Sofia University "St. Kliment Ohridski

Faculty of Mathematics and Informatics

Assia Petrova Rousseva

FINITE GEOMETRIES AND CODES

Abstract

of a dissertation
for awarding the degree "Doctor of Sciences"
in the professional field
4.5. Mathematics

Sofia, 2020

This DSc Thesis contains 180 pages of text structured in five chapters and list of references containing 201 titles.

The present work contains results on problems from finite geometry that are related to the theory of error-correcting codes. These two areas of mathematical research emerge at the same time and develop independently from each other for some time. The birth date of coding theory is the publication of C.SHANNON's remarkable paper [50], where he proves that for every rate strictly less than the capacity of a given channel there exist block codes and a decoding rule such that the decoding error is less than any fixed constant. Unfortunately, the random codes introduced in this paper are of such big length that their practical use is completely excluded. In this connection, the converse theorem is of great practical importance: in cases where the rate of the used codes is greater than the capacity of the channel data transmission with arbitrarily small decoding error is impossible. From practical point of view it is very important to have "good" codes and algorithms for their decoding. Usually good codes are considered to be such codes whose parameters are meeting, or lying close to the known theoretical bounds.

In the years after SHANNON's paper, linear codes become the most investigated class of block codes. The presence of a good mathematical structure makes them easy to describe and work with and leads to effective decoding algorithms. It has to be noted that although the general decoding problem for linear codes is NP-complete [12], this does not exclude the existence of linear codes for which there exists an effective decoding algorithm.

The intensive investigation of finite geometric structures starts around 1950 although there exist single earlier results. So, for instance, G. FANO in his paper [20] investigated the possibility of coincidence of the fourth harmonic point with its conjugate. This leads to the construction of a three-dimensional space with 15 points, 35 lines and 15 planes, known today as $\mathrm{PG}(3,2)$. In 1955 B. SEGRE proves in [49] that every set of $q+1$ points in $\mathrm{PG}(2,q)$, q odd, no three of which are collinear, is a conic. The following years are marked by intensive investigations in finite geometry. The research in coding theory during the same period leads to the rediscovery of many geometric results. In the early 70's the deep connection between the linear codes and the sets of points in the finite geometries becomes much more visible. Central results, which influence the research in coding theory to a big extent, are the discovery of the algebraic-geometric codes by V. GOPPA [22, 23, 24], the construction of the 56-cap by R. HILL [28, 29], as

well as the construction by M. Tsfasman, S. Vladut and Th. Zink [54] of a family of algebraic-geometric codes that improve asymptotically the Gilbert-Varshamov bound [21, 55].

In the 80s and the 90s of the 20th century it became clear that the so-called main problem in coding theory has a geometric nature and can be stated in a natural way as a distribution problem for points in certain geometries over a finite field. In its most popular form it can be stated as the problem of minimizing the length of linear code over a fixed field given its dimension and minimum distance. A natural lower bound for the length of a linear code is the so-called Griesmer bound [26, 51]. Of great importance is the characterization of the codes that meet this bound. Despite the huge progress due to the research of various authors such as B. I. Belov, V. N. Logachev, V. P. Sandimirov, S. Dodunekov, N. Manev, I. Buyukliev, N. Hamada, R. Hill, T. Helleseth, H. van Tilborg, T. Maruta, L. Storme this problem is not solved for arbitrary fields.

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's proof for the maximal cardinality of a set of points in general position in $\mathrm{PG}(r, p)$, p a prime [2, 8]; this is equivalent to the celebrated MDS-hypothesis in coding theory about the maximal length of a MDS-code over a field;

- H. N. Ward's theorem about the divisibility of linear codes meeting the Griesmer bound [56];

- Bruen's lower bound for the cardinality of a t-fold blocking set in a finite affine geometry $\mathrm{AG}(n, q)$ [15], as well as its improvements made by S. Ball and A. Blokhuis [3, 6];

- the non-existence proof for maximal arcs in finite projective planes of odd order by S. Ball, A. Blokhuis, and F. Mazzocca [5, 7].

In this thesis we present solutions of problems from finite geometry that are directly connected to problems from coding theory. Although all results are stated in its geometric form, their re-formulation in coding theoretic terms is clear and straightforward. Below we give a concise description of all results in this thesis.

Chapter 1. Introduction. The first chapter is introductory. It contains some classical recent geometric results related closely to coding theory. Further the chapter contains a brief summary of the main results in this thesis.

Chapter 2. Preliminaries. This section contains definitions and results on finite projective geometries, special pointsets in finite projective geometries and linear codes over finite fields. In Section 2.1 we introduce projective geometries over finite fields. In this section we describe the finite projective spaces $\mathrm{PG}(r,q)$ over the fields $\mathbb{F}_q$ and formulate the so-called fundamental theorems of projective geometry. Furthermore, we define the notions of arc and blocking set as special multisets of points in $\mathrm{PG}(r,q)$, in which the multiplicity of every hyperplane is upperbounded (resp. lowerbounded). We introduce some special constructions for arcs (resp. blocking sets). The most important constructions are projection from a subspace and dualization, i.e construction of the so-called σ-dual arc for a fixed function σ. In Section 2.2 we describe classes of important multisets of points such as n-arcs, (n,w)-arcs and n-caps. The classification of some arcs in small projective planes used throughout this text is also given. Section 2.3 deals with linear codes over finite fields. We define basic notions such as linear code, the orthogonal of a given code, a generator and a parity check matrix of a linear code, the spectrum and the weight enumerator of a linear code. Several important bounds on the parameters of a linear code are presented. These include the Singleton bound, the Gilbert-Varshamov bound, the generalized Singleton bound and the Griesmer bound. In Section 2.4 we describe the connection between the k-dimensional linear codes and the multisets of points in the geometries $\mathrm{PG}(k-1,q)$. We present geometric versions of important results about linear codes such as the theorems by H. N. Ward about the divisibility of codes meeting the Griesmer bound, and the extendability theorem by Hill and Lizak. We describe some improvements of the Hill-Lizak theorem following from a result by Beutelspacher [13] on blocking sets. At the end of the section we give a table that describes the correspondence between some notions from coding theory and finite geometry.

The following three chapters contain the original results of this thesis.

Chapter 3. Arcs and optimal codes. The main subject in this section is the achievement of the Griesmer bound and a geometric characterization of the

codes meeting this bound. The GRIESMER bound says that for a linear code with parameters $[n,k,d]_q$ the following inequality holds true:

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

Codes whose parameters satisfy this bound with equality are called GRIESMER codes. The arcs associated with these codes are called GRIESMER arcs. A large class of GRIESMER codes was constructed by BELOV, LOGACHEV and SANDIMIROV in [11]. Their construction consists in deletion of simplex codes of small dimension from a concatenation of simplex codes of dimension k. Geometrically this construction is more natural: it consists in deletion of a blocking set from several copies of $\mathrm{PG}(k-1,q)$. The minimal length n, for which there exists an $[n,k,d]_q$-code for fixed k, d and q, is denoted by $n_q(k,d)$. It turns out that the following representation of D is very convenient:

$$d = sq^{k-1} - \lambda_{k-2}q^{k-2} - \ldots - \lambda_1 q - \lambda_0, \tag{2}$$

where $0 \leq \lambda_i \leq q-1$. In this case,

$$g_q(k,d) = sv_k - \lambda_{k-2}v_{k-1} - \ldots \lambda_1 v_2 - \lambda_0 v_1, \tag{3}$$

where $v_i = (q^i-1)/(q-1)$.

A central problem is to determine the behavior of the function $t_q(k)$ defined as the maximal deviation of the optimal length of a code of dimension k from the value given by the GRIESMER bound:

$$t_q(k) := \max_{0 \leq d < \infty} (n_q(k,d) - g_q(k,d)), \tag{4}$$

where the field $\mathbb{F}_q$ is fixed. It is known [30] that for any fixed dimension k there exists a constant $\delta(k,q)$ such that $n_q(k,d) = g_q(k,d)$ for all $d \geq \delta_q(k,d)$. Fix d and let k tend to infinity. Then $(n_q(k,d) - g_q(k,d)) \to \infty$, whence also $t_q(k) \to \infty$. This fact is not trivial and is noted for the first time by DODUNEKOV in [18]. In Sections 3.1–3.3 we investigate the rate of this growth.

In Section 3.1 we give three equivalent formulations of the problem of determining the maximal deviation from the GRIESMER bound of the best codes of fixed dimension over a fixed field. Formally, this is equivalent to finding the rate of growth of the function $t_q(k)$ defined by (4). The three formulations are in

terms of linear codes, arcs, and blocking sets (or minihypers) in $\mathrm{PG}(k-1,q)$, respectively.

Problem A. *Given a power of a prime q and a positive integer k, find the minimal value t for which there exist $[g_q(k,d)+t,k,d]_q$-codes for all d.*

Problem B. *Given a power of a prime q and a positive integer k, find the minimal value t for which there exists an arc with parameters $(g_q(k,d)+t, w_q(k,d)+t)$ in $\mathrm{PG}(k-1,q)$ for all d.*

Problem C. *Given a power of a prime q and a positive integer k, find the maximal value t such that for all d given by (2) there exists a minihyper in $\mathrm{PG}(k-1,q)$ with parameters*

$$(\sigma v_k + \lambda_{k-2}v_{k-1} + \lambda_1 v_2 + \lambda_0 v_1 - t, \sigma v_{k-1} + \lambda_{k-2}v_{k-2} + \lambda_1 v_1 - t),$$

with maximal point multiplicity not exceeding $\sigma + s$.

We start the section with a new proof of Dodunekov's theorem on the unbounded growth of $t_q(k)$ as a function of k. Furthermore, we prove several results simplifying the investigation of $t_q(k)$. One of the important lemmas is the following.

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

It follows by this lemma that it is enough to compute the maximum in (4) only for a finite number of values for d:

$$t_q(k) := \max_{0\le d<q^{k-1}-q^{k-2}} (n_q(k,d) - g_q(k,d)). \tag{5}$$

The main result in section 3.2 is Theorem 3.10, which can be viewed as a generalization of the construction by Belov, Logachev and Sandimirov for non-Griesmer codes.

Theorem 3.10. *Let $d = sq^{k-1} - \lambda_{k-2}q^{k-2} - \ldots - \lambda_1 q - \lambda_0$, and let the multiset $\mathcal{F}$ be a minihiper in $\mathrm{PG}(k-1,q)$ with parameters*

$$(\sigma v_k + \lambda_{k-2}v_{k-1} + \ldots + \lambda_0 v_1 - \tau_1, \sigma v_{k-1} + \lambda_{k-2}v_{k-2} + \ldots + \lambda_1 v_1 - \tau_1).$$

Define a new multiset $\mathcal{F}'$ in the following way:

$$\mathcal{F}'(x) = \begin{cases} \mathcal{F}(x), & \text{if } \mathcal{F}(x) \le \sigma + s, \\ \sigma + s, & \text{if } \mathcal{F}(x) > \sigma + s. \end{cases}$$

Let $N = |\mathcal{F}|$ and $N' = |\mathcal{F}'|$. If $\mathcal{F} - \mathcal{F}'$ is an $(N - N', \tau_2)$-arc then there exists a $(g_q(k,d) + t, w_q(k,d) + t)$-arc in $\mathrm{PG}(k-1,q)$, or, equivalently, a linear code with parameters $[g_q(k,d) + t, k, d]_q$, where $t = \tau_1 + \tau_2$.

Geometrically, this construction consists in deleting a blocking set obtained as a sum of subspaces of given dimensions from the s-fold sum of the whole geometry $\mathrm{PG}(k-1,q)$. The problem is that in the constructed blocking set there might appear points of multiplicity greater than s. The idea of Theorem 3.10 is to cut down the multiplicities of such points and replace them by points of multiplicity exactly s. In such case, some hyperplanes turn out to be underblocked and have to be compensated for by taking some additional suitably chosen points.

There is a lot of freedom in the choice of subspaces that form the blocking set to be removed in Theorem 3.10. For geometries of odd dimension, i.e. the geometries $\mathrm{PG}(2l-1,q)$, there exist spreads of $(l-1)$-dimensional subspaces which can be used to construct the blocking sets needed. Using this idea, we prove an estimate on on $t_q(k)$ in the case of even k.

Theorem 3.13. *If $k = 2l$, then*

$$t_q(k) \leq 2\frac{q^l - 1}{q - 1} - (2l + q - 1).$$

Asymptotically, we get $t_q(k) \lesssim q^{k/2}$, whence we obtain the following interesting corollary.

Corollary 3.14. $t_q(4) \leq q - 1$.

This result gives a partial answer to the question of determining the growth of $t_q(4)$ as a function of q. This is an interesting modification of the main question about the behavior of the function $t_q(k)$. In the case of plane arcs, the problem of finding the asymptotics of $t_q(3)$ as a function of q was asked by S. Ball [4]. He even made the conjecture that

$$t_q(3) \leq \log q.$$

In section 3.3 we investigate the problem of the rate of growth of $t_q(3)$. First, we prove that if there exists an (n,w)-arc in $\mathrm{PG}(2,q)$ with $n = (w-1)q + w - \alpha$, then there exists an $[n,3,d]_q$-code, where $d = n - w$ and $n = t + g_q(3,d)$, with $t = \lfloor \alpha/q \rfloor$ (Lemma 3.15). This relates the trivial upper bound for the size of an

arc to the deviation from the GRIESMER bound of the parameters of the code associated with this bound. The main result in this section is a proof of BALL's conservative estimate for the possible deviation of the best 3-dimensional linear codes from the GRIESMER bound. The idea resembles DENNISTON's construction for maximal arcs in planes of even order. We construct a family of arcs that are a sum of suitably chosen maximal arcs. Such arcs do exist in planes of even order by various constrictions [17, 46, 52, 53]. Our theorem is based on two lemmas.

Lemma 3.16. *Let $q = 2^h$ and let $\mathcal{K}_i$, $i = 1, \ldots, r$, be maximal arcs. Define the arc $\mathcal{K} = \sum_{i=1}^{r} \mathcal{K}_i$. If the code $C_{\mathcal{K}}$, associated with $\mathcal{K}$, has parameters $[n, 3, d]_q$, then $n = g_q(3, d) + (r - 1)$.*

Lemma 3.17. *Let $q = 2^h$. Every integer $m \leq q$ can be represented in the form $m = 2^{a_1} + \ldots + 2^{a_r} - r$, where $a_i \in \{1, \ldots, h - 1\}$ and $r \leq h$.*

These two lemmas imply the following result.

Theorem 3.18. *If $q = 2^h$, then $t_q(3) \leq \log_2 q - 1$.*

In planes of odd order maximal arcs do not exist [5, 7] and we use a result by R. HILL and J. MASON [33] to give a weaker estimate.

Theorem 3.19. *If q is an even power of an odd prime, then $t_q(3) \leq \sqrt{q} - 1$.*

In section 3.4 we find new exact values of $n_q(k, d)$ for $q = 4$, $k = 5$. For codes over $\mathbb{F}_4$, $k = 5$ is the smallest dimension, for which there still exist minimum distances d, such that $n_4(5, d)$ is unknown. In subsections 3.4.1 and 3.4.2 we give a characterization of the arcs with parameters $(100, 26)$, $(117, 30)$, and $(118, 30)$ in $\mathrm{PG}(3, 4)$. This characterization is used further in the nonexistence proofs for arcs in higher dimensions, but it is also of independent interest.

The characterization of the arcs with parameters $(118, 30)$ is made in Lemmas 3.20–3.25. A $(118, 30)$-arc in $\mathrm{PG}(3, 4)$ is of one of the following types:

(α) $\mathcal{K} = 2 - \mathcal{F}$, where $\mathcal{F}$ is a $(52, 12)$-blocking set; $\mathcal{F}$ is the sum of two planes and two lines, chosen is such way that the maximal point multiplicity is 2. Two spectra are possible:

$$a_{14} = 2, a_{22} = 0, a_{26} = 10, a_{30} = 73, \quad \lambda_0 = 9, \lambda_1 = 34, \lambda_2 = 42;$$
$$a_{14} = 2, a_{22} = 1, a_{26} = 8, a_{30} = 74, \quad \lambda_0 = 10, \lambda_1 = 32, \lambda_2 = 43$$

(β) $\mathcal{K} = 2 - \chi_{\pi_0 \cup \pi_1} + \chi_L - \mathcal{F}$, where π_i are the planes through a fixed line L, $\mathcal{F}$ is a $(15, 3)$-blocking set, contained in $\pi_2 \cup \pi_3 \cup \pi_4$. There exist two such arcs. They are obtained if the blocking set $\mathcal{F}$ is taken to be either

(a) the sum of three mutually skew lines, or else

(b) the subgeometry $\mathrm{PG}(3, 2)$.

In both cases we obtain the same spectrum:

$$a_{18} = 2, a_{22} = 0, a_{26} = 12, a_{30} = 71, \lambda_0 = 3, \lambda_1 = 46, \lambda_2 = 36.$$

(γ) $\mathcal{K}$ is the dual to a multiset of cardinality 18 with maximal point cardinality 2 and intersection numbers 2, 6, and 10. There exist three such multisets which give the following possible spectra for $\mathcal{K}$:

$$(\gamma') \quad a_{22} = 5, a_{26} = 8, a_{30} = 73, \quad \lambda_0 = 2, \lambda_1 = 48, \lambda_2 = 35;$$
$$(\gamma'') \quad a_{22} = 9, a_{26} = 0, a_{30} = 76, \quad \lambda_0 = 6, \lambda_1 = 40, \lambda_2 = 39.$$
$$(\gamma''') \quad a_{22} = 9, a_{26} = 0, a_{30} = 76, \quad \lambda_0 = 6, \lambda_1 = 40, \lambda_2 = 39.$$

(γ') The two 0-points are incident with a 6-line; the planes through this 6-line have multiplicities 22, 30, 30, 30, 30.

(γ'') There exists a 30-plane containing all six 0-points; five of them are collinear; the planes through the obtained 0-line have multiplicities 30, 22, 22, 22, 22; the 2-points outside this 30-plane form a cone with vertex the sixth 0-point and a hyperoval as a ruling curve.

(γ''') There exists a 22-plane with seven 2-points; through each one of the four 2-lines there exist two 22- and two 30-planes; each one of these 22-planes contains four 2-points (the characterization of the $(q^2 + q + 2, q + 2)$-arcs is described in [9]).

The characterization of the $(118, 30)$-arcs in $\mathrm{PG}(3, 4)$ implies also the characterization of the $(117, 30)$-arcs by the following result.

Lemma 3.26. *Every* $(117, 30)$*-arc in* $\mathrm{PG}(3, 4)$ *is extendable.*

The arcs with parameters $(100, 26)$ can be obtained from the $(102, 26)$-arc via deletion of two points (not necessarily different). The latter is a sum of a 17-cap

in PG$(3,4)$ and the whole space. Of particular interest is the construction of the nonextendable $(100,26)$-arc in PG$(3,4)$, which turns out to be unique.

Theorem 3.34. *Let $\mathcal{K}$ be a $(100,26)$-arc in* PG$(3,4)$*. Then $\mathcal{K}$ is of one of the following two types:*

(1) *a sum of a maximal cap and the whole space minus two points;*
(2) *a cone without the vertex, with a ruling curve a hyperoval plus the whole space minus the symmetric difference of the hyperoval and a line from the cone.*

Until the end of the section we give nonexistence proofs for several hypothetical arcs in PG$(4,4)$ associated with GRIESMER codes, whose existence was not yet decided. Below, we list the nonexistence theorems for these arcs. The corresponding results for the associated codes and the exact values of $n_4(5,d)$ are given as corollaries.

Theorem 3.35. *There exist no $(467,118)$-arcs in* PG$(4,4)$*.*

Corollary 3.36. *There exist no linear codes with parameters $[467,5,349]_4$. This determines the exact values $n_4(5,349+i)=468+i$ for $i=0,1,2,3$.*

Theorem 3.37. *There exist no $(465,117)$-arcs in* PG$(4,4)$*.*

Theorem 3.38. *There exist no $(464,117)$-arcs in* PG$(4,4)$*.*

Corollary 3.39. *There exist no linear codes with parameters $[464,5,347]_4$. This determines the exact values $n_4(5,347+i)=465+i$ for $i=0,1$.*

Theorem 3.40. *There exist no $(398,101)$-arcs in* PG$(4,4)$*.*

Corollary 3.41. *There exist no linear codes with parameters $[398,5,297]_4$ and $[399,5,298]_4$. Consequently, $n_4(5,297)=399$ and $n_4(5,298)=400$.*

Theorem 3.42. *There exist no $(396,100)$-arcs in* PG$(4,4)$*.*

Theorem 3.43. *There exist no $(395,100)$-arcs in* PG$(4,4)$*.*

Corollary 3.44. *There exist no linear codes with parameters $[395,5,295]_4$ and $[396,5,296]_4$. Consequently, $n_4(5,295)=396$ and $n_4(5,296)=397$.*

These results imply the exact value of $n_4(5,d)$ for ten minimal distances $d=295,296,297,298,347,\ldots,352$. At the end of chapter 3 we present a table with all minimum distances d for which the exact value of $n_4(5,d)$ remains still undecided.

Chapter 4. Extendability of arcs and codes. In chapter 4 we investigate the extendability problem for arcs in projective geometries and, equivalently for the linear codes associated with them. It is well-known that every binary $[n, k, d]$-code with odd minimal distance is extendable to an $[n+1, k, d+1]$-code. This observation was generalized by R. HILL and P. LIZAK in [31, 32]. They proved that every q-ary $[n, k, d]_q$-code with $(d, q) = 1$, in which every word has weight congruent to 0 or d modulo q is extendable to a $[n+1, k, d+1]_q$-code. A typical case shows up for GRIESMER codes with $d \equiv -1 \pmod{q}$. This train of research was followed by T. MARUTA who proved new results for the extendability of linear codes [40, 42, 43, 44]. The most interesting of them is from [43], where he proves that for odd $q \geq 5$ every $[n, k, d]_q$-code with $d \equiv -2 \pmod{q}$, having weights $\equiv -2, -1, 0 \pmod{q}$, is extendable.

The investigations on the extendability of arcs were initiated before the corresponding problem for codes. Maybe the first result of this type is a theorem by A. BARLOTTI [10], who proved that every $((w-1)(q+1), w)$-arc in $\mathrm{PG}(2, q)$ is extendable to a maximal $((w-1)(q+1)+1, w)$-arc. The extendability results are a special case of a broad class of theorems known as stability results.

In this chapter we present a new geometric approach to the extendability problem for codes and arcs. In other words we aim at formulating conditions under which an (n, w)-arc in $\mathrm{PG}(r, q)$ 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 $\mathcal{K}$ with the structure of a special arc $\widetilde{\mathcal{K}}$ in the dual geometry. The extendability of the so-called arcs with t-quasidivisibility is of special interest. Such arcs are rather common when we consider GRIESMER codes with $d \equiv -t \pmod{q}$, $t < q$.

In section 4.1 we introduce a special class of arcs called $(t \mod q)$-arcs. These are obtained by a special dualization of arcs with the property t-quasidivisibility. The t-quasidivisible arcs, in turn, are associated with GRIESMER codes with minimal distance $d \equiv -t \pmod{q}$. Let $\mathcal{K}$ is a (n, w)-arc in $\Sigma = \mathrm{PG}(r, q)$ with spectrum $(a_i)_{i \geq 0}$ and $w \equiv n+t \pmod{\Delta}$, $1 \leq t < \Delta$. The arc $\mathcal{K}$ is said to be t-quasidivisible with divisor Δ, if $a_i = 0$, for every $i \not\equiv n, n+1, \ldots, n+t \pmod{\Delta}$. For $\mathcal{K}$ we define an arc $\widetilde{\mathcal{K}}$ in the dual geometry $\widetilde{\Sigma}$, with pointset $\widetilde{\mathcal{H}} = \{\widetilde{H} | H - \text{ a hyperplane in } \Sigma\}$, by

$$\widetilde{\mathcal{K}} : \begin{cases} \widetilde{\mathcal{H}} & \to & \{0, 1, \ldots, t\} \\ \widetilde{H} & \to & \widetilde{\mathcal{K}}(H) \equiv n + t - \mathcal{K}(H) \pmod{q} \end{cases}, \tag{6}$$

Theorem 4.1. *Let $\mathcal{K}$ be an (n, w)-arc in $\Sigma = \mathrm{PG}(r, q)$, which is t-quasidivisible modulo q with $t < q$. Then for each subspace $\widetilde{S}$ in $\widetilde{\Sigma}$ of dimension $\dim \widetilde{S} \geq 1$ it holds*

$$\widetilde{\mathcal{K}}(\widetilde{S}) \equiv t \pmod{q}.$$

This observation justifies the following definition. Let t be a non-negative integer. An arc $\mathcal{K}$ in Σ is called a $(t \mod q)$-arc if the multiplicity of each subspace S of projective dimension at least 1 satisfies $\mathcal{K}(S) \equiv t \pmod{q}$. The following theorem is the main result of this section.

Theorem 4.3. *Let $\mathcal{K}$ be an (n, w)-arc in $\Sigma = \mathrm{PG}(r, q)$, which is t-quasidivisible modulo q with $t < q$. Let $\widetilde{\mathcal{K}}$ be the dual of $\mathcal{K}$, defined by (6). If $\widetilde{\mathcal{K}}$ is represented in the form*

$$\widetilde{\mathcal{K}} = \sum_{i=1}^{c} \chi_{\widetilde{P}_i} + \mathcal{K}'$$

where $\mathcal{K}'$ is an arc in $\widetilde{\Sigma}$, and $\widetilde{P}_1, \ldots, \widetilde{P}_c$ are c not necessarily different hyperplanes in $\widetilde{\Sigma}$, then $\mathcal{K}$ is c-extendable. In particular, if $\widetilde{\mathcal{K}}$ contains a hyperplane in its support then $\mathcal{K}$ is extendable.

According to this theorem, a sufficient condition for c-fold extendability of an arc $\mathcal{K}$ which is t-quasidivisible is that the dual arc $\widetilde{\mathcal{K}}$ is a sum of c hyperplanes and some other arc. In particular, a t-quasidivisible arc $\mathcal{K}$ is 1-extendable (or simply extendable) if its support $\mathrm{Supp}\,\mathcal{K} = \{X \mid \mathcal{K}(X) > 0\}$ contains a hyperplane. This explains the importance of the problem of determining the structure of the $(t \mod q)$-arcs.

In section 4.2 we investigate the structure of $(t \mod q)$-arcs unrelated to the extendability problem. We present a non-trivial construction which starting from a $(t \mod q)$-arc in $\mathrm{PG}(r-1, q)$ produces a $(t \mod q)$-arc in $\mathrm{PG}(r, q)$.

Theorem 4.6. *Let $\mathcal{F}_0$ be a $(t \mod q)$-arc in the hyperplane $H \cong \mathrm{PG}(r-1, q)$ of $\Sigma = PG(r, q)$. Let the point $P \in \Sigma \setminus H$ be fixed. The arc $\mathcal{F}$ in Σ, defined in the following way:*

– $\mathcal{F}(P) = t$;

– for every point $Q \neq P$: $\mathcal{F}(Q) = \mathcal{F}_0(R)$, where $R = \langle P, Q \rangle \cap H$.

is a $(t \mod q)$-arc of cardinality $q|\mathcal{F}_0| + t$.

A central problem here is to determine the structure of the $(0 \mod q)$-arcs, i.e. those arcs in which every arc has multiplicity $\equiv 0 \pmod q$. From this point on our investigation is restricted to the geometries $\mathrm{PG}(r,p)$ of prime order p. In this case, the point multiplicities can be considered as elements of $\mathbb{F}_p$ and the set of all $(0 \mod p)$-arcs is a vector space over $\mathbb{F}_p$ under the usual addition and scalar multiplication of arcs. The main result in this section is Theorem 4.12.

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

This result is obtained by using the classical formula of N. Hamada [27] on the p-rank of the incidence matrix of $\mathrm{PG}(r,q)$, in which the rows are indexed by the points and the columns – by the lines in this geometry. A closed form for the rank of these matrices is found by J. van Lint. His proof is contained in a paper by P. V. Ceccherini and J. Hirschfeld [16]. It follows from Theorem 4.12 that every $(0 \mod p)$-arc, and, consequently, every $(t \mod p)$-arc for $t < p$ is a sum of lifted arcs (Corollaries 4.13 and 4.14). Theorem 4.12 does not answer the question about how large the number of summands can be large. In Theorem 4.15 we prove that this number is at most p.

Theorem 4.15. *Let* $P_1, \ldots, P_{p+1}$ *be the points of a conic in* $\mathrm{PG}(2,p)$*. Denote by* V_i *the vector space of all* $(0 \mod p)$*-arcs, that are lifted from the point* P_i*,* $i = 1, \ldots, p+1$*, and by* V *– the vector space of all* $(0 \mod p)$*-arcs. Then*

$$V = V_1 + V_2 + \cdots + V_p.$$

It is plausible that a similar assertion holds true for geometries of any dimension. The proof of such a result depends on a condition which guarantees the validity of the inclusion/exclusion formula for the dimensions of the subspaces, which is not true in general.

In Section 4.3 we investigate $(t \mod q)$-arcs, in which the maximal point multiplicity is t. The section opens with a theorem in which we prove that if a $(t \mod q)$ arc has the additional property that its restriction to every hyperplane is lifted then the original $(t \mod q)$-arc is lifted itself.

Theorem 4.18. *Let $\mathcal{K}$ be a $(t \mod q)$-arc in $\mathrm{PG}(r,q)$ and let the restriction to every hyperplane H, $\mathcal{K}|_H$, is lifted from a point. Then the arc $\mathcal{K}$ is also lifted from a point.*

In the plane case, $(t \mod q)$-arcs with restricted point multiplicity are obtained as σ-dual of blocking sets, for which the line multiplicities are contained in an interval of length t.

Theorem 4.19. *A necessary and sufficient condition for the existence of a $(t \mod q)$-arc in $\mathrm{PG}(2,q)$ of cardinality $mq+t$ and maximal point multiplicity t is the existence of a blocking set in the same plane with parameters $((m-t)q+m, m-t)$ and line multiplicities contained in the set $\{m-t, m-t+1, \ldots, m\}$.*

At the end of this section we characterize the $(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$ with a small number of points: 18, 23, 28 and 33. From this characterization we deduce the following partial result on the structure of $(3 \mod 5)$-arcs in $\mathrm{PG}(3,5)$.

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

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

In the next section 4.4, we investigate the extendability of Griesmer arcs having the property t-quasidivisibility modulo q. In the cases, when the minimum distance d of the code associated with such arc satisfies $d \equiv -t \pmod q$, these arcs are t quasidivisible with $t \equiv -d \pmod q$. So, we can apply for them the results from the previous three sections. Let $\mathcal{K}$ be a Griesmer (n,w)-arc in $\mathrm{PG}(k-1,q)$, which is t-quasidivisible for some $t < q$. Let $C_{\mathcal{K}}$ be a linear code, associated with $\mathcal{K}$. Then $C_{\mathcal{K}}$ has parameters $[n,k,d]_q$, where $d = n - w$. Let us write d as:

$$d = sq^{k-1} - \sum_{i=0}^{k-2} \varepsilon_i q^i, \tag{7}$$

where $0 \leq \varepsilon_i < q$ for all $i = 0, \ldots, k-2$.

In the next lemmas we establish important properties of the arc $\widetilde{\mathcal{K}}$, defined in (6). The first of them gives a relation between the multiplicity of the hyperlines

(subspaces of codimension 2), contained in a given hyperplane and their respective multiplicity with respect to the dual arc $\widetilde{\mathcal{K}}$.

Lemma 4.22. *Let $\mathcal{K}$ be a Griesmer arc in $\Sigma = \mathrm{PG}(k-1,q)$ with parameters $(n, n-d)$, which is t-quasidivisible. Let d be represented in the form (7) and let S be a subspace of codimension 2, contained in a hyperplane H_0 of multiplicity $\mathcal{K}(H_0) = w_{k-2} - aq$ for some integer $a \geq 0$.*

(i) *If $\mathcal{K}(S) = w_{k-3} - a - b$, $0 \leq b \leq t-2$, then $\widetilde{\mathcal{K}}(\widetilde{S}) \leq t + bq$;*

(ii) *If $\mathcal{K}(S) = w_{k-3} - a - b$, $b \geq t-1$, then $\widetilde{\mathcal{K}}(\widetilde{S}) \leq t + (t-1)q$.*

The next few lemmas provide an estimate on the multiplicity of the hyperplanes in the dual space, corresponding to maximal (with respect to $\mathcal{K}$) subspaces in Σ of different codimensions.

Lemma 4.23. *Let $\mathcal{K}$ be a Griesmer $(n, n-d)$-arc in $\mathrm{PG}(k-1,q)$, having the property t-quasidivisibility. Let d be represented in the form (7) and let $\widetilde{\mathcal{K}}$ be the dual $\mathcal{K}$, obtained by (6). Let T be a subspace of $\mathrm{PG}(k-1,q)$ of codimension 3 of the maximal multiplicity $\mathcal{K}(T) = w_{k-4}$. Then*

$$\widetilde{\mathcal{K}}(\widetilde{T}) \leq t(q+1) + \varepsilon_1 q.$$

Lemma 4.24. *Let $\mathcal{K}$ be a Griesmer $(n, n-d)$-arc in $\mathrm{PG}(k-1,q)$, $q \geq 3$, having the property t-quasidivisibility, where d is represented in the form (7). Let $\widetilde{\mathcal{K}}$ be the dual of $\mathcal{K}$, given by (6). Finally, let $\varepsilon_0, \varepsilon_1 < \sqrt{q}$. Then for every subspace T in $\mathrm{PG}(k-1,q)$ of codimension 3 with $\mathcal{K}(T) = w_{k-4}$, it holds*

$$\widetilde{\mathcal{K}}(\widetilde{T}) = t(q+1).$$

Lemma 4.25. *Let $\mathcal{K}$ be a Griesmer (n,w)-arc in $\mathrm{PG}(k-1,q)$, $q \geq 3$, having the property t-quasidivisibility for which $d = n-w$ is presented in the form (7). Let $\widetilde{\mathcal{K}}$ be dual to $\mathcal{K}$, as defined in (6). Let U be a subspace in $\mathrm{PG}(k-1,q)$ of codimension $\operatorname{codim} U = r$, $1 \leq r \leq k$, having the maximal multiplicity w_{k-1-r} (if $U = \varnothing$, we set $\operatorname{codim} U = k$). Under these conditions, if $\varepsilon_0 = t, \varepsilon_1, \ldots, \varepsilon_{r-2} < \sqrt{q}$, then*

$$\widetilde{\mathcal{K}}(\widetilde{U}) = \varepsilon_0 v_{r-1}.$$

The main result in section 4.4 is the following theorem, which is obtained and formulated as a result about arcs.

Theorem 4.26. *Let $\mathcal{K}$ be a Griesmer $(n, n-d)$-arc in $\mathrm{PG}(k-1,q)$, 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 $\mathcal{K}$ is t-extendable.

This result can be reformulated for linear codes.

Theorem 4.27. *Let C be a* Griesmer *code with parameters $[n,k,d]_q$, that is t-quasidivisible. Let d be represented by*

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

where $0 \leq \varepsilon_i < q$ for all $i = 0, \ldots, k-2$. If the numbers ε_i satisfy the 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 general, the parameters of a t-quasidivisible arc $\mathcal{K}$ do not determine the parameters of the dual arc $\widetilde{\mathcal{K}}$. In some cases, we know the possible spectra of the restriction of $\mathcal{K}$ to the maximal hyperplanes. Then it is possible to obtain a restriction on the cardinality of $\widetilde{\mathcal{K}}$, and hence gain knowledge about its possible structure. In many cases, this allows to prove the extendability of $\mathcal{K}$. One such result is presented in Theorem 4.28, which gives a sufficient condition for extendability, which depends on the spectrum of $\mathcal{K}|_H$, where H is a maximal hyperplane.

Theorem 4.28. *Let $\mathcal{K}$ be a Griesmer arc in* $\mathrm{PG}(k-1,q)$ *with parameters* (n,w), $w = n-d$, *which is* t*-quasidivisible modulo* q. *For a fixed hyperplane* H_0 *of multiplicity* w *let* $(a_i)_{i\geq 0}$ *be the spectrum of the arc* $\mathcal{K}|_{H_0}$. *Denote by* A *the largest integer for which every blocking set with parameters* $(tv_{k-1}+A, tv_{k-2})$ *contains a hyperplane in its support. If*

$$(8)\quad qa_{w-\lceil d/q\rceil-1} + 2qa_{w-\lceil d/q\rceil-2} + \ldots + (t-2)qa_{w-\lceil d/q\rceil-t+2} + (t-1)q \sum_{u\leq w-\lceil d/q\rceil-t+1} a_u \leq A,$$

then $\mathcal{K}$ *is extendable.*

At the end of section 4.4 we give two examples which use the obtained extendability results. In the first example, we investigate a class of hypothetical arcs in $\mathrm{PG}(3,q)$ with parameters (q^3-3q-6, q^2-3). It turns out that all they are extendable to the nonexistent (q^3-3q-3, q^2-3)-arcs. For $q \geq 11$ this result follows from Theorem 4.29. For $q = 5,7,8,9$ the hypothetical arcs with parameters (q^3-3q-6, q^2-3) are again extendable, but the proof requires additional geometric arguments. In the second example we prove the t-extendability of (q^2+1-t)-caps in $\mathrm{PG}(3,q)$ for every $t < \sqrt{q}$.

In section 4.5 we use the methods developed in section 4.4 to prove the nonexistence of arcs with parameters $(104,22)$ in $\mathrm{PG}(3,5)$.

Theorem 4.36. *There exists no* $(104,22)$*-arc in* $\mathrm{PG}(3,5)$.

This solves one of the four open cases for codes with $k=4, q=5$ [45]. The idea is that if there exists such an arc $\mathcal{K}$, then it is 3-quasidivisible and non-extendable. So, the dual arc $\widetilde{\mathcal{K}}$ does not have a hyperplane in its support. In addition, a sophisticated counting argument shows that there is no 18-hyperplane with respect to $\widetilde{\mathcal{K}}$ which contains just an 18-line, i.e. a line with six 3-points. Using the characterization of the plane $(3 \mod 5)$-arcs and some additional observations for the spectrum of the hypothetical $(104,22)$-arc $\mathcal{K}$ in $\mathrm{PG}(3,5)$, we get a contradiction.

Chapter 5. Affine blocking sets. In Chapter 5 we present new constructions of affine blocking sets. A set of points $\mathcal{B}$ in $\mathrm{AG}(n,q)$ is called an affine t-fold blocking set if every hyperplane in $\mathrm{AG}(n,q)$ contains at least t points from $\mathcal{B}$.

Section 5.1 contains a survey of the known lower bounds on the cardinality of a blocking set in $\mathrm{AG}(n,q)$. The lower bound on the size of an 1-fold blocking set is proved independently by R. Jamison [34] and A. Brouwer and A. Schrijver [14]:

$$|\mathcal{B}| \geq n(q-1)+1.$$

This bound is sharp for all dimensions n and all finite fields $\mathbb{F}_q$. An example of such blocking set is given by n concurrent lines, no three of which lie in a plane. A generalization of this bound was given by A. Bruen [15], who proved that if $\mathcal{B}$ is a t-fold blocking set then its cardinality is lowerbounded by:

$$|\mathcal{B}| \geq (n+t-1)(q-1)+1.$$

This bound is not trivial for $1 \leq t \leq (n-1)(q-1)$ since for values of t outside this interval it becomes weaker than the trivial bound

$$|\mathcal{B}| \geq tq.$$

For large values of t the Bruen bound cannot be achieved. C. Zanella [57] proved that for values of t satisfying

$$t > \frac{(n-1)(q-1)+1}{2}$$

there exist no blocking sets meeting the Bruen bound. The Bruen bound can be improved for some special values of t and n. S. Ball [1] proved that for $t < q$ a t-fold blocking set $\mathcal{B}$ in $\mathrm{AG}(n,q)$, $q = p^h$, has cardinality at least $(n+t-1)(q-1)+k$ provided there exists an integer j, for which

$$\binom{k-n-t}{j} \not\equiv \pmod{p}.$$

In particular, if $\binom{-n}{t-1} \not\equiv 0 \pmod{p}$, then

$$|\mathcal{B}| \geq (n+t-1)q - n + 1.$$

In the same paper [1] S. BALL constructs blocking sets in $\mathrm{AG}(n,q)$ with parameters $((n+t-1)q-n+\varepsilon, 2)$ where

$$\varepsilon = \begin{cases} 1 & \text{for } n \not\equiv 0 \pmod{p}, \\ 0 & \text{for } n \equiv 0 \pmod{p}. \end{cases}$$

In the case of $\varepsilon = 0$ the constructed blocking sets meet the BRUEN bound. Independently, C. ZANELLA [57] and S. BALL [1] note that if one removes a plane from a hyperbolic quadric in $\mathrm{PG}(3,q)$ intersecting the quadric in two lines the resulting pointset is a $(q^2, q-1)$-blocking set in $\mathrm{AG}(3,q)$, which meets the BRUEN bound. Thus around 2010, the known values for which there exist blocking sets meeting the BRUEN bound were the following:

(1) $t = 1$ for all n and q;
(2) $t = 2$ for all $n \equiv 0 \pmod{p}$ and every $q = p^h$;
(3) $t = q-1$, $n = 3$ for every $q = p^h$.

Section 5.2 contains the main result of this chapter. This is Theorem 5.6, in which we present a new general construction for affine blocking sets.

Theorem 5.6. *Let $n \geq 3$ be an integer and let $q = p^h$ be a power of a prime. If there exist*

- *an arc with parameters (M, w) in $\mathrm{PG}(r,q)$, where $2 \leq r \leq n-2$, and*
- *a blocking set with parameters (M', u) in the affine geometry $\mathrm{AG}(n-r-1, q)$,*

then there exists an (N,t)-blocking set in $\mathrm{AG}(n,q)$ with parameters

$$N = qM, \quad t = \min\{M - w, aqu\}.$$

where $a = \lfloor M/M' \rfloor$.

Several corollaries following the theorem describe important special cases of Theorem 5.6.

Corollary 5.7. *Let $n \geq 3$ be an integer and let $q = p^h$ be a prime power. If there exist*

- *an (M,w)-arc in $\mathrm{PG}(r,q)$, $1 \leq r \leq n-2$, and*
- *an (M,u)-blocking set in $\mathrm{AG}(n-r-1,q)$,*

then there exists an (N,t)-blocking set in $\mathrm{AG}(n,q)$ with parameters $N = qM$ and $t = \min\{M-w, qu\}$.

Corollary 5.8. *Let $n \geq 4$ be an integer and let $q = p^h$ be a prime power. If there exists an arc with parameters (M, w) in $\mathrm{PG}(n-2, q)$, then there exists an (N, t)-blocking set in $\mathrm{AG}(n, q)$ with parameters*

$$N = qM,\ t = \min\{M - w, q\lfloor M/q \rfloor\}.$$

Corollary 5.9. *Let $n \geq 3$ be an integer and let $q = p^h$ be a prime power. If there exists an (M, w)-arc in $\mathrm{PG}(n-1, q)$, then there exists a $(qM, M - w)$-blocking set in $\mathrm{AG}(n, q)$.*

Corollary 5.10. *Let $n \geq 3$ be an integer and let $q = p^h$ be a prime power. If there exist*

- *an (M, w)-arc in $\mathrm{PG}(r, q)$, where $1 \leq r \leq n-2$, and*
- *an (M', u)-blocking set in $\mathrm{AG}(n-r-1, q)$,*

then for every $i \geq 1$ and all $\alpha \in \{1, \ldots, q-1\}$ there exists an (N, t)-blocking set in $\mathrm{AG}(n, q)$ with parameters

$$N = qM - i\alpha,\ \ t = \min\{M - w - i, aqu - b\alpha\},$$

where $a = \lfloor M/M' \rfloor$ and $b = \lfloor i/M' \rfloor$.

In section 5.3 we present several applications of the general construction from Theorem 5.6. and Corollaries 5.7–5.10, that give blocking sets with good parameters (small cardinality). So, for instance, we obtain Theorem 5.12 as a special case of Corollary 5.7. In this theorem we obtain a new class of blocking sets meeting the Bruen bound.

Theorem 5.12. *For every n with $3 \leq n \leq q-1$, there exists a $(q^2, q-n+2)$-blocking set in $\mathrm{AG}(n, q)$.*

This class contains as a special case the hyperbolic quadrics from (3) obtained for $n = 3$. This class is used further for the construction of new examples of optimal blocking sets that have the minimal cardinality for fixed t, n and q.

Theorem 5.13. *For every $s = 0, 1, \ldots, q+1-n$, $3 \leq n \leq q-1$, there exist blocking sets with parameters $(q^2 - s(n-2+s), q-(n-2+s))$ in $\mathrm{AG}(n, q)$.*

Theorem 5.14. *For every $n \geq 2$ and every prime power $q = p^h$ there exists an affine blocking set in $\mathrm{AG}(n,q)$ with parameters $(q^2 - n + 1, q - n + 1)$. These blocking sets are optimal.*

Corollary 5.15. *For every prime power $q = p^h$ there exist blocking sets in $\mathrm{AG}(n,q)$, $3 \leq n \leq q-1$, with parameters $(q^2 - 2n, q - n)$.*

Theorem 5.16. *There exist $(q^2 + 2q - 1, q - n + 3)$-blocking sets in $\mathrm{AG}(n,q)$ for every $3 \leq n \leq q - 1$.*

Furthermore, by using Theorem 5.6, we construct blocking sets with the following parameters:

$$\begin{array}{rlrlrl} (28,4) & \text{in} & \mathrm{AG}(5,4); & (40,4) & \text{in} & \mathrm{AG}(9,4); \\ (52,4) & \text{in} & \mathrm{AG}(13,4); & (64,4) & \text{in} & \mathrm{AG}(17,4); \\ (120,8) & \text{in} & \mathrm{AG}(9,8). & & & \end{array}$$

These blocking sets are optimal and meet the new bounds found by Ball in [3] and by Ball and Blokhuis from [6]. These are the first examples meeting these two bounds. Up to this moment, these are the only examples for blocking sets meeting the Ball or the Ball–Blokhuis bound.

In section 5.4 we present two tables. The first one is a table of blocking sets in $\mathrm{AG}(n,4)$, obtained by the construction of Theorem 5.6, compared with the lower bounds from [3, 6]. The second table contains lower and upper bounds for the cardinality of 3-fold and 4-fold blocking sets in small affine geometries $\mathrm{AG}(n,q)$, for $n = 3, 4, 5$, $q = 5, 7, 8, 9, 11, 13$.

Main results of the thesis

The main results in these thesis are the following:

(1) 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 $t_q(k) \lesssim q^{k/2}$. In case of $k = 4$, the inequality $t_q(4) \leq q - 1$ is proved.

(2) The inequality $t_q(3) \leq \log_2 q - 1$ 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 $t_q(3) \leq \sqrt{q} - 1$ is proved.

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

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

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

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

(5) 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.

(6) A partial characterization of the ($3 \mod 5$)-arcs in $\mathrm{PG}(2, 5)$ and $\mathrm{PG}(3, 5)$ is made.

(7) A proof of the nonexistence of $(104, 22)$-arcs in $\mathrm{PG}(3, 5)$ 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.

(8) 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.

(9) Five examples of blocking sets meeting the bounds by BALL and BALL–BLOKHUIS are constructed:

$(28, 4)$ in $\mathrm{AG}(5, 4)$, $(40, 4)$ in $\mathrm{AG}(9, 4)$, $(52, 4)$ in $\mathrm{AG}(13, 4)$,
$(64, 4)$ in $\mathrm{AG}(17, 4)$, $(120, 8)$ in $\mathrm{AG}(9, 8)$.

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

Publications related to the DSc thesis

(1) I. Landjev, A Rousseva, An extension theorem for arcs and linear codes, *Probl. Inf. Transmission* **42**(2006), 65–76.

(2) I. Landjev, A. Rousseva, Characterization of some optimal arcs, *Adv. Math. Comm.* **5**(2)(2011), 317–331.

(3) I. Landjev, A. Rousseva, On the extendability of Griesmer arcs, *Ann. de l'Univ. de Sofia* **101**(2013/14), 183–191.

(4) I. Landjev, A. Rousseva, The Nonexistence of (104,22;3,5)-Arcs, *Advances in Mathematics of Communications* **10**(3)(2016), 601–611.

(5) I. Landjev, A. Rousseva, Linear codes close to the Griesmer bound and the related geometric structures, *Designs, Codes and Cryptography* **87**(4)(2019), 841-854.

(6) A. Rousseva, A General construction for blocking sets in finite affine geometries, *Compt. Rend. Acad. Bulg. des Sciences* **71**(4)(2018), 460-466.

(7) A. Rousseva, On the structure of some arcs related to caps and the nonexistence of some optimal codes, *Ann. de l'Univ de Sofia*, 2019, to appear.

References

[1] S. Ball, On intersection sets in Desarguesian affine spaces, *European J. Comb.* **21**(2000), 441-446.

[2] S. Ball, On sets of vectors of a finite vector space in which every subset of basis size is a basis, *J. Eur. Math. Soc.* **14** (2012) 733–748.

[3] S. Ball, A p-adic condition on the weight of a codeword of a linear code, *Des. Codes Cryptogr.* **72** (2014) 177–183.

[4] S. Ball, Table of bounds on three dimensional linear codes or (n, r)-arcs in PG$(2, q)$, `https://mat-web.upc.edu/people/simeon.michael.ball/codebounds.html`

[5] S. Ball, A. Blokhuis, An easier proof of the maximal arcs conjecture, *Proc. Amer. Math. Soc.* **126** (1998) 3377–3380.

[6] S. Ball, A. Blokhuis, A bound for the maximum weight of a linear code, *SIAM J. Discrete Math.* **27** (2013) 575–583.

[7] S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica*, **17** (1997) 31–41.

[8] S. Ball, J. De Beule, On sets of vectors of a finite vector space in which every subset of basis size is a basis II, *Des. Codes Cryptogr.* **65** (2012) 5–14.

[9] S. Ball, R. Hill, I.Landjev, H. N. Ward, On $(q^2+q+2, q+2)$-arcs in the projective plane $PG(2, q)$, *Designs, Codes and Cryptography*, **24**, 2001, 205–224.

[10] A. Barlotti, Su $\{k; n\}$-archi di un piano lineare finito, *Boll. Un. Mat. Ital.* **1**(1956), 553–556.

[11] B. I. Belov, V. N. Logachev, V. P. Sandimirov, Construction of a class of linear binary codes achieving the Varshamov-Griesmer bound, *Probl. Inf. Transm.* **10**(3)(1974), 211–217.

[12] E. R. Berlekamp, R. C. McEliece, H. C. van Tilborg, On the inherent intractability of certain coding theoretic problems, *IEEE Trans. Inf. Theory* **IT-24**(1978), 384-386.

[13] A. Beutelspacher, Blocking sets and partial spreads in finite projective spaces, *Geom. Dedicata* 9(1980), 130–157.

[14] A. E. Brouwer, A. Schrijver, The blocking number of an affine space, *J. Combin. Th. Ser. A* **24**(1978), 251–253.

[15] A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *J. Comb. Th. Ser. A* **60**(1992), 19–33.

[16] P. V. Cechherini, J. W. P Hirschfeld, The dimension of projective geometry code, *Discrete Math.* **106/107**(1992), 117–126.

[17] R.H.F.Denniston, Some maximal arcs in finite projective planes, *J. Comb. Theory* Ser. A, **6**(1969), 317–319.

[18] S. Dodunekov, Optimal Codes, DSc Thesis, Institute of Mathematics, Sofia, 1985.

[19] S.Dodunekov, I.Landjev, On Near-MDS Codes, *Journal of Geometry*, **54**(1995), 30–43.

[20] G. Fano, Sui postulati fondamentali della geometria proiettiva, *Giornale di Matematiche* **30**(1892), 106–132.

[21] E.N. Gilbert, A comparisonof sigmaling alphabets, *Bell System Tech. J.* **31**(1952), 504–522.

[22] V. D. Goppa, A new class of linear error-correcting codes, *Probl. Peredach. Inform.* **6**(3)(1970), 24–30.
[23] V. D. Goppa, Rational representation of codes and (L, g) codes, *Probl. Peredach. Inform.* **7**(3)(1971), 41–49.
[24] V. D. Goppa, Some codes constructed on the basis of (L, g) codes, *Probl. Peredach. Inform.* **8**(2)(1972), 107–109.
[25] M. Grassl, Code Tables: Bounds on the parameters of various types of codes. `http://codetables.markus-grassl.de`
[26] J.H. Griesmer, A bound for error-correcting codes, *IBM J. Res. Develop.* 4, 1960, 532–542.
[27] N. Hamada, The Rank of the Incidence Matrix of Points and d-Flats in Finite Geometries, *J. Sci. Hiroshima Univ.* Ser. A-I 32(1968), 381–396.
[28] R. Hill, On the largest size of cap in $S_{5,3}$, *Atti Accad. Naz. Linzei Rend.* **54** (1973), 378–384.
[29] R. Hill, Caps and codes, *Discrete Math.* **22** (1978), 111–137.
[30] R. Hill, Optimal Linear Codes, Cryptography and Coding II (C. Mitchell ed.), Oxford Univ. Press (1992), 75–104.
[31] R. Hill, P. Lizak, Extensions of linear codes, in: *Proc. Int. Symp. on Inf. Theory*, Whistler, Canada, 1995, 345.
[32] R. Hill, An extension theorem for linear codes, *Des. Codes and Cryptogr.* **17**(1999), 151–157.
[33] R. Hill, J. R. M. Mason, On (k, n)-arcs and the falsity of the Lunelli-Sce conjecture, "Finite Geometries and Designs", London Math. Soc. Lecture Note Series 49, Cambridge Univ. Press, cambridge, 1981, 153–168.
[34] R. Jamison, Covering finite fields with cosets of subspaces, *J. Comb. Th. Ser. A* **22**(1977), 253–256.
[35] I. Landjev, A Rousseva, An extension theorem for arcs and linear codes, *Probl. Inf. Transmission* **42**(2006), 65–76.
[36] I. Landjev, A. Rousseva, Characterization of some optimal arcs, *Adv. Math. Comm.* **5**(2)(2011), 317–331.
[37] I. Landjev, A. Rousseva, On the extendability of Griesmer arcs, *Ann. de l'Univ. de Sofia* **101**(2013/14), 183–191.
[38] I. Landjev, A. Rousseva, The Nonexistence of (104,22;3,5)-Arcs, *Adv. Math. Comm.* **10**(3)(2016), 601–611.
[39] I. Landjev, A. Rousseva, Linear codes close to the Griesmer bound and the related geometric structures, *Designs, Codes and Cryptography* **87**(4)(2019), 841-854.
[40] T. Maruta, On the extendability of linear codes, *Finite Fields Appl.* **7**(2001), 350–354.
[41] T. Maruta, The nonexistence of some quaternary linear codes of dimension 5, *Discrete Mathematics* 238(2001), 99–113.
[42] T. Maruta, Extendability of linear codes over GF(q) with minimum distance d, $\gcd(d, q) = 1$, *Discrete Math.* **266**(2003), 377–385.
[43] T. Maruta, A new extension theorem for linear codes, *Finite Fields and Appl.* **10**(2004), 674–685.

[44] T. Maruta, Extension theorems for linear codes over finite fields, *J. of Geom.* **101**(2011), 173–183.
[45] T. Maruta, `http://www.mi.s.oskafu-u.ac.jp/ maruta/griesmer.htm`
[46] R. Mathon, New maximal arcs in Desarguesian planes, *j. Combin. theory*, Ser A, **97**(2002), 353–368.
[47] A. Rousseva, A General construction for blocking sets in finite affine geometries, *Compt. Rend. Acad. Bulg. des Sciences* **71**(4)(2018), 460-466.
[48] A. Rousseva, On the structure of some arcs related to caps and the non-existence of some optimal codes, *Ann. de l'Univ de Sofia*, 2020, to appear.
[49] B. Segre, Ovals in a finite projective plane, *Can. J. Math.* **7**(1955), 414–416.
[50] C. Shannon, A mathematical theory of communication, *Bell Systems Technical Journal* **27**(1948), 379–423.
[51] G. Solomon, J. J. Stiffler, Algebraically punctured cyclic codes, *Inf. and Control* **8**(1965), 170–179.
[52] J. Thas Construction of maximal arcs and partial geometries, *Geom. Dedicata* **3**(1974), 61–64.
[53] J.Thas, Constructions of maximal arcs and dual ovals in translation planes, *European J. Comb* **1**(1980), 189–192.
[54] M. A. Tsfasman, S. G. Vladut, Th. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Mth. Nachr.* **109**(1982), 21–28.
[55] R. R. Varshamov, Estimate of the number of signals in error-correcting codes, *Dokl. Akad. Nauk SSSR* **117**(1957), 739–741.
[56] H.N. Ward, Divisibility of codes meeting the Griesmer bound, *Journal of Combinatorial Theory*, Ser. A, **83**(1998), 79–93.
[57] C. Zanella, Intersection sets in $AG(n,q)$ and a characterization of the hyperbolic quadric in $\mathrm{PG}(3,q)$, *Discrete Math.* **255**(2002), 381–386.