BLOCKING SETS IN FINITE PROJECTIVE SPACES AND THE EXTENSION PROBLEM FOR LINEAR CODES

Assia Rousseva
Sofia University

(joint work with Ivan Landjev)

– Seventh International Workshop on Optimal Codes and Related Topics, Albena, Bulgaria, 06.09.–12.09.2013 –

1. Linear Codes

◇ 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

◇ The code obtained by deleting the same coordinate from all codewords of C is called a punctured code for C.

◇ A linear $[n, k, d]_q$-code C is called extendable if there exists an $[n+1, k, d+1]_q$ code C' which gives C as a punctured code. In such case C' is called an extension of C.

Theorem.(Folklore) Every binary linear code of odd minimal weight is extendable.

Example.

$$G = \begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{pmatrix} \quad \Longrightarrow \quad G' = \begin{pmatrix} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&1&0&1&1 \\ 0&0&1&0&1&1&0&1 \\ 0&0&0&1&1&1&1&0 \end{pmatrix}$$

the $[7,4,3]_2$ Hamming code $\Longrightarrow$ the $[8,4,4]_2$ extended Hamming code

Theorem. (R. Hill, P. Lizak, 1995) Let C be a linear $[n,k,d]_q$-code with $\gcd(q,d)=1$ in which $A_i=0$ for all $i \not\equiv 0, d \pmod{q}$. Then C is extendable.

2. Multisets of points

◇ 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.

◇ $\mathcal{Q} \subset \mathcal{P}$: $\mathcal{K}(\mathcal{Q}) = \sum_{P \in \mathcal{Q}} \mathcal{K}(P)$ – multiplicity of the set $\mathcal{Q}$.

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

◇ Points, lines, ... ,hyperplanes of multiplicity i are called i-points, i-lines, ... , i-hyperplanes.

◇ 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)-arc 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 set 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: $\mathcal{K}(H_0) = w$.

Definition. An (n, w)-arc $\mathcal{K}$ in $\mathrm{PG}(k-1, q)$ is called extendable (or incomplete), if there exists an $(n+1, w)$-arc $\mathcal{K}'$ in $\mathrm{PG}(k-1, q)$ with $\mathcal{K}'(P) \geq \mathcal{K}(P)$ for every point $P \in \mathcal{P}$.

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 arc $\mathcal{K}$ 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 arcs $\mathcal{K}_1$ 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	$\Leftrightarrow$	$(n, w = n - d)$-arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$
$\mathbf{0} \neq \boldsymbol{u} \in C$, $\mathrm{wt}(\boldsymbol{u}) = u$	$\Leftrightarrow$	a hyperplane H with $\mathcal{K}(H) = n - u$,
$(A_i)_{i \geq 0}$	$\Leftrightarrow$	$(a_i)_{i \geq 0}$
		$a_i = \frac{1}{q-1} A_{n-i}$
extendable $[n,k,d]_q$-code C	$\Leftrightarrow$	extendable $(n, n-d)$-arc $\mathcal{K}$

Theorem. (R. Hill, P. Lizak, 1995) Let $\mathcal{K}$ be an (n,w)-arc in $\mathrm{PG}(k-1,q)$ with $\gcd(n-w,q) = 1$. Let further $\mathcal{K}(H) \equiv n$ or $w \pmod q$ for all hyperplanes H. Then $\mathcal{K}$ is extendable to an $(n+1,w)$-arc in $\mathrm{PG}(k-1,q)$.

4. Earlier Extension Results

Theorem.(Simonis,2000) An $[n, k, d]_q$-code with $\gcd(d, q) = 1$ is extendable if

$$\sum_{i \not\equiv d \pmod q} A_i = q^{k-1}.$$

Theorem.(Maruta,2001) An $[n, k, d]_q$-code with $\gcd(d, q) = 1$ is extendable if

$$\sum_{i \not\equiv d \pmod q} A_i < q^{k-1} + q^{k-3}\sqrt{q}(q-1).$$

Theorem.(Maruta,2004) Let C be an $[n, k, d]_q$ code such that $A_i = 0$ for all $i \not\equiv 0, -1, -2 \pmod q$ for odd $q \geq 5$. Then C is extendable.

Theorem. (Maruta, geometric version) Let $\mathcal{K}$ be an (n, w)-arc in $\mathrm{PG}(k-1, q)$, $q \geq 5$, odd. Let further $\mathcal{K}(H) \equiv n, n+1$ or $n+2 \pmod{q}$ for all hyperplanes H. Then $\mathcal{K}$ is extendable to an $(n+1, w)$-arc in $\mathrm{PG}(k-1, q)$.

5. A New Extension Theorem

$\diamond$ $\mathcal{K}$ - (n, w)-arc in $\Sigma = \mathrm{PG}(k-1, q)$

$\diamond$ for every hyperplane H, we have $\mathcal{K}(H) \equiv n, n+1, \ldots, n+t \pmod{q}$ where $0 < t < q$ is an integer constant.

$\diamond$ Define an arc $\widetilde{\mathcal{K}}$ in the dual space $\widetilde{\Sigma}$

$$\widetilde{\mathcal{K}} : \begin{cases} \mathcal{H} & \rightarrow & \mathbb{N}_0, \\ H & \rightarrow & \widetilde{\mathcal{K}}(H) := n + t - \mathcal{K}(H) \pmod{q}. \end{cases}$$

where $\mathcal{H}$ is the set of all hyperplanes of Σ.

Theorem. Let $\mathcal{K}$ be an (n, w)-arc in $\Sigma = \mathrm{PG}(k-1, q)$ and let $\widetilde{\Sigma}$ contain a hyperplane H^* with $\widetilde{\mathcal{K}}(x^*) \geq a > 0$, a an integer, for all points x^* incident with H^*. Then the arc $\mathcal{K}$ is a-extendable, there exists an extension $\mathcal{K}'$ of $\mathcal{K}$ with parameters $(n + a, w)$.

Theorem. Let S^* be a subspace of $\widetilde{\Sigma}$ then $\widetilde{\mathcal{K}}(S^*) \equiv t \pmod{q}$.

◇ By the above theorem, the arc $\widetilde{\mathcal{K}}$ has the following properties:

- the multiplicity of each point is at most t;

- the multiplicity of each subspace of dimension r, $1 \leq r \leq k-1$, is at least tv_r.

◇ Notation: $v_r = \dfrac{q^r - 1}{q - 1}$.

◇ Griesmer bound: Let $\mathcal{C}$ be an $[n, k, d]_q$-code. Then

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

◇ Griesmer arcs: arcs associated with codes meeting the Griesmer bound

Theorem. Consider a Griesmer (n,w)-arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$ with $\mathcal{K}(H) \equiv n, n+1, \ldots, n+t \pmod{q}$ for all hyperplanes H. Denote by (a_i) the spectrum of the arc $\mathcal{K}|_H$, where H is a fixed hyperplane of multiplicity w, with respect to $\mathcal{K}$. Let A be the largest integer such that a $(tv_{k-1}+A, tv_{k-2})$-minihyper contains necessarily a hyperplane in its support. If

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

then $\mathcal{K}$ is extendable.

Problem. What is the maximal integer A such that a $(tv_{k-1}+A, tv_{k-2})$-minihyper with the divisibility properties outlined above contains a hyperplane?