New Bulgarian University

Informatics Department

Nevyana Dimitrova Georgieva

NETWORK CODING AND ANALOGUES OF DESIGNS

Summary

of the PhD Thesis
in the professional field
4.6. Informatics

Scientific Advisor: Prof. DSc Ivan Landjev
Sofia, 2022

The thesis consists of 78 pages of text which is structured in an introduction, three chapters and a list of references, containing 85 items.

The present PhD thesis is devoted to the problem of the existence of designs in projective coordinate geomtries over finite chain rings. These geometries are usually referred to as Hjelmslev geometries. Their investigation was initiated in the beginning of the 20th century by the Danish mathematician Johannes Hjelmslev. A serious advance in the understanding of these structures was achieved in the works of Barbilian, Klingenberg, and Artman [1, 2, 3, 29, 30].

Coordinates of points in classic coordinate geometries are elements of a commutative or noncommutative field. The first step in the consideration of geometries over rings was made by Corrado Segre in 1911 in [49]. He considered a three-dimensional projective geometry over the ring of dual numbers $\mathbb{R}[\varepsilon]$ with $\varepsilon^2 = 0$, as well as geometries over some other extensions of $\mathbb{R}$. Chain rings over the real numbers were studied at this time also in the geometries of Grunveld, Petersen, Studi and Oscar Klein (see in [51]). Their appearance is not surprising and it has already happened in the mechanics. Through the period 1929-1949 Johannes Hjelmslev suggested "a more natural view to geometry" which is in "more precise correspondence with the physical reality" [19, 20, 21]. Systematic research of projective planes over a wide class of associative rings was started by D. Barbilian (1940-1941) [3]. The axiomatic rules he received were unsatisfactory because they are partly of geometric and partly of algebraic nature referring to the coordinate ring.

The investigations of Segre and Hjelmslev were extended by W. Klingenberg [29, 30], E. Kleinfeld [28], D.A Drake [7, 8, 9], P. Dembowski [6], A. Cronheim [5] and other authors. They introduced axiomatic rules for projective and affine planes over Hjelmslev's rings and described their main properties. These rings are local rings which satisfy some additional conditions.

The existence problem we study in this dissertation is motivated mainly by its link to coding theory, although, it also represents a geometrical problem. At the end of the 20th century it was proven that two famous families of nonlinear codes – those of Kerdock and Preparata [48], can be presented as binary images of codes over $\mathbb{Z}_4$ [43, 18]. The research of linear codes over general finite rings was started by Nechaev and J. A. Wood's works [42, 43, 44, 46, 47, 52, 53, 54, 55]. At about the same time, the research of linear codes was connected to the research of special sets of points in Hjelmslev geometries. In T. Honold and I. Landjev's works, the

equivalence of full length linear codes over finite chain rings and multisets of points in coordinate geometries over those rings was proven. [22, 23, 24].

The random network coding originates from one paper by R. Koetter and F. Kschischang from 2008 [31]. Let $\mathbb{F}_q$ be a finite field of order q and let $\mathcal{P}_q(n)$ be the set of all subspaces of $\mathbb{F}_q^n$ – the vector space of n-tuples over $\mathbb{F}_q$. We call a code of subsets Ω with length n over $\mathbb{F}_q$ every nonempty set of elements of $\mathcal{P}_q(n)$. Equivalently, one code of subsets can be considered as a set of subspaces in $\mathrm{PG}(n-1,q)$. A code Ω in which all the subspaces have the same dimension is called code with constant dimension. Below an example of such a code is given:

$$\Omega = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right\}$$

This is a binary code of subspaces with constant dimension 2 and package length 4. At the same time two-dimensional subspaces generated by the rows of these matrices can be considered as lines in $\mathrm{PG}(3,2)$. Moreover, these lines form a special configuration called a spread of lines in $\mathrm{PG}(3,2)$, i.e. a set of lines which is a partition of the set of points in $\mathrm{PG}(3,2)$. In this way every word is a line in $\mathrm{PG}(3,2)$.

Let us introduce a new metric in $\mathcal{P}_q(n)$ proposed originally by Delsarte and a bit later by Gabidulin. It is called the rank metric and it sets the distances between code words of a code of subspaces. For $U, V \in \mathcal{P}_q(n)$ we define:

$$\begin{aligned} d_S(U,V) &= \dim(U+V) - \dim(U \cap V) \\ &= \dim U + \dim V - 2\dim(U \cap V) \\ &= 2\dim(U+V) - \dim U - \dim V. \end{aligned}$$

The minimal distance of a code of subspaces is defined by

$$d_S(\Omega) = \min\left\{ d_S(U,V) |\ U, V \in \Omega, U \neq V \right\}.$$

Let the data transmission be done by the so-called operator channel [26] by using a code of subspaces Ω with package length n. Let during the transmission of the word U there occur ρ erasures and t mistakes and as a result the word

V is received. If $2(\rho + t) < d_S(\Omega)$ then a decoder working on the principle of decoding in the nearest neighbour (in the sense of the rank metrics) recovers the word U which was sent. There exist analogues for all classic bounds for codes in rank metrics, such as spherical packaging bound, Singleton bound, Johnson bound, Gilbert-Varshamov bound, etc.

The two major directions of research just like in classical coding theory, are:

- Constructing optimal network codes (for example with maximal number of words with all other parameters given),
- creating algorithms for efficient decoding of given network codes.

The present PhD thesis can be considered as a contribution to the first problem. The interest in codes of subspaces has appeared before their application in network coding. The problem of finding and characterizing q-analogues of classical combinatorial configurations is much older [38] (Chapter 24). Design theory is a well developed area and has obvious connections with coding theory. A lot of famous combinatorial results have their q-analogues, such as Sperner [50] and Erdős-Ko-Rado [10] theorems. The number of papers on q-analogues of designs increased in the past few years. Some problems were very popular such as the problem of the existence of q-analogues of a Steiner system [4, 11, 12, 14]. The result of this PhD thesis may be considered as a contribution to this circle of problems in which a finite field is replaced by a finite chain ring.

The present dissertation is structured in an introduction, three chapters and a list of used literature.

In **chapter 2**, we define the main objects studied in this PhD thesis as well as some important results related to them. In section 2.1, we introduce chain rings by the condition that their ideals form a chain by inclusion. Examples of some important classes of chain rings are introduced, such as the rings of the σ-dual numbers and the Galois rings. The main characterization theorem for chain rings is given. According to it every chain ring can be presented as a factor ring of polynomials over a certain Galois ring. Furthermore, a canonical representation of the elements of an arbitrary ring is presented, as well as a linear order over them which is used in the computer representation of the elements of such rings and in the algorithms for working with modules in **chapter 3**. The stated definitions are demonstrated on the example of a Galois ring with 16 elements over $\mathbb{F}_4$.

In section 2.2, we present some fundamental facts for modules over finite chain rings. The basic structure theorem for modules over chain rings, which is a corollary of the general Krul-Schmidt theorem, is formulated. Notions like the type, the dual type, the rank and the free rank of module are defined. Furthermore, we state the central combinatorial result of this section. It gives the number of the submodules of a given type μ which are contained in a fixed R-module of type λ. This number happens to be a product of Gauss' coefficients. A theorem characterizing the orthogonal module $M_R^{\perp}$ of a fixed module ${}_RM$ is formulated at the end of section 2.2.

In section 2.3, we give some important definitions for objects in projective Hjelmslev geometries. These geometries are defined in a similar way as the classical geometries $\mathrm{PG}(n-1,q)$ in which the finite field $\mathbb{F}_q$ is replaced by a chain ring R. For a given free-rank module $M = {}_RR^n$ the set of points consists of all submodules of M of free rank 1, lines are the submodules of M of free rank 2 and the incidence is defined by theoretical set inclusion. The difference from the classical case is that every two points are incident with *at least one line*; two points which are simultaneously incident with more than one line are called neighbors. Hjelmslev geometries can also be defined axiomatically. It is known [32, 33, 34, 35, 36] that under certain natural conditions they can be coordinatized by chain rings. A lot of results for classic geometries over finite fields have their analogues in Hjelmslev geometries [39, 40]. In this work, only coordinatized Hjelmslev geometries are considered.

Neighbour relation can be extended over lines and in general over subspaces of arbitrary type. It turns out that neighbour relation is equivalence relation over subspaces of one and the same type. The equivalence classes turn out to be well structured. They can be embedded in Hjelmslev geometries over chain rings with smaller nilpotency index. This important structure result is given in section 2.3.

The original contributions of this PhD thesis are contained in chapters 3 and 4.

Chapter 3 is devoted to the definition of a standard form of a matrix over chain ring R. This question is of huge practical importance because of the necessity of an effective way to represent submodules of ${}_RR^n$ and manipulations the need to perform computer manipulations with them. We say that the matrix $A = (a_{ij})_{k\times n}$, $a_{ij} \in R$, $\operatorname{rad} R = R\theta$ is in standard form if the following conditions are satisfied:

(1) $a_{ij_i} = \theta^{m-t_i}$, $t_i \in \{0, \ldots, m\}$;
(2) $a_{is} = \theta^{m-t_i+1}\beta$, $\beta \in R$, for every $s < j_i$;
(3) $a_{is} = \theta^{m-t_i}\beta$, $\beta \in R$, for every $s > j_i$;
(4) $a_{sj_i} \prec a_{ij_i}$ for every $s \neq i$ here $\prec$ is the lexicographic order defined in section 2.1);
(5) $j_1 < j_2 < j_3 < \ldots$.

The main result here is contained in the following theorem:

Theorem 3.3. For every R-module ${}_RM \leq {}_RR^n$ there exists a unique matrix in standard form whose rows generate the module.

Algorithms for working with modules are described in the remaining part of this chapter. These algorithms include:

(A) algorithms for finding the standard form of a matrix;
(B) algorithms for finding the matrix which rows generate the union of two given modules;
(C) algorithms that check whether a given module U is a submodule of other module V.

Next we state a result from which we can obtain the orthogonal module $M_R^{\perp}$ of a given module ${}_RM$ generated by the rows of a matrix in standard form. The orthogonal module is generated by the rows of a matrix over R which is explicitly given.

Theorem 3.8. Let ${}_RM$ be a submodule of ${}_RR^n$ generated by the rows of the matrix A in the form:

$$\begin{pmatrix} I_{k_0} & A_{01} & A_{02} & \ldots & A_{0,m-1} & A_{0,m} \\ 0 & \theta I_{k_1} & \theta A_{12} & \ldots & \theta A_{1,m-1} & \theta A_{1,m} \\ 0 & 0 & \theta^2 I_{k_2} & \ldots & \theta^2 A_{2,m-1} & \theta^2 A_{2,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \theta^{m-1} I_{k_{m-1}} & \theta^{m-1} A_{m-1,m} \end{pmatrix}.$$

Then $M_R^{\perp}$ is generated by the rows of the matrix:

$$B = \begin{pmatrix} B_{0,m} & B_{1,m} & B_{2,m} & \cdots & B_{m-2,m} & B_{m-1,m} & I_{k_m} \\ B_{0,m-1}\theta & B_{1,m-1}\theta & B_{2,m-1}\theta & \cdots & B_{m-2,m-1}\theta & I_{k_{m-1}}\theta & 0 \\ B_{0,m-2}\theta^2 & B_{1,m-2}\theta^2 & B_{2,m-2}\theta^2 & \cdots & I_{k_{m-2}}\theta^2 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ B_{02}\theta^{m-2} & B_{12}\theta^{m-2} & I_{k_2}\theta^{m-2} & \cdots & 0 & 0 & 0 \\ B_{01}\theta^{m-1} & I_{k_1}\theta^{m-1} & 0 & \cdots & 0 & 0 & 0 \end{pmatrix},$$

where $k_m = n - k_0 - \ldots - k_{m-1}$ and

$$B_{ij} = -(A_{ij} - \sum_{1<k<j+1} A_{ik}A_{k,j+1} + \sum_{i<k<l<j+1} A_{ik}A_{kl}A_{l,j+1} - \cdots + (-1)^{j-i+1}A_{i,i+1}A_{i+1,i+2}\ldots A_{j,j+1})^T.$$

Next we present further algorithms for:

(D) finding the orthogonal module $M_R^{\perp}$ of a given module ${}_RM$;
(E) finding the intersection of two given modules ${}_RM$ and ${}_RN$;
(F) generating all the submodules of fixed type of a given module ${}_RM$.

Chapter 4 is devoted to the problem of finding necessary and sufficient conditions for the existence of spreads in Hjelmslev projective geometries. In section 4.1, we describe R-analogues (analogues over the chain rings R) for different types of designs. Firstly, we describe the Grassmannian $\mathcal{G}_R(n,\kappa)$ as the set of all left submodules of ${}_RR^n$ of type κ, where $\kappa = (k_1, \ldots, k_n)$, $m \geq k_1 \geq \ldots \geq k_n \geq 0$. Then we describe the link between R-covering designs and Turan R-designs (Theorem 4.4). We find a necessary and sufficient condition for the existence of τ-(n,κ,l) designs – analogues of the classic t-(v,k,λ) designs. Geometric spreads are a special case of τ-designs with $\tau = (m, 0, \ldots, 0)$.

In section 4.2, we study the question of finding necessary and sufficient conditions for the existence of spreads in projective Hjelmslev geometries. In the classic case of spreads of r-dimensional subspaces in $\mathrm{PG}(n,q)$, the combinatorial necessary condition, which states that the number of points in the r-dimensional subspace should divide the number of points in $\mathrm{PG}(n,q)$, is also sufficient. The situation is much more complicated in the case of chain rings. It is known that in the classic case of spreads of free rank submodules the combinatorial necessary

condition is also sufficient. Main results in this section are contained in theorems 4.10-4.12, which we will define next.

Theorem 4.10 Let R be a chain ring of length m. If there exists a λ-spread in $\mathrm{PHG}({}_R R^n)$, where $\lambda = (\lambda_1, \ldots, \lambda_n)$, $\lambda_1 \geq \ldots \geq \lambda_n > 0$, then there exists also a μ-spread in the geometry $\mathrm{PHG}({}_{\widetilde{R}}\widetilde{R}^n)$, $\widetilde{R} = R/(\operatorname{rad} R)^{m-\lambda_n}$, where

$$\mu = (\lambda_1 - \lambda_n, \lambda_2 - \lambda_n, \ldots, \lambda_{n-1} - \lambda_n, 0).$$

Once again, let R be a fixed chain ring with $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Let also $q = p^r$ and $\operatorname{char} R = p^s$. Let us write m in the following way $m = (s-1)l + t$. The ring R may also be presented as (Theorem 2.2)

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

where $S = \mathrm{GR}(q^s, p^s)$ and σ is an automorphism of S. It is clear that $S/\operatorname{rad} S \cong \mathbb{F}_q$. We define a Galois extension $T = S[Y]/(f(Y))$ for the ring S, where f is irreducible over S and of power h. Let us now define the ring

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

Theorem 4.11 Let R be a chain ring with $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Let from here on Q be the extension of R we define earlier. Let $n = hl$ and let us assume that there exists a λ-spread in $\mathrm{PHG}({}_Q Q^l)$, with

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_l), \quad m = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_l \geq 0.$$

Then there exists a μ-spread in $\mathrm{PHG}({}_R R^n)$, with

$$\mu = (\underbrace{\lambda_1, \ldots, \lambda_1}_{h}, \underbrace{\lambda_2, \ldots, \lambda_2}_{h}, \ldots, \underbrace{\lambda_l, \ldots, \lambda_l}_{h}).$$

Teorema 4.12 Let R be an arbitrary chain ring with $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, and let n be an integer. For every divisor h of n and for every type λ:

$$\lambda = m^h (m-1)^{a_{m-1}h} (m-2)^{a_{m-2}h} \ldots 1^{a_1 h},$$

where $a_i \geq 0$ i $1 + a_1 + \ldots + a_{m-1} = \dfrac{n}{h}$, there exists a λ-spread in $\mathrm{PHG}({}_R R^n)$.

The question of the existence of spreads of submodules of types which are different from those mentioned in theorems 4.10–4.12 is of great interest. In section 4.3

we find types of submodules for which the combinatorial necessary condition is satisfied, but spreads do not exist. This fact is the stated in Theorem 4.13.

Scientific contibutions

The main scientific contributions of the present PhD thesis according to the author are:

(1) A standard form of a matrix over finite chain ring R is found. It has the property that for every finitely generated module ${}_RM$ there exists a unique matrix in standard form whose rows generate ${}_RM$.
(2) For a given right module ${}_RM$ generated by the rows of a matrix in standard form is found whose rows generate the orthogonal module $M_R^{\perp}$.
(3) Algorithms for working with modules are presented: finding a matrix in standard form which generates a given module, finding a module generated by given submodules, an algorithm which checks containment in a module, an algorithm generating the orthogonal module, an algorithm for finding the intersection of two modules, and an algorithm generating all the submodules of fixed type for a given module.
(4) Sufficient conditions for the existence of spreads of non-free rank submodules are proven.
(5) Examples for some types λ are constructed for which the combinatorial necessary conditon is not sufficient.

Publications on the PhD thesis

(1) N. Georgieva, Basic algorithms for manipulation of modules over finite chain rings, *Serdica J. Computing* **10**(2016), No. 3-4, 285–297. [24]
(2) N. Georgieva, I. Landjev, On the representation of modules over finite chain rings, *Ann. Sofia Univ. Math. and Inf.* **104**(2017), 89–98. [25]
(3) I. Landjev, N. Georgieva, Conditions for the existence of spreads in prijective Hjelmslev geometries, *Des. Codes Cryptogr.* **87**(2019), 785-794. (IF 1.524; Q2) [64]

The results ot the resent PhD thesis were reported on the following scientific confereces:

- Spring scientific session of FMI;
- Computer Science and Education in Computer Science, Fulda, Germany 2016;
- Computer Science and Education in Computer Science, Boston University, 2018;
- Computer Science and Education in Computer Science, Fulda, Germany, 2019
- International Workshop on Algebraic and Combinatorial Coding Theory, Pomorie 2012;
- International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk 2014, Russia;
- International Workshop on Algebraic and Combinatorial Coding Theory, Albena 2016;
- International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk 2018.

References

[1] B. Artmann, Hjelmslev-Ebenen mit verfeinerten Nachbarschaftsrelationen, *Mathematische Zeitschrift* **112** (1969), 163–180.

[2] B. Artmann, Desarguessche Hjelmslev-Ebenen n-ter Stufe, *Mitt. Math. Sem. Gießen* **91**(1971), 1–19.

[3] D. Barbilian, Zur Axiomatik der projektiven ebenen Ringgeometrien I und II, *Jahresbericht der DMV* **50**(1940) 179–229 und **51**(1941) 34–76.

[4] M. Braun, T. Etzion, P. Östergard, A. Vardy, A. Wasserman, Existence of q-analogs of Steiner systems, *Forum of Math.*, Pi, **4**(2016), E7.

[5] A. Cronheim, Dual numbers, Witt vectors, and Hjelmslev planes, *Geometriae Dedicata* **7** (1978), 287–302.

[6] P. Dembowski, *Finite Geometries*, Springer Verla, Berlin-Heidelberg-New York, 1968.

[7] D.A Drake, Projective extension of uniform affine Hjelmslev planes, *Math. Zeitschrift* **105**(1968), 196–207.

[8] D.A. Drake, On n-uniform Hjelmslev planes, *Journal of Combinatorial Theory* **9** (1970), 267–288.

[9] D.A. Drake, Nonexistence results for finite Hjelmslev planes, *Abh. Math. Sem. der Univ. Hamburg* **40**(1974), 100–110.

[10] P. Erdős, C. Ko, R. Rado, Intersection theorems for systems of finite sets, *Quarterly J. Math.* **12**(1961), 313-320.

[11] T. Etzion, A new approach to examining q-Steiner systems, *Electronic J. Combin.* **25**(2)(2018), #P 2.8.

[12] T. Etzion, S. Kurz, K. Otal, F. Özbudak, Subspace packings: constructiuons and bounds, *Des. Codes Cryptogr.* **88**(9)(2020), 1781–1810.

[13] T. Etzion, N. Silberstein, Codes and designs relkated to lifted MRD-codes, *IEEE Trans. Inf. Theory* **59**(2013), 1004-1017.

[14] T. Etzion, A. Vardy, On q-analogs of Steiner systems and covering designs, *Adv. Math. Comm.* **5**(2)(2011).

[15] P. Frankl, R. M. Wilson, The Erdős-Ko-Rado theorem for vector spaces, *J. Combin. Theory* Ser. A **43**(1986), 228–236.

[16] N. Georgieva, Basic algorithms for manipulation of modules over finite chain rings, *Serdica J. Computing* **10**(2016), No. 3-4, 285–297.

[17] N. Georgieva, I. Landjev, On the representation of modules over finite chain rings, *Ann. Sofia Univ. Math. and Inf.* **104**(2017), 89–98.

[18] A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Sole, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **IT-40**(1994), 301–319.

[19] J. Hjelmslev, Geometrie der Wirklichkeit, *Acta Mathematica* **40**(1916), 33-66.

[20] J. Hjelmslev, Die natürliche Geometrie, *Abh. des Math. Sem. der Univ. Hamburg* **2**(1923), 1–36.

[21] J. Hjelmslev, Einleitung in die allgemeine Kongruenzlehre I-VI, alles in *KGI Dansk. Vid. Selsk. Math. Fys. Medd.*, I. Mitt. **8**(1929); II. Mitt. **10**(129); III. Mitt. **19**(1942) no.12; IV. Mitt. **22**(1945) no.6; V. Mitt. **22**(1945) no.13; VI. Mitt. **25**(1949) no.10.

[22] T. Honold, I. Landjev, All Reed-Muller codes are linearly representable over the ring of dual numbers over $\mathbb{Z}_2$, *IEEE Trans. Inform. Theory*, **IT-45**(1999),700-701.
[23] T. Honold, I. Landjev, Linearly representable codes over chain rings, *Abh. aus dem Math. Seminar der Universität Hamburg* **69**(1999), 187–203.
[24] T. Honold, I. Landjev, *Electronic Journal of Combinatorics*, **7**(2000), No. 11.
[25] W. N. Hsieh, Intersection theorems for systems for systems for finite vector spaces, *Discrete Matrh.* **12**(1975), 1–16.
[26] W. Cary Huffman, Jon-Lark KIm, Patrick Solé, Concise Encyclopaediae of Coding Theory, Chapman and Hall/CRC, 2021.
[27] N. Johnson, V. Zha, M. Bilioti, Handbook of finite translation planes, Chapman & Hall/CRC, 2007.
[28] E. Kleinfeld, Finite Hjelmslev planes, *Illinois Journal of Mathematics* **3** (1959), 403–407.
[29] W. Klingenberg, Projektive und affine Ebenen mit Nachbarelementen, *Math. Zetschrift* **60**(1954), 384–406.
[30] W. Klingenberg, Desarguessche Ebenen mit Nachbarelementen, *Abh. Math. Sem. der Univ. Hamburg* **20**(1955), 97–111.
[31] R. Koetter, F. Kschischang, Coding for Errors and Erasures in Random Network Coding, *IEEE Trans. Inform. Theory* 54(8)(2008), 3579-3591. doi: 10.1109/TIT.2008.926449.
[32] A. Kreuzer, *Hjelmslev-Räume*, *Resultate der Mathematik* **12** (1987), 148–156.
[33] A. Kreuzer, Projektive Hjelmslev-Räume, Dissertation, Technische Universität München, 1988.
[34] A. Kreuzer, Hjelmslevsche Inzidenzgeometrie - ein Bericht, Bericht TUM-M9001, Technische Universität München, January 1990, Beiträge zur Geometrie und Algebra Nr. 17.
[35] A. Kreuzer, Fundamental theorem of projective Hjelmslev spaces, *Mitteilungen der Mathematischen Gesellschaft in Hamburg* **12** (1991), no. 3, 809–817.
[36] A. Kreuzer, A system of axioms for projective Hjelmslev spaces, *Journal of Geometry* **40**(1991), 125–147.
[37] I. Landjev, N. Georgieva, Conditions for the existence of spreads in prijective Hjelmslev geometries, *Des. Codes Cryptogr.* **87**(2019), 785-794.
[38] J. H. van Lint, R. M. Wilson, A Course in Combinatorics, Cambridge University Press, 1992, 2001.
[39] K. Mathiak, Ein Beweis der Dimensionsformel in projektiven Hjelmslevschen Räumen, *J. für die reine u. angew. Mathematik* **256**(1972), 215–220.
[40] K. Mathiak, Valuations of skew-fields and projective Hjelmslev spaces, Lecture Notes in Mathematics no.1175, 1986, Springer-Verlag.
[41] B.R. McDonald, Finite rings with identity, Marcel Dekker, New York, 1974.
[42] A.A. Nechaev, Finite principal ideal rings, *Russian Academy of Sciences. Sbornik. Mathematics* **20** (1973), 364–382.
[43] A.A. Nechaev, Kerdock code in a cyclic form, *Discr. Math. and Appl.* **1**no.4(1991), 365-384.

[44] A.A. Nechaev, Linear codes over modules and over spaces. MacWilliams'identity, Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl. (Victoria B.C., Canada), 1996, pp. 35–38.

[45] A.A. Nechaev, Finite rings with applications, in: handbook of Algebra vol. 5 (ed. M. Hazewinkel), Elsevier-North Holland, 2008, 217–319.

[46] A.A. Nechaev, A.S. Kuzmin, Linearly presentable codes, Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl. (Victoria B.C., Canada), 1996, pp. 31–34.

[47] A.A. Nechaev, A.S. Kuzmin, V.T. Markov, Linear codes over finite rings and modules, Preprint N 1995-6-1, Center of New Information Technologies, Moscow State University, 1995.

[48] F.P. Preparata, A class of optimum nonlinear double-error correcting codes, *Information and Control* **13**(1968), 378-400.

[49] C. Segre, La geometrie proiettive nei campi di numeri duali, *Atti Acad. Sci. Torino* **47**(1911), 114–133; 164–185.

[50] E. Sperner, Ein Satz über Untermengen einer endlichen Menge, *math. Z.* **27**(11)(1928), 544–548.

[51] F.D. Veldkamp, Geometry over rings, Handbook of Incidence Geometry – Buildings and Foundations (Francis Buekenhout, ed.), Elsevier Science Publishers, 1995, pp. 1033–1084.

[52] J.A. Wood, Extension theorems for linear codes over finite rings, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC) 12 (Teo Mora and Harold F. Mattson, Jr., eds.), Lecture Notes in Computer Science, no. 1255, Springer-Verlag, 1997, pp. 329–340.

[53] J.A. Wood, Duality for modules over finite rings and applications to coding theory, *American Journal of Mathematics* **121**(3) (1999), 555–575.

[54] J.A. Wood, Weight functions and the extension theorem for linear codes over finite rings, *Contemporary Mathematics*, vol. 225, American Mathematical Society, 1999.

[55] J. A. Wood, Foundation of linear codes over finite modules: the extension theorem and the MacWilliams identities, in: Codes over Rings (ed. P. Solé), World Scientific, 2009, 124–190.