B(b_0, b_1, \ldots, b_{h-1}) > 0$$

if and only if $(b_0, b_1, \ldots, b_{h-1})$ is a nonnegative, increasing vector. These boundary conditions and the difference equation

$$B(b_0, b_1, \ldots, b_{h-1}) = \sum_{i=0}^{h-1} B(b_0, \ldots, b_{i-1}, b_i - 1, b_{i+1}, \ldots, b_{h-1})$$

completely determine the function $B(b_0, b_1, \ldots, b_{h-1})$.

There is an equivalent combinatorial problem. Suppose that the initial ballot vector

is

$$a^* = (0, 1, 2, \ldots, h-1)$$

and the final ballot vector is

$$b = (b_0, b_1, \ldots, b_{h-1}).$$

Let

$$m = \sum_{i=0}^{h-1}(b_i - i) = \sum_{i=0}^{h-1} b_i - \binom{h}{2}.$$

Let $\hat{B}(b_0, b_1, \ldots, b_{h-1})$ denote the number of ways that m votes can be cast so that all of the ballot vectors v_k are nonnegative and strictly increasing. We shall call this the strict h-dimensional ballot number.

A path $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_m$ in Z^h will be called a strictly increasing path if every lattice point $\mathbf{v}_k$ on the path is strictly increasing. Then $\hat{B}(b_0, b_1, \ldots, b_{h-1})$ is the number of strictly increasing paths from a^* to $b = (b_0, b_1, \ldots, b_{h-1})$.

The strict h-dimensional ballot numbers satisfy the boundary conditions

$$\hat{B}(0, 1, \ldots, h-1) = 1$$

and

$$\hat{B}(b_0, b_1, \ldots, b_{h-1}) > 0$$

if and only if $(b_0, b_1, \ldots, b_{h-1})$ is a nonnegative, strictly increasing vector. These boundary conditions and the difference equation

$$\hat{B}(b_0, b_1, \ldots, b_{h-1}) = \sum_{i=0}^{h-1} \hat{B}(b_0, \ldots, b_{i-1}, b_i - 1, b_{i+1}, \ldots, b_{h-1})$$

completely determine $\hat{B}(b_0, b_1, \ldots, b_{h-1})$.

There is a simple relationship between the numbers $B(b_0, b_1, \ldots, b_{h-1})$ and $\hat{B}(b_0, b_1, \ldots, b_{h-1})$. The lattice point

$$\mathbf{v} = (v_0, v_1, \ldots, v_{h-1})$$

is nonnegative and strictly increasing if and only if the lattice point

$$\mathbf{v}' = \mathbf{v} - (0, 1, 2, \ldots, h-1) = \mathbf{v} - a^*$$

is nonnegative and increasing. It follows that

$$a^* = \mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m = b$$

is a path of strictly increasing vectors from a^* to b if and only if

$$0, \mathbf{v}_1 - a^*, \mathbf{v}_2 - a^*, \ldots, b - a^*$$

is a path of increasing vectors from 0 to $b - a^*$. Thus,

$$\hat{B}(b_0, b_1, \ldots, b_{h-1}) = B(b_0, b_1 - 1, \ldots, b_{h-1} - (h-1)).$$

For $1 \leq i < j \leq h$, let $H_{i,j}$ be the hyperplane in R^h consisting of all vectors $(x_1, \ldots, x_h)$ such that $x_i = x_j$. There are $\binom{h}{2}$ such hyperplanes. A path

$$a = \mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m = b$$

will be called intersecting if there exists at least one vector $\mathbf{v}_k$ on the path such that $\mathbf{v}_k \in H_{i,j}$ for some hyperplane $H_{i,j}$.

The symmetric group S_h acts on R^h as follows. For $\sigma \in S_h$ and $\mathbf{v} = (v_0, v_1, \ldots, v_{h-1}) \in R^h$, let

$$\sigma\mathbf{v} = (v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(h-1)}).$$

A path is intersecting if and only if there is a transposition $\tau = (i, j) \in S_h$ such that $\tau \mathbf{v}_k = \mathbf{v}_k$ for some lattice point $\mathbf{v}_k$ on the path.

Let $I(a, b)$ denote the number of intersecting paths from a to b. Let $J(a, b)$ denote the number of paths from a to b that do not intersect any of the hyperplanes $H_{i,j}$. Then

$$P(a, b) = I(a, b) + J(a, b).$$

Lemma 1.1 *Let a be a lattice point in Z^h, and let $b = (b_0, \ldots, b_{h-1})$ be a strictly increasing lattice point in Z^h. A path from a to b is strictly increasing if and only if it intersects none of the hyperplanes $H_{i,j}$, and*

$$\hat{B}(b_0, \ldots, b_{h-1}) = J(a^*, b).$$

Proof Let $a = \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_m = b$ be a path, and let

$$\mathbf{v}_k = (v_{0,k}, v_{1,k}, \ldots, v_{h-1,k})$$

for $k = 0, 1, \ldots, m$. If the path is strictly increasing, then every vector on the path is strictly increasing, and so the path does not intersect any of the hyperplanes $H_{i,j}$. Conversely, if the path is not strictly increasing, then there exists a greatest integer k such that the lattice point v_{k-1} is not strictly increasing. Then $1 \leq k \leq m$, and

$$v_{j,k-1} \leq v_{j-1,k-1}$$

for some $j = 1, \ldots, h-1$. Since the vector $\mathbf{v}_k$ is strictly increasing, we have

$$v_{j-1,k} \leq v_{j,k} - 1.$$

Since $\mathbf{v}_{k-1}$ and $\mathbf{v}_k$ are successive vectors in a path, we have

$$v_{j-1,k-1} \leq v_{j-1,k}$$

and

$$v_{j,k} - 1 \leq v_{j,k-1}.$$

Combining these inequalities, we obtain

$$v_{j,k-1} \leq v_{j-1,k-1} \leq v_{j-1,k} \leq v_{j,k} - 1 \leq v_{j,k-1}.$$

This implies that

$$v_{j,k-1} = v_{j-1,k-1}$$

and so the vector $\mathbf{v}_{k-1}$ lies on the hyperplane $H_{j-1,j}$. Therefore, if b is a strictly increasing vector, then a path from a to b is strictly increasing if and only if it is non-intersecting. It follows that $J(a,b)$ is equal to the number of strictly increasing paths from a to b, and $J(a^*,b)$ is equal to the strict ballot number $\hat{B}(b_0,\ldots,b_{h-1})$.

Lemma 1.2 *Let a and b be strictly increasing vectors. Then*

$$P(\sigma a,b) = I(\sigma a,b)$$

for every $\sigma \in S_h$, $\sigma \neq id$.

Proof. If a is strictly increasing and $\sigma \in S_h$, $\sigma \neq id$, then σa is not strictly increasing, and so every path from σa to b must intersect at least one of the hyperplanes $H_{i,j}$, and so $P(\sigma a,b) \leq I(\sigma a,b)$. and since $I(\sigma a,b) \leq P(\sigma a,b)$ therefore, we get the equality.

Lemma 1.3 *Let a and b be strictly increasing lattice points. Then*

$$\sum_{\sigma \in S_h} sign(\sigma) I(\sigma a, b) = 0$$

Proof. Since a is strictly increasing, it follows that there are $h!$ distinct lattice points of the form σa, where $\sigma \in S_h$, and none of these lattice points lies on a hyperplane $H_{i,j}$. Let Ω be the set of all intersecting paths that start at any one of the $h!$ lattice points σa and end at b. We shall construct an involution from the set Ω to itself.

Let $\sigma \in S_h$, and let

$$\sigma a = \mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_m = b$$

be a path that intersects at least one of the hyperplanes. Let k be the least integer such that $\mathbf{v}_k \in H_{i,j}$ for some $i < j$. Then $k \geq 1$ since a is strictly increasing, and the hyperplane $H_{i,j}$ is uniquely determined since $\mathbf{v}_k$ lies on a path. Consider the transposition $\tau = (i, j) \in S_h$. Then

$$\tau \mathbf{v}_k = \mathbf{v}_k \in H_{i,j}$$

and

$$\tau \sigma a \neq \sigma a.$$

Moreover

$$\tau \sigma a = \tau \mathbf{v}_0, \tau \mathbf{v}_1, \ldots, \tau \mathbf{v}_k = \mathbf{v}_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_m = b$$

is an intersecting path in Ω from $\tau \sigma a$ to b. For $i = 0, 1, \ldots, k-1$, none of the vectors $\tau \mathbf{v}_0, \tau \mathbf{v}_1, \ldots, \tau \mathbf{v}_{k-1}$ lies on any of the hyperplanes, and $H_{i,j}$ is still the unique hyperplane containing $\mathbf{v}_k$. Since τ^2 is the identity permutation for every transposition

τ, it follows that if we apply the same mapping to this path from $\tau\sigma a$ to b, we recover the original path from σa to b. Thus, this mapping is an involution on the set Ω of intersecting paths from the $h!$ lattice points σa to b. Moreover, if σ is an even (resp. odd) permutation, then an intersecting path from σa is sent to an intersecting path from $\tau\sigma a$, where τ is a transposition and so $\tau\sigma$ is an odd (resp. even)permutation. Therefore, the number of intersecting paths that start at even permutations of a is equal to the number of intersecting paths that start at odd permutations of a, and so

$$\sum_{\sigma\in S_h,\ sign(\sigma)=1} I(\sigma a.b) = \sum_{\sigma\in S_h,\ sign(\sigma)=-1} I(\sigma a.b).$$

This statement is equivalent to Lemma 1.3.

$[x]_r$ denote the polynomial $x(x-1)\cdots(x-r+1)$. If b_i and $\sigma(i)$ are nonnegative integers, then

$$\begin{aligned}[b_i]_{\sigma(i)} &= b_i(b_i-1)(b_i-2)\cdots(b_i-\sigma(i)+1)\\ &= \begin{cases} \frac{b_i!}{(b_i-\sigma(i))!} & \text{if } \sigma(i)\le b_i \\ 0 & \text{if } \sigma(i) > b_i \end{cases}\end{aligned}$$

in [1] the following result was proved:

Theorem 1.1 *Let $h \ge 2$ and let $b_0, b_1, \ldots, b_{h-1}$ be integers such that*

$$0 \le b_0 < b_1 \ldots < b_{h-1}.$$

Then

$$\hat{B}(b_0, b_1, \ldots, b_{h-1}) = \frac{\left(b_0+b_1+\cdots+b_{h-1}-\binom{h}{2}\right)!}{b_0!b_1!\ldots b_{h-1}!}\prod_{0\le i<j\le h-1}(b_j-b_i)$$

Proof. Let $a^* = (0, 1, 2, \ldots, h-1)$ and $b = (b_0, b_1, \ldots, b_{h-1}) \in Z^h$. Applying the preceding lemmas, we obtain

$$\begin{aligned}
&\hat{B}(b_0, b_1, \ldots, b_{h-1}) \\
&= J(a^*, b) \\
&= P(a^*, b) - I(a^*, b) \\
&= P(a^*, b) + \sum_{\sigma \in S_h, \sigma \neq id} sign(\sigma) I(\sigma a^*, b) \\
&= P(a^*, b) + \sum_{\sigma \in S_h, \sigma \neq id} sign(\sigma) P(\sigma a^*, b) \\
&= \sum_{\sigma \in S_h} sign(\sigma) P(\sigma a^*, b) \\
&= \sum_{\sigma \in S_h, \sigma a^* \leq b} sign(\sigma) \frac{(b_0 + \cdots + b_{h-1} - \binom{h}{2})!}{\prod_{i=0}^{h-1} (b_i - \sigma(i))!} \\
&= \frac{(b_0 + \cdots + b_{h-1} - \binom{h}{2})!}{b_0! b_1! \cdots b_{h-1}!} \sum_{\sigma \in S_h, \sigma a^* \leq b} sign(\sigma) [b_0]_{\sigma(0)} [b_1]_{\sigma(1)} \cdots [b_{h-1}]_{\sigma(h-1)} \\
&= \frac{(b_0 + \cdots + b_{h-1} - \binom{h}{2})!}{b_0! b_1! \cdots b_{h-1}!} \sum_{\sigma \in S_h} sign(\sigma) [b_0]_{\sigma(0)} [b_1]_{\sigma(1)} \cdots [b_{h-1}]_{\sigma(h-1)} \\
&= \frac{(b_0 + \cdots + b_{h-1} - \binom{h}{2})!}{b_0! b_1! \cdots b_{h-1}!} \begin{vmatrix} 1 & [b_0]_1 & [b_0]_2 & \cdots & [b_0]_{h-1} \\ 1 & [b_1]_1 & [b_1]_2 & \cdots & [b_1]_{h-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & [b_{h-1}]_1 & [b_{h-1}]_2 & \cdots & [b_{h-1}]_{h-1} \end{vmatrix} \\
&= \frac{(b_0 + \cdots + b_{h-1} - \binom{h}{2})!}{b_0! b_1! \cdots b_{h-1}!} \prod_{0 \leq i < j \leq h-1} (b_j - b_i).
\end{aligned}$$

Theorem 1.2 *Let $h \geq 2$ and let $0 \leq b_0 < b_1 < \ldots < b_{h-1}$ be integers such that*

$$0 \leq b_0 < b_1 < \ldots < b_{h-1} < p$$

and

$$b_0 + b_1 + \cdots + b_{h-1} < \binom{h}{2} + p$$

Then

$$\hat{B}(b_0, b_1, \ldots, b_{h-1}) \not\equiv 0 \ (mod\ p)$$

Proof: This follows immediately from Theorm 1.1

Definition 1.1 *Let $\Lambda^h V$ be the h^{th} exterior power of V. Let f be a linear operator on V. We denote by Df the derivative of f on $\Lambda^h V$, defined by:*

$$Df(v_0 \wedge \ldots \wedge v_{h-1}) = \sum_{j=0}^{h-1} v_0 \wedge \ldots \wedge v_{j-1} \wedge f(v_j) \wedge v_{j+1} \wedge \ldots \wedge v_{h-1}$$

$v_0, v_1, \ldots, v_{h-1} \in V$

In [1] the following result was proved:

Theorem 1.3 *Let f: be a linear operator on the finite dimensional vector space V. And let $Df : \Lambda^h V \to \Lambda^h V$ be the derivative of f. For $v_0 \in V$.*

Define

$$v_i = f^i(v_0) \in V$$

for $i \geq 1$ and let

$$W = v_0 \wedge \cdots \wedge v_{h-1} \in \Lambda^h V$$

Then for every $k \geq 0$

$$\begin{aligned} (Df)^k(W) &= (Df)^k(v_0 \wedge \cdots \wedge v_{h-1}) \\ &= \sum \hat{B}(i_0, i_1, \ldots, i_{h-1}) v_{i_0} \wedge \cdots \wedge v_{i_{h-1}} \end{aligned}$$

where the sum is over all integer lattice points $(i_0, \ldots, i_{h-1}) \in Z^h$ *such that*

$$0 \leq i_0 < i_1 \ldots < i_{h-1} \leq k + h - 1$$

and

$$i_0 + i_1 + \cdots + i_{h-1} = \binom{h}{2} + k$$

and where $\hat{B}(i_0, i_1, \ldots, i_{h-1})$ *is the strict h-dimensional ballot number corresponding to the lattice point* $(i_0, i_1, \ldots, i_{h-1})$.

Proof. The proof will be by induction on k. For $k = 0$, we have

$$\begin{aligned}
(Df)^0(w) &= w \\
&= v_0 \wedge v_1 \wedge \cdots \wedge v_{h-1} \\
&= \hat{B}(0, 1, 2, \ldots, h-1) v_0 \wedge v_1 \wedge \cdots \wedge v_{h-1}
\end{aligned}$$

since $\hat{B}(0, 1, 2, \ldots, h-1) = 1$. Suppose the result holds for some integer $k \geq 0$. Then $(Df)^{k+1}(w)$

$$\begin{aligned}
&= Df\left((Df)^k(w)\right) \\
&= Df\left(\sum \hat{B}(i_0, i_1, \ldots, i_{h-1}) v_{i_0} \wedge \cdots \wedge v_{i_{h-1}}\right) \\
&= \sum \hat{B}(i_0, i_1, \ldots, i_{h-1}) Df\left(v_{i_0} \wedge \cdots \wedge v_{i_{h-1}}\right) \\
&= \sum \hat{B}(i_0, i_1, \ldots, i_{h-1}) \sum_{j=0}^{h-1} \left(v_{i_0} \wedge \cdots \wedge v_{i_{j-1}} \wedge f(v_{i_j}) \wedge v_{i_{j+1}} \wedge \cdots \wedge v_{i_{h-1}}\right) \\
&= \sum \hat{B}(i_0, i_1, \ldots, i_{h-1}) \sum_{j=0}^{h-1} \left(v_{i_0} \wedge \cdots \wedge v_{i_{j-1}} \wedge v_{i_j+1} \wedge v_{i_{j+1}} \wedge \cdots \wedge v_{i_{h-1}}\right) \\
&= \sum C(i_0, i_1, \ldots, i_{h-1}) v_{i_0} \wedge \cdots \wedge v_{i_{h-1}},
\end{aligned}$$

where the last sum is over all integer lattice points $(i_0, i_1, \ldots, i_{h-1}) \in Z^h$ such that

$$0 \leq i_0 < i_1 < \cdots < i_{h-1} \leq k + h$$

and

$$i_0 + i_1 + \cdots + i_{h-1} = \binom{h}{2} + k + 1,$$

and the integer $C(i_0, i_1, \ldots, i_{h-1})$ satisfies the difference equation

$$C(i_0, i_1, \ldots, i_{h-1}) = \sum_{j=0}^{h-1} \hat{B}(i_0, \ldots, i_{j-1}, i_j - 1, i_{j+1}, \ldots, i_{h-1}).$$

This difference equation determines the strict h-dimensional ballot numbers, and so

$$C(i_0, i_1, \ldots, i_{h-1}) = \hat{B}(i_0, i_1, \ldots, i_{h-1}).$$

Therefore, the result holds in the case $k + 1$. This completes the induction.

Chapter 2

Matrices Controllability and Invariant Factors

2.1 Invariant Factors

The following theorem is proved in [3]. It is called the Rational Decomposition Theorem.

Theorem 2.1 *Let f be a linear operator on a finite-dimensional vector space V. There exist non-zero vectors $v_1, \ldots, v_r$ in V with respective f-annihilators $p_1, \ldots, p_r$ such that:*

(i) $V = C_f(v_1) \oplus \cdots \oplus C_f(v_r)$

(ii) p_k *divides* p_{k-1}, $k = 2, \ldots, r$.

Furthermore, the integer r and the annihilators $p_1, \ldots, p_r$ are uniquely determined by (i),(ii), and the fact that no v_k is 0.

We note that p_1 is the minimal polynomial of f and the product $\prod_1^r p_i$ is the characteristic polynomial of f. The polynomials $p_1, \ldots, p_r$ are called the invariant factors of f.

In this paper we use P_f to denote the minimal polynomial of f and $\alpha_{f,1} | \ldots | \alpha_{f,m} = P_f$ to denote the invariant factors of f by taking

$$\alpha_{f,m-i+1} = p_i \text{ for } i = 1, \ldots, r$$

and

$$\alpha_{f,m-i+1} = 1 \text{ for } i = r+1, \ldots, m$$

(so that each $\alpha_{f,i}$ divides all subsequent polynomials $\alpha_{f,i+1}, \ldots, \alpha_{f,m}$). For every $v \in V$, $C_f(v)$ is the f-cyclic space of v , i.e

$$C_f(v) = \left\langle f^i(v) : i \in Z^+ \right\rangle$$

Let F be an arbitrary field and denote by $\overline{F}$ the algebraic closure of F. Let $V \neq \{0\}$ be an m dimensional vector space over the field F and let f be a linear operator on V. 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 $\overline{F}$. 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 roots of the characteristic polynomial and for a diagonal linear operator f

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

Indeed, f is diagonal is equivalent that

$$P_f = (x - c_1)(x - c_2)\cdots(x - c_k)$$

where $c_i \;\; i = 1, \ldots, k$ are the distinct eigenvalues of f.

$$(x - c_j) \mid \alpha_{f,m-i+1} \Rightarrow (x - c_j) \mid \alpha_{f,m-i+2}\,, (x - c_j) \mid \alpha_{f,m-i+3}\,, \ldots, and\ (x - c_j) \mid \alpha_{f,m}$$

therefore $(x - c_j)^i$ divides the characteristic polynomial of f, then c_j has algebraic multiplicity greater or equal to i.

Conversely, if c_j has algebraic multiplicity greater or equal to i then $(x - c_j)^i$ divides the characteristic polynomial of f, then

$$(x - c_j) \mid \alpha_{f,m-i+1}, (x - c_j) \mid \alpha_{f,m-i+2}\,, (x - c_j) \mid \alpha_{f,m-i+3}\,, \ldots, and\ (x - c_j) \mid \alpha_{f,m}$$

We conclude that:

$$(x - c_j) \mid \alpha_{f,m-i+1} \Leftrightarrow c_j \text{ has algebraic multiplicity greater or equal to i}$$

Definition 2.1 *Let $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ be two sequences of nonnegative integers. Denote by $(\overline{a}_1, \ldots, \overline{a}_n)$ and $(\overline{b}_1, \ldots, \overline{b}_n)$ the reordering, in a nonincreasing way, of a and b, respectively. We say that b weakly dominates a and we write $a \prec b$ if*

$$\sum_{i=1}^{k} \overline{a}_i \leq \sum_{i=1}^{k} \overline{b}_i \quad k = 1, \ldots, n$$

We say that b dominates a and write $a \preceq b$ if: $a \prec b$ and

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$$

Theorem 2.2 *Let V be a finite dimensional vector space over the field F of dimension m. Let f be a linear operator on V. Let $s_1, \ldots, s_t$ be positive integers. If there exist $v_1, \ldots, v_t \in V$ such that*

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

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

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

For the proof of this Theorem we need some definitions and results.

2.2 Controllability and Indices

Definition 2.2 *Let $v_1, \ldots, v_t \in V$ and let f be a linear operator on V. The subspace*

$$C_f(v_1, \ldots, v_t) = \left\langle f^j(v_i) : j \in Z^+, \ i = 1, \ldots, t \right\rangle$$

will be called the generalized f-cyclic subspace associated to $v_1, \ldots, v_t$. We say that the pair $((v_1, \ldots, v_t), f)$ or the generalized f-cyclic subspace is completely Controllable if:

$$C_f(v_1, \ldots, v_t) = V.$$

Definition 2.3 *Let f be a linear operator on V and let $v_1, \ldots, v_t \in V$. A basis $\mathcal{B}$ of $C_f(v_1, \ldots, v_t)$ selected from $\{f^j(v_i) : j \in Z^+, \ i = 1, \ldots, t\}$ is nice if it is of the form:*

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

We say that the nonnegative integers $r_1, \ldots, r_t$ are indices of $\mathcal{B}$.

in [4] the following result is proved.

Proposition 2.1 *Let A be an $l \times l$ matrix and let $\alpha_1|\alpha_2|\cdots|\alpha_l$ be its invariant factors. Let m be a positive integer satisfying $m > l$. Let $\gamma_1, \ldots, \gamma_m$ be monic polynomials over F such that $deg(\gamma_1\gamma_2\cdots\gamma_m) = m$ and $\gamma_1|\gamma_2|\cdots|\gamma_m$.*

Then there exist $C \in F^{(m-l)\times l}$ and $D \in F^{(m-l)\times(m-l)}$ such that the $m \times m$ matrix

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

has invariant factors $\gamma_1, \ldots, \gamma_m$ if and only if $\gamma_i|\alpha_i|\gamma_{i+m-l}$ $i = 1, \ldots, l$

The next theorem is proved in [5] corollary 2.2.

Theorem 2.3 *Let V be an m-dimensional vector space over the field F. Let f be a linear operator on V and let $r_1, \ldots, r_t$ be positive integers. Then there exist linearly independent vectors $v_1, \ldots, v_t$ such that $C_f(v_1, \ldots, v_t)$ is completely controllable, and a nice basis of $C_f(v_1, \ldots, v_t)$ with indices $r_1, \ldots, r_t$ if and only if the following conditions hold:*

$$\alpha_{f,i} = 1, \quad i = 1, \ldots, m - t$$

and

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

Theorem 2.4 *Let V be an m-dimensional vector space over the field F and let f be a linear operator on V. Let $r_1, \ldots, r_t$ be positive integers. If there exist linearly independent vectors $v_1, \ldots, v_t$ and a nice basis of $C_f(v_1, \ldots, v_t)$ with indices $r_1, \ldots, r_t$, then*

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

Proof:

Let $U = C_f(v_1, \ldots v_t)$ and let $l = dim\, U$. Let f_u denote the restriction of f to U. Clearly, $C_{f_u}(v_1, \ldots, v_t)$ is completely Controllable and from Theorem 2.3 we have

$$(r_1, \ldots, r_t) \preceq (\deg(\alpha_{f_u,l}), \ldots, \deg(\alpha_{f_u,l-t+1})) \tag{2.1}$$

By proposition 2.1 we know that:

$$\alpha_{f,i} | \alpha_{f_u,i} | \alpha_{f,i+m-l} \quad i = 1, \ldots, l$$

Therefore

$$\alpha_{f_u,l}\alpha_{f_u,l-1} \cdots \alpha_{f_u,l-j} \mid \alpha_{f,m}\alpha_{f,m-1} \cdots \alpha_{f,m-j} \quad j = 0, \ldots, l-1 \tag{2.2}$$

Taking degrees in (2.2) we have

$$\sum_{i=0}^{j} \deg(\alpha_{f_u,l-i}) \leq \sum_{i=0}^{j} \deg(\alpha_{f,m-i}) \quad j = 0, \ldots, l-1 \tag{2.3}$$

Therefore from (2.1), (2.3) and since $t \leq l$ we get:

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

Proof of Theorem 2.2:

Let $s_1, \ldots, s_t$ be positive integers and suppose that

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

is a linearly independent $(s_1 + \cdots + s_t)$-set. In order to use Theorem 2.4 we complete this set to a nice basis of $C_f(v_1, \ldots, v_t)$. For each $q \in \{1, \ldots, t\}$, let r_q be the positive integer such that

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

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

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

It's obvious, from the definition, that

$$f\left(\left\langle \bigcup_{i=1}^{t} \{v_i, f(v_i), f^2(v_j), \ldots, f^{r_i-1}(v_i)\} \right\rangle \right) \subseteq \left\langle \bigcup_{i=1}^{t} \{v_i, f(v_i), f^2(v_i), \ldots, f^{r_i-1}(v_i)\} \right\rangle \tag{2.4}$$

We now show that

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

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

$$f^r(v_i) \notin \left\langle \bigcup_{i=1}^{t} \{v_i, f(v_i), f^2(v_i), \ldots, f^{r_i-1}(v_i)\} \right\rangle. \tag{2.5}$$

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

$$f^{r-1}(v_i) \in \left\langle \bigcup_{i=1}^{t} \{v_i, f(v_i), f^2(v_i), \ldots, f^{r_i-1}(v_i)\} \right\rangle$$

and

$$f^r(v_i) \in f\left(\left\langle \bigcup_{i=1}^{t} \{v_i, f(v_i), f^2(v_i), \ldots, f^{r_i-1}(v_i)\} \right\rangle \right)$$

using (2.4) we get

$$f^r(v_i) \in \left\langle \bigcup_{i=1}^{t} \{v_i, f(v_i), f^2(v_i), \ldots, f^{r_i-1}(v_i)\} \right\rangle$$

which contradicts (2.5). By Theorem 2.4 we conclude that

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

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

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

This completes the proof of the Theorem 2.2

Proposition 2.2 *Given a finite subset $A \subseteq F$, Let V be a vector space over F of dimension $|A|$. Let f be a linear operator on V with spectrum $\sigma(f) = A$. Then*

$$m_i(Df) = \mu_i^{(h)} \quad i \in N$$

Proof

Suppose $A = \{a_1, \ldots, a_n\}$. It is easily derived from the definitions that the spectrum of Df is the family:

$$\sigma(Df) = \{a_{i_0} + a_{i_1} + \cdots + a_{i_{h-1}} \; and \; 1 \leq i_0 < \cdots < i_{h-1} \leq n\} = \Lambda^h A$$

then for $i \in N$ we have

$$m_i(Df) = |\{x \in \Lambda^h A : |\{(i_0, \ldots, i_{h-1}) : \; 1 \leq i_1 < \cdots < i_{h-1} \leq n$$

$$and \;\; a_{i_0} + a_{i_1} + \cdots + a_{i_{h-1}} = x\}| \geq i\}| = \mu_i^{(h)}.$$

This completes the proof of proposition 2.2

Let f be a linear operator on V and let $v \in V$ be such that $n = \dim \mathcal{C}_f(v) \geq 2$ then: $(v, f(v), \ldots, f^{n-1}(v))$ is a basis of $\mathcal{C}_f(v)$. We assume that $n \leq p$.

Definition 2.4 *Let $x \in \Lambda^h \mathcal{C}_f(v)$, we define the weight of x as the maximal element of the set*

$$\{i_0 + \cdots + i_{h-1} : 0 \leq i_0 < \cdots < i_{h-1} \leq n - 1$$

and x has non zero coefficient of $f^{i_0}(v) \wedge \cdots \wedge f^{i_{h-1}}(v)$}

The following results will allow us to evaluate the weight of

$$Z_{k,j} = (Df)^k \left(f^{j-1}(v) \wedge f^j(v) \wedge \cdots \wedge f^{j+h-2}(v) \right)$$

for $j \geq 1$ and $k \geq 0$.

Take

$$\begin{aligned} v_{0,j} &= f^{j-1}(v) \\ v_{1,j} &= f^{j}(v) \\ v_{2,j} &= f^{j+1}(v) \\ &\vdots \\ v_{h-1,j} &= f^{j+h-2}(v) \end{aligned}$$

By using Theorem 1.3 we get

$$Z_{kj} = \sum \hat{B}(i_0, i_1, \ldots, i_{h-1}) v_{i_0,j} \wedge \ldots \wedge v_{i_{h-1},j}$$

$$0 \leq i_0 < \ldots < i_{h-1} \leq k + h - 1$$

$$i_0 + \cdots + i_{h-1} = \binom{h}{2} + k$$

$$Z_{k,j} = \sum \hat{B}(i_0, i_1, \ldots, i_{h-1}) f^{j+i_0-1}(v) \wedge \ldots \wedge f^{j+i_{h-1}-1}(v)$$

$$0 \leq i_0 < \ldots < i_{h-1} \leq k + h - 1$$

$$i_0 + \cdots + i_{h-1} = \binom{h}{2} + k$$

For j satisfying $1 \leq j \leq t \leq n - h + 1$

We look for the values of k for which we can always find $(i_0, i_1, \ldots, i_{h-1})$ such that:

$$0 \leq i_0 < i_1 < \cdots < i_{h-1} \leq n - j < p$$

and

$$i_0 + \cdots + i_{h-1} = \binom{h}{2} + k < \binom{h}{2} + p$$

$I_j = [0, n-j]$

$$\begin{aligned} \Lambda^h I_j &= \left[\binom{h}{2}, h(n-j+1) - \binom{h+1}{2}\right] \\ &= \left[\binom{h}{2}, h(n-j+1) - h^2 + \binom{h}{2}\right] \\ &= \binom{h}{2} + [0, h(n-j+1) - h^2] \end{aligned}$$

Therefore for

$$0 \leq k \leq \min(p-1, h(n-t+1) - h^2)$$

We can always find $(i_0, \ldots, i_{h-1})$ such that:

$$0 \leq i_0 < \cdots < i_{h-1} \leq n - j < p$$

and

$$i_0 + \cdots + i_{h-1} = \binom{h}{2} + k < \binom{h}{2} + p$$

Let $f^{j+i_0-1}(v) \wedge \ldots \wedge f^{j+i_{h-1}-1}(v)$ be a vector that satisfies

$$0 \leq i_0 < \ldots < i_{h-1} \leq k + h - 1$$

and

$$i_0 + \cdots + i_{h-1} = \binom{h}{2} + k.$$

if $j + i_l - 1 \geq n$ for some $l \in [0, h-1]$ then $f^{j+i_0-1}(v) \wedge \ldots \wedge f^{j+i_{h-1}-1}(v)$ is a linear combination of basis vectors of the form

$$f^{j_0}(v) \wedge \ldots \wedge f^{j_{h-1}}(v)$$

where

$$0 \leq j_0 < j_1 < \cdots < j_{h-1} \leq n-1$$

and

$$j_0 + \cdots + j_{h-1} < \binom{h}{2} + k + h(j-1)$$

It follows that $Z_{k,j}$ is a linear combination of basis vectors

$f^{j_0}(v) \wedge \ldots \wedge f^{j_{h-1}}(v)$ such that

$$0 \leq j_0 < \cdots < j_{h-1} \leq n-1$$

and

$$j_0 + \cdots + j_{h-1} < \binom{h}{2} + k + h(j-1)$$

or (inclusive)

$$j-1 \leq j_0 < \cdots < j_{h-1} \leq n-1$$

and

$$j_0 + \cdots + j_{h-1} = \binom{h}{2} + k + h(j-1)$$

in the second case the basis vector appears with a coefficient

$$\hat{B}(j_0 - j + 1, j_1 - j + 1, \ldots, j_{h-1} - j + 1) \not\equiv 0 \mod p$$

Therefore we deduce the following theorem

Theorem 2.5 *For*

$$1 \leq j \leq t \leq n-h+1$$

and

$$0 \leq k \leq \min(p-1, h(n-t+1) - h^2)$$

the weight of $Z_{k,j}$ *is:*

$$\binom{h}{2} + k + h(j-1)$$

Theorem 2.6 *Let* F *and* p *be as usual, let* $a, b, k \in Z^+$ *satisfy* $b + 2k \leq a < p$ *then the* $(k+1) \times (k+1)$ *matrix over* F, $C(a,b,k) = [c_{ij}]$ *where*

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

is invertible

Proof We proceed by induction on k.

If $k = 0$ we have

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

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

We have

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

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

$i, j = 1, \ldots, k$

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

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

If $b+i-j>0$ we have

$$\begin{aligned} b_{ij} &= \frac{(a-i)!(b+i-1)!}{(a-i-j+1)!(b+i-j)!}[-(a-i+1)(b+i-j)+(b+i)(a-i-j+1)] \\ &= \frac{(a-i)!(b+i-1)!j(a-b-2i+1)}{(a-i-j+1)!(b+i-j)!} \end{aligned}$$

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.

Chapter 3

Main Results

Notation : Let A be a finite subset of the field F. Recall that if i is a positive integer. $\mu_i^{(h)}$ is the cardinality of the set $\{x \in \Lambda^h A : \ \nu_x^{(h)} \geq i\}$. notice that:

$$\mu_i^{(h)} = 0 \ \ for \ \ i > \binom{|A|}{h-1}/h$$

because if $c \in \Lambda^h A$

$$\begin{aligned} h!\nu_c^{(h)} &= |\{(a_1, \ldots, a_h): \ a_1 + \cdots + a_h = c \ \ a_i \neq a_j \ for \ i \neq j\}| \\ &\leq |\{(a_1, \ldots, a_{h-1}, c - \sum_{i=1}^{h-1} a_i); a_i \neq a_j \ for \ i \neq j\}| \\ &= \binom{|A|}{h-1}(h-1)! \end{aligned}$$

therefore

$$\nu_c^{(h)} \leq \binom{|A|}{h-1}\frac{(h-1)!}{h!}$$

and

$$\nu_c^{(h)} \leq \binom{|A|}{h-1}/h$$

Theorem 3.1 *Let V be a vector space of dimension m over the field F. Let f be a linear operator on V with minimal polynomial P_f. If*

$$2 \leq h \leq \deg P_f \leq p$$

then for all integers t such that

$$1 \leq t \leq \min\left(\binom{m}{h}, \deg P_f - h + 1\right)$$

we have:

$$\sum_{i=1}^{t} \deg\left(\alpha_{Df}, \binom{m}{h} - i + 1\right) \geq t \ \min\left(p, h(\deg P_f - t + 1) - h^2 + 1\right)$$

Theorem 3.2 *Let A be a finite subset of the field F. If*

$$2 \leq h \leq |A| \leq p.$$

then for all integers t such that

$$1 \leq t \leq \min\left(\left\lfloor \binom{|A|}{h-1} / h \right\rfloor, |A| - h + 1\right)$$

we have:

$$\sum_{i=1}^{t} \mu_i^{(h)} \geq t \ min\left(p, h(|A| - t + 1) - h^2 + 1\right)$$

Proof

Let $n = |A|$ and let f be a diagonal linear operator on F^n whose spectrum is A. Then Df is diagonal with spectrum $\Lambda^h A$, then by using Proposition 2.2 we get:

$$m_i(Df) = \mu_i^{(h)}$$

and since Df is diagonal:

$$m_i(Df) = \deg\left(\alpha_{Df}, \binom{n}{h} - i + 1\right)$$

and

$$n = \deg P_f$$

therefore

$$\sum_{i=1}^{t} \mu_i^{(h)} = \sum_{i=1}^{t} \deg\left(\alpha_{Df}, \binom{n}{h} - i + 1\right) \quad t = 1, 2, \ldots, \binom{n}{h}$$

and since

$$\binom{n}{h-1}/h \leq \binom{n}{h}$$

then for all integers t satisfying

$$1 \leq t \leq \min\left(\left\lfloor \binom{n}{h-1}/h \right\rfloor, n - h + 1\right)$$

we have by using Theorem 3.1

$$\sum_{i=1}^{t} \mu_i^{(h)} \geq t \min\left(p, h(n-t+1) - h^2 + 1\right)$$

Proof of Theorem 3.1

Let $v \in V$ be such that $dim\ C_f(v) = deg(P_f) = n$ and let $\mathcal{B}$ the basis of $\Lambda^h C_f(v)$ defined by

$$\mathcal{B} = \{f^{\nu_0}(v) \wedge \ldots \wedge f^{\nu_{h-1}}(v)\ ; 0 \leq \nu_0 < \cdots < \nu_{h-1} \leq n-1\}$$

Let

$$1 \leq t \leq \min\left(\binom{m}{h}, n - h + 1\right)$$

and

$$1 \leq j \leq t$$

Define

$$Z_{k,j} = (Df)^k(f^{j-1}(v) \wedge f^j(v) \wedge \cdots \wedge f^{j+h-2}(v))$$

Let $q = t\min(p, h(n-t+1) - h^2 + 1)$ we shall prove that:

$$\mathcal{C} = \left\{Z_{kj} : \ 1 \leq j \leq t, \ \ 0 \leq k \leq \min(p-1, h(n-t+1) - h^2)\right\}$$

is a linear independent q-set in the vector space $\Lambda^h V$ of dimension $\binom{m}{h}$ and use Theorem 2.2 to conclude that:

$$\left(\deg\left(\alpha_{Df}, \binom{m}{h}\right), \deg\left(\alpha_{Df}, \binom{m}{h} - 1\right), \ldots, \deg\left(\alpha_{Df}, \binom{m}{h} - t + 1\right)\right)$$

weakly dominates the t-tuple

$$\left(\min\left(p, h(n-t+1) - h^2 + 1\right), \ldots, \min\left(p, h(n-t+1) - h^2 + 1\right)\right)$$

thereby obtaining the result.

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

From Theorem 2.5 it is easy to see that the maximum weight of the vectors of $\mathcal{C}$ is

$$\begin{aligned} M_t &= \binom{h}{2} + h(t-1) + \min(p-1, h(n-t+1) - h^2) \\ &= \min\left(\binom{h}{2} + h(t-1) + p - 1, hn + \binom{h}{2} - h^2\right) \end{aligned}$$

and the minimum weight is

$$m_t = \binom{h}{2}$$

For $r = m_t, \ldots, M_t$ let S_r be the index set of the subset of the elements of C of weight r. That is:

$$\begin{aligned} S_r &= \{(k,j) \in Z^+ \times N : \text{ such that } 1 \leq j \leq t\,, \\ 0 &\leq k \leq \min(p-1, h(n-t+1) - h^2) \text{ and } \binom{h}{2} + h(j-1) + k = r\} \\ &= \left\{\left(r - h(j-1) - \binom{h}{2}, j\right) \in Z^+ \times N : \text{such that } a_r \leq j \leq b_r\right\} \end{aligned}$$

where

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

and

$$b_r = \min\left(t, 1 + \left\lfloor \frac{r - \binom{h}{2}}{h} \right\rfloor\right)$$

We have

$$C = \bigcup_{r=\binom{h}{2}}^{M_t} \{Z_{k,j} : \ (k,j) \in S_r\}$$

Claim1: For any fixed $r \in \left[\binom{h}{2}, M_t\right]$, the set $\{Z_{k,j} : \ (k,j) \in S_r\}$ is linearly independent.

Proof:

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

$$\mathcal{B}_r = \{f^{\nu_0}(v) \wedge \ldots \wedge f^{\nu_{h-1}}(v) \ ; 0 \leq \nu_0 < \cdots < \nu_{h-1} \leq n-1 \ \textit{and} \ \nu_0 + \cdots + \nu_{h-1} = r\}$$

Let π_r be the projection of $\Lambda^h C_f(v)$ onto $< \mathcal{B}_r >$ along

$$\oplus_{s=\binom{h}{2}, s \neq r}^{hn-h^2+\binom{h}{2}} < \mathcal{B}_s >$$

Apply π_r on $Z_{k,j}$.

For $(k,j) \in \mathcal{S}_r$ we get:

$$\pi_r(Z_{k,j}) = \sum \hat{B}(\nu_0 - j + 1, \nu_1 - j + 1, \ldots, \nu_{h-1} - j + 1) f^{\nu_0}(v) \wedge \ldots \wedge f^{\nu_{h-1}}(v)$$

the sum is over all h-tuples such that

$$j - 1 \leq \nu_0 < \cdots < \nu_{h-1} \leq n - 1$$

and

$$\nu_0 + \cdots + \nu_{h-1} = r.$$

We concluded also that: $\hat{B}(\nu_0 - j + 1, \nu_1 - j + 1, \ldots, \nu_{h-1} - j + 1) \not\equiv 0 \mod p$

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

$$y_j = \pi_r(Z_{k,a_r - 1 + j})$$

$$j = 1, \ldots, q_r$$

To prove **claim1** it is sufficient to prove:

Claim1': $\{y_1, \ldots, y_{q_r}\}$ is linearly independent.

$$y_j = \sum \hat{B} \quad (\nu_0 - j - a_r + 2, \nu_1 - j - a_r + 2, \ldots, \nu_{h-1} - j - a_r + 2) f^{\nu_0}(v) \wedge \ldots \wedge f^{\nu_{h-1}}(v)$$

$$j \quad + a_r - 2 \leq \nu_0 < \cdots < \nu_{h-1} \leq n - 1$$

$$\nu_0 \quad + \cdots + \nu_{h-1} = r$$

For $1 \leq j \leq q_r$

Proof:

Take $r = \binom{h}{2} + uh + d$ where $u \geq 0$ and $0 \leq d \leq h - 1$

Then

$$\begin{aligned} a_r &= \max\left(1, u+1+\left\lceil\frac{d-p+1}{h}\right\rceil, h+u-n+t+1-\delta_{d0}\right) \\ b_r &= \min(t, u+1) \end{aligned}$$

where δ_{d0} is the Kronecker symbol.

we have $h+u-n+t+1-\delta_{d0} \leq t$ then $h+u-\delta_{d0} \leq n-1$

Take $T \geq 0$ such that $h+u-\delta_{d0}+T = n-1$

$$r = (u+1)+(u+2)+\cdots+(u+h-1)+u+d$$

Since $0 \leq d \leq h-1$,we can add it to the first h-1 terms to get:

$$r = (u+1+d_1)+(u+2+d_2)+\ \cdots+(u+h-1+d_{h-1})+u$$

where

$$d_i = \begin{cases} 1 & \text{if } d \geq h-i \\ 0 & \text{if } d < h-i \end{cases} \qquad for\ i = 1,\ldots,h-1$$

Notice that $T+u+h-1+d_{h-1} = h+u-\delta_{d0}+T = n-1$

Case 1

If $a_r - 1 \leq u - T(h-1)$

$$r = u-T(h-1)+(u+1+d_1+T)+(u+2+d_2+T)+\cdots+(u+h-1+d_{h-1}+T)$$

take the following q_r h-tuples $\nu^i = (\nu^i_0,\ldots,\nu^i_{h-1})$

$$\nu^0_0 = u-T(h-1)$$

$$\begin{aligned}
\nu_1^0 &= u+1+d_1+T \\
\nu_2^0 &= u+2+d_2+T \\
&\vdots \\
\nu_{h-1}^0 &= u+h-1+d_{h-1}+T
\end{aligned}$$

$$\begin{aligned}
\nu_0^1 &= u-T(h-1)+1 \\
\nu_1^1 &= u+1+d_1+T-1 \\
\nu_2^1 &= u+2+d_2+T \\
&\vdots \\
\nu_{h-1}^1 &= u+h-1+d_{h-1}+T \\
&\vdots
\end{aligned}$$

$$\begin{aligned}
\nu_0^{q_r-1} &= u-T(h-1)+q_r-1 \\
\nu_1^{q_r-1} &= u+1+d_1+T-(q_r-1) \\
\nu_2^{q_r-1} &= u+2+d_2+T \\
&\vdots \\
\nu_{h-1}^{q_r-1} &= u+h-1+d_{h-1}+T
\end{aligned}$$

Notice that

$$\begin{aligned}
\nu_0^i &= u-T(h-1)+i \\
\nu_1^i &= u+1+d_1+T-i \\
\nu_j^i &= u+j+d_j+T \quad \textit{for all } 0 \le i \le q_r-1 \textit{ and all } 2 \le j \le h-1
\end{aligned}$$

and

$$\nu_0^i + \cdots + \nu_{h-1}^i = r \quad for \;\; 0 \leq i \leq q_r - 1.$$

Since $b_r - a_r \leq t - (h + u - n + t + 1 - \delta_{d0}) = -h - u + n - 1 + \delta_{d0} = T$ then $q_r - 1 \leq T$

$\nu_1^i = u + 1 + d_1 + T - i \geq u + 1 + d_1 \geq u + 1 \quad for \; i = 0, \ldots, q_r - 1$

$\nu_0^i = u - T(h-1) + i \leq u - T(h-1) + q_r - 1 \leq u - T(h-1) + T \leq u$

We conclude then:

$\nu_0^i < \nu_1^i \quad for \quad i = 0, \ldots, q_r - 1$

For the h-tuple with $\nu_0^i \geq j + a_r - 2$ the coefficient of y_j over the basis vector $f^{\nu_0^i}(v) \wedge \ldots \wedge f^{\nu_{h-1}^i}(v)$, by taking $x_j = j + a_r - 2$ is:

$$\begin{aligned}
&= \hat{B}(\nu_0^i - j - a_r + 2, \nu_1^i - j - a_r + 2, \ldots, \nu_{h-1}^i - j - a_r + 2) \\
&= \hat{B}(\nu_0^i - x_j, \nu_1^i - x_j, \ldots, \nu_{h-1}^i - x_j) \\
&= \frac{\left(r - hx_j - \binom{h}{2}\right)!}{(\nu_0^i - x_j)! \cdots (\nu_{h-1}^i - x_j)!} \prod_{0 \leq q < l \leq h-1} (\nu_l^i - \nu_q^i) \\
&= \frac{\prod_{2 \leq q < l \leq h-1} (\nu_l^i - \nu_q^i)}{(\nu_2^i - x_j)! \cdots (\nu_{h-1}^i - x_j)!} \frac{\left(r - hx_j - \binom{h}{2}\right)! \prod_{q < l \leq h-1; q=0 \text{ or } q=1} (\nu_l^i - \nu_q^i)}{(\nu_0^i - x_j)!(\nu_1^i - x_j)!}
\end{aligned}$$

Take

$$C(j) = \frac{\prod_{2 \leq q < l \leq h-1} (\nu_l^0 - \nu_q^0)}{(\nu_2^0 - x_j)! \cdots (\nu_{h-1}^0 - x_j)!}$$

(Notice $C(j)$ does not depend on i) and take

$$L_{ij} = \begin{cases} \frac{\left(r - hx_j - \binom{h}{2}\right)! \prod_{q < l \leq h-1; q=0 \text{ or } q=1} (\nu_l^i - \nu_q^i)}{(\nu_0^i - x_j)!(\nu_1^i - x_j)!} & \text{if } \nu_0^i - x_j \geq 0 \\ 0 & \text{if } \nu_0^i - x_j < 0 \end{cases}$$

We found a submatrix M of the matrix of the coefficients of $\{y_1, \ldots, y_{q_r}\}$ with respect to the basis $\mathcal{B}_r$ where $M_{ij} = C(j) L_{ij}$, $0 \leq i \leq q_r - 1$ and $1 \leq j \leq q_r$.

We prove that the matrix M is invertible. We have

$$\det(M) = C(1)C(2)\cdots C(q_r)\det(L)$$

where

$$det(L) = \prod_{j=1}^{q_r} \alpha_j \prod_{i=0}^{q_r-1} \beta_i \det(D)$$

and

$$\begin{aligned}
\alpha_j &= \left(r - h(j + a_r - 2) - \binom{h}{2}\right)! \\
\beta_i &= \prod_{q<l\leq h-1; q=0 \text{ or } q=1} (\nu_l^i - \nu_q^i) \\
D_{ij} &= \begin{cases} \frac{1}{(\nu_0^i - x_j)!(\nu_1^i - x_j)!} & \text{if } \nu_0^i - x_j \geq 0 \\ 0 & \text{if } \nu_0^i - x_j < 0 \end{cases}
\end{aligned}$$

Where $1 \leq j \leq q_r$ and $0 \leq i \leq q_r - 1$

$$\nu_{h-1}^0 - x_j = u + h - 1 + d_{h-1} + T - j - a_r + 2 = n - j - a_r + 1 \leq n - j < p$$

$$\begin{aligned}
\nu_2^0 - x_j &= u + 2 + d_2 + T - j - a_r + 2 \\
&\geq u + 2 + d_2 + T - q_r - a_r + 2 \\
&= u + 2 + d_2 + T - b_r + 1 \\
&= (u + 1 - b_r) + d_2 + T + 2 \\
&\geq 1
\end{aligned}$$

and

$$1 \leq \nu_l^0 - \nu_q^0 < p \ \ for\ all\ \ 2 \leq q < l \leq h - 1$$

Therefore $C(j) \not\equiv 0 \mod p$ and well defined for all $1 \leq j \leq q_r$, then $C(1)C(2)\cdots C(q_r) \not\equiv 0 \mod p$.

$$0 \leq r - \binom{h}{2} - hx_j = k < p$$

therefore $\alpha_j \not\equiv 0 \mod p$ for all $1 \leq j \leq q_r$.

$$1 \leq \nu_l^i - \nu_q^i \leq n - 1 < p \quad for\ all\ q < l \leq h-1; q = 0\ or\ q = 1$$

therefore $\beta_i \not\equiv 0 \mod p$ for all $0 \leq i \leq q_r - 1$

$$D_{ij} = \begin{cases} \frac{1}{(\nu_0^{i-1} - x_j)!(\nu_1^{i-1} - x_j)!} & \text{if } \nu_0^{i-1} - x_j \geq 0 \\ 0 & \text{if } \nu_0^{i-1} - x_j < 0 \end{cases}$$

Where $1 \leq j \leq q_r$ and $1 \leq i \leq q_r$

$$\nu_0^{i-1} - x_j = u - T(h-1) - a_r + 1 + i - j = b + i - j$$

by taking

$$b = u - T(h-1) - a_r + 1$$

$$\nu_1^{i-1} - x_j = u + 1 + d_1 + T + 1 - a_r - i - j + 2 = a - i - j + 2$$

by taking

$$a = u + 1 + d_1 + T + 1 - a_r$$

therefore

$$D_{ij} = \begin{cases} \frac{1}{(a-i-j+2)!((b+i-j)!} & \text{if } b + i - j \geq 0 \\ 0 & \text{if } b + i - j < 0 \end{cases}$$

a,b and q_r satisfy the condition of Theorem 2.6 indeed:

$$b \geq 0 \text{ because } u - T(h-1) \geq a_r - 1$$

and

$$b + 2(q_r - 1) \leq a \Leftrightarrow 0 \leq d_1 + 1 + Th - 2(q_r - 1)$$

and the right hand side inequality is true because $h \geq 2$ and $T \geq q_r - 1$

$$\begin{aligned} a &= u + 1 + d_1 + T + 1 - a_r \\ &= u + T + 2 + d_1 - a_r \\ &= n - 1 - h + \delta_{d0} + 2 + d_1 - a_r \\ &= n - 1 - (h + a_r - \delta_{d0} - d_1 - 2) \\ &< p \ because \ h + a_r - \delta_{d0} - d_1 - 2 \geq 0 \end{aligned}$$

Then, the matrix $C(a, b, q_r - 1) = C$ is invertible, therefore D is invertible, because $C = PD$ where P is a diagonal matrix such that $P_{ii} = (a - i + 1)!(b + i - 1)!$

and

$$\begin{aligned} a - i + 1 &\geq a - q_r + 1 \\ &= u + 1 + d_1 + T + 1 - a_r - q_r + 1 \\ &= (u + 1 - b_r) + d_1 + T + 1 \\ &\geq 0 \end{aligned}$$

Then

$$0 \leq (a - i + 1) \leq a < p$$

and

$$0 \leq b+i-1 \leq b+q_r-1 \leq b+2(q_r-1) \leq a < p$$

then

$$(a-i+1)!(b+i-1)! \not\equiv 0 \mod p \text{ for all } 1 \leq i \leq q_r$$

We conclude then that $\{y_1, \ldots, y_{q_r}\}$ are linearly independent.

Case2

If $a_r - 1 > u - T(h-1)$

then $T \neq 0$ because $a_r \leq b_r \leq u+1$

$$r = (u+1+d_1) + (u+2+d_2) + \cdots + (u+h-1+d_{h-1}) + u$$

Take w such that $a_r = 1 + u - w$, $0 \leq w < T(h-1)$

$$r = u + (u+1+d_1) + (u+2+d_2) + \cdots + (u+h-1+d_{h-1})$$

Since we can add $T(h-1)$ by adding T to each of the h-1 terms

$$(u+1+d_1), (u+2+d_2), \ldots, (u+h-1+d_{h-1})$$

without exceeding n-1,because the maximum term is $(u+h-1+d_{h-1}+T = n-1)$

then we can add all numbers less than or equal to w, because $w < T(h-1)$

$q_r = b_r - a_r + 1 \leq u+1-u-1+w+1 = w+1$ then $q_r - 1 \leq w$

Therefore we can find q_r h-tuples $(\nu_0^i, \ldots, \nu_{h-1}^i)$ that satisfy

$$a_r - 1 \leq \nu_o^i < \cdots < \nu_{h-1}^i \leq n-1 \text{ and } \nu_o^i + \cdots + \nu_{h-1}^i = r$$

The first coordinate ν_0^i is defined as

$$\nu_0^i = u - (w-i) = (i+1) + a_r - 2 \quad 0 \leq i \leq q_r - 1$$

and

$$\nu_q^i = u + q + d_q + w_{qi} \; ; 1 \leq q \leq h-1 \;\; , 0 \leq i \leq q_r - 1$$

where w_{qi} is such that $\sum_{q=1}^{q=h-1} w_{qi} = w - i$. Therefore we found a lower triangular submatrix M of the matrix of the coefficients of $\{y_1, \ldots, y_{q_r}\}$ with respect to the basis $\mathcal{B}_r$ and $det(M) \not\equiv 0 \bmod p$, because all the scalars in the diagonal are different from $0 \bmod p$. In both cases, I proved that $\{y_1, \ldots, y_{q_r}\}$ are linearly independent.

We have

$$\langle \mathcal{C} \rangle = \sum_{r=\binom{h}{2}}^{M_t} \langle Z_{kj} : (k,j) \in \mathcal{S}_r \rangle$$

next we prove that this sum is direct.

suppose that

$$\sum_{r=\binom{h}{2}}^{M_t} \sum_{(k,j) \in \mathcal{S}_r} u_{kj} Z_{kj} = 0$$

then

$$\sum_{r=\binom{h}{2}}^{M_t} \sum_{(k,j) \in \mathcal{S}_r} u_{kj} \pi_{M_t}(Z_{kj}) = 0$$

For $(k,j) \notin \mathcal{S}_{M_t}$ the vector Z_{kj} has weight $\binom{h}{2} + h(j-1) + k < M_t$ and thus $\pi_{M_t}(Z_{kj}) = 0$ then we get

$$\sum_{(k,j) \in \mathcal{S}_{M_t}} u_{kj} \pi_{M_t}(Z_{kj}) = 0$$

From claim1' it follows that $u_{kj} = 0$ for all $(k,j) \in \mathcal{S}_{M_t}$.

If we repeat this procedure with π_s, $s = M_t - 1, M_t - 2, \ldots, = \binom{h}{2}$ we conclude that

$$u_{kj} = 0, \quad (k,j) \in \mathcal{S}_r \quad r = \binom{h}{2}, \ldots, M_t$$

then the sum is direct and $\mathcal{C}$ is linearly independent which proves Theorem 3.1.

Bibliography

[1] **M.B Nathanson,** *Additive Number theory: Inverse Problems and the geometry of sum set.* Springer verlag, New York/Berlin. 1996.

[2] **C. Caldiera & J. A. Dias da Silva,** *A Pollard Type Result for Restricted sums.* Journal of Number Theory 72. 153-173 (1998).

[3] **K. Hoffman & R. Kunze,** *Linear Algebra.* Prentice Hall. 1961.

[4] **I. Zaballa,** *Matrices with prescribed rows and invariant factors.* Linear Algebra Appl. 87 (1987), 113-146.

[5] **I. Zaballa,** *Controllability and Hermite indices of matrix pairs.* INT.J.Control. 1997. Vol.68, No.1, 61-86.

[6] **C. Caldiera & J. A. Dias da Silva,** *The invariant polynomials degrees of the Kronecker sum of two linear operators and additive theory.* preprint.