On the constructions of optimal linear codes

Tatsuya Maruta

(Joint work with Yuuki Kageyama)

Department of Mathematics
and Information Sciences
Osaka Prefecture University
maruta@mi.s.osakafu-u.ac.jp

Overview

We construct some optimal linear codes over $\mathbb{F}_q$ through projective geometry, using the geometric methods such as projective dual and geometric puncturing.

Contents

1. Basic notions

$\mathbb{F}_q^n = \{(a_1, a_2, ..., a_n) \mid a_1, ..., a_n \in \mathbb{F}_q\}$.
For $a = (a_1, ..., a_n), b = (b_1, ..., b_n) \in \mathbb{F}_q^n$,
the (Hamming) distance between a and b is

$$d(a, b) = |\{i \mid a_i \neq b_i\}|.$$

The weight of a is $wt(a) = |\{i \mid a_i \neq 0\}| = d(a, \mathbf{0})$.

An $[n, k, d]_q$ code $\mathcal{C}$ means a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum distance d,

$$\begin{aligned} d &= \min\{d(a, b) \mid a \neq b,\ a, b \in \mathcal{C}\} \\ &= \min\{wt(a) \mid wt(a) \neq 0,\ a \in \mathcal{C}\}. \end{aligned}$$

The elements of $\mathcal{C}$ are called codewords.

For an $[n,k,d]_q$ code $\mathcal{C}$, a generator matrix G is a $k \times n$ matrix over $\mathbb{F}_q$ whose k rows form a basis of $\mathcal{C}$.

We assume G has no all-zero column.

The weight distribution (w.d.) of $\mathcal{C}$ is the list of numbers $A_i = |\{c \in \mathcal{C} \mid wt(c) = i\}|$.

The weight distribution with

$$(A_0, A_d, ..., A_i, ...) = (1, \alpha, ..., w, ...)$$

is also expressed as

$$0^1 d^\alpha \cdots i^w \cdots.$$

Two $[n,k,d]_q$ codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if there exists a monomial matrix M with entries in $\mathbb{F}_q$ such that $\mathcal{C}_2$ coincides with $\mathcal{C}_1 M = \{\boldsymbol{c}M \mid \boldsymbol{c} \in \mathcal{C}_1\}$.

A good $[n,k,d]_q$ code will have

small length n for fast transmission of messages,

large dimension k to enable transmission of a wide variety of messages,

large minimum distance d to correct many errors.

Optimal linear codes problem.

Optimize one of the parameters n, k, d for given the other two.

An $[n,k,d]_q$ code $\mathcal{C}$ is

N-optimal if $\nexists [n-1,k,d]_q$

K-optimal if $\nexists [n,k+1,d]_q$

D-optimal if $\nexists [n,k,d+1]_q$.

N-optimal codes are K-optimal and D-optimal.

Problem 1. Find $n_q(k,d)$, the minimum value of n for which an $[n,k,d]_q$ code exists for given k,d,q.

An $[n,k,d]_q$ code is called optimal if $n = n_q(k,d)$.

The Griesmer bound

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

where $\lceil x \rceil$ is a smallest integer $\geq x$.

Griesmer (1960) proved for binary codes.
Solomon and Stiffler (1965) proved for all q.

A linear code attaining the Griesmer bound is called a Griesmer code. Griesmer codes are optimal.

Since $n_q(k,d) = g_q(k,d)$ for $k = 1, 2$, we assume $k \geq 3$.

Known results for small q

The exact values of $n_q(k,d)$ are known for all d for

$q = 2,\ k \le 8,$

$q = 3,\ k \le 5,$

$q = 4,\ k \le 4,$

$q = 5, 7, 8, 9,\ k \le 3.$

$n_5(4,d)$ is not determined yet only for

$d =$81,82,161,162.

Landjev-Rousseva announced $\nexists [g_5(4,d), 4, d]_5$ codes for $d = 82, 162$ at ALCOMA15 (March 2015). Hence

$$n_5(4,d) = g_5(4,d) + 1 \quad \text{for } d = 82, 162.$$

$n_5(4,d) = g_5(4,d)$ or $g_5(4,d) + 1$ for $d = 81, 161$.

Known results for small q

The exact values of $n_q(k,d)$ are known for all d for

$q = 2,\ k \le 8,$

$q = 3,\ k \le 5,$

$q = 4,\ k \le 4,$

$q = 5, 7, 8, 9,\ k \le 3.$

$n_5(4,d)$ is not determined yet only for

$d =$81,82,161,162.

Landjev-Rousseva announced $\nexists [g_5(4,d), 4, d]_5$ codes for $d = 82, 162$ at ALCOMA15 (March 2015). See

`http://www.mi.s.osakafu-u.ac.jp/~maruta/griesmer.htm.`

for the $n_q(k,d)$ tables for some small q and k.

2. Geometric method

$\mathrm{PG}(r,q)$: projective space of dim. r over $\mathbb{F}_q$

j-flat: j-dim. projective subspace of $\mathrm{PG}(r,q)$

$\theta_j := |\mathrm{PG}(j,q)| = q^j + q^{j-1} + \cdots + q + 1$

Assume $\mathcal{C}$ has no coordinate which is identically zero.

G: a generator matrix of $\mathcal{C}$

The columns of G can be considered as a multiset of n points in $\Sigma = \mathrm{PG}(k-1,q)$ denoted by $\mathcal{M}_{\mathcal{C}}$. Conversely, $\mathcal{M}_{\mathcal{C}}$ gives linear codes which are equivalent to $\mathcal{C}$.

$\mathcal{F}_j :=$ the set of all j-flats in Σ

$\Sigma \ni P$: i-point $\Leftrightarrow$ P has multiplicity i in $\mathcal{M}_{\mathcal{C}}$

$\gamma_0 = \max\{i \mid \exists P : \ i\text{-point in } \Sigma\}$

$C_i = \{P \in \Sigma \mid P : i\text{-point}\}$, $0 \leq i \leq \gamma_0$

$\Delta_1 + \cdots + \Delta_s$: the multiset consisting of the s sets

$\Delta_1, \cdots, \Delta_s$ in Σ.

$s\Delta = \Delta_1 + \cdots + \Delta_s$ when $\Delta_1 = \cdots = \Delta_s = \Delta$.

Then, $\mathcal{M}_{\mathcal{C}} = C_1 + 2C_2 + \cdots + \gamma_0 C_{\gamma_0}$.

For any set S in Σ, $\mathcal{M}_{\mathcal{C}}(S)$ is the multiset

$$\{P \in \mathcal{M}_{\mathcal{C}} \mid P \in S\}.$$

The multiplicity of S, denoted by $m_{\mathcal{C}}(S)$, is defined as

$$m_{\mathcal{C}}(S) = |\mathcal{M}_{\mathcal{C}}(S)| = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|.$$

Then it holds that

$$\begin{aligned} n &= m_{\mathcal{C}}(\Sigma), \\ n-d &= \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}. \end{aligned}$$

Conversely, a multiset on Σ satisfying the above equalities gives an $[n,k,d]_q$ code in the natural manner.

Let $a_i := |\{\pi \in \mathcal{F}_{k-2} \mid m_{\mathcal{C}}(\pi) = i\}|$.

The list of a_i's is the spectrum of $\mathcal{C}$. Note that

$$a_i = A_{n-i}/(q-1) \text{ for } 0 \le i \le n-d.$$

Then it holds that

$$\begin{aligned} n &= m_{\mathcal{C}}(\Sigma), \\ n-d &= \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}. \end{aligned}$$

Conversely, a multiset on Σ satisfying the above equalities gives an $[n,k,d]_q$ code in the natural manner.

Example 1. Take $C_s = \Sigma$, i.e., $\mathcal{M}_{\mathcal{C}} = s\Sigma$ with $s \in \mathbb{N}$, $\Sigma = \mathrm{PG}(k-1,q)$.
Then $\mathcal{C}$ is a Griesmer $[s\theta_{k-1}, k, sq^{k-1}]_q$ code.
Since $m_{\mathcal{C}}(\pi) = s\theta_{k-2}$ for any $\pi \in \mathcal{F}_{k-2}$, $a_{s\theta_{k-2}} = \theta_{k-1}$ and every non-zero codeword has weight sq^{k-1}.
$\mathcal{C}$ is called an s-fold simplex code.

Example 2.

Let $\mathcal{C}$ be a $[20, 4, 10]_2$ code with generator matrix $G =$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Then $\mathcal{C}$ is Griesmer with w.d. $0^1 10^{11} 12^3 14^1$.

$C_1 = \{0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001\}$

$C_2 = \{1010, 1011, 1100, 1101, 1110, 1111\}$

$\mathcal{M}_{\mathcal{C}} = C_1 + 2C_2$

0001 is the only 0-point in PG$(3, 2)$.

Q 1. How can we construct G?

Lemma 1. (Maruta-Oya, 2011)
$\mathcal{C}$: $[n, k, d]_q$ code
If $\mathcal{M}_{\mathcal{C}} \supset \Delta$: a t-flat and $d > q^t$
$\quad\Rightarrow\quad \exists\mathcal{C}'$: $[n - \theta_t, k, d']_q$ code with $d' \geq d - q^t$.

The above $\mathcal{C}'$ can be constructed from the multiset $\mathcal{M}_{\mathcal{C}}$ by deleting Δ. We denote the resulting multiset by $\mathcal{M}_{\mathcal{C}'} = \mathcal{M}_{\mathcal{C}} - \Delta$.

Lemma 1. (Maruta-Oya, 2011)
$\mathcal{C}$: $[n, k, d]_q$ code
If $\mathcal{M}_{\mathcal{C}} \supset \Delta$: a t-flat and $d > q^t$
$\Rightarrow \quad \exists \mathcal{C}'$: $[n - \theta_t, k, d']_q$ code with $d' \geq d - q^t$.

The puncturing to construct new codes from a given $[n, k, d]_q$ code by deleting the coordinates corresponding to some geometric object in PG$(k-1, q)$ is called geometric puncturing, see

T. Maruta, Construction of optimal linear codes by geometric puncturing, *Serdica J. Computing*, **7**, 73–80, 2013.

Lemma 1. (Maruta-Oya, 2011)
$\mathcal{C}$: $[n,k,d]_q$ code
If $\mathcal{M}_\mathcal{C} \supset \Delta$: a t-flat and $d > q^t$
$\quad\Rightarrow\quad \exists\mathcal{C}'$: $[n-\theta_t, k, d']_q$ code with $d' \geq d - q^t$.

It could happen that the punctured code $\mathcal{C}'$ has the same minimum distance with the original code $\mathcal{C}$, see

I. Bouyukliev, Y. Kageyama, T. Maruta, On the minimum length of linear codes over $\mathbb{F}_5$, *Discrete Math.* **338**, 938–953, 2015.

Lemma 1. (Maruta-Oya, 2011)
$\mathcal{C}$: $[n,k,d]_q$ code
If $\mathcal{M}_{\mathcal{C}} \supset \Delta$: a t-flat and $d > q^t$
$\quad \Rightarrow \quad \exists \mathcal{C}'$: $[n-\theta_t, k, d']_q$ code with $d' \geq d - q^t$.

Lemma 2. (Bouyukliev-Kageyama-M, 2015)
Let $\mathcal{C}$ be an $[n,k,d]_q$ code with $a_{n-d} = 1$ such that $a_i = 0$ for $n-d-q^t < i < n-d$ for some $t \in \mathbb{N}$. Let H be the $(n-d)$-hyperplane. If $\mathcal{M}_{\mathcal{C}}(H)$ contains a t-flat Δ, then $\mathcal{M}_{\mathcal{C}} - \Delta$ gives an $[n-\theta_t, k, d]_q$ code.

Example 2. How to construct a $[20,4,10]_2$ code $\mathcal{C}$

$\mathcal{C}_0$: 2-fold simplex $[30,4,16]_2$ code

$\downarrow$ geometric puncturing

$\mathcal{C}_1$: $[23,4,12]_2$ code

$\downarrow$ geometric puncturing

$\mathcal{C}$: $[20,4,10]_2$ code

$\mathcal{M}_{\mathcal{C}_0} = 2\Sigma \quad (\Sigma = \mathrm{PG}(3,2))$

$\downarrow$ geometric puncturing

$\mathcal{M}_{\mathcal{C}_1} = 2\Sigma - \delta \quad$ (δ: a plane)

$\downarrow$ geometric puncturing

$\mathcal{M}_{\mathcal{C}} = 2\Sigma - (\delta + \ell) \quad$ (ℓ: a line)

Q 2. How many $[20, 4, 10]_2$ codes are there?

We use the package Q-Extension, which can be downloaded from Iilya Bouyukliev's website:

http://www.moi.math.bas.bg/~iliya/

for free, see

I.G. Bouyukliev, What is Q-Extension?, *Serdica J. Computing* **1** (2007) 115–130.

Q 2. How many $[20, 4, 10]_2$ codes are there?

Ans. There are three up to equivalence:

(1) $\mathcal{M}_{\mathcal{C}} = 2\Sigma - (\delta + \ell) \quad (\ell \not\subset \delta)$

w.d. $0^1 10^{11} 12^3 14^1$, spec. $(a_6, a_8, a_{10}) = (1, 3, 11)$

(2) $\mathcal{M}_{\mathcal{C}} = 2\Sigma - (\delta + \ell) \quad (\ell \subset \delta)$

w.d. $0^1 10^{12} 12^2 16^1$, spec. $(a_4, a_8, a_{10}) = (1, 2, 12)$

(3) $\mathcal{M}_{\mathcal{C}} = ?$

w.d. $0^1 10^{10} 12^5$, spec. $(a_8, a_{10}) = (5, 10)$

Q 2. How many $[20,4,10]_2$ codes are there?

Ans. There are three up to equivalence:

(1) $\mathcal{M}_{\mathcal{C}} = 2\Sigma - (\delta + \ell) \quad (\ell \not\subset \delta)$

w.d. $0^1 10^{11} 12^3 14^1$, spec. $(a_6, a_8, a_{10}) = (1,3,11)$

(2) $\mathcal{M}_{\mathcal{C}} = 2\Sigma - (\delta + \ell) \quad (\ell \subset \delta)$

w.d. $0^1 10^{12} 12^2 16^1$, spec. $(a_4, a_8, a_{10}) = (1,2,12)$

(3) $\mathcal{M}_{\mathcal{C}} = ?$

w.d. $0^1 10^{10} 12^5$, spec. $(a_8, a_{10}) = (5,10)$

Q 3. What is $\mathcal{M}_{\mathcal{C}}$ in (3) ? (Hint: there are five 2-pts)

Ans. (3) $\mathcal{C}$: $[20, 4, 10]_2$ code with w.d. $0^1 10^{10} 12^5$.

Q 3. What is $\mathcal{M}_\mathcal{C}$? (Hint: there are five 2-pts)

Ans. Let λ_i be the number of i-points. Then

- $(\lambda_0, \lambda_1, \lambda_2) = (0, 15, 5)$
- $\mathcal{M}_\mathcal{C} - \Sigma$ $(\Sigma = \mathrm{PG}(3, 2))$

  gives an MDS $[20 - \theta_3 = 5, 4, 10 - 2^3 = 2]_2$ code.
- $\mathcal{M}_\mathcal{C} = \Sigma + K$

  where K is a 5-arc in Σ.

An s-set K in $\mathrm{PG}(r, q)$ is an s-arc if no $r + 1$ points of K are on a hyperplane.

Q 2. How many $[20, 4, 10]_2$ codes are there?

Ans. There are three up to equivalence:

(1) $\mathcal{M}_{\mathcal{C}} = 2\Sigma - (\delta + \ell) \quad (\ell \not\subset \delta)$

w.d. $0^1 10^{11} 12^3 14^1$

(2) $\mathcal{M}_{\mathcal{C}} = 2\Sigma - (\delta + \ell) \quad (\ell \subset \delta)$

w.d. $0^1 10^{12} 12^2 16^1$

(3) $\mathcal{M}_{\mathcal{C}} = \Sigma + K \quad (K\text{: 5-arc})$

w.d. $0^1 10^{10} 12^5$

Remark. Helleseth proved that every $[g_2(k,d),k,d]_2$ code with $d \leq 2^{k-1}$ is obtained from an $s\Sigma$ by deleting some flats or adding some arc or a point, where $\Sigma =$ PG$(k-1,2)$, see

T. Helleseth, A characterization of cods meeting the Griesmer bound, *Information and Control* **50** (1981), 128–159.

Q 2. How many $[20,4,10]_2$ codes are there?

Ans. There are three up to equivalence:

(1) $\mathcal{M}_{\mathcal{C}} = 2\Sigma - (\delta + \ell) \quad (\ell \not\subset \delta)$

w.d. $0^1 10^{11} 12^3 14^1$

(2) $\mathcal{M}_{\mathcal{C}} = 2\Sigma - (\delta + \ell) \quad (\ell \subset \delta)$

w.d. $0^1 10^{12} 12^2 16^1$

(3) $\mathcal{M}_{\mathcal{C}} = \Sigma + K \quad (K$: 5-arc)

w.d. $0^1 10^{10} 12^5$

Q 4. When can we find r flats $\Delta_1, ..., \Delta_r$ so that $s\Sigma$ contains $\Delta_1 + \cdots + \Delta_r$?

3. Geometric puncturing from simplex codes

Let $\Sigma = \mathrm{PG}(k-1, q)$, let $r, s \in \mathbb{N}$ and let $u_1, \ldots, u_r$ be integers with $0 \le u_r \le u_{r-1} \le \cdots \le u_1 \le k-2$.

Q 4. When can we find u_i-flats Δ_i $(1 \le i \le r)$ so that $s\Sigma$ contains $\Delta_1 + \cdots + \Delta_r$?

Obvious when $r \le s$.

If at most $q-1$ of $u_1, ..., u_r$ are the same value, then $s\Sigma - (\Delta_1 + \cdots + \Delta_r)$ gives a Griesmer code by Lemma 1.

Assume $r \ge s+1$.

The following result was essentially proved by Belov-Logachev-Sandimirov (1974) for $q = 2$ and by Hill (1992) for any prime power q.

Lemma 3.
There exist u_j-flats Δ_j in Π $(1 \le j \le r)$ s.t. the multiset $s\Sigma$ contains $\Delta_1 + \cdots + \Delta_r$ provided

(a) $\sum_{i=1}^{s+1} u_i \le s(k-1) - 1$, and

(b) # of i's with $u_i = u$ is at most $N_q(k-1-u)$ for any integer u with $0 \le u \le k-2$,

where $N_q(m)$ is the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m.

Proof. For $m \in \mathbb{N}$, $1 \leq m \leq k-1$, let $\mathcal{I}_m$ be the set of irreducible monic polynomials of degree m over $\mathbb{F}_q$. For $f(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + x^m \in \mathcal{I}_m$, let $F(f)$ be the $(k-m-1)$-flat containing the $k-m$ points

$\mathbf{P}(a_0, ..., a_{m-1}, 1, 0, ..., 0)$, $\mathbf{P}(0, a_0, ..., a_{m-1}, 1, 0, ..., 0)$, ...
..., $\mathbf{P}(0, ..., 0, a_0, a_1, ..., a_{m-1}, 1)$.

• $\mathbf{P}(b_0, b_1, ..., b_{k-1})$ in Σ is in $F(f)$ $\Leftrightarrow$ the polynomial $g(x) = b_0 + b_1 x + \cdots + b_{k-1}x^{k-1}$ is divisible by $f(x)$.

From condition (b), one can find r distinct irreducible monic polynomials $f_i \in \mathcal{I}_{k-u_i-1}$ for $1 \leq i \leq r$. Then $\Delta_i := F(f_i)$ is a u_i-flat.

Since the least common multiple of any $s+1$ of the polynomials $f_1, ..., f_r$ has degree at least

$$\sum_{i=1}^{s+1}(k-u_i-1)=(k-1)s-1-\sum_{i=1}^{s+1}u_i+k\geq k$$

by the condition (a), any $s+1$ of $\Delta_1, ..., \Delta_r$ have no common point. Hence, the multiset $s\Sigma$ contains $\Delta_1+\cdots+\Delta_r$. $\square$

Since the least common multiple of any $s+1$ of the polynomials $f_1, ..., f_r$ has degree at least

$$\sum_{i=1}^{s+1} (k - u_i - 1) = (k-1)s - 1 - \sum_{i=1}^{s+1} u_i + k \geq k$$

by the condition (a), any $s+1$ of $\Delta_1, ..., \Delta_r$ have no common point. Hence, the multiset $s\Sigma$ contains $\Delta_1 + \cdots + \Delta_r$. $\square$

Note. $N_q(m) = \dfrac{1}{m} \sum_{e|m} \mu(e)\, q^{m/e}$,

where $\mu(m)$ is the Moebius function defined by

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1, \\ (-1)^w & \text{if } m \text{ is the product of } w \text{ distinct primes,} \\ 0 & \text{if } m \text{ is divisible by the square of a prime.} \end{cases}$$

Let $d \in \mathbb{N}$ to construct an $[n, k, d]_q$ code.
Since s-fold simplex $[g_q(k, sq^{k-1}), k, sq^{k-1}]_q$ codes exist for any $s \in \mathbb{N}$, we assume d is not divisible by q^{k-1}.
Then, d can be uniquely expressed with $s = \lceil d/q^{k-1} \rceil$ as

$$d = sq^{k-1} - \sum_{j=1}^{r} q^{u_j} \tag{1}$$

where r and u_j's are integers satisfying

$$k - 2 \geq u_1 \geq u_2 \geq \cdots \geq u_r \geq 0, \tag{2}$$

$$u_j > u_{j+q-1} \text{ for } 1 \leq j \leq r - q + 1. \tag{3}$$

The condition (3) means that at most $q-1$ of $u_1, \ldots, u_r$ can take any given value.

To construct a code of length $n = s\theta_{k-1} - \sum_{i=0}^{k-2} u_i\theta_i$, we shall make a multiset $s\Sigma - (\Delta_1 + \cdots + \Delta_r)$ with some u_j-flats Δ_j $(1 \le j \le r)$ if possible. Then, by Lemma 1, the multiset gives a $[g_q(k,d), k, d]_q$ code.

Q 5. When is it possible?

Ans. (1) $r \le s$.
(2) $r \ge s+1$ and $\sum_{i=1}^{s+1} u_i \le s(k-1) - 1$ by Lemma 3 since $N_q(m) \ge q-1$.

Note. The Griesmer codes constructed in this way are called the Griesmer codes of Belov type.

Lemma 3.
There exist u_j-flats Δ_j in Π $(1 \le j \le r)$ s.t. the multiset $s\Sigma$ contains $\Delta_1 + \cdots + \Delta_r$ provided

(a) $\sum_{i=1}^{s+1} u_i \le s(k-1) - 1$, and

(b) # of i's with $u_i = u$ is at most $N_q(k-1-u)$ for any integer u with $0 \le u \le k-2$,

where $N_q(m)$ is the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m.

To construct a code of length $n = s\theta_{k-1} - \sum_{i=0}^{k-2} u_i\theta_i$, we shall make a multiset $s\Sigma - (\Delta_1 + \cdots + \Delta_r)$ with some u_j-flats Δ_j $(1 \leq j \leq r)$ if possible. Then, by Lemma 1, the multiset gives a $[g_q(k,d), k, d]_q$ code.

Q 5. When is it possible?

Ans. (1) $r \leq s$.
(2) $r \geq s+1$ and $\sum\limits_{i=1}^{s+1} u_i \leq s(k-1) - 1$ by Lemma 3 since $N_q(m) \geq q-1$.

Note. The Griesmer codes constructed in this way are called the Griesmer codes of Belov type.

To construct a code of length $n = s\theta_{k-1} - \sum_{i=0}^{k-2} u_i\theta_i$, we shall make a multiset $s\Sigma - (\Delta_1 + \cdots + \Delta_r)$ with some u_j-flats Δ_j $(1 \le j \le r)$ if possible. Then, by Lemma 1, the multiset gives a $[g_q(k,d), k, d]_q$ code.

Q 5. When is it possible?

Ans. (1) $r \le s$.

(2) $r \ge s+1$ and $\sum_{i=1}^{s+1} u_i \le s(k-1) - 1$ by Lemma 3 since $N_q(m) \ge q-1$.

Note. The above is impossible if $r \ge s+1$ and $\sum_{i=1}^{s+1} u_i \ge s(k-1)$, see [Hill, 1992].

To construct a code of length $n = s\theta_{k-1} - \sum_{i=0}^{k-2} u_i\theta_i$, we shall make a multiset $s\Sigma - (\Delta_1 + \cdots + \Delta_r)$ with some u_j-flats Δ_j $(1 \le j \le r)$ if possible. Then, by Lemma 1, the multiset gives a $[g_q(k,d),k,d]_q$ code.

Q 5. When is it possible?

Ans. (1) $r \le s$.
(2) $r \ge s+1$ and $\sum_{i=1}^{s+1} u_i \le s(k-1) - 1$ by Lemma 3 since $N_q(m) \ge q-1$.

Q 6. What can we do when

$$r \ge s+1 \text{ and } \sum_{i=1}^{s+1} u_i \ge s(k-1)?$$

Thm 4. Let $w = s + 1$ and assume $\sum_{i=1}^{w} u_i = s(k-1) - 1 + t$ with an integer t, $1 \le t \le q-1$. Then, there exists a $[g_q(k,d) + t, k, d]_q$ code if one of the following conditions holds:

(a) $u_{w-t+1} = \cdots = u_w > u_{w+1}$ and

$N_q(k-m) \ge tq + d_{m-1}$;

(b) $u_{w-t+1} = \cdots = u_w$, $r = w$ and $N_q(k-m) \ge tq$;

(c) $u_i = u_{i+1} = \cdots = u_{i+t-1} = u_w + 1$ for some i and

$N_q(k-m-1) \ge tq + d_m$.

Example 3.

It is known that $n_3(6,189) = g_3(6,189) + 2$.

For $q = 3$, $k = 6$ and $d = 189$, we have

$d = 3^5 - 2 \cdot 3^3$, $s = 1$, $u_1 + u_2 = s(k-1) - 1 + 2$.

d can be also expressed as

$d = 3^5 - 6 \cdot 3^2$ with $s = 1$, $u'_1 + u'_2 = s(k-1) - 1$.

Since $N_3(3) = 8$, one can find planes $\delta_1, ..., \delta_6$ so that $\Sigma = \mathrm{PG}(5,3)$ contains $\delta_1 + \cdots + \delta_6$, where $\delta_1, \ldots, \delta_6$ are planes corresponding to six monic irreducible polynomials of degree 3 over $\mathbb{F}_3$. Then, the multiset $\Sigma - (\delta_1 + \cdots + \delta_6)$ gives a $[g_3(6,189)+2, 6, 189]_3$ code.

Thm 4. Let $w = s + 1$ and assume $\sum_{i=1}^{w} u_i = s(k-1)-1+t$ with an integer t, $1 \le t \le q-1$. Then, there exists a $[g_q(k,d)+t,k,d]_q$ code if one of the following conditions holds:

(a) $u_{w-t+1} = \cdots = u_w > u_{w+1}$ and

$$N_q(k-m) \ge tq + d_{m-1};$$

(b) $u_{w-t+1} = \cdots = u_w$, $r = w$ and $N_q(k-m) \ge tq$;

(c) $u_i = u_{i+1} = \cdots = u_{i+t-1} = u_w + 1$ for some i and

$$N_q(k-m-1) \ge tq + d_m.$$

Especially when $t = 1$, we get the following.

Assume $r \geq s+1$ and $u = \sum_{i=1}^{s+1} u_i \ = s(k-1)$.

Thm 5. (Kageyama-M)

(1) For $q = 2$, ${}^{\exists}[g_2(k,d)+1, k, d]_2$ code.

(2) ${}^{\exists}[g_q(k,d)+1, k, d]_q$ code if $1 \leq s \leq k-3$, $q \geq 3$ and if one of the following conditions holds:

(a) $u_{s+1} > u_{s+2}$ if $r > s+1$;

(b) $r = s+1$;

(c) $u_\varepsilon = u_{s+1} + 1$ for some integer ε.

(3) ${}^{\exists}[g_q(k,d)+1, k, d]_q$ code for $(k-2)q^{k-1} - kq^{k-2} + 1 \leq d \leq (k-2)q^{k-1} - (k-1)q^{k-2}$ for $q \geq k \geq 3$.

Thm 5 (2) yields the following.

Corollary 6. $\exists\ [g_q(k,d)+1,k,d]_q$ code for

(a) $sq^{k-1}-sq^{k-2}-2q^s+1 \le d \le sq^{k-1}-sq^{k-2}-q^s$
for $1 \le s \le k-3$, $q \ge s+1$, $k \ge 4$;

(b) $(k-3)q^{k-1}-(k-2)q^{k-2}+1 \le d \le (k-3)q^{k-1}$
$-(k-3)q^{k-2}-2q^{k-3}$ for $q \ge k-2 \ge 3$;

(c) $q^{k-1}-2q^{k/2}+1 \le d \le q^{k-1}-q^{k/2}-q^{k/2-1}$
for all q if k is even;

(d) $q^{k-1}-3q^{(k-1)/2}+1 \le d \le q^{k-1}-2q^{(k-1)/2}$
for $q \ge 3$ if k is odd.

Thm 7. (Klein-Metsch, 2007)

Let $d = sq^{k-1} - \sum_{i=1}^{k-1} t_i q^{k-1-i}$ with $0 \leq t_i < q$.

Assume $t_1 > 0$, $t_2 = 0$ and $\sum_{i=3}^{k-1} t_i q^{k-1-i} \leq rq^{k-4}$. Then

$n_q(k,d) \geq g_q(k,d) + 1$ if the following conditions hold:

(a) $s < \min\{t_1, k-1\}$.

(b) $t_1 \leq (q+1)/2$.

(c) $t_1 + r \leq q$ and r is a non-negative integer.

Thm 7. (Klein-Metsch, 2007)
Let $d = sq^{k-1} - \sum_{i=1}^{k-1} t_i q^{k-1-i}$ with $0 \leq t_i < q$.
Assume $t_1 > 0$, $t_2 = 0$ and $\sum_{i=3}^{k-1} t_i q^{k-1-i} \leq rq^{k-4}$. Then $n_q(k,d) \geq g_q(k,d) + 1$ if the following conditions hold:

(a) $s < \min\{t_1, k-1\}$.
(b) $t_1 \leq (q+1)/2$.
(c) $t_1 + r \leq q$ and r is a non-negative integer.

Ex. $d = (k-2)q^{k-1} - (k-1)q^{k-2} - \sum_{j=0}^{k-4} d_j q^j$, $q \geq 2k-3$, $k \geq 4$, $0 \leq d_{k-4} \leq k-3$, $0 \leq d_j \leq q-1$ for $j \leq k-5$.

Thm 7. (Klein-Metsch, 2007)

Let $d = sq^{k-1} - \sum_{i=1}^{k-1} t_i q^{k-1-i}$ with $0 \le t_i < q$.

Assume $t_1 > 0$, $t_2 = 0$ and $\sum_{i=3}^{k-1} t_i q^{k-1-i} \le rq^{k-4}$. Then $n_q(k,d) \ge g_q(k,d) + 1$ if the following conditions hold:

(a) $s < \min\{t_1, k-1\}$. $s = k-2,\ t_1 = k-1$

(b) $t_1 \le (q+1)/2$. $\Leftrightarrow q \ge 2k-3$

(c) $t_1 + r \le q$ and r is a non-negative integer. $r = k-2$

Ex. $d = (k-2)q^{k-1} - (k-1)q^{k-2} - \sum_{j=0}^{k-4} d_j q^j$, $q \ge 2k-3$, $k \ge 4$, $0 \le d_{k-4} \le k-3$, $0 \le d_j \le q-1$ for $j \le k-5$.

♣ $n_q(k,d) = g_q(k,d)$ for $d > (k-2)q^{k-1} - (k-1)q^{k-2}$.

$n_q(k,d) > g_q(k,d)$ for

- $d = (k-2)q^{k-1} - (k-1)q^{k-2} (:= d_1)$ for $q \geq k$, $k = 3,4,5$; for $q \geq 2k-3$, $k \geq 6$ (M, 1997).
- $d_1 - (k-2)q^{k-4} + 1 \leq d \leq d_1$ for $q \geq 2k-3$, $k \geq 4$ (Klein-Metsch, 2007).

Thms 5 and 7 determine $n_q(k,d)$:

Corollary 8. $n_q(k,d) = g_q(k,d) + 1$ for $d_1 - (k-2)q^{k-4} + 1 \leq d \leq d_1$ if $q \geq 2k-3$ and $k \geq 5$.

Example 4. For the case when $q = 5$ and $k = 5$, $[g_5(5, d) + 1, 5, d]_5$ codes exist for $d =$ 491-495, 551-575, 876-975, 1251-1375 by Thm 5 and Cor 6, at least 57 of which are optimal.

Example 4. For the case when $q = 5$ and $k = 5$, $[g_5(5,d)+1,5,d]_5$ codes exist for $d =$ 491-495, 551-575, 876-975, 1251-1375 by Thm 5 and Cor 6, at least 57 of which are optimal.

Q 7. Find $n_q(5,d)$ for $q \geq 5$ for
(1) $q^4 - q^3 - q^2 + 1 \leq d \leq q^4 - q^3 - q$,
(2) $2q^4 + 1 \leq d \leq 2q^4 + q^2 - q$,
(3) $q^4 - q^3 - 2q^2 + 1 \leq d \leq q^4 - q^3 - q^2$.

Note that $\sum_{i=1}^{s+1} u_i \geq s(k-1)$ for the above d.

4. Construction of q-divisible codes

An $[n, k, d]_q$ code is called m-divisible if all codewords have weights divisible by an integer $m > 1$.

Thm 9. (Ward, 1998)
Let $\mathcal{C}$ be a Griesmer $[n, k, d]_p$ code with p prime.
If p^e divides d, then $\mathcal{C}$ is p^e-divisible.

Lemma 10. $\mathcal{C}$: m-divisible $[n,k,d]_q$ code, $q=p^h$, p prime, $m=p^r$, $1 \le r < h(k-2)$, $\lambda_0 > 0$, with spec.

$$a_{n-d-im} = \alpha_i \text{ for } 0 \le i \le w-1.$$

$\Rightarrow \exists \mathcal{C}^*$: t-divisible $[n^*,k,d^*]_q$ code with $t = q^{k-2}/m$, $n^* = ntq - \frac{d}{m}\theta_{k-1}$, $d^* = ((n-d)q-n)t$, whose spectrum is

$$a_{n^*-d^*-it} = \lambda_i \text{ for } 0 \le i \le \gamma_0$$

where $\lambda_i = |C_i|$ (# of i-points for $\mathcal{C}$).

$\mathcal{C}^*$ is called a projective dual (p.d.) of $\mathcal{C}$, see

A.E. Brouwer, M. van Eupen, The correspondence between projective codes and 2-weight codes, *Des. Codes Cryptogr.* **11** (1997) 261–266.

The multiset $\mathcal{M}_{\mathcal{C}^*}$ is given by considering the hyperplanes H with $m_{\mathcal{C}}(H) = n - d - jm$ as j-points in the dual space Σ^* of Σ for $0 \leq j \leq w-1$.

Example 5.

$\mathcal{C}_1$: 3-div $[19, 6, 9]_3$

with spec. $(a_1, a_4, a_7, a_{10}) = (6, 114, 201, 43)$

$\downarrow$ projective dual

$\mathcal{C}_1^*$: 27-div $[447, 6, 297]_3$ $(n^* = 3a_1 + 2a_4 + a_7)$

with spec. $(a^*_{123}, a^*_{150}) = (19, 345)$

$\mathbf{P}(a_0, a_1, ..., a_5) \in \mathrm{PG}(5,3)$ is a j-point for $\mathcal{C}_1^*$ if

$$wt((a_0, ..., a_5)G_0) = 3j + 9.$$

Q 7. Find $n_q(5, d)$ for $q \geq 5$ for

(1) $q^4 - q^3 - q^2 + 1 \leq d \leq q^4 - q^3 - q$,

(2) $2q^4 + 1 \leq d \leq 2q^4 + q^2 - q$,

(3) $q^4 - q^3 - 2q^2 + 1 \leq d \leq q^4 - q^3 - q^2$.

Lemma 11. $\exists$ q-div. $[q^2+q, 5, q^2-q]_q$ code with spec.
$(a_0, a_q, a_{2q}) = (\frac{q^2-q}{2},\ q^4 - q^2 + q + 1,\ \frac{2q^3+3q^2+q}{2})$.

Lemma 12. $\exists$ q-div. $[q^2, 5, q^2 - 3q]_q$ code with spec.

$$(a_0, a_q, a_{2q}, a_{3q}) = (\tfrac{q}{6}(q-1)(2q+5)+1,\\ q^4 + \tfrac{q^3-q^2}{2} + 3q,\ 3\tbinom{q}{2},\ \tbinom{q}{3}).$$

K: an s-arc in PG(r, q) if

- K is a set of s points in PG(r, q).
- no $r+1$ points of K are on a hyperplane.

When $q \geq r$, there exists a $(q+1)$-arc.

Lemma 11. There exists a q-divisible $[q^2+q, 5, q^2-q]_q$ code $\mathcal{C}_2$ with spectrum $(a_0, a_q, a_{2q}) = (\frac{q^2-q}{2}, q^4 - q^2 + q + 1, \frac{2q^3+3q^2+q}{2})$.

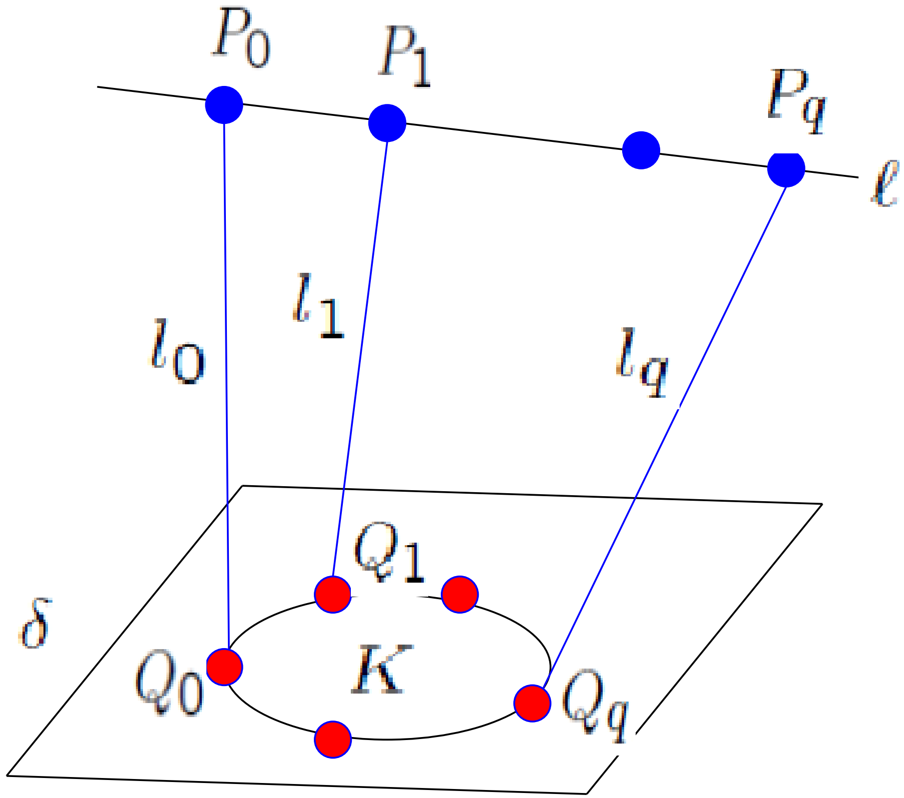
Construction

ℓ: line, δ: plane with $\ell \cap \delta = \emptyset$ in $\Sigma = \mathrm{PG}(4, q)$

$K = \{Q_0, Q_1, \ldots, Q_q\}$: a $(q+1)$-arc in δ

$\ell = \{P_0, P_1, \ldots, P_q\}$, $l_i = \langle P_i, Q_i \rangle$.

Setting $C_1 = (\cup_{i=0}^{q} l_i) \setminus \ell$ and $C_0 = \Sigma \setminus C_1$, we get a q-divisible $[q^2 + q, 5, q^2 - q]_q$ code $\mathcal{C}_2$.



$\Sigma = \mathrm{PG}(4, q)$

$\ell \cap \delta = \emptyset$

K: a $(q+1)$-arc in δ

$l_i = \langle P_i, Q_i \rangle$

$C_1 = (\bigcup_{i=0}^{q} l_i) \setminus \ell$

$C_0 = \Sigma \setminus C_1$

$\Rightarrow$ $\mathcal{C}_2$ is a q-divisible $[q^2+q, 5, q^2-q]_q$ code.

Lemma 12. There exists a q-divisible $[q^2, 5, q^2 - 3q]_q$ code $\mathcal{C}_3$ with spectrum

$$(a_0, a_q, a_{2q}, a_{3q}) = \left(\tfrac{q}{6}(q-1)(2q+5)+1,\; q^4 + \tfrac{q^3-q^2}{2} + 3q,\; 3\tbinom{q}{2},\; \tbinom{q}{3}\right).$$

Construction

H: hyperplane of $\Sigma = \mathrm{PG}(4, q)$

P: point $\notin H$

$K = \{Q_1, \ldots, Q_q\}$: a q-arc in H

$l_i = \langle P, Q_i \rangle$.

Setting $C_1 = (\cup_{i=1}^{q} l_i) \setminus P$ and $C_0 = \Sigma \setminus C_1$, we get a q-divisible $[q^2, 5, q^2 - 3q]_q$ code $\mathcal{C}_3$.

H: a hyperplane of $\Sigma = \mathrm{PG}(4, q)$

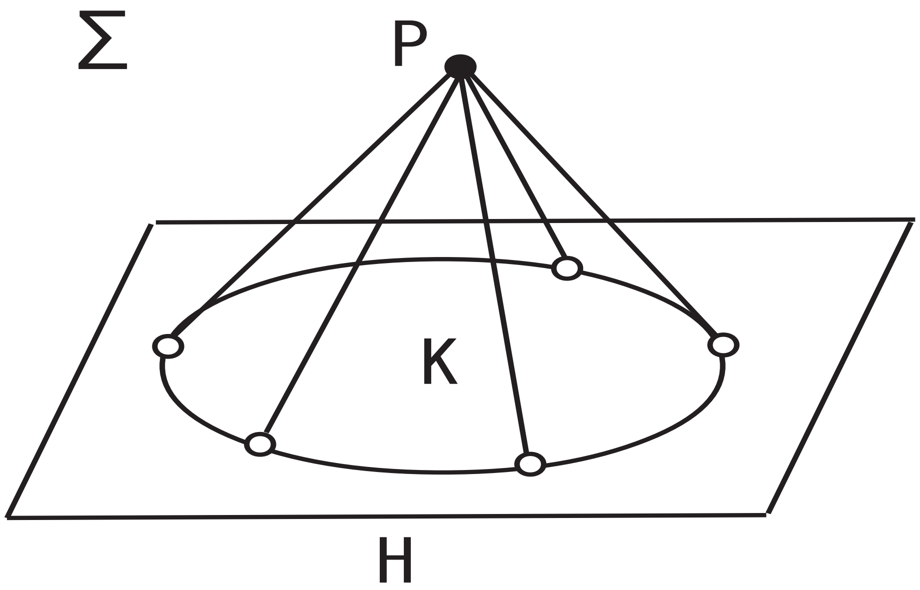
K: q-arc in H

P: a point of Σ out of H

$l_1, \cdots, l_q$: lines through P s.t. $\cup_{i=1}^{q}(l_i \cap H) = K$

$C_1 = (\cup_{i=1}^{q} l_i) \setminus P$, $C_0 = \Sigma \setminus C_1$

$\Rightarrow$ $\mathcal{C}_3$ is a q-divisible $[q^2, 5, q^2 - 3q]_q$ code.



Lemma 11. $\exists \mathcal{C}_2$: q-div. $[q^2+q, 5, q^2-q]_q$ code with $(a_0, a_q, a_{2q}) = (\frac{q^2-q}{2},\ q^4-q^2+q+1,\ \frac{2q^3+3q^2+q}{2})$.

Lemma 12. $\exists \mathcal{C}_3$: q-div. $[q^2, 5, q^2-3q]_q$ code with $(a_0, a_q, a_{2q}, a_{3q}) = (\frac{q}{6}(q-1)(2q+5)+1,$

$$q^4 + \frac{q^3-q^2}{2} + 3q,\ 3\binom{q}{2},\ \binom{q}{3}).$$

K: an s-arc in PG(r,q) if

- K is a set of s points in PG(r,q).
- no $r+1$ points of K are on a hyperplane.

When $q \geq r$, there exists a $(q+1)$-arc.

Thm 13.

$\mathcal{C}_2$: q-divisible $[q^2+q, 5, q^2-q]_q$ code

$\downarrow$ projective dual

$\mathcal{C}_2^*$: q^2-divisible $[q^4+1, 5, q^4-q^3]_q$ code

$\downarrow$ geometric puncturing

$[q^4+1-t(q+1), 5, q^4-q^3-tq]_q$ code for $1 \le t \le q-1$

- $n^* = q^4+1 = g_q(5, q^4-q^3)+1$.
- $\mathcal{C}_2^*$ is not optimal, for $\exists [g_q(5,d), 5, d]_q$ if $d = q^4-q^3$.
- The resulting codes are optimal, giving

$n_q(5,d) = g_q(5,d)+1$ for $q^4-q^3-q^2+1 \le d \le q^4-q^3-q$.

Lemma 11. $\exists\mathcal{C}_2$: q-div. $[q^2+q,5,q^2-q]_q$ code with $(a_0,a_q,a_{2q}) = (\frac{q^2-q}{2},\ q^4-q^2+q+1,\ \frac{2q^3+3q^2+q}{2})$.

Lemma 12. $\exists\mathcal{C}_3$: q-div. $[q^2,5,q^2-3q]_q$ code with $(a_0,a_q,a_{2q},a_{3q}) = (\frac{q}{6}(q-1)(2q+5)+1,$

$$q^4+\frac{q^3-q^2}{2}+3q,\ 3\binom{q}{2},\ \binom{q}{3}).$$

K: an s-arc in $\mathrm{PG}(r,q)$ if

- K is a set of s points in $\mathrm{PG}(r,q)$.
- no $r+1$ points of K are on a hyperplane.

When $q \geq r$, there exists a $(q+1)$-arc.

$\mathcal{C}_3$: q-divisible $[q^2, 5, q^2 - 3q]_q$ code

$\downarrow$ projective dual

$\mathcal{C}_3^*$: q^2-divisible $[2\theta_4 + 1, 5, 2q^4]_q$ code

with weights $2q^4$ and $2q^4 + q^2$.

Lemma 14. (Hill-Newton, 1992)
$\mathcal{C}$: $[n, k, d]_q$ code
$\mathcal{C}_0$: $[n_0, k-1, d_0]_q$ code

If $\exists c \in \mathcal{C}$ with $wt(c) \geq d + d_0$

$\Rightarrow \exists \mathcal{C}'$: $[n + n_0, k, d + d_0]_q$ code

• We apply Lemma 14 to
$\mathcal{C}$: $[2\theta_4 + 1, 5, 2q^4]_q$ code, $wt(c) = 2q^4 + q^2$
$\mathcal{C}_0$: $[q^2 + 1, 4, q^2 - q]_q$ code.

$\Rightarrow \exists \mathcal{C}'$: $[2\theta_4^4 + q^2 + 2, 5, 2q^4 + q^2 - q]_q$ code

Thm 15.

$\mathcal{C}_3$: q-divisible $[q^2, 5, q^2-3q]_q$ code

$\downarrow$ projective dual

$\mathcal{C}_3^*$: q^2-divisible $[2\theta_4+1, 5, 2q^4]_q$ code

$\downarrow$ Lemma 14 with $[q^2+1, 4, q^2-q]_q$

$[2\theta_4^4+q^2+2, 5, 2q^4+q^2-q]_q$ code

$\downarrow$ geometric puncturing

$[2\theta_4^4+q^2+2-u\theta_1, 5, 2q^4+q^2-(u+1)q]_q$ code

for $0 \le u \le q-2$

- $n^* = 2\theta^4 = g_q(5, 2q^4)+1$.
- $\mathcal{C}_3^*$ is not optimal, for $\exists [g_q(5,d), 5, d]_q$ if $d = 2q^4$.

Thm 15.

$\mathcal{C}_3$: q-divisible $[q^2, 5, q^2 - 3q]_q$ code

$\downarrow$ projective dual

$\mathcal{C}_3^*$: q^2-divisible $[2\theta_4 + 1, 5, 2q^4]_q$ code

$\downarrow$ Lemma 14 with $[q^2 + 1, 4, q^2 - q]_q$

$[2\theta_4^4 + q^2 + 2, 5, 2q^4 + q^2 - q]_q$ code

$\downarrow$ geometric puncturing

$[2\theta_4^4 + q^2 + 2 - u\theta_1, 5, 2q^4 + q^2 - (u + 1)q]_q$ code

for $0 \le u \le q - 2$

- The resulting codes are Griesmer, giving

$n_q(5, d) = g_q(5, d)$ for $2q^4 + 1 \le d \le 2q^4 + q^2 - q$.

5. Open problems

Q 7. Find $n_q(5,d)$ for $q \geq 5$ for
(1) $q^4 - q^3 - q^2 + 1 \leq d \leq q^4 - q^3 - q$,
(2) $2q^4 + 1 \leq d \leq 2q^4 + q^2 - q$,
(3) $q^4 - q^3 - 2q^2 + 1 \leq d \leq q^4 - q^3 - q^2$.

Note that $\sum_{i=1}^{s+1} u_i \geq s(k-1)$ for the above d.

We have solved the above question for (1) and (2).

But it is still open for (3)!

Problem 2. $\exists$ q-div. $[(q+1)^2, 5, q^2]_q$ code?

$\mathcal{C}$: q-divisible $[(q+1)^2, 5, q^2]_q$ code

$\downarrow$ projective dual

$\mathcal{C}^*$: q^2-divisible $[q^4 - q^2 - q, 5, q^4 - q^3 - q^2]_q$ code.

$n^* = q^4 - q^2 - q = g_q(5, q^4 - q^3 - q^2) + 1.$

$\mathcal{C}^*$ is optimal, for $\nexists [g_q(5,d), 5, d]_q$ if $d = q^4 - q^3 - q^2$.

If $\mathcal{C}$ is projective, then the spectrum is

$(a_1, a_{q+1}, a_{2q+1}) = (\binom{q+1}{2}, q^4 - 2q^2 - 2q, q^3 + 5\binom{q+1}{2} + 1).$

- A $[9, 5, 4]_2$ code does not exist.
- A q-div. $[(q+1)^2, 5, q^2]_q$ code exists for $q = 3, 4, 5$.
- For $q = 4$, there are 31 such codes, two of which are non-projective: $(a_1, a_5, a_9; \lambda_2) = (14, 208, 119; 1)$

Conjecture. $n_q(k,d) \le g_q(k,d) + k - 2$ for $k \ge 3$.

Problem 3. Construct $[g_q(k,d) + k - 2, k, d]_q$ codes for all q, d and $k \ge 3$.

For $k = 3$, the conjecture is valid for all $q \le 19$, see Simeon Ball's website:

S. Ball, Table of bounds on three dimensional linear codes or (n,r)-arcs in PG$(2,q)$,
http://www-ma4.upc.es/~simeon/codebounds.html

Conjecture. $n_q(k,d) \le g_q(k,d) + k - 2$ for $k \ge 3$.

Problem 3. Construct $[g_q(k,d) + k - 2, k, d]_q$ codes for all q, d and $k \ge 3$.

For $k = 3$, the conjecture is valid for all $q \le 19$, see Simeon Ball's website:

S. Ball, Table of bounds on three dimensional linear codes or (n, r)-arcs in PG$(2, q)$, http://www-ma4.upc.es/~simeon/codebounds.html

Thank you for your attention!

References

[1] R. Hill, Optimal linear codes, in: Mitchell C. (ed.) Cryptography and Coding II, pp. 75–104. Oxford Univ. Press, Oxford (1992).

[2] Y. Kageyama, T. Maruta, On the construction of Griesmer codes of dimension 5, *Des. Codes, Cryptogr.*, **75** (2015) 277–280.

[3] Y. Kageyama, T. Maruta, On the geometric constructions of optimal linear codes, submitted.

[4] T. Maruta, Construction of optimal linear codes by geometric puncturing, *Serdica J. Computing* **7** (2013) 73–80.

[5] T. Maruta and Y. Oya, On the minimum length of ternary linear codes, *Des. Codes, Cryptogr.* **68** (2013) 07–425.