ON SOME OPEN PROBLEMS IN FINITE RING GEOMETRIES

Ivan Landjev
New Bulgarian University

– Fifth Irsee Conference "Finte Geometries", Kloster Irsee, 10.–16.09.2017 –

0. Preliminaries

Chain ring: the lattice of left (right) ideals is a chain

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

- m – the length of R;
- $q = p^s$ – order of the residue field of R, $\mathbb{F}_q \cong R/\operatorname{rad} R$;
- p^r – the characteristic of R.

Examples.

- $\mathbb{Z}_{p^m} > (p) > (p^2) > \ldots > (p^{m-1}) > (0)$;
- $\mathrm{GR}(q^m, p^m) = \mathbb{Z}_{p^m}[X]/(f(X))$, $f(X)$ – basic irredusible;

$$\mathrm{GR}(q^m, p^m) > (p) > (p^2) > \ldots > (p^{m-1}) > (0);$$

- $\mathbb{F}_p[X]/(X^m) > (X) > (X^2) > \ldots > (X^{m-1}) > (0)$;
- $\mathbb{F}_p[X;\sigma]/(X^m) > (X) > (X^2) > \ldots > (X^{m-1}) > (0)$,

  where $\sigma \in \mathrm{Aut}(R/\operatorname{rad} R)$, $a^\sigma X = Xa$.

Special interest: the case $m = 2$

$$R > \operatorname{rad} R > (0), \quad |R/\operatorname{rad} R| = p^s.$$

There exist $s + 1$ nonisomorphic rings of length 2:

- $\mathbb{S}_q^{(i)} = \mathbb{F}_q[X; \sigma]/(X^2)$, $\sigma \in \operatorname{Aut}\ \mathbb{F}_q$;
- $\mathbb{G}_q = \operatorname{GR}(q^2, p^2)$.

Modules over finite chain rings:

Theorem. Let R be a finite chain ring of length m and let ${}_RM$ be a finite module over R. There exists a uniquely determined non-increasing sequence $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k, \ldots)$, $0 \leq \lambda_i \leq m$, such that

$$ {}_RM \cong \bigoplus_i R/(\operatorname{rad} R)^{\lambda_i}. $$

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

The conjugate partition $\lambda' = (\lambda'_1, \lambda'_2, \ldots)$, where $\lambda'_i = \#(\lambda_j \mid \lambda_j \geq i)$ is called the **conjugate shape** of ${}_RM$.

The largest number k with $\lambda_k > 0$ is called the **rank** of ${}_RM$.

The number λ'_m is called the **free rank** of ${}_RM$.

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.

The projective Hjelmslev geometry $\mathrm{PHG}({}_R R^n)$:

- $M = {}_R R^n$; $M^* := M \setminus M\theta$;
- $\mathcal{P} = \{Rx \mid x \in M^*\}$;
- $\mathcal{L} = \{Rx + Ry \mid x, y \text{ linearly independent}\}$;
- $I \subseteq \mathcal{P} \times \mathcal{L}$ – incidence relation;
- $\owns\!\!\!\!\!\!\supset$ - **neighbour relation**:

  (N1) $X \owns\!\!\!\!\!\!\supset Y$ if $\exists s, t \in \mathcal{L}$: $X, Y\, I\, s, X, Y\, I\, t$;

  (N2) $s \owns\!\!\!\!\!\!\supset t$ if $\forall X\ I\ s\ \exists Y\ I\ t$: $X \owns\!\!\!\!\!\!\supset Y$ and $\forall Y\ I\ t\ \exists X\ I\ s$: $Y \owns\!\!\!\!\!\!\supset X$.

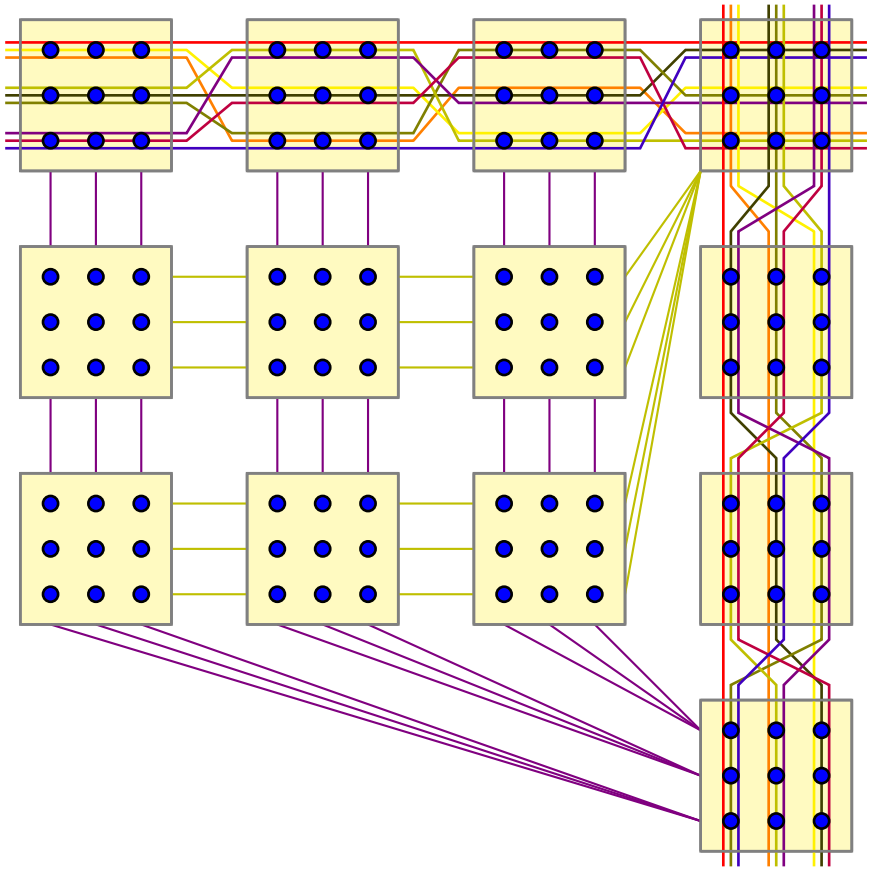
Remark. We can define a set of neighbour relations $\backsim_i$. $i = 0, 1, \ldots, m$, by

$$X \backsim_i Y, X = Rx, Y = Ry \text{ iff } Rx + Ry \text{ is of shape } (m, m-i).$$

Definition. The incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, I)$ with neighbour relation $\backsim$ is called the (left) projective Hjelmslev geometry over the chain ring R.

Notation: $\mathrm{PHG}({}_R R^n)$, $\mathrm{PHG}(n-1, R)$

$\mathrm{PHG}(\mathbb{Z}_9^3)$



1. Ovals and Hyperovals

- $m_2(2, R)$ – the maximal cardinality of a pointset in $\mathrm{PHG}(2, R)$ no three of which are collinear.

- An upper bound on $m_2(2, R)$:

$$m_2(2, R) \leq \begin{cases} q^2 + q + 1 & \text{for } q \text{ even}, \\ q^2 & \text{for } q \text{ odd}. \end{cases}$$

  In case of equality:

  - for q even, every neighbour class contains exactly one point;

  - for q odd, every neighbour class of points contains at most one point and the empty classes are collinear in the factor plane.

- If $q = 2^s$, $R = \mathbb{G}_q$, there exist $(q^2+q+1, 2)$-arcs in $\mathrm{PHG}(2, R)$.

  (Th. Honold, I. Landjev)

- If $q = 2^s$, $R = \mathbb{F}_q[X;\sigma]/(X^2)$, there exist no $(q^2+q+1, 2)$-arcs in $\mathrm{PHG}(2, R)$.

  (Th. Honold, I. Landjev)

- If $q = 2^s$, $R = \mathbb{F}_q[X;\sigma]/(X^2)$, there exist $(q^2+2, 2)$-arcs in $\mathrm{PHG}(2, R)$.

  (Th. Honold, I. Landjev)

- If $q = p^s$, p odd, $R = \mathbb{F}_q[X;\sigma](f(X))$, there exist $(q^2, 2)$-arcs in $\mathrm{PHG}(2, R)$.

  (Th. Honold, M. Kiermaier)

- If $q = p^s$, p odd, $R = \mathbb{G}_q$, there exist $((\frac{q+1}{2})^2, 2)$-arcs in $\mathrm{PHG}(2, R)$.

  (Th. Honold, M. Kiermaier)

Exact values and bounds for $m_2(2, R)$

	$\mathbb{G}_q$	$\mathbb{S}_q^{(i)}$
q even	q^2+q+1	$q^2+2 \leq \cdot \leq q^2+q$
q odd	$\left(\frac{q+1}{2}\right)^2 \leq \cdot \leq q^2$	q^2

Partial Results

- $m_2(2, \mathbb{S}_2) = 6$
- $m_2(2, \mathbb{Z}_9) = 9$
- $m_2(2, \mathbb{S}_4^{(0)}) = m_2(\mathbb{S}_4^{(1)}) = 18$
- $m_2(2, \mathbb{Z}_{25}) = 21$

Problems:

1. Decide the unresolved cases in the above table, i.e. find the size of an oval in a plane over the Galois rings $\mathbb{G}_q$, q odd, and $\mathbb{S}_q^{(i)}$, q even.

2. Are the $(4^s+2^s+1, 2)$-arcs in $\mathbb{G}_{4^s} = \mathrm{GR}(4^s, 2^s)$ unique (up to equivalence)?

   This is known to be the case for $q^2 = 4$ and 16.

3. Find bounds on the size of an $(n, 2)$-arcs in the Hjelmslev planes over rings of larger length.

   For instance,

$$m_2(2, \mathbb{Z}_8) = 10, m_2(2, \mathbb{Z}_{16}) = 16, m_2(2, \mathbb{Z}_{27}) = 21, m(2, \mathbb{Z}_{32}) = 26.$$

2. Arcs and Blocking Sets

w	$\mathbb{Z}_4$	$\mathbb{S}_2$	$\mathbb{Z}_9$	$\mathbb{S}_3$	$\mathbb{Z}_{25}$	$\mathbb{S}_5$
2	7	6	9	9	21	25
3	10	10	19	18	$40-43$	$42-43$
4	16	16	30	30	$66-70$	$64-70$
5	22	22	39	38	$87-102$	$90-102$
6	28	28	49	50	$114-130$	130
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

w	$\mathbb{G}_4$	$\mathbb{S}_4^{(0)}$	$\mathbb{S}_4^{(1)}$
2	21	18	18
3	$29-30$	$29-30$	$29-30$
4	52	52	52
5	68	68	68
6	84	$81-103$	$81-103$
7	$97-101$	$96-101$	$96-101$
8	126	$120-125$	$120-125$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

For any subspace $S \subset \mathcal{P}$ define the homogenious weight of S by:

$$\omega(S) = \mathcal{K}(S) - \frac{1}{q-1}\mathcal{K}([S] \setminus S).$$

Definition. The mapping $\mathcal{K} : \mathcal{P} \to \mathbb{N}_0$ is called a homogeneous (N, W)-arc if

(a) $\mathcal{K}(\mathcal{P}) = N$;

(b) $\omega(H) \leq W$ for any hyperplane;

(c) $\omega(H_0) = W$ for at least one hyperplane H_0.

Problems:

1. Fill in the gaps in the existing tables.

2. (A. A. Nechaev) Can one distinguish geometrically Hjelmslev planes (and, more generally, Hjelmslev geometries) over nonisomorphic rings of the same size, same length, and same characteristic.

3. Find nontrivial examples of new two-weight homogeneous arcs. (It is known that these should be regular, i.e. each neighbour class of points has the same multiplicity).

4. Find the size of the smallest non-trivial blocking set in $\mathrm{PHG}(2, \mathbb{G}_q)$.

5. Find the minimal size of a blocking set in $\mathrm{AHG}(2, R)$.

   Hypothesis: $q(2q-1)$.

3. Spreads

Definition. An λ-**spread** in the projective Hjelmslev geometry $\mathrm{PHG}({}_R R^{n+1})$ is a set $\mathcal{S}$ of subspaces of shape λ such that every point is contained in exactly one subspace of $\mathcal{S}$.

Let m be a positive integer with $m = (s-1)k + t$. Let

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

where $S = \mathrm{GR}(q^s, p^s)$. Clearly,

$$|R| = q^m, |S/\operatorname{rad} S| = q.$$

Set $T = S[Y]/(f(Y))$, where f, $\deg f = r+1$, is basic irreducible. Let

$$Q = T[X;\sigma]/(g(X), p^{s-1}X^t).$$

We have

$$|Q| = q^{m(r+1)}, |T/\operatorname{rad} T| = q^{r+1}.$$

Theorem. Let Q and R be as above, and let

$$n+1=(r+1)(l+1).$$

Assume there exists a λ-spread with $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_{l+1})$ of $\mathrm{PHG}({}_QQ^{l+1})$. Then there exists a μ-spread of $\mathrm{PHG}({}_RR^{n+1})$ with

$$\mu=(\underbrace{\lambda_1,\ldots,\lambda_1}_{r+1},\ldots,\underbrace{\lambda_{l+1},\ldots,\lambda_{l+1}}_{r+1}).$$

Corollary. A spread of $\mathrm{PHG}({}_RR^{n+1})$ by Hjelmslev r-subspaces exists iff $r+1$ divides $n+1$.

Theorem. Let R be a chain ring of length 2 and with residue field of order q. Let n be even and let

$$\lambda = (\underbrace{2, 2, \ldots, 2}_{n/2}, \underbrace{1, \ldots, 1}_{n/2-a}, \underbrace{0, \ldots, 0}_{a}), \quad 1 \leq a \leq n/2.$$

Then there exists no spread in $\mathrm{PHG}({}_R R^n)$.

The number of points in a subspace of shape λ is

$$q^{n-a-1} \begin{bmatrix} n/2 \\ 1 \end{bmatrix}_q = q^{n-a-1} \frac{q^{n/2} - 1}{q - 1}.$$

It divides the number of all points in $\mathrm{PHG}({}_R R^n)$ which is $q^{n-1}(q^n - 1)/(q-1)$.

Problems:

1. Given an integer n and a sequence $\lambda = (\lambda_1 = m, \lambda_2, \ldots)$, find a general necessary and sufficient condition for the existence of λ-spreads in $\mathrm{PHG}({}_R R^{n+1})$.

2. Do there exist spreads in $\mathrm{PHG}({}_R R^4)$ consisting of lines no two of which are neighbours.

3. Construct nontrivial R-designs in $\mathrm{PHG}({}_R R^{n+1})$ for different parametrs.

4. Do there exist R-analogs of Steiner systems?

4. Rank Problems

Let $\Omega = \mathrm{PHG}({}_R R^n)$, $|R| = q^m$. Denote by $M_{\sigma,\tau}(\Omega)$ the $(0,1)$-incidence matrix of all shape σ by shape τ submodules of Ω.

Set $\boldsymbol{m}^s = (\underbrace{m,\ldots,m}_{s},\underbrace{0,\ldots,0}_{n-s})$. If $\boldsymbol{m}^s \preceq \tau \preceq \boldsymbol{m}^{n-s}$ then

$$\mathrm{rk}_{\mathbb{Q}}\, M_{\boldsymbol{m}^s,\tau} = \begin{bmatrix} \boldsymbol{m}^n \\ \boldsymbol{m}^s \end{bmatrix}_{q^m},$$

This is a partial analogue of the result by Kantor on the incidenece matrix of s-dimensional vs. t-dimensional subspaces of $\mathrm{PG}(n,q)$.

Remark. There exist shapes σ and τ for which the rank of $M_{\sigma,\tau}$ is not maximal.

On the p-rank of the point-by-lines incidence matrix M of $\mathrm{PHG}({}_R R^3)$:

If $|R| = 4$, we can easily get

$$\operatorname{rk} M = \begin{cases} 13 & \text{if } \operatorname{char} R = 2, \\ 12 & \text{if } \operatorname{char} R = 4. \end{cases}$$

Generally, for $|R| = q^2$, $q = p^s$:

$$\operatorname{rk} M < (q^2 + q + 1)\binom{p+1}{2}^s.$$

Problems:

1. Find the $\mathbb{Q}$-rank of $M_{\sigma,\tau}(\Omega)$ for any σ and τ.

2. Find the p-rank of the point-by-lines incidence matrix of $\mathrm{PHG}({}_R R^3)$ for a chain ring R of length 2.

   (Maybe one should start with ring for which the residue field is $\mathbb{F}_p$.)

3. More generally, find the p-rank of the points-by-hyperplanes matrix of $\mathrm{PHG}({}_R R^{n+1})$ for an arbitrary chain ring R.

6. Sperner Theory

Theorem. (E. Sperner, 1928) If $A_1, A_2, \ldots, A_m$ are subsets of $X = \{1, 2, \ldots, n\}$ such that A_i is not a subset of A_j if $i \neq j$, then $m \leq \binom{n}{\lfloor n/2 \rfloor}$.

Theorem. If $\mathcal{A}$ is an antichain in the partially ordered set of all subspaces of $\mathbb{F}_q^n$, then

$$|\mathcal{A}| \leq \begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}_q.$$

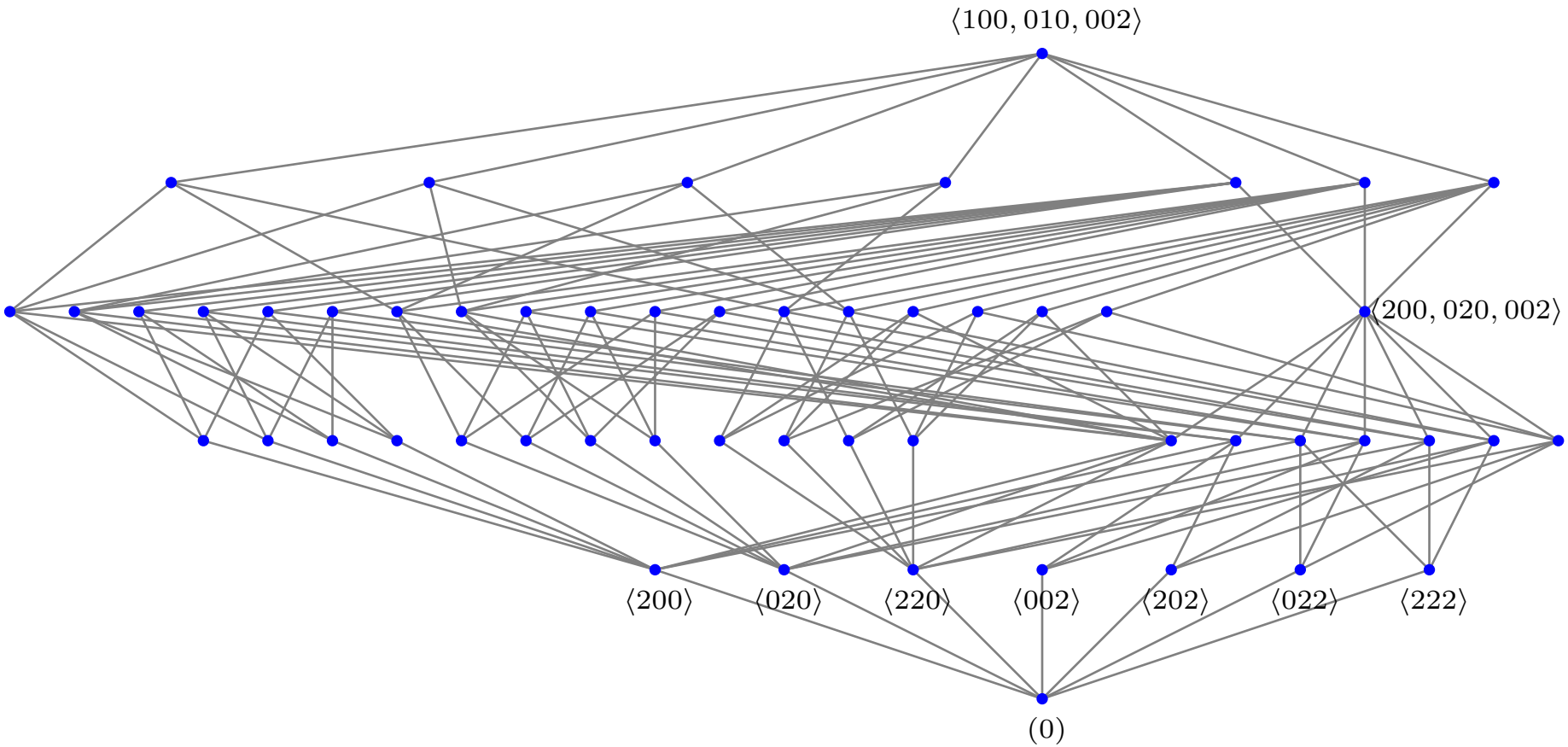
Theorem. Let $\mathcal{P} = \mathcal{P}_n(R)$ be the partially ordered set of all submodules of ${}_R R^n$ with partial order given by inclusion. Then the size of a maximal antichain in $\mathcal{P}$ is equal to

$$\sum_{\mu \prec \boldsymbol{m}^n} \begin{bmatrix} \boldsymbol{m}^n \\ \mu \end{bmatrix}_{q^m},$$

where the sum is over all non-increasing sequences $\mu = (\mu_1, \ldots, \mu_n) \prec \boldsymbol{m}^n$ with

$$\sum_{i=1}^{n} \mu_i = \lfloor \frac{mn}{2} \rfloor.$$

$\mathcal{P}(\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus 2\mathbb{Z}_4)$



Problem. Let R be a finite chain ring and let ${}_RM$ be a (left) module over R of shape $\lambda = (\lambda_1, \ldots, \lambda_n)$. Find the cardinality of the largest antichain in the lattice of all submodules of ${}_RM$?