LINEAR CODES CLOSE TO THE GRIESMER BOUND AND THE RELATED GEOMETRIC STRUCTURES

Ivan Landjev
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences

(joint work with Assia Rousseva)

– ACCT-XV, Albena, 18.06.–24.06.2016 –

The Main Problem in Coding Theory

Given the positive integers q, k and d, find the smallest value of n for which there exists a linear $[n, k, d]_q$-code. This value is denoted by $n_q(k, d)$.

The Griesmer bound:

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

- k, q - fixed, $d \to \infty$ large: $n_q(k,d) - g_q(k,d) = 0$

  Theorem. For a given dimension k, $n_q(k,d) = g_q(k,d)$ for all values of $d \geq (k-2)q^{k-1} + 1$.

  (V. I. Belov, V. N. Logachev, V. P. Sandimirov, R. Hill)

- d, q - fixed, $k \to \infty$ large: $n_q(k,d) - g_q(k,d) \to \infty$

  Theorem. For every two integers l and $d \geq 3$, there exists an integer k_0 such that $n_q(k,d) \geq l + g_q(k,d)$ for all $k \geq k_0$.

  (S. Dodunekov)

Problem A. Given the positive integers q and k, what is the smallest value of t, denoted $t_q(k)$, such that there exists a

$$[t + g_q(k,d), k, d]_q\text{-code}$$

for all d.

Or, in other words, how far from the Griesmer bound a linear code of fixed dimension can be?

The Geometric Approach to Linear Codes

$[g_q(k,d)+t,k,d]_q$-code $\sim$

$(g_q(k,d)+t, g_q(k,d)+t-d)$-arc in $\mathrm{PG}(k-1,q)$.

Write

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

where $0 \leq \lambda_i < q$. Then

$$\begin{aligned} g_q(k,d) &= sv_k - \lambda_{k-2}v_{k-1} - \ldots - \lambda_1 v_2 - \lambda_0 v_1, \\ w = g_q(k,d) - d &= sv_{k-1} - \lambda_{k-2}v_{k-2} - \ldots - \lambda_1 v_1, \end{aligned}$$

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

Problem B. Find the smallest t for which there exists a $(g_q(k,d)+t, w+t)$-arc in $\mathrm{PG}(k-1,q)$.

If $\mathcal{K}$ is a $(g_q(k,d)+t, w+t)$-arc in $\mathrm{PG}(k-1,q)$, then $s\,\mathrm{PG}(k-1,q)-\mathcal{K}$ is a minihyper with parameters

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

with maximal point multiplicity s.

Generalized Hill Conjecture. If $d \leq sq^{k-1}$ then there always exist an optimal $[n_q(k,d),k,d]_q$-code such that the associated $(n_q(k,d), n_q(k,d)-d)$-arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$ has maximal point multiplicity s.

Problem C. Find the minimum value of t for which there exists a minihyper in $\mathrm{PG}(k-1,q)$ with parameters

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

with maximal point multiplicity s.

Theorem. Let $d = sq^{k-1} - \lambda_{k-2}q^{k-2} - \ldots - \lambda_1 q - \lambda_0$, and let the multiset $\mathcal{F}$ be the sum of λ_{k-2} hyperplanes, λ_{k-3} hyperlines etc. λ_1 lines, λ_0 points. Define the multiset $\mathcal{F}'$ by

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

Let $N = |\mathcal{F}|$ and $N' = |\mathcal{F}'|$. If $\mathcal{F} - \mathcal{F}'$ is an $(N - N', t)$-arc then there exists a code with parameters $[t + g_q(k,d), k, d]_q$-code.

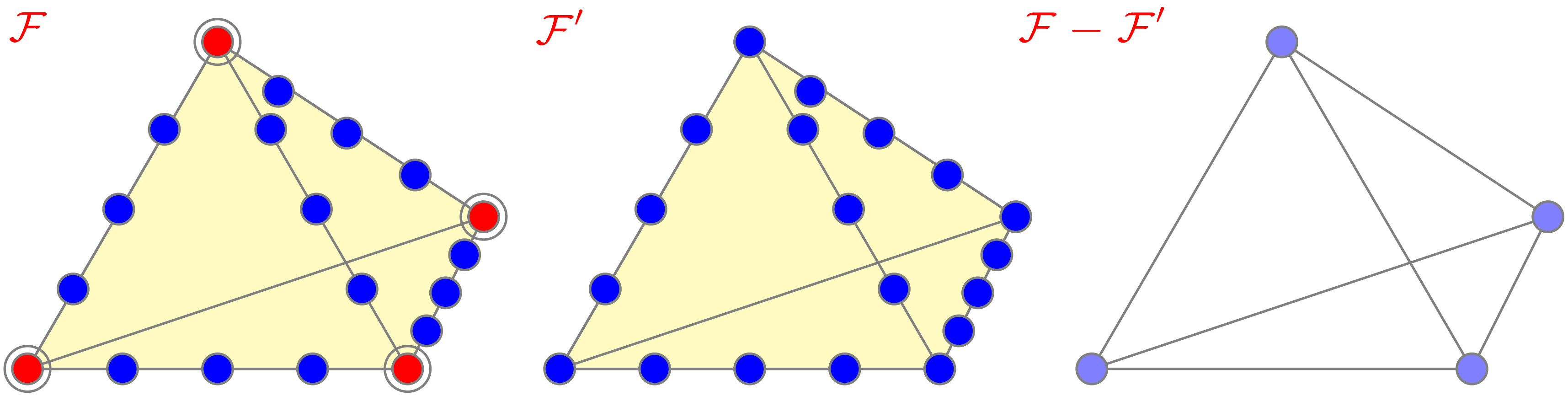
Example.

$k = 4$, $d = 2q^3 - 4q^2 - \lambda_1 q - \lambda_0$, $s = 2$

$(4v_3 + \lambda_1 v_2 + \lambda_0 v_1, 4v_2 + \lambda_1 v_1)$-minihyper

$(4v_3 + \lambda_1 v_2 + \lambda_0 v_1 - 4, 4v_2 + \lambda_1 v_1 - 3)$-minihyper

$[g_q(4, d) + 3, 4, d]_q$-code



Theorem. Let

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

and assume there exists a minhyper in $\mathrm{PG}(k-2,q)$ with parameters

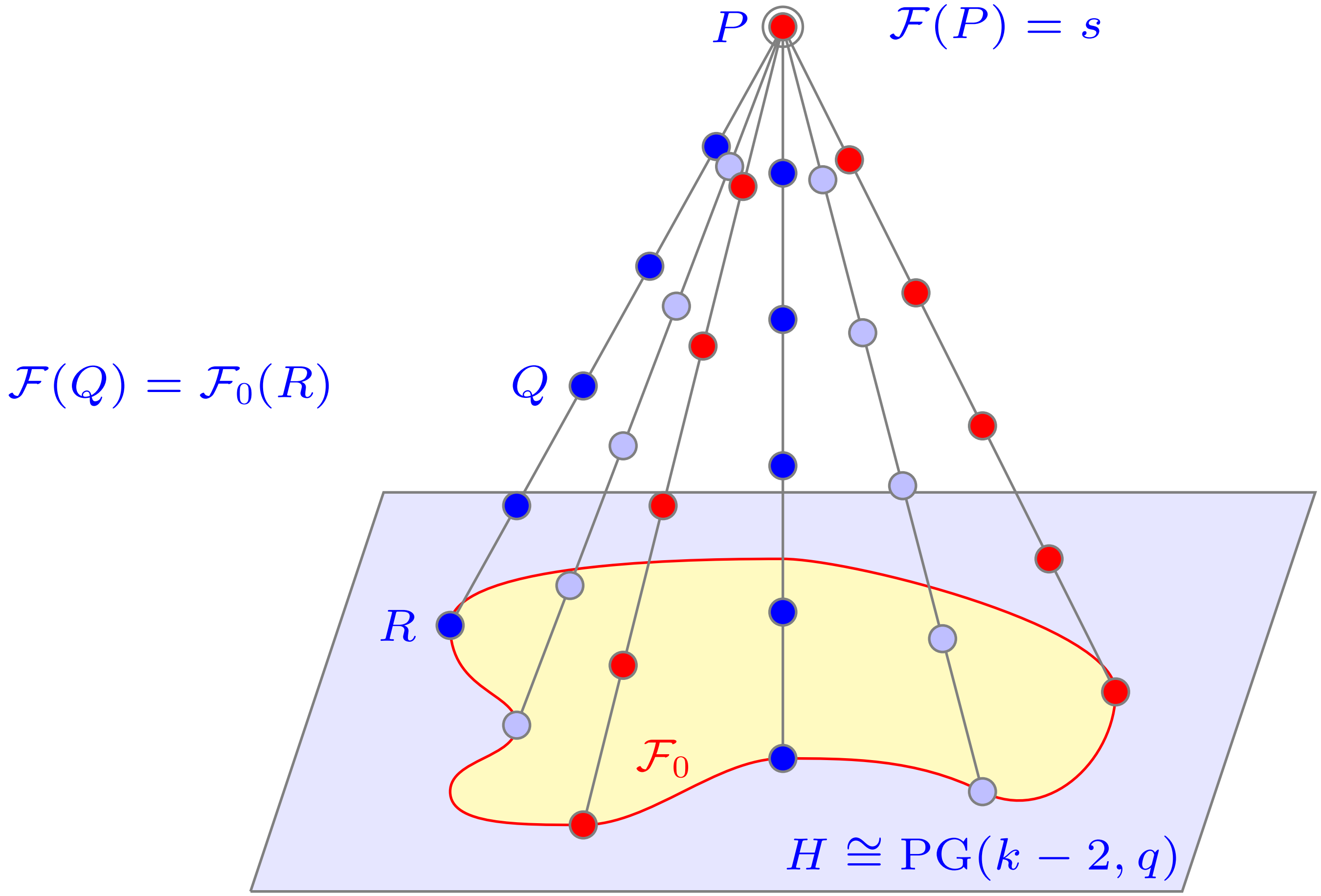
$$(\lambda_{k-2}v_{k-2} + \ldots + \lambda_1 v_1 - t, \lambda_{k-2}v_{k-3} + \ldots + \lambda_2 v_1 - t).$$

with maximal point multiplicity s. Then there exists a minihyper in $\mathrm{PG}(k-1,q)$ with parameters

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

with maximal point multiplicity s, where

$$f(t) = qt + \lambda_1 + \lambda_2 - s.$$


P
$\mathcal{F}(P) = s$
$\mathcal{F}(Q) = \mathcal{F}_0(R)$
Q
R
$\mathcal{F}_0$
$H \cong \mathrm{PG}(k-2, q)$

Corollary.

$$t_q(k) \leq q t_q(k-1) + 2q - 3.$$

Corollary.

$$t_q(k) \lesssim q^{k-2}.$$

Known Results for Small k

- $t_q(2) = 0$ for all q
- $t_q(3) = 1$ for all $q \leq 19$;
- $t_q(3) \leq 2$ for $q = 23, 25, 27, 29$;
- $t_3(4) = 1$;
- $t_4(4) = 1$;
- $t_5(4) = 2$ ($t = 2$ for $d = 25$ only);
- $t_5(5) \leq 5$.

The Case $k = 3$

Problem B′. (S. Ball): For a fixed $n - d$, is there always a 3-dimensional code meeting the Griesmer bound (maybe a constant or $\log q$ away)?

Theorem. For all $d \geq q^2$ (i.e. $s \geq 2$) there exist Griesmer $[n, 3, d]_q$ codes (arcs).

Lemma. Let $\mathcal{K}$ be an (n, w)-arc in $\mathrm{PG}(2, q)$ with $n = (w - 1)q + w - \alpha$ and let $\mathcal{C}_{\mathcal{K}}$ be the $[n, 3, d]_q$-code associated with this arc. Then $n = t + g_q(3, d)$ with $t = \lfloor \alpha/q \rfloor$.

Lower Bounds on the size of an (n, w)-arc in $\mathrm{PG}(2, q)$

w	q	$\geq$	$t = \lfloor \alpha/q \rfloor$
3		$2q+3-(q+3-2\sqrt{q})$	0
$\sqrt{q}$	square	$(w-1)q+w-(w-1)$	0
$q-\sqrt{q}$	square	$(w-1)q+w-(w-\sqrt{q})$	0
w	square	$(w-1)q+w-\sqrt{q}(q-w+1)$	$\sqrt{q}$
$(q-w)\|q$		$(w-1)q+w-(q-2w)$	0
$\frac{q+1}{2}, \frac{q+3}{2}$	odd	$(w-1)q+w-(w-1)$	0
$q-1$		$(w-1)q+w-(w-1)$	0
$q-2$	even	$(w-1)q+w-(w-2)$	0

Let $d = q^2 - \lambda_1 q - \lambda_0, \quad 0 \leq \lambda_0, \lambda_1 < q.$

Then

$$g_q(3, d) = v_3 - \lambda_1 v_2 - \lambda_0 v_1.$$

The Griesmer code is associated with an arc (Griesmer arc) with parameters:

$$(v_3 - \lambda_1 v_2 - \lambda_0 v_1, v_2 - \lambda_1 v_1)$$

As a minihyper:

$$(\lambda_1 v_2 + \lambda_0 v_1, \lambda_1 v_1).$$

For $d < q^2$, we consider only projetcive codes. This is justified by the following conjecture by R. Hill.

Conjecture. (R. Hill) If $d \leq q^2$, then there exists an $[n_q(3,d), 3, d]$ code over $\mathbb{F}_q$ which is projective.

The problem of finding $t_q(3)$ is equivalent to the following:

What is the smallest value of t for which there exists a **projective**

$(\lambda_1(q+1) + \lambda_0 - t, \lambda_1 - t)$-blocking set.

Lemma. Let $d_0 = q^2 - \lambda q - \lambda'$ and assume there exists an $[n_0, 3, d_0]_q$-code with $n_0 = t + g_q(3, d_0)$. Then for $d = q^2 - \mu q - \mu'$, $\mu \geq \lambda$, $\mu' \geq \lambda'$, there exists an $[n, 3, d]_q$-code with $n = t + g_q(3, d) + (\mu - \lambda)$.

Theorem. For $q = 2^h$

$$t_q(3) \leq \frac{q}{2} - 5.$$

Theorem. For every odd prime power q

$$t_q(3) \leq \frac{q-3}{2}.$$

Theorem. For q square

$$t_q(3) \leq 2\sqrt{q} - 1.$$

Conjecture. (Ball)

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

$$t_q(k) \le (\log q)^{k-2}.$$

Conjecture. (Maruta)

$$t_q(k) \le k - 2.$$