ON THE ASYMPTOTIC TIGHTNESS OF THE GRIESMER BOUND

Assia Rousseva
Sofia University

(joint work with Ivan Landjev)

– Fifth Irsee Conference “Finte Geometries”, Kloster Irsee, 10.–16.09.2017 –

The Main Problem in Coding Theory

Given the positive integers k and d, and a prime power q, 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:

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

Griesmer code: an $[n, k, d]_q$ code with $n = g_q(k, d)$.

k, q - fixed, $d \to \infty$

Theorem. For a given dimension k, there exists an integer d_0 such that for all $d \geq d_0$

$$n_q(k,d) - g_q(k,d) = 0.$$

- Baumert, McEliece: $n_2(k,d) - g_2(k,d) = 0$ for all $d \geq \lceil \frac{k-1}{2} \rceil 2^{k-1}$.

- V. I. Belov, V. N. Logachev, V. P. Sandimirov, R. Hill: $n_q(k,d) - g_q(k,d) = 0$ for all $d \geq (k-2)q^{k-1} + 1$.

- Maruta: $n_q(k,d) - g_q(k,d) > 0$ for $d = (k-2)q^{k-1} - (k-1)q^{k-2}$ for $q \geq k$, $k = 3,4,5$, and for $q \geq 2k+3$, $k \geq 6$.

d, q - fixed, $k \to \infty$

Theorem. (S. Dodunekov) For every two integers t and $d \geq 3$, there exists an integer k_0 such that for all $k \geq k_0$

$$n_q(k, d) - g_q(k, d) \geq t.$$

Idea of proof.

d, q, $R = \lfloor (d-1)/2 \rfloor$ - fixed, $k \to \infty$

$$|B_q^{g_q(k,d)}(R)| = \sum_{i=0}^{R} \binom{g_q(k,d)}{i} (q-1)^R \longrightarrow_{k \to \infty} \infty.$$

Consider an optimal $[n_q(k,d),k,d]_q$-code. From the sphere-packing bound:

$$\begin{aligned} q^{n_q(k,d)} &\geq q^k \cdot \sum_{i=0}^{R} \binom{n_q(k,d)}{i}(q-1)^i \\ &\geq q^k \cdot \sum_{i=0}^{R} \binom{g_q(k,d)}{i}(q-1)^i \end{aligned}$$

whence

$$n_q(k,d) - k \geq \log_q |B_R^{g_q(k,d)}(R)| \to \infty.$$

On the other hand

$$
\begin{aligned}
g_q(k,d) &= d + \lceil\frac{d}{q}\rceil + \lceil\frac{d}{q^2}\rceil + \ldots + \lceil\frac{d}{q^{k-1}}\rceil \\
&< d + \frac{d}{q} + \frac{d}{q^2} + \ldots + \frac{d}{q^{k-1}} + k - 1
\end{aligned}
$$

whence

$$
g_q(k,d) - k < d\frac{q^k - 1}{q^k - q^{k-1}} - 1,
$$

and

$$
n_q(k,d) - g_q(k,d) > \log_q |B_q^{g_q(k,d)}(R)| - d\frac{q^k - 1}{q^k - q^{k-1}} + 1 \to \infty.
$$

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

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

for all d.

Or, in other words, what is

$$t_q(k) := \max_d (n_q(k,d) - g_q(k,d)).$$

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 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

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

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

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

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

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

Let $\mathcal{K}$ be a $(g_q(k,d)+t, w_q(k,d)+t)$-arc in $\mathrm{PG}(k-1,q)$

Denote the maximal point multiplicity in $\mathcal{K}$ by $s_0 \le t+s$.

Construct the multiset $\mathcal{F} := s_0\,\mathrm{PG}(k-1,q) - \mathcal{K}$.

This multiset $\mathcal{F}$ is a minihyper with parameters

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

where

$$\sigma = \begin{cases} s_0 - s & \text{if } s < s_0 \le t+s, \\ 0 & \text{if } s_0 \le s, \end{cases}$$

with maximal point multiplicity $\sigma + s$.

Problem C. For all d given by

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

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

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

with maximal point multiplicity $\sigma + s$.

Example. Let $d = 85, k = 4, q = 5$. Then

$$s = 1, \lambda_2 = 1, \lambda_1 = 3, \lambda_0 = 0, g_5(4, 85) = 107, w = 22.$$

As a code: Find the smallest t so that there exists a $[107 + t, 4, 85]_5$-code.

As an arc: Find the smallest t so that there exists a $(107 + t, 22 + t)$-arc in $\mathrm{PG}(3, 5)$

As a minihyper:

$\sigma + s$ / t	1	2	3	4
0	$(49, 9)$			
1	$(48, 8)$	$(204, 39)$		
2	$(47, 7)$	$(203, 38)$	$(359, 69)$	
3	$(46, 6)$	$(202, 37)$	$(358, 68)$	$(514, 99)$

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 a minihyper in $\mathrm{PG}(k-1,q)$ with parameters

$$(\sigma v_k + \lambda_{k-2}v_{k-1} + \ldots + \lambda_0 v_1 - \tau_1, \sigma v_{k-1} + \lambda_{k-2}v_{k-2} + \ldots + \lambda_1 v_1 - \tau_1).$$

Define the multiset $\mathcal{F}'$ by

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

Let $N = |\mathcal{F}|$ and $N' = |\mathcal{F}'|$. If $\mathcal{F} - \mathcal{F}'$ is an $(N - N', \tau_2)$-arc then there exists a $(g_q(k,d) + t, w_q(k,d) + t)$-arc in $\mathrm{PG}(k-1,q)$, or, equivalently, a code with parameters $[g_q(k,d) + t, k, d]_q$, with $t = \tau_1 + \tau_2$.

Example.

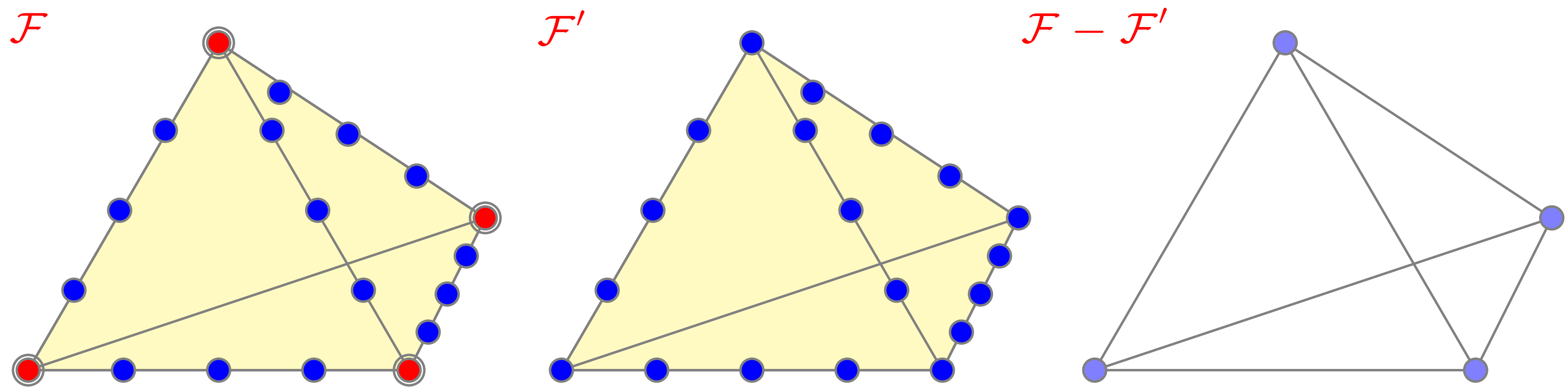
$k = 4$, $d = 2q^3 - 4q^2$; $s = 2$, $\lambda_2 = 4$, $\lambda_1 = 0$

s_0 / t	2	3	4
0	$(4v_3, 4v_2)$		
1	$(4v_3 - 1, 4v_2 - 1)$	$(v_4 + 4v_3 - 1, v_3 + 4v_2 - 1)$	
2	$(4v_3 - 2, 4v_2 - 2)$	$(v_4 + 4v_3 - 2, v_3 + 4v_2 - 2)$	$(2v_4 + 4v_3 - 2, 2v_3 + 4v_2 - 2)$
3	$(4v_3 - 3, 4v_2 - 3)$	$(v_4 + 4v_3 - 3, v_3 + 4v_2 - 3)$	$(2v_4 + 4v_3 - 3, 2v_3 + 4v_2 - 3)$

$(4v_3, 4v_2)$-minihyper, $\sigma = 0$, $\tau_1 = 0$

$(4v_3 - 3, 4v_2 - 3)$-minihyper with maximal point multiplicity 2

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

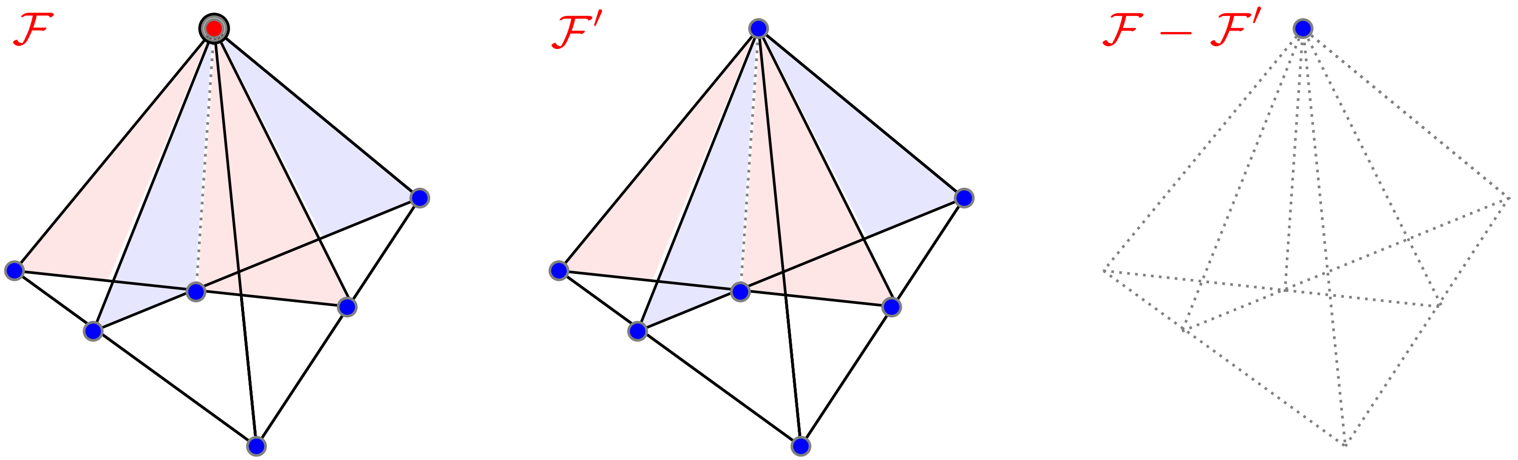


$(4v_3-2, 4v_2-2)$-minihyper with maximal point multiplicity 2:

Take the four planes to have a common point, but no three with a common line

$\mathcal{F}-\mathcal{F}'$ is a $(2,2)$-arc, i.e. $t=2$

$[g_q(4,d)+2,4,d]_q$-code for all q



For $q=5$ there exists a code with $t=1$, i.e. a $[189,4,150]_5$-code, which is optimal.

$$D_q^{(t)}(k) := \{d \in \mathbb{Z} \mid 1 \leq d \leq q^{k-1},\ n_q(k,d) = g_q(k,d) + t\}.$$

Lemma. Let $d_1 < d_2$ be integers from $D_q^{(t)}(k)$. Then for every integer d with $d_1 < d < d_2$

$$n_q(k,d) \leq g_q(k,d) + t + \sum_{i=1}^{k-2}(\lceil \frac{d_2}{q^i} \rceil - \lceil \frac{d_1}{q^i} \rceil).$$

Theorem.

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

Theorem.

$$t_q(4) \leq q-1.$$

The Case $k = 3$

Problem D. (S. Ball): For a fixed $n - d$, is there always a 3-dimensional linear $[n, 3, d]$-code meeting the Griesmer bound (or at least close to the Griesmer bound, maybe a constant or $\log q$ away)?

The answer to the first part of the question in Problem D is NO.

Take $w = n - d = q + 2$. Then an optimal arcs has $n = q^2 + q + 2$, but a $[q^2 + q + 2, 3, q^2]_q$-code is NOT a Griesmer code.

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 $\mathcal{K}$. Then $n = t + g_q(3, d)$ with $t = \lfloor \alpha/q \rfloor$.

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

In fact, Griesmer codes do exist for all $d \geq q^2 - 2q + 1$

For $q^2 - 3q + 1 \leq d \leq q^2 - 2q$ we have $t = 0$ or $t = 1$.

Theorem. If $q = 2^h$ then

$$t_q(3) \leq \log_2 q - 1 = h - 1.$$

The proof is based on the following two lemmas.

Lemma. Let $q = 2^h$. The sum of r maximal arcs is equivalent to a linear $[n, 3, d]_q$-code whose length satisfies $n = g_q(3, d) + (r - 1)$, i.e. its length exceeds by $r - 1$ the corresponding Griesmer bound.

Lemma. Let $q = 2^h$. Every integer $m \leq q - 1$ can be represented as

$$m = 2^{a_1} + \ldots + 2^{a_r} - r,$$

for some $a_i \in \{1, \ldots, h - 1\}$ and some $r \leq h = \log_2 q$.

Theorem. For q odd square

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

Theorem. For every odd prime power q

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

Conjecture. (Ball)

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

Conjecture. (Maruta)

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