SCUOLA DI DOTTORATO

UNIVERSITÀ DEGLI STUDI DI MILANO-BICOCCA

Dipartimento di / Department of

Matematica e Applicazioni

Dottorato di Ricerca in / PhD program Matematica Pura ed Applicata   Ciclo / Cycle XXX

Algebra of sets, permutation groups and invariant factors

Cognome / Surname **Prandelli** Nome / Name **Mariateresa**

Matricola / Registration number **798743**

Tutore / Tutor: Francesca Dalla Volta

Coordinatore / Coordinator: Roberto Paoletti

ANNO ACCADEMICO / ACADEMIC YEAR 2016/2017

Contents

Introduction

In this thesis we deal with the problem to find particular forms for incidence matrices of incidence structures $\mathcal{I}_{tk}^n = (L_t^n, L_k^n; \subseteq)$.

Denote by Ω a set of finite size n, say $\Omega = \{1, 2, \cdots, n\}$ and by L^n the power set of Ω. We partition it into the sets L_i^n, for $0 \leq i \leq n$, where L_i^n is the set of subsets of Ω of size i; i.e. the elements of L_i^n are the i-subsets of Ω.
$\mathcal{I}_{tk}^n = (L_t^n, L_k^n; \subseteq)$ is the incidence structure so defined: for $x \in L_t^n$ and $y \in L_k^n$, x and y are incident if and only if $x \subseteq y$. Its incidence matrix is denoted by W_{tk}.

R.M.Wilson in [15] (Theorem 3.1.6) finds a diagonal form for W_{tk} with purely combinatorics methods. For shortness we will refer to this result as "Wilson's Theorem".
Many other authors have dealt with the same problem, see for example [2], [7], [8] and [11].

The heart of the thesis is Chapter 4 where we give a new proof of Wilson's Theorem via linear maps.

Looking at [5] and starting from $\mathcal{I}_{tk}^n$ we construct a new algebraic structure:

let $G \subseteq Sym(n)$ be a permutation group on Ω. The action of G on Ω induces a natural action on L^n. Formally, if $g \in Sym(n)$ and $\alpha_1, \cdots \alpha_i \in \Omega$ then

$$\{\alpha_1, \cdots, \alpha_i\}^g = \{\alpha_1^g, \cdots, \alpha_i^g\}.$$

So G acts on any L_i^n.

This action partitions each L_i^n into orbits; τ_i denotes the number of orbits of G on L_i^n.

For $0 \leq t \leq k \leq n$, if we call $\Omega^t = \{\Delta_1, \Delta_2, \cdots, \Delta_{\tau_t}\}$ and $\Omega^k = \{\Gamma_1, \Gamma_2, \cdots, \Gamma_{\tau_k}\}$ the G-orbits sets on L_t^n and L_k^n, the pair (Ω^t, Ω^k) is a tactical decomposition of $\mathcal{I}_{tk}^n$. Then we can define two matrices

$$X_{tk}^+ = (x_{ij}^+) \qquad \text{and} \qquad X_{tk}^- = (x_{ji}^-)$$

where

$$x_{ij}^+ = |\{x \in \Delta_j \ : \ x \subseteq y, \text{ for one fixed } y \in \Gamma_i\}|$$

and

$$x_{ji}^- = |\{y \in \Gamma_i \ : \ x \subseteq y, \text{ for one fixed } x \in \Delta_j\}|.$$

To be precise we should write $(X_{tk}^+)^G$, but we cut G to avoid too heavy notation.

X_{tk}^+ and X_{tk}^- are called the incidence matrices of (Ω^t, Ω^k). Clearly, X_{tk}^+ and X_{tk}^- are integral $\tau_k \times \tau_t$ and $\tau_t \times \tau_k$-matrices, respectively.

If $G = \{1_G\}$ then the orbits of G correspond to the subsets and $X_{tk}^+ = W_{tk}^T$ is the transpose matrix of the incidence structure $\mathcal{I}_{tk}^n$.

In Chapter 5 we will give some new results related to the invariant factors of X_{tk}^+.

The thesis is so organized: in Chapter 2 we give the necessary prerequisites about modules and equivalence of matrices; in Chapter 3 we present the original Wilson's proof given in [15].

In Chapter 4 we introduce an algebra related to the boolean poset L^n, in order to give our new proof of Wilson's Theorem, drawing from [4], [13] and [14],

Let R be one of $\mathbb{Q}$ or $\mathbb{R}$, we construct the vector space RL^n of formal sums of elements of L^n with coefficients in R, i.e.

$$RL^n = \left\{ \sum_{x \in L^n} r_x x \ : \ x \in L^n, r_x \in R \right\}.$$

We give to RL^n the structure of algebra by adding a multiplication operation. For $x, y \in L^n$ we define a product in the following way:

$$x \cdot y = x \cup y$$

and extend this linearly to RL^n. If $f = \sum_{x \in L^n} f_x x$ and $h = \sum_{y \in L^n} f_y y$, we put

$$f \cdot h = \sum_{x,y \in L^n} f_x h_y x \cdot y.$$

We want to extend the $\subseteq$ relation from L^n into RL^n. To do this we define incidence maps:

$$\epsilon^{(n)}(x) = \begin{cases} \sum\limits_{\substack{y \supseteq x \\ |y|=|x|+1}} y & \text{if } |x| < n \\ 0 & \text{otherwise} \end{cases} \qquad \text{and} \qquad \partial^{(n)}(y) = \begin{cases} \sum\limits_{\substack{x \subseteq y \\ |x|=|y|-1}} x & \text{if } |y| > 0 \\ 0 & \text{otherwise} \end{cases}.$$

We also consider in section 4.1, for any $0 \le t \le k \le n$, the functions $\epsilon_t^{(n)k}$ and $\partial_k^{(n)t}$ so defined

$$\epsilon_t^{(n)k} : \begin{cases} RL_t^n & \longrightarrow & RL_k^n \\ x & \longrightarrow & \sum\limits_{\substack{y \supseteq x \\ y \in L_k^n}} y \end{cases} \qquad \text{and} \qquad \partial_k^{(n)t} : \begin{cases} RL_k^n & \longrightarrow & RL_t^n \\ y & \longrightarrow & \sum\limits_{\substack{x \subseteq y \\ x \in L_t^n}} x \end{cases} .$$

We observe that the matrices associated to $\epsilon_t^{(n)k}$ and $\partial_k^{(n)t}$, with respect to the bases L_t^n and L_k^n, are W_{tk}^T and W_{tk}, respectively.

The results of Chapter 4 are achieved considering a particular basis for RL_i^n.

Given $0 \le t \le n-1$ and $k = t+1$, we construct two symmetric maps

$$\nu_t^+ = \partial_{t+1}^{(n)t} \epsilon_t^{(n)t+1} : RL_t^n \longrightarrow RL_t^n \qquad \text{and} \qquad \nu_{t+1}^- = \epsilon_t^{(n)t+1} \partial_{t+1}^{(n)t} : RL_{t+1}^n \longrightarrow RL_{t+1}^n$$

and we state Theorems 4.2.2 and 4.2.3.

Theorem 4.2.2. *Suppose that $2t \le n$. Then ν_t^- has $t+1$ eigenvalues*

$$\lambda_{t-1,0} > \lambda_{t-1,1} > \cdots > \lambda_{t-1,t-1} > \lambda_{t-1,t} = 0$$

and ν_t^+ has $t+1$ eigenvalues

$$\lambda_{t,0} > \lambda_{t,1} > \cdots > \lambda_{t,t-1} > \lambda_{t,t} \ge 0,$$

with multiplicity $n_i = \binom{n}{i} - \binom{n}{i-1}$, for $0 \le i \le t$. In particular we have the decomposition

$$RL_t^n = E_{t,0}^n \oplus E_{t,1}^n \oplus \cdots \oplus E_{t,t}^n$$

where $E_{t,i}^n$ is the ν_t^+-eigenspace with eigenvalue $\lambda_{t,i}$ and $dim_R\, E_{t,i}^n = \binom{n}{i} - \binom{n}{i-1}$.

Theorem 4.2.3. *If $2t > n$ and $0 < t \leq n$, then ν_t^- has $n-t+1$ positive eigenvalues. In particular we have the decomposition*

$$RL_t^n = E_{t,0}^n \oplus E_{t,1}^n \oplus \cdots \oplus E_{t,n-t-1}^n \oplus E_{t,n-t}^n.$$

We prove that the eigenspaces $E_{t,i}^n$ are irreducible $Sym(n)$-invariant and that

$$\epsilon_t^{(n)k}(E_{t,i}^n) = E_{k,i}^n.$$

We observe that from these decompositions it is immediate to find two bases in RL_t^n and RL_k^n, respectively, such that the associated matrix to $\epsilon_t^{(n)k} : RL_t^n \to RL_k^n$ is the diagonal form of W_{tk} found by R.M. Wilson.

If we consider W_{tk} as incidence matrix of the incidence structure $\mathcal{I}_{tk}^n$, we can see W_{tk}^T as matrix associated to $\epsilon_t^{(n)k}$ restricted to the $\mathbb{Z}$-module $\mathbb{Z}L_t^n$.

This suggested us to address the problem via linear algebra. Unluckly the result for the $\mathbb{Z}$- modules is not immediate.

In section 4.3, looking at [4], we give a generating set S_i^n of eigenvectors for the vector space RL_i^n, with $i = 0, \cdots, n$, called polytopes.

For our approach an important role is played by the $\mathbb{Z}$-module $\mathbb{Z}L_i^n$ with basis L_i^n $(i = 0, \cdots, n)$ together with the submodule $\mathbb{Z}S_i^n$ generated by polytopes.

It is easy to prove that the following restrictions hold:

$$\epsilon_t^{(n)k} : \mathbb{Z}L_t^n \to \mathbb{Z}L_k^n, \qquad \partial_k^{(n)t} : \mathbb{Z}L_k^n \to \mathbb{Z}L_t^n$$

$$\epsilon_t^{(n)k} : \mathbb{Z}S_t^n \to \mathbb{Z}S_k^n, \qquad \partial_k^{(n)t} : \mathbb{Z}S_k^n \to \mathbb{Z}S_t^n.$$

We will determine the invariant factors of the matrix W_{tk}^T finding the Smith group of $\epsilon_t^{(n)k} : \mathbb{Z}L_t^n \to \mathbb{Z}L_k^n$ (see Definition 2.4.21). The result is obtained constructing in section 4.4 a standard basis of polytopes. We report here the final results.

Theorem 4.5.1. *Let $0 \le t \le k \le n$ and $t + k \le n$. Then the Smith group of*

$$\epsilon_t^{(n)k} : \mathbb{Z}S_t^n \to \mathbb{Z}S_k^n$$

is isomorphic to

$$(C_{d_0})^{n_0} \times \cdots \times (C_{d_t})^{n_t} \times \mathbb{Z}^l,$$

where $d_i = \binom{k-i}{t-i}$, $n_i = \binom{n}{i} - \binom{n}{i-1}$, for $i = 0, \cdots, t$ and $l = \binom{n}{k} - \binom{n}{t}$.

Theorem 4.5.4. *Let $0 \le t \le k$ with $t + k \le n$ and $s_{x_i}^i$ be a standard polytope of type (i, i), for $i = 0, \cdots, t$. Then $\mathbb{Z}S_{k,0}^n \oplus \cdots \oplus \mathbb{Z}S_{k,t}^n$ is isomorphic to $\mathbb{Z}L_k^n \cap (E_{k,0} \oplus \cdots \oplus E_{k,t})$.*

An isomorphism is given by the map $\varphi_t^{(n)k}$ linear extension of the map defined on a standard basis of polytopes by

$$\varphi_t^{(n)k}\left(\epsilon_i^{(n)k}(s_{x_i}^i)\right) = \epsilon_i^{(n)k}(x_i). \tag{1.1}$$

Corollary 4.5.5. *Let $0 \le t \le k \le n$ with $t + k \le n$ and $s_{x_i}^i$ be a standard polytope of type (i, i), for $i = 0, \cdots, t$. Then the map*

$$\varphi : \mathbb{Z}S_k^n / \epsilon_t^{(n)k}(\mathbb{Z}S_t^n) \to \mathbb{Z}L_k^n / \epsilon_t^{(n)k}(\mathbb{Z}L_t^n)$$

defined by

$$\varphi(\epsilon_i^{(n)k}(s_{x_i}^i) + \epsilon_t^{(n)k}(\mathbb{Z}S_t^n)) = \epsilon_i^{(n)k}(x_i) + \epsilon_t^{(n)k}(\mathbb{Z}L_t^n),$$

and extended by linearity, is an isomorphism.

In Chapter 5 we introduce the submodule of $\mathbb{Z}L_i^n$ which consists of elements fixed by G, that is

$$(\mathbb{Z}L_i^n)^G = \{v \in \mathbb{Z}L_i^n \, : \, v^g = v, \text{ for any } g \in G\};$$

we denote by $(\mathbb{Z}S_i^n)^G$ the module $(\mathbb{Z}L_i^n)^G \cap \mathbb{Z}S_i^n$, and we prove the following

Theorem 5.1.7. *Let $0 \leq t \leq k$ and $t + k \leq n$. Then the Smith group of*

$$\epsilon_t^{(n)k} : (\mathbb{Z}S_t^n)^G \longrightarrow (\mathbb{Z}S_k^n)^G$$

is isomorphic to

$$(C_{d_0})^{m_0} \times (C_{d_1})^{m_1} \times \cdots \times (C_{d_t})^{m_t} \times \mathbb{Z}^l,$$

where $d_i = \binom{k-i}{t-i}$, $m_i = \tau_i - \tau_{i-1}$, $i = 0, \cdots, t$ and $l = \tau_k - \tau_t$.

In section 5.2 we restrict our attention to the case $t + k = n$ and we consider the G-isomorphism

$$+_N : \mathbb{Q}L_t^n \longrightarrow \mathbb{Q}L_k^n$$

defined on basis elements in the following way: if $x \in L_t^n$ and y is its complement in Ω, the map $+_N$ is so defined

$$+_N : x \longrightarrow y.$$

The map $+_N$ restricts to isomorphisms between $(\mathbb{Z}L_t^n)^G$ and $(\mathbb{Z}L_k^n)^G$ and between $(\mathbb{Z}S_t^n)^G$ and $(\mathbb{Z}S_k^n)^G$. This allows us to prove

Theorem 5.2.5. *Let $0 \leq t \leq k \leq n$ and $t + k = n$. Then the groups $(\mathbb{Z}L_k^n)^G / \epsilon_t^{(n)k}((\mathbb{Z}L_t^n)^G)$ and $(\mathbb{Z}S_k^n)^G / \epsilon_t^{(n)k}((\mathbb{Z}S_t^n)^G)$ have the same order.*

Actually we conjecture that, for any group $G \subseteq Sym(n)$ and $t + k = n$, the Smith group of $\epsilon_t^{(n)k} : (\mathbb{Z}L_t^n)^G \longrightarrow (\mathbb{Z}L_k^n)^G$ is isomorphic to $(C_{d_0})^{m_0} \times (C_{d_1})^{m_1} \times \cdots \times (C_{d_t})^{m_t}$.

Some evidence is given from results in section 5.3, in particular from Theorem 5.3.4. Moreover, using Magma Computational Algebra System (see Appendix A) we can see that, for $n \leq 11$, $t \leq k$ and $t + k = n$, our conjecture is true, while the statement is not true in general for $t + k < n$ (see example 5.3.6). I would especially like to thank Prof. Pablo Spiga for the stimulating discussions we had and for his help with the computational load in the case $t + k = n$.

About the matrices X^+_{tk} we just prove that, for $0 \leq t \leq k = n - t$, the matrix

$$M^+_{tk} = \left(X^+_{0k} | X^+_{1k} | \cdots | X^+_{tk} \right)$$

has index one (see Definition 2.4.15) and rank τ_t.

This is actually the analogue of the first step of Wilson's original proof given in [15]; this suggested us to follow Wilson's proof to get result for X^+_{tk}, but this is not possible. In his proof it is necessary that the matrix M_{tk} has index 1 also for $t < k < n - t$ (see Proposition 3.1.3). This is not true in our case for matrix M^+_{tk}.

Notation

M^G	The centralizer algebra of G on M	*p. 83*
$\mathcal{B}_{\Omega^t}$	$\{\sum\limits_{x\in\Delta} x \ : \ \Delta \in \Omega^t\}$	*p. 17*
Ω	The set $\{1, \cdots, n\}$	*p. 16*
Ω^t	The set of orbits of G on L_t^n	*p. 17*
$\mathbb{Q}L_t^n$	The vector space with basis L_t^n	*p. 58*
$E_{t,i}^n$	The i^{th} eigenspace of v^+ in L_t^n	*p. 54*
G	A finite permutation group on Ω	*p. 83*
L^n	The power set of Ω	*p. 16*
L_i^n	The set of subsets of Ω of size i	*p. 16*
n_i	$\binom{n}{i} - \binom{n}{i-1}$	*p. 8*
n_i	$\binom{n}{i} - \binom{n}{i-1}$	*p. 53*
t'	$min\{t, n-t\}$	*p. 54*
W_{tk}	The incidence matrix associated to incidence structure $(L_t^n, L_k^n, \subseteq)$	*p. 16*

X^+_{tk}	The matrix associated to $\epsilon_t^{(n)k} : (\mathbb{Z}L_t^n)^G \to (\mathbb{Z}L_k^n)^G$ with respect to bases $\mathcal{B}_{\Omega^t}$ and $\mathcal{B}_{\Omega^k}$	*p. 17*
X^-_{tk}	The matrix associated to $\partial_k^{(n)t} : (\mathbb{Z}L_k^n)^G \to (\mathbb{Z}L_t^n)^G$ with respect to bases $\mathcal{B}_{\Omega^k}$ and $\mathcal{B}_{\Omega^t}$	*p. 17*

In this thesis, groups always act on the right and for group action we use exponential notation. Maps are applied on the left.

CHAPTER 2

Modules over a P.I.D. and Matrix Normal Form

In this Chapter we reorganize and deepen various concepts found in the literature. We consider the necessary prerequisites about modules and equivalence of matrices. For more references see [1], [5], [9] and [12].

2.1 Incidence matrices

For completeness we recall some well-known notion about incidence structures.

Definition 2.1.1. *A finite incidence structure is a triple* $\mathcal{I}_{\mathcal{P}\mathcal{B}} = (\mathcal{P}, \mathcal{B}; \mathcal{I})$ *where* $\mathcal{P}$ *and* $\mathcal{B}$ *are nonempty finite sets and* $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$*. The sets* $\mathcal{P}$ *and* $\mathcal{B}$ *are called the point set and the block set of* $\mathcal{I}_{\mathcal{P}\mathcal{B}}$*, respectively, and their elements are called points and blocks. The set* $\mathcal{I}$ *is called the incidence relation.*

Definition 2.1.2. *An incidence matrix of the incidence structure* $\mathcal{I}_{\mathcal{P}\mathcal{B}}$ *is the* $(0,1)$*-matrix whose rows are indexed by the points of* $\mathcal{I}_{\mathcal{P}\mathcal{B}}$*, columns are indexed by the blocks of* $\mathcal{I}_{\mathcal{P}\mathcal{B}}$ *and the* (p, b)*-entry is equal to* 1 *if and only if* $(p, b) \in \mathcal{I}$*.*

In this work we deal with particular incidence structure, which we are going to define now.

Given $\Omega = \{1, 2, \cdots, n\}$ a finite set, we denote by L^n the power set of Ω and we partition it into the sets L_i^n, for $0 \le i \le n$, where L_i^n is the set of subsets of Ω of size i; i.e. the elements of L_i^n are the i-subsets of Ω.

Put $\mathcal{P} = L_t^n$, $\mathcal{B} = L_k^n$ and $\mathcal{I}$ the containment relation for subsets of Ω, that is $(T, K) \in \mathcal{I}$ if and only if $T \subseteq K$; the triple $\mathcal{I}_{tk}^n = (L_t^n, L_k^n; \subseteq)$ is an incidence structure.

The incidence matrix associated to this incidence structure is denoted by $W_{tk}(n)$ and it is called *the incidence matrix of t-subsets vs. k-subsets of* Ω. When there is no chance of confusion, we will write W_{tk} for $W_{tk}(n)$.

We conclude this section with the introduction of a concept useful later on. A tactical decomposition of an incidence structure $\mathcal{I}_{\mathcal{P}\mathcal{B}} = (\mathcal{P}, \mathcal{B}; \mathcal{I})$ is a partition of $\mathcal{P}$ into disjoint point sets (called the point classes) Δ, together with a partition of $\mathcal{B}$ into disjoint block sets (block classes) Γ, such that for any point class Δ and any block class Γ, the number of points of Δ on a block $B \in \Gamma$ depends only on Δ and Γ, not on B, and can hence be denoted by $y_{\Gamma,\Delta}$. Dually, the number of blocks of Γ through $P \in \Delta$ depends only on Γ and Δ, and can be denoted by $x_{\Delta,\Gamma}$.

Now let $\mathcal{I}'_{\mathcal{P}\mathcal{B}}$ be a tactical decomposition of a finite incidence structure $\mathcal{I}_{\mathcal{P}\mathcal{B}}$ and let the (point and block) classes of $\mathcal{I}'_{\mathcal{P}\mathcal{B}}$ be numbered in an arbitrary but fixed way: $\Delta_1, \cdots, \Delta_r$ and $\Gamma_1, \cdots, \Gamma_s$. Then we define two matrices

$$Y = (y_{\Gamma_i,\Delta_j}) \qquad \text{and} \qquad X = (x_{\Delta_j,\Gamma_i}).$$

Y and X are called incidence matrices of $\mathcal{I}'_{\mathcal{P}\mathcal{B}}$, with respect to the chosen numbering of the $\mathcal{I}'_{\mathcal{P}\mathcal{B}}$-c1asses. Clearly, Y and X are integral $s \times r$- and $r \times s$-matrices, respectively.

Now, if we denote by $Sym(n)$ the symmetric group on Ω, the action of $Sym(n)$ is extended in natural way to L_i^n. Formally, if $g \in Sym(n)$ and $\alpha_1, \cdots \alpha_i \in \Omega$ then

$$\{\alpha_1, \cdots, \alpha_i\}^g = \{\alpha_1^g, \cdots, \alpha_i^g\}.$$

Taken $G \subseteq Sym(n)$ a permutation group on Ω, we denote by τ_i the number of orbits of G on L_i^n. For $0 \le t \le k \le n$, we put $\Omega^t = \{\Delta_1, \cdots, \Delta_{\tau_t}\}$ and $\Omega^k = \{\Gamma_1, \cdots, \Gamma_{\tau_k}\}$ the G-orbits sets on L_t^n and L_k^n, respectively. The pair (Ω^t, Ω^k) is a tactical decomposition of $\mathcal{I}_{tk}^n$.

We denote by $X_{tk}^+ = (x_{ij}^+)$ and $X_{tk}^- = (x_{ji}^-)$ the incidence matrices of (Ω^t, Ω^k), where

$$x_{ij}^+ = |\{x \in \Delta_j \,:\, x \subseteq y, \text{ for one fixed } y \in \Gamma_i\}|$$

and

$$x_{ji}^- = |\{y \in \Gamma_i \,:\, x \subseteq y, \text{ for one fixed } x \in \Delta_j\}|.$$

2.2 Equivalence of matrices with entries in a P.I.D.

In the following D is a principal ideal domain. Here we give some results of Module Theory (see [9]).

Definition 2.2.1. *Let A and B be two matrices over D of the same size $m \times n$. Then B is said to be* equivalent *to A (over D), and we write $A \sim B$, if there exist invertible matrices $Q \in GL_m(D)$ and $P \in GL_n(D)$ such that $A = Q^{-1}BP$.*

In particular, a matrix $B \in Mat_{m,n}(D)$ is said to be a diagonal form *for the matrix A, if $A \sim B$ and the entry (i, j) is 0 when $i \neq j$. Observe that in general $m \neq n$; so we have the following possible cases for diagonal matrices*

$$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \cdots & \\ & & \cdots & \lambda_n \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \; if \;\; m > n, \; \begin{pmatrix} \lambda_1 & & & & 0 & \cdots & 0 \\ & \lambda_2 & & & 0 & \cdots & 0 \\ & & \cdots & & 0 & \cdots & 0 \\ & & & \lambda_m & 0 & \cdots & 0 \end{pmatrix} \; if \;\; m < n \quad (2.1)$$

or

$$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \cdots & \\ & & & \lambda_m \end{pmatrix} \; if \;\; m = n \qquad (2.2)$$

In general, if s the minimum between m and n, we will write these matrices

$$diag(\lambda_1, \cdots, \lambda_s).$$

The relation defined in 2.2.1 is an equivalence relation. It is possible to obtain equivalent matrices by appropriate elementary row and column operations (see [9], Chapter 7)

Definition 2.2.2. *We say that the matrix $B \in Mat_{m,n}(D)$ is in Smith Normal Form if $B = diag(d_1, \cdots, d_s)$ such that the entry d_i divides d_{i+1}. If $A \in Mat_{m,n}(D)$ is equivalent to $B = diag(d_1, \cdots, d_s)$, then the sequence $d_1, \cdots, d_s$ is called a sequence of invariant factors of A over D.*

We observe that the sequence of invariant factors is unique up to multiplication by units.

We will make use of the two following Theorems, we give them without proof (see [9]).

Theorem 2.2.3. *Every matrix $A = (a_{ij}) \in Mat_{m,n}(D)$ is equivalent to a matrix in Smith Normal Form over D.*

Theorem 2.2.4. *Two $m \times n$ matrices over a principal ideal domain D are equivalent over D if and only if they have the same sequence of invariant factors over D up to units.*

2.3 Finitely Generated Modules over a P.I.D.

Throughout D denotes a P.I.D. We assume that concepts about direct sums, linear independence and free modules are known (see [9]). We are now in a position to state and prove the theorem on the structure of the finitely generated modules over a P.I.D. D (see Theorem 2.3.8). It leads, in fact, to a classification of such modules (in terms of certain sequences of elements of D), achieved by expressing them as direct sums of certain cyclic submodules.

Despite the fact that the theorem is well known, it is also the theoretical framework of this thesis and, accordingly, we will report it with proof. Our reference for the content of this section is [9].

Theorem 2.3.1. *Let M be a free D-module of finite rank n, and N a submodule of M. Then there exists a basis $\{v_1, .., v_n\}$ of M and $d_1, \cdots, d_n \in D$ such that*

(1) the non-zero elements of $\{d_1 v_1, \cdots, d_n v_n\}$ form a basis for N and

(2) $d_1 | d_2 | \cdots | d_n$

Proof.
Let N be a submodule of a free D-module M and $\mathcal{B} = \{v_1, \cdots, v_n\}$ be a basis of M. If $N = \{0\}$, then $\{d_1 v_1, \cdots, d_n v_n\}$, where $d_i = 0$, is a basis of N.

If $N \neq \{0\}$, N is free. Let now $C = \{w_1, \cdots w_m\}$ be a basis of N. Then $w_i = \sum_{j=1}^{n} a_{ji} v_j$. Let $\alpha : N \longrightarrow M$ be the map such that $\alpha(w) = w$. The matrix associated to α with respect to C and $\mathcal{B}$ of N and M is $A = (a_{ji})$.

Then there exist two invertible matrices Q and P over D such that $B = Q^{-1}AP = diag(d_1, \cdots, d_m)$ and $d_1|d_2|\cdots|d_m$ (see Theorem 2.2.3). Q and P determine two new bases $\mathcal{B}' = \{v_1', \cdots, v_n'\}$ and $C' = \{w_1', \cdots, w_m'\}$ of M and N such that

$$v_i' = \sum_{j=1}^{n} q_{ji} v_j$$

and

$$w_i' = \sum_{j=1}^{m} p_{ji} w_j$$

The elements v_i are expressed in terms of the v_j' by means of the matrix Q^{-1}. The matrix of α with respect to C' and $\mathcal{B}'$ is $B = Q^{-1}AP$, which is the Smith Normal Form of A. In particular

$$\begin{cases} w_1' = d_1 v_1' \\ \vdots \\ w_m' = d_m v_m' \end{cases} \tag{2.3}$$

Put $d_{m+1} = \cdots = d_n = 0$ we have the claim. $\square$

Definition 2.3.2. *If M is a D-module, then the annihilator of M, denoted $Ann(M)$, is defined by*

$$Ann(M) = \{d \in D : \ dm = 0 \textit{ for all } m \in M\}.$$

Definition 2.3.3. *Let M be a D-module. We say that $m \in M$ is a torsion element if there exists $d \neq 0 \in D$ such that $dm = 0$. Let T be the set of torsion elements of M, i.e.*

$$T = \{m \in M \ : \ \exists\, d \neq 0 \in \mathbb{Z} \ s.t. \ dm = 0\}.$$

M is said to be torsion-free if $T = \{0\}$, and M is a torsion module if $M = T$.

Theorem 2.3.4. *Let M be a D-module and let T be the set of torsion elements of M. Then*

1. *T is a submodule of M, called the torsion submodule.*
2. *M/T is torsion-free.*

Proof.

1. Clearly $0 \in T$. Let $t_1, t_2 \in T$, then by definition there exist non-zero $r_1, r_2 \in D$ such that $r_1 t_1 = r_2 t_2 = 0$. Hence $r_1 r_2 (t_1 - t_2) = (r_2 r_1) t_1 - (r_1 r_2) t_2 = 0$. Since D has no zero divisors, $r_1 r_2 \neq 0$ and so $t_1 - t_2 \in T$. Furthermore, if $r \in D$, then $r_1(rt_1) = r(r_1 t_1) = 0$, and $rt_1 \in T$.
2. Suppose that $r \neq 0 \in D$ and $r(m + T) = T \in M/T$. Then $rm \in T$, so there is $s \neq 0 \in D$ with $(sr)m = s(rm) = 0$. Since $sr \neq 0$, it follows that $m \in T$, i.e. $m + T = T \in M/T$.

□

Definition 2.3.5. *Let M be a cyclic D-module and let Ann(M) be the annihilator of M. Since D is a principal ideal domain, $Ann(M) = Dd$, where $d \in D$. Then we say that d is the* order *of M.*

We will deal always with finitely generated D-module. We just remind

Lemma 2.3.6. *Every finitely generated D-module is a homomorphic image of a free D-module.*

Lemma 2.3.7. *Let $L = L_1 \oplus \cdots \oplus L_t$ be an internal direct sum of D-submodules. For each i, let N_i be a submodule of L_i and $N = N_1 \oplus \cdots \oplus N_t$. Then, if $\nu : L \longrightarrow \frac{L}{N}$ is the natural epimorphism, we have $\frac{L}{N} = \nu(L) = \nu(L_1) \oplus \cdots \oplus \nu(L_t)$ and $\nu(L_i) \cong \frac{L_i}{N_i}$*

We are now ready to prove

Theorem 2.3.8. *Let M be a finitely generated D-module. Then M can be expressed as an internal direct sum $M = M_1 \oplus \cdots \oplus M_t$, $t \geq 0$, such that M_i is a non-trivial cyclic submodule of M of order d_i and $d_1|d_2|\cdots|d_t$.*

Proof. Since M is a finitely generated module, by Lemma 2.3.6 there exists a free module V such that $\phi : V \longrightarrow M$ is an epimorphism. Put $W = Ker\ \phi \subseteq V$, there exists an isomorphism $\psi : \frac{V}{W} \longrightarrow M$.

Let now $\mathcal{B} = \{v_1, \cdots, v_n\}$ be a basis of V, then $V = Dv_1 \oplus \cdots \oplus Dv_n$ and $W \subseteq V$ is free. So there exist $c_1, \cdots, c_n$ such that $c_1|\cdots|c_n$ and the non-zero elements of $\{c_1v_1, \cdots, c_nv_n\}$ form a basis of W, by Theorem 2.3.1. Then $W = D(c_1v_1) \oplus \cdots \oplus D(c_nv_n)$. If $\nu : V \longrightarrow \frac{V}{W}$ is the canonical epimorphism, then we have

$$\frac{V}{W} = \nu(V) = \nu(Dv_1) \oplus \cdots \oplus \nu(Dv_n) = D\nu(v_1) \oplus \cdots \oplus D\nu(v_n) \tag{2.4}$$

In particolar $\nu(v_i)$ has order c_i. Actually, $d\nu(v_i) = 0$, where $0 \neq d \in D$ if and only if $\nu(dv_i) = 0$ if and only if $dv_i \in W = Ker\ \nu$ if and only if $dv_i \in D(c_iv_i)$ (because it belongs to $W \cap Dv_i$) if and only if $c_i|d$.

Since ψ is an isomorphism, it maps the direct decomposition of V/W into a direct decomposition of M.

Let u be the last integer i such that c_i is a unit. Then $c_1, \cdots, c_u$ are all units by the divisibility condition, and the corresponding modules in Equation 2.4 are exactly the zero modules and can be omitted. Therefore, $t = n - u$ and $M = M_1 \oplus \cdots \oplus M_t$, where $M_i = D\psi\nu(v_{u+i}) = D\phi(v_{u+i})$ is a non-trivial cyclic module of order $d_i = c_{u+i}$ and $d_1|d_2|\cdots|d_t$. This concludes the proof. □

If $M = M_1 \oplus \cdots \oplus M_s = M_1^{'} \oplus \cdots \oplus M_t^{'}$ are two direct decompositions of M into non-trivial cyclic modules M_i of order d_i and $M_i^{'}$ of order $d_i^{'}$ such that $d_1|d_2|\cdots|d_s$ and $d_1^{'}|d_2^{'}|\cdots|d_t^{'}$, then $s = t$ and $Dd_i = Dd_i^{'}$, for $i = 1, \cdots, s$. In particular d_i and $d_i^{'}$ are associates.

The sequence $d_1, d_2, \cdots, d_s$ is called *sequence of invariant factors of M*, unique up to multiplication by units.

Corollary 2.3.9. *Let M be a finitely generated D-module. Then if T is the torsion submodule of M, we have $M = T \oplus V$, where V is a free submodule of finite rank.*

2.4 Pure modules and index of submodules

In this section we introduce the concept of pure module and of index of a matrix (see [3] , [12] and [15]). These topics play a fundamental role in our proof of "Wilson's Theorem" (Theorem 4.5.4). For this reason we reorganize known notions, integrating them with useful properties for achieve our purpose. We observe that we will use properties of pure module, while R.M. Wilson considers the concept of index of a matrix. In Proposition 2.4.17 is pointed out the relation between purity and index of a matrix.

In the sequel we take $D = \mathbb{Z}$, that is we consider $\mathbb{Z}$-modules, and M will denote a $\mathbb{Z}$-module.

Definition 2.4.1. *[12] Let M_1 be a submodule of M. Then we say that M_1 is a pure submodule of M if $M_1 \cap aM = aM_1$, for every $a \in \mathbb{Z}$.*

Example 2.4.2. *Given $M = \mathbb{Z} \times \mathbb{Z}$, let N and L be the submodules generated by $(1, 0)$ and $(2, 0)$ respectively. Then N is pure in M, while L is not pure. To see this it is enough to take $a = 4$. The element $(4, 0) = 4(1, 0) = 2(2, 0) \in L \cap 4M$, but it is not in $4L$.*

We often will make use of the following remark.

Remark 2.4.3. *We observe that the inclusion $aM_1 \subseteq M_1 \cap aM$ is always true; moreover, the equality is trivial if $a = 0$.*

Proposition 2.4.4. *Let M_1 and M_2 be submodules of M such that $M_1 \subseteq M_2$. If M_1 is a pure submodule of M, then it is also a pure submodule of M_2.*

Proof. Since $M_1 \cap aM = aM_1$, for every $a \in \mathbb{Z}$, and $aM_2 \subseteq aM$, we have $M_1 \cap aM_2 \subseteq M_1 \cap aM = aM_1$. The claim follows. □

Proposition 2.4.5. *Let M_2 be a pure submodule of M and let M_1 be a pure submodule of M_2. Then M_1 is a pure submodule of M.*

Proof. Let $a \in \mathbb{Z} \setminus \{0\}$, by hypothesis $M_1 \cap aM_2 = aM_1$ and $M_2 \cap aM = aM_2$. Let $x \in M_1 \cap aM$, since $M_1 \subseteq M_2$, then $x \in M_2 \cap aM = aM_2$, so $x \in M_1 \cap aM_2 = aM_1$. It follows that $M_1 \cap aM \subseteq aM_1$. □

Proposition 2.4.6. *Let M_1, M_2 be $\mathbb{Z}$-modules, and $\rho : M_1 \longrightarrow M_2$ an isomorphism. If a submodule L_1 of M_1 is pure in M_1 then $L_2 = \rho(L_1)$ is pure in M_2.*

Proof. Let $a \in \mathbb{Z} \setminus \{0\}$ and $y \in L_2 \cap aM_2$. There exist $x \in L_1$ and $m_2 \in M_2$ such that $\rho(x) = y$ and $y = am_2$. But $m_2 = \rho(m_1)$ for some $m_1 \in M_1$, it follows that $y = a\rho(m_1) = \rho(am_1)$ and so $y = \rho(am_1) = \rho(x)$. We conclude that $am_1 = x$ by injectivity of ρ. Therefore, $x \in L_1 \cap aM_1 = aL_1$, by purity of L_1 in M_1, then there exists $l_1 \in L_1$ such that $x = al_1$. Finally, $y = \rho(x) = a\rho(l_1) \in aL_2$. □

For later use, we focus our attention on properties of purity when M is a free $\mathbb{Z}$-module.

Proposition 2.4.7. *Let M be a free $\mathbb{Z}$-module of rank n and let M_i, $i \in I$, be a non-empty family of pure submodules of M. Then $F = \bigcap_{i\in I} M_i$ is a pure submodule of M.*

Proof. It is enough to prove that $F \cap aM \subseteq aF$, for every $a \in \mathbb{Z}$. As usual we suppose $a \neq 0$. Then let $f \in F \cap aM$, there is $m \in M$ such that $f = am$ and since $f \in F$, we have $f \in M_i$, $i \in I$. But $M_i \cap aM = aM_i$, hence there are $m_i \in M_i$ such that $f = am_i$. We consider $i \neq j$, by $f = am_i = am_j$, we deduce that $a(m_i - m_j) = 0 \in M$, where $a \neq 0$. So $m_i = m_j$, for each $i, j \in I$, because M is torsion-free. It follows that $m_j \in \cap_{i\in I} M_i$, thus $f = am_j \in aF$. □

Here we introduce an operator of closure of modules. This relates the concept of pure module to that of index of a matrix (see Definition 2.4.15).

Definition 2.4.8. *[3] Let M be a free $\mathbb{Z}$-module of rank n and let F be a submodule of M. Then the pure closure of F in M is the module $\overline{F}$ defined as the intersection of all pure submodules of M containing F. Clearly if F is a pure submodule of M, we have $\overline{F} = F$.*

Proposition 2.4.9. *[3] Let M be a free $\mathbb{Z}$-module of rank n and let F be a submodule of M. Then*

$$\overline{F} = \{l \in M \ : \exists c \in \mathbb{Z} \setminus \{0\} \ s.t. \ cl \in F\}.$$

Proof. Put $L = \{l \in M \ : \exists c \in \mathbb{Z} \setminus \{0\} \ s.t. \ cl \in F\}$. We want to prove $\overline{F} = L$. Clearly $F \subseteq L$ and so $\overline{F} \subseteq \overline{L}$. We prove that L is a pure submodule of M, i.e. $L \cap aM \subseteq aL$, for any $a \in \mathbb{Z} \setminus \{0\}$, so we can deduce that $\overline{F} \subseteq L$. For $l \in L \cap aM$, there is $m \in M$ such that $l = am$; as $l \in L$, there exists $c \in \mathbb{Z} \setminus \{0\}$ such that $cl \in F$. Thus, $cl = acm \in F$, with $ac \neq 0$, and we deduce that $m \in L$ by definition. We conclude that $l = am \in aL$. It follows that L is a pure submodule of M and, by definition of purity, $\overline{L} = L$. Hence $\overline{F} \subseteq L$.

Conversely, if $l \in L$, then there is $a \in \mathbb{Z} \setminus \{0\}$ such that $al \in F$. So $al \in aM \cap \overline{F} = a\overline{F}$. We conclude that there exists $f \in \overline{F}$ such that $al = af$, hence $l = f$, as M is torsion free. Thus $L \subseteq \overline{F}$. □

We give the definition of index of submodules.

Definition 2.4.10. *Let M be a free $\mathbb{Z}$-module of rank n and let F be a submodule of M. The index of F is the index of F as a subgroup of $\overline{F}$.*

Note that F is pure in M if and only if F has index 1.

The following results prove that a pure submodule F of a free module M coincides with M if F and M have the same rank (Lemma 2.4.14).

Theorem 2.4.11. *Let M be a free $\mathbb{Z}$-module of rank n and let F be a submodule of M of rank r. Then there exist a basis $\{v_1, \cdots, v_n\}$ of M and non-zero integers $d_1, \cdots, d_r$ such that $\{d_1v_1, \cdots, d_rv_r\}$ and $\{v_1, \cdots, v_r\}$ are bases for F and $\overline{F}$, respectively.*

Proof. By Theorem 2.3.1, there exist a basis $\{v_1, \cdots, v_n\}$ of M and non-zero integers $d_1, \cdots, d_r$ such that $\{d_1v_1, \cdots, d_rv_r\}$ is a basis of F.

Now, we prove that $\{v_1, \cdots, v_r\}$ is a basis for $\overline{F}$. Since $d_iv_i \in F$, for $i = 1, \cdots, r$, we have $v_i \in \overline{F}$, by Proposition 2.4.9. Thus it is enough to prove that $\overline{F} = span_{\mathbb{Z}}\{v_1, \cdots, v_r\}$. Let $x \in \overline{F}$, then there exists a non-zero integer c such that $cx \in F$. The vector cx is a linear combination of elements of a F-basis, i.e. $cx = \sum_{i=1}^{r} k_id_iv_i$. On the other hand, $x \in M$, so $x = \sum_{i=1}^{n} h_iv_i$. It follows that $cx = \sum_{i=1}^{n} ch_iv_i$ and $ch_i = k_id_i$, for $i = 1, \cdots, r$ and $h_{r+1} = \cdots = h_n = 0$. We conclude that $x = \sum_{i=1}^{r} h_iv_i$ is a linear combination of vectors $v_1, \cdots, v_r$. Thus $x \in span_{\mathbb{Z}}\{v_1, \cdots, v_r\}$. □

Proposition 2.4.12. *[15] Let M be a free $\mathbb{Z}$-module of rank n. Let F and L be submodules of M such that $F \subseteq L$ and F is pure in M. Then the quotient L/F is a free $\mathbb{Z}$-module.*

Proof. Let $l + F \in L/F$ be a torsion element, then there exists $c \in \mathbb{Z} \setminus \{0\}$such that $c \cdot (l + F) = F$. It follows that $cl \in F$, so $l \in \overline{F} = F$. □

Note that in general the quotient of free modules is not free.

Proposition 2.4.13. *Let M be a free $\mathbb{Z}$-module of rank n and let F, L be submodules of M. If F is pure in M, then any $\mathbb{Z}$-basis of F can be extended to a $\mathbb{Z}$-basis of $F + L$ by adjoining elements of L.*

Proof. $F \subseteq F + L \subseteq M$ and by hypothesis F is pure in M. Then, by proprosition 2.4.12, $(F + L)/F$ is a free $\mathbb{Z}$-module, so there exists a basis $\{l_1 + F, l_2 + F, \cdots, l_r + F\}$, where $\{l_1, l_2, \cdots, l_r\} \subseteq L$. Let $\{f_1, f_2, \cdots, f_t\}$ be a basis of the free module F. Now we prove that $\{f_1, \cdots, f_t, l_1, \cdots, l_r\}$ is a basis of $F + L$.

Let $m \in F + L$, then $m + F = \sum_{i=1}^{r} h_i(l_i + F) = (\sum_{i=1}^{r} h_i l_i) + F$, it follows that $m - \sum_{i=1}^{r} h_i l_i \in F$. Hence $m - \sum_{i=1}^{r} h_i l_i = \sum_{j=1}^{t} k_j f_j$, and $m = \sum_{j=1}^{t} k_j f_j + \sum_{i=1}^{r} h_i l_i$.

The vectors $f_1, \cdots, f_t, l_1, \cdots, l_r$ are linearly independent, indeed if $k_1 f_1 + \cdots + k_t f_t + h_1 l_1 + \cdots + h_r l_r = 0$, then $F = (k_1 f_1 + \cdots + k_t f_t + h_1 l_1 + \cdots + h_r l_r) + F = (h_1 l_1 + \cdots + h_r l_r) + F = h_1(l_1 + F) + \cdots + h_r(l_r + F)$. Since $\{l_1 + F, l_2 + F, \cdots, l_r + F\}$ is a basis for the quotient module, $h_i = 0$, for $i = 1, \cdots, r$. It follows that $k_1 f_1 + \cdots + k_t f_t = 0$, so $k_j = 0$ because $\{f_1, f_2, \cdots, f_t\}$ is a basis of F. □

The following proposition is very important in our Wilson's Theorem proof.

Lemma 2.4.14. *[3] Let M be a free $\mathbb{Z}$-module of rank n. If F and L are submodules of M such that*

1. $F \subseteq L$,

2. F is pure in M,

3. $rank(F) = rank(L)$,

then $F = L$.

Proof. We consider the submodule $L = F + L$. By Proposition 2.4.13, any basis of F can be extended to a basis of L adjoining elements of L. But F and L have the same rank, so any basis of F is a basis of L. □

Now we return to the matrices with coefficient in $\mathbb{Z}$ and we work on modules generated by their rows.

Let A be an integral matrix $m \times n$. Then we use $row_{\mathbb{Z}}(A)$ to denote the $\mathbb{Z}$-module spanned by the row vectors of A, and $row_{\mathbb{Q}}(A)$ to denote the vector space over $\mathbb{Q}$, generated by the rows of A.

Definition 2.4.15. *[15] We define the* index *of an integral matrix A to be the index of $row_{\mathbb{Z}}(A)$ as a subgroup of the module $Z(A)$ of all integral vectors which belong to $row_{\mathbb{Q}}(A)$.*

We observe that if A has index 1, then every integral vector which is a rational linear combination of the rows of A is already an integral linear combination of the rows of A, that is $row_{\mathbb{Z}}(A)$ is a pure submodule of $\mathbb{Z}^n$.

About index we recall the proposition proved by Wilson below.

Proposition 2.4.16. *[15] Let A be an integral matrix. Then A has index* 1 *if and only if $A = ABA$ for some integral matrix B.*

Proof. Suppose $A = ABA$ and let x be an integral vector in $row_{\mathbb{Q}}(A)$, say $x = yA$, where y is rational. Then

$$x = yA = yABA = (xB)A = zA$$

where z is integral; so $x \in row_{\mathbb{Z}}(A)$ and this shows that A has index 1.

Conversely, suppose $EAF = D$, where E, F are unimodular and D is diagonal with entries 0 and 1. Say A is $m \times n$. If $m \leq n$, let $F' = F$ and E' be obtained from E by adjoining $(n - m)$ rows of zeros; if $m \geq n$, let $E' = E$ and let F' be obtained from F by adjoining $(m - n)$ columns of zeros. In either case, $AF'E'A = A$. □

Proposition 2.4.17. *Let A be an integral matrix of size $s \times n$. Put $F = row_{\mathbb{Z}}(A)$. Then $\overline{F} = Z(A)$ in $\mathbb{Z}^n$.*

Proof. Let $\{A_1, \cdots, A_s\}$ be the rows of A, that is a generating set of $row_{\mathbb{Z}}(A)$. First we prove that $\overline{F} \subseteq Z(A)$. Let $\mathbf{x} \in \overline{F}$, then there exists $c \neq 0 \in \mathbb{Z}$ such that $c\mathbf{x} \in F \subseteq Z(A) \subseteq row_{\mathbb{Q}}(A)$. Since $row_{\mathbb{Q}}(A)$ is a vector space and $c \neq 0$ we have $\mathbf{x} = c^{-1}(c\mathbf{x}) \in row_{\mathbb{Q}}(A)$. So $\mathbf{x} \in Z(A)$. Conversely, let $\mathbf{y} \in Z(A)$, then $\mathbf{y} \in \mathbb{Z}^n \cap row_{\mathbb{Q}}(A)$. Hence $\mathbf{y} = q_1A_1 + \cdots + q_sA_s$, where $q_i \in \mathbb{Q}$, and there exists $c \neq 0 \in \mathbb{Z}$ such that $c\mathbf{y} \in row_{\mathbb{Z}}(A) = F$. We conclude that $\mathbf{y} \in \overline{F}$. □

The following proposition allows to link the non-zero invariant factors of a matrix A with the index of the module generated by its rows.

Proposition 2.4.18. *Let B be a diagonal form of an integral matrix A and suppose that it has non-zero entries $d_1, d_2, \cdots, d_r$. Then the group $\frac{Z(A)}{row_{\mathbb{Z}}(A)}$ is finite and is isomorphic to the direct sum of cyclic groups of orders $d_1, d_2, \cdots, d_r$.*

Proof. We want to apply Lemma 2.3.7. We put $F = row_{\mathbb{Z}}(A)$; by Proposition 2.4.17 we have that $\overline{F} = Z(A)$.

Let $\alpha : \mathbb{Z}^m \longrightarrow \mathbb{Z}^n$ be the map induced by A^T with respect to the canonical bases, so defined

$$\begin{pmatrix} x_1 \\ \cdots \\ x_m \end{pmatrix} \longrightarrow A^T \begin{pmatrix} x_1 \\ \cdots \\ x_m \end{pmatrix}$$

$Im\,\alpha = span_{\mathbb{Z}}(A^T e_1, \cdots, A^T e_m) = row_{\mathbb{Z}}(A)$, where $\{e_1, \cdots, e_m\}$ is a canonical basis of $\mathbb{Z}^m$. Let $A^T \sim B = diag(d_1, \cdots, d_r)$, where $d_1, \cdots, d_r$ are non-zero integers. So there exist two bases $\{w_1, \cdots, w_m\}$ di $\mathbb{Z}^m$ and $\{v_1, \cdots, v_n\}$ of $\mathbb{Z}^n$, such that $\alpha(w_i) = d_i v_i$ for $i = 1, \cdots, r$ and $\alpha(w_i) = 0$ for $i = r+1, \cdots, m$.

It follows that $F = Im\,\alpha = span_{\mathbb{Z}}(\alpha(w_1), \cdots, \alpha(w_m)) = span_{\mathbb{Z}}(d_1 v_1, \cdots, d_r v_r)$.

$\mathcal{B}' = \{d_1 v_1, \cdots, d_r v_r\}$ is a basis of F, since $\mathbb{Z}^n$ is torsion free. By Theorem 2.4.11, $\{v_1, \cdots, v_r\}$ is a basis of $\overline{F}$. So $\overline{F} = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r$ and $F = \mathbb{Z}(d_1 v_1) \oplus \cdots \oplus \mathbb{Z}(d_r v_r)$. The claim follows from Lemma 2.3.7. $\square$

Now we quote Proposition 3 in [15]

Proposition 2.4.19. *Let $v_1, v_2, \cdots, v_r$ be a $\mathbb{Z}$-basis of a module $M \subseteq \mathbb{Z}^n$ of index 1. Then the matrix whose rows are $d_1 v_1, d_2 v_2, \cdots, d_r v_r$ has as a diagonal form the $r \times n$ diagonal matrix with entries $d_1, d_2, \cdots, d_r$ and in particular it has index $d_1 d_2 \cdots d_r$, if all d_i are non-zero.*

Proof. Let $\mathcal{D} = \{v_1, ..., v_r\}$ be a $\mathbb{Z}$-basis of M. Fixed $d_1, ..., d_r \in \mathbb{Z}$, we consider the linear map

$$\varphi : \begin{cases} M & \longrightarrow & \mathbb{Z}^n \\ \sum_{i=1}^{r} h_i v_i & \longrightarrow & \sum_{i=1}^{r} d_i h_i v_i \end{cases}$$

Since M has index 1, it is pure and we can extend $\mathcal{D}$ to a basis $C = \{v_1, ..., v_r, w_{r+1}, ..., w_n\}$ of $\mathbb{Z}^n$ (see Proposition 2.4.13). Thus $Im\,\varphi = span_{\mathbb{Z}}(d_1 v_1, ..., d_r v_r)$ and the matrix associated to φ with respect to the bases $\mathcal{D}$ and C is

$$D^T = \begin{pmatrix} d_1 & 0 & ... & 0 \\ 0 & d_2 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & d_r \\ 0 & 0 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & 0 \end{pmatrix}.$$

Now we consider the canonical basis $\mathcal{E} = \{e_1, e_2, \cdots, e_n\}$ in $\mathbb{Z}^n$. With respect to the bases $\mathcal{D}$ and $\mathcal{E}$, the matrix associated to φ is

$$A^T = \begin{pmatrix} d_1 v_1 & | & d_2 v_2 & | & ... & | & d_r v_r \end{pmatrix},$$

whose columns are $d_i v_i$ for any $i = 1, ..., r$. We conclude that D^T and A^T are equivalent, that is D^T is a diagonal form of A^T.

Now we suppose $d_i \neq 0$, for $i = 1, \cdots, r$. Since $Im(\varphi) = span_{\mathbb{Z}}(d_1 v_1, ..., d_r v_r) \subseteq M$ and M is pure in $\mathbb{Z}^n$ we get $\overline{Im\,\varphi} \subseteq M$, by Definition 2.4.8. Thus $Im\,\varphi \subseteq \overline{Im\,\varphi} \subseteq M$. From $rank(Im\,\varphi) = rank(M)$, we have $rank(\overline{Im\,\varphi}) = rank(M)$. By Lemma 2.4.14, we get $\overline{Im\,\varphi} = M$.

Applying Lemma 2.3.7 to $\overline{Im\,\varphi} = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r$ and $Im\,\varphi = \mathbb{Z}d_1 v_1 \oplus \cdots \oplus \mathbb{Z}d_r v_r$, we have that the module $\frac{\overline{Im\,\varphi}}{Im\,\varphi}$ is direct sum of cyclic modules of order d_i, that is

$$\frac{\overline{Im\,\varphi}}{Im\,\varphi} \cong \frac{\mathbb{Z}v_1}{\mathbb{Z}d_1v_1} \times \cdots \times \frac{\mathbb{Z}v_r}{\mathbb{Z}d_rv_r}.$$

The claim follows considering the matrices A and D and observing that $Im\,\varphi = row_{\mathbb{Z}}(A)$.

□

Example 2.4.20. *If you take* $M = \mathbb{Z}^3$, $v_1 = (1,0,0)$, $v_2 = (1,1,0)$, $v_3 = (1,0,1)$ *and* $d_1 = 2$, $d_2 = 3$, $d_3 = 4$, *then*

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 3 & 3 & 0 \\ 4 & 0 & 4 \end{pmatrix}.$$

Applying the elementary column operations we get

$$A \sim \begin{pmatrix} 2 & 0 & 0 \\ 3 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

If we consider the map φ *defined in Proposition 2.4.19, then* $Im\,\varphi = \{2v_1, 3v_2, 4v_3\} = row_{\mathbb{Z}}(A)$ *and* $\overline{Im\,\varphi} = span_{\mathbb{Z}}\{v_1, v_2, v_3\} = \mathbb{Z}^3$. *So*

$$\frac{\overline{Im\,\varphi}}{Im\,\varphi} \cong C_2 \times C_3 \times C_4,$$

where C_i *is the cyclic group of order* i.

We conclude this chapter with the definition of Smith group of a linear map.

Definition 2.4.21. *Given the free* $\mathbb{Z}$*-modules* M, N *of finite rank and a linear map*

$$\varphi : N \longrightarrow M.$$

Then the Smith group of φ *is defined as*

$$\frac{M}{\varphi(N)}.$$

We observe that in general $\frac{M}{\varphi(N)} = T \oplus V$, where T is the torsion submodule and V is a free submodule of finite rank (Corollary 2.3.9). If $M = \overline{\varphi(N)}$, then $\frac{M}{\varphi(N)} = T$.

CHAPTER 3

A diagonal form for incidence matrices of t-subsets vs k-subsets

In this chapter we deal with well-known results about a diagonal form for incidence matrices of t-subets vs k-subsets on a n-set Ω. These matrices, introduced in Chapter 2 and denoted by $W_{tk}(n)$ have been studied by Wilson in [15] and Bier in [2].

3.1 A diagonal form for the incidence matrix W_{tk} (Wilson's proof)

Here we give Wilson's original proof. He uses the notion of *index* introduced in section 2.4: the index of an integral matrix M is the index of the $\mathbb{Z}$-module generated by the rows of M, called $row_{\mathbb{Z}}(M)$, as a subgroup of the module $Z(M)$ of all integral vectors which belong to $row_{\mathbb{Q}}(M)$, the vector space generated by the rows of M.

We will construct a matrix $M_{tk}(n)$ using the matrices $W_{ik}(n)$, for $i = 0, \cdots, t$; in Proposition 3.1.3 we will prove that $M_{tk}(n)$ has index 1, that is $Z(M_{tk}(n)) = row_{\mathbb{Z}}(M_{tk}(n))$ and that $W_{tk}(n)$ and $M_{tk}(n)$ have the same rank. Thus, in order to give a diagonal form of $W_{tk}(n)$, (see Theorem 3.1.6), it will be enough to find appropriate bases of $row_{\mathbb{Z}}(M_{tk}(n))$ and $row_{\mathbb{Z}}(W_{tk}(n))$ (see Propositions 3.1.4 and 3.1.5).

We begin with some notation. Given the $n_i \times m$ matrices A_i with $i = 0, \cdots, t$, we denote by

$$\bigcup_{i=0}^{t} A_i$$

the $n_0 + n_1 + \cdots + n_t \times m$ matrix obtained by stacking the matrices $A_0, A_1, \cdots, A_t$ one on top of the other, that is

$$A = \begin{pmatrix} A_0 \\ A_1 \\ \vdots \\ A_t \end{pmatrix}.$$

For $0 \leq t \leq k \leq n$ we define

$$M_{tk}(n) = \bigcup_{i=0}^{t} W_{ik}(n) = \begin{pmatrix} W_{0k}(n) \\ W_{1k}(n) \\ \vdots \\ W_{tk}(n) \end{pmatrix}.$$

Example 3.1.1. *Taken $n = 3$, $t = 1$ and $k = 2$, the matrix $M_{12}(3)$, whose rows are* *indexed by* $\emptyset, \{1\}, \{2\}, \{3\}$ *and columns are indexed by* $\{1,2\}, \{1,3\}, \{2,3\}$*, is*

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

In the sequel, if there is not confusion, we write W_{tk} instead $W_{tk}(n)$ and M_{tk} instead $M_{tk}(n)$. The following Lemma will be of fundamental importance

Lemma 3.1.2. *For* $0 \le j \le t \le k \le n$

$$W_{jt}W_{tk} = \binom{k-j}{t-j} W_{jk}. \tag{3.1}$$

Proof. The proof follows immediatly from the relation

$$W_{jt}W_{tk}(S,K) = \sum_T W_{jt}(S,T)W_{tk}(T,K),$$

for an j-subset S and a k-subset K and where the sum is extended over all t-subsets T of Ω. We have the claim observing that the number of t-subsets T such that $S \subseteq T \subseteq K$ is $\binom{k-j}{t-j}$ if $S \subseteq K$, and 0 otherwise. □

Now, we observe that the Equation 3.1 shows that $row_{\mathbb{Q}}(W_{jk}) \subseteq row_{\mathbb{Q}}(W_{tk})$ for $j \le t$ and hence $row_{\mathbb{Q}}(M_{tk}) = row_{\mathbb{Q}}(W_{tk})$. In particular, M_{tk} has rank at most $\binom{n}{t}$ (i.e. the number of rows of W_{tk}).

More precisely, we get:

Proposition 3.1.3. *For non-negative integers* t, k, n *with* $0 \le t \le k \le n - t$*, the matrix* M_{tk} *has rank* $\binom{n}{t}$ *and index* 1*.*

Proof. We consider separately two cases:

1. $0 \leq t \leq k \leq n$ and $k = n - t$,
2. $0 \leq t \leq k \leq n$ and $k < n - t$.

Case 1. We claim that

$$\sum_{i=0}^{t} (-1)^i \bar{W}_{ik}^T W_{ik} = I_{\binom{n}{k}}, \tag{3.2}$$

where $I_{\binom{n}{k}}$ is the identity matrix of order $\binom{n}{k}$ and $\bar{W}_{ik}$ is the $\binom{n}{i} \times \binom{n}{k}$ matrix defined by

$$\bar{W}_{ik}(S,K) = \begin{cases} 1 & \text{if } S \cap K = \emptyset \\ 0 & \text{otherwise} \end{cases} \tag{3.3}$$

for a i-subset S and a k-subset K. To prove this just note that the entry in row A and column B on the left-hand side of 3.2 is

$$\sum_{i=0}^{t} (-1)^i \binom{|B| - |A \cap B|}{i} = \begin{cases} 0 & \text{if } A \neq B \\ 1 & \text{if } A = B \end{cases} \tag{3.4}$$

Indeed, for an i fixed, $\bar{W}_{ik}^T W_{ik}(A,B)$ is the number of all i-subsets S of Ω such that $S \cap A = \emptyset$ and $S \subseteq B$, that is $\binom{|B|-|A\cap B|}{i}$. If $A = B$ it is clear that the left-hand side of equation (3.4) is 1. If $A \neq B$, then $|A \cap B| \geq n - 2t$, as both A and B have cardinality $n - t$ (the bound is achieved when A contains the complement of B), hence $t \geq n - t - |A \cap B| = |B| - |A \cap B|$. Put $q = |B| - |A \cap B|$; we get

$$\sum_{i=0}^{t} (-1)^i \binom{|B| - |A \cap B|}{i} = \sum_{i=0}^{q} (-1)^i \binom{q}{i} = (-1+1)^q.$$

So 3.2 can be written as

$$\bar{M}_{tk}^T M_{tk} = I_{\binom{n}{t}},$$

where

$$\bar{M}_{tk} = \bigcup_{i=0}^{t} (-1)^i \bar{W}_{ik}.$$

The matrix $A = \bar{M}_{tk}^T$ is an integral matrix such that $AM_{tk} = I_{\binom{n}{t}}$. We deduce that $row_{\mathbb{Z}}(I_{\binom{n}{t}}) \subseteq row_{\mathbb{Z}}(M_{tk})$; so $\binom{n}{t} = rank(I_{\binom{n}{t}}) \leq rank(M_{tk})$ and $rank(M_{tk}) = \binom{n}{t}$. About the index, we observe that $M_{tk}AM_{tk} = M_{tk}$, so that by Proposition 2.4.16, M_{tk} has index 1.

Case 2. We assume $k < n - t$ and we prove the statement by induction on $n + t + k$. If $t = 0$ then the claim follows observing that

$$M_{0k} = W_{0k} = \begin{pmatrix} 1 \cdots 1 \end{pmatrix}.$$

Now we suppose $0 < t \leq k < n-t$. Given $1 \leq j \leq t$, choose a point x_0 in the n-set Ω. Then the rows (j-subsets) and columns (k-subsets) of $W_{jk}(n)$ are partitioned according to whether or not they contain x_0. This gives us a block decomposition of $W_{jk}(n)$:

$$W_{jk}(n) = \left(\begin{array}{c|c} W_{j-1,k-1}(n-1) & 0 \\ \hline W_{j,k-1}(n-1) & W_{jk}(n-1) \end{array}\right).$$

After permuting rows, we find that $M_{tk}(n)$ is equivalent to

$$\left(\begin{array}{c|c} M_{t-1,k-1}(n-1) & 0 \\ \hline M_{t,k-1}(n-1) & M_{tk}(n-1) \end{array}\right).$$

By the induction hypothesis applied to $M_{t-1,k-1}(n-1)$ and $M_{tk}(n-1)$, we can use elementary integral row and column operations to reduce the above matrix to

$$\left(\begin{array}{cc|cc} I_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline * & * & I_2 & 0 \\ * & * & 0 & 0 \end{array}\right) \tag{3.5}$$

where I_1 and I_2 are identity matrices of orders $\binom{n-1}{t-1}$ and $\binom{n-1}{t}$, respectively. Then $rank(M_{tk}(n)) \geq \binom{n-1}{t-1} + \binom{n-1}{t} = \binom{n}{t}$, hence $rank(M_{tk}(n)) = \binom{n}{t}$.

Further row operations on the matrix in 3.5 can be used to create an identity of order $\binom{n}{t}$ as a submatrix of some $M \sim M_{tk}(n)$.

Since $\binom{n}{t}$ is the rank of $M_{tk}(n)$, all other entries of M must be zeros. We deduce that $M_{tk}(n)$ is equivalent to a diagonal matrix with 1's entries, so its index is 1.

□

The argument in Lemma 3.1.3 shows that $Z(M_{tk}(n)) = row_{\mathbb{Z}}(M_{tk}(n))$, of rank $\binom{n}{t}$. As $row_{\mathbb{Z}}(W_{tk}) \subseteq row_{\mathbb{Z}}(M_{tk}(n))$ and $rank\,(row_{\mathbb{Z}}(M_{tk}(n))) = rank\,(row_{\mathbb{Z}}(W_{tk}))$, by 2.4.14 we have that $Z(W_{tk}) = Z(M_{tk}(n))$.

As said above, we want to find an appropriate basis of $Z(M_{tk}(n))$ and, consequently, a basis of $row_{\mathbb{Z}}(W_{tk})$ such that it is easy to determine the module $\frac{Z(M_{tk}(n))}{row_{\mathbb{Z}}(W_{tk})}$.

Proposition 3.1.4. *Let $k \leq n$ and $l = min\{k, n-k\}$. There exist integral matrices $E_{0k}, E_{1,k}, ..., E_{l,k}$ such that E_{ik} is a $\left(\binom{n}{i} - \binom{n}{i-1}\right) \times \binom{n}{k}$ matrix, the rows of which are in $row_{\mathbb{Z}}(W_{ik})$ and such that for each $t \leq l$, the rows of $E_{0k} \cup ... \cup E_{tk}$ form a $\mathbb{Z}$-basis for $row_{\mathbb{Z}}(M_{tk})$.*

Proof. Let $E_{0k} = W_{0k}$. By induction on i, we suppose $E_{0k} \cup E_{1,k} \cup \cdots \cup E_{i,k}$ basis of $row_{\mathbb{Z}}(M_{ik})$, with $i < l$. By Proposition 2.4.13 we extend the $\mathbb{Z}$-basis $E_{0k} \cup ... \cup E_{ik}$ of $row_{\mathbb{Z}}(M_{ik})$, which has index 1 by Proposition 3.1.3, to a $\mathbb{Z}$-basis of $row_{\mathbb{Z}}(M_{i+1,k}) = row_{\mathbb{Z}}(M_{ik}) + row_{\mathbb{Z}}(W_{i+1,k})$, by adding $\binom{n}{i+1} - \binom{n}{i}$ vectors from $row_{\mathbb{Z}}(W_{i+1,k})$. By recursion we obtain the claim. □

Proposition 3.1.5. *Let $E_{0k}, E_{1,k}, ..., E_{l,k}$ be as in Proposition 3.1.4. Then, for $t \leq l$, a*

$\mathbb{Z}$-basis for $row_{\mathbb{Z}}(W_{tk})$ is provided by the rows of

$$\binom{k}{t}E_{0k} \cup \binom{k-1}{t-1}E_{1k} \cup \binom{k-2}{t-2}E_{2k} \cup \ldots \cup E_{tk}. \tag{3.6}$$

Proof. The proof is by induction on k. The case $k = 0$ is trivial. Fix $k > 0$. There is nothing to prove if $t = k$, because $W_{kk} = I$ and $row_{\mathbb{Z}}(W_{kk}) = row_{\mathbb{Z}}(M_{kk})$, (in general $row_{\mathbb{Z}}(W_{tk}) \subseteq row_{\mathbb{Z}}(M_{tk})$). The assertion reduces to Proposition 3.1.4. So we assume $t < k$. The equation 3.1 shows that the rows of $\binom{k-i}{t-i}W_{ik}$ are contained in $row_{\mathbb{Z}}(W_{tk})$. The matrix $E = \bigcup_{i=0}^{t} E_{ik}$ has index 1, because its rows form a $\mathbb{Z}$-basis for $row_{\mathbb{Z}}(M_{tk}) = Z(M_{tk})$, so $row_{\mathbb{Z}}(E) = row_{\mathbb{Z}}(M_{tk}) = Z(M_{tk}) = Z(E)$.

By Proposition 2.4.19 the rows of $\bigcup_{i=0}^{t} \binom{k-i}{t-i}E_{ik}$ span a submodule $\mathcal{M}$ of $row_{\mathbb{Z}}(M_{tk})$ of rank $\binom{n}{t}$ and index

$$N = \prod_{i=0}^{t} \binom{k-i}{t-i}^{\binom{n}{i}-\binom{n}{i-1}}. \tag{3.7}$$

In particular we observe that $\mathcal{M} \subseteq row_{\mathbb{Z}}(W_{tk})$, by Lemma 3.1.2. We will show that $row_{\mathbb{Z}}(W_{tk})$ has index N, defined by 3.7.

We have $2t \leq n$. Let $E_{0t}, E_{1t}, \ldots, E_{tt}$ be the $\left(\binom{n}{i} - \binom{n}{i-1}\right) \times \binom{n}{t}$ matrices as in Proposition 3.1.4. Define integral matrices A_{itk} for $0 \leq i \leq t$ by

$$E_{it}W_{tk} = \binom{k-i}{t-i}A_{itk}. \tag{3.8}$$

In the following we prove that

$$A = \bigcup_{i=0}^{t} A_{itk}$$

forms a $\mathbb{Z}$-basis for $row_{\mathbb{Z}}(M_{tk}(n))$ and

$$\bigcup_{i=0}^{t} \binom{k-i}{t-i}A_{itk}$$

forms a $\mathbb{Z}$-basis for $row_{\mathbb{Z}}(W_{tk})$.

Given that the rows of E_{it} are linear combinations of the rows of W_{it}, we have that the rows of $E_{it}W_{tk}$ are linear combination of the rows of $W_{it}W_{tk}$ and by equation 3.1, each A_{itk} is a matrix $\left(\binom{n}{i} - \binom{n}{i-1}\right) \times \binom{n}{k}$, whose rows are linear combinations of the rows of W_{ik}.

$W_{tt} = I$, so $row_{\mathbb{Z}}(M_{tt})$ consists of all integral vectors of lenght $\binom{n}{t}$. Moreover the union of the rows of $E_{0t}, E_{1t}, ..., E_{tt}$ forms a $\mathbb{Z}$-basis of $row_{\mathbb{Z}}(M_{tt})$. It follows that the rows of

$$\bigcup_{i=0}^{t} \binom{k-i}{t-i} A_{itk}$$

form a $\mathbb{Z}$-basis of $row_{\mathbb{Z}}(W_{tk})$. They span $row_{\mathbb{Z}}(W_{tk})$ because taken $w \in row_{\mathbb{Z}}(W_{tk})$, this vector is a linear combination of the rows of W_{tk},

$$w = h_1 w_1 + ... + h_s w_s = (h_1, ..., h_s) \begin{pmatrix} w_1 \\ w_2 \\ ... \\ w_s \end{pmatrix}$$

where $s = \binom{n}{t}$ and $w_1, ..., w_s$ are the rows of W_{tk}.

Since $(h_1, ..., h_s)$ is a vector of lenght $\binom{n}{t}$, it is a linear combination of $\bigcup_{i=0}^{t} E_{it}$. So the product $(h_1, ..., h_s) \begin{pmatrix} w_1 \\ w_2 \\ ... \\ w_s \end{pmatrix}$ is a linear combination of $\bigcup_{i=0}^{t} E_{it}W_{tk} = \bigcup_{i=0}^{t} \binom{k-i}{t-i} A_{itk}$.

Our aim is to prove that the rows of

$$A = \bigcup_{i=0}^{t} A_{itk}$$

form a $\mathbb{Z}$-basis for $row_{\mathbb{Z}}(M_{tk})$, which has index 1. Applying the Proposition 2.4.19 we conclude that $row_{\mathbb{Z}}(W_{tk})$ has index N.

For this purpose we observe that the rows of A are contained in $row_{\mathbb{Z}}(M_{tk})$, because they are integral vectors, rational linear combination of the rows of W_{tk} and M_{tk} has index 1. Now by our induction hypothesis, $row_{\mathbb{Z}}(W_{jt})$ has $\mathbb{Z}$-basis consisting of the rows of

$$\bigcup_{i=0}^{j} \binom{t-i}{j-i} E_{it}.$$

By equation 3.8 and since $\binom{k-j}{t-j} W_{jk} = W_{jt} W_{tk}$, the rows of $\binom{k-j}{t-j} W_{jk}$ are integral linear combinations of the rows of

$$\begin{aligned}(\bigcup_{i=0}^{j} \binom{t-i}{j-i} E_{it}) W_{tk} = \bigcup_{i=0}^{j} \binom{t-i}{j-i} (E_{it} W_{tk}) = \bigcup_{i=0}^{j} \binom{t-i}{j-i} \binom{k-i}{t-i} A_{itk} = \\ = \binom{k-j}{t-j} \left(\bigcup_{i=0}^{j} \binom{k-i}{j-i} A_{itk} \right).\end{aligned}$$

It follows that the rows of W_{jk} are integral linear combinations of the rows of

$$\bigcup_{i=0}^{j} \binom{k-i}{j-i} A_{itk}$$

and these are integral linear combinations of the rows of A. This prove that $row_{\mathbb{Z}}(W_{jk}) \subseteq row_{\mathbb{Z}}(A)$ and completes the proof. $\square$

Theorem 3.1.6. *Let $t \leq k \leq n-k$. Then W_{tk} has as a diagonal form the $\binom{n}{t} \times \binom{n}{k}$ matrix with diagonal entries*

$$\binom{k-i}{t-i} \text{ with multiplicity } \binom{n}{i} - \binom{n}{i-1}, \quad i = 0, 1, \dots, t.$$

Proof. The propositions 3.1.4 and 3.1.5 assert the existence of an integral matrix E, of size $\binom{n}{t} \times \binom{n}{k}$, such that the rows of which form a $\mathbb{Z}$-basis for an index 1 module $row_{\mathbb{Z}}(M_{tk})$ and, called B the diagonal matrix with $\binom{n}{i} - \binom{n}{i-1}$ occurrences of $\binom{k-i}{t-i}$ on the diagonal, the rows of BE form a $\mathbb{Z}$-basis for $row_{\mathbb{Z}}(W_{tk})$. Then the rows of W_{tk} are integral linear combinations of the rows of BE. This means that we can obtain W_{tk} from BE with row elementary operations and so $W_{tk} \sim BE$. By Proposition 2.4.19 the matrix BE has as a diagonal form the matrix B. $\square$

For simplicity, in the sequel we refer to the Theorem 3.1.6 as Wilson's Theorem.

CHAPTER 4

A diagonal form for the incidence matrix W_{tk} via linear algebra

Here we give a new proof of Wilson's Theorem seen in the previous chapter. Many of the ideas of sections 4.1 and 4.2 are based upon [4], [13] and [14]. In section 4.3 we will determine a particular basis for $\mathbb{Q}L_t^n$ related to $Sym(n)$-irreducible representations. Our reference is [10].

4.1 The Boolean lattice

We begin this chapter with a short introduction to the Boolean lattice, essential for the use we will make later. In the following R is one of $\mathbb{Q}$ or $\mathbb{R}$; Ω is the finite set $\{1, 2, \cdots, n\}$; L^n is the power set of Ω and RL^n is the vector space of formal sums of elements of L^n with coefficients in R, i.e.

$$RL^n = \left\{ \sum_{x \in L^n} r_x x \ : \ x \in L^n, r_x \in R \right\}.$$

Of course RL^n has dimension 2^n.

We give to RL^n the structure of algebra by adding a multiplication operation. For $x, y \in L^n$ we define a product in the following way:

$$x \cdot y = x \cup y \tag{4.1}$$

and extend this linearly to RL^n. If $f = \sum\limits_{x \in L^n} f_x x$ and $h = \sum\limits_{y \in L^n} f_y y$, we put

$$f \cdot h = \sum_{x,y \in L^n} f_x h_y x \cdot y.$$

This means that a i-set is a product of its i elements, so we can write $\alpha_1 \cdots \alpha_i$ instead of $\{\alpha_1, \cdots, \alpha_i\}$. Note that the union of sets induces an associative product on RL^n.

Definition 4.1.1. *We call $f = \sum f_x x$ and $h = \sum f_y y$ disjoint from each other provided that for all $x, y \in L^n$, with $x \cap y \neq \emptyset$, we have $f_x = 0$ or $h_y = 0$.*

On RL^n we define the standard inner product $\langle \, ; \, \rangle$ by setting

$$\langle x; y \rangle = 1 \text{ if } x = y \text{ and } \langle x; y \rangle = 0 \text{ otherwise},$$

for all $x, y \in L^n$. We extend this into RL^n linearly in both arguments. Note that this product is positive-definite and bilinear by construction. It also transforms the basis L^n of RL^n into an orthonormal basis. So if

$$f = \sum_{y \in L^n} f_y y \in RL^n,$$

with $f_y \in R$, we get

$$\langle f; x \rangle = \langle \sum_{y \in L^n} f_y y; x \rangle = \sum_{y \in L^n} f_y \langle y; x \rangle = f_x \langle x; x \rangle = f_x.$$

With an inner product we get a natural norm on RL^n, defined to be

$$\|f\|^2 = \langle f; f \rangle.$$

As we said, L^n is an orthonormal basis of RL^n since for any $x \in L^n$ we have

$$\|x\| = \sqrt{\langle x; x \rangle} = 1.$$

Example 4.1.2. *If* $f = -3\{1,2\} + \{1,3,5\}$ *and* $h = 4\{1,3\} + \{1,2,4\}$*, then*

$$f \cdot h = -12\{1,2,3\} - 3\{1,2,4\} + 4\{1,3,5\} + \{1,2,3,4,5\}$$

and

$$\langle f; \{1,2\} \rangle = -3.$$

Now we encode the partial order $\subseteq$ of the Boolean lattice $(L^n, \subseteq)$ into the algebra RL^n in an algebraic way. To this end we introduce the maps $\epsilon^{(n)} : RL^n \to RL^n$ and $\partial^{(n)} : RL^n \to RL^n$ defined on basis elements $x, y \in L^n$ by

$$\epsilon^{(n)}(x) = \begin{cases} \sum\limits_{\substack{y \supseteq x \\ |y|=|x|+1}} y & \text{if } |x| < n \\ 0 & \text{otherwise} \end{cases} \qquad \text{and} \qquad \partial^{(n)}(y) = \begin{cases} \sum\limits_{\substack{x \subseteq y \\ |x|=|y|-1}} x & \text{if } |y| > 0 \\ 0 & \text{otherwise} \end{cases}$$

and extended linearly. This means that $\langle \epsilon^{(n)}(x); y \rangle = 1$ if and only if $|y| = |x| + 1$ and $y \supseteq x$. Moreover, $\langle x; \partial^{(n)}(y) \rangle = 1$ if and only if $|x| = |y| - 1$ and $x \subseteq y$.

We observe that $\epsilon^{(n)}(\Omega) = 0$ since Ω is the maximal element of L^n. The same is true for $\partial^{(n)}(\emptyset)$.

Proposition 4.1.3. *If $f_1, f_2 \in RL^n$ then $\langle \epsilon^{(n)}(f_1); f_2 \rangle = \langle f_1; \partial^{(n)}(f_2) \rangle$. In particular $\epsilon^{(n)}$ and $\partial^{(n)}$ are adjoints of each other.*

Proof. Since $\langle\, ; \,\rangle$ is linear in the first and second variables, it is enough to prove this for $x, y \in L^n$. Note that

$$\langle \epsilon^{(n)}(x); y \rangle = \begin{cases} 1 & \text{if } |y| = |x| + 1 \text{ and } x \subseteq y \\ 0 & \text{otherwise} \end{cases}.$$

However, this is the same when we look at $\partial^{(n)}$:

$$\langle x; \partial^{(n)}(y) \rangle = \begin{cases} 1 & \text{if } |x| = |y| - 1 \text{ and } x \subseteq y \\ 0 & \text{otherwise} \end{cases}.$$

□

As we know, $L^n = \cup_{i=0}^{n} L_i^n$. The space RL^n splits naturally into a direct sum

$$RL^n = RL_0^n \oplus RL_1^n \oplus \cdots \oplus RL_n^n,$$

where RL_i^n is the subspace with basis the i-sets of L^n.

We can restrict $\epsilon^{(n)}$ and $\partial^{(n)}$-maps:

$$\epsilon_t^{(n)t+1} : RL_t^n \to RL_{t+1}^n \qquad \partial_{t+1}^{(n)t} : RL_{t+1}^n \to RL_t^n.$$

In the following, unless necessary, we write ϵ, ∂, ϵ_t^{t+1} and ∂_{t+1}^t instead $\epsilon^{(n)}$, $\partial^{(n)}$, $\epsilon_t^{(n)t+1}$ and $\partial_{t+1}^{(n)t}$.

Note that if we compose ϵ_t^{t+1} with ∂_{t+1}^t we obtain a vector space endomorphism of RL_t^n, denoted by

$$\nu_t^+ := \partial_{t+1}^t \epsilon_t^{t+1}.$$

ν_t^+ is non-zero only if $0 \le t \le n-1$. Observe that ν_t^+ is the restriction of the linear map $\nu^+ = \partial\epsilon$ to RL_t^n. Similarly, we define the restriction

$$\nu_t^- := \epsilon_{t-1}^t \, \partial_t^{t-1}$$

of $\nu^- = \epsilon\partial$. This is non-zero only if $1 \le t \le n$.

By Proposition 4.1.3 we know that ϵ and ∂ are adjoints of each other and so

$$\langle \nu^+(f_1); f_2 \rangle = \langle \epsilon(f_1); \epsilon(f_2) \rangle = \langle f_1; \nu^+(f_2) \rangle. \tag{4.2}$$

Hence ν^+ is symmetric. Similarly for ν^-.

A basic property of the maps ν^+ and ν^- is given by next Lemma.

Lemma 4.1.4. *Let $0 \le t \le n$ and let id_t be the identity map on RL_t^n. Then*

$$\nu_t^+ - \nu_t^- = (n-2t) id_t.$$

Proof. The statement is true for $t = 0$. We assume $t \neq 0$. Since ν_t^+ and ν_t^- are linear it is enough to prove this for basis elements.

Since ϵ_t^{t+1} and ∂_{t+1}^t are adjoints of each other, for any $x, y \in L_t^n$, we have that

$$\langle \nu_t^+(x); y \rangle = \langle \partial_{t+1}^t \epsilon_t^{t+1}(x); y \rangle = \langle \epsilon_t^{t+1}(x); \epsilon_t^{t+1}(y) \rangle$$

is the number of $z \in L_{t+1}^n$ containing both x and y. Thus

$$\langle \nu_t^+(x); y \rangle = \begin{cases} n-t & \text{if} \quad x = y \\ 1 & \text{if} \quad x \cap y \in L_{t-1}^n \\ 0 & \quad \text{otherwise} \end{cases}.$$

Similarly, $\langle \nu_t^-(x); y\rangle = \langle \epsilon_{t-1}^t \partial_t^{t-1}(x); y\rangle = \langle \partial_t^{t-1}(x); \partial_t^{t-1}(y)\rangle$ is the number of all $z \in L_{t-1}^n$ contained in both x and y. Thus

$$\langle \nu_t^-(x); y\rangle = \begin{cases} t & \text{if} \quad x = y \\ 1 & \text{if} \quad x \cap y \in L_{t-1}^n \\ 0 & \quad \text{otherwise} \end{cases}.$$

We get

$$\langle (\nu_t^+ - \nu_t^-)(x); y\rangle = \begin{cases} n - 2t & \text{if} \quad x = y \\ 0 & \quad \text{otherwise} \end{cases}.$$

The claim follows remembering that

$$(\nu_t^+ - \nu_t^-)(x) = \sum_{y \in L_t^n} \langle (\nu_t^+ - \nu_t^-)(x); y\rangle y.$$

□

We conclude this section with some notion about the action of $Sym(n)$ on RL^n.

The natural action of $Sym(n)$ on Ω induces an action on L_i^n: for $g \in Sym(n)$ and $x = \{\alpha_1, \cdots, \alpha_i\} \in L_i^n$ we have

$$\{\alpha_1, \cdots, \alpha_i\}^g = \{\alpha_1^g, \cdots, \alpha_i^g\}.$$

RL_i^n becomes a $RSym(n)$-space, if we think to L_i^n as a basis of RL_i^n.

Moreover it is easy to prove the following Lemmas

Lemma 4.1.5. *If $f_1, f_2 \in RL^n$ and $g \in Sym(n)$ then $\langle f_1; f_2\rangle = \langle f_1^g; f_2^g\rangle$.*

Lemma 4.1.6. *Let $f_1, f_2 \in RL^n$ and $g \in Sym(n)$ then $(f_1 \cdot f_2)^g = f_1^g \cdot f_2^g$.*

It follows that the action of $Sym(n)$ on RL^n commutes with the maps ϵ and ∂ we have introduced.

Lemma 4.1.7. *The action of $Sym(n)$ on RL^n commutes with the ϵ and ∂-functions. In particular, for $f \in RL^n$ we have*

$$\epsilon(f)^g = \epsilon(f^g) \qquad \textit{and} \qquad \partial(f)^g = \partial(f^g).$$

Proof. Since ϵ and ∂ are linear, it is enough to show the equality for basis elements. So let $x \in L^n_t$, then

$$\epsilon_t^{t+1}(x)^g = \left(\sum_{y \in L^n_{t+1}} \langle \epsilon_t^{t+1}(x); y \rangle y \right)^g = \sum_{y \in L^n_{t+1}} \langle \epsilon_t^{t+1}(x); y \rangle y^g,$$

and

$$\epsilon_t^{t+1}(x^g) = \sum_{y \in L^n_{t+1}} \langle \epsilon_t^{t+1}(x^g); y \rangle y \,.$$

For $z \in L^n_{t+1}$, $\langle \epsilon_t^{t+1}(x); z \rangle = 1$ if and only if $\langle \epsilon_t^{t+1}(x^g); z^g \rangle = 1$, since $x \subseteq z$ implies $x^g \subseteq z^g$ and conversely. So, in the first equation z^g has coefficient 1 if and only if the coefficient of z^g in the second equation is 1. This argument works in reverse, proving equality. Similarly we prove $\partial(f)^g = \partial(f^g)$. □

Lemma 4.1.7 tells us that the $Sym(n)$-action also commutes with

$$\nu^+ = \partial \epsilon \text{ and } \nu^- = \epsilon \partial.$$

4.2 Eigenspace decomposition

Our aim is to split RL^n_t into a direct sum of irreducible $Sym(n)$-invariant spaces. We will do this using the symmetric map ν^+_t. Next Lemma allows us to relate eigenspaces and eigenvalues of ν^+_t and ν^-_t to each other.

Lemma 4.2.1. *Let A and B be vector spaces and let $\alpha : A \longrightarrow B$ and $\beta : B \longrightarrow A$ be linear maps. Then $\beta\alpha : A \longrightarrow A$ and $\alpha\beta : B \longrightarrow B$ have the same non-zero eigenvalues. Furthermore, if λ is a non-zero eigenvalue with eigenspaces $A_\lambda \subseteq A$ and $B_\lambda \subseteq B$ for $\beta\alpha$ and $\alpha\beta$ respectively, then α and β restrict to isomorphisms $\alpha : A_\lambda \longrightarrow B_\lambda$ and $\beta : B_\lambda \longrightarrow A_\lambda$.*

Proof. In order to prove that $\beta\alpha$ and $\alpha\beta$ have the same non-zero eigenvalues, we consider an eigenvalue $\lambda \neq 0$ of $\alpha\beta$. Then we have some $w \in B$ such that $\alpha\beta(w) = \lambda w$. Applying β to both sides, we get

$$\beta\alpha(\beta(w)) = \lambda(\beta(w),$$

so λ is also an eigenvalue of $\beta\alpha$. Now we consider the map $\alpha : A_\lambda \longrightarrow B_\lambda$ and suppose that $\alpha(v) = \alpha(w)$ for $v, w \in A_\lambda$. Applying β we have $\beta\alpha(v) = \beta\alpha(w)$, whence $\lambda v = \lambda w$. It follows that α is injective from A_λ to B_λ. Now we prove that it is surjective. For this purpose, let $w \in B_\lambda$, so $\frac{1}{\lambda}\beta(w) \in A_\lambda$ and $\alpha\left(\frac{1}{\lambda}\beta(w)\right) = w$. The claim follows. A similar argument shows that β is an isomorphism from B_λ to A_λ. $\square$

In particular we may take $A = RL_t^n$, $B = RL_{t+1}^n$, $\alpha = \epsilon_t^{t+1}$ and $\beta = \partial_{t+1}^t$. Above Lemma implies that ϵ_t^{t+1} and ∂_{t+1}^t restrict to isomorphisms between non-zero eigenspaces of ν_t^+ and ν_{t+1}^-, and any eigenvector for ν_{t+1}^- with eigenvalue $\lambda \neq 0$ is also an eigenvector for ν_{t+1}^+ with eigenvalue $\lambda + n - 2t - 2$, by Lemma 4.1.4.

In the following Theorem using Lemma 4.1.4 we get the eigenvalues ν_t^+ and ν_t^-.

Theorem 4.2.2. *Suppose that $2t \leq n$. Then ν_t^- has $t+1$ eigenvalues*

$$\lambda_{t-1,0} > \lambda_{t-1,1} > \cdots > \lambda_{t-1,t-1} > \lambda_{t-1,t} = 0$$

and ν_t^+ has $t+1$ eigenvalues

$$\lambda_{t,0} > \lambda_{t,1} > \cdots > \lambda_{t,t-1} > \lambda_{t,t} \geq 0,$$

with multiplicity $n_i = \binom{n}{i} - \binom{n}{i-1}$, *for* $0 \leq i \leq t$. *In particular we have the decomposition*

$$RL_t^n = E_{t,0}^n \oplus E_{t,1}^n \oplus \cdots \oplus E_{t,t}^n \tag{4.3}$$

where $E_{t,i}^n$ *is the* v_t^+*-eigenspace with eigenvalue* $\lambda_{t,i}$ *and* $dim_R\, E_{t,i}^n = n_i$.

Proof. Clearly $\binom{n}{t} > \binom{n}{t-1}$ and $n - 2t \geq 0$. If $t = 0$, then v_0^- has only one zero eigenvalue. Now let $t > 0$ and by induction hypothesis, for $0 \leq i \leq t-1$, let $\lambda_{t-2,i}$ be non-negative eigenvalues of v_{t-1}^-, with multiplicity n_i. Thus there exist non-zero eigenvectors $w_i \in RL_{t-1}^n$ such that $v_{t-1}^-(w_i) = \lambda_{t-2,i} w_i$ and by Lemma 4.1.4

$$v_{t-1}^+(w_i) = v_{t-1}^-(w_i) + (n-2t+2)w_i = [\lambda_{t-2,i} + (n-2t+2)]w_i.$$

Called $\lambda_{t-1,i} = \lambda_{t-2,i} + (n-2t+2)$, it is clear that $\lambda_{t-1,i}$ are positive eigenvalues of v_{t-1}^+, with $i = 0, \cdots, t-1$. By Lemma 4.2.1 v_{t-1}^+ and v_t^- have the same non-zero eigenvalues, we deduce that they are

$$\lambda_{t-1,0} > \lambda_{t-1,1} > \cdots > \lambda_{t-1,t-1}.$$

Since $dim\, RL_t^n > dim\, RL_{t-1}^n$, it follows that there exists a zero eigenvalue $\lambda_{t-1,t}$ of v_t^-, with multiplicity $\binom{n}{t} - \binom{n}{t-1}$.

Applying again Lemma 4.1.4, we obtain the eigenvalues of v_t^+:

$$\lambda_{t,0} > \lambda_{t,1} > \cdots > \lambda_{t,t-1} > \lambda_{t,t} \geq 0,$$

where

$$\lambda_{t,i} := \lambda_{t-1,i} + (n-2t) > 0,$$

with $0 \leq i \leq t-1$, and $\lambda_{t,t} = 0 + n - 2t \geq 0$. From $v_t^+ = v_t^- + (n-2t)id_t$ follows that v_t^+ and v_t^- have the same eigenspaces. So $\lambda_{t,i}$ has multiplicity n_i, for $0 \leq i \leq t$. □

Theorem 4.2.3. *If $2t > n$ and $0 < t \leq n$, then ν_t^- has $n - t + 1$ positive eigenvalues. In particular we have the decomposition*

$$RL_t^n = E_{t,0}^n \oplus E_{t,1}^n \oplus \cdots \oplus E_{t,n-t-1}^n \oplus E_{t,n-t}^n. \tag{4.4}$$

Proof. We prove the Theorem for induction on $n-t$. Let $n-t = 0$, so $\nu_n^- : RL_n^n \longrightarrow RL_n^n$ is defined by $\nu_n^-(\Omega) = n\Omega$. The claim follows. Now we take $n - t > 0$ and we suppose that the statement is true for $n-t-1 \geq 0$, i.e. for $t+1 \leq n$. So $\nu_{t+1}^- = \epsilon_t^{t+1}\partial_{t+1}^t : RL_{t+1}^n \longrightarrow RL_{t+1}^n$ has eigenvalues

$$\lambda_{t,0} > \lambda_{t,1} > \cdots > \lambda_{t,n-t-1} > 0,$$

with multiplicity $n_i = \binom{n}{i} - \binom{n}{i-1}$, for $i = 0, \cdots, n - t - 1$. By Lemma 4.2.1, ν_{t+1}^- and ν_t^+ have the same non-zero eigenvalues. Since $dim\, RL_t^n > dim\, RL_{t+1}^n$, we have that ν_t^+ has an eigenvalue $\lambda_{t,n-t} = 0$ with multiplicity $\binom{n}{t} - \binom{n}{t+1} = \binom{n}{n-t} - \binom{n}{n-t-1}$.

For any $\lambda_{t,i}$ there exists a non-zero eigenvector w_i such that $\nu_t^+(w_i) = \lambda_{t,i}w_i$. So, by Lemma 4.1.4,

$$\nu_t^-(w_i) = \nu_t^+(w_i) - (n - 2t)w_i = (\lambda_{t,i} - n + 2t)w_i.$$

Put $\lambda_{t-1,i} = \lambda_{t,i} - n + 2t$, for $i = 0, \cdots, n - t$, we have $\lambda_{t-1,i} > 0$ with multiplicity n_i. Called $E_{t,i}^n$ the eigenspaces associated to $\lambda_{t,i}$, for any $i = 0, \cdots, n - t$, we have that $dim\, E_{t,i}^n = n_i$ and $RL_t^n = E_{t,0}^n \oplus E_{t,1}^n \oplus \cdots \oplus E_{t,n-t-1}^n \oplus E_{t,n-t}^n$. □

The decompositions 4.3 and 4.4 give the scheme in Table 4.1.

In the sequel we use the following notation: $t' = min\{t, n - t\}$.

Remark 4.2.4. *We note that $\epsilon_t^{t+1}(E_{t,i}^n) = 0$ if and only if $i = t'$ and $t \geq n/2$, while $\partial_t^{t-1}(E_{t,i}^n) = 0$ if and only if $i = t'$ and $t \leq n/2$. Except this cases, by Lemma 4.2.1 and Theorems 4.2.2 and 4.2.3, the maps ϵ_t^{t+1} and ∂_{t+1}^t restrict to isomorphisms*

$$\epsilon_t^{t+1} : E_{t,j}^n \longrightarrow E_{t+1,j}^n, \qquad \partial_{t+1}^t : E_{t+1,j}^n \longrightarrow E_{t,j}^n$$

$$\begin{array}{lcccccccccc}
RL^n_n & = & E^n_{n,0} & & & & & & & & \\
 & & \wr\| & & & & & & & & \\
RL^n_{n-1} & = & E^n_{n-1,0} & \oplus & E^n_{n-1,1} & & & & & & \\
 & & \wr\| & & \wr\| & & & & & & \\
\vdots & = & \vdots & & \vdots & & \cdots & & \ddots & & \\
 & & \wr\| & & \wr\| & & & & & & \\
RL^n_t & = & E^n_{t,0} & \oplus & E^n_{t,1} & \oplus & \cdots & \oplus & E^n_{t,t-1} & \oplus & E^n_{t,t} \\
 & & \wr\| & & \wr\| & & & & \wr\| & & \\
RL^n_{t-1} & = & E^n_{t-1,0} & \oplus & E^n_{t-1,1} & \oplus & \cdots & \oplus & E^n_{t-1,t-1} & & \\
 & & \wr\| & & \wr\| & & & & & & \\
\vdots & = & \vdots & & \vdots & & \cdots & & \iddots & & \\
 & & \wr\| & & \wr\| & & & & & & \\
RL^n_1 & = & E^n_{1,0} & \oplus & E^n_{1,1} & & & & & & \\
 & & \wr\| & & & & & & & & \\
RL^n_0 & = & E^n_{0,0} & & & & & & & &
\end{array}$$

Table 4.1: Eigenspace Decomposition

for $0 \leq j \leq t'$. In other words, all modules in the same column of Table 4.1 are isomorphic to each other via powers of ϵ_t^{t+1} or ∂_{t+1}^t. In particular,

$$E^n_{0,0}, E^n_{1,0}, E_{2,0}, \cdots, E^n_{n,0}$$

have dimension 1, while

$$E^n_{1,1}, E^n_{2,1}, E^n_{3,1}, \cdots, E^n_{n-1,1}$$

have dimension $\binom{n}{1} - \binom{n}{0}$, and so on.

In the sequel if there is not confusion, we write $E_{t,i}$ instead $E^n_{t,i}$.

Corollary 4.2.5. *Let $0 \leq t \leq n$ and let $\mathbb{Q} \subseteq R$ be a field. Then the eigenvalues of $\nu_t^+ : RL_t^n \to RL_t^n$ are*

$$\lambda_{t,i} = (t-i+1)(n-t-i) \geq 0 \text{ with multiplicity } \binom{n}{i} - \binom{n}{i-1},$$

for $i = 0, \cdots, t'$.

Proof. Applying induction on t and using Lemma 4.1.4, Theorems 4.2.2 and 4.2.3, we have

$\lambda_{t,i} = \sum_{i \leq j \leq t} (n-2j) = (t-i+1)n - 2(i + \cdots + t) = (t-i+1)n - 2\left(\frac{t(t+1)}{2} - \frac{i(i-1)}{2}\right) = (t-i+1)(n-t-i)$, with multiplicity $\binom{n}{i} - \binom{n}{i-1}$. □

In the following we will assume $R = \mathbb{Q}$ as the eigenvalues of ν_t^+ are rational numbers.

Corollary 4.2.6. *For each $0 \leq t \leq n$ and $0 \leq i \leq t'$, the eigenspaces $E_{t,i}$ are $Sym(n)$-invariant.*

Proof. Let $f \in E_{t,i}$ for some $0 \leq i \leq t' \leq n$ and let $g \in Sym(n)$. Then

$$\nu^+(f^g) = (\nu^+(f))^g = \lambda_{t,i} f^g.$$

This means that f^g is an eigenvector of ν^+ with eigenvalue $\lambda_{t,i}$ and so $f^g \in E_{t,i}$. Hence the $E_{t,i}$ are $Sym(n)$-invariant. □

Theorem 4.2.7. *Each of the $E_{t,i}$, for $0 \leq i \leq t'$, is $\mathbb{Q}Sym(n)$-irreducible.*

Proof. Take $x \in L_t^n$. Then the stabilizer in $Sym(n)$ of x has $t'+1$ orbits on L_t^n, corresponding to the possible intersection cardinalities of $y \cap x$ for $y \in L_t^n$. In other words, $Sym(n)$ has permutation rank $t'+1$ on L_t^n. Therefore $\mathbb{Q}L_t^n$ decomposes into at most $t' + 1$ irreducibles. Since the decomposition of $\mathbb{Q}L_t^n$ already has $t' + 1$ summands which are $Sym(n)$-invariant it follows that each of the summands is irreducible. The dimension of $E_{t,i}$ is the multiplicity $\binom{n}{i} - \binom{n}{i-1}$ of $\lambda_{t,i}$ and as these are pairwise distinct for $i = 0, \cdots, t'$ the $E_{t,i}$ are pairwise non-isomorphic. □

Theorem 4.2.8. *Let $0 \leq t < k \leq n$, with $t + k \leq n$. Then we have*

$$\mathbb{Q}L_k^n = E_{k0} \oplus E_{k1} \oplus \cdots \oplus E_{kt} \oplus K$$

$$\mathbb{Q}L_t^n = E_{t0} \oplus E_{t1} \oplus \cdots \oplus E_{tt} \tag{4.5}$$

where

$$K = E_{k,t+1} \oplus \cdots \oplus E_{k,k'}$$

is the kernel of $\partial_{t+1}^t \cdots \partial_k^{k-1} : \mathbb{Q}L_k^n \to \mathbb{Q}L_t^n$. Furthermore, $E_{k,i} \cong E_{t,i}$ for $0 \leq i \leq t$. We have $E_{k,i} \cong E_{t,j}$ if and only if $i = j$ and furthermore $dim_{\mathbb{Q}}(E_{k,i}) = n_i = \binom{n}{i} - \binom{n}{i-1}$.

Proof. We consider the maps $\epsilon_t^k : \mathbb{Q}L_t^n \to \mathbb{Q}L_k^n$ defined by

$$\epsilon_t^k(x) := \sum_{y \supseteq x} y, \text{ with } y \in L_k^n$$

for $x \in L_t^n$ and $\partial_k^t : \mathbb{Q}L_k^n \to \mathbb{Q}L_t^n$ defined by

$$\partial_k^t(y) := \sum_{x \subseteq y} x, \text{ with } x \in L_t^n$$

for $y \in L_k^n$. These maps can be expressed as powers of ϵ and ∂. Let $d = k - t$. Then there are (d!) distinct chains $x = x_0 \subset x_1 \subset \cdots \subset x_d = y$ of subsets of Ω for any y appearing in $\epsilon_t^k(x)$. Therefore

$$\epsilon_t^k = (d!)^{-1} \epsilon_{k-1}^k \epsilon_{k-2}^{k-1} \cdots \epsilon_t^{t+1} \tag{4.6}$$

and similarly

$$\partial_k^t = (d!)^{-1} \partial_{t+1}^t \partial_{t+2}^{t+1} \cdots \partial_k^{k-1}. \tag{4.7}$$

Let $E_{t,i}$ and $E_{k,i}$ be the eigenspaces in 4.3 and 4.4. Since $0 \leq t < k \leq n$ and $t + k \leq n$ we have $t = min\{t, n-t\} \leq min\{k, n-k\}$. From 4.6 and 4.7 it follows that ϵ_t^k restricts to an injective map $E_{t,i} \longrightarrow E_{k,i}$ and that ∂_k^t restricts to a surjective map $E_{k,i} \longrightarrow E_{t,i}$ for each $i = 0, \cdots, t$. The eigenvalues of $\partial_k^t \epsilon_t^k$ can be computed from 4.6 and 4.7 using Corollary 4.2.5. □

This decomposition is called *the spectral decomposition of the incidence structure* $\mathcal{I}_{tk}^n = (L_t^n, L_k^n; \subseteq)$.

4.3 Polytopes

Now the next thing to do is to give to $\mathbb{Q}L_t^n$ a generating set of eigenvectors. To this end, drawing from [4] we introduce the so-called polytopes.

In the sequel, we will consider the natural order in Ω.

Definition 4.3.1. *Let $0 \leq t \leq n$, $0 \leq i \leq t'$ and $j = t - i$. If $\alpha_1, \cdots, \alpha_i, \beta_1, \cdots, \beta_i$ are pairwise distinct elements of Ω and $\gamma_1, \cdots, \gamma_u$ the collection of all j-subsets of $\Omega \setminus \{\alpha_1, \cdots, \alpha_i, \beta_1, \cdots, \beta_i\}$, then we define a polytope of type (t, i), with head*

$$(\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)$$

and tail

$$(\gamma_1 + \cdots + \gamma_u)$$

to be the element

$$s_{t,i} := [\alpha_1, \cdots, \alpha_i; \beta_1, \cdots, \beta_i]_j = (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)(\gamma_1 + \cdots + \gamma_u) \in \mathbb{Q}L_t^n.$$

Denote the set of all polytopes of type (t, i) by $S_{t,i}^n$ and $S_t^n = S_{t,0}^n \cup \cdots \cup S_{t,t'}^n$.

Example 4.3.2. *If $n = 6$ and $t = 2$, then the element*

$$s_{2,1} = (\{1\} - \{2\}) (\{3\} + \{4\} + \{5\} + \{6\})$$

is a polytope of type $(2, 1)$. Now we write explicitly $s_{2,1}$ as

$$\{1, 3\} + \{1, 4\} + \{1, 5\} + \{1, 6\} - \{2, 3\} - \{2, 4\} - \{2, 5\} - \{2, 6\}. \qquad (4.8)$$

For every set x that appears in 4.8 we say that x occurs in the expansion of the polytope. For example the set $\{2, 3\}$ occurs in the expansion of $s_{2,1}$ with coefficient -1.

Remark 4.3.3. *The group $Sym(n)$ acts on S^n_t with orbits $S^n_{t,i}$.*

For convenience put $s_{t,i} = 0$ if $s_{t,i}$ is undefined, for instance if $t < 0$, $n < t$, $t' < i$ or $n < 2i$.

We define two maps which arise for polytopes.

Definition 4.3.4. *For $0 \leq t \leq n$ and $0 \leq i \leq t'$, we define the tail-extension*

$$+ : S^n_{t,i} \rightarrow S^n_{t+1,i}$$

by

$$s_{t,i} = [\alpha_1, \cdots, \alpha_i; \beta_1, \cdots, \beta_i]_j \rightarrow s^+_{t,i} = [\alpha_1, \cdots, \alpha_i; \beta_1, \cdots, \beta_i]_{j+1}.$$

Similarly, the tail-cutting map

$$- : S^n_{t,i} \rightarrow S^n_{t-1,i}$$

by

$$s_{t,i} = [\alpha_1, \cdots, \alpha_i; \beta_1, \cdots, \beta_i]_j \rightarrow s^-_{t,i} = [\alpha_1, \cdots, \alpha_i; \beta_1, \cdots, \beta_i]_{j-1}.$$

Remark 4.3.5. *Note that $s^+_{t,i} = 0$ when $t \geq \frac{n}{2}$ and $i = t'$, and that $s^-_{t,i} = 0$ when $t \leq \frac{n}{2}$ and $i = t'$. Apart from these cases the tail-extension and tail-cutting are functions which are inverse to each other.*

We remember the Leibniz Rule that will be used in 4.3.7.

Lemma 4.3.6. *(Leibniz Rule) If f, h in $\mathbb{Q}L^n$ are disjoint then $\partial(f \cdot h) = \partial(f) \cdot h + f \cdot \partial(h)$.*

Proof. It is enough to consider the case when $f = x$ and $h = y$ are subsets of Ω. In this case it is obvious and the remainder follows by linearity. □

Lemma 4.3.7. *Let $0 \leq t \leq n$ and $0 \leq i \leq t'$. Then*

(a) $\partial(s_{t,i}) = (n - t - i + 1)s^{-}_{t,i}$;

(b) $s_{t,i} \in E_{t,i}$.

Proof. (a) Note that $\partial(\alpha - \beta) = \emptyset - \emptyset = 0$ and hence by Lemma 4.3.6 we have

(a.1) $\partial((\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)) = 0$,

(a.2) Let $s_{t,i} = (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)(\gamma_1 + \cdots + \gamma_u)$. Then

$$\partial\left((\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)(\gamma_1 + \cdots + \gamma_u)\right) = \partial\left((\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)\right)$$
$$(\gamma_1 + \cdots + \gamma_u) + (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)\partial(\gamma_1 + \cdots + \gamma_u) =$$
$$= (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)\partial(\gamma_1 + \cdots + \gamma_u).$$

Clearly, $\partial(\gamma_1 + \cdots + \gamma_u)$ is equal to a constant δ times the sum of all $(t - i - 1)$-subsets of $\Omega \setminus \{\alpha_1, \cdots, \alpha_i, \beta_1, \cdots, \beta_i\}$. Therefore $\delta = (n - t - i + 1)$.

(b) Let $i = t = t'$ and consider a polytope $s_{i,i} = (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)$ of type (i, i). We prove that $s_{i,i} \in E_{i,i}$. By Lemma 4.3.6 we have $\partial(s_{i,i}) = 0$. So $s_{i,i} \in Ker\,(\partial) = E_{i,i}$, by Theorem 4.2.8.

In general, let $s_{t,i} = (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)(\gamma_1 + \cdots + \gamma_u)$ be a polytope of type (t, i). By part (a), applying $(t - i)$-times the map ∂, we get

$$\partial^{t-i}(s_{t,i}) = c(\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i),$$

for some $c \in \mathbb{Q}$. On the other hand if $s_{n-i,i}$ is the polytope of type $(n-i, i)$ with head $(\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)$, for some $a, b \in \mathbb{Q}$ we have

$$\partial^{n-i-t}(s_{n-i,i}) = a s_{t,i}, \tag{4.9}$$

and

$$\partial^{n-2i}(s_{n-i,i}) = b(\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i). \tag{4.10}$$

Since ∂^{n-2i} is an isomorphism between $\mathbb{Q}L^n_{n-i}$ and $\mathbb{Q}L^n_i$ (see table 4.1), which restricts to an isomorphism between $E_{n-i,i}$ and $E_{i,i}$, we have that $s_{n-i,i} \in E_{n-i,i}$, by equation 4.10. Using equation 4.9 we conclude that $s_{t,i} \in E_{t,i}$, as ∂^{n-i-t} is an isomorphism from $E_{n-i,i}$ to $E_{t,i}$.

□

Theorem 4.3.8. *Let* $0 \leq t \leq n$ *and* $0 \leq i \leq t'$. *Then the polytopes of type* (t, i) *span* $E_{t,i}$ *as a vector space.*

Proof. We prove the statement distinguishing two cases

Case 1 $i = t = t'$. Fix a polytope $s_{i,i}$ in $E_{i,i}$ and consider the space

$$span_{\mathbb{Q}}\{s^g_{i,i} \ : \ g \in Sym(n)\}.$$

This is a subspace of $E_{i,i}$ and by construction it is $Sym(n)$-invariant. Since $E_{i,i}$ is irreducible, by Theorem 4.2.7, $E_{i,i} = span_{\mathbb{Q}}\{s^g_{i,i} \ : \ g \in Sym(n)\}$. So the set of all polytopes of type (i, i) is a generating set of $E_{i\,i}$, for $0 \leq i \leq \frac{n}{2}$.

Case 2 Now, let $s_{t,i}$ be a polytope of type (t, i). By Lemma 4.3.7, $s_{t,i} \in E_{t,i}$. Since the power of ∂ is an isomorphism between $E_{t,i}$ and $E_{i,i}$, by Case 1 and part (a) of Lemma 4.3.7, we have that the set of all polytopes of type (t, i) is a spanning set of $E_{t,i}$.

$\square$

Corollary 4.3.9. *Let* $0 \leq t \leq n$ *and* $0 \leq i \leq t'$. *Then*

$$\epsilon(s_{t,i}) = (t+1-i)s^+_{t,i}.$$

Proof. If $i < n-t$, as $s_{t,i} \in E_{t,i}$, by Corollary 4.2.5 we have

$$\partial\epsilon(s_{t,i}) = \nu^+_t(s_{t,i}) = (t+1-i)(n-t-i)s_{t,i}.$$

Using Lemma 4.3.7 applied to $s^+_{t,i}$, we get $\partial\epsilon(s_{t,i}) = (t+1-i)(n-t-i)s_{t,i} = (t+1-i)\partial(s^+_{t,i})$. Since ∂ is an isomorphism between $E_{t+1,i}$ and $E_{t,i}$, we deduce that

$$\epsilon(s_{t,i}) = (t+1-i)s^+_{t,i}.$$

If $i = n-t$ then $\epsilon(s_{t,i}) = 0$, since $\epsilon(E_{t,n-t}) = 0$, by remark 4.2.4. $\square$

Obviously we have

Corollary 4.3.10. *The tail-extension and tail-cutting maps extend to* $\mathbb{Q}Sym(n)$*-isomorphisms*

$$+ : E_{t,i} \longrightarrow E_{t+1,i} \qquad \textit{and} \qquad - : E_{t,i} \longrightarrow E_{t-1,i},$$

for $0 \leq t \leq n$ *and* $0 \leq i \leq t'$, *except the particular cases seen in remark 4.3.5.*

Proof. From Lemma 4.2.1 we have that the maps

$$\epsilon^{t+1}_t : E_{t,i} \longrightarrow E_{t+1,i} \qquad \text{and} \qquad \partial^t_{t+1} : E_{t+1,i} \longrightarrow E_{t,i}$$

are isomorphisms. Applying Lemmas 4.3.7 and 4.3.9 we get the claim. $\square$

Notation 4.3.11. *Put* $d = k-t$, *we denote by* $s^{+d}_{t,i}$ *the polytope obtained from* $s_{t,i}$ *by* d*-fold tail-extension. Similarly* $s^{-d}_{k,i}$ *is the polytope obtained from* $s_{k,i}$ *by* d*-fold tail-cutting,*

Remark 4.3.12. *Let $0 \leq t < k \leq n$, with $t + k \leq n$, and $d = k - t$. Using repeatedly Lemma 4.3.9 we have*

$$(\epsilon_{k-1}^{k}\epsilon_{k-2}^{k-1}\cdots\epsilon_{t}^{t+1})(s_{t,i}) = (k-i)(k-i-1)\cdots(t-i+1)s_{t,i}^{+d}$$

Since $(k-t)!\epsilon_t^k = (\epsilon_{k-1}^{k}\epsilon_{k-2}^{k-1}\cdots\epsilon_{t}^{t+1})$ we have

$$\epsilon_t^k(s_{t,i}) = \frac{(k-i)(k-i-1)\cdots(t-i+1)}{(k-t)!}s_{t,i}^{+d} = \binom{k-i}{t-i}s_{t,i}^{+d}, \tag{4.11}$$

Remark 4.3.13. *Let $0 \leq t \leq k \leq n$, with $t + k \leq n$, and $d = k - t$. Using repeatedly Lemma 4.3.7 we have*

$$(\partial_{t+1}^{t}\partial_{t+2}^{t+1}\cdots\partial_{k}^{k-1})(s_{k,i}) = (n-k-i+1)\cdots(n-t-i-1)(n-t-i)s_{k,i}^{-d}.$$

Since $(k-t)!\partial_k^t = (\partial_{t+1}^{t}\partial_{t+2}^{t+1}\cdots\partial_{k}^{k-1})$ we have

$$\partial_k^t(s_{k,i}) = \frac{(n-k-i+1)\cdots(n-t-i-1)(n-t-i)}{(k-t)!}s_{k,i}^{-d} = \binom{n-t-i}{n-k-i}s_{k,i}^{-d} \tag{4.12}$$

4.4 Standard basis of polytopes

Let $\mathbb{Z}S_t^n$ be the submodule generated by the set of all polytopes S_t^n. The aim of this section is to find a basis for $\mathbb{Z}S_t^n$, called "standard basis", which will be essential in section 4.5.

We know that $\mathbb{Z}S_{t,i}^n \subseteq E_{t,i}$ and we observe that

$$\mathbb{Z}S_t^n = \mathbb{Z}S_{t,0}^n \oplus \mathbb{Z}S_{t,1}^n \oplus \cdots \oplus \mathbb{Z}S_{t,t'}^n.$$

Definition 4.4.1. *Let*

$$s_{t,i} = [\alpha_1, \cdots, \alpha_i; \beta_1, \cdots, \beta_i]_{t-i} := (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i) \cdot (\gamma_1 + \cdots + \gamma_s)$$

be a polytope of type (t, i), with $i \leq t'$. Then

1. *if $i = 0$, $s_{t,0}$ is a "standard polytope",*
2. *if $i > 0$, we say that $s_{t,i}$ is a "standard polytope" provided that*
   (a) $\alpha_1 < \alpha_2 < \cdots < \alpha_i$ *and* $\beta_1 < \beta_2 < \cdots < \beta_i$,
   (b) $\alpha_i < \delta$ *for all* $\delta \in \Omega \setminus \{\alpha_1, \cdots, \alpha_i, \beta_1, \cdots, \beta_i\}$, *and*
   (c) $\alpha_j < \beta_j$ *for all* $1 \leq j \leq i$.

Example 4.4.2. *If $n = 6$ and $t = 2$, we have the following standard polytopes*

- *of type* $(2, 0)$:

  $\{1,2\} + \{1,3\} + \{1,4\} + \{1,5\} + \{1,6\} + \{2,3\} + \{2,4\} + \{2,5\} + \{2,6\} + \{3,4\} + \{3,5\} + \{3,6\} + \{4,5\} + \{4,6\} + \{5,6\}$;

- *of type* $(2, 1)$:

  $(\{1\} - \{2\})(\{3\} + \{4\} + \{5\} + \{6\})$, $(\{1\} - \{3\})(\{2\} + \{4\} + \{5\} + \{6\})$,

  $(\{1\} - \{4\})(\{2\} + \{3\} + \{5\} + \{6\})$, $(\{1\} - \{5\})(\{2\} + \{3\} + \{4\} + \{6\})$,

  $(\{1\} - \{6\})(\{2\} + \{3\} + \{4\} + \{5\})$;

- *of type* $(2, 2)$:

  $(\{1\} - \{2\})(\{3\} - \{4\})$, $(\{1\} - \{2\})(\{3\} - \{5\})$, $(\{1\} - \{2\})(\{3\} - \{6\})$,

  $(\{1\} - \{3\})(\{2\} - \{4\})$, $(\{1\} - \{3\})(\{2\} - \{5\})$, $(\{1\} - \{3\})(\{2\} - \{6\})$,

  $(\{1\} - \{4\})(\{2\} - \{5\})$, $(\{1\} - \{4\})(\{2\} - \{6\})$, $(\{1\} - \{5\})(\{2\} - \{6\})$.

Next Lemmas 4.4.3 and 4.4.5 prove that a standard polytope is actually determined by the set $\{\beta_1, \cdots, \beta_i\}$.

Lemma 4.4.3. *Let* $0 < i \leq n/2$ *and* $s_{i,i} = (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)$, $\bar{s}_{i,i} = (\bar{\alpha}_1 - \bar{\beta}_1) \cdots (\bar{\alpha}_i - \bar{\beta}_i)$ *be distinct standard polytopes of type* (i,i)*. Then the sets* $x = \{\beta_1, \cdots, \beta_i\}$ *and* $\bar{x} = \{\bar{\beta}_1, \cdots, \bar{\beta}_i\}$ *are distinct.*

Proof. Suppose that the ordered sets x and $\bar{x}$ are equal, that is $\beta_j = \bar{\beta}_j$, for $j = 1, \cdots, i$. As $s_{i,i} \neq \bar{s}_{i,i}$, let j_0 be the smallest index such that $\alpha_{j_0} \neq \bar{\alpha}_{j_0}$. We write

$$s_{i,i} = (\alpha_1 - \beta_1) \cdots (\alpha_{j_0-1} - \beta_{j_0-1})(\alpha_{j_0} - \beta_{j_0}) \cdots (\alpha_i - \beta_i)$$

and

$$\bar{s}_{i,i} = (\alpha_1 - \beta_1) \cdots (\alpha_{j_0-1} - \beta_{j_0-1})(\bar{\alpha}_{j_0} - \beta_{j_0}) \cdots (\bar{\alpha}_i - \beta_i).$$

In particular, without loss of generality, we can suppose that $\alpha_{j_0} < \bar{\alpha}_{j_0}$; by definition 4.4.1, we have that α_{j_0} does not appear in the polytope $\bar{s}_{i,i}$.

So $\alpha_{j_0} \in \Omega \backslash \{\alpha_1, \cdots, \alpha_{j_0-1}, \bar{\alpha}_{j_0}, \cdots, \bar{\alpha}_i, \beta_1, \cdots, \beta_i\}$, contradicting the hypothesis $\bar{\alpha}_{j_0} < \delta$, for all $\delta \in \Omega \backslash \{\alpha_1, \cdots, \alpha_{j_0-1}, \bar{\alpha}_{j_0}, \cdots, \bar{\alpha}_i, \beta_1, \cdots, \beta_i\}$ (point 2b of the definition 4.4.1). □

In order to prove that if x and $\bar{x}$ are distinct, then $s_{i,i} \neq \bar{s}_{i,i}$, we introduce the following order relation on L_t^n.

Definition 4.4.4. *[6] (The reverse lexicographic order). We fix* $1 \leq t \leq n$ *and consider the reverse lexicographic order on* L_t^n*. That is for all* $y, x \in L_t^n$ *we say* $y < x$ *if and only if* $max(y \setminus x) < max(x \setminus y)$*.*

Lemma 4.4.5. *Let* $0 < i \leq n/2$ *and* $s_{i,i} = (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)$, $\bar{s}_{i,i} = (\bar{\alpha}_1 - \bar{\beta}_1) \cdots (\bar{\alpha}_i - \bar{\beta}_i)$ *be standard polytopes of type* (i,i) *such that* $x = \{\beta_1, \cdots, \beta_i\}$ *and* $\bar{x} = \{\bar{\beta}_1, \cdots, \bar{\beta}_i\}$ *are distinct. Then* $s_{i,i}$ *and* $\bar{s}_{i,i}$ *are distinct.*

Proof. As $x \neq \bar{x}$, without loss of generality, we can suppose $x < \bar{x}$, with respect to reverse lexicographic order. Now, we note that x is the largest set y for which y occurs in the expansion of $s_{i,i}$. So $\bar{x}$ does not appear in $s_{i,i}$. It follows that $s_{i,i} \neq \bar{s}_{i,i}$. □

As $x = \{\beta_1, \cdots, \beta_i\}$, with $\beta_1 < \cdots < \beta_i$, determines the corresponding standard polytope $(\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)$ of type (i,i), we put $s_x^i = (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)$.

The $\mathbb{Q}Sym(n)$-irreducible modules are well known. For reference on the representation of the symmetric groups $Sym(n)$ see for example [10]. These $\mathbb{Q}Sym(n)$-irreducible modules are the Specht modules. We are interested to find a basis for $E_{i,i}$. It is not difficult to see that the standard polytopes of type (i, i) correspond one-to-one to the standard polytabloids, via the following correspondence

$$e_{tab(x)} \longrightarrow s_x^i = (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i),$$

where $e_{tab(x)}$ is the standard polytabloid associated with the standard tableau

$$tab(x) = \begin{array}{ccccccccccc} \alpha_1 & < & \cdots & < & \alpha_i & < & \alpha_{i+1} & < & \cdots & < & \alpha_{n-i} \\ \beta_1 & < & \cdots & < & \beta_i & & & & & & \end{array}.$$

Every partition $(n-i, i)$ of n determines a Specht module, a basis of whose is given from standard polytabloids (see [10]).

We summarize this in the following lemma.

Lemma 4.4.6. *Let $0 \leq i \leq \frac{n}{2}$. Then the standard polytopes of type (i,i) correspond one-to-one to the standard polytabloids for the partition $(n-i,i)$ of n. Moreover the cardinality of the set of all standard polytopes of type (i,i) is $\binom{n}{i} - \binom{n}{i-1}$.*

We thank Prof. Antonio Pasini for the following alternative purely combinatoric proof of Lemma 4.4.6, that avoids any reference to polytabloids:

Proof. By induction on i, for $i = 1, \cdots, \frac{n}{2}$, we prove that the cardinality of the set of all standard polytopes of type (i,i) is $\binom{n}{i} - \binom{n}{i-1}$. The result is true for $i = 1$, as $\{1\} - \{j\}$, with $j = 2, 3, \cdots, n$, are the $n-1 = \binom{n}{1} - \binom{n}{0}$ standard polytopes. If $i > 1$, we suppose that the statement is true for standard polytopes of type (j, j), with $j < i$ and we count all the standard polytopes of type (i,i). Let $(\alpha_1 - \beta_1)\cdots(\alpha_i - \beta_i)$ be a standard polytope of type (i,i). β_i can be any value within the set $\{2i, \cdots, n\}$. If $k+1$ is the value chosen for β_i, the other terms $\beta_1, \cdots, \beta_{i-1}$ must be selected within the set $\{1, 2, \cdots, k\}$. By induction hypothesis the standard polytopes of type $(\alpha_1 - \beta_1)\cdots(\alpha_{i-1} - \beta_{i-1})$ are $\binom{k}{i-1} - \binom{k}{i-2}$. So the number of standard polytopes of type $(i,\, i)$ is

$$\sum_{k=2i-1}^{n-1} (\binom{k}{i-1} - \binom{k}{i-2}). \tag{4.13}$$

Now it is enough to prove that the sum in equation 4.13 is equal to $\binom{n}{i} - \binom{n}{i-1}$, that is

$$\sum_{k=2i-1}^{n-1} (\binom{k}{i-1} - \binom{k}{i-2}) = \binom{n}{i} - \binom{n}{i-1}. \tag{4.14}$$

We prove the equation 4.14 by induction on $n \geq 2i$. If $n = 2i$, 4.14 becomes

$$\binom{2i-1}{i-1} - \binom{2i-1}{i-2} = \binom{2i}{i} - \binom{2i}{i-1}. \tag{4.15}$$

Since

$$\begin{aligned}\binom{2i}{i} - \binom{2i}{i-1} &= \binom{2i-1}{i} + \binom{2i-1}{i-1} - \binom{2i-1}{i-1} - \binom{2i-1}{i-2} = \binom{2i-1}{i} - \binom{2i-1}{i-2} = \\ &= \binom{2i-1}{i-1} - \binom{2i-1}{i-2},\end{aligned}$$

the equation 4.15 holds.

Now we suppose that 4.14 holds for n and we prove it for $n+1$, that is

$$\sum_{k=2i-1}^{n} (\binom{k}{i-1} - \binom{k}{i-2}) = \binom{n+1}{i} - \binom{n+1}{i-1}. \tag{4.16}$$

We can rewrite 4.16 as follows:

$$\left(\sum_{k=2i-1}^{n-1}\left(\binom{k}{i-1}-\binom{k}{i-2}\right)\right)+\binom{n}{i-1}-\binom{n}{i-2}=\binom{n}{i}-\binom{n}{i-2}.$$

By induction hypothesis we have

$$\binom{n}{i}-\binom{n}{i-1}+\binom{n}{i-1}-\binom{n}{i-2}=\binom{n}{i}-\binom{n}{i-2}. \tag{4.17}$$

The last equation is trivial. So the claim follows. □

By Theorem 4.2.8, $\binom{n}{i}-\binom{n}{i-1}$ is the dimension of the vector space $E_{i,i}$. It is easy to realize that the set of all s_x^i is linearly independent: this is immediate for $i = 0$, and for $i > 0$ we write explicitly the polytope s_x^i (see example 4.4.8). We note that x is the largest set y (with respect to reverse lexicographic order) for which y occurs in the expansion of s_x^i. Since different x determine different standard polytopes (Lemma 4.4.5), it is not difficult to see that the set of all s_x^i is linearly independent over $\mathbb{K}$. It is enough to consider the matrix whose columns are the coordinates of s_x^i with respect to the basis L_i^n. This matrix contains a square triangular submatrix, of size $\binom{n}{i}-\binom{n}{i-1}$, which has ±1 on the main diagonal.

This proves the following Lemma

Lemma 4.4.7. *Let $\mathbb{K}$ be an arbitrary field, $0 \le i \le n/2$ and let $\mathbb{K}L_i^n$ be the vector space of basis L_i^n. Then the set of standard polytopes s_x^i of type (i,i) is linearly independent in $\mathbb{K}L_i^n$.*

We clarify the proof of Lemma 4.4.7 with an example.

Example 4.4.8. *We refer back to Example 4.4.2 and we denote*

$$\mathcal{F}(6,2)=\{\{2,4\},\{2,5\},\{2,6\},\{3,4\},\{3,5\},\{3,6\},\{4,5\},\{4,6\},\{5,6\}\}.$$

and

$s^2_{\{2,4\}} = (\{1\} - \{2\})(\{3\} - \{4\}),$ $\quad s^2_{\{2,5\}} = (\{1\} - \{2\})(\{3\} - \{5\}),$

$s^2_{\{2,6\}} = (\{1\} - \{2\})(\{3\} - \{6\}),$ $\quad s^2_{\{3,4\}} = (\{1\} - \{3\})(\{2\} - \{4\}),$

$s^2_{\{3,5\}} = (\{1\} - \{3\})(\{2\} - \{5\}),$ $\quad s^2_{\{3,6\}} = (\{1\} - \{3\})(\{2\} - \{6\}),$

$s^2_{\{4,5\}} = (\{1\} - \{4\})(\{2\} - \{5\}),$ $\quad s^2_{\{4,6\}} = (\{1\} - \{4\})(\{2\} - \{6\}),$

$s^2_{\{5,6\}} = (\{1\} - \{5\})(\{2\} - \{6\})$

the standard polytopes of type $(2,2)$*.*

We write every s^2_x *as linear combination of the elements of the canonical basis*

$L^6_2 = \{\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{1,6\},\{2,3\},\{2,4\},\{2,5\},\{2,6\},\{3,4\},\{3,5\},\{3,6\},\{4,5\},$

$\{4,6\},\{5,6\}\}.$

For example $s^2_{\{2,4\}} = (\{1\} - \{2\})(\{3\} - \{4\}) = \{1,3\} - \{1,4\} - \{2,3\} + \{2,4\}.$

The dimension of the vector space $\mathbb{K}S^6_{2,2}$ *is given from* $rank$ *of the matrix* A *of size* 15×9*, whose columns are the coordinates of all the standard polytopes of type* $(2,2)$ *with respect to the basis* L^6_2*.*

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & -1 & 0 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

It is immediate to see that the last 9 *rows are independent, so that* $rank(A) = 9$ *for any field* $\mathbb{K}$*: if* B *is the submatrix of* A *consisting of the last* 9 *rows, then* $det(B) = 1$.

We note that in the expansion of s_x^i the set x appears with coordinate ± 1.

Our aim is to prove that the set of all standard polytopes of type (t, i), for $i = 0, \cdots, t'$, forms a basis of the $\mathbb{Z}$-module $\mathbb{Z}S_t^n$.

Theorem 4.4.9. *If* $0 \leq i \leq t'$*, then the set of standard polytopes of type* (t, i) *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}S_{t,i}^n$*, called standard basis. It follows that the union of all standard polytopes is a standard basis of*

$$\mathbb{Z}S_t^n = \mathbb{Z}S_{t,0}^n \oplus \mathbb{Z}S_{t,1}^n \oplus \cdots \oplus \mathbb{Z}S_{t,t'}^n.$$

Proof. We observe that $i \leq \frac{n}{2}$, as $i \leq t'$. Put $n_i = \binom{n}{i} - \binom{n}{i-1}$, by Theorem 4.2.8, we have $E_{i,i} \cong E_{t,i}$ and $dim\, E_{i,i} = n_i$. Moreover, from Lemma 4.4.7, we get that the n_i's standard polytopes of type (i,i) are linearly independent in $\mathbb{Z}S^n_{i,i} \subseteq \mathbb{Q}L^n_i$. Applying the map tail-extension, we obtain n_i independent polytopes in $\mathbb{Z}S^n_{t,i}$. In particular we deduce that $rank(\mathbb{Z}S^n_{t,i}) \geq n_i$. Since $\mathbb{Z}S^n_{t,i} \subseteq E_{t,i}$ and $dim_{\mathbb{Q}} E_{t,i} = n_i$, it follows that $rank(\mathbb{Z}S^n_{t,i}) = n_i$, for any t and $i \leq t'$.

It remains to prove that they span $\mathbb{Z}S^n_{t,i}$. For this purpose we prove that the standard polytopes of type (i,i) span $\mathbb{Z}S^n_{i,i}$. Let L' be the submodule of $\mathbb{Z}S^n_{i,i}$ spanned by standard polytopes of type (i,i). We have $rank(L') = rank(\mathbb{Z}S^n_{i,i}) = n_i$, hence $\frac{\mathbb{Z}S^n_{i,i}}{L'}$ is a finite group. Suppose for contradiction that $\mathbb{Z}S^n_{i,i} \neq L'$. Then there exist $w \in \mathbb{Z}S^n_{i,i} \setminus L'$ and a prime p such that $pw \in L'$. We have

$$pw = \sum_{s^i_x \text{ standard polytope}} a_x s^i_x, \tag{4.18}$$

where $a_x \in \mathbb{Z}$ and not all divisible by p, otherwise $w \in L'$. Reducing mod p the equation in 4.18, we infer that the set of standard polytopes of type (i,i) is linearly dependent in $\mathbb{Z}/p\mathbb{Z}$. This contradicts Lemma 4.4.7. Thus $\mathbb{Z}S^n_{i,i} = L'$. By tail-extension, $\mathbb{Z}S^n_{t,i}$ is spanned by standard polytopes of type (t,i). It follows immediately that the union of all standard polytopes of type (t,i), for each $0 \leq i \leq t'$, forms a basis for $\mathbb{Z}S^n_t$. □

Remark 4.4.10. *Note that in general a basis of $\mathbb{Z}S^n_i$ is not a basis of $\mathbb{Z}L^n_i$.*

Example 4.4.11. *Going back to examples 4.4.2 and 4.4.8, we consider the expansion of every standard polytope of $\mathbb{Q}L^6_2$. The matrix of change of basis from the set of all standard polytopes to the canonical basis L^6_2 is*

$$B = \begin{pmatrix}
1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 1 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & -1 & 0 & 0 & -1 & 0 & -1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & -1 & -1 \\
1 & -1 & -1 & 0 & 0 & 0 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & 0 & 0 \\
1 & -1 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 \\
1 & -1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
1 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.$$

The determinant of B is -15360. This means that B is not invertible in $\mathbb{Z}$ and the set of all standard polytopes is not a basis of $\mathbb{Z}L_2^6$. It follows that $\mathbb{Z}S_2^6 \subset \mathbb{Z}L_2^6$.

This shows us that to find a diagonal form of W_{tk} is not enough to consider a basis of polytopes of $\mathbb{Z}S_t^n$ and $\mathbb{Z}S_k^n$. This observation is the starting point of the next section, where we give our proof of Wilson's Theorem.

4.5 Wilson's Theorem via linear maps

In [15] R.M. Wilson proves that the incidence matrix W_{tk} associated to the incidence structure $\mathcal{I}^n_{tk} = (L^n_t, L^n_k, \subseteq)$, where $0 \le t \le k \le n$ and $t + k \le n$, is equivalent to a diagonal form, with non-zero diagonal entries $d_i = \binom{k-i}{t-i}$ and multiplicity $\binom{n}{i} - \binom{n}{i-1}$. For this purpose, he constructs a matrix $M_{tk} = \bigcup_{i=0}^{t} W_{ik}$ and he proves that it has index one and rank $\binom{n}{t}$, for any $t \le k$ where $t + k \le n$ (Proposition 3.1.3).

Now, the maps ϵ^k_t and ∂^t_k, which we have introduced in proof of Theorem 4.2.8 on vector spaces, restrict to $\mathbb{Z}$-modules

$$\epsilon^k_t : \mathbb{Z}L^n_t \longrightarrow \mathbb{Z}L^n_k \qquad \text{and} \qquad \partial^t_k : \mathbb{Z}L^n_k \longrightarrow \mathbb{Z}L^n_t.$$

The matrices associated to them, with respect to the bases L^n_t and L^n_k are W^T_{tk} and W_{tk}, respectively. Thus to determine the invariant factors of W_{tk} is equivalent to find the Smith group of $\epsilon^k_t : \mathbb{Z}L^n_t \longrightarrow \mathbb{Z}L^n_k$.

We observe that, in terms of pure modules and linear maps, Wilson's Proposition 3.1.3 means that

$$\epsilon^k_0(\mathbb{Z}L^n_0) + \cdots + \epsilon^k_t(\mathbb{Z}L^n_t)$$

is a pure submodule of $\mathbb{Z}L^n_k$ of rank $\binom{n}{t}$.

In [2] T. Bier improves Wilson's Theorem showing that an opportune basis of $\mathbb{Z}$-module $row_{\mathbb{Z}}(M_{tk})$ can be chosen from the rows of matrix M_{tk} itself, as it contains a $\binom{n}{t} \times \binom{n}{t}$ submatrix of index 1. Moreover, in [8] the authors modify slightly the concept of standard tableau to study the notion of rank of a finite set of positive integers, which was introduced by Frankl [6]. Utilizing this, they construct an incidence matrix equivalent to M_{tk}.

In this work, with arguments inspired by the results in previous papers ([2], [6] and [8]), using the standard basis of polytopes of $\mathbb{Z}S_j^n$, we will explicitly construct a standard basis C_j of $\mathbb{Z}L_j^n$, for $j = 0, \cdots, n$, such that the matrix associated to ϵ_t^k with respect to C_t and C_k is the diagonal form found by R.M. Wilson in [15].

We fix the following facts that will be used later. In the sequel, for convenience, put:

$$\mathcal{F}(n,i) = \{x \in L_i^n \ : \ s_x^i \text{ is a standard polytope of type } (i,i)\}$$

(note that for $n = 6$ and $i = 2$, we already used the notation in Example 4.4.8).

For any $x_i \in \mathcal{F}(n,i)$, going back to the definition of $s_{x_i}^i$ we have:

1. $s_{x_i}^i \in \mathbb{Z}S_{i,i}^n \subseteq E_{i,i}$;
2. $\epsilon_i^k(s_{x_i}^i) \in \mathbb{Z}S_{k,i}^n$;
3. if $s_{x_i}^i = (\alpha_1 - \beta_1)\cdots(\alpha_i - \beta_i)$, then $\epsilon_i^k(s_{x_i}^i) = (\alpha_1 - \beta_1)\cdots(\alpha_i - \beta_i)(\gamma_1 + \cdots + \gamma_u)$ is a standard polytope of type (k,i), where $\gamma_1, \cdots, \gamma_u$ is the collection of all $(k-i)$-subsets of $\Omega \setminus \{\alpha_1, \cdots, \alpha_i, \beta_1, \cdots, \beta_i\}$;
4. the set
$$\{\epsilon_i^k(s_{x_i}^i) \ : \ s_{x_i}^i \text{ standard polytope of type } (i,i),\ i = 0, \cdots, t\}$$
is a basis of $\mathbb{Z}S_{k,0}^n \oplus \cdots \oplus \mathbb{Z}S_{k,t}^n$ (by Theorem 4.4.9 and points (1), (2) and (3)).

Our proof is given by three steps.

Step 1. We find the Smith group of $\epsilon_t^k : \mathbb{Z}S_t^n \to \mathbb{Z}S_k^n$ (see definition 2.4.21).

Theorem 4.5.1. *Let* $0 \leq t \leq k \leq n$ *and* $t + k \leq n$*. Then the Smith group of*

$$\epsilon_t^k : \mathbb{Z}S_t^n \to \mathbb{Z}S_k^n$$

is isomorphic to $(C_{d_0})^{n_0} \times \cdots \times (C_{d_t})^{n_t} \times \mathbb{Z}^l$*, where* $d_i = \binom{k-i}{t-i}$*,* $n_i = \binom{n}{i} - \binom{n}{i-1}$*, for* $i = 0, \cdots, t$ *and* $l = \binom{n}{k} - \binom{n}{t}$*.*

Proof. If $t = k$ the claim is trivial, since ϵ_t^t is the identity map. So we assume $t \neq k$. Since $t < k$ and $t + k \leq n$, we have $\epsilon_t^k(E_{t,i}) \neq 0$, for all $i = 0, \cdots, t$. In particular, if $f \in \mathbb{Z}S_k^n$ is written as $f = f_{k,0} + f_{k,1} + \cdots + f_{k,k'}$, with $f_{k,j} \in \mathbb{Z}S_{k,j}^n$, then f has finite order over $\epsilon_t^k(\mathbb{Z}S_t^n)$ if and only if $f_{k,t+1} = \cdots = f_{k,k'} = 0$. Therefore the module of all elements $f \in \mathbb{Z}S_k^n$ which have finite order over $\epsilon_t^k(\mathbb{Z}S_t^n)$ is

$$\mathbb{Z}S_{k,0}^n \oplus \cdots \oplus \mathbb{Z}S_{k,t}^n.$$

In particular,

$$\mathbb{Z}S_k^n/\epsilon_t^k(\mathbb{Z}S_t^n) \cong \mathbb{Z}S_{k,0}^n/\epsilon_t^k(\mathbb{Z}S_{t,0}^n) \oplus \cdots \oplus \mathbb{Z}S_{k,t}^n/\epsilon_t^k(\mathbb{Z}S_{t,t}^n) \oplus \mathbb{Z}^l$$

where $l = \binom{n}{k} - \binom{n}{t}$.

Let $d = k - t$ and select some $0 \leq i \leq t$. Although we now introduce some other notation a little bit heavy for the reader, we prefer to give the proof using a general basis for $\mathbb{Z}S_t^n$. Let $B_{t,i} = \{s_{t,i,1}, \cdots, s_{t,i,n_i}\}$ be a basis of $\mathbb{Z}S_{t,i}^n$, then replacing each $s_{t,i,j}$ by $s_{t,i,j}^{+d}$ we obtain a basis $B_{t,i}^{+d} = \{s_{t,i,1}^{+d}, \cdots, s_{t,i,n_i}^{+d}\}$ of $\mathbb{Z}S_{k,i}^n$ (see Notation 4.3.11) .

Furthermore,

$$\epsilon_t^k(s_{t,i,j}) = \binom{k-i}{t-i} s_{t,i,j}^{+d},$$

with $1 \leq j \leq n_i$, by equation 4.11. We conclude that $\mathbb{Z}S_{k,i}^n/\epsilon_t^k(\mathbb{Z}S_{t,i}^n) \cong (C_{d_i})^{n_i}$, where $d_i = \binom{k-i}{t-i}$ and $n_i = \binom{n}{i} - \binom{n}{i-1}$ and so

$$\mathbb{Z}S_k^n/\epsilon_t^k(\mathbb{Z}S_t^n) \cong (C_{d_0})^{n_0} \times \cdots \times (C_{d_t})^{n_t} \times \mathbb{Z}^l,$$

with $l = \binom{n}{k} - \binom{n}{t}$. □

Step 2. Of fundamental importance are Lemmas 4.5.2 and 4.5.3.

Lemma 4.5.2. *Let $1 \le i \le \frac{n}{2}$ and $x = \{\beta_1, \cdots, \beta_i\} \in L_i^n$ such that $n \in x$ and $\beta_1 < \cdots < \beta_i = n$. Then $x \in \mathcal{F}(n,i)$ if and only if $x' \in \mathcal{F}(n-1, i-1)$, where $x' = x \setminus \{n\}$.*

Proof. For $x \in \mathcal{F}(n,i)$ let $s_x^i = (\alpha_1 - \beta_1)\cdots(\alpha_i - \beta_i)$ be the standard polytope based on x. By definition $s_{x'}^{i-1} = (\alpha_1 - \beta_1)\cdots(\alpha_{i-1} - \beta_{i-1})$ is a standard polytope based on $x' \in \mathcal{F}(n-1, i-1)$. Vice versa, we observe that, by hypothesis, $n \ge 2$. If $x' = \emptyset$, then $x = \{n\}$ and $s_x^1 = (1-n)$ is a standard polytope of type $(1,1)$. If $i > 1$ and $x' \in \mathcal{F}(n-1, i-1)$, $s_{x'}^i = (\alpha_1 - \beta_1)\cdots(\alpha_{i-1} - \beta_{i-1})$ is the standard polytope based on x'. Then $s_x^i = (\alpha_1 - \beta_1)\cdots(\alpha_{i-1} - \beta_{i-1})(\alpha_i - n)$ is the standard polytope based on $x = \{\beta_1, \cdots, \beta_{i-1}, n\}$, where

$$\alpha_i = min\{\delta \,:\, \delta \in \Omega \setminus \{\alpha_1, \cdots, \alpha_{i-1}, \beta_1, \cdots, \beta_{i-1}, n\}\}.$$

□

Lemma 4.5.3. *Let $1 \le i \le \frac{n-1}{2}$ and $x = \{\beta_1, \cdots, \beta_i\} \in L_i^n$, such that $n \notin x$ and $\beta_1 < \cdots < \beta_i$.*

1. *$x \in \mathcal{F}(n,i)$ if and only if $x \in \mathcal{F}(n-1,i)$;*
2. *$\mathcal{F}(n,0) = \mathcal{F}(n-1,0)$.*

Proof.

1. Applying the Definition 4.4.1, the claim follows.
2. $\mathcal{F}(n,0) = \{\emptyset\} = \mathcal{F}(n-1,0)$.

□

Step 3. With methods similar to those used in [8] we prove the following

Theorem 4.5.4. *Let $0 \le t \le k$ with $t + k \le n$ and $s_{x_i}^i$ be a standard polytope of type (i,i), for $i = 0, \cdots, t$. Then $\mathbb{Z}S_{k,0}^n \oplus \cdots \oplus \mathbb{Z}S_{k,t}^n$ is isomorphic to $\mathbb{Z}L_k^n \cap (E_{k,0} \oplus \cdots \oplus E_{k,t})$.*

An isomorphism is given by the map $\varphi_t^{(n)k}$ linear extension of the map defined on a standard basis of polytopes by

$$\varphi_t^{(n)k}\left(\epsilon_i^{(n)k}(s_{x_i}^i)\right) = \epsilon_i^{(n)k}(x_i). \tag{4.19}$$

Proof. Put $d = k - i$ and $(s_{x_i}^i)^{+d}$ as in Notation 4.3.11, with $s_{x_i}^i$ a standard polytope of type (i, i) in $\mathbb{Z}S_{i,i}^n$. By equation 4.11 we have that the standard polytope of type (k, i) based on x is $\epsilon_i^{(n)k}(s_{x_i}^i) = (s_{x_i}^i)^{+d}$. From Theorem 4.4.9 we deduce that

$$\{\epsilon_i^{(n)k}(s_{x_i}^i) \,:\, s_{x_i}^i \text{ is a standard polytope of type } (i,i),\ i = 0, \cdots, t\}$$

is a basis of $\mathbb{Z}S_{k,0}^n \oplus \cdots \oplus \mathbb{Z}S_{k,t}^n$. We note that $\epsilon_i^{(n)k}(x_i) \in \mathbb{Z}L_k^n \cap (E_{k,0} \oplus \cdots \oplus E_{k,t})$.

In the following $A_t^{(n)k}$ denotes the matrix $\binom{n}{k} \times \binom{n}{t}$ with the columns indexed by $\epsilon_i^{(n)k}(x_i)$, for $i = 0, \cdots, t$ and the rows indexed by $y \in L_k^n$; moreover we rearrange the terms in accord to whether or not they contain n.

In order to apply Lemma 2.4.14 to get that $\varphi_t^{(n)k}$ is bijective, we must prove that $Im\, \varphi_t^{(n)k}$ is a pure submodule of $\mathbb{Z}L_k^n$ of rank $\binom{n}{t}$. For this purpose it is enough to prove that $A_t^{(n)k}$ has index 1 and rank $\binom{n}{t}$. This implies that

$$\{\epsilon_i^{(n)k}(x_i) \,:\, s_{x_i}^i \text{ is a standard polytope of type } (i,i),\ i = 0, \cdots, t\}$$

spans a pure submodule of $\mathbb{Z}L_k^n$ of rank $\binom{n}{t}$.

We prove the claim by induction on $n + t$.

If $t = 0$, obviously $\mathbb{Z}S_{k,0}^n = \mathbb{Z}L_k^n \cap E_{k,0}$ and $s_\emptyset^0 = \emptyset$, so $\varphi_0^{(n)k}$ is the identity map.

If $n = 1$ then we have two possibilities

1. $t = k = 0$;

2. $t = 0$ and $k = 1$,

which are part of previous case.

Instead if $n = 2$, the four cases are

1. $t = k = 0$;
2. $t = 0$, $k = 1$;
3. $t = 0$, $k = 2$;
4. $t = k = 1$.

In this last case, it is easy to prove the claim. Actually, since the standard polytope of type $(1,1)$ is $(\{1\} - \{2\})$, we have $\epsilon_0^{(2)1}(\emptyset) = \{1\} + \{2\}$ and $\epsilon_1^{(2)1}(\{2\}) = \{2\}$. It follows that $A_1^{(2)1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ has index 1 and rank 2.

The above observations prove the first step of induction. So we can consider $t > 0$ and $n \geq 3$. By induction we suppose that the statement is true for $\overline{n} + \overline{t} < n + t$, i.e. $A_{\overline{t}}^{(\overline{n})\overline{k}}$ has index 1 and rank $\binom{\overline{n}}{\overline{t}}$, with $0 \leq \overline{t} \leq \overline{k}$ and $\overline{t} + \overline{k} \leq \overline{n}$. In particular

(I) $A_t^{(n-1)k}$ has index 1 and rank $\binom{n-1}{t}$, with $0 \leq t \leq k$ and $t + k \leq n - 1$,

(II) $A_{t-1}^{(n-1)k-1}$ has index 1 and rank $\binom{n-1}{t-1}$, with $0 \leq t-1 \leq k-1$ and $t-1+k-1 \leq n-1$,

(III) $A_t^{(n-1)k-1}$ has index 1 and rank $\binom{n-1}{t}$, with $0 \leq t \leq k - 1$ and $t + k - 1 \leq n - 1$,

(IV) $A_{t-1}^{(n-1)t}$ has index 1 and rank $\binom{n-1}{t-1}$, with $0 \leq t - 1 \leq t$ and $t + t - 1 \leq n - 1$,

(V) $A_t^{(n-1)t}$ has index 1 and rank $\binom{n-1}{t}$, with $t \geq 0$ and $t + t \leq n - 1$, We distinguish four cases

1. Let $t = k = \frac{n}{2}$.

   We index the columns and the rows of $A_t^{(n)t}$ in accord to

   $$\{\epsilon_i^{(n)t}(x_i) : n \in x_i, i = 1, \cdots, t\} \cup \{\epsilon_i^{(n)t}(x_i) : n \notin x_i, i = 0, \cdots, t-1\},$$

   and $\{y \in L_t^n : n \in y\} \cup \{y \in L_t^n : n \notin y\}$, respectively.

   Observe that in $\{\epsilon_i^{(n)t}(x_i) : n \notin x_i, i = 0, \cdots, t-1\}$ the index i runs between 0 and $t-1$, since if $s_{x_t}^t = (\alpha_1 - \beta_1) \cdots (\alpha_t - \beta_t)$ is a standard polytope of type (t, t), then $\beta_t = n$; whence $n \in x_t$.

   If $n \in x_i$, then $\epsilon_i^{(n)t}(x_i) = \{n\}\epsilon_{i-1}^{(n-1)t-1}(x_i')$, where $x_i' = x_i \setminus \{n\}$, by Lemmas 4.5.2 and 4.5.3 we get

   $$A_t^{(n)t} = \left(\begin{array}{c|c} A_{t-1}^{(n-1)t-1} & * \\ \hline 0 & A_{t-1}^{(n-1)t} \end{array}\right).$$

   By induction hypothesis, the square matrices $A_{t-1}^{(n-1)t-1}$, of size $\binom{n-1}{t-1}$, and $A_{t-1}^{(n-1)t}$, of size $\binom{n-1}{t-1}$, have index 1 and rank $\binom{n-1}{t-1}$. Since $n-1 = t+t-1$, we have that $\binom{n-1}{t-1} = \binom{n-1}{t}$. So $A_t^{(n)t}$ has index 1 and rank $\binom{n-1}{t-1} + \binom{n-1}{t} = \binom{n}{t}$.

2. Let $t = k < \frac{n}{2}$.

   Again in this case, we index the columns and the rows of $A_t^{(n)t}$ in accord to

   $$\{\epsilon_i^{(n)t}(x_i) : n \in x_i, i = 1, \cdots, t\} \cup \{\epsilon_i^{(n)t}(x_i) : n \notin x_i, i = 0, \cdots, t\}$$

   and $\{y \in L_t^n : n \in y\} \cup \{y \in L_t^n : n \notin y\}$, respectively. As above, by Lemmas 4.5.2 and 4.5.3 we have

   $$A_t^{(n)t} = \left(\begin{array}{c|c} A_{t-1}^{(n-1)t-1} & * \\ \hline 0 & A_t^{(n-1)t} \end{array}\right).$$

By induction hypothesis, the square matrices $A_{t-1}^{(n-1)t-1}$, of size $\binom{n-1}{t-1}$, and $A_t^{(n-1)t}$, of size $\binom{n-1}{t}$, have index 1 and rank $\binom{n-1}{t-1}$ and $\binom{n-1}{t}$, respectively. So $A_t^{(n)t}$ has index 1 and rank $\binom{n-1}{t-1} + \binom{n-1}{t} = \binom{n}{t}$.

3. Let $t + k = n$ and $t < k$. We index the columns and the rows of $A_t^{(n)k}$ in accord to

$$\{\epsilon_i^{(n)k}(x_i) : n \in x_i, i = 1, \cdots, t\} \cup \{\epsilon_t^{(n)k}(x_t) : n \notin x_t\} \cup \{\epsilon_i^{(n)k}(x_i) : n \notin x_i, i = 0, \cdots, t-1\}$$

and $\{y \in L_k^n : n \in y\} \cup \{y \in L_k^n : n \notin y\}$, respectively. So we have

$$A_t^{(n)k} = \left(\begin{array}{c|c|c} A_{t-1}^{(n-1)k-1} & * & A_{t-1}^{(n-1)k-1} \\ \hline 0 & ** & A_{t-1}^{(n-1)k} \end{array}\right)$$

So $A_t^{(n)k}$ is equivalent to

$$\left(\begin{array}{c|c|c} A_{t-1}^{(n-1)k-1} & * & 0 \\ \hline 0 & ** & A_{t-1}^{(n-1)k} \end{array}\right) = \left(\begin{array}{cc|c} \multicolumn{2}{c|}{A_t^{(n-1)k-1}} & 0 \\ \hline 0 & \multicolumn{1}{|c|}{**} & A_{t-1}^{(n-1)k} \end{array}\right).$$

By induction hypothesis, the matrix $A_{t-1}^{(n-1)k}$, of size $\binom{n-1}{t-1}$, has index 1 and rank $\binom{n-1}{t-1}$. Thus

$$\left(\begin{array}{cc|c} \multicolumn{2}{c|}{A_t^{(n-1)k-1}} & 0 \\ \hline 0 & \multicolumn{1}{|c|}{**} & A_{t-1}^{(n-1)k} \end{array}\right) \sim \left(\begin{array}{cc|c} \multicolumn{2}{c|}{A_t^{(n-1)k-1}} & 0 \\ \hline 0 & \multicolumn{1}{|c|}{**} & I \end{array}\right) \sim \left(\begin{array}{c|c} A_t^{(n-1)k-1} & 0 \\ \hline 0 & I \end{array}\right)$$

where I is the identity matrix of size $\binom{n-1}{t-1}$. By induction hypothesis, the matrix $A_t^{(n-1)k-1}$, of size $\binom{n-1}{t}$, has index 1 and rank $\binom{n-1}{t}$. As $\binom{n-1}{t-1} + \binom{n-1}{t} = \binom{n}{t}$, the claim follows.

4. Let $t + k < n$ and $t < k$. In this case we index the columns and the rows of $A_t^{(n)k}$ in accord to

$$\{\epsilon_i^{(n)k}(x_i) : n \in x_i, i = 1, \cdots, t\} \cup \{\epsilon_i^{(n)k}(x_i) : n \notin x_i, i = 0, \cdots, t\}$$

and $\{y \in L_k^n : n \in y\} \cup \{y \in L_k^n : n \notin y\}$, respectively. So we have

$$A_t^{(n)k} = \left(\begin{array}{c|c} A_{t-1}^{(n-1)k-1} & * \\ \hline 0 & A_t^{(n-1)k} \end{array}\right),$$

and by induction hypothesis, the matrices $A_{t-1}^{(n-1)k-1}$ and $A_t^{(n-1)k}$ have index 1 and rank $\binom{n-1}{t-1}$ and $\binom{n-1}{t}$, respectively. We have the thesis.

□

Corollary 4.5.5. *Let $0 \le t \le k \le n$ with $t + k \le n$ and $s^i_{x_i}$ be a standard polytope of type (i,i), for $i = 0, \cdots, t$. Then the map*

$$\varphi : \mathbb{Z}S^n_k/\epsilon^k_t(\mathbb{Z}S^n_t) \to \mathbb{Z}L^n_k/\epsilon^k_t(\mathbb{Z}L^n_t)$$

defined by

$$\varphi(\epsilon^k_i(s^i_{x_i}) + \epsilon^k_t(\mathbb{Z}S^n_t)) = \epsilon^k_i(x_i) + \epsilon^k_t(\mathbb{Z}L^n_t),$$

and extended by linearity, is an isomorphism.

Proof. By Theorem 4.5.4, we have that $\varphi_t^{(n)k}$ is an isomorphism. Hence

$$\{\epsilon^k_i(x_i) : s^i_{x_i} \text{ is a standard polytope of type } (i,i),\ i = 0, \cdots, t\}$$

forms a basis of $\mathbb{Z}L^n_k \cap (E_{k0} \oplus \cdots \oplus E_{kt})$. In particular

$$\{\epsilon^k_i(x_i) : s^i_{x_i} \text{ is a standard polytope of type } (i,i),\ i = 0, \cdots, k'\} \tag{4.20}$$

and

$$\{\epsilon^t_i(x_i) : s^i_{x_i} \text{ is a standard polytope of type } (i,i),\ i = 0, \cdots, t\} \tag{4.21}$$

are bases of $\mathbb{Z}L^n_t$ and $\mathbb{Z}L^n_k$ respectively.

Clearly the claim is true if $t = k$, so we take $t < k$. By equation 4.6 we get

$$\binom{k-i}{t-i}\epsilon^k_i = \epsilon^k_t \epsilon^t_i. \tag{4.22}$$

The relations 4.20, 4.21 and 4.22 together with Theorem 4.5.1 give us

$$\mathbb{Z}L_k^n/\epsilon_t^k(\mathbb{Z}L_t^n) \cong \mathbb{Z}S_k^n/\epsilon_t^k(\mathbb{Z}S_t^n) \cong (C_{d_0})^{n_0} \times \cdots \times (C_{d_t})^{n_t} \times \mathbb{Z}^l,$$

with $l = \binom{n}{k} - \binom{n}{t}$, $d_i = \binom{k-i}{t-i}$ and $n_i = \binom{n}{i} - \binom{n}{i-1}$. □

CHAPTER 5

G-modules and orbit matrices

In this section we consider a generic permutation group $G \subseteq Sym(n)$, $n = |\Omega|$, with the induced action over L^n. If R is one of $\mathbb{Q}$ or $\mathbb{Z}$ we define the "orbit module" of G in the following way

Definition 5.0.1. *Let M be a submodule of RL_i^n. Then the "orbit module" of G on M, denoted by M^G, is the centralizer algebra*

$$M^G := \{v \in M \,:\, v^g = v \textit{ for any } g \in G\}.$$

Since the action of G on $\mathbb{Q}L^n$ commutes with ϵ, we have the following restrictions

$$\epsilon_t^k : (\mathbb{Z}L_t^n)^G \to (\mathbb{Z}L_k^n)^G \tag{5.1}$$

and

$$\epsilon_t^k : (\mathbb{Z}S_t^n)^G \to (\mathbb{Z}S_k^n)^G. \tag{5.2}$$

$S_t^n = S_{t,0}^n \cup S_{t,1}^n \cup \cdots \cup S_{t,t'}^n$, denotes the set of polytopes. As G maps polytopes of type (t,i) in polytopes of the same type, it is immediate to recognize:

$$(\mathbb{Z}S_t^n)^G = (\mathbb{Z}S_{t,0}^n)^G \oplus \cdots \oplus (\mathbb{Z}S_{t,t'}^n)^G.$$

We are interested to Smith groups of the restrictions of ϵ_t^k to the orbit modules of G on $\mathbb{Z}L_t^n$ and $\mathbb{Z}S_t^n$.

If $G = \{1_G\}$ then the orbits on L_t^n correspond to the subsets. So $(\mathbb{Z}L_t^n)^G = \mathbb{Z}L_t^n$ and $(\mathbb{Z}S_t^n)^G = \mathbb{Z}S_t^n$. Hence we can see the problem to find the Smith group of

$$\epsilon_t^k : (\mathbb{Z}L_t^n)^G \longrightarrow (\mathbb{Z}L_k^n)^G$$

as a generalization of Wilson's Theorem, 3.1.6 and 4.5.5.

The main original result of this chapter is Theorem 5.1.7 where we obtain the Smith group of $\epsilon_t^k : (\mathbb{Z}S_t^n)^G \longrightarrow (\mathbb{Z}S_k^n)^G$. This generalizes Theorem 4.5.1. Moreover in sections 5.2 and 5.3 we give some ideas which lead to conjecture that if $t + k = n$, then

$$(\mathbb{Z}L_k^n)^G / \epsilon_t^k (\mathbb{Z}L_t^n)^G \cong (\mathbb{Z}S_k^n)^G / \epsilon_t^k (\mathbb{Z}S_t^n)^G. \tag{5.3}$$

The conjecture will be formally stated in 5.3.5.

Finally in section 5.4, we consider the orbits $\Delta_1, \cdots, \Delta_{\tau_t}$ of G over the t-subsets L_t^n and the orbits $\Gamma_1, \cdots, \Gamma_{\tau_k}$ of G over the k-subsets L_k^n. Denote by Ω^t the orbit set $\{\Delta_1, \cdots, \Delta_{\tau_t}\}$ and by Ω^k the orbit set $\{\Gamma_1, \cdots, \Gamma_{\tau_k}\}$.

It is not difficult to recognize that the incidence matrices X_{tk}^+ and X_{tk}^-, denoted by *G-orbits matrices*, of the tactical decomposition (Ω^t, Ω^k) of $\mathcal{I}_{tk}^n = (L_t^n, L_k^n; \subseteq)$ are actually the matrices of

$$\epsilon_t^k : (\mathbb{Z}L_t^n)^G \longrightarrow (\mathbb{Z}L_k^n)^G \qquad \text{and} \qquad \partial_k^t : (\mathbb{Z}L_k^n)^G \longrightarrow (\mathbb{Z}L_t^n)^G$$

with respect to the canonical bases (see Corollary 5.1.6)

$$\mathcal{B}_{\Omega^t} = \{\sum_{x \in \Delta_j} x \, : \, j = 1, \cdots, \tau_t\} \qquad \text{and} \qquad \mathcal{B}_{\Omega^k} = \{\sum_{y \in \Gamma_i} y \, : \, i = 1, \cdots, \tau_k\}.$$

So again for $G = \{1_G\}$, X_{tk}^+ and X_{tk}^- coincide with the matrices W_{tk}^T and W_{tk}.

To look for a diagonal form of X^+_{tk} is equivalent to determine the Smith group of $\epsilon^k_t : (\mathbb{Z}L^n_t)^G \longrightarrow (\mathbb{Z}L^n_k)^G$.

We give some results about the matrices X^+_{tk} and X^-_{tk} in the case $t + k = n$, reinforcing our conjecture (see 5.3.5).

As usual, when there is not confusion, we write $(\mathbb{Q}L_t)^G$, $(\mathbb{Z}L_t)^G$, $(\mathbb{Q}S_t)^G$, $(\mathbb{Z}S_{t,i})^G$ instead $(\mathbb{Q}L^n_t)^G$, $(\mathbb{Z}L^n_t)^G$, $(\mathbb{Q}S^n_t)^G$, $(\mathbb{Z}S^n_{t,i})^G$.

5.1 G-orbit decomposition

The Smith group of $\epsilon^k_t : (\mathbb{Z}S_t)^G \longrightarrow (\mathbb{Z}S_k)^G$ will be determined in Theorem 5.1.7. To achieve the result we need some preliminary theorems, which make use of the concept of pure module.

Theorem 5.1.1. *For each* $0 \leq t \leq n$, *denote by* $\Delta_1, \cdots, \Delta_{\tau_t}$ *the orbits of G over* L^n_t. *Then the set* Ω^t *is a generating set for the vector space* $(\mathbb{Q}L_t)^G$, *that is*

$$(\mathbb{Q}L_t)^G = span_{\mathbb{Q}} \left\{ \sum_{x\in\Delta_j} x \ : \ \Delta_j \in \Omega^t \ and \ j = 0, \cdots, \tau_t \right\}.$$

Proof. For any $g \in G$ and $j = 0, \cdots, \tau_t$

$$(\sum_{x\in\Delta_j} x)^g = \sum_{x\in\Delta_j} x^g = \sum_{x\in\Delta_j} x.$$

Hence $span_{\mathbb{Q}}\{ \sum_{x\in\Delta_j} x \ : \ \Delta_j \in \Omega^t$ and $j = 0, \cdots, \tau_t\} \subseteq (\mathbb{Q}L_t)^G$.

Conversely, let $f \in (\mathbb{Q}L_t)^G$, we can write

$$f = \sum_{x\in L^n_t} r_x x = \sum_{x_1\in\Delta_1} r_{x_1} x_1 + \cdots + \sum_{x_{\tau_t}\in\Delta_{\tau_t}} r_{x_{\tau_t}} x_{\tau_t}.$$

By hypothesis, $f^g = f$ for all $g \in G$, so

$$\sum_{x_1 \in \Delta_1} r_{x_1} x_1^g + \cdots + \sum_{x_{\tau_t} \in \Delta_{\tau_t}} r_{x_{\tau_t}} x_{\tau_t}^g = \sum_{x_1 \in \Delta_1} r_{x_1} x_1 + \cdots + \sum_{x_{\tau_t} \in \Delta_{\tau_t}} r_{x_{\tau_t}} x_{\tau_t}.$$

We deduce that r_{x_j} depends only from the orbit. Thus

$$f = r_1 \sum_{x_1 \in \Delta_1} x_1 + \cdots + r_{\tau_t} \sum_{x_{\tau_t} \in \Delta_{\tau_t}} x_{\tau_t}.$$

The statement follows. In particular, we get that $dim_{\mathbb{Q}}(\mathbb{Q}L_t)^G = \tau_t$. □

Following some ideas of [13] and previous section we get Theorem 5.1.2.

Theorem 5.1.2. *Put $G \subseteq Sym(n)$ and $t \leq k \leq n$, with $t + k \leq n$. Then*

$$(\mathbb{Q}S_{t,i})^G \cong (\mathbb{Q}S_{k,i})^G$$

for all $0 \leq i \leq t$. Actually, the tail-cutting and tail-extension maps restrict to G-isomorphisms between the two G-orbit vector spaces and are inverse to each other.

Proof. First we consider $i = 0$. The polytope $\sum_{x \in L_t^n} x$ of type $(t, 0)$ belongs to $(\mathbb{Q}S_{t,0})^G$. So $E_{t,0} = span_{\mathbb{Q}}(\sum_{x \in L_t^n} x) = (\mathbb{Q}S_{t,0})^G$. The claim follows since that $E_{k,0} \cong E_{t,0}$.

For $0 \leq i \leq t$, we saw in Corollary 4.3.10 that the map tail-cutting $- : E_{t+1,i} \longrightarrow E_{t,i}$ is a $\mathbb{Q}Sym(n)$-isomorphism, so also a $\mathbb{Q}G$-isomorphism. It follows that for $f \in (\mathbb{Q}S_{t+1,i})^G$, $(f^-)^g = (f^g)^- = f^-$, so that $f^- \in (\mathbb{Q}L_t)^G \cap E_{t,i} = (\mathbb{Q}S_{t,i})^G$.

Similarly, the map $+ : E_{t,i} \longrightarrow E_{t+1,i}$ restricts to the map $+ : (\mathbb{Q}S_{t,i})^G \longrightarrow (\mathbb{Q}S_{t+1,i})^G$. Whence $(\mathbb{Q}S_{t,i})^G \cong (\mathbb{Q}S_{t+1,i})^G$. The maps $+$ and $-$ are inverse to each other. □

Theorem 5.1.3. *[13] Let $0 \leq t \leq n$, then*

$$(\mathbb{Q}L_t)^G = (\mathbb{Q}S_{t,0})^G \oplus \cdots \oplus (\mathbb{Q}S_{t,t'})^G.$$

In particular, $dim_{\mathbb{Q}}(\mathbb{Q}S_{t,i})^G = \tau_i - \tau_{i-1}$.

Proof. We observe that $(\mathbb{Q}S_{t,0})^G \oplus \cdots \oplus (\mathbb{Q}S_{t,t'})^G \subseteq (\mathbb{Q}L_t)^G$.

Let now f be an element of $(\mathbb{Q}L_t)^G$, that is $f^g = f$ for any $g \in G$. We have $(\mathbb{Q}L_t)^G \subseteq \mathbb{Q}L_t = E_{t,0} \oplus \cdots \oplus E_{t,t'}$ and $E_{t,i}$ are G-invariant subspaces of $\mathbb{Q}L_t^n$. So, we write

$$f = f_{t,0} + \cdots + f_{t,t'} = f_{t,0}^g + \cdots + f_{t,t'}^g,$$

where $f_{t,i} \in E_{t,i}$. As $f^g = f$ and $f_{t,i}^g \in E_{t,i}$, we get $f_{t,i}^g = f_{t,i}$ by the uniqueness of writing. This proves $(\mathbb{Q}L_t)^G \subseteq (\mathbb{Q}S_{t,0})^G \oplus \cdots \oplus (\mathbb{Q}S_{t,t'})^G$. So the equality holds.

Now, we argue on the dimension and we prove by induction that $dim_{\mathbb{Q}}(\mathbb{Q}S_{i,i})^G = \tau_i - \tau_{i-1}$, for $0 \leq i \leq \frac{n}{2}$.

If $i = 0$, then $dim_{\mathbb{Q}}(\mathbb{Q}S_{0,0})^G = \tau_0 = 1$. Now we assume that

$$dim_{\mathbb{Q}}(\mathbb{Q}S_{j,j})^G = \tau_j - \tau_{j-1},$$

for any $j < i$. By Theorem 5.1.2, we have $dim_{\mathbb{Q}}(\mathbb{Q}S_{i,j})^G = \tau_j - \tau_{j-1}$. Since

$$(\mathbb{Q}L_i)^G = (\mathbb{Q}S_{i,0})^G \oplus (\mathbb{Q}S_{i,1})^G \oplus \cdots \oplus (\mathbb{Q}S_{i,i-1})^G \oplus (\mathbb{Q}S_{i,i})^G,$$

we have

$$\tau_i = dim_{\mathbb{Q}}(\mathbb{Q}L_i)^G = dim_{\mathbb{Q}}(\mathbb{Q}S_{i,0})^G \oplus dim_{\mathbb{Q}}(\mathbb{Q}S_{i,1})^G \oplus \cdots \oplus dim_{\mathbb{Q}}(\mathbb{Q}S_{i,i-1})^G \oplus dim_{\mathbb{Q}}(\mathbb{Q}S_{i,i})^G$$

and by induction hypothesis, we get

$$\tau_i = \tau_0 + \tau_1 - \tau_0 + \cdots + \tau_{i-1} - \tau_{i-2} + dim_{\mathbb{Q}}(\mathbb{Q}S_{i,i})^G.$$

Thus

$$dim_{\mathbb{Q}}(\mathbb{Q}S_{i,i})^G = \tau_i - \tau_{i-1}.$$

Applying again Theorem 5.1.2 we get $dim_{\mathbb{Q}}(\mathbb{Q}S_{t,i})^G = \tau_i - \tau_{i-1}$, for $0 \leq i \leq t'$. $\square$

Now we examine the $\mathbb{Z}$-module $(\mathbb{Z}L_t)^G$.

Proposition 5.1.4. *Let* $0 \leq t \leq n$*, then* $(\mathbb{Z}L_t)^G$ *is a pure submodule of* $\mathbb{Z}L_t^n$*.*

Proof. As usual we just prove that $(\mathbb{Z}L_t)^G \cap a\mathbb{Z}L_t^n \subseteq a(\mathbb{Z}L_t)^G$, for any $a \in \mathbb{Z} \setminus \{0\}$. If $v \in (\mathbb{Z}L_t)^G \cap a\mathbb{Z}L_t^n$ then $v = aw$, with $w \in \mathbb{Z}L_t^n$. Since $v^g = v$, for any $g \in G$, we have that $a(w^g - w) = 0$. As $\mathbb{Z}L_t^n$ is torsion-free, we get $w \in (\mathbb{Z}L_t)^G$. The claim follows. □

We use the previous result to get the analogue of Theorem 5.1.1 for the $\mathbb{Z}$-module $(\mathbb{Z}L_t)^G$.

Proposition 5.1.5. *Let* $0 \leq t \leq n$ *and* $\Omega^t = \{\Delta_1, \cdots, \Delta_{\tau_t}\}$*. Then*

$$span_{\mathbb{Z}}\{\sum_{x \in \Delta_j} x \ : \ j = 1, \cdots, \tau_t\}$$

is a pure submodule of $\mathbb{Z}L_t^n$ *of rank* τ_t*.*

Proof. Let $a \in \mathbb{Z} \setminus \{0\}$ and $v \in span_{\mathbb{Z}}\{\sum_{x \in \Delta_j} x \ : \ j = 1, \cdots, \tau_t\} \cap a\mathbb{Z}L_t^n$, then there exists $w \in \mathbb{Z}L_t^n$ such that $v = aw$. But $v = \sum_{j=1}^{\tau_t} r_j \sum_{x \in \Delta_j} x$ and $w = \sum_{j=1}^{\tau_t} \sum_{x \in \Delta_j} s_x x$, for some r_j and s_x in $\mathbb{Z}$. As L_t^n is a basis of $\mathbb{Z}L_t^n$ and $\sum_{j=1}^{\tau_t} r_j \sum_{x \in \Delta_j} x = \sum_{j=1}^{\tau_t} \sum_{x \in \Delta_j} a s_x x$, we get $r_j = a s_x$, for any $x \in \Delta_j$ and $j = 1, \cdots, \tau_t$. So $w \in span_{\mathbb{Z}}\{\sum_{x \in \Delta_j} x \ : \ j = 1, \cdots, \tau_t\}$. □

Corollary 5.1.6. *Let* $0 \leq t \leq n$ *and* $\Omega^t = \{\Delta_1, \cdots, \Delta_{\tau_t}\}$*. Then*

$$span_{\mathbb{Z}}\{\sum_{x \in \Delta_j} x \ : \ j = 1, \cdots, \tau_t\} = (\mathbb{Z}L_t)^G$$

and its rank is τ_t*.*

Proof. As $span_{\mathbb{Z}}\{\sum_{x \in \Delta_j} x \ : \ j = 1, \cdots, \tau_t\} \subseteq (\mathbb{Z}L_t)^G$, then $rank\,(\mathbb{Z}L_t)^G \geq \tau_t$. Since $(\mathbb{Z}L_t)^G \subseteq (\mathbb{Q}L_t)^G$, it follows that $rank\,(\mathbb{Z}L_t)^G = \tau_t$; applying the Lemma 2.4.14, we get the claim. □

In the next Theorem we find the Smith group of $\epsilon_t^k : (\mathbb{Z}S_t)^G \to (\mathbb{Z}S_k)^G$, which is our main result of this section. As usual, we put $d = k - t$ and s_{tij}^{+d} the polytope of type (k, i) obtained from s_{tij} by d-fold tail extension.

Theorem 5.1.7. *Let $0 \leq t \leq k$ and $t + k \leq n$. Then the Smith group of*

$$\epsilon_t^k : (\mathbb{Z}S_t)^G \to (\mathbb{Z}S_k)^G$$

is isomorphic to

$$(C_{d_0})^{m_0} \times (C_{d_1})^{m_1} \times \cdots \times (C_{d_t})^{m_t} \times \mathbb{Z}^l,$$

where $d_i = \binom{k-i}{t-i}$, $m_i = \tau_i - \tau_{i-1}$, $i = 0, \cdots, t$ and $l = \tau_k - \tau_t$.

Proof. The claim is trivial if $k = t$, since ϵ_t^k is the identity map. So we consider $t \neq k$ and $t + k \leq n$. Select some $0 \leq i \leq t$ and let $C_{ti} = \{c_{ti1}, \cdots, c_{tim_i}\}$ be a basis of $(\mathbb{Z}S_{t,i})^G$. Take $\{s_{ti1}, \cdots, s_{tin_i}\}$ a basis of polytopes of $\mathbb{Z}S_{t,i}^n$, then there exist $a_{il1}, \cdots, a_{iln_i} \in \mathbb{Z}$ such that $c_{til} = \sum_{j=1}^{n_i} a_{ilj} s_{tij}$, with $1 \leq l \leq m_i$. Thus

$$\epsilon_t^k(c_{til}) = \epsilon_t^k(\sum_{j=1}^{n_i} a_{ilj} s_{tij}) = \begin{pmatrix} k-i \\ t-i \end{pmatrix} \sum_{j=1}^{n_i} a_{ilj} s_{tij}^{+d}.$$

It is easy to prove that the maps tail-extension and tail-cutting restrict to the isomorphisms

$$+ : (\mathbb{Z}S_{t,i})^G \to (\mathbb{Z}S_{t+1,i})^G \text{ and } - : (\mathbb{Z}S_{t+1,i})^G \to (\mathbb{Z}S_{t,i})^G,$$

since $+(\mathbb{Z}S_{t,i})^G \subseteq (\mathbb{Z}S_{t+1,i})^G$, $-(\mathbb{Z}S_{t+1,i})^G \subseteq (\mathbb{Z}S_{t,i})^G$ and they are inverse to each other.

So the set $C_{ti}^{+d} = \{(c_{ti1})^{+d}, \cdots, (c_{tim_i})^{+d}\}$, obtained from C_{ti} applying d-times tail-extension map, is a basis of $(\mathbb{Z}S_{k,i})^G$. It follows $(\mathbb{Z}S_{k,i})^G / \epsilon_t^k((\mathbb{Z}S_{t,i})^G) \cong (C_{d_i})^{m_i}$, with $d_i = \binom{k-i}{t-i}$ and $m_i = \tau_i - \tau_{i-1}$.

It follows that

$$\frac{(\mathbb{Z}S_k)^G}{\epsilon_t^k((\mathbb{Z}S_t)^G)} \cong (C_{d_0})^{m_0} \times \cdots \times (C_{d_t})^{m_t} \times \mathbb{Z}^l,$$

where $l = \tau_k - \tau_t$. □

Example 5.1.8. *Let $n = 6$, $t = 1$, $k = 2$ and $G = \langle(1,2,3),(1,2)(4,5)\rangle$. Then*

$$(\mathbb{Z}S_2)^G/\epsilon_1^2(\mathbb{Z}S_1)^G \cong C_2 \times \mathbb{Z}^2.$$

$$(\mathbb{Z}S_1)^G = (\mathbb{Z}S_{1,0})^G \oplus (\mathbb{Z}S_{1,1})^G$$

and

$$(\mathbb{Z}S_2)^G = (\mathbb{Z}S_{2,0})^G \oplus (\mathbb{Z}S_{2,1})^G \oplus (\mathbb{Z}S_{2,2})^G.$$

As usual, for avoid confusion, we denote the set Ω by $\{\alpha_1, \alpha_2, \cdots, \alpha_6\}$ instead $\{1, 2, \cdots, 6\}$.

The G-orbits on L_1^6 are $\Lambda_1 = \{\alpha_1, \alpha_2, \alpha_3\}, \Lambda_2 = \{\alpha_4, \alpha_5\}, \Lambda_3 = \{\alpha_6\}$, while those on L_2^6 are

$$\Delta_1 = \{\{1,2\},\{2,3\},\{1,3\}\}, \Delta_2 = \{\{1,4\},\{2.4\},\{2,5\},\{3,4\},\{1,5\},\{3,5\}\},$$

$$\Delta_3 = \{\{1,6\},\{2,6\},\{3,6\}\}, \Delta_4 = \{\{5,6\},\{4,6\}\}, \Delta_5 = \{\{4,5\}\}.$$

We want to find a basis of $(\mathbb{Z}S_1)^G$. For this purpose we give a $\mathbb{Z}$-basis of $(\mathbb{Z}S_{1,0})^G$ and of $(\mathbb{Z}S_{1,1})^G$.

***1.** The module $(\mathbb{Z}S_{1,0})^G$ is spanned by $\epsilon_0^1(\emptyset) = \sum_{x \in L_1^6} x$.*

***2.** To find a generating set of $(\mathbb{Z}S_{1,1})^G$ we consider the standard basis of polytopes of type $(1,1)$:*

$$\{(\alpha_1 - \alpha_2), (\alpha_1 - \alpha_3), (\alpha_1 - \alpha_4), (\alpha_1 - \alpha_5), (\alpha_1 - \alpha_6)\}.$$

It is easy to see that the elements $v = (\alpha_1 - \alpha_4) + (\alpha_1 - \alpha_5) - 2(\alpha_1 - \alpha_6)$ and $w = (\alpha_1 - \alpha_2) + (\alpha_1 - \alpha_3) - 3(\alpha_1 - \alpha_6)$ are fixed by every $g \in G$. So they are in $(\mathbb{Z}S_{1,1})^G$. On the other hand they are linearly independent and span a pure submodule of $\mathbb{Z}S_{1,1}$. To see this, put $N = span_{\mathbb{Z}}\{v, w\}$ and prove that for any non-zero integer a, $N \cap a\mathbb{Z}S_{1,1} \subseteq aN$. Let $u \in N \cap a\mathbb{Z}S_{1,1}$. Then $u = b_1 v + b_2 w = a \sum_{i=2}^{6} a_i(\alpha_1 - \alpha_i)$, for some $b_1, b_2, a_i \in \mathbb{Z}$. Whence a divides b_1 and b_2. It follows that $u \in aN$.

Since $(\mathbb{Z}S_{1,1})^G$ has rank $\tau_1 - \tau_0 = 2$, by Lemma 2.4.14 we have

$$(\mathbb{Z}S_{1,1})^G = span_{\mathbb{Z}}\{v, w\}.$$

Now we consider the module $(\mathbb{Z}S_2)^G$. The element $\epsilon_0^2(\emptyset) = \sum_{x \in L_2^6} x = \frac{1}{2}\epsilon_1^2(\sum_{x \in L_1^6} x)$ is a basis of $(\mathbb{Z}S_{2,0})^G$. Moreover $(\mathbb{Z}S_{2,1})^G = \epsilon_1^2(\mathbb{Z}S_{1,1})^G$. Remembering Theorem 2.3.8 and Corollary 2.3.9, by direct computation we get

$$\frac{(\mathbb{Z}S_2)^G}{\epsilon_1^2(\mathbb{Z}S_1)^G} \cong C_2 \times \mathbb{Z}^2.$$

5.2 The case $t + k = n$

Here we assume $t + k = n$ and we prove that the Smith groups of

$$\epsilon_t^k : (\mathbb{Z}L_t)^G \to (\mathbb{Z}L_k)^G$$

and

$$\epsilon_t^k : (\mathbb{Z}S_t)^G \to (\mathbb{Z}S_k)^G$$

have the same order (see Theorem 5.2.5).

In chapter 4 we defined the maps $+$ and $-$ between $\mathbb{Q}L_t^n$ and $\mathbb{Q}L_{t+1}^n$. Applying them d-times ($d = k - t$) we got two isomorphisms between $\mathbb{Q}L_t^n$ and $\mathbb{Q}L_k^n$, which we called $+d$ and $-d$. We notice that they do not restrict to isomorphisms between $\mathbb{Z}$-modules $\mathbb{Z}L_t^n$ and $\mathbb{Z}L_k^n$. We clarify this concept with an example.

Example 5.2.1. *Let $\Omega = \{1, 2, 3, 4, 5, 6\}$, $t = 2$ and $k = 4$. For avoid confusion, we denote by α_i the i^{th}-element of Ω. We do the calculation using Magma Computational Algebra System (see Appendix B). Taken*

$$v = -\alpha_1\alpha_2 - \alpha_1\alpha_4 + \alpha_2\alpha_4 + 2\alpha_2\alpha_5 + \alpha_1\alpha_6 + \alpha_4\alpha_6 \in \mathbb{Z}L_2^6,$$

we get $v^{+2} = -\frac{1}{2}\alpha_3\alpha_4\alpha_5\alpha_6 + \frac{3}{2}\alpha_2\alpha_4\alpha_5\alpha_6 + \frac{1}{2}\alpha_1\alpha_3\alpha_5\alpha_6 + \alpha_1\alpha_3\alpha_4\alpha_6 + \frac{1}{2}\alpha_1\alpha_2\alpha_5\alpha_6 + \frac{1}{2}\alpha_2\alpha_3\alpha_4\alpha_6 + \frac{3}{2}\alpha_2\alpha_3\alpha_4\alpha_5 - \alpha_1\alpha_3\alpha_4\alpha_5 - \alpha_1\alpha_2\alpha_3\alpha_4 + \frac{1}{2}\alpha_1\alpha_2\alpha_3\alpha_5 - \frac{1}{2}\alpha_1\alpha_2\alpha_3\alpha_6 \notin \mathbb{Z}L_4^6$

In order to argue on the order of $(\mathbb{Z}L_k)^G/\epsilon_t^k(\mathbb{Z}L_t)^G$ we need to define a new map between $\mathbb{Q}L_t^n$ and $\mathbb{Q}L_k^n$ (and conversely), which restrict to $\mathbb{Z}$-isomorpshim.

We define the new tail-extension $+_N : \mathbb{Q}L_t^n \longrightarrow \mathbb{Q}L_k^n$ in the following way.

We consider the canonical bases L_t^n and L_k^n of $\mathbb{Z}L_t^n$ and $\mathbb{Z}L_k^n$, respectively. For $x \in L_t^n$, denote by $\bar{x}$ the complement of x in Ω. We put $x^{+_N} = \bar{x}$ and we extend linearly.

Similarly, we define the new tail-cutting $-_N : \mathbb{Q}L_k^n \longrightarrow \mathbb{Q}L_t^n$ such that $y^{-_N} = \bar{y}$.

Summarizing,

$$+_N : \begin{cases} \mathbb{Q}L_t^n & \longrightarrow & \mathbb{Q}L_k^n \\ x & \longrightarrow & \bar{x} \end{cases} \qquad\qquad -_N : \begin{cases} \mathbb{Q}L_k^n & \longrightarrow & \mathbb{Q}L_t^n \\ y & \longrightarrow & \bar{y} \end{cases}$$

In the next Theorem we prove that $s_{t,i}^{+_N} = (-1)^i s_{t,i}^{+d}$, where $d = n - 2t$ and $s_{t,i}$ is a polytope of type (t, i), for $i = 0, \cdots, t$.

Theorem 5.2.2. *Let* $0 \le t \le k \le n$ *with* $t + k = n$*. Then for every polytopes* $s_{t,i}$ *of type* (t, i)*, we have* $s_{t,i}^{+_N} = (-1)^i s_{t,i}^{+d}$*, where* $d = n - 2t$*.*

Proof. Let $s_{t,i} = (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)(\gamma_1 + \cdots + \gamma_u)$ be a polytope of type (t, i). Then

$$s_{t,i}^{+d} = (\alpha_1 - \beta_1) \cdots (\alpha_i - \beta_i)(\gamma_1' + \cdots + \gamma_u'),$$

where γ_j' is the complement of γ_j in $\Omega \setminus \{\alpha_1, \cdots, \alpha_i, \beta_1, \cdots, \beta_i\}$, for $j = 0, \cdots, u$.

If $i = 0$ the statement is trivial. We assume $i > 0$. Let x be a t-set such that it appears in $s_{t,i}$ and let $y = \bar{x}$ be the complement of x in Ω. Note that $\gamma_j \subseteq x$ if and only if $\gamma_j' \subseteq y$, for $j = 0, \cdots, u$ and $\alpha_r \in x$ if and only if $\beta_r \in y$, for $0 \leq r \leq i$ (conversely $\beta_r \in x$ if and only if $\alpha_r \in y$). For example, if $x = \{\alpha_1, \cdots, \alpha_i\} \cup \gamma_1$, then $y = \{\beta_1, \cdots, \beta_i\} \cup \gamma_1'$.

The image $s_{t,i}^{+_N}$ is obtained from $s_{t,i}$ by substitution of every α_r with β_r and γ_j with γ_j'. Whence

$$\begin{aligned} s_{t,i}^{+_N} &= (\beta_1 - \alpha_1)\cdots(\beta_i - \alpha_i)(\gamma_1' + \cdots + \gamma_u') \\ &= (-1)^i(\alpha_1 - \beta_1)\cdots(\alpha_i - \beta_i)(\gamma_1' + \cdots + \gamma_u') \\ &= (-1)^i s_{t,i}^{+d} \end{aligned}$$

□

This Theorem justifies the symbols $+_N$ and $-_N$ used to indicate these maps, which we call *new tail-extension* and *new tail-cutting*.

Example 5.2.3. *If $n = 6$, $t = 2$, $k = 4$ and $s_{2,1} = (\alpha_1 - \alpha_3)(\alpha_2 + \alpha_4 + \alpha_5 + \alpha_6)$. Then*

$$s_{2,1}^{+_N} = (\alpha_3 - \alpha_1)(\alpha_4\alpha_5\alpha_6 + \alpha_2\alpha_5\alpha_6 + \alpha_2\alpha_4\alpha_6 + \alpha_2\alpha_4\alpha_5).$$

Remark 5.2.4. *It is easy to see that the maps $+_N$ and $-_N$ restrict to*

$$+_N : (\mathbb{Z}L_t)^G \to (\mathbb{Z}L_k)^G, \qquad -_N : (\mathbb{Z}L_k)^G \to (\mathbb{Z}L_t)^G$$

and

$$+_N : (\mathbb{Z}S_t)^G \to (\mathbb{Z}S_k)^G, \qquad -_N : (\mathbb{Z}S_k)^G \to (\mathbb{Z}S_t)^G.$$

We conclude this section proving that the groups $(\mathbb{Z}L_k)^G/\epsilon_t^k((\mathbb{Z}L_t)^G)$ and $(\mathbb{Z}S_k)^G/\epsilon_t^k((\mathbb{Z}S_t)^G)$ have the same order.

Theorem 5.2.5. *Let $0 \leq t \leq k \leq n$ and $t + k = n$, then the groups $(\mathbb{Z}L_k)^G/\epsilon_t^k((\mathbb{Z}L_t)^G)$ and $(\mathbb{Z}S_k)^G/\epsilon_t^k((\mathbb{Z}S_t)^G)$ have the same order.*

Proof. The proof is given by three steps.

Step 1.

$$(\mathbb{Z}L_k)^G/(\mathbb{Z}S_k)^G \cong (\mathbb{Z}L_t)^G/(\mathbb{Z}S_t)^G.$$

We observe that $(\mathbb{Z}L_t)^G$ and $(\mathbb{Z}S_t)^G$ have the same rank τ_t, the number of G-orbits on L_t^n. So by 2.4.11 there exist a basis $\{v_1, \cdots, v_{\tau_t}\}$ of $(\mathbb{Z}L_t)^G$ and non-zero integers $r_1, \cdots, r_{\tau_t}$ such that $\{r_1 v_1, \cdots, r_{\tau_t} v_{\tau_t}\}$ is a basis of $(\mathbb{Z}S_t^n)^G$. We denote by $v_1^{+N}, \cdots, v_{\tau_t}^{+N}$ the images of $v_1, \cdots, v_{\tau_t}$ by the map new tail-extension. The map new tail-extension is a G-isomorphism between the $\mathbb{Z}$-modules $(\mathbb{Z}L_t)^G$ and $(\mathbb{Z}L_k)^G$. It follows that the set $\{v_1^{+N}, \cdots, v_{\tau_t}^{+N}\}$ is a basis of $(\mathbb{Z}L_k)^G$. Moreover, the restriction of $+_N$ to the $\mathbb{Z}$-module $(\mathbb{Z}S_t)^G$ is an isomorphism between $(\mathbb{Z}S_t)^G$ and $(\mathbb{Z}S_k)^G$, so the set $\{r_1 v_1^{+N}, \cdots, r_{\tau_t} v_{\tau_t}^{+N}\}$ is a basis of $(\mathbb{Z}S_k)^G$. The claim follows.

Step 2.

$$\epsilon_t^k((\mathbb{Z}L_t)^G)/\epsilon_t^k((\mathbb{Z}S_t)^G) \cong (\mathbb{Z}L_t)^G/(\mathbb{Z}S_t)^G.$$

The statement follows immediately from the first isomorphism Theorem, considering the linear map

$$\gamma : (\mathbb{Z}L_t)^G \longrightarrow \epsilon_t^k((\mathbb{Z}L_t)^G)/\epsilon_t^k((\mathbb{Z}S_t)^G)$$

defined by $\gamma(f_t) = \epsilon_t^k(f_t) + \epsilon_t^k((\mathbb{Z}S_t)^G)$. It is obviously surjective and its kernel is $(\mathbb{Z}S_t)^G$.

Step 3. We use second isomorphism Theorem: we have

$$\frac{\frac{(\mathbb{Z}L_k)^G}{\epsilon_t^k((\mathbb{Z}S_t)^G)}}{\frac{(\mathbb{Z}S_k)^G}{\epsilon_t^k((\mathbb{Z}S_t)^G)}} \cong \frac{(\mathbb{Z}L_k)^G}{(\mathbb{Z}S_k)^G} \text{ and } \frac{\frac{(\mathbb{Z}L_k)^G}{\epsilon_t^k((\mathbb{Z}S_t)^G)}}{\frac{\epsilon_t^k((\mathbb{Z}L_t)^G)}{\epsilon_t^k((\mathbb{Z}S_t)^G)}} \cong \frac{(\mathbb{Z}L_k)^G}{\epsilon_t^k((\mathbb{Z}L_t)^G)}$$

By parts (1)-(2) we deduce that the order of $(\mathbb{Z}L_k)^G/\epsilon_t^k((\mathbb{Z}L_t)^G)$ is the same of the order of $(\mathbb{Z}S_k)^G/\epsilon_t^k((\mathbb{Z}S_t)^G)$. $\square$

5.3 Particular cases

The result of Theorem 5.2.5 suggests us the following question. When $t + k = n$, does exist an isomorphism between the finite groups

$$(\mathbb{Z}S_k)^G/\epsilon_t^k(\mathbb{Z}S_t)^G \text{ and } (\mathbb{Z}L_k)^G/\epsilon_t^k(\mathbb{Z}L_t)^G?$$

A positive answer is suggested by some cases (see in particular Theorem 5.3.4) which we are going to describe below and by numerical computational results which confirm the existence of isomorphism for any subgroup $G \subseteq Sym(n)$, with $n \leq 11$ (see Appendix A).

In the sequel G is any permutation subgroup of $Sym(n)$.

To avoid confusion among coefficients and integers of Ω, in this section we rename the elements of Ω putting

$$\Omega = \{\alpha, \beta_1, \cdots, \beta_{n-1}\}.$$

Theorem 5.3.1. *Take $t = 1$, $k = 2$ and $n = 3$. Let*

$$\varphi : \frac{(\mathbb{Z}S_2)^G}{\epsilon_1^2\left((\mathbb{Z}S_1)^G\right)} \to \frac{(\mathbb{Z}L_2)^G}{\epsilon_1^2\left((\mathbb{Z}L_1)^G\right)}$$

be the linear map defined by $\varphi\left(f + \epsilon_1^2\left((\mathbb{Z}S_1)^G\right)\right) = f + \epsilon_1^2\left((\mathbb{Z}L_1)^G\right)$. Then φ is an isomorphism.

Proof. Clearly φ is well defined and a homomorphism. So it is enough to prove that φ is an injection, since the groups $\frac{(\mathbb{Z}S_2)^G}{\epsilon_1^2((\mathbb{Z}S_1)^G)}$ and $\frac{(\mathbb{Z}L_2)^G}{\epsilon_1^2((\mathbb{Z}L_1)^G)}$ have the same order.

We remember that $(\mathbb{Z}S_2)^G = (\mathbb{Z}S_{2,0})^G \oplus (\mathbb{Z}S_{2,1})^G$. Since

$$\epsilon_1^2((\mathbb{Z}S_{1,1})^G) = (\mathbb{Z}S_{2,1})^G$$

and

$$\epsilon_1^2((\mathbb{Z}S_{1,1})^G) \subseteq \epsilon_1^2((\mathbb{Z}S_1)^G),$$

we get

$$(\mathbb{Z}S_2)^G = (\mathbb{Z}S_{2,0})^G + \epsilon_1^2((\mathbb{Z}S_1)^G).$$

Now note that $(\mathbb{Z}S_{2,0})^G = \frac{1}{2}\epsilon_1^2\epsilon_0^1((\mathbb{Z}S_{0,0})^G)$, so

$$(\mathbb{Z}S_2)^G = \epsilon_1^2\left(\frac{1}{2}\epsilon_0^1((\mathbb{Z}S_{0,0})^G) + (\mathbb{Z}S_1)^G\right)$$

Hence, if $f + \epsilon_1^2((\mathbb{Z}S_1)^G) \in Ker\,\varphi$ then, for some $f_0 \in (\mathbb{Z}S_{0,0})^G$ and $f_1 \in (\mathbb{Z}S_1)^G$, we have

$$f = \epsilon_1^2\left(\frac{1}{2}\epsilon_0^1(f_0) + f_1\right) \in (\mathbb{Z}S_2)^G \cap \epsilon_1^2\left((\mathbb{Z}L_1)^G\right).$$

Since ϵ_1^2 is injective we get $\frac{1}{2}\epsilon_0^1(f_0) + f_1 \in (\mathbb{Z}L_1)^G$.

It follows

$$\frac{1}{2}\epsilon_0^1(f_0) \in (\mathbb{Z}L_1)^G.$$

The latter means that for the inner product we have

$$< \frac{1}{2}\epsilon_0^1(f_0), x >= \frac{1}{2} < f_0, \partial_1^0(x) >= \frac{1}{2} < f_0, \emptyset > \in \mathbb{Z}$$

for all $x \in L_1^3$. Thus f_0 is an even multiple of $\emptyset$ and $\frac{1}{2}\epsilon_0^1(f_0) \in \epsilon_0^1((\mathbb{Z}S_{0,0})^G)$. We conclude that $f \in \epsilon_1^2\left((\mathbb{Z}S_1)^G\right)$. □

Remark 5.3.2. *We observe that the injectivity is independent from n, that is φ is injective for any n, when $t = 1$ and $k = 2$.*

Theorem 5.3.3. *Let $t = 3$, $k = 4$ and $n = 7$. Then the map*

$$\varphi : \frac{(\mathbb{Z}S_4)^G}{\epsilon_3^4\left((\mathbb{Z}S_3)^G\right)} \longrightarrow \frac{(\mathbb{Z}L_4)^G}{\epsilon_3^4\left((\mathbb{Z}L_3)^G\right)}$$

defined by $\varphi\left(f + \epsilon_3^4((\mathbb{Z}S_3)^G)\right) = f + \epsilon_3^4\left((\mathbb{Z}L_3)^G\right)$ is an isomorphism.

Proof. Clearly φ is a linear map well defined, so by Lemma 5.2.5 it is enough to prove that it is an injection. First we consider a standard basis $\mathcal{B}$ of polytopes of type $(2,2)$. Put $\Omega = \{\alpha, \beta_1, \beta_2, \cdots, \beta_6\}$ and $\mathcal{B} = \{s_1, s_2, \cdots, s_{14}\}$, where

$s_1 = (\alpha-\beta_1)(\beta_2-\beta_3)$, $s_2 = (\alpha-\beta_1)(\beta_2-\beta_4)$, $s_3 = (\alpha-\beta_1)(\beta_2-\beta_5)$,
$s_4 = (\alpha-\beta_1)(\beta_2-\beta_6)$, $s_5 = (\alpha-\beta_2)(\beta_1-\beta_3)$, $s_6 = (\alpha-\beta_2)(\beta_1-\beta_4)$,
$s_7 = (\alpha-\beta_2)(\beta_1-\beta_5)$, $s_8 = (\alpha-\beta_2)(\beta_1-\beta_6)$, $s_9 = (\alpha-\beta_3)(\beta_1-\beta_4)$,
$s_{10} = (\alpha-\beta_3)(\beta_1-\beta_5)$, $s_{11} = (\alpha-\beta_3)(\beta_1-\beta_6)$, $s_{12} = (\alpha-\beta_4)(\beta_1-\beta_5)$,
$s_{13} = (\alpha-\beta_4)(\beta_1-\beta_6)$, $s_{14} = (\alpha-\beta_5)(\beta_1-\beta_6)$
are the standard polytopes of type $(2,2)$.

Now let $f + \epsilon_3^4\left((\mathbb{Z}S_3)^G\right) \in Ker\,\varphi$. We want to prove that $f \in \epsilon_3^4\left((\mathbb{Z}S_3)^G\right)$. For this purpose we observe that

$$(\mathbb{Z}S_4)^G = \epsilon_3^4\left(\frac{1}{4}(\mathbb{Z}S_{3,0})^G + \frac{1}{3}(\mathbb{Z}S_{3,1})^G + \frac{1}{2}(\mathbb{Z}S_{3,2})^G + (\mathbb{Z}S_{3,3})^G\right).$$

So

$$f = \epsilon_3^4\left(\frac{1}{4}f_{30} + \frac{1}{3}f_{31} + \frac{1}{2}f_{32} + f_{33}\right) \in \epsilon_3^4\left((\mathbb{Z}L_3)^G\right),$$

with $f_{30} \in (\mathbb{Z}S_{3,0})^G, f_{31} \in (\mathbb{Z}S_{3,1})^G, f_{32} \in (\mathbb{Z}S_{3,2})^G$ and $f_{33} \in (\mathbb{Z}S_{3,3})^G$. By injectivity of ϵ_3^4 we have

$$h = \frac{1}{4}f_{30} + \frac{1}{3}f_{31} + \frac{1}{2}f_{32} \in (\mathbb{Z}L_3)^G. \tag{5.4}$$

In particular $4h \in (\mathbb{Z}L_3)^G$ and so

$$\frac{4}{3}f_{31} \in (\mathbb{Z}L_3)^G. \tag{5.5}$$

Since $f_{31} \in (\mathbb{Z}S_{3,1})^G$, there exists $f_{11} \in (\mathbb{Z}S_{1,1})^G$ such that $f_{31} = \epsilon_1^3(f_{11})$ and $f_{11} = \sum_{j=1}^{6} z_j(\alpha - \beta_j)$, where $\{\alpha-\beta_1, \alpha-\beta_2, \cdots, \alpha-\beta_6\}$ is a standard basis of polytopes of $\mathbb{Z}S_{1,1}$.

Then chosen $x = \{\beta_{i_1}, \beta_{i_2}, \beta_{i_3}\}$ and $y = \{\alpha, \beta_{i_4}, \beta_{i_5}\}$ two distinct sets in L_3^7, we have

$$\frac{4}{3} < f_{31}, x + y > \in \mathbb{Z}.$$

Using the equation 4.6, we have

$$\frac{4}{3} < f_{31}, x+y >= \frac{4}{3}(-z_{i_1} - z_{i_2} - z_{i_3} - z_{i_4} - z_{i_5} + \sum_{r=1}^{6} z_r).$$

Whence $z_j \equiv 0 \, mod \, 3$, for any $1 \leq j \leq 6$. It follows $\frac{1}{3} f_{31} \in (\mathbb{Z}S_{3,1})^G$.

To this point it remains to prove that $h' = h - \frac{1}{3} f_{31} = \frac{1}{4} f_{30} + \frac{1}{2} f_{32} \in (\mathbb{Z}S_3)^G$. From equations 5.4 and 5.5 we deduce

$$h' \in (\mathbb{Z}L_3)^G,$$

whence $2h' = \frac{1}{2} f_{30} + f_{32} \in (\mathbb{Z}L_3)^G$ and so $h_{30} = \frac{1}{2} f_{30} \in (\mathbb{Z}L_3)^G \cap E^7_{3,0} = (\mathbb{Z}S_{3,0})^G$. Replacing it in h' we have $h' = \frac{1}{2} h_{30} + \frac{1}{2} f_{32}$. We can suppose

$$h' = \frac{1}{2}(2\zeta_0 + \rho_0) s^3_{\emptyset} + \frac{1}{2} \sum_{i=1}^{14} (2\zeta_i + \rho_i) s^3_i,$$

where $\zeta_0, \zeta_i \in \mathbb{Z}$, $\rho_0, \rho_i \in \{0,1\}$, $s^3_{\emptyset}$ is the polytope of type $(3,0)$, s_i as above and $s^3_i = \epsilon^3_2(s_i)$. Our goal is to prove that $\rho_0 = \rho_1 = \cdots = \rho_{14} = 0$.

For this purpose, put $h'' = \frac{1}{2}\rho_0 s^3_{\emptyset} + \frac{1}{2}\sum_{i=1}^{14} \rho_i s^3_i$, for any $x, y \in L^7_3$ we have

$$< h'', x - y >= \frac{1}{2} < \rho_0 s^3_{\emptyset}, x - y > + \frac{1}{2} < \sum_{i=1}^{14} \rho_i s^3_i, x - y >= \frac{1}{2} < \sum_{i=1}^{14} \rho_i s^3_i, x - y > \in \mathbb{Z}.$$

If $x = \{\alpha, \beta_1, \beta_2\}$ and $y = \{\beta_3, \beta_4, \beta_5\}$ then

$$< h'', x - y >= \frac{1}{2}(\sum_{i=9}^{14} \rho_i - \rho_9 - \rho_{10} - \rho_{12}) = \frac{1}{2}(\rho_{11} + \rho_{13} + \rho_{14}) \in \mathbb{Z}. \tag{5.6}$$

If $x = \{\alpha, \beta_1, \beta_2\}$ and $y = \{\beta_3, \beta_4, \beta_6\}$ then

$$< h'', x - y >= \frac{1}{2}(\sum_{i=9}^{14} \rho_i - \rho_9 - \rho_{11} - \rho_{13}) = \frac{1}{2}(\rho_{10} + \rho_{12} + \rho_{14}) \in \mathbb{Z}. \tag{5.7}$$

If $x = \{\alpha, \beta_1, \beta_2\}$ and $y = \{\beta_3, \beta_5, \beta_6\}$ then

$$< h'', x - y >= \frac{1}{2}(\sum_{i=9}^{14} \rho_i - \rho_{10} - \rho_{11} - \rho_{14}) = \frac{1}{2}(\rho_9 + \rho_{12} + \rho_{13}) \in \mathbb{Z}. \tag{5.8}$$

If $x = \{\alpha, \beta_1, \beta_2\}$ and $y = \{\beta_4, \beta_5, \beta_6\}$ then

$$< h'', x - y >= \frac{1}{2}(\sum_{i=9}^{14} \rho_i - \rho_{12} - \rho_{13} - \rho_{14}) = \frac{1}{2}(\rho_9 + \rho_{10} + \rho_{11}) \in \mathbb{Z}. \tag{5.9}$$

If $x = \{\alpha, \beta_1, \beta_3\}$ and $y = \{\beta_2, \beta_4, \beta_5\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_6 + \rho_7 + \rho_8 + \rho_{12} + \rho_{13} + \rho_{14} - \rho_6 - \rho_7 - \rho_{12}) = \frac{1}{2}(\rho_8 + \rho_{13} + \rho_{14}) \in \mathbb{Z}. \tag{5.10}$$

From equations 5.6 and 5.10, we have $\frac{1}{2}(\rho_{11} - \rho_8) \in \mathbb{Z}$, so

$$\rho_8 = \rho_{11}.$$

If $x = \{\alpha, \beta_1, \beta_3\}$ and $y = \{\beta_2, \beta_4, \beta_6\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_6 + \rho_7 + \rho_8 + \rho_{12} + \rho_{13} + \rho_{14} - \rho_6 - \rho_8 - \rho_{13}) = \frac{1}{2}(\rho_7 + \rho_{12} + \rho_{14}) \in \mathbb{Z}. \tag{5.11}$$

From equations 5.7 and 5.11 we have $\frac{1}{2}(\rho_{10} - \rho_7) \in \mathbb{Z}$, so

$$\rho_{10} = \rho_7.$$

Again if $x = \{\alpha, \beta_1, \beta_3\}$ and $y = \{\beta_2, \beta_5, \beta_6\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_6 + \rho_7 + \rho_8 + \rho_{12} + \rho_{13} + \rho_{14} - \rho_7 - \rho_8 - \rho_{14}) = \frac{1}{2}(\rho_6 + \rho_{12} + \rho_{13}) \in \mathbb{Z}. \tag{5.12}$$

From equations 5.8 and 5.12, $\frac{1}{2}(\rho_6 - \rho_9) \in \mathbb{Z}$, thus

$$\rho_6 = \rho_9.$$

If $x = \{\alpha, \beta_1, \beta_4\}$ and $y = \{\beta_2, \beta_3, \beta_5\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_5 + \rho_7 + \rho_8 + \rho_{10} + \rho_{11} + \rho_{14} - \rho_5 - \rho_7 - \rho_{10}) = \frac{1}{2}(\rho_8 + \rho_{11} + \rho_{14}) \in \mathbb{Z}. \tag{5.13}$$

From 5.10 and 5.13, $\frac{1}{2}(\rho_{11} - \rho_{13}) \in \mathbb{Z}$, thus

$$\rho_{11} = \rho_{13},$$

moreover from 5.13 and $\rho_8 = \rho_{11} = \rho_{13}$, we have $\frac{1}{2}(\rho_8 + \rho_{11} + \rho_{14}) = \frac{1}{2}(2\rho_8 + \rho_{14}) \in \mathbb{Z}$, so

$$\rho_{14} = 0.$$

If $x = \{\alpha, \beta_1, \beta_4\}$ and $y = \{\beta_3, \beta_5, \beta_6\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_5 + \rho_7 + \rho_8 + \rho_{10} + \rho_{11} + \rho_{14} - \rho_{10} - \rho_{11} - \rho_{14}) = \frac{1}{2}(\rho_5 + \rho_7 + \rho_8) \in \mathbb{Z}. \tag{5.14}$$

From equations 5.14, 5.9, $\rho_{11} = \rho_8$ and $\rho_{10} = \rho_7$, we have $\frac{1}{2}(\rho_9 - \rho_5) \in \mathbb{Z}$, so

$$\rho_9 = \rho_5.$$

If $x = \{\alpha, \beta_1, \beta_5\}$ and $y = \{\beta_2, \beta_3, \beta_4\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_5 + \rho_6 + \rho_8 + \rho_9 + \rho_{11} + \rho_{13} - \rho_5 - \rho_6 - \rho_9) = \frac{1}{2}(\rho_8 + \rho_{11} + \rho_{13}) \in \mathbb{Z}. \tag{5.15}$$

From equation 5.15 and $\rho_8 = \rho_{11} = \rho_{13}$, we have $\frac{1}{2}(3\rho_8) \in \mathbb{Z}$ and so

$$\rho_8 = 0,$$

whence

$$\rho_8 = \rho_{11} = \rho_{13} = 0.$$

If $x = \{\alpha, \beta_1, \beta_6\}$ and $y = \{\beta_2, \beta_3, \beta_4\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_5 + \rho_6 + \rho_7 + \rho_9 + \rho_{10} + \rho_{12} - \rho_5 - \rho_6 - \rho_9) = \frac{1}{2}(\rho_7 + \rho_{10} + \rho_{12}) \in \mathbb{Z}. \tag{5.16}$$

From equation 5.16 and $\rho_7 = \rho_{10}$ we have $\frac{1}{2}(2\rho_7 + \rho_{12}) \in \mathbb{Z}$, so

$$\rho_{12} = 0$$

moreover from equation 5.7 and $\rho_{12} = \rho_{14} = 0$,

$$\frac{1}{2}(\rho_{10} + \rho_{12} + \rho_{14}) = \frac{1}{2}\rho_{10} \in \mathbb{Z},$$

hence

$$\rho_{10} = 0$$

and by equation 5.9 and $\rho_{11} = \rho_{10} = 0$,

$$\rho_9 = 0.$$

If $x = \{\alpha, \beta_2, \beta_3\}$ and $y = \{\beta_1, \beta_4, \beta_5\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_2 + \rho_3 + \rho_4 - \rho_2 - \rho_3 + \rho_{13} + \rho_{14}) = \frac{1}{2}(\rho_4 + \rho_{13} + \rho_{14}) \in \mathbb{Z}. \tag{5.17}$$

Since $\rho_{13} = \rho_{14} = 0$, we have

$$\rho_4 = 0.$$

If $x = \{\alpha, \beta_2, \beta_3\}$ and $y = \{\beta_1, \beta_4, \beta_6\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_2 + \rho_3 + \rho_4 - \rho_2 - \rho_4 + \rho_{12}) = \frac{1}{2}(\rho_3 + \rho_{12}) \in \mathbb{Z}. \tag{5.18}$$

By equation 5.18 and $\rho_{12} = 0$ we have

$$\rho_3 = 0.$$

Again if $x = \{\alpha, \beta_2, \beta_3\}$ and $y = \{\beta_1, \beta_5, \beta_6\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_2 + \rho_3 + \rho_4 - \rho_3 - \rho_4) = \frac{1}{2}\rho_2 \in \mathbb{Z}, \tag{5.19}$$

so

$$\rho_2 = 0.$$

Finally if $x = \{\alpha, \beta_2, \beta_4\}$ and $y = \{\beta_1, \beta_5, \beta_6\}$ then

$$< h'', x - y >= \frac{1}{2}(\rho_1 + \rho_3 + \rho_4 - \rho_9 - \rho_3 - \rho_4) = \frac{1}{2}(\rho_1 - \rho_9) \in \mathbb{Z}, \tag{5.20}$$

whence

$$\rho_1 = 0.$$

We conclude that $h'' = \frac{1}{2}\rho_0 s_\emptyset^3 \in (\mathbb{Z}L_3)^G$, hence

$$\rho_0 = 0$$

and this concludes the proof. $\square$

Next Theorem considers a more general situation.

Theorem 5.3.4. *Let $t = 2$, $k = n - 2$ and $gcd(n, 3) = 1$. Let*

$$\varphi : \frac{(\mathbb{Z}S_{n-2})^G}{\epsilon_2^{n-2}\left((\mathbb{Z}S_2)^G\right)} \longrightarrow \frac{(\mathbb{Z}L_{n-2})^G}{\epsilon_2^{n-2}\left((\mathbb{Z}L_2)^G\right)}$$

be a map defined by $\varphi(f + \epsilon_2^{n-2}\left((\mathbb{Z}S_2)^G\right)) = f + \epsilon_2^{n-2}\left((\mathbb{Z}L_2)^G\right)$. Then φ is an isomorphism.

Proof. Clearly φ is a linear map well defined. Since $\frac{(\mathbb{Z}S_{n-2})^G}{\epsilon_2^{n-2}\left((\mathbb{Z}S_2)^G\right)}$ and $\frac{(\mathbb{Z}L_{n-2})^G}{\epsilon_2^{n-2}\left((\mathbb{Z}L_2)^G\right)}$ have the same order, it is enough to prove that φ is injective. Note that, by proof of Theorem 4.5.1, we have

$$\begin{aligned}(\mathbb{Z}S_{n-2})^G =& (\mathbb{Z}S_{n-2,0})^G \oplus (\mathbb{Z}S_{n-2,1})^G \oplus (\mathbb{Z}S_{n-2,2})^G = \\ &= \frac{2}{(n-2)(n-3)}\epsilon_2^{n-2}\left((\mathbb{Z}S_{2,0})^G\right) + \frac{1}{(n-3)}\epsilon_2^{n-2}\epsilon_1^2\left((\mathbb{Z}S_{1,1})^G\right) + \epsilon_2^{n-2}\left((\mathbb{Z}S_{2,2})^G\right) = \\ &= \epsilon_2^{n-2}\left(\frac{2}{(n-2)(n-3)}(\mathbb{Z}S_{2,0})^G + \frac{1}{(n-3)}\epsilon_1^2\left((\mathbb{Z}S_{1,1})^G\right) + (\mathbb{Z}S_{2,2})^G\right)\end{aligned}$$

hence if $f + \epsilon_2^{n-2}((\mathbb{Z}S_2)^G) \in Ker\,\varphi$ then

$$f = \epsilon_2^{n-2}\left(\frac{2}{(n-2)(n-3)}f_{20} + \frac{1}{(n-3)}\epsilon_1^2(f_{11}) + f_{22}\right) \in \epsilon_2^{n-2}\left((\mathbb{Z}L_2)^G\right)$$

with $f_{20} \in (\mathbb{Z}S_{2,0})^G$, $f_{11} \in (\mathbb{Z}S_{1,1})^G$ and $f_{22} \in (\mathbb{Z}S_{2,2})^G$. This implies

$$h = \frac{2}{(n-2)(n-3)}f_{20} + \frac{1}{(n-3)}\epsilon_1^2(f_{11}) \in (\mathbb{Z}L_2)^G \tag{5.21}$$

by injectivity of ϵ_2^{n-2}. We want to prove that $\frac{2}{(n-2)(n-3)}f_{20} \in (\mathbb{Z}S_{2,0})^G$ and $\frac{1}{(n-3)}\epsilon_1^2(f_{11}) \in (\mathbb{Z}S_{2,1})^G$, so that $h \in (\mathbb{Z}S_2)^G$.

Clearly

$$(n-3)h = \frac{2}{n-2}f_{20} + \epsilon_1^2(f_{11}) \in (\mathbb{Z}L_2)^G, \tag{5.22}$$

whence

$$\frac{2}{n-2}f_{20} \in (\mathbb{Z}S_{2,0})^G.$$

Put $h_{20} = \frac{2}{n-2}f_{20}$, by definition

$$h_{20} = bs_{20}$$

with $s_{20} = \sum_{x\in L_2^n} x$ polytope of type $(2,0)$ and $b \in \mathbb{Z}$. We can write

$$h = \frac{1}{n-3}h_{20} + \frac{1}{n-3}\epsilon_1^2(f_{11}) \in (\mathbb{Z}L_2)^G,$$

with $h_{20} \in (\mathbb{Z}S_{2,0})^G$ and $f_{11} \in (\mathbb{Z}S_{1,1})^G$.

It is enough to prove that $b \equiv 0\, mod(n-3)$. We consider $\{\alpha-\beta_1, \alpha-\beta_2, \cdots, \alpha-\beta_{n-1}\}$ a standard basis of polytopes of type $(1,1)$. Let $x = \{\alpha, \beta_i\}$, $y = \{\alpha, \beta_j\}$, with $i \neq j$ and $1 \leq i, j \leq n-1$.

It is easy to see that $\frac{1}{n-3} < h_{20}, x-y >= \frac{1}{n-3}(b-b) = 0$. It follows

$$< h, x-y >= \frac{1}{n-3} < \epsilon_1^2(f_{11}), x-y >= \frac{1}{n-3} < f_{11}, \partial_2^1(x-y) >= \frac{1}{n-3} < f_{11}, \beta_i-\beta_j > \tag{5.23}$$

is integer as $h \in (\mathbb{Z}L_2)^G$. Since $f_{11} \in (\mathbb{Z}S_{1,1})^G$, we have

$$f_{11} = z_1(\alpha-\beta_1) + z_2(\alpha-\beta_2) + \cdots + z_{n-1}(\alpha-\beta_{n-1}),$$

for some integer $z_1, \cdots, z_{n-1}$. As $f_{11} = (z_1+z_2+\cdots+z_{n-1})\alpha - z_1\beta_1 - z_2\beta_2 - \cdots - z_{n-1}\beta_{n-1}$, then the inner product 5.23 becomes

$$< h, x-y >= \frac{1}{n-3}(-z_i + z_j) \in \mathbb{Z},$$

thus

$$-z_i + z_j \equiv 0\, mod(n-3). \tag{5.24}$$

Moreover

$$\begin{aligned} < h, x > &= \frac{1}{n-3} < h_{20}, x > + \frac{1}{n-3} < \epsilon_1^2(f_{11}), x >= \frac{1}{n-3} < h_{20}, x > + \frac{1}{n-3} < f_{11}, \partial_2^1(x) >= \\ &= \frac{1}{n-3} < h_{20}, x > + \frac{1}{n-3} < f_{11}, \alpha+\beta_i >= \frac{1}{n-3}b + \frac{1}{n-3}(z_1 + \cdots + z_{n-1} - z_i) \in \mathbb{Z}, \end{aligned}$$

whence

$$b + z_1 + \cdots + z_{n-1} - z_i \equiv 0\, mod(n-3). \tag{5.25}$$

Now let $w = \{\beta_i, \beta_j\}$, with $1 \leq i, j \leq n-1$ and $i \neq j$, so $< h, w >= \frac{1}{n-3} < h_{20}, w >$ $+ \frac{1}{n-3} < \epsilon_1^2(f_{11}), w >= \frac{1}{n-3}b + \frac{1}{n-3} < f_{11}, \partial_2^1(w) >= \frac{1}{n-3}b + \frac{1}{n-3} < f_{11}, \beta_i + \beta_j >=$

$\frac{1}{n-3}(b - z_i - z_j)$. So we conclude

$$b - z_i - z_j \equiv 0 \, mod(n-3) \tag{5.26}$$

From equations 5.24 and 5.26 we have

$$b - 2z_i \equiv 0 \, mod(n-3). \tag{5.27}$$

Again, from 5.26 and 5.25, for each set of three distinct indexes i, j, l, where $1 \leq i, j, l \leq n-1$ we have

$$b + z_1 + \cdots + z_{n-1} - z_i + \sum_{j=1, j\neq i,l}^{n-1} (b - z_l - z_j) = b + (n-3)b + z_l - (n-3)z_l \equiv 0 \, mod(n-3),$$

thus

$$b + z_l \equiv 0 \, mod(n-3) \tag{5.28}$$

Finally, by 5.27 and 5.28, we can deduce

$$b - 2z_l + 2b + 2z_l = 3b \equiv 0 \, mod(n-3)$$

for each $1 \leq l \leq n-1$. Since $gcd(n, 3) = 1$ by hypothesis, we conclude

$$b \equiv 0 \, mod(n-3).$$

This concludes the proof. □

We conclude this section giving the following conjecture

Conjecture 5.3.5. *If* $0 \leq t \leq k \leq n$ *and* $t + k = n$, *then*

$$\frac{(\mathbb{Z}L_k^n)^G}{\epsilon_t^k(\mathbb{Z}L_t^n)^G} \cong (C_{d_0})^{m_0} \times (C_{d_1})^{m_1} \times \cdots \times (C_{d_t})^{m_t}, \tag{5.29}$$

where $d_i = \binom{k-i}{t-i}$ *and* $m_i = \tau_i - \tau_{i-1}$, *for* $i = 0, \cdots, t$.

In general this statement is not true for $t+k<n$.

Example 5.3.6. *If $n=8$, $t=2$, $k=3$ and*

$$G=\langle(1,2,3,8)(4,6,7,5),(5,8,6),(1,4,7),(2,6)(5,8),(2,8)(5,6),(1,7)(3,4),(1,4)(3,7)\rangle,$$

we consider the bases above introduced $\mathcal{B}_{\Omega^t}$ and $\mathcal{B}_{\Omega^k}$ (see the beginning of chapter) and we write the matrix X^+_{23} associated to the map

$$\epsilon^3_2 : (\mathbb{Z}L^8_2)^G \to (\mathbb{Z}L^8_3)^G,$$

with respect to these bases. By direct computation with Magma Computational Algebra System, we get $X^+_{23}=\begin{pmatrix}3 & 0\\ 1 & 2\end{pmatrix}$. Its invariant factors are 1 and 6. So that

$$\frac{(\mathbb{Z}L^8_3)^G}{\epsilon^3_2(\mathbb{Z}L^8_2)^G}\cong C_6.$$

If the equation 5.29 is true for $t+k<n$, then

$$\frac{(\mathbb{Z}L^8_3)^G}{\epsilon^3_2(\mathbb{Z}L^8_2)^G}\cong (C_{d_0})^{m_0}\times(C_{d_1})^{m_1}\times(C_{d_2})^{m_2},$$

with $d_0=3$, $d_1=2$, $d_2=1$, $m_0=1$, $m_1=0$ and $m_2=1$. So $C_6\cong C_3$. Contradiction.

5.4 Matrices X^-_{tk} and X^+_{tk}

In this last section we report some consideration about the matrices $X^+_{tk}=(x^+_{ij})$ and $X^-_{tk}=(x^-_{ji})$ of the tactical decomposition (Ω^t,Ω^k). Here, we follow closely the original proof of Wilson's Theorem ([15]) for a diagonal form of W_{tk}. Actually we will prove that the Equations 5.30 and 5.31 hold in order to get that the matrices

$$M^+_{tk}=\left(X^+_{0k}|X^+_{1k}|\cdots|X^+_{tk}\right)$$

and

$$M^-_{tk} = \begin{pmatrix} X^-_{0k} \\ X^-_{1k} \\ \cdots \\ X^-_{tk} \end{pmatrix}$$

have rank τ_t and index 1. See chapter 3, Proposition 3.1.3.

We begin giving an example for matrices $X^+_{tk} = (x^+_{ij})$ and $X^-_{tk} = (x^-_{ji})$ where $n = 6$, $t = 2$ and $G = \langle(1,2,3),(1,2)(4,5)\rangle$. We recall that $X^+_{tk} = (x^+_{ij})$ and $X^-_{tk} = (x^-_{ji})$ are the matrices associated to $\epsilon^k_t : (\mathbb{Z}L^n_t)^G \longrightarrow (\mathbb{Z}L^n_k)^G$ and $\partial^t_k : (\mathbb{Z}L^n_k)^G \longrightarrow (\mathbb{Z}L^n_t)^G$ with respect to the bases above introduced $\mathcal{B}_{\Omega^t}$ and $\mathcal{B}_{\Omega^k}$ (see the beginning of chapter).

Example 5.4.1. *Let $n = 6$, $t = 2$ and $G = \langle(1,2,3),(1,2)(4,5)\rangle$. Then the 2-orbits are*

$$\Delta_1 = \{\{1,2\},\{2,3\},\{1,3\}\}, \Delta_2 = \{\{1,4\},\{2.4\},\{2,5\},\{3,4\},\{1,5\},\{3,5\}\},$$

$$\Delta_3 = \{\{1,6\},\{2,6\},\{3,6\}\}, \Delta_4 = \{\{5,6\},\{4,6\}\}, \Delta_5 = \{\{4,5\}\}$$

and the 4-orbits

$$\Gamma_1 = \{\{3,4,5,6\},\{1,4,5,6\},\{2,4,5,6\}\},$$

$$\Gamma_2 = \{\{2,3,5,6\},\{1,3,5,6\},\{1,3,4,6\},\{1,2,5,6\},\{2,3,4,6\},\{1,2,4,6\}\},$$

$$\Gamma_3 = \{\{2,3,4,5\},\{1,3,4,5\},\{1,2,4,5\}\}, \Gamma_4 = \{\{1,2,3,4\},\{1,2,3,5\}\}, \Gamma_5 = \{\{1,2,3,6\}\}.$$

So we have that

$$(\mathbb{Z}L_2)^G = span_{\mathbb{Z}}(\sum_{x\in\Delta_j} x \ : \ j = 1,\cdots,5),$$

and

$$(\mathbb{Z}L_4)^G = span_{\mathbb{Z}}(\sum_{y\in\Gamma_i} y \ : \ i = 1,\cdots,5).$$

Then

$$X_{24}^{+} = X_{24}^{-} = \begin{pmatrix} 0 & 2 & 1 & 2 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 1 & 4 & 0 & 0 & 1 \\ 3 & 3 & 0 & 0 & 0 \\ 3 & 0 & 3 & 0 & 0 \end{pmatrix}.$$

To determine the matrix $M_{14}^{+} = \left(X_{04}^{+} | X_{14}^{+} \right)$ *we consider the* 1*-orbits*

$$\{1,2,3\} \qquad \{4,5\} \qquad \{6\}.$$

Then

$$M_{14}^{+} = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 2 & 2 & 0 \\ 1 & 3 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{pmatrix}.$$

Now to prove that matrices M_{tk}^{+} and M_{tk}^{-} have index 1 we introduce some Lemmas. Denoting by H_t the incidence matrix between t-subsets and t-orbits, that is $H_t(T, \Delta_j) = 1$ if $T \in \Delta_j$ and $H_t(T, \Delta_j) = 0$ otherwise; put $H_t^T H_t = N_t$; it is easy to recognize that N_t is the diagonal matrix such that $N_t(j, j)$ is the number of elements in the orbit Δ_j. We have the following results (see also [5] section 1.3, and [13]).

Lemma 5.4.2. *[13](Lemma 3.1)*

1. $H_k X_{tk}^{+} = W_{tk}^T H_t$ *and* $H_t X_{tk}^{-} = W_{tk} H_k$;
2. $(X_{tk}^{+})^T N_k X_{tk}^{+} = H_t^T W_{tk} W_{tk}^T H_t$ *and* $(X_{tk}^{-})^T N_t X_{tk}^{-} = H_k^T W_{tk}^T W_{tk} H_k$;
3. $N_k X_{tk}^{+} = (X_{tk}^{-})^T N_t, \qquad N_k (X_{tk}^{+} X_{tk}^{-}) = (X_{tk}^{-})^T N_t X_{tk}^{-},$

   $N_t (X_{tk}^{-} X_{tk}^{+}) = (X_{tk}^{+})^T N_k X_{tk}^{+}$ *and* $N_t (X_{tk}^{-} X_{tk}^{+}) N_t^{-1} = (X_{tk}^{-} X_{tk}^{+})^T$.

Lemma 5.4.3. *Let* $0 \le j \le t \le k \le n$*, then*

$$X_{jt}^{-} X_{tk}^{-} = \binom{k-j}{t-j} X_{jk}^{-} \tag{5.30}$$

Proof. By Lemmas 5.4.2 and 3.1.2,

$$N_j X_{jt}^{-} X_{tk}^{-} = H_j^T H_j X_{jt}^{-} X_{tk}^{-} = H_j^T W_{jt} H_t X_{tk}^{-} = H_j^T W_{jt} W_{tk} H_k =$$

$$= H_j^T \binom{k-j}{t-j} W_{jk} H_k = \binom{k-j}{t-j} H_j^T H_j X_{jk}^{-} = \binom{k-j}{t-j} N_j X_{jk}^{-}.$$

It follows

$$X_{jt}^{-} X_{tk}^{-} = \binom{k-j}{t-j} X_{jk}^{-}$$

because N_j is non-singular. □

Lemma 5.4.4. *Let* $0 \le j \le t \le k \le n$*, then*

$$X_{tk}^{+} X_{jt}^{+} = \binom{k-j}{t-j} X_{jk}^{+} \tag{5.31}$$

Proof. By Lemmas 5.4.2 and 3.1.2,

$$N_k X_{tk}^{+} X_{jt}^{+} = H_k^T H_k X_{tk}^{+} X_{jt}^{+} = H_k^T W_{tk}^T H_t X_{jt}^{+} = H_k^T W_{tk}^T W_{jt}^T H_j =$$

$$= H_k^T \binom{k-j}{t-j} W_{jk}^T H_j = \binom{k-j}{t-j} H_k^T H_k X_{jk}^{+} = \binom{k-j}{t-j} N_k X_{jk}^{+}.$$

It follows

$$X_{tk}^{+} X_{jt}^{+} = \binom{k-j}{t-j} X_{jk}^{+}$$

because N_k is non-singular. □

We introduce now a new matrix

Definition 5.4.5. *Let $0 \leq t \leq k \leq n$ and $t+k \leq n$. Then for any $0 \leq i \leq t$ we define $\bar{X}_{ik}$ the matrix whose rows are indexed by all G-orbits Λ on L_i^n and the columns by G-orbits Γ on L_k^n, such that*

$$\bar{X}_{ik}(\Lambda, \Gamma) = |\{y \in \Gamma \,:\, y \cap x = \emptyset, \text{for one fixed } x \in \Lambda\}|.$$

Lemma 5.4.6. *Let $0 \leq t \leq k \leq n$ and $t+k \leq n$. Then for any $0 \leq i \leq t$*

$$H_i \bar{X}_{ik} = \bar{W}_{ik} H_k,$$

where for each i-set x and k-set y

$$\bar{W}_{ik}(x,y) = \begin{cases} 1 \text{ if } x \cap y = \emptyset \\ 0 \text{ otherwise} \end{cases}.$$

Proof. First we note that $x \cap y = \emptyset$ if and only if $x^g \cap y^g = \emptyset$, for any $g \in G$.

So $|\{y \in \Gamma \,:\, y \cap x = \emptyset, \text{for one fixed } x \in \Lambda\}|$ depends only on the orbit Λ and not on a choice of x. Then

$$H_i \bar{X}_{ik}(x, \Gamma) = \sum_{\Lambda} H_i(x, \Lambda) \bar{X}_{ik}(\Lambda, \Gamma), \tag{5.32}$$

since $H_i(x, \Lambda) = 1$ if and only if $x \in \Lambda$, we have that the right-hand side of equation 5.32 is equal to $H_i(x, \Lambda)\bar{X}_{ik}(\Lambda, \Gamma) = \bar{X}_{ik}(\Lambda, \Gamma)$, with $x \in \Lambda$.

On the other hand, by definition of $\bar{X}_{ik}$, we have

$$\bar{W}_{ik} H_k(x, \Gamma) = \sum_{y \in L_k^n} \bar{W}_{ik}(x,y) H_k(y, \Gamma) = \sum_{x \cap y = \emptyset, y \in \Gamma} 1 = \bar{X}_{ik}(\Lambda, \Gamma).$$

The claim follows. $\square$

Theorem 5.4.7. *Let $0 \leq t < k \leq n$ and $t+k = n$. Then*

$$M_{tk}^{+} = \left(X_{0k}^{+} | X_{1k}^{+} | \cdots | X_{tk}^{+} \right)$$

has rank τ_k and index 1. Moreover the $\mathbb{Z}$-module spanned by its columns is equal to $\mathbb{Z}^{\tau_k}$.

Proof. First we prove that

$$N_k M_{tk}^{+} \begin{pmatrix} +\bar{X}_{0k} \\ -\bar{X}_{1k} \\ \cdots \\ (-1)^t \bar{X}_{tk} \end{pmatrix} = N_k.$$

Indeed by Lemma 5.4.2, we have $H_k X_{ik}^{+} = W_{ik}^T H_i$; moreover by Lemma 5.4.6, $H_i \bar{X}_{ik} = \bar{W}_{ik} H_k$ and finally, by Equation 3.2 , $\sum_{i=0}^{t} (-1)^i \bar{W}_{ik}^T W_{ik} = I_{\binom{n}{k}}$, where $I_{\binom{n}{k}}$ is the identity matrix of order $\binom{n}{k}$, we deduce

$$N_k M_{tk}^{+} \begin{pmatrix} +\bar{X}_{0k} \\ -\bar{X}_{1k} \\ \cdots \\ (-1)^t \bar{X}_{tk} \end{pmatrix} = H_k^T H_k M_{tk}^{+} \begin{pmatrix} +\bar{X}_{0k} \\ -\bar{X}_{1k} \\ \cdots \\ (-1)^t \bar{X}_{tk} \end{pmatrix} =$$

$$= H_k^T H_k \left(X_{0k}^{+} | X_{1k}^{+} | \cdots | X_{tk}^{+} \right) \begin{pmatrix} +\bar{X}_{0k} \\ -\bar{X}_{1k} \\ \cdots \\ (-1)^t \bar{X}_{tk} \end{pmatrix} = H_k^T \sum_{i=0}^{t} (-1)^i H_k X_{ik}^{+} \bar{X}_{ik} =$$

$$H_k^T \sum_{i=0}^{t} (-1)^i W_{ik}^T H_i \bar{X}_{ik} = H_k^T \sum_{i=0}^{t} (-1)^i W_{ik}^T \bar{W}_{ik} H_k = H_k^T \left(\sum_{i=0}^{t} (-1)^i W_{ik}^T \bar{W}_{ik} \right) H_k =$$

$$= H_k^T H_k = N_k.$$

Hence, since N_k is a non-singular matrix,

$$M_{tk}^{+} \begin{pmatrix} +\bar{X}_{0k} \\ -\bar{X}_{1k} \\ \cdots \\ (-1)^t \bar{X}_{tk} \end{pmatrix} = I_{\tau_k},$$

with I_{τ_k} identity matrix of order τ_k. So

$$M_{tk}^{+}\begin{pmatrix} +\bar{X}_{0k} \\ -\bar{X}_{1k} \\ \cdots \\ (-1)^t\bar{X}_{tk} \end{pmatrix} M_{tk}^{+} = M_{tk}^{+}$$

and, by Proposition 2.4.16, M_{tk}^{+} has index 1. This means that the $\mathbb{Z}$-module spanned by the columns of M_{tk}^{+} is a pure submodule of $\mathbb{Z}^{\tau_k}$ of rank τ_k. By Lemma 2.4.14 we have the claim. □

Remark 5.4.8. *By equation $H_k X_{tk}^{+} = W_{tk}^{T} H_t$, we deduce that the non-zero invariant factors of X_{tk}^{+} are the same of $W_{tk}^{T} H_t$, which is the matrix associated to the restriction*

$$\epsilon_t^k : (\mathbb{Z}L_t)^G \longrightarrow \mathbb{Z}L_k,$$

with respect to the canonical bases $\mathcal{B}_{\Omega^t}$ and L_k^n, respectively.

Using the relations given in Lemma 5.4.2 it is possible to prove Theorem

Theorem 5.4.9. *Let $0 \le t < k \le n$ and $t + k = n$. Then*

$$M_{tk}^{-} = \bigcup_{i=0}^{t} X_{ik}^{-} = \begin{pmatrix} X_{0k}^{-} \\ X_{1k}^{-} \\ \cdots \\ X_{tk}^{-} \end{pmatrix}$$

has rank τ_t and index 1*.*

Theorems 5.4.7 and 5.4.9 are exactly the first step of Wilson's proof. This suggested us conjecture 5.3.5. We tried to continue following the arguments of Wilson. We realized (see Proposition 3.1.3) that in his proof it is necessary that the matrix M_{tk} has index 1 also for $t < k < n - t$. This is not true in our cases for matrices M_{tk}^{+} and M_{tk}^{-}.

APPENDIX A

Smith group of $\epsilon_t^k : (\mathbb{Z}L_t)^G \longrightarrow (\mathbb{Z}L_k)^G$

In this section we insert the program used in the Magma Computational Algebra System to verify that for any permutation group G on $\Omega = \{1, \cdots, n\}$, where $n \leq 11$, $0 \leq t \leq k$ and $t + k = n$, the orbit matrix X_{tk}^+ is equivalent to a diagonal form with entries $d_i = \binom{k-i}{t-i}$ and multiplicity $m_i = \tau_i - \tau_{i-1}$, for $i = 0, \cdots, t$.

```
checkG:=function(G,k,t)
local  deg,Lk,Lt,Ll,Ok,Ot,Ol,Op,X,i,j,Ti,Kj,x,M,min,u,Y,W,molt,d,l,r,col,r
deg:=Degree(G);
Lk:=Subsets({1..deg},k);
Lt:=Subsets({1..deg},t);
Lk:=GSet(G,Lk);
Lt:=GSet(G,Lt);
Ok:=Orbits(G,Lk);
Ot:=Orbits(G,Lt);
```

```
Op:=0;
row:=#Ot;
col:=#Ok;
min:=Minimum(col,row);
Y:=[];
r:=1;
for l in [0..t] do
   Ll:=Subsets({1..deg},l);
   Ll:=GSet(G,Ll);
   Ol:=Orbits(G,Ll);
   molt:=#Ol-Op;
   if molt ne 0 then
      for i in [r..r+molt-1] do
          for j in [1..col] do
             if i ne j then
                 d:=0;
             else
                 d:=Binomial(k-l,t-l);
             end if;
             Y:=Append(Y,d);
          end for;
      end for;
      r:=r+molt;
   end if;
   Op:=#Ol;
end for;
W:=Matrix(Integers(),row,col,Y);
```

```
return(<ElementaryDivisors(W)>);
end function;

checkGG:=function(G,k,t)
local deg,Lk,Lt,Ok,Ot,i,j,Tj,Ki,y,x,L,N;
deg:=Degree(G);
Lk:=Subsets({1..deg},k);
Lt:=Subsets({1..deg},t);
Lk:=GSet(G,Lk);
Lt:=GSet(G,Lt);
Ok:=Orbits(G,Lk);
Ot:=Orbits(G,Lt);
L:=[];
for i in [1..#Ok] do
  Ki:=Ok[i];
  y:=Representative(Ki);
  for j in [1..#Ot] do
    Tj:=Ot[j];
    L:=Append(L,#{x:x in Tj|x subset y});
  end for;
end for;
N:=Matrix(Integers(),#Ok,#Ot,L);
return(<ElementaryDivisors(N)>);
end function;

S:=Sym(8);
Sub:=Subgroups(S);
```

```
Sub:=[x Alt+96 subgroup:x in Sub];
for G in Sub do
        nr:=Degree(G);
        for k in [1..nr] do
                if k ne nr-k then
                        for t in [1..Minimum(k,nr-k)] do
                                c:=checkG(G,k,t);
                                cc:=checkGG(G,k,t);
                                if not c[1] eq cc[1] then
                                        print <G,c[1],cc[1],t,k,nr>;
                                end if;

                        end for;
                end if;
        end for;
end for;
print <"Terminato">;
```

APPENDIX B

The case $t + k = n$

Here we write the program used to determine the vector v^{+2} in the case $\Omega = \{1, 2, 3, 4, 5, 6\}$, $t = 2$ and $k = 4$. For avoid confusion, we denote by α_i the i^{th} element of Ω, with $i = 1, \cdots, 6$.

Let

$$\begin{aligned} C_2 =\{&\alpha_1\alpha_2,\ \alpha_2\alpha_3,\ \alpha_1\alpha_3,\ \alpha_1\alpha_4,\ \alpha_2\alpha_4,\ \alpha_2\alpha_5,\ \alpha_3\alpha_4,\ \alpha_1\alpha_5,\\ &\alpha_3\alpha_5,\ \alpha_1\alpha_6,\ \alpha_2\alpha_6,\ \alpha_3\alpha_6,\ \alpha_5\alpha_6,\ \alpha_4\alpha_6,\ \alpha_4\alpha_5\} \end{aligned}$$

be a canonical basis and

$$\begin{aligned} \mathcal{P}_2 =\{&\sum_{x\in L_2^6} x, (\alpha_1-\alpha_2)(\alpha_3-\alpha_4), (\alpha_1-\alpha_2)(\alpha_3-\alpha_5), (\alpha_1-\alpha_2)(\alpha_3-\alpha_6), (\alpha_1-\alpha_3)(\alpha_2-\alpha_4),\\ &(\alpha_1-\alpha_3)(\alpha_2-\alpha_5), (\alpha_1-\alpha_3)(\alpha_2-\alpha_6), (\alpha_1-\alpha_4)(\alpha_2-\alpha_5), (\alpha_1-\alpha_4)(\alpha_2-\alpha_6),\\ &(\alpha_1-\alpha_5)(\alpha_2-\alpha_6), \epsilon_1^2(\alpha_1-\alpha_2), \epsilon_1^2(\alpha_1-\alpha_3), \epsilon_1^2(\alpha_1-\alpha_4), \epsilon_1^2(\alpha_1-\alpha_5), \epsilon_1^2(\alpha_1-\alpha_6)\} \end{aligned}$$

be a standard basis of $\mathbb{Q}L_2^6$.

Similarly, let

$$
\begin{aligned}
C_4 = \{ & \alpha_3\alpha_4\alpha_5\alpha_6,\ \alpha_1\alpha_4\alpha_5\alpha_6,\ \alpha_2\alpha_4\alpha_5\alpha_6,\ \alpha_2\alpha_3\alpha_5\alpha_6,\ \alpha_1\alpha_3\alpha_5\alpha_6,\ \alpha_1\alpha_3\alpha_4\alpha_6,\ \alpha_1\alpha_2\alpha_5\alpha_6,\\
& \alpha_2\alpha_3\alpha_4\alpha_6,\ \alpha_1\alpha_2\alpha_4\alpha_6,\ \alpha_2\alpha_3\alpha_4\alpha_5,\ \alpha_1\alpha_3\alpha_4\alpha_5,\ \alpha_1\alpha_2\alpha_4\alpha_5,\ \alpha_1\alpha_2\alpha_3\alpha_4,\ \alpha_1\alpha_2\alpha_3\alpha_5,\ \alpha_1\alpha_2\alpha_3\alpha_6\}
\end{aligned}
$$

be a canonical basis and

$$
\begin{aligned}
\mathcal{P}_4 = \{ & \sum_{y\in L_4^6} y, \epsilon_2^4((\alpha_1-\alpha_2)(\alpha_3-\alpha_4)), \epsilon_2^4((\alpha_1-\alpha_2)(\alpha_3-\alpha_5)), \epsilon_2^4((\alpha_1-\alpha_2)(\alpha_3-\alpha_6)),\\
& \epsilon_2^4((\alpha_1-\alpha_3)(\alpha_2-\alpha_4)), \epsilon_2^4((\alpha_1-\alpha_3)(\alpha_2-\alpha_5)), \epsilon_2^4((\alpha_1-\alpha_3)(\alpha_2-\alpha_6)),\\
& \epsilon_2^4((\alpha_1-\alpha_4)(\alpha_2-\alpha_5)), \epsilon_2^4((\alpha_1-\alpha_4)(\alpha_2-\alpha_6)), \epsilon_2^4((\alpha_1-\alpha_5)(\alpha_2-\alpha_6)),\\
& \epsilon_1^4(\alpha_1-\alpha_2), \epsilon_1^4(\alpha_1-\alpha_3), \epsilon_1^4(\alpha_1-\alpha_4), \epsilon_1^4(\alpha_1-\alpha_5), \epsilon_1^4(\alpha_1-\alpha_6)\}
\end{aligned}
$$

be a standard basis of $\mathbb{Q}L_4^6$.

We call x and y the matrices of change of basis from $\mathcal{P}_2$ to C_2 and from $\mathcal{P}_4$ to C_4, respectively.

```
\begin{lstlisting}

Q:=RealField();
Q<o>:=CyclotomicField(3);
R<a>:=PolynomialRing(Q,1);
F<a>:=FieldOfFractions(R);
```

```
G:=MatrixAlgebra(F,15);

x:=G![
1,0,0,0,1,1,1,1,1,1,0,1,1,1,1,
1,-1,-1,-1,-1,-1,-1,0,0,0,-1,-1,0,0,0,
1,1,1,1,0,0,0,0,0,0,1,0,1,1,1,
1,-1,0,0,-1,0,0,0,0,0,1,1,0,1,1,
1,1,0,0,0,0,0,-1,-1,0,-1,0,-1,0,0,
1,0,1,0,0,0,0,0,0,-1,-1,0,0,-1,0,
1,0,0,0,1,0,0,0,0,0,0,-1,-1,0,0,
1,0,-1,0,0,-1,0,-1,0,0,1,1,1,0,1,
1,0,0,0,0,1,0,0,0,0,0,-1,0,-1,0,
1,0,0,-1,0,0,-1,0,-1,-1,1,1,1,1,0,
1,0,0,1,0,0,0,0,0,0,-1,0,0,0,-1,
1,0,0,0,0,0,1,0,0,0,0,-1,0,0,-1,
1,0,0,0,0,0,0,0,0,1,0,0,0,-1,-1,
1,0,0,0,0,0,0,0,1,0,0,0,-1,0,-1,
1,0,0,0,0,0,0,1,0,0,0,0,-1,-1,0];

y:=G![
1,0,0,0,1,1,1,1,1,1,0,-1,-1,-1,-1,
1,-1,-1,-1,-1,-1,-1,0,0,0,1,1,0,0,0,
1,1,1,1,0,0,0,0,0,0,-1,0,-1,-1,-1,
1,-1,0,0,-1,0,0,0,0,0,-1,-1,0,-1,-1,
1,1,0,0,0,0,0,-1,-1,0,1,0,1,0,0,
```

```
1,0,1,0,0,0,0,0,0,-1,1,0,0,1,0,
1,0,0,0,1,0,0,0,0,0,0,1,1,0,0,
1,0,-1,0,0,-1,0,-1,0,0,-1,-1,-1,0,-1,
1,0,0,0,0,1,0,0,0,0,0,1,0,1,0,
1,0,0,-1,0,0,-1,0,-1,-1,-1,-1,-1,-1,0,
1,0,0,1,0,0,0,0,0,0,1,0,0,0,1,
1,0,0,0,0,0,1,0,0,0,0,1,0,0,1,
1,0,0,0,0,0,0,0,0,1,0,0,0,1,1,
1,0,0,0,0,0,0,0,1,0,0,0,1,0,1,
1,0,0,0,0,0,0,1,0,0,0,0,1,1,0];

Determinant(x);
print" ";

V:=VectorSpace(F,15);

v:=V![-1,0,0,-1,1,2,0,0,0,1,0,0,0,1,0];

z:=x^-1;



w:=v*Transpose(z);

print v;
print w;

w*Transpose(y);
```

Bibliography

[1] William Adkins and Steven Weintraub. *Algebra: an approach via module theory*, volume 136. Springer Science & Business Media, 2012.

[2] Thomas Bier. Remarks on recent formulas of Wilson and Frankl. *European journal of combinatorics*, 14(1):1–8, 1993.

[3] Cristina Caldeira and João Filipe Queiró. Invariant factors of products over elementary divisor domains. *Linear Algebra and its Applications*, 485:345–358, 2015.

[4] Francesca Dalla Volta and Johannes Siemons. *The boolean lattice and invariant factors of a matrix*. Private communication, 2013.

[5] Peter Dembowski. *Finite Geometries: Reprint of the 1968 edition*. Springer Science & Business Media, 2012.

[6] Peter Frankl. Intersection theorems and mod p rank of inclusion matrices. *Journal of Combinatorial Theory, Series A*, 54(1):85–94, 1990.

[7] Katalin Friedl and Lajos Rónyai. Order shattering and Wilson's Theorem. *Discrete Mathematics*, 270(1):127–136, 2003.

[8] Ebrahim Ghorbani, Gholamreza B Khosrovshahi, Ch Maysoori, and M Mohammad-Noori. Inclusion matrices and chains. *Journal of Combinatorial Theory, Series A*, 115(5):878–887, 2008.

[9] Brian Hartley and Trevor O. Hawkes. *Rings, Modules and Linear Algebra*. Chapman & Hall, 1970.

[10] Gordon Douglas James. *The representation theory of the symmetric groups*, volume 682. Springer, 2006.

[11] Rafael Plaza and Qing Xiang. Resilience of ranks of higher inclusion matrices. *arXiv preprint arXiv:1612.08124*, 2016.

[12] Joseph Rotman. *An introduction to homological algebra*. Springer Science & Business Media, 2008.

[13] Johannes Siemons. On a class of partially ordered sets and their linear invariants. *Geometriae Dedicata*, 41(2):219–228, 1992.

[14] Johannes Siemons. Decompositions of modules associated to finite partially ordered sets. *European Journal of Combinatorics*, 15(1):53–56, 1994.

[15] Richard M Wilson. A diagonal form for the incidence matrices of t-subsets vs k-subsets. *European Journal of Combinatorics*, 11(6):609–615, 1990.