ON THE RANK OF INCIDENCE MATRICES IN PROJECTIVE HJELMSLEV SPACES

Ivan Landjev
New Bulgarian University

– WCC 2013, International Workshop on Coding and Cryptography, 15.-19.04.2013, Bergen, Norway –

1. Preliminaries

Theorem. (Folklore) Let X be a finite set with $|X| = n$ and let $1 \leq s \leq t \leq n - s$ be integers. The incidence matrix $M_{s,t}$ of all s-element subsets versus all t-element subsets of X is of rank $\binom{n}{s}$ over $\mathbb{R}$.

Theorem. (Kantor, 1972) Let $0 \leq e < f \leq d - e + 1$, and let $M_{e,f}$ be an incidence matrix of all e-spaces versus all f-spaces of $\mathrm{PG}(d, q)$ or $\mathrm{AG}(d, q)$. Then the rank over $\mathbb{R}$ of $M_{e,f}$ is the number of e-spaces in the geometry.

W. M. Kantor, On Incidence Matrices of Finite Projective and Affine Spaces, *Math. Z.* **124**(1972),315–318.

2. Finite Chain Rings

Definition. A ring (associative, $1 \neq 0$, ring homomorphisms preserving 1) is called a **left (right) chain ring** if the lattice of its left (right) ideals forms a chain.

A. Nechaev, *Mat. Sbornik* **20**(1973).

$$R > \operatorname{rad} R > (\operatorname{rad} R)^2 > \ldots > (\operatorname{rad} R)^{m-1} > (\operatorname{rad} R)^m = (0).$$

- m – the **length** of R;
- $\mathbb{F}_q$ – the **residue field** of R;
- p^h – the **characteristic** of R.

Theorem. Let R be a finite chain ring of length m, characteristic p^h, and residue field of order q. Let $S = \mathrm{GR}(q^h, p^h)$. Then there exist unique integers k, t satisfying $m = (h-1)k + t$, $1 \le t \le k$ ($k = t = m$ if $h = 1$), an automorphism $\sigma \in \mathrm{Aut}\, S$ and an Eisenstein polynomial (not necessarily unique) $g(X) \in S[X;\sigma]$ of degree k such that

$$R \cong S[X;\sigma]/(g(X), p^{s-1}X^t).$$

By an Eisenstein polynomial we mean a polynomial $g(X)$ from the skew polynomial ring $S[X;\sigma]$ which is of the form $g(X) = X^k + p(g_{k-1}X^{k-1} + \ldots + g_0)$, with $g_0 \in S \setminus pS = S^*$.

A. Nechaev, Mat. Sbornik **20**(1973).

W.E. Clark, D. A. Drake, Abh. Math. Sem. der Univ. Hamburg **39**(1974), 364–382.

3. Modules over Finite Chain Rings

Theorem. Let R be a finite chain ring of length m. For any finite module ${}_RM$ there exists a uniquely determined partition

$$\lambda = (\lambda_1, \ldots, \lambda_k) \vdash \log_q |M|,$$

$0 \leq \lambda_i \leq m$, such that

$${}_RM \cong R/(\mathrm{rad}\, R)^{\lambda_1} \oplus \ldots \oplus R/(\mathrm{rad}\, R)^{\lambda_k}.$$

The partition λ is called the **shape** of ${}_RM$.

The number k is called the **rank** of ${}_RM$.

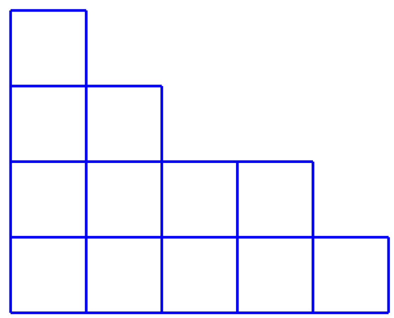
$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$

$N = \lambda_1 + \lambda_2 + \ldots + \lambda_n,$

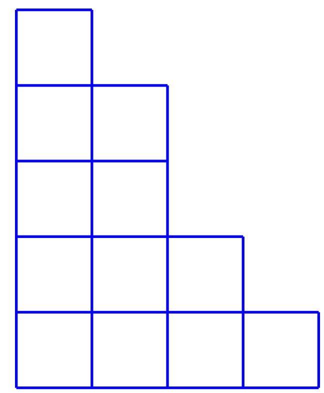
the **conjugate partition**: $\lambda' = (\lambda'_1, \lambda'_2, \ldots)$

$\lambda'_i =$ number of parts in λ that are greater or equal to i

$N = \lambda'_1 + \lambda'_2 + \ldots,$



$$\lambda = (4, 3, 2, 2, 1)$$



$$\lambda' = (5, 4, 2, 1)$$

Theorem. Let ${}_RM$ be a module of shape $\lambda = (\lambda_1, \ldots, \lambda_n)$. For every sequence $\mu = (\mu_1, \ldots, \mu_n)$, $\mu_1 \geq \ldots \geq \mu_n \geq 0$, satisfying $\mu \preceq \lambda$ the module ${}_RM$ has exactly

$$\begin{bmatrix}\lambda\\ \mu\end{bmatrix}_{q^m} = \prod_{i=1}^{m} q^{\mu'_{i+1}(\lambda'_i-\mu'_i)} \cdot \begin{bmatrix}\lambda'_i - \mu'_{i+1}\\ \mu'_i - \mu'_{i+1}\end{bmatrix}_q$$

submodules of shape μ. In particular, the number of free rank s submodules of ${}_RM$ equals

$$q^{s(\lambda'_1-s)+\ldots+s(\lambda'_{m-1}-s)} \cdot \begin{bmatrix}\lambda'_m\\ s\end{bmatrix}_q .$$

Here

$$\begin{bmatrix}n\\ k\end{bmatrix}_q = \frac{(q^n-1)\ldots(q^{n-k+1}-1)}{(q^k-1)\ldots(q-1)}.$$

are the Gaussian coefficients.

4. The Grasmannian $\mathcal{G}_R(n, \kappa)$

Let R be a chain ring with $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$.

Let $\kappa = (\kappa_1, \ldots, \kappa_n)$, $m \geq \kappa_1 \geq \kappa_2 \geq \ldots \geq \kappa_n \geq 0$.

$\mathcal{G}_R(n, \kappa)$ – the set of all submodules of ${}_R R^n$ of shape κ.

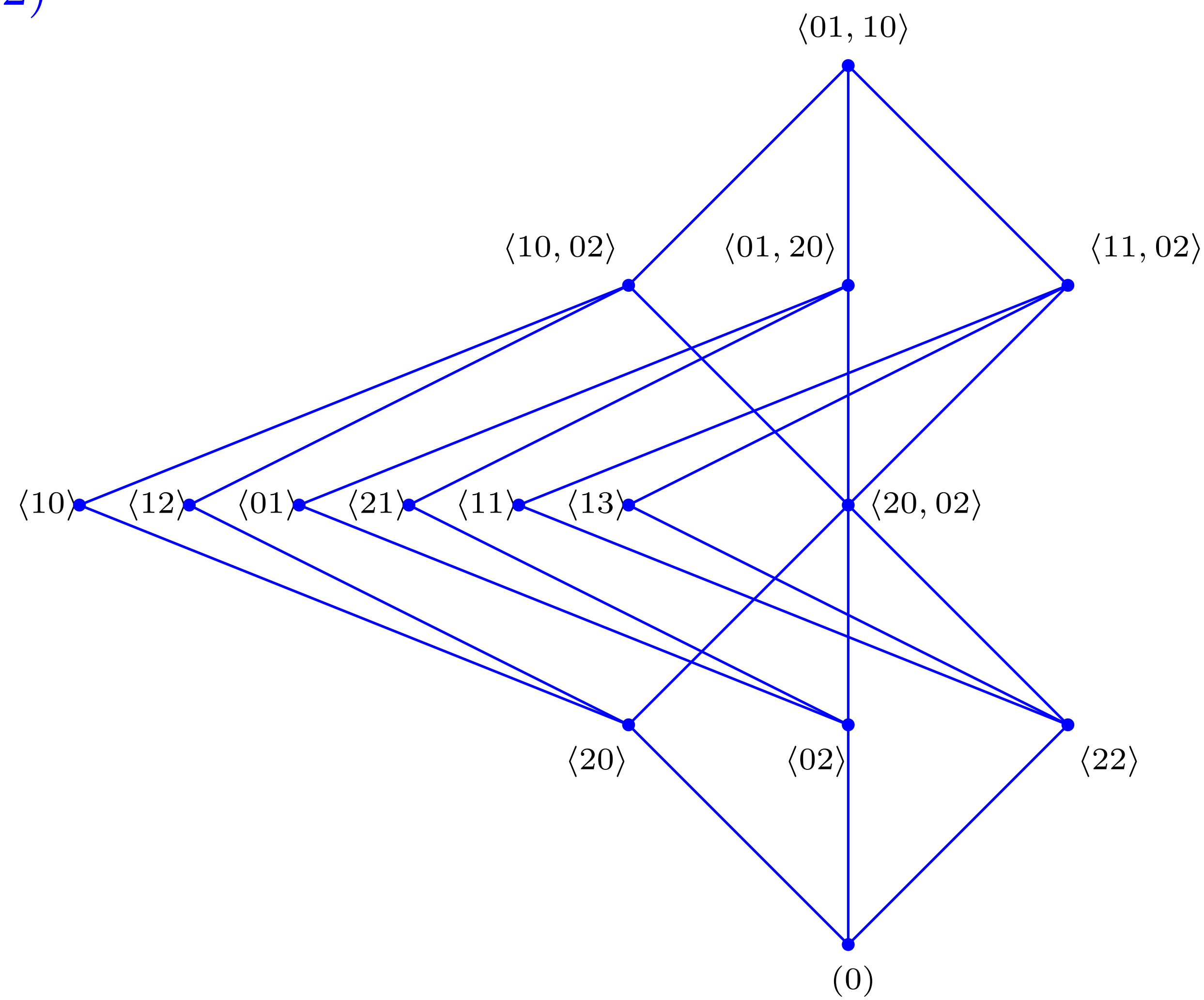
$\mathcal{H}_R(\kappa)$ – the lattice of all submodules of

$$R/(\operatorname{rad} R)^{\kappa_1} \oplus \ldots \oplus R/(\operatorname{rad} R)^{\kappa_n},$$

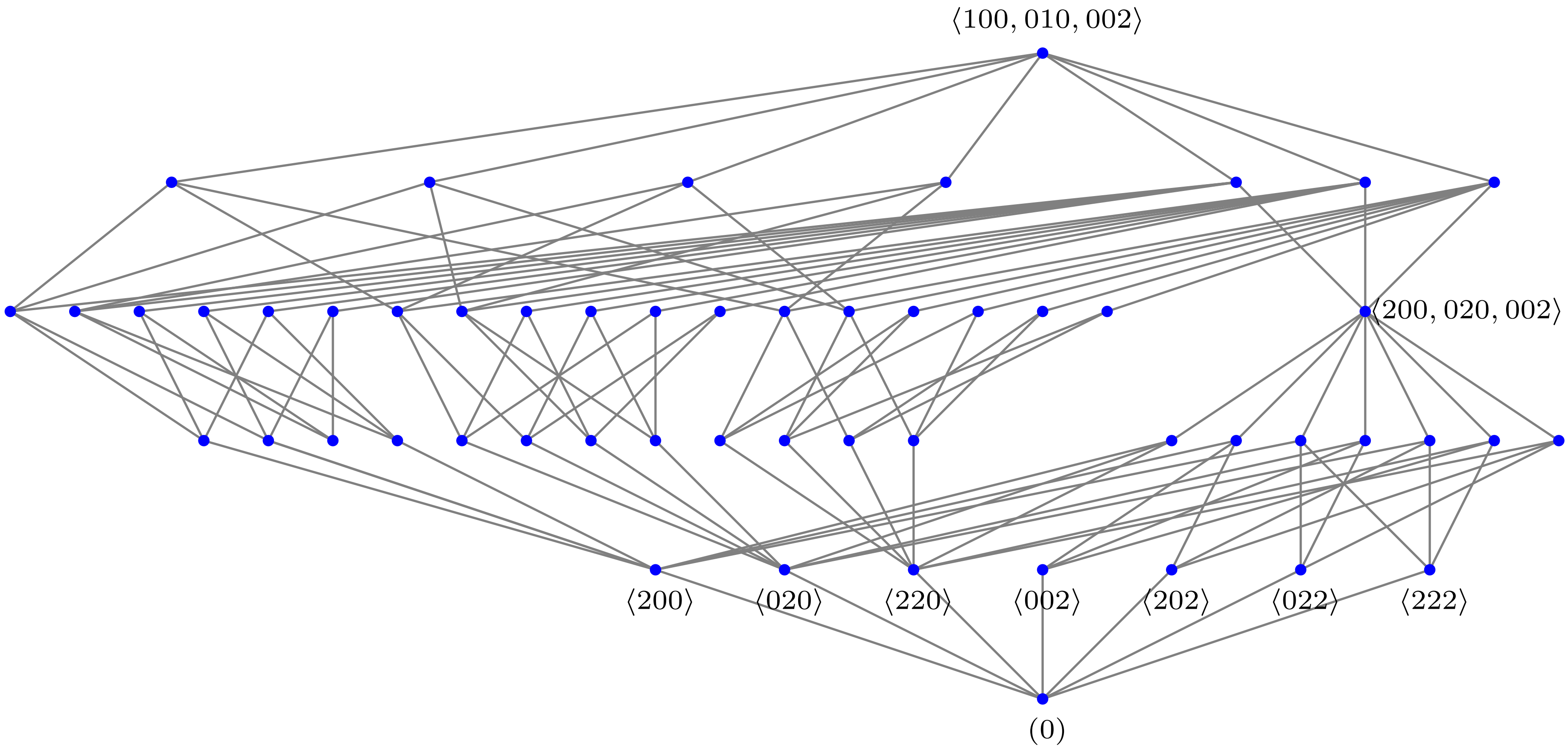
ordered by inclusion.

$\mathcal{H}_R(n)$ – the lattice of all submodules of ${}_R R^n$.

$\mathcal{H}_{\mathbb{Z}_4}(2)$



$\mathcal{H}_R(\kappa)$, $\kappa = (2, 2, 1)$



5. The Theorem

R – a finite chain ring with $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$

$\Omega = \mathrm{PHG}({}_RR^n)$

$\sigma = (\sigma_1, \ldots, \sigma_n)$ and $\tau = (\tau_1, \ldots, \tau_n)$: non-increasing sequences of non-negative integers $m \geq \sigma_1 \geq \ldots \geq \sigma_n \geq 0$, $m \geq \tau_1 \geq \ldots \geq \tau_n \geq 0$, with $\sigma \preceq \tau$

$\mathrm{Supp}(\sigma)$ – the set of indices j for which $\sigma_j \neq 0$.

$M_{\sigma,\tau}$: a $(0,1)$-matrix in which

- the rows are indexed by the elements $\mathcal{G}(n,\sigma)$,

- the columns are indexed by the elements of $\mathcal{G}(n,\tau)$,

- the element $m(S,T)$ which is in the row indexed by $S \in \mathcal{G}(n,\sigma)$ and the column indexed by $T \in \mathcal{G}(n,\tau)$ is defined by

$$m(S,T) = \begin{cases} 1 & \text{if } S \subset T, \\ 0 & \text{if } S \not\subset T. \end{cases}$$

An Important Special Case

The case when $\sigma = (m, 0, \ldots, 0)$ and $\tau = (m, \ldots, m, 0)$ uses the following lemma.

Lemma. Let m be a positive integer, let $k_0, k_1, \ldots, k_m$ be positive integers with $k_0 = 1$, $k_1 | k_2, \ldots, k_{m-1} | k_m$. Let $a_0, a_1, \ldots, a_m$ be arbitrary elements of a field F and let $A = (a_{ij})$ be the $k_m \times k_m$ matrix over F given by $a_{ij} = a_{\min\left\{t : \left\lfloor \frac{i}{k_t} \right\rfloor = \left\lfloor \frac{j}{k_t} \right\rfloor \right\}}$, where the rows and columns are labeled from 0 up to $k_m - 1$. Then

$$\det(A) = \prod_{i=0}^{m} \left(\sum_{j=0}^{i} k_j (a_j - a_{j+1}) \right)^{\frac{k_m}{k_i} - \frac{k_m}{k_{i+1}}},$$

where by convention $a_{m+1} = 0$ and $k_{m+1} = +\infty$.

We have

$$M_{\sigma,\tau} M_{\sigma,\tau}^T = A,$$

where

$$k_0 = 1, k_1 = q^{n-1}, k_2 = q^{2(n-1)}, \ldots,$$

$$k_{m-1} = q^{(m-1)(n-1)}, k_m = q^{(m-1)(n-1)} \frac{q^n - 1}{q - 1}.$$

and

$$a_0 = q^{(m-1)(n-2)} \frac{q^{n-1} - 1}{q - 1}, a_i = q^{(m-1)(n-2)-i+1} \frac{q^{n-2} - 1}{q - 1}, \quad i = 1, \ldots, m.$$

Obviously, then

$$\det A \neq 0$$

and $M_{\sigma,\tau}$ is of full rank.

The General Case

Lemma. Let R be a chain ring with $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, and let $\Omega = \mathrm{PHG}({}_R R^n)$. Let further s and t be integers with $1 \leq s \leq t \leq n - s$ and $\sigma = \boldsymbol{m}^s$, $\tau = \boldsymbol{m}^t$. Then the rank of $M_{\sigma,\tau}(\Omega)$ is equal to the number of free Hjelmslev subspaces of Ω of dimension $s - 1$ i.e. the rank is equal to $\begin{bmatrix} \boldsymbol{m}^n \\ \boldsymbol{m}^s \end{bmatrix}_q$.

Corollary. Let $\sigma = \boldsymbol{m}^s$ and let τ be an arbitrary sequence with $\sigma \preceq \tau \preceq \boldsymbol{m}^n - \sigma$. Then $M_{\sigma,\tau}$ is of full rank.

Lemma. Let $\tau = \boldsymbol{m}^t$ and let σ be an arbitrary sequence with $\sigma \preceq \tau \preceq \boldsymbol{m}_n - \sigma$. Then $M_{\sigma,\tau}$ is of full rank.

Here $\boldsymbol{m}^s = (\underbrace{m, \ldots, m}_{s}, \underbrace{0, \ldots, 0}_{n-s})$.

Main Theorem. Let $\sigma = (\sigma_1, \ldots, \sigma_n)$ and $\tau = (\tau_1, \ldots, \tau_n)$ be two non-increasing sequences of non-negative integers with

$$\sigma \preceq \tau \text{ and } \boldsymbol{m}^{|\operatorname{Supp}(\tau)|} \preceq \boldsymbol{m}^n - \sigma.$$

Then the rank of $M_{\sigma,\tau}(\Omega)$ is equal to the number of shape σ subspaces of Ω, i.e. $\begin{bmatrix} \boldsymbol{m}^n \\ \sigma \end{bmatrix}_{q^m}$.

Remark. The theorem covers the most important cases when $\sigma = \boldsymbol{m}^s$, or $\tau = \boldsymbol{m}^t$, or both.

It does not cover the case where there is no k with $\sigma \preceq \boldsymbol{m}^k \preceq \tau$. This case will require an additional argument.

Example.

- $m = 2$,
- $\sigma = (2, 1, 0, 0, \ldots, 0)$
- $\tau = (2, 1, 1, 0, \ldots, 0)$
- $M_{\sigma,\tau} = I \otimes A$, where A is the lines-by-planes incidence matrix of $\mathrm{PG}(n-1, q)$