Mathematica
Balkanica

New Series Vol. 18, 2004, Fasc. 1-2

A Necessary Condition for the Existence of Arcs and Codes

Assia P. Rousseva

In this paper, we prove a simple necessary condition for the existence of arcs with given parameters in the finite projective geometries $PG(k,q)$. This result is applied to rule out the existence of certain arcs and linear codes.

AMS Subj. Classification: 51E15, 51E21, 51E22, 94B65

Key Words: finite projective geometries, arcs, linear codes,

1. Introduction

A *multiset in* $PG(k-1,q)$ is a mapping $\mathcal{K}\colon \mathcal{P} \to N_0$, where $\mathcal{P}$ denotes the pointset of $PG(k-1,q)$. The integer $\mathcal{K}(P) = \sum_{P\in\mathcal{P}} \mathcal{K}(P)$ is called the *multiplicity* of the point P. For any $\mathcal{Q} \subseteq \mathcal{P}$, we set $\mathcal{K}(\mathcal{Q}) = \sum_{P\in\mathcal{Q}} \mathcal{K}(P)$. A point of multiplicity i is called an i-point; i-lines, i-planes etc. are defined in a similar way. A multiset $\mathcal{K}$ in $PG(k-1,q)$ is called an $(n,w,k-1,q)$*-arc*, or an (n,w)-arc for short, if (a) $\mathcal{K}(\mathcal{P}) = n$; (b) for every hyperplane H in $PG(k-1,q)$, $\mathcal{K}(H) \le w$, and (c) there exists a hyperplane H_0 with $\mathcal{K}(H_0) = w$.

It is known that the existence of $(n,n-d)$ arcs in $PG(k-1,q)$ is equivalent to that of linear $[n,k,d]_q$ codes of full length (i.e. no coordinate is identically 0) [2, 8]. Thus the problem of the construction of arcs has a clear coding-theoretic relevance. In this note we prove a combinatorial necessary condition for the existence of arcs with given parameters. Furthermore, we apply it to rule out the existence of certain arcs and codes that are listed as undecided cases in [3, 10]. We refer to [4, 5, 9, 11] for further results on linear codes and sets of points in finite geometries.

Let $\mathcal{K}$ be a (n,w)-arc in $PG(k-1,q)$. We denote by $\gamma_i(\mathcal{K})$ the maximal multiplicity of an i-dimensional flat in $PG(k-1,q)$, i.e. $\gamma_i(\mathcal{K}) = \max_\delta \mathcal{K}(\delta)$, $i = 0,\dots,k-1$, where δ runs over all i-dimensional flats in $PG(k-1,q)$. If $\mathcal{K}$ is clear from the context we write γ_i. The following lemma which is proved by a straightforward counting (cf. [10]). Set $\phi_i = (q^i - 1)/(q - 1)$.

Lemma 1.1 *Let $\mathcal{K}$ be an $(n, n-d; k-1, q)$-arc, and let Π be an $(s-1)$-dimensional flat in $PG(k-1, q)$, $2 \le s < k$, with $\mathcal{K}(\Pi) = w$. Then, for any $(s-2)$-dimensional flat Δ contained in Π, we have*

$$\mathcal{K}(\Delta) \le \gamma_{s-1}(\mathcal{K}) - \frac{n-w}{\phi_{k-s} - 1}.$$

Denote by a_i the number of hyperplanes H in $PG(k-1, q)$ with $\mathcal{K}(H) = i$, $i = 0, 1, \dots$, and by λ_j – the number of points P from $\mathcal{P}$ with $\mathcal{K}(P) = j$. The sequence $(a_0, a_1, \dots)$ is called *the spectrum* of $\mathcal{K}$.

2. The necessary condition

Theorem 2.1. *Let $\mathcal{K}$ be a (n, w)-arc in $PG(k-1, q)$. Assume there exists a hyperplane H such that the restriction of $\mathcal{K}$ to H_0 has spectrum $(\tilde{a}_i)_{i \ge 0}$. Let*

$$\eta_i = \max_{\delta : \mathcal{K}(\delta) = i} \sum_{j=1}^{q} \binom{w - \mathcal{K}(H_j^{(\delta)})}{2},$$

where δ runs the $(k-3)$-dimensional subspaces in H_0 and $H_i^{(\delta)}$, $i = 0, 1, \dots, q$, are the other hyperplanes in $PG(k-1, q)$ through δ. Then

$$\sum_j \tilde{a}_j \eta_j + \binom{w - \mathcal{K}(H_0)}{2} \ge \binom{w}{2}\phi_k - n(w-1)\phi_{k-1} + \binom{n}{2}\phi_{k-2} + q^{k-2} \cdot \sum_{i=2}^{\gamma_0} \binom{i}{2}\lambda_i. \tag{1}$$

P r o o f. Denote the spectrum of $\mathcal{K}$ by (a_i). Simple counting arguments yield the following identities:

$$\sum_{i=0}^{w} a_i = \frac{q^k - 1}{q - 1}, \tag{2}$$

$$\sum_{i=1}^{w} i a_i = n \cdot \frac{q^{k-1} - 1}{q - 1}, \tag{3}$$

$$(4)\qquad \sum_{i=2}^{w}\binom{i}{2}a_i = \binom{n}{2}\frac{q^{k-2}-1}{q-1} + q^{k-2}\cdot\sum_{i=2}^{\gamma_0}\binom{i}{2}\lambda_i.$$

In (2) we count all hyperplanes; in (3) we count all flags (P,H), where P is a point and H is a hyperplane incident with P; in (4) we count all flags (P,Q,H), where P and Q are points and H a hyperplane incident with P. Taking a suitable linear combination of (2–4), we obtain:

$$(5)\ \sum_{i=0}^{w}\binom{w-i}{2}a_i = \binom{w}{2}\phi_k - n(w-1)\phi_{k-1} + \binom{n}{2}\phi_{k-2} + q^{k-2}\cdot\sum_{i=2}^{\gamma_0}\binom{i}{2}\lambda_i.$$

The sum on the left-hand side can be written as $\sum_H \binom{w-\mathcal{K}(H)}{2}$, where H runs over all hyperplanes of $PG(k-1,q)$. Now we have

$$\begin{aligned}\sum_H \binom{w-\mathcal{K}(H)}{2} &= \sum_{\delta:\delta\subset H_0}\sum_{i=1}^{n}\binom{w-\mathcal{K}(H_i^{(\delta)})}{2} + \binom{w-\mathcal{K}(H_0)}{2}\\ &\le \sum_j \tilde{a_j}\eta_j + \binom{w-\mathcal{K}(H_0)}{2},\end{aligned}$$

which implies the desired inequality. ∎

Remark 2.2. If $\mathcal{K}$ is projective, the numbers λ_i, $i \ge 2$, are all zero. Hence the right hand-side of the sum in (1) depends only on the parameters of the arc and can be viewed as a constant. For non-projective arcs, we can bound the numbers λ_i using additional arguments and still get a constant in (1).

3. The nonexistence of some arcs in $PG(4,4)$

First we prove the nonexistence of $(66,18)$ and $(65,18)$-arcs in $PG(4,4)$. For a hypothetical $(65,18)$- or $(66,18)$-arc we have by Lemma 1.1 $\gamma_)=2$, $\gamma_1=3$, $\gamma_2=6$ and $\gamma_3=18$. In addition, $\lambda_2=0$ or 1.

Lemma 3.1 *Let $\mathcal{K}$ be a $(66,18)$-arc in $PG(4,4)$. Then $a_i=0$ for $i=0,1,\dots,13$.*

Proof. Solids with 0, 1, 2 or 10 points are violated by Theorem 2.1. Here, we prove only $a_{10}=0$. Assume H_0 is a 10-solid. Then $\mathcal{K}_{H_0}$ is a $(10,4)$-arc. Hence its spectrum is one of the following [1]:

$$(6)\qquad \tilde{a}_0=5, \tilde{a}_1=20, \tilde{a}_2=15, \tilde{a}_3=20, \tilde{a}_4=25;$$

$$(7)\qquad \tilde{a}_0=6, \tilde{a}_1=16, \tilde{a}_2=21, \tilde{a}_3=16, \tilde{a}_4=28.$$

The right-hand side of (1) is 1848 if $\lambda_2 = 0$ and 1912 if $\lambda_2 = 1$. Further we have

$$\eta_4 = 0, \eta_3 = 6, \eta_2 = 28, \eta_1 = 34, \eta_0 = 56.$$

Now we get a contradiction to (1) for both spectra (6) and (7). The rest follows by Lemma 1.1. ∎

Theorem 3.2 *There exist no* $(66, 18)$*-arcs in* $PG(4, 4)$*. Equivalently, there exist no* $[66, 5, 48]_4$ *codes.*

Proof. By Lemma 3.1, a hyperplane has 14, 15, 16, 17 or 18 points. Assume H_0 is a hyperplane with 14, 15 or 16 points. Then $\mathcal{K}_{H_0}$ is an extendable cap by [13] and, therefore, it has an empty plane, π say. If H_i, $i = 1, \ldots, 4$, are the other solids through π, we have $66 = \sum_{i=0}^{4} \mathcal{K}(H_i) - 4 \cdot \mathcal{K}(\pi) \geq 70$, a contradiction. Hyperplanes with 17 points are ruled out in the same way. Now we have that every hyperplane has 18 points which is impossible by (3). ∎

Corollary 3.3 *There exist no* $(65, 18)$*-arcs in* $PG(4, 4)$*. Equivalently, there exist no* $[65, 5, 47]_4$ *codes.*

Proof. As above, we can rule out the existence of hyperplanes with 0, 3, 4, 6, 7, 8, 11, 12, 15, and 16 points. Now the result follows by Hill's extension theorem [6, 7, 12] and by Theorem 3.2. ∎

Using the same technique, one can prove the following new results.

Theorem 3.4 *There exist no* $(44, 13)$*-arcs in* $PG(4, 4)$*. Equivalently, there exist no* $[44, 5, 31]_4$ *codes.*

Theorem 3.5 *There exist no* $(84, 23)$*-arcs in* $PG(4, 4)$*. Equivalently, there exist no* $[84, 5, 61]_4$ *codes.*

Theorem 3.6 *There exist no* $(81, 22)$*-arcs in* $PG(4, 4)$*. Equivalently, there exist no* $[81, 5, 59]_4$ *codes.*

References

[1] S. Dodunekov, I. Landjev, On the Quaternary [11,6,5] and [12,6,6] Codes, Applications of Finite Fields (ed. D. Gollmann), *IMA Conference Series 59*, Clarendon Press, Oxford, 1996, 75–84.

[2] S. Dodunekov, J. Simonis, Codes and Projective Multisets, *Electronic Journal of Combinatorics*, **5** (1998), no. #R37.

[3] N. Hamada, T. Maruta, A survey of recent results on optimal codes and minihypers, *Discrete Mathematics*, submitted.

[4] W. Heise, P. Quattrocchi, *Informations- und Codierungstheorie*, Springer Verlag, Berlin, 3rd Edition, 1995.

[5] R. Hill, *A first course in coding theory*, Oxford University Press, Oxford, 1986.

[6] R. Hill, An extension theorem for linear codes, *Designs, Codes and Cryptography*, **17**(1999), 151-157.

[7] R. Hill, P. Lizak, Extensions of linear codes, *Proc. Intern. Symposium on Inform. Theory*, Canada, 1995, 345.

[8] Th. Honold, I. Landjev, Linear Codes over Finite Chain Rings, *Electronic Journal of Combinatorics*, **7** (2000),(1), no. #R11.

[9] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-correcting Codes*, North Holland, Amsterdam, 1977.

[10] I. Landjev, T. Maruta, On the minmum length of quaternary linear codes of dimension five, *Discrete Mathematics*, **202** (1999), 145–161.

[11] V. S. Pless, W. C. Huffman, R. A. Brualdi, An introduction to algebraic codes, in: *Handbook of Coding Theory*, (V. Pless and W. C. Huffman eds.), North Holland, 1998, 3–139.

[12] J. Simonis, Extensions of linear codes, *Proc. 7th Intern. Workshop on ACCT*, Bansko, Bulgaria, 2000, 279–282.

[13] H. N. Ward, A sequence of unique quaternary Griesmer codes, *Designs, Codes and Cryptography*, to appear.

Faculty of Mathematics and Informatics
5 J. Bourchier Blvd.
Sofia University
Sofia 1126, BULGARIA

Received 30.09.2003