# BASIC ALGORITHMS FOR MANIPULATION OF MODULES OVER FINITE CHAIN RINGS* 

Nevyana Georgieva


#### Abstract

In this paper, we present some basic algorithms for manipulation of finitely generated modules over finite chain rings. We start with an algorithm that generates the standard form of a matrix over a finite chain ring, which is an analogue of the row reduced echelon form for a matrix over a field. Furthermore we give an algorithm for the generation of the union of two modules, an algorithm for the generation of the orthogonal module to a given module, as well as an algorithm for the generation of the intersection of two modules. Finally, we demonstrate how to generate all submodules of fixed shape of a given module.


1. Introduction. The importance of the class of linear codes over finite chain rings was recognized only in the last two decades. The interest in these codes was initiated by the remarkable discovery that some notorious classes of

[^0]codes like the Kerdock- and Preparata-codes outperform the classical linear codes with the same parameters [1, 2]. Attempts were made to develop a general theory of linear codes over finite chain rings. This was done in a series of papers by Honold and Landjev [3, 4, 5, 6]. It turned out that linear codes over finite chain rings are equivalent to multisets of points in special geometries, the so-called projective Hjelmslev geometries [7, 8, 9]. The efforts of various researches were focused on proving analogs for all important results known from finite geometry. However, the situation in the projective Hjelmslev geometries turned out to be far more unclear due to their complicated internal structure. This has to do with the more complex structure of finitely generated modules over finite chain rings compared with vector spaces over finite fields. In some cases even the construction of examples turns out to be a problem. For instance, it is difficult to construct $R$-spreads of mutually non-neighbouring lines in $\operatorname{PHG}\left(R^{4}\right)$ (cf. [10]). This makes computer searches unavoidable and explains the need for efficient algorithms that deal with finitely generated modules over finite chain rings.

The paper is structured as follows. In Section 2 we give some basic facts concerning the structure of finite chain rings and the representation of the elements of a finite chain ring. Further we give a structure theorem for modules and results about the orthogonal module, and explain notions like the shape and the dual shape of a module. In Section 3 we define the standard form of a matrix and describe an algorithm that puts a matrix into standard form. Furthermore, this algorithm is applied to get algorithms for the generation of the union of two modules and for containment of a given module in another module. Section 4 is devoted to the generation of the orthogonal module $M_{R}^{\perp}$ to a given module ${ }_{R} M$. We use an explicit form for a matrix whose rows generate $M_{R}^{\perp}$ that was recently found in [11]. This algorithm in turn allows us to find the intersection of two modules. Finally in Section 5 we describe an algorithm that generates all submodules of given shape for a module defined by the rows of a matrix in standard form.
2. Basic facts. In this section we describe briefly some basic properties of finite chain rings and finitely generated modules over finite chain rings. For a more in-depth introduction to this subject we refer to [12, 13, 14].

An associative ring with identity is called a left (right) chain ring if the lattice of its left (right) ideals is a chain. In such case, there exists an element $\theta \in \operatorname{Rad} R \backslash \operatorname{Rad}^{2} R$ whose powers generate all ideals

$$
R>(\theta)>\left(\theta^{2}\right)>\cdots>\left(\theta^{m-1}\right)>\left(\theta^{m}\right)=(0)
$$

The smallest $m$ such that $\theta^{m}=0$ is called the length (or nilpotency index) of $R$. The field $R /(\theta)$ is called the residue field of the ring $R$. If we set $|R /(\theta)|=q$, we have $|R|=q^{m}$. Let $\Gamma=\left\{\gamma_{0}=0, \gamma_{1}=1, \gamma_{2}, \ldots, \gamma_{q-1}\right\}$ be a set of elements of $R$ with $\gamma_{i} \not \equiv \gamma_{j}(\bmod \operatorname{Rad} R)$ for all $i, j$ with $0 \leq i \leq j \leq q-1$. For every element $a$ from $R$ there exists a unique representation

$$
a=a_{0}+a_{1} \theta+\cdots+a_{m-1} \theta^{m-1}, a_{i} \in \Gamma .
$$

We fix some linear order on $\Gamma$ :

$$
\gamma_{0} \prec \gamma_{1} \prec \ldots \prec \gamma_{m-1} .
$$

This order is extended to all elements of $R$ as follows. For two elements $a=$ $a_{0}+a_{1} \theta+\ldots+a_{m-1} \theta^{m-1}$ and $b=b_{0}+b_{1} \theta+\ldots+b_{m-1} \theta^{m-1}$ from $R, a_{i}, b_{i} \in \Gamma$, we write $a \prec b$ if and only if

$$
a_{m-1}=b_{m-1}, \ldots, a_{j+1}=b_{j+1}, a_{j} \prec b_{j},
$$

for some $0 \leq j \leq m-1$. This is in fact the lexicographic order on the $n$-tuples $\left(a_{0}, \ldots, a_{m-1}\right)$. We can define a bijection $\varphi: R \rightarrow\left\{0,1, \ldots, q^{m}-1\right\}$ which is consistent with the linear order of the elements of $R$ given above. Set $\varphi\left(\gamma_{i}\right)=i$. Further for $a=a_{0}+a_{1} \theta+\ldots+a_{m-1} \theta^{m-1}, a_{i} \in \Gamma$, we let $\varphi(a)=\sum_{i=0}^{m-1} \varphi\left(a_{i}\right) q^{i}$.

In [11] we proved the following lemma.

## Lemma 1.

(1) The element $a$ is in $\Gamma$ if and only if $\varphi(a)<q$; more generally, the elements a with $\varphi(a)<q^{i}$ form a system of distinct representatives modulo $(\operatorname{Rad} R)^{i}$;
(2) for each $i \in \mathbb{N}, a \in(\operatorname{Rad} R)^{i}$, i.e., $a=b \theta^{i}, b \in R$, if and only if $\varphi(a)$ divides $q^{i}$;
(3) if $q^{i}$ divides $\varphi(b)$ then $b=a \theta^{i}$ with $a=\varphi^{-1}\left(\frac{\varphi(b)}{q^{i}}\right)$.

The next theorem is the main structure result for finitely generated modules over finite chain rings.

Theorem 1. Let $R$ be a finite chain ring. For every finite module ${ }_{R} M$ there exists a uniquely determined partition $\lambda=\left(\lambda_{1}, \ldots, \lambda_{k}\right) \vdash \log _{R}|M|$ into parts $1 \leq \lambda_{i} \leq m$ such that

$$
{ }_{R} M \cong R /(\operatorname{Rad} R)^{\lambda_{1}} \oplus \ldots \oplus R /(\operatorname{Rad} R)^{\lambda_{k}}
$$

The parts of the conjugate partition $\lambda^{\prime}=\left(\lambda_{1}^{\prime}, \lambda_{2}^{\prime}, \ldots\right) \vdash \log _{q}|M|$ are the UlmKaplansky invariants $\lambda_{i}^{\prime}=\operatorname{dim}_{R / \operatorname{Rad} R}\left(M[\theta] \cap \theta^{i-1} M\right)$.

The partitions $\lambda$ and $\lambda^{\prime}$ are called the shape and conjugate shape of ${ }_{R} M$. The integer $k=\lambda_{1}^{\prime}=\operatorname{dim}_{R / \operatorname{Rad} R} M[\theta]$ is called the rank of ${ }_{R} M$ and the integer $\lambda_{m}^{\prime}$ is called the free rank of ${ }_{R} M$.

Let ${ }_{R} M$ be a finitely generated left $R$-module. We say that the element $x \in{ }_{R} M$ has period $\theta^{i}$ if $i \geq 0$ is the smallest integer with $\theta^{i} x=0$. The set of all elements of period $m$ are called torsion elements. We also set $M^{*}=\{x \in$ $M \mid x$ has period $\left.\theta^{m}\right\}$. The element $x$ has height $j$ if $j$ is the largest integer with $x=\theta^{j} y, y \in M^{*}$.
3. The standard form. In this section we introduce the notion of standard form of a matrix over a finite chain ring. It is analogous to the notion of row-reduced echelon form of a matrix over a field. Denote by $\boldsymbol{M}_{k, n}(R)$ the set of all matrices over the finite chain ring $R$. The following definition was given in [11].

Definition 1. The matrix $A=\left(a_{i j}\right) \in \boldsymbol{M}_{k, n}$ is said to be in standard form if
(1) $a_{i j_{i}}=\theta^{m-t_{i}}$ for some $t_{i} \in\{0, \ldots, m\}$;
(2) $a_{i s}=\theta^{m-t_{i}+1} \beta, \beta \in R$, for all $s<j_{i}$;
(3) $a_{i s}=\theta^{m-t_{i}} \beta, \beta \in R$, for all $s>j_{i}$;
(4) $a_{s j_{i}} \prec a_{i j_{i}}$ for all $s \neq i$ (here $\prec$ is the lexicographic order defined in section 2);
(5) $i_{1}<i_{2}<i_{3}<\ldots$

The integer $t_{i}$ is called the type of row $i, i=1, \ldots, k$. Let $\boldsymbol{a}=\left(a_{1}, \ldots, a_{n}\right) \in$ ${ }_{R} R^{n}$. The smallest $i \in\{0, \ldots, m\}$ such that $\theta^{i} a=0$ is called the type of $\boldsymbol{a}$. The leftmost component $a_{j}$ with $a_{j} \in(\operatorname{Rad} R)^{m-i} \backslash(\operatorname{Rad} R)^{m-i+1}$ is called the leader
of $\boldsymbol{a}$. For a matrix $A \in \boldsymbol{M}_{k, n}(R)$ in standard form we denote the set of coordinate positions of the row-leaders of $A$, i. e., $J(A)=\left\{j_{1}, j_{2}, \ldots, j_{k}\right\}$. Note that in the definition we decided to suppress the zero-rows. In [11] the following two results were proved.

Theorem 2. Let ${ }_{R} M \leq{ }_{R} R^{n}$ be a module and let $A$ be a matrix in standard form whose rows generate ${ }_{R} M$. For an arbitrary element $\boldsymbol{v} \in{ }_{R} M$ denote by $s$ the position of its leader. Then $s \in J(A)$.

Theorem 3. For every module $M \leq{ }_{R} R^{n}$ there exists a unique matrix $B$ in standard form such that $M$ is spanned by the rows of $B$.

Corollary 1. Let $A$ be a $(k \times n)$-matrix in standard form over the chain ring $R$. There exist permutation matrices $T_{1}$ of size $(k \times k)$ and $T_{2}$ of size $(n \times n)$ such that

$$
T_{1} A T_{2}=\left(\begin{array}{rrrlrr}
I_{k_{0}} & A_{01} & A_{02} & \ldots & A_{0, m-1} & A_{0, m}  \tag{1}\\
0 & \theta I_{k_{1}} & \theta A_{12} & \ldots & \theta A_{1, m-1} & \theta A_{1, m} \\
0 & 0 & \theta^{2} I_{k_{2}} & \ldots & \theta^{2} A_{2, m-1} & \theta^{2} A_{2, m} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & \theta^{m-1} I_{k_{m-1}} & \theta^{m-1} A_{m-1, m}
\end{array}\right),
$$

where the entries in the matrices $A_{i j}$ are from $R$.
Let a matrix $M$ generating the module ${ }_{R} M$ be given. The following algorithm generates a matrix in standard form, whose rows generate ${ }_{R} M$.

Algorithm 1: The standard form of a matrix
Input: a $k \times n$ matrix $M$ with entries from $R$
Output: a matrix $A$ in standard form whose rows generate the same module as the rows of $M$
for $t=m, \ldots, 1$ do
2: for every row $r$ of the matrix $M$ do
3: $\quad$ if not all components of $r$ are multiples of $\theta^{m-t+1}$ then
4: $\quad$ Find $i$ the leftmost position $i$ of $r$ that is not a multiple of $\theta^{m-t+1}$

5: $\quad$ Left multiply all components of $r$ by $\left(\varphi^{-1}\left(\frac{\varphi\left(r_{i}\right)}{q^{m-t}}\right)\right)^{-1}$
6: $\quad$ Set the matrix to be $B=A \cup M \backslash\{r\}$
$/ / B$ is the union of the rows of $A$ and $M$ with $r$ excluded
7: $\quad$ for every row $r^{\prime}$ of $B$ do

8:
Let $c=\varphi^{-1}\left(\left\lfloor\frac{\varphi\left(r_{i}\right)}{q^{m-t}}\right\rfloor\right)$ and replace $r^{\prime}$ by $r^{\prime}-c \cdot r$
9:
if $r^{\prime}=0$, remove it from $M$
endfor
11: $\quad$ Put $r$ as the $i$ th row of $A$ and remove it from $M$
12: endif
13: endfor
4: endfor
for every row $a$ of the matrix $A$
Let $j$ be the leftmost position in $a$ that is $>0$
Let $b=A \backslash\{a\}$ be a row of $A$ preceding $a$
if $b_{j} \geq a_{j}$ do
19: $\quad$ Set $c_{1}=\left\lceil\frac{q^{m}-b_{j}}{a_{j}}\right\rceil$ and replace $b$ by $b+c_{1} \cdot a$
20: endif
: endfor
return $A$

Algorithm 1 can be used in an obvious way to generate the union of two submodules. We just consider a new matrix consisting of the generator matrices of the two given modules and put it in standard form by Algorithm 1.

## Algorithm 2: Union of submodules

Input: two matrices $M$ and $N$ of sizes $k_{1}$-by- $n$ and $k_{2}$-by- $n$
Output: a matrix $A$ in standard form whose rows generate the module spanned by the rows of $M$ and $N$

1: Let $P=\left(\frac{M}{N}\right)$
2: Apply Algorithm 1 to get the standrard form $U$ of the matrix $P$
3: return $U$

Now we can also easily test whether a submodule is contained in a given module. This is done by the following algorithm.

Algorithm 3: Submodule-test
Input: matrices $A$ and $B$ in standard form with the same number of columns

Output: Yes if the submodule spanned by the rows of $B$ is contained in $A$; No otherwise

1: Create the matrix $C=\left(\frac{A}{B}\right)$
2: Generate the matrix $C_{1}$ which is the standard form of $C$
3: If $C_{1}=A$ then $B$ is contained in $A$;
4: print: Yes
5: else print: No
4. The orthogonal submodules. Let $R$ be a finite chain ring and consider a left module ${ }_{R} M \leq{ }_{R} R^{n}$. For two vectors $\boldsymbol{x}=\left(x_{1}, \ldots, x_{n}\right)$ and $\boldsymbol{y}=$ $\left(y_{1}, \ldots, y_{n}\right)$ we define their inner product by

$$
x \boldsymbol{y}=x_{1} y_{1}+\ldots+x_{n} y_{n} .
$$

The right orthogonal to ${ }_{R} M$ is defined by

$$
M_{R}^{\perp}=\left\{\boldsymbol{y} \in R^{n} \mid \boldsymbol{x} \boldsymbol{y}=0 \text { for all } \boldsymbol{x} \in M\right\} .
$$

Note that the orthogonal to a left module is a right module and vice versa. The following well-known theorem summarizes some basic properties of the orthogonal module (cf. [5, 6]).

Theorem 4. Let $R$ be a chain ring with $|R|=q^{m}, R / \operatorname{Rad} R \cong \mathbb{F}_{q}$, and let ${ }_{R} M \leq{ }_{R} R^{N}$ be a left submodule of shape $\lambda=\left(\lambda_{1}, \ldots, \lambda_{n}\right)$.
(1) The right module $M_{R}^{\perp}$ has shape $\bar{\lambda}=\left(m-\lambda_{n}, \ldots, m-\lambda_{1}\right)$. In particular $|M|\left|M^{\perp}\right|=\left|R^{n}\right|$.
(2) ${ }^{\perp}\left(M^{\perp}\right)=M$.
(3) $M \rightarrow M^{\perp}$ defines an antiisomorphism between the lattices of left (resp. right) submodules of $R^{n}$ and hence

$$
\left(M_{1} \cap M_{2}\right)^{\perp}=M_{1}^{\perp}+M_{2}^{\perp},\left(M_{1}+M_{2}\right)^{\perp}=M_{1}^{\perp} \cap M_{2}^{\perp},
$$

for $M_{1}, M_{2} \leq R^{n}$.
Theorem 5. Let ${ }_{R} M$ be a submodule of ${ }_{R} R^{n}$ generated by the rows of the matrix $A$ of the form (1). Then $M_{R}^{\perp}$ is generated by the matrix

$$
B=\left(\begin{array}{llllll}
B_{01} \theta^{m-1} & I_{k_{1}} \theta^{m-1} & 0 & 0 & \ldots & 0  \tag{2}\\
B_{02} \theta^{m-2} & B_{12} \theta^{m-2} & I_{k_{2}} \theta^{m-2} & 0 & \ldots & 0 \\
B_{03} \theta^{m-3} & B_{13} \theta^{m-3} & B_{23} \theta^{m-3} & I_{k_{3}} \theta^{m-3} & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
B_{0, m-1} & B_{1, m-1} & B_{2, m-1} & B_{3, m-1} & \ldots & I_{k_{m-1}}
\end{array}\right),
$$

where
(3) $B_{i j}=-\left(A_{i j}-\sum_{1<k<j+1} A_{i k} A_{k, j+1}+\sum_{i<k<l<j+1} A_{i k} A_{k l} A_{l, j+1}-\ldots+\right.$

$$
\left.(-1)^{j-i+1} A_{i, i+1} A_{i+1, i+2} \ldots A_{j, j+1}\right)^{T} .
$$

Corollary 2. Let $A \in \boldsymbol{M}_{k, n}$ be a matrix over a chain ring $R$ whose rows generate the module ${ }_{R} M$. Let $A^{\prime}=T_{1} A T_{2}$, where $T_{1}$ and $T_{2}$ are permutation matrices of orders $k$ and $n$, respectively, be of the form (1). The module $M_{R}^{\perp}$ is generated by the rows of

$$
B=T_{1}^{T} B^{\prime} T_{2}^{T},
$$

where $B^{\prime}$ is the matrix given by (2).

Theorem 5 gives an explicit expression for a set of generators of the orthogonal module.

Algorithm 4: The orthogonal module $M^{\perp}$
Input: a matrix $A$ whose rows generate a left module ${ }_{R} M$
Output: a matrix $C$ whose rows generate the right module $M_{R}^{\perp}$ that is orthogonal to $A$

1: Find permutation matrices $T_{1}$ and $T_{2}$ that transform $A$ to the form (1)
2: Compute the matrices $B_{i j}$ by (3)
3: Compute the matrix $B$ by (2)
4: $C=T_{1}^{T} B T_{2}^{T}$
5: return $C$

The intersection of two modules is obtained from Theorem 4(3) which gives that $M_{1} \cup M_{2}={ }^{\perp}\left(M_{1}^{\perp}+M_{2}^{\perp}\right)$. Hence we have the following algorithm.

Algorithm 5: The intersection of two modules
Input: matrices $A$ and $B$ in standard form whose rows generate the modules $M$ and $N$, respectively
Output: a matrix $C$ generating the intersection of $A$ and $B$

1: Use Algorithm 4 to find matrices $A^{\perp}$ and $B^{\perp}$ which generate the right orthogonal modules to $A$ and $B$, respectively.
2: Set $U=\binom{A^{\perp}}{B^{\perp}}$
3: Apply Algorithm 4 to find a matrix ${ }^{\perp} U$-left orthogonal to the matrix $U$
4: return $C={ }^{\perp} U$
5. Generation of all submodules of fixed shape. Let ${ }_{R} M \leqq{ }_{R} R^{n}$ be a module of shape $\lambda$, where

$$
\lambda=(\underbrace{m, \ldots, m}_{k_{0}}, \underbrace{m-1, \ldots, m-1}_{k_{1}}, \ldots, \underbrace{1, \ldots, 1}_{k_{m-1}})=\left(\lambda_{1}, \lambda_{2}, \ldots, \lambda_{k}\right), \quad k=\sum_{i=0}^{m-1} k_{i} .
$$

In this section we present an algorithm that generates all submodules ${ }_{R} N$ of ${ }_{R} M$ of shape $\mu=\left(\mu_{1}, \mu_{2}, \ldots, \mu_{l}\right)$ where $\mu \prec \lambda$. Here $l \leqq k$ and we suppress the trailing zeros. We assume that the module ${ }_{R} M$ is generated by the rows of a $k \times m$ matrix $A$ which is in the form (1). Let ${ }_{R} N$ be generated by the rows of a $l \times n$ matrix $B$ in standard form. The rows of $B$ are linear combinations of the rows of $A$. Then there exists a matrix $C$ (also in standard form) such that

$$
B=C A .
$$

Moreover $C$ has the following properties:
(1) if the leader in row $i$ of $B$ is in position $j_{i}$ then the leader of row $i$ in $C$ is in position $l_{i} \geqq j_{i}$;
(2) the components of $C$ contained in the $j$ th column where

$$
k_{0}+\cdots+k_{s-1}+1 \leq j \leq k_{0}+\cdots+k_{s-1}+k_{s}, k_{-1}=0
$$

are from $\Gamma+\theta \Gamma+\cdots+\theta^{m-s-1} \Gamma$.
Thus the generation of all submodules of ${ }_{R} M$ is equivalent to the generation of all matrices $C$ with properties (1) and (2). Unfortunately, the shape of the module generated by the rows of $B$ does not follow immediately from the shape of the matrix $C$, so we have to check this in a separate step.

Algorithm 6: The generation of all submodules
Input: a matrix $A$ in standard form whose rows generate a module of shape $\lambda=\left(\lambda_{1}, \ldots, \lambda_{k}\right)$;
a fixed shape $\mu=\left(\mu_{1}, \ldots, m u_{k}\right) \prec \lambda$
Output: a set of matrices whose rows generate all submodules of $M$ of shape $\mu$.

1: Find permutation matrices $T_{1}$ and $T_{2}$ to transform $A$ to $A^{\prime}$ which is of the form (1)

2: for every $k$-tuple $\left\{j_{1}, \ldots, j_{l}\right\} \subseteq\{1, \ldots, k\}$ do
3: $\quad$ for every $l$-tuple $\left(t_{1}, \ldots, t_{l}\right), t_{i} \in\{0, \ldots, m-1\}$
4: $\quad$ Set $c_{i j_{i}}=\theta^{t_{i}}, i=1, \ldots, l$
5: $\quad$ for every choice of the remaining elements of $C$ subject to (1) and (2)
6: construct the matrix C
7: $\quad$ if shape of $C A$ is $\mu$ then print: $C$
8: construct all matrices

Let us remark that the check of the shape in step [7:] can be avoided if we generate in step [3:] only such $l$-tuples that yield a submodule of shape $\mu$.

Example 1. Let $R=\mathbb{Z}_{4}$ and let $A$ be the matrix

$$
A=\left(\begin{array}{lllll}
1 & 0 & 1 & 1 & 2 \\
0 & 1 & 1 & 0 & 1 \\
0 & 0 & 2 & 0 & 0 \\
0 & 0 & 0 & 2 & 2
\end{array}\right)
$$

The module $M$ generated by the rows (but also by the columns) of $A$ is of shape $\lambda=(2,2,1,1)$. We want to generate all submodules $N \leq M$ of shape $\mu=(2,1)$. Their number is 84. We are going to construct the possible matrices $C$ that yield all subodules of shape $\mu$. The matrix $A$ is already in the required form so we skip step [1:]. In step [2:] we generate all possible positions for the leaders.

$$
\begin{aligned}
& \left(\begin{array}{llll}
\bullet & 0 & 0 & 0 \\
0 & \bullet & 0 & 0
\end{array}\right), \quad\left(\begin{array}{llll}
\bullet & 0 & 0 & 0 \\
0 & 0 & \bullet & 0
\end{array}\right), \quad\left(\begin{array}{llll}
\bullet & 0 & 0 & 0 \\
0 & 0 & 0 & \bullet
\end{array}\right) \\
& \left(\begin{array}{llll}
\circ & \bullet & \circ & 0 \\
\circ & \circ & \bullet & 0
\end{array}\right), \quad\left(\begin{array}{llll}
\circ & \bullet & 0 & \circ \\
\circ & \circ & 0 & \bullet
\end{array}\right), \quad\left(\begin{array}{llll}
\circ & \circ & \bullet & 0 \\
\circ & 0 & \circ & \bullet
\end{array}\right)
\end{aligned}
$$

In step [3:] we try all possibilities for the leaders. Some of them will give rise to submodules that are not of shape $\mu$. Using the remark before this example we have
the following possibilities for the leaders themselves.

$$
\begin{aligned}
& \left(\begin{array}{llll}
1 & \circ & \circ & \circ \\
\circ & 2 & \circ & \circ
\end{array}\right), \quad\left(\begin{array}{llll}
2 & \circ & \circ & \circ \\
\circ & 1 & \circ & \circ
\end{array}\right), \quad\left(\begin{array}{cccc}
1 & \circ & \circ & \circ \\
\circ & \circ & 1 & \circ
\end{array}\right) \\
& \left(\begin{array}{llll}
1 & \circ & \circ & \circ \\
\circ & \circ & \circ & 1
\end{array}\right), \quad\left(\begin{array}{llll}
\circ & 1 & \circ & \circ \\
\circ & \circ & 1 & \circ
\end{array}\right), \quad\left(\begin{array}{llll}
\circ & 1 & \circ & \circ \\
\circ & \circ & \circ & 1
\end{array}\right)
\end{aligned}
$$

Now we have the following possibilities to complete the matrix $C$. Note that the last two columns can contain only entries from $\Gamma=\{0,1\}$.

$$
\left.\begin{array}{c}
\left(\begin{array}{cccc}
1 & \Gamma & \Gamma & \Gamma \\
0 & 2 & 0 & 0
\end{array}\right), \quad\left(\begin{array}{cccc}
2 & 0 & 0 & 0 \\
0 & 1 & \Gamma & \Gamma
\end{array}\right), \quad\left(\begin{array}{ccc}
1 & R & 0 \\
0 & \operatorname{Rad} R & 1
\end{array}\right. \\
\Gamma
\end{array}\right)
$$

Here $R=\{0,1,2,3\}, \Gamma=\{0,1\}$, and $\operatorname{Rad} R=\{0,2\}$. Thus the number of matrices $C$ of the first type is 8; of the second type, 4; of the third type, 32; of the fourth type, 16; of the fifth type, 16; and of the sixth type, 8. This gives a total of

$$
8+4+32+16+16+8=84
$$

as already obtained.

## REFERENCES

[1] Nechaev A. A. Kerdock code in a cyclic form. Discrete Mathematics and Applications, 1 (1991), No 4, 365-384.
[2] Hammons A. R., Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé. The $\mathbb{Z}_{4}$-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. on Inf. Theory, 40 (1994), No 2, 301-319.
[3] Honold Th., I. Landjev. Linear codes over finite chain rings. In: Proc. of the International Workshop on Optimal Codes, Sozopol, 1998, 116-126.
[4] Honold Th., I. Landjev. Linearly representable codes over finite chain rings. Abh. Math. Semin. Univ. Hamburg, 69 (1999), 187-203.
[5] Honold Th., I. Landjev. Linear codes over finite chain rings. Electronic Journal of Combinatorics, 7 (2000), \#R11.
[6] Honold Th., I. Landjev. Linear codes over finite chain rings and finite projective geometries. In: P. Solé (ed.). Codes over Rings, World Scientific, 2009, 60-123.
[7] Honold Th., I. Landjev. Projective Hjelmslev geometries. In: Proc. of the International Workshop on Optimal Codes, Sozopol, 1998, 97-115.
[8] Honold Th., I. Landjev. Arcs in projective Hjelmslev planes. Discrete Mathematics, 11 (2001), No 1, 53-70. Originally published in: Diskretnaya Matematika, 13 (2001), 90-109 (in Russian).
[9] Landjev I. On blocking sets in projective Hjelmslev planes. Advances in Mathematics of Communications, 1 (2007), No 1, 65-81.
[10] Kiermaier M., I. Landjev. Designs in projective Hjelmslev spaces. In: M. Lavrauw et al. (eds). Theory and Applications of Finite Fields. Contemporary Mathematics, 579 (2012), 111-122.
[11] Georgieva N., I. Landjev. On the representation of modules over finite chain rings. Annuaire de l'Université de Sofia "St. Kliment Ohridski", 2017 (submitted).
[12] Nechaev A. A. Finite principal ideal rings. Math. USSR-Sb., 20 (1973), No 3, 364-382.
[13] McDonald B. R. Finite Rings with Identity. Marcel Dekker, New York, 1974.
[14] Lam T.-Y. Lectures on Modules and Rings. Graduate Text in Mathematics, 189. Springer Science \& Business Media, 1999.

Nevyana Georgieva
New Bulgarian University
21, Montevideo St.
1618 Sofia, Bulgaria
e-mail: nevyanag@fmi.uni-sofia.bg
Received March 15, 2017
Final Accepted May 16, 2017


[^0]:    ACM Computing Classification System (1998): G.1.3, G.4.
    Key words: chain rings, finitely generated modules over finite chain rings, the orthogonal module, linear codes over finite chain rings, standard form of a matrix over a chain ring.
    *This research was partially supported by the Scientific Research Fund of Sofia University.

