REVIEW
by Nikola Petkov Zyapkov, PhD,
Professor, Faculty of Mathematics and Informatics,
Bishop K. Preslavski University of Shumen

of a thesis titled „Finite geometries and codes" by Assia Petrova Rousseva submitted for acquiring the scientific degree of "Doctor of Science" in professional field: "4. Natural sciences, mathematics and informatics", professional area: "4.5. Mathematics", doctoral program "Geometry".

General presentation of the received materials

By order No P 38-186/ 14.05.2020 from the Sofia University (SU) "St. Kliment"'s Rector I'm appointed as a member of the scientific jury in the procedure for thesis defense of a dissertation titled "Finite geometries and codes" by Assoc. Prof. Assia Petrova Rousseva, PhD for acquiring the scientific degree of „Doctor of Science" in professional field: "4. Natural sciences, mathematics and informatics", professional area: "4.5. Mathematics", doctoral program "Geometry".

All materials send to me are in accordance to SU rules as well as LDASRB (Law for the development of the academic staff in the Republic of Bulgaria).

Relevance of the topic and advisability of goals and objectives of the thesis

This work is dedicated to research in the field of finite geometries that are connected to the theory error-correcting codes. Modern coding theory was established in the 1948 with Shannon's seminal work

C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J., 27 (1948), 379-423, 623-656.

The goal was to solve the following Main problem in data transmission over distance:

There are errors generated by noise in the channel.

In the years following Shannon's work, linear codes became the most researched class of block codes. They possess nice mathematical structure that makes them easy to describe and analyze thus there are effective decoding algorithms. Linear codes over finite filed with q elements have three major parameters: length n, dimension k and minimal distance d and are denoted by: $(n,k,d)_q$. The best codes amongst all with fixed two of those parameters are those codes that have optimal third parameter. Natural low bound for the length n is the so called Griesmer bound. One of the main research goals in coding theory is finding codes that meet the known bounds and when such codes does not exist, we try to sharpen the known bounds and find codes with best parameters.

In the 80-s and 90-s of the XX-th century it was discovered that the main problem of coding theory has geometric nature and may be reformulated as a problem of distributing points in a projective geometry over finite field.

In the last few years, several very important results for linear codes over finite fields were proved. All they were obtained as results for special sets of points in finite geometries. The most important of them are the following: S. Ball, H. N. Ward, A. Bruen, A. Blokhuis, F. Mazzocca among others.

Characteristics and evaluation of the dissertation

The thesis is structured as follows: introduction (denoted as chapter one), four chapters, and references; the total number of pages in 180. The references are a total of 201 papers and monographs.

In the introduction some classical recent geometric results related closely to coding theory are shown. These results mainly focus on optimal codes over finite fields and are established by propositions of special sets of points in finite geometries. A short summary of the main results in this thesis is also included in this chapter.

Chapter two has a great merit in the thesis. This section contains definitions and results on finite projective geometries, special pointsets in finite projective geometries and linear codes over finite fields. In §2.1 the finite projective spaces PG(r, q) over the fields F_q are described and the so-called fundamental theorems of projective geometry are formulated. Furthermore, the notions of arc and blocking set as special multisets of points in PG(r, q), are shown. Some special constructions for arcs the most important of which are subspace and dualization, i.e. construction of the so-called σ-dual arc. In §2.2 classes of important arcs are described and a classification of arcs in small projective plains is shown. § 2.3 is mainly focused on linear codes over finite fields. Basic notions as well as some classical bound are described: the Singleton bound, the Gilbert-Varshamov bound, the generalized Singleton bound and the Griesmer bound. In § 2.4 a description of the connection between linear codes and the multisets of points in the geometries in PG(r, q) is shown. Versions of important results about linear codes such as the theorems Ward about the divisibility of codes meeting the Griesmer bound, and the extendibility theorem by Hill and Lizak are also here. Some improvements of Hill-Lizak theorem, following from a result by Beutelspacher for blocking set, are shown. At the end of the section a table that describes the correspondence between some notions from coding theory and finite geometry is given.

The next three chapters contain the original results included in this thesis.

The main goal in chapter three is the achievement of Griesmer bound

$$n > g_q(k,d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

and a geometric characterization of the codes meeting this bound.

Codes whose parameters satisfy this bound with equality are called Griesmer codes and the arcs associated with these codes are called Griesmer arcs.

It is essential to study the behavior of the function $t_q(k)$, equivalent formulations of the problem of determining the maximal deviation from the Griesmer bound:

$$t_q(k) := \max(n_q(k,d) - g_q(k,d)).$$

Stefan Dodunekov first showed that if d is fixed and k grows to infinity therefore $t_q(k) \to \infty$. In § 3.1.-3.3 the rate of the growth is studied.

In §3.1 a new proof of the Dodunekov's theorem for infinite growth of $t_q(k)$ as a function of k. After that some results which simplify the investigation of $t_q(k)$ are derived. The most important is the following:

Lemma 3.6. *If* $n_q(k, d) = g_q(k, d) + t$, *then* $n_q(k, d + q^{k-1}) < g_q(k, d + q^{k-1}) + t$.

The main result in § 3.2 is Theorem 3.10 which can be viewed as a generalization of the construction by Belov, Logachev and Sandimirov.

Important result in §3.3 is the proof of Ball's conjecture for arcs in Desarguesian plains of even order.

In § 3.4 new exact values of $n_q(k, d)$ for $q = 4$, $k = 5$ are shown. For codes over the field F_4, $k = 5$ is the smallest dimension, for which there still exist minimum distances d, such that the exact value $n_4(5, d)$ is not known. The characterization of the arcs with parameters (118, 30) is made in Lemmas 3.20-3.25. A (118, 30)-arc in PG(3, 4) is of one of the following types: (a) $K = 2 - F$, where F is a (52,12)-blocking set, F is the sum of two plains and two lines chosen such that the maximal point multiplicity is 2. Two spectrae are shown. The proof of the following results is completed:

- Every (117, 30)-arc in PG(3, 4) is extendable.
- The nonextendable (100, 26)-arc in PG(3, 4) is not unique.

Later in the chapter the proofs of nonexistence of arcs associated with Griesmer codes is performed.

The exact values of $n_4(5,d)$ for ten minimal distances d = 295, 296, 297, 298, 347,..., 352 are calculated. At the end of chapter 3 there is a table of all values of d for which the exact values of $n_4(5,d)$ are still an open question.

In chapter 4 an investigation of the extendability problem for arcs in projective geometries and, equivalently for the linear codes associated with them is performed. The investigations on the extendability of arcs were initiated before the corresponding problem for codes and are performed independently. In this chapter a new geometric approach to the extendability problem for codes and arcs is shown, the aim is to formulate conditions under which an (n,w)-arc in PG(r, q) is extendable to an $(n+1,w)$-arc by increasing the multiplicity of one point The main idea is to relate the extendability of a given arc K with the structure of a special arc K in the dual geometry.

In §4.1 the new special class of arcs called (t mod q)-arc is introduced. These are obtained by a special dualization of arcs with the property t-quasidivisibility, which in turn, are associated with Griesmer codes with minimal distance $d \equiv -t \pmod q$. The main result here is the following: a sufficient condition for c-fold extendability of an arc K which is t-quasidivisible is that the dual arc K is a sum of c hyperplanes and some other arc (follows from T4.3)

In § 4.2 the structure of (t mod q)-arcs unrelated to the extendability problem is investigated. The main result is:

Theorem 4.12. *The vector space of all* (0 mod p)*-arcs in* PG(r, p) *is generated from the complements of the hyperpalnes.*

In § 4.3 (t mod q)-arcs, in which the maximal point multiplicity is t. The main result is the following:

Theorem 4.21. Every (3 mod 5)-arc F in PG(3, 5) of cardinality $|F| \leq 158$ is a lifted arc from a 3-point. In particular, $|F| = 93$, 118, and 143.

This result is used further in section 4.5 to prove the nonexistence of (104, 22)-arcs in PG(3, 5).

In § 4.4 the extendability of Griesmer arcs having the property t-quasidivisibility modulo q are investigated. The main result is in T4.26 which for linear codes states:

Let K be a Griesmer $(n, n-d)$*-arc in* PG$(k-1, q)$*, which is t-quasidivisible and let d be presented in the form*

$$d = sq^{k-1} - \sum_{i=0}^{k-2} \varepsilon_i q^i,$$

where $0 \leq \varepsilon_i < q$ *for all* $i = 0, \ldots, k-2$. *If for the numbers* ε_i *we have the following inequalities*

$$t = \varepsilon_0 < \sqrt{q}, \varepsilon_1 < \sqrt{q}, \ldots, \varepsilon_{k-2} < \sqrt{q},$$

then C is t-extendable, i.e. there exists a linear code with parameters $[n+t, k, d+t]_q$.

In § 4.5 it is proven the nonexistence of (104, 22)-arcs in PG(3, 5) and their associated $[104, 4, 82]_5$ codes.

In Chapter 5 a new constructions of affine blocking sets are shown. The main problem is the finding of the maximal cardinality of affine blocking set in relation to hyperplains. This problem shows connections to coding theory: the existence of affine blocking sets is equivalent to the existence of words with high weight (close to the code's length) in linear codes over finite fields.

§ 5.1 contains a survey of the known lower bounds on the cardinality of a blocking set in AG(n,q).

§5.2 presents a new general construction for affine blocking sets that are optimal or near optimal. This construction is described in T5.6.

In §5.3 are presented several applications of the general construction from Theorem 5.6. and its corollaries, that give blocking sets with good parameters (small cardinality). For example, as a special case of Corollary 5.7 Theorem 5.12 is derived and it is shown that these are a new class of blocking sets meeting the Bruen bound.

Main contributions of the thesis

After getting acquainted with the dissertation, I find that the main goals and objectives of the dissertation are fulfilled. I accept the contributions described in the conclusion of the dissertation, namely:

- The function $t_q(k)$, is investigated, defined as the maximal deviation from the Griesmer bound of an optimal q-ary code of dimension k. It is proved that for even dimensions it holds $t_q(k) \hat{} \omega q^{k/2}$. In case of $k = 4$ the inequality $t_q(4) \leq q - 1$ is proved.

- The inequality $t_q(3) < \log_2 q - 1$ for the case of q even is proved. This gives a partial solution of one hypothesis of S. Ball about plane arcs (threedimensional codes). For even powers of odd prime numbers q the weaker inequality $t_q(3) < \sqrt{q} - 1$ is proven.

- The nonexistence of hypothetical Griesmer arcs (and Griesmer codes) for $q = 4$, $k = 5$ is proved for the following minimal distances d:

$$d = 295, 296, 297, 298, 347, 348, 349.$$

These results solve ten open cases for the function $n_4(5,d)$. This reduces the number of the open cases to 98.

- A new geometric object called a (t mod q)-arc is introduced. It is proved that the extendability of a t-quasidivisible arc K is equivalent to the existence of a hyperplane in the support of special dual arc K, which is a (t mod q)-arc.

- It is proved that every (0 mod p)-arc, p – a prime, is a sum of complements of hyperplanes. In particular, every (t mod p)-arc is a sum of lifted arcs from arcs in geometries in smaller dimension. In the case of plane arcs, it is proved that every (t mod p)-arc is a sum of at most p lifted arcs.

- A partial characterization of the (3 mod 5)-arcs in PG(2, 5) and PG(3, 5) is made.

- A proof of the nonexistence of (104, 22)-arcs in PG(3, 5) is given. Equivalently, this proves the nonexistence of linear codes with parameters $[104, 4, 82]_5$. This determines the exact value of $n_4(5, d)$ in one of the four open cases for d.

- A new general construction for affine blocking sets is described. As a special case a new infinite class of t blocking sets with $t=q-n+2$ meeting the Bruen bound is constructed. This is the third example of blocking sets meeting the Bruen bound. This class gives rise to an infinite family of optimal affine blocking sets with $t=q-n+1$. These blocking sets meet the first bound by S. Ball from 2000.

- Five examples of blocking sets meeting the bounds by Ball and Ball–Blokhuis are constructed: (28, 4) in AG(5,4), (40,4) in AG(9,4), (52,4) in AG(13,4), (64, 4) in AG(17,4), (120,8) in AG(9,8).

These are the first examples for blocking sets meeting these two bounds.

An assessment of the publications included in the thesis

The results included in the thesis are published in 7 scientific papers (of these six are already published and one is accepted for publishing).

These results are presented in the following scientific journals:

- [131] *Designs, Codes and Cryptography* , IF 1,224 , Q2.
- [130] *Adv. Math. Comm.*,IF 0,8 ; Q3.
- [164] *Compt. Rend. Acad. Bulg. des Sciences,*IF 0,321, Q4
- [129] *Ann. de l'Univ. de Sofia* ,Ref: Zhl-MATH
- [127] *Probl. Inf. Transmission*
- [128] *Advances in Mathematics of Communications*
- [165] *Ann. de l'Univ de Sofia (to appear),* Ref: Zhl-MATH

Of the above papers: in two Assoc. Prof. Rousseva is the sole author, and all the rest are coauthored by Ivan Landjev.

There are 13 citations to the publications included in this thesis, of which 11 are in scientific papers published in impact factor journals.

The publications and citations meet the minimal national requirements for the scientific degree of „Doctor of Science" in professional area: "4.5. Mathematics", (indicator 7 – 177 pts, indicator 11 - 104 pts).

The contributions of the thesis have been reported in a large number of scientific conferences at home and abroad (this is reflected in the dissertation on page 15).

Thesis abstract

The abstract has a total of 28 pages and describes the thesis's main results. I believe that the abstract correctly reflects the main goals of the thesis and the contributions of the candidate. It gives a complete picture of the studied problems, the obtained results and their approbation.

Conclusion

The thesis contains scientific and applied scientific results that are original contributions in the field of Mathematics. The thesis complies with the LDASRB, the RALDASRB (Rules on the application of LDASRB) and the SU "St. Kliment"'s requirements for awarding the scientific degree „Doctor of Science" in professional area: "4.5. Mathematics".

All materials and thesis results **fully** comply to specific requirements of FMI and SU that are accepted in regard to RALDASRB.

All mentioned above give me a reason to give my ***positive assessment*** of the presented research, the above reviewed thesis, the thesis's abstract, the main results and contributions. Therefore, ***I propose to the esteemed scientific jury to award the scientific degree "Doctor of Science"*** to Assoc. Prof. Assia Petrova Rousseva, PhD in professional field: "4. Natural sciences, mathematics and informatics", professional area: "4.5. Mathematics", scientific speciallity "Geometry".

17.06.2020 Reviewer: