# On the construction of optimal codes over $\mathbb{F}_q$

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 $[g_q(k,d)+1,k,d]_q$ codes for some $q,k,d$, through projective geometry over finite fields, where $g_q(k,d)=\sum_{i=0}^{k-1}\left\lceil d/q^i\right\rceil$. to determine $n_q(k,d)$, the minimum value of $n$ for which an $[n,k,d]_q$ code exists.

## Contents

## 1. Main results

$\mathbb{F}_q^n = \{(a_1, a_2, ..., a_n) \mid a_1, ..., a_n \in \mathbb{F}_q\}$.
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.

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

small $n$ for fast transmission of messages,

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

large $d$ to correct many errors.

**Optimal linear codes problem.**

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

## Optimal linear codes problem.

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

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

See

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

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

## 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.

**Thm A.** (Maruta-Landjev-Rousseva, 2005)
$n_q(k,d) \geq g_q(k,d) + 1$ for $k \geq 5$, $q \geq 3$
for $q^{k-1} - q^{k-2} - q^2 + 1 \leq d \leq q^{k-1} - q^{k-2} - q$.

**Note.** $n_q(k,d) = g_q(k,d) + 1$ for $k \geq 5$, $q \geq 3$ for $q^{k-1} - q^{k-2} - 2q + 1 \leq d \leq q^{k-1} - q^{k-2} - q$.

**Problem 2.** Does a $[g_q(k,d) + 1, k, d]_q$ code exist for $q^{k-1} - q^{k-2} - q^2 + 1 \leq d \leq q^{k-1} - q^{k-2} - 2q$ for $k \geq 5$?

**Thm A.** (Maruta-Landjev-Rousseva, 2005)
$n_q(k,d) \geq g_q(k,d)+1$ for $k \geq 5$, $q \geq 3$
for $q^{k-1}-q^{k-2}-q^2+1 \leq d \leq q^{k-1}-q^{k-2}-q$.

**Note.** $n_q(k,d) = g_q(k,d)+1$ for $k \geq 5$, $q \geq 3$ for $q^{k-1}-q^{k-2}-2q+1 \leq d \leq q^{k-1}-q^{k-2}-q$.

**Problem 2.** Does a $[g_q(k,d)+1,k,d]_q$ code exist for $q^{k-1}-q^{k-2}-q^2+1 \leq d \leq q^{k-1}-q^{k-2}-2q$ for $k \geq 5$?

**Answer.** Yes for $k=5$. (Thm 1)

**Thm B.** (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 B.** (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) $s < \min\{t_1, k-1\}$.

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

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

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

**Thm B.** (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 $\sum_{i=3}^{k-1} t_i q^{k-1-i} \le r q^{k-4}$. 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.** $d = (k-2)q^{k-1} - (k-1)q^{k-2} - \sum_{j=0}^{k-4} u_j q^j$, $q \ge 2k-3$, $k \ge 4$, $0 \le u_{k-4} \le k-3$, $0 \le u_j \le q-1$ 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).
- $d_1 - q^{k-4} \leq d \leq d_1$ for $q \geq 2k-3$, $k \geq 4$ (Klein, 2004).
- $d_1 - (k-2)q^{k-4} + 1 \leq d \leq d_1$ for $q \geq 2k-3$, $k \geq 4$ (Klein-Metsch, 2007).

To show $n_q(k,d) = g_q(k,d) + 1$ for the above values of $d$, we construct $[g_q(k,d)+1, k, d]_q$ codes.

**Lemma 2.** $n_q(k,d) \geq g_q(k,d)+1$ if $q \geq 2k-3$, $k \geq 4$ for $d_1-(k-2)q^{k-4}+1 \leq d \leq d_1$.

**Lemma 3.** There exists a $[g_q(k,d)+1,k,d]_q$ code with $q \geq k \geq 5$ for $d_1-(q-k+1)q^{k-3}+1 \leq d \leq d_1$.

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

**Lemma 3'.** There exists a $[g_q(k,d)+1,k,d]_q$ code with $q \geq k \geq 5$ for $d = d_1 - \sum_{i=1}^{k-3} t_i q^i$ with $0 \leq t_{k-3} \leq q-k$ and $0 \leq t_j \leq q-1$ for $1 \leq j \leq k-4$.

## 2. Gometric method

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

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

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

$\mathcal{C}$: an $[n,k,d]_q$ code with $B_1 = 0$
i.e. with 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 $\mathcal{M}_{\mathcal{C}}$.

$\mathcal{F}_j :=$ the set of $j$-flats of $\Sigma$

$\Sigma \ni P$: $i$-point $\quad\Leftrightarrow\quad$ $P$ 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

$$\Delta_1, \cdots, \Delta_s \text{ in } \Sigma.$$

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

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

For any set $S$ in $\Sigma$, $\mathcal{M}_{\mathcal{C}}(S)$ 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 $\Sigma$ satisfying the above equalities gives an $[n, k, d]_q$ code in the natural manner.

A line $l$ is called an $i$-line if $m_{\mathcal{C}}(l) = i$.
An $i$-plane, an $i$-hp and so on are defined similarly.

$a_i = |\{H \in \mathcal{F}_{k-2} \mid m_{\mathcal{C}}(H) = i\}| = \#$ of $i$-hps

List of $a_i$'s: the spectrum of $\mathcal{C}$

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

**Lemma 4.** $\mathcal{C}$: $m$-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 $t = q^{k-2}/m$, $n^* = \sum_{j=0}^{w-1} j\alpha_j = ntq - \frac{d}{m}\theta_{k-1}$, $d^* = ((n-d)q-n)t$, 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 the projective dual (PD) 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.

**Lemma 5.** (Maruta-Oya, 2011)
$\mathcal{C}$: $[n, k, d]_q$ code
$\cup_{i=0}^{\gamma_0} C_i$: the partition of $\Sigma$ obtained from $\mathcal{C}$.
If $\cup_{i \geq 1} C_i \supset \Delta$: $t$-flat and $d > q^t$

$\Rightarrow \quad \exists \mathcal{C}'$: $[n - \theta_t, k, d']_q$ code with $d' \geq d - q^t$.

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

**Lemma 5.** (Maruta-Oya, 2011)
$\mathcal{C}$: $[n, k, d]_q$ code
$\cup_{i=0}^{\gamma_0} C_i$: the partition of $\Sigma$ obtained from $\mathcal{C}$.
If $\cup_{i \geq 1} C_i \supset \Delta$: $t$-flat and $d > q^t$
$\Rightarrow$ $\exists \mathcal{C}'$: $[n - \theta_t, k, d']_q$ 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 5 can be generalized as follows.

**Lemma 6**.
$\mathcal{C}$: $[n,k,d]_q$ code, $\Sigma = \mathrm{PG}(k-1,q)$, $0 \le t \le k-2$
$\cup_{i=0}^{\gamma_0} C_i$: the partition of $\Sigma$ obtained from $\mathcal{C}$.
If $\cup_{i\ge 1} C_i \supset \mathcal{F}$: $\{f, m; k-1, q\}$-minihyper
s.t. $(C_1 \setminus \mathcal{F}) \cup (\cup_{i\ge 2} C_i)$ spans $\Sigma$
$\Rightarrow$ $\exists \mathcal{C}'$: $[n-f, k, d+m-f]_q$ code

An $f$-set $F$ in $\mathrm{PG}(r,q)$ is an $\{f, m; r, q\}$-minihyper if

$$m = \min\{|F \cap \pi| \mid \pi \in \mathcal{F}_{r-1}\}.$$

Ex. A $j$-flat is a $\{\theta_j, \theta_{j-1}; r, q\}$-minihyper.
A blocking $b$-set in some plane is a $\{b, 1; r, q\}$-minihyper.

**Lemma 7.**
$\mathcal{C}$: $s$-fold simplex $[s\theta_{k-1}, k, sq^{k-1}]_q$ code, $s \geq 1$,
i.e., $C_s = \Sigma = \mathrm{PG}(k-1, q)$.
If there exist $F_1, ..., F_t$ ($F_j \in \mathcal{F}_{m_j}$, $0 \leq m_j \leq k-2$) s.t.

- $m_1 \geq \cdots \geq m_t$ with $m_{i+q-1} < m_i$ for any $i$
- $\bigcap_{i \in I} F_i = \emptyset$ for any $(s+1)$-set $I \subset \{1, \cdots, t\}$

$\Rightarrow$ $\mathcal{M}_{\mathcal{C}} - (F_1 + \cdots + F_t)$ generates a $[g_q(k,d), k, d]_q$ code with $d = sq^{k-1} - \sum_{i=1}^{t} q^{m_i}$.

The Griesmer codes constructed in this way is said to be of Belov type.
For the existence of Griesmer codes of Belov type, the following is known.

**Thm 8.** $\exists \mathcal{C}$: $[g_q(k,d),k,d]_q$ code of Belov type iff

$$d = sq^{k-1} - \sum_{i=1}^{t} q^{u_i-1}, \qquad \sum_{i=1}^{\min\{s+1,t\}} u_i \le sk,$$

where $s = \left\lceil d/q^{k-1} \right\rceil$, $k > u_1 \ge u_2 \ge \cdots \ge u_t \ge 1$ with $u_i > u_{i+q-1}$ for $1 \le i \le t-q+1$.

Thm 8 was first proved by Belov, Logachev, Sandimirov (1974) for binary codes, and generalized to non-binary codes by Dodunekov (1985) and Hill (1992). For $q = 2$, see

F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.

**Thm 8.** $\exists \mathcal{C}$: $[g_q(k,d),k,d]_q$ code of Belov type iff

$$d = sq^{k-1} - \sum_{i=1}^{t} q^{u_i-1}, \qquad \sum_{i=1}^{\min\{s+1,t\}} u_i \le sk,$$

where $s = \lceil d/q^{k-1} \rceil$, $k > u_1 \ge u_2 \ge \cdots \ge u_t \ge 1$ with $u_i > u_{i+q-1}$ for $1 \le i \le t-q+1$.

**Cor.** $n_q(k,d) = g_q(k,d)$ for all $d$ when $k = 1, 2$ and for $d > d_1 = (k-2)q^{k-1} - (k-1)q^{k-2}$ for $q \ge k \ge 3$.

Thm 8 was proved by geometric puncturing from $s$-fold simplex code as Lemma 7, and the following lemma can be proved similarly.

**Lemma 9.** Let $\Pi$ be a $t$-flat in $\Sigma = \mathrm{PG}(k-1,q)$, $2 \le t \le k-1$ and let $u_1, \cdots, u_r$ be integers with $0 \le u_r \le u_{r-1} \le \cdots \le u_1 \le t-1$ and $u_i > u_{i+q-1}$ $({}^\forall i)$.
$\Rightarrow \exists \Delta_{u_j}$: $u_j$-flat in $\Pi$ $(1 \le j \le r)$ s.t. the multiset $s\Pi$ contains $\Delta_{u_1} + \cdots + \Delta_{u_r}$ if

$$\sum_{i=1}^{s+1} u_i \le st - 1.$$

## 3. Construction of new codes 1

**Lemma 3'.** There exists a $[g_q(k,d)+1, k, d]_q$ code with $q \geq k \geq 5$ for $d = (k-2)q^{k-1} - (k-1)q^{k-2} - \sum_{i=1}^{k-3} t_i q^i$ with $0 \leq t_{k-3} \leq q-k$ and $0 \leq t_j \leq q-1$ for $1 \leq j \leq k-4$.

$s$-arc in PG$(r,q)$

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

When $q \geq r$, it is known that there exists a $(q+1)$-arc. A set of $s$ hps is an $s$-arc of hps if it forms an $s$-arc in the dual space.

## 3. Construction of new codes 1

**Lemma 3'.** There exists a $[g_q(k,d)+1,k,d]_q$ code with $q \geq k \geq 5$ for $d = (k-2)q^{k-1} - (k-1)q^{k-2} - \sum_{i=1}^{k-3} t_i q^i$ with $0 \leq t_{k-3} \leq q-k$ and $0 \leq t_j \leq q-1$ for $1 \leq j \leq k-4$.

**Proof.** $\Sigma = \mathrm{PG}(k-1,q)$

$\{H_1, H_2, \cdots, H_k\}$: a $k$-arc of hps in $\Sigma$

Let $P$ be the point $P = H_1 \cap \cdots \cap H_{k-1} \notin H_k$.

$\mathcal{S} = (k-2)\Sigma + P - (H_1 + \cdots + H_{k-1})$

$\mathcal{C}$ : the code with $\mathcal{M}_{\mathcal{C}} = \mathcal{S}$.

$\Rightarrow$ $\mathcal{C}$ is a $[g_q(k,d_1)+1,k,d_1]_q$ code with

$d_1 = (k-2)q^{k-1} - (k-1)q^{k-2}$.

The set of 0-points in $\Sigma$ consists of $k-1$ lines through $P$ meeting $H_k$ in $k-1$ points.

Let $\pi_i = H_k \cap H_i$ for $1 \le i \le k-1$.
$\Rightarrow$ $\{\pi_1, \cdots, \pi_{k-1}\}$ is a $(k-1)$-arc of $(k-3)$-flats in $H_k$ and $\mathcal{M}_{\mathcal{C}}(H_k) = (k-2)H_k - (\pi_1 + \cdots + \pi_{k-1})$.
Since $(k-1)$-arcs in a $(k-2)$-flat are unique up to projective equivalence, it follows from Lemma 9 that the multiset $\mathcal{M}_{\mathcal{C}}(H_k)$ contains $\Delta_{u_1} + \cdots + \Delta_{u_r}$, where $\Delta_{u_j}$ is a $u_j$-flat in $H_k$ for $1 \le j \le r$ with $u_r \le \cdots \le u_1 \le k-2$ s.t. $u_i > u_{i+q-1}$ and $\Delta_{u_j} = \pi_j$ for $1 \le j \le k-1$ since $\sum_{i=1}^{k-1} u_i \le (k-2)(k-1)$.
So, the multiset $\mathcal{M}_{\mathcal{C}} - (\Delta_{u_k} + \Delta_{u_{k+1}} + \cdots + \Delta_{u_r})$ gives a $[g_q(k,d)+1, k, d]_q$ code for $d = d_1 - \sum_{i=1}^{r} q^{u_i}$. $\square$

**Remark.** For $k = 5$, Lemma 3 implies $\exists [g_q(5, d) + 1, 5, d]_q$ code for $d_1 - q^3 + 4q^2 + 1 \le d \le d_1$. We can improve this as follows.

**Thm 10.** There exists a $[g_q(k, d) + 1, k, d]_q$ code for $d_1 - q^{k-2} + 1 \le d \le d_1$ for $k = 4, 5$.

**Problem 3.** Does a $[g_q(k, d) + 1, k, d]_q$ code exist for $d_1 - q^{k-2} + 1 \le d \le d_1 = (k-2)q^{k-1} - (k-1)q^{k-2}$ for $k \ge 6$?

## 4. Construction of new codes 2

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

We need the above lemma to prove the following.

**Thm 1.** There exists a $[g_q(5,d)+1, 5, d]_q$ code for $q^4 - q^3 - q^2 + 1 \le d \le q^4 - q^3 - 2q$.

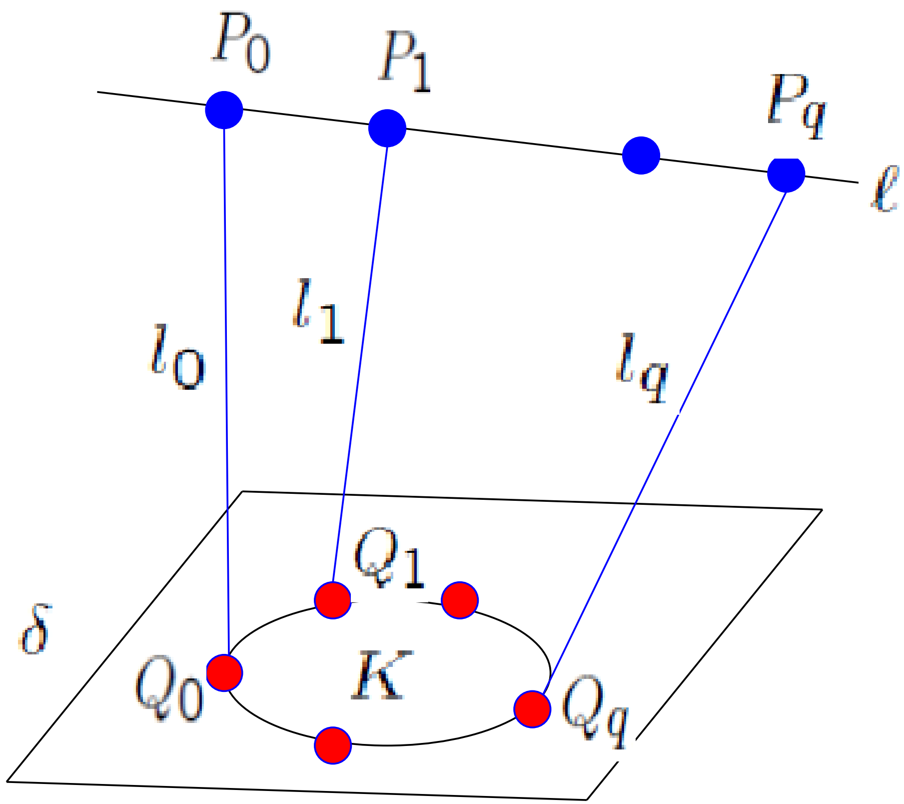
## 4. Construction of new codes 2

**Lemma 11.** There exists a $q$-divisible $[q^2+q, 5, q^2-q]_q$ code $\mathcal{C}$ 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**

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

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 $\mathcal{C}$.




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

$\ell \cap \delta = \emptyset$

$K$: a $(q+1)$-arc in $\delta$

$l_i = \langle P_i, Q_i \rangle$

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

$C_0 = \Sigma \setminus C_1$

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

**Note.** A $q$-divisible $[q^2+q,5,q^2-q]_q$ code was first found for $q=5$ by the package Q-Extension, see

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

As for recent results on optimal codes over $\mathbb{F}_5$, see

Y. Kageyama, T. Maruta, I. Bouyukliev, On the minimum length of linear codes over $\mathbb{F}_5$, submitted for publication.

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

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

$\downarrow$ projective dual

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

| $\mathcal{C}$ | $\mathcal{C}^*$ |
|---|---|
| $2q$-solid | 0-point |
| $q$-solid | 1-point |
| 0-solid | 2-point |
| line $\ell$ | plane $\ell^*$ |
| line $l_i$ | plane $l_i^*$ |

| $\|m \cap K\|$ | $\langle m, \ell \rangle$ |
|---|---|
| 2 | $2q$-solid |
| 1 | $q$-solid |
| 0 | 0-solid |

$m$: a line on $\delta$

- Every 0-point in $\Sigma^*$ for $\mathcal{C}^*$ is a point on some plane $l_i^*$ or on the plane $\ell^*$.
- From a counting argument, one can take $q-1$ skew lines containing no 0-point for $\mathcal{C}^*$.

Hence, from our code $\mathcal{C}^*$, one can construct a $[q^4+1-t(q+1), 5, q^4-q^3-tq]_q$ code for $1 \leq t \leq q-1$ by geometric puncturing. $\square$

**Remark.** We constructed a $q^2$-div. $[q^4+1, 5, q^4-q^3]_q$ code from a $q$-div. $[q^2+q, 5, q^2-q]_q$ code by PD.

The PD of a $q^{k-3}$-div. $[q^{k-1}+1, k, q^{k-1}-q^{k-2}]_q$ code is a $q$-div. $[q^2+q, k, q^2-q]_q$ code for $k \geq 4$.

- For $k=4$, $\exists q$-div. $[q^2+q, 4, q^2-q]_q$ code (take $q$ skew lines in PG$(3, q)$).
- For $k=5$, $\exists q$-div. $[q^2+q, 5, q^2-q]_q$ code.
- For $k \geq 6$, existence of a $q$-div. $[q^2+q, k, q^2-q]_q$ code is unknown except for

**Remark.** We constructed a $q^2$-div. $[q^4+1, 5, q^4-q^3]_q$ code from a $q$-div. $[q^2+q, 5, q^2-q]_q$ code by PD.

The PD of a $q^{k-3}$-div. $[q^{k-1}+1, k, q^{k-1}-q^{k-2}]_q$ code is a $q$-div. $[q^2+q, k, q^2-q]_q$ code for $k \geq 4$.

- For $k = 4$, $\exists q$-div. $[q^2+q, 4, q^2-q]_q$ code (take $q$ skew lines in PG$(3, q)$).
- For $k = 5$, $\exists q$-div. $[q^2+q, 5, q^2-q]_q$ code.
- For $k \geq 6$, existence of a $q$-div. $[q^2+q, k, q^2-q]_q$ code is unknown except for the extended ternary Golay $[12, 6, 6]_3$ code ($k = 6$ and $q = 3$).

## References


[1] A. Klein and K. Metsch, Parameters for which the Griesmer bound is not sharp, *Discrete Math.*, **307**, 2695–2703, 2007.

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

[3] T. Maruta, I.N. Landjev and A. Rousseva, On the minimum size of some minihypers and related linear codes, *Des. Codes Cryptogr.*, **34**, 5–15, 2005.

[4] T. Maruta and Y. Oya, On optimal ternary linear codes of dimension 6, *Adv. Math. Commun.*, **5** (2011) 505–520.


Thank you for your attention!