THE NONEXISTENCE OF SOME OPTIMAL ARCS IN $PG(4,4)$

Assia Rousseva

Sofia University

Ivan Landjev

Institute of Mathematics and Informatics, BAS

– Optimal Codes and Related Topics, Varna, 16.-22.06.2009 –

1. Multisets of points

Definition. A **multiset** in $\mathrm{PG}(k-1,q)$ is a mapping

$$\mathcal{K} : \begin{cases} \mathcal{P} & \rightarrow & \mathbb{N}_0, \\ P & \rightarrow & \mathcal{K}(P). \end{cases}$$

◇ $\mathcal{K}(P)$ – **multiplicity** of the point P.

◇ $\mathcal{K}(\mathcal{P})$ – the **cardinality** of $\mathcal{K}$.

◇ $\mathcal{Q} \subset \mathcal{P}$: $\mathcal{K}(\mathcal{Q}) = \sum_{P \in \mathcal{Q}} \mathcal{K}(P)$.

◇ a_i – the number of hyperplanes H with $\mathcal{K}(H) = i$

◇ $(a_i)_{i \geq 0}$ – the **spectrum** of $\mathcal{K}$

Definition. (n, w)-**multiarc** in $\mathrm{PG}(k-1, q)$: a multiset $\mathcal{K}$ with

1) $\mathcal{K}(\mathcal{P}) = n$;

2) for every hyperplane H: $\mathcal{K}(H) \leq w$;

3) there exists a hyperplane H_0: $\mathcal{K}(H_0) = w$.

Definition. (n, w)-**blocking multiset** in $\mathrm{PG}(k-1, q)$

(or (n, w)-**minihyper**):

a multiset $\mathcal{K}$ with

1) $\mathcal{K}(\mathcal{P}) = n$;

2) for every hyperplane H: $\mathcal{K}(H) \geq w$;

3) there exists a hyperplane H_0: $\mathcal{K}(H_0) = w$.

2. Linear codes over finite fields

◇ **Linear $[n,k]_q$ code**: $C < \mathbb{F}_q^n$, $\dim C = k$

◇ $[n,k,d]_q$-**code**: $d = \min\{d(\boldsymbol{u},\boldsymbol{v}) \mid \boldsymbol{u},\boldsymbol{v} \in C, \boldsymbol{u} \neq \boldsymbol{v}\}$.

- n - the **length** of C;
- k - the **dimension** of C;
- d - the **minimum distance** of C.

◇ A_i – number of codewords of (Hamming) weight i

◇ $(A_i)_{i\geq 0}$ – the **spectrum** of C

3. Linear codes as multisets of points

A **linear code of full length** over $\mathbb{F}_q$:

A linear code $C \in \mathbb{F}_q^n$ is said to be of **full length** if $\forall i \in \{1, \ldots, n\}$, $\exists\ \boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in C$ with $c_i \neq 0$.

Theorem. For every multiset $\mathcal{K}$ of cardinality n in $\mathrm{PG}(k-1, q)$ there exist a linear code of full length $C < \mathbb{F}_q^n$ and a generating sequence of vectors $S = (\boldsymbol{c}_1, \cdots, \boldsymbol{c}_k)$ from C which induces $\mathcal{K}$. Two multisets $\mathcal{K}_1$ and $\mathcal{K}_2$ in $\mathrm{PG}(k-1, q)$ associated with the linear codes of full length C_1 and C_2 over $\mathbb{F}_q$, respectively, are equivalent if and only if C_1 and C_2 are semilinearly isomorphic.

$[n,k,d]_q$-code C of full length	$\Leftrightarrow$	$(n,n-d)$-multiarc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$
$\boldsymbol{u} \in C$, $\mathrm{wt}(\boldsymbol{u}) = n - w$	$\Leftrightarrow$	a hyperplane H with $\mathcal{K}(H) = w$,
$(A_i)_{i\geq 0}$	$\Leftrightarrow$	$(a_i)_{i\geq 0}$
		$a_i = \frac{1}{q-1} A_{n-i}$

3. The main problem of coding theory

Given the positive integers k, d, and the prime power q, find $n_q(k,d)$ the smallest value of n for which there exists a $[n,k,d]_q$ code.

4. The Griesmer bound

$$n_q(k,d) \geq g_q(k,d) := \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$$

In case of equality: **Griesmer codes**

◇ For k, q-fixed, d large enough, Griesmer codes always exist. (**Tamari**)

◇ For d, q-fixed, k large enough the Hamming bound gets better than the Griesmer bound and Griesmer codes do not exist. (**Dodunekov**)

◇ C: $[n, k, d]_q$-code with $n = t + g_q(k, d)$

◇ $\mathcal{K}$: $(n, n - d)$-(multi)arc in $\mathrm{PG}(k - 1, q)$ associated with C

◇ $\gamma_i :=$ maximal multiplicity of an i-dimensional subspace of $\mathrm{PG}(k - 1, q)$

◇ **Fact.**

$$\gamma_i \leq t + \sum_{j=0}^{i} \lceil \frac{d}{q^j} \rceil.$$

5. The status quo for $q = 4$

Problem.

For codes over $\mathbb{F}_4$, $n_4(k,d)$ has been found for $k \leq 4$ for all d.

For $k = 5$, $n_4(5,d)$ has been found for all but ≈110 values of d.

Some open cases for $k = 5$, $q = 4$:

d	$g_4(5,d)$	$n_4(5,d)$	(n,w)-arc
285	382	382–383	$(382, 97)$-arc
286	383	383–384	$(383, 97)$-arc
287	384	384–385	$(384, 97)$-arc
288	385	385–386	$(385, 97)$-arc

6. The Nonexistence result

Theorem. There exist no arcs with parameters $(384, 97)$ and $(385, 97)$ in $\mathrm{PG}(4, 4)$.

Corollary. There exist no codes with parameters $[384, 5, 287]_4$ and $[385, 5, 288]_4$. Consequently, $n_4(5, 287) = 385$ and $n_4(5, 288) = 386$.

d	$g_4(5, d)$	$n_4(5, d)$	(n, w)-arc
285	382	382–383	? $(382, 97)$
286	383	383–384	? $(383, 97)$
287	384	$\not{3}84$–385	$\nexists$ $(384, 97)$
288	385	$\not{3}85$–386	$\nexists$ $(385, 97)$

7. Sketch of proof

Step 1. For a $(385, 97)$-arc in $\mathrm{PG}(4, 4)$:

$$\gamma_0 = 2,\ \gamma_1 = 7,\ \gamma_2 = 25,\ \gamma_3 = 97.$$

A maximal hyperplane is a $(97, 25)$-arc in $\mathrm{PG}(3, 4)$.

Step 2. By Ward's divisibility result and additional combinatorial arguments, all multiplicities of hyperplanes (planes) for a $(97, 25)$-arc are 1 modulo 4.

It turns out that $a_i = 0$ for all $i \neq 9, 13, 17, 21, 25$.

Step 3. The possible multiplicities of hyperplanes (solids) for a $(385, 97)$-arc are $65, 81, 97$.

Step 4. Dualize a $(385, 97)$-arc in $\mathrm{PG}(4, 4)$ as follows:

$$\begin{array}{ccc} 65\text{-solids} & \longrightarrow & 2\text{-points} \\ 81\text{-solids} & \longrightarrow & 1\text{-points} \\ 97\text{-solids} & \longrightarrow & 0\text{-points} \end{array}$$

One gets a $(22, \{2, 6, 10\})$-arc in $\mathrm{PG}(4, 4)$.

Step 5. A $(22, \{2, 6, 10\})$-arc obtained by dualizing a $(385, 97)$-arc has a 3-line.

Step 6. A $(22, \{2, 6, 10\})$-arc cannot have a 3-line.

◦ projection from a 3-line: $(19, \{3, 7\})$-arc in $\mathrm{PG}(2, 4)$;

◦ characterization of all $(19, \{3, 7\})$-arcs in $\mathrm{PG}(2, 4)$;

◦ none of them is extendible to a $(22, \{2, 6, 10\})$-arc in $\mathrm{PG}(4, 4)$

(a straightforward computer search).

$\diamond$ The proof of the nonexistence of $(384, 97)$-arcs in $\mathrm{PG}(4, 4)$ follows from the geometric verison of **Hill**-**Lizak**'s extension theorem.

Theorem. (**Hill**, **Lizak**) Let $\mathcal{K}$ be an (n, w)-arc in $\mathrm{PG}(k-1, q)$ with $\gcd(n-w, q) = 1$. Assume that the multiplicities of all hyperplanes are congruent to n or w modulo q. Then $\mathcal{K}$ can be extended to an $(n+1, w)$-arc.