R E P O R T

on a Thesis for awarding the degree "Doctor"

Scientific field: 4. Natural sciences, mathematics and informatics

Professional field: 4.6. Informatics

Title: Network coding and analogues of designs

Author: Nevyana Dimitrova Georgieva

Overview

The presented thesis deals with a problem which can be related to the area of finite geometry and design theory with straightforward applications to coding theory and particularly to the newly emerged area of random network coding. The main problem considered here is the proof of necessary and sufficient conditions for the existence of spreads in projective Hjelmslev geometries – these are the most simple of designs in these geometries. In the Galois geometries which are the coordinate geometries over finite fields, there exists a satisfactory necessary and sufficient condition for the existence of spreads. In the more complex geometries over finite chain rings the solution of this problem seems to be much more difficult. In this thesis, the author gives a solution for some important special cases.

State of the current research

My general impression is that the author is well acquainted with the state of the art and the most recent results in the research on the treated problems. A good deal of the investigations that are carried out are considered in the field as important theoretically. The author demonstrates deep knowledge of his field of research and capacity to apply his knowledge to the solution of important problems.

Methods

In his investigations the author uses a wide spectrum of mathematical methods that can be related to the fields of linear algebra, abstract algebra (rings and modules),

design theory. These methods are applied to related fields like finite geometry and ring geometries.

Brief description of the thesis

The presented thesis amounts 78 pages of text and consists of four chapters, and a list of references including 85 items. In what follows, I shall describe briefly the main results obtained in this dissertation.

Chapter 1 is introductory and contains a brief description of several subjects related to this thesis. Firstly, these are the coordinate geometries over finite chain rings, the so-called Hjelmslev geometries. Secondly, this is the theory of linear codes over finite rings. This theory was developed only recently in connection of the ring representation of the Kerdock and Preparata codes. It is followed by the geometric representation of the liear ring codes. Finally the author addresses the theory of the design analogues, as well as its connection with the network codes and the codes in the rank metric of Delsrate and Gabidulin. The second part of chapter 1 contains a brief overview of the main results obtained in the thesis.

Chapter 2 contains the main theoretical results used in the thesis. It is divided in three sections which deal with finite chain rings, finitely generated modules over finite chain rings and coordinate projective geoemtries over finite chain rings. The first section contains an interesting and a relatively unknown result which provides the characterization of the finite chain rings (Theorem 2.2). It was formulated by A. A. Nechaev and states that every finite chain ring is a certain factor of a Galois ring. A complete classification of the finite chain rings (up to isomorphism) is not known, but in the case of rings of nilpotency index 2 it was completed by Cronheim. Section 2.2 contains a description of the general structure of a module over a finite chain ring (Theorem 2.7), which is a well-known algebraic result. A central result in this section is Theorem 2.8 which gives a formula for the number of the submodules of type μ contained in a fixed module of some given type λ.

Section 2.3 contains several important results about Hjelmlsev geometries. The axiomatic definition by A. Kreuzer is presented. It turns out that when these geometries are desargeuesian and satisfy some mild additional conditions they are precisely the coordinate geometries over finite chain rings. These geometries have a more complex nested structure than the finite Galois geometries but nevertheless diplay some nice structural properties that are described in Theorems 2.11-2.14. For instance the factor geometry of an Hjelmslev geometry is again an Hjelmslev geometry but over a chain ring of smaller nilpotency index.

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

Chapter 3 deals with a problem which arises in connection with the representation (especially, computer representation) of a certain module. It is clear that each module

is unambiguously defined with the vectors of a basis, or by the rows of a certain matrix. But such representations are plenty and it is importatant to select one of them which is in a sense unique. This representation should be easy to work with in the following sense: it should admit easy comparison of modules, easy operation with modules (union, intersection), easy computation of the orthogonal module, easy generation of all submodules of a given type contained in some fixed module.

Such a representation is introduced in definition 3.1 and is called the standard form of a matrix. The central result in this chapter is Theorem 3.3. according to which for each module ${}_RM$ over a chain ring R there exists a unique matrix in standard form whose rows generate ${}_RM$. This theorem implies the important Corollary 3.4, which introduces the general form of a matrix representing a module of a given fixed type. Comparing with the theory of linear codes, formula (3.1) can be viewed as a generator matrix of the code in standard form. This form admits a relatively easy computation of a generator matrix for the orthogonal code.

Furthermore, the author describes in pseudocode several algorithms for manipulation of modules in which the introduced standard form is used. They include an algorithm for computation the standard form for a given matrix, algorithms for union and intersection of modules, an inclusion test, an algorithm for the generation of all submodules of a fixed type of a given module. The most interesting result until the end of the section is Theorem 3.8. It describes explicitly a matrix whose rows generate the orthogonal to a given module.

Chapter 4 is devoted to R-analogues of designs and to a special type of designs, the so-called spreads. This chapter is divided in three section.

In section 4.1, R-analogues of designs are introduced similarly to the q-analogues over a finite field $\mathbb{F}_q$: this is a family of submodules of type κ that contain each submodule of a fixed type the same number of tymes. In this section, some simple combinatorial facts are proved that explain the connections between the different types of designs. Some simple numerical necessary conditions for the existence of R-analogues of designs are also given. Towards the end of the section the author introduces spreads as a family of subspaces of a certain type in an Hjelmslev geometry that contain each point of $\mathrm{PHG}({}_RR^{n+1})$ exactly once. In this sense, they are even akin to the Steiner systems.

Section 4.2. isdevoted to the formulation of necessary and sufficient conditions for the existence of spreads of subspaces of certain type. The starting point is Theorem 4.7 (taken from a paper by Kiermaier and Landjev) according to which in the case of spreads of Hjelmslev subspaces (free submodules) there exists a necessary and sufficient condition for the existence of spreads that is similar to the one known for the Galois geometries.

In Theorem 4.8 the author gives a new necessary condition for the existence of

spreads that generalizes the condition from the theorem by Kiermaier and Landjev. This condition turns out not to be sufficient, as demonstrated in section 2.3. In Theorems 4.10–4.12 several sufficient conditions for the existence of spreads are proved that provide large classes of spreads of subspaces that are not Hjelmslev subspaces. The author formulates a hypothesis for a necessary and sufficient condition for the existence of spreads in the general case (arbitrary nilpotency index of the underlying ring, arbitrary dimension of the geometry).

Section 4.3 is devoted to the construction of an example which demonstrates that the combinatorial necessary condition for the existence of spreads is not always sufficient. It should be noted that this is not a counterexample to Theorem 4.8. This section contain just one result, Theorem 4.13, in which it is proved that for even n there exist no spreads in $\mathrm{PHG}({}_R R^n)$ of non-free submodules of type $\lambda = 2^{n/2}1^a$ for every a, $1 \leq a \leq \frac{n}{2}$. This theorem is proved for chain ring of nilpotency index 2. It provides a large class of subspaces for which the combinatorial necessary condition turns out to be not sufficient. This suggests that the proof of a general necessary and sufficient condition for spreads in Hjelmslev geometries is probably a tough problem.

Main results

The main contributions of this thesis amount to the following:

(1) A standard form of a matrix over a finite chain ring is introduced. This is the only matrix of the described form whose rows generate the given module.

(2) Algorithms for module manipulation are described that make use of the introduced standard form.

(3) A matrix in standard form is explicitly described whose rows generate the orthogonal to a given module.

(4) A new necessary condition for the existence of spreads of non-free subspaces is proved.

(5) Several new sufficient conditions for the existence of spreads of non-free subspaces are proved.

(6) A family of types is given for which the combinatorial necessary condition for the existence of spreads is not sufficient.

Remarks and comments

I have the following remarks, questions and comments related to this thesis:

(1) The generalized Gauss index from Theorem 2.8 does not depend on the nilpotency index of the ring R, but only on the types λ and μ and on the order of the residue field q. That is why the notation $\begin{bmatrix}\lambda\\ \mu\end{bmatrix}_q$ is better than $\begin{bmatrix}\lambda\\ \mu\end{bmatrix}_{q^m}$.

(2) It is interesting to generalize Theorem 4.13 to chain rings of arbitrary nilpotency index.

(3) The results of this thesis are reported at two workshops in coding theory and two spring sessions of the Faculty of Mathematics and Informatics. It would be desirable to report them also at more specialized conferences, where they could get a more adequate assessment.

Publications related to the thesis

The results in this thesis are published in three papers. The respective journals are as follows:

- Designs, Codes an Cryptography (IF 1.524, Q2)

- Annuaire de l'Universite de Sofia - 1 paper

- Serdica Journal of Computing - 1 paper

One of the papers is in a journal with an impact factor. The other papers are in journals that are refereed in Zentralblatt.
In one of the papers the candidate is the only author and in the other two she has one coauthor.

Authorship of the obtained results

I have been following the scientific output of the author for a long time. That is why I have no doubt that his contribution in this research is significant.

Citations

The candidate has attached no list of citations of the papers used in this thesis.

Authors summary

The author's summary is made according to the existing regulations and reflects properly the main results and contributions of this thesis.

Conclusion

This thesis is focused on problems from finite geometry, combinatorics and coding theory that are important for the theory and with obvious application to the network coding. This work answers some open problems of principal importance, and motivates new directions for an ongoing research. I am deeply convinced that the presented thesis **"Network coding and analogues of designs"** by **Nevyana Dimitrova Georgieva** contains results that are an original contribution to the finite geometry and design theory. The candidate demonstrates deep knowledge of the theory and capacity to develop it in new and important ways. With this, she meets the legal national requirements prescribed by the law, as well as the specific requirements of the INew Bulgarian University for the professional field 4.6 "Informatics". I assess **positively** the presented PhD Thesis and recommend to this panel to award **Nevyana Dimitrova Georgieva** the scientific degree "Doctor" in the scientific field 4. Natural Sciences, Mathematics and Informatics, Professional field 4.6 "Informatics".

Sofia, 10.06.2022 Member of the Scientific Panel:

(Assoc. Prof. DSc Assia Rousseva)