ГОДИШНИК НА СОФИЙСКИЯ УНИВЕРСИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“

ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
Том 100

ANNUAIRE DE L'UNIVERSITE DE SOFIA „ST. KLIMENT OHRIDSKI“

FACULTE DE MATHEMATIQUES ET INFORMATIQUE
Tome 100

ON THE DIVISIBILITY OF ARCS WITH MULTIPLE POINTS[1]

IVAN N. LANDJEV, ASSIA P. ROUSSEVA

In this paper, we generalize a result by Ball, Hill, Landjev and Ward on plane arcs to arcs with multiple points in spaces of arbitrary dimension. This result is further applied to the characterization of some non-Griesmer arcs in the 3-dimensional projective geometry over $\mathbb{F}_4$.

Keywords: Divisible arcs, divisible codes, the polynomial method, the Griesmer bound, Griesmer codes, Griesmer arcs

2000 MSC: main 94B05, secondary 05E30, 94B60, 51C05

1. INTRODUCTION

In a series of papers in the mid-nineties H. N. Ward introduced and investigated the so-called divisibility property of linear codes over finite fields. It turns out that many important classes of codes are divisible. A celebrated result by Ward establishes the divisibility of Griesmer codes of minimum weight divisible by some power of the field order [7].

By the equivalence of the linear codes of full length and the arcs in $\mathrm{PG}(r, q)$, divisibility can be translated into geometric language. This makes it possible to use a geometric technique, the so-called polynomial method [1, 2], in the investigation of divisibility properties for arcs and codes. For instance, the condition on the arc in question being a Griesmer arc can be replaced by a milder condition on the number of points of maximal multiplicity. A result of this type has been obtained

[1]This research has been supported by the Scientific Research Fund of Sofia University under Contract No 192/2010.

in [3] for arcs with parameters $(q^2+q+2, q+2)$ in the projective plane $\mathrm{PG}(2,q)$. In what follows, we generalize this result to arcs in projective geometries of arbitrary dimension.

The paper is organized as follows. In Section 2, we give some basic definitions and results on arcs and codes. Section 3 contains the main theorem which establishes the divisibility of non-Griesmer arcs having some additional properties. Section 4 contains a characterization of non-Griesmer arcs in $\mathrm{PG}(3,4)$ with enough maximal points.

2. PRELIMINARIES

Let $\Pi = \mathrm{PG}(r,q)$ be the r-dimensional projective geometry of order q. A multiset of points is a mapping $\mathcal{K} : \mathcal{P} \to \mathbb{N}_0$ from the pointset $\mathcal{P}$ of Π into the nonnegative integers. This mapping is extended trivially to the power set of $\mathcal{P}$ by $\mathcal{K}(\mathcal{Q}) = \sum_{x \in \mathcal{Q}} \mathcal{K}(x)$, $\mathcal{Q} \subseteq \mathcal{P}$. The integer $\mathcal{K}(x)$ is called the multiplicity of the point x. Similarly, we define multiplicities of lines, planes, hyperplanes etc. A multiset $\mathcal{K}$ is called a (n,w)-arc if (1) $\mathcal{K}(\mathcal{P}) = n$, (2) $\mathcal{K}(H) \leq w$ for any hyperplane H, (3) $\mathcal{K}(H_0) = w$ for at least one hyperplane H_0. Denote by a_i the number of hyperplanes in Π of multiplicity exactly i and by Λ_i – the number of points of multiplicity i. The sequence $(a_i)_{i \geq 0}$ is called the spectrum of $\mathcal{K}$.

Let $\mathbb{F}_q^n$ be the vector space of all n-tuples over the finite field $\mathbb{F}_q$. Any k-dimensional subspace C of $\mathbb{F}_q^n$ is called a linear code of length n and dimension k. If, in addition, the minimum Hamming distance between different codewords of C is d the code is referred to as an $[n,k,d]_q$-code. It is well-known that with every linear $[n,k,d]_q$-code of full length, i.e. a code in which no coordinate is identically zero, one can associate an $(n, n-d)$-arc in $\mathrm{PG}(k-1,q)$ so that isomorphic codes lead to equivalent arcs and vice versa. This means that linear codes and arcs are in some sense equivalent objects.

A fundamental bound on the parameters of a linear code is the so-called Griesmer bound [4]. It says that if C is an $[n,k,d]_q$-code then

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil . \tag{2.1}$$

A linear code meeting the Griesmer bound is called a Griesmer code. An arc associated with a Griesmer code is called a Griesmer arc.

A divisible linear code is defined as a code whose word weights have a nontrivial common divisor [6]. It has been proved in [7] that every $[n,k,d]_q$-code meeting the Griesmer bound with minimum weight divisible by some power of q is also divisible. Using the equivalence between linear codes and arcs in the projective geometries $\mathrm{PG}(k-1,q)$, we can translate this in geometric language. An (n,w)-arc $\mathcal{K}$ is said to be divisible if there exists an integer $\Delta > 1$ such that $\mathcal{K}(H) \equiv n \pmod{\Delta}$ for any hyperplane H. Ward's divisibility result from [7] can be restated for Griesmer arcs as follows [5].

Theorem 1. *Let $\mathcal{K}$ be a Griesmer (n,w)-arc in* $\mathrm{PG}(k-1,p)$ *with* $w \equiv n \pmod{p^e}$*, p – a prime, $e \geq 1$. Then* $\mathcal{K}(H) \equiv n \pmod{p^e}$ *for every hyperplane H in* $\mathrm{PG}(k-1,p)$.

This result can be generalized to arcs and codes over non-prime fields. However the condition on the arc of meeting the Griesmer bound remains essential. Interestingly, some non-Griesmer arcs and codes also exhibit divisibility properties. In their investigation of arcs with parameters $(q^2+q+2, q+2)$ in $\mathrm{PG}(2,q)$ Ball et al. [3] observed that the presence of many double points implies divisibility of the arc. In the next section, we extend this observation to get a divisibility result for non-Griesmer arcs in finite projective geometries of arbitrary dimension.

3. THE MAIN THEOREM

Consider the projective geometry $\mathrm{PG}(r,q)$ and fix a hyperplane H_∞. Clearly, $\mathrm{PG}(r,q) \setminus H_\infty$ can be regarded as the r-dimensional affine geometry $\mathrm{AG}(r,q)$. The finite field $\mathbb{F}_{q^r}$ is an r-dimensional vector space over $\mathbb{F}_q$ and can be identified by the points of $\mathrm{AG}(r,q) = \mathrm{PG}(r,q) \setminus H_\infty$. The line through the points $X, Y \in \mathbb{F}_q^r$ is given parametrically by

$$L = \langle X, Y\rangle = \{tX + (1-t)Y \mid t \in \mathbb{F}_q\} \subset \mathbb{F}_{q^r}.$$

Let $X, Y, X', Y' \in \mathbb{F}_{q^r}$ be four points from $\mathrm{AG}(r,q)$ such that $\langle X, Y\rangle \cap H_\infty = \langle X', Y'\rangle \cap H_\infty$. If $\mathbb{F}_{q^r} = \mathbb{F}_q(\alpha)$, we can write the above four points as

$$\begin{aligned} X &= x_0 + x_1\alpha + \ldots + x_{r-1}\alpha^{r-1}, \quad & Y &= y_0 + y_1\alpha + \ldots + y_{r-1}\alpha^{r-1} \\ X' &= x'_0 + x'_1\alpha + \ldots + x'_{r-1}\alpha^{r-1}, \quad & Y' &= y'_0 + y'_1\alpha + \ldots + y'_{r-1}\alpha^{r-1} \end{aligned}$$

where $x_i, y_i, x'_i, y'_i \in \mathbb{F}_q$. In $\mathrm{PG}(r,q)$, the four points can be viewed as

$$(1, x_0, \ldots, x_{r-1}), (1, y_0, \ldots, y_{r-1}), (1, x'_0, \ldots, x'_{r-1}), (1, y'_0, \ldots, y'_{r-1}).$$

The common point of $\langle X, Y\rangle$ and $\langle X', Y'\rangle$, which lies in H_∞, is

$$(0, x_0 - y_0, x_1 - y_1, \ldots, x_{r-1} - y_{r-1}) = t(0, x'_0 - y'_0, x'_1 - y'_1, \ldots, x'_{r-1} - y'_{r-1})$$

where $t \in \mathbb{F}_q^*$. Hence

$$(X - Y) = \sum_{i=0}^{r-1}(x_i - y_i)\alpha^i = t\sum_{i=0}^{r-1}(x'_i - y'_i)\alpha^i = t(X' - Y')$$

and $(X-Y)^{q-1} = t^{q-1}(X'-Y')^{q-1} = (X'-Y')^{q-1}$. Therefore the points on H_∞ can be identified with the $\frac{q^r-1}{q-1}$-st roots of unity in $\mathbb{F}_{q^r}$. Denote by G the subgroup of $\mathbb{F}_{q^r}^*$ that contains the $\frac{q^r-1}{q-1}$-st roots of unity. The element of G identified with the intersecting point of the line L from $\mathrm{AG}(r,q)$ and H_∞ is denoted by ζ_L. The above argument shows that L and L' are parallel if and only if $\zeta_L = \zeta_{L'}$.

The next theorem is an application of the so-called polynomial method in finite geometry.

Theorem 2. *Let $\mathcal{K}$ be a (n,w)-arc in $\mathrm{PG}(r,q)$, $r \geq 2$, $q = p^h$, p – a prime. Let all lines through a point of maximal multiplicity m have the same multiplicity. If $\Lambda_m > (q-1)p^{t-1}$, where $t \leq (r-1)h$, then for every hyperplane H*

$$\mathcal{K}(H) \equiv n \pmod{p^t}.$$

Proof. Denote by s the multiplicity of a line through a maximal point and set, as usual, $v_i = \frac{q^i-1}{q-1}$. Then $n = m + (s-m)v_r$, and the multiplicity of a hyperplane H containing a maximal point is $\mathcal{K}(H) = m + (s-m)v_{r-1}$. Then

$$n - \mathcal{K}(H) = (s-m)(v_r - v_{r-1}) = (s-m)q^{r-1} \equiv 0 \pmod{q^{r-1}}.$$

Now consider a hyperplane which is not incident with points of maximal multiplicity. We can assume with no loss of generality that $0 \in \mathbb{F}_{q^r}$ is not a point of maximal multiplicity (otherwise, we translate the points of the affine geometry to ensure this). Consider the polynomial

$$\begin{aligned} F(x,y) &= \prod_{P\in\mathbb{F}_{q^r}} \left(1-(1-Px)^{q-1}y\right)^{\mathcal{K}(P)} \prod_{\zeta\in G}(1-\zeta x^{q-1}y)^{\mathcal{K}(\zeta)} \\ &= \sum_{i=0}^{n} F_i(x)y^i. \end{aligned}$$

Let $Q \in \mathbb{F}_{q^r}$ be a point of maximal multiplicity and set $x = Q^{-1}$. Note that $Q \neq 0$. When $P \neq Q$ we have

$$(1-PQ^{-1})^{q-1} = (Q-P)^{q-1}Q^{1-q} = \zeta_L Q^{1-q},$$

where $L = \langle P, Q\rangle$. Collecting the factors in the product above, we get

$$F(Q^{-1},y) = \prod_{\zeta\in G}(1-\zeta Q^{-1}y)^{\mathcal{K}(L)-\mathcal{K}(Q)}$$

where L is a line incident with Q and such that $L \cap H_\infty$ is identified with ζ. Further, we have

$$\begin{aligned} F(Q^{-1},y) &= \left(\prod_{\zeta\in G}(1-\zeta Q^{-1}y)\right)^{s-m} \\ &= (1-y^{v_r})^{s-m} \\ &= 1 - \binom{s-m}{1}y^{v_r} + \binom{s-m}{2}y^{2v_r} - \dots. \end{aligned}$$

Therefore $F_i(Q^{-1}) = 0$ for $i = 1, \ldots, v_r - 1$. The polynomial $F_i(x)$ is of degree at most $i(q-1)$ and since $\Lambda_m > (q-1)p^{t-1}$, we have $F_i(x) \equiv 0$ for all $i \leq p^{t-1}$. On the other hand,

$$\begin{aligned} F(0,y) &= (1-y)^{n-\mathcal{K}(H_\infty)} \\ &= 1 - \binom{n-\mathcal{K}(H_\infty)}{1} y + \binom{n-\mathcal{K}(H_\infty)}{2} y^2 - \ldots. \end{aligned}$$

This implies in particular that

$$\binom{n-\mathcal{K}(H_\infty)}{p^j} \equiv 0 \pmod{p}$$

for $j = 0, \ldots, t-1$. Now by Lucas theorem, $n - \mathcal{K}(H_\infty) \equiv 0 \pmod{p^t}$. □

4. ONE EXAMPLE

As an illustration of Theorem 2, consider the non-Griesmer arcs with parameters $(86, 22)$ in $\mathrm{PG}(3,4)$. Clearly, every line through a 2-point has multiplicity of 6. Assume $t = 2$ and $\Lambda_2 > (q-1)p^{t-1} = 6$. Recall the classification of the $(22,6)$-arcs in $\mathrm{PG}(2,4)$ from [3]. There exist six equivalence classes of such arcs:

(1) arcs with one 2-point and no 0-points;

(2) arcs with two 2-points and one 0-point, which are collinear;

(3) arcs with three 2-points and two 0-points, which are collinear;

(4) arcs with four 2-points and three collinear 0-points, which form a Baer subplane; the 0-points are collinear in the Baer subplane;

(5) arcs with six 2-points and five 0-points; the 2-points form a hyperoval and the 0-points form an external line to the hyperoval;

(6) arcs with seven 2-points and six 0-points, which are represented as a sum of two copies of a hypeoval plus the sum of two external lines to it.

By Theorem 2, the possible multiplicities of hyperplanes are: 2, 6, 10, 14, 18, 22. Planes of multiplicity 2 are impossible by a counting argument since 22- and 18-planes do not have 1-lines; 10-planes are ruled out by the nonexistence of $(10,3)$-arcs in $\mathrm{PG}(2,4)$. In order to rule out 6-planes, assume such a plane π exists and consider a projection φ from an arbitrary 0-point in π. The planes through an arbitrary 2-line in π are all 22-planes. Their image under φ is a line of type $(6,6,6,2,2)$ or $(6,6,4,4,2)$. In all cases, we get a line in the projection plane of multiplicity larger than 22, which is impossible.

It is easily checked that a 14-plane cannot be the complement of a line and two further points. So, it is the complement of a Baer subplane. If a plane of this size does not exist, the $(86, 22)$-arc is a sum of a plane $(22, 6)$-arc of type (6) and $AG(3, 4)$. Assume there is a 14-plane. Then there is exactly one 14-plane which is easily proved by considering the projection from a 0-point in this plane. But then an easy counting gives $\Lambda_2 = 8, \Lambda_1 = 70, \Lambda_0 = 7$. Such an arc is obtained by taking the 2- and 0-points to form a $PG(3, 2)$, where the 0-points are coplanar (all of them are on the 14-plane).

As a matter of fact, all $(86, 22)$-arcs with $\Lambda_2 < 7$ are obtained as the sum of a plane $(22, 6)$-arc and $AG(3, 4)$.

REFERENCES

1. Ball, S. Polynomials in finite geometries. In: Surveys in Combinatorics (eds J, D. Lamb, D. A. Preece), London Math. Society, Lecture Notes Series **267**, Cambridge University Press, 1999, 17–35.
2. Ball, S. The polynomial method in Galois geometries, In: Galois Geometries and Their Applications (eds J. de Beule, L. Storme), NOVA Publishers, 2010, to appear.
3. Ball, S., 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.
4. Griesmer, J. H. A Bound for Error-correcting Codes. *IBM J. Res. Develop.* **4**, 1960, 532–542.
5. Landjev, I. The geometric approach to linear codes. In: Finite Geometries (eds A. Blokhuis, J. Hirschfeld, D. Jungnickel, J. Thas) Ser. Developments in Mathematics, 2001, 247–257.
6. Ward, H. N. Quadratic residue codes and divisibility. In: Handbook of Coding Theory (eds V. S. Pless and W. C. Huffman; asst. ed. R. A. Brualdi) Elsevier, Amsterdam, 1998, 827–870.
7. Ward, H. N. Divisibility of codes meeting the Griesmer bound. *Journal of Combin. Theory Ser. A* **83**, No. 1, 1998, 79–93.

Received on December 17, 2009
Revised on June 1, 2010

Ivan N. Landjev
New Bulgarian University
21, Montevideo Str.
1618 Sofia, BULGARIA

Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8
1113 Sofia, BULGARIA
E-mail: i.landjev@nbu.bg, ivan@math.bas.bg

Assia P. Rousseva
Faculty of Mathematics and Informatics
"St. Kl. Ohridski" University of Sofia
5, J. Bourchier Blvd
1164 Sofia, BULGARIA
E-mail: assia@fmi.uni-sofia.bg