

Optimal 4-dimensional linear codes over finite fields

Tatsuya Maruta

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

Overview

We give how to construct optimal linear codes by projective puncturing to determine $n_q(4, d)$, the minimum value of n for which an $[n, 4, d]_q$ code exists.

Contents

1. Optimal linear codes problem
2. Puncturing
3. The geometric method
4. Optimal 4-dimensional linear codes
5. Proof of Theorem 2

1. Optimal linear codes problem

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

For $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in \mathbb{F}_q^n$,

the (Hamming) distance between a and b is

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

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

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.

\mathcal{C} : $[n, k, d]_q$ code, $d > 1$, with generator matrix G .

- G is a $k \times n$ matrix over \mathbb{F}_q whose k rows form a basis of \mathcal{C} .

Assume G has no all-zero column.

- A $k \times (n - 1)$ matrix G_p obtained from G with one column deleted generates an $[n - 1, k, d_p]_q$ code, $d_p = d - 1$ or d , called a **punctured code** of \mathcal{C} .

- Assume $G = \left[\begin{array}{c|cccc} 1 & * & * & * \\ \hline 0 & & & & \\ \vdots & & G_s & & \\ 0 & & & & \end{array} \right]$.

G_s generates an $[n - 1, k - 1, d_s]_q$ code, $d_s \geq d$, called a **shortened code** of \mathcal{C} .

- $\exists [n, k, d]_q \Rightarrow \exists [n - 1, k, d - 1]_q, \exists [n - 1, k - 1, d]_q$

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 (Hill [2]).

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 $n = n_q(k, d)$.

Known results for small q

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

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

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

$$q = 4, k \leq 4,$$

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

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

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

see

Y. Edel, I. Landjev, On multiple caps in finite projective spaces,
Des. Codes Cryptogr. **56** (2010) 163–175.

As for the updated bounds on the existence of $[n, k, d]_q$ codes for small q and n , see

<http://www.codetables.de/>

(maintained by Markus Grassl)

or

[http://www.algorithm.uni-bayreuth.de/en/research/
Coding_Theory/Linear_Codes_BKW/](http://www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/Linear_Codes_BKW/)

(maintained by Axel Kohnert).

As for some tables on $n_q(k, d)$ for small q and k , see

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

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.

Problem 2.

Find all values of q, k, d for which $n_q(k, d) = g_q(k, d)$ holds.

Some known results.

- $n_q(k, d) = g_q(k, d)$ for all d, q when $k = 1, 2$.
- The exact values of $n_q(3, d)$ are known for all d only for $q \leq 9$, see Simeon Ball's website [1]:

<http://www-ma4.upc.es/~simeon/codebounds.html>

$[k = 4, q = 2]$

d	$g_2(4, d)$	$n_2(4, d)$
1	4	4
2	5	5
3	7	7
4	8	8
5	11	11
6	12	12
7	14	14
8	15	15

d	$g_2(4, d)$	$n_2(4, d)$
9	19	19
10	20	20
11	22	22
12	23	23
13	26	26
14	27	27
15	29	29
16	30	30

- $n_2(4, d) = g_2(4, d)$ for all d .

$[k = 4, q = 3]$

d	$g_3(4, d)$	$n_3(4, d)$
1	4	4
2	5	5
3	6	7
4	8	8
5	9	9
6	10	10
7	12	13
8	13	14
9	14	15

d	$g_3(4, d)$	$n_3(4, d)$
10	17	17
11	18	18
12	19	19
13	21	22
14	22	23
15	23	24
16	25	25
17	26	26
18	27	27

- $n_3(4, d) = g_3(4, d)$ for all $d \geq 16$.

$$[k = 4, q = 4] \quad g = g_4(4, d), n = n_4(4, d)$$

d	g	n
1	4	4
2	5	5
3	6	7
4	7	8
5	9	9
6	10	10
7	11	12
8	12	13
9	14	14
10	15	15
11	16	16
12	17	17
13	19	20
14	20	21
15	21	22
16	22	23
17	25	25
18	26	26
19	27	27
20	28	28

d	g	n
21	30	30
22	31	31
23	32	33
24	33	34
25	35	36
26	36	37
27	37	38
28	38	39
29	40	41
30	41	42
31	42	43
32	43	44
33	46	46
34	47	47
35	48	48
36	49	49
37	51	52
38	52	53
39	53	54
40	54	55

d	g	n
41	56	57
42	57	58
43	58	59
44	59	60
45	61	61
46	62	62
47	63	63
48	64	64
49	67	67
50	68	68
51	69	69
52	70	70
53	72	72
54	73	73
55	74	74
56	75	75
57	77	77
58	78	78
59	79	79
60	80	80

d	g	n
61	82	82
62	83	83
63	84	84
64	85	85
65	89	89
66	90	90
67	91	91
68	92	92
69	94	94
70	95	95
71	96	96
72	97	97
73	99	99
74	100	100
75	101	101
76	102	102
77	104	105
78	105	106
79	106	107
80	107	108

- $n_4(4, d) = g_4(4, d)$ for all $d \geq 81$.

[$k = 4$]

- The exact values of $n_q(4, d)$ are known for all d only for $q = 2, 3, 4$.
- There are only four open cases for $q = 5$:
 $n_5(4, d) = g_5(4, d)$ or $g_5(4, d) + 1$ for $d = 81, 82, 161, 162$.
- Table for $n_7(4, d)$ for all d is under construction.
- There are 454 open cases for $q = 8$.
- Can we generalize $n_4(4, d)$ -table to $q \geq 5$?

2. Puncturing

Question 1.

Let \mathcal{C} be a $[9, 4, 4]_2$ code with the following generator matrix G . Can you find an $[8, 4, 4]_2$ code from \mathcal{C} by puncturing?

$$G = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

2. Puncturing

Question 1.

Let \mathcal{C} be a $[9, 4, 4]_2$ code with the following generator matrix G . Can you find an $[8, 4, 4]_2$ code from \mathcal{C} by puncturing?

$$G = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Answer.

Yes, by deleting the 3rd column of G . Why?

2. Puncturing

Question 1.

Let \mathcal{C} be a $[9, 4, 4]_2$ code with the following generator matrix G . Can you find an $[8, 4, 4]_2$ code from \mathcal{C} by puncturing?

$$G = \begin{bmatrix} 0 & \color{red}{1} & \color{blue}{0} & 0 & \color{red}{1} & 0 & \color{red}{1} & 0 & \color{red}{1} \\ 1 & 0 & \color{blue}{1} & 0 & 1 & 0 & 0 & 1 & 1 \\ \color{red}{1} & \color{red}{1} & 0 & 0 & \color{red}{1} & \color{red}{1} & 0 & 0 & 0 \\ \color{red}{1} & 0 & \color{blue}{0} & 1 & 0 & \color{red}{1} & 0 & 1 & 0 \end{bmatrix}$$

Answer.

Yes, by deleting the 3rd column of G . Why?

Question 2.

Let \mathcal{C} be a $[13, 3, 9]_3$ code with the following generator matrix G . Can you find an $[9, 3, 6]_3$ code from \mathcal{C} by puncturing?

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

Question 2.

Let \mathcal{C} be a $[13, 3, 9]_3$ code with the following generator matrix G . Can you find an $[9, 3, 6]_3$ code from \mathcal{C} by puncturing?

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

Answer.

Yes, by deleting the first four columns of G . Why?

3. The geometric method

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

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

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

\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 $\Sigma = \text{PG}(k - 1, q)$ denoted by \overline{G} .

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

$\Sigma \ni P$: *i-point* $\Leftrightarrow P$ has multiplicity i in \overline{G}

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

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

For $\forall S \subset \Sigma$ we define *the multiplicity of S* , denoted by $m(S)$, as

$$m(S) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|.$$

Then we obtain the partition $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ s.t.

$$n = m(\Sigma),$$

$$n - d = \max\{m(\pi) \mid \pi \in \mathcal{F}_{k-2}\}.$$

Conversely such a partition of Σ as above gives an $[n, k, d]_q$ code in the natural manner.

When \mathcal{C} is projective, i.e. $\gamma_0 = 1$,

\overline{G} forms an n -set in $\Sigma = \text{PG}(k - 1, q)$ satisfying

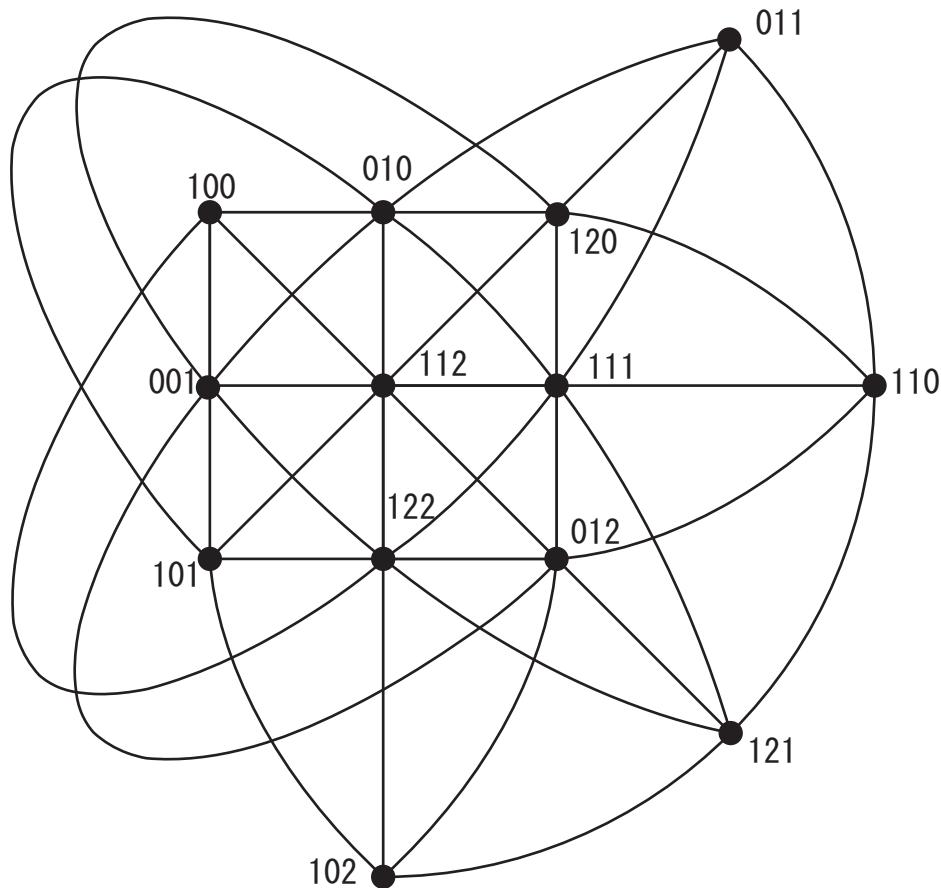
$$|\overline{G} \cap H| \leq n - d \quad \text{for } \forall H \in \mathcal{F}_{k-2}$$

where \mathcal{F}_j is the set of j -flats of Σ .

Such an n -set is called an $(n, n - d)$ -arc in $\text{PG}(k - 1, q)$.

Note. $(n, n - d)$ -arcs in $\text{PG}(k - 1, q)$ and projective $[n, k, d]_q$ codes are equivalent objects.

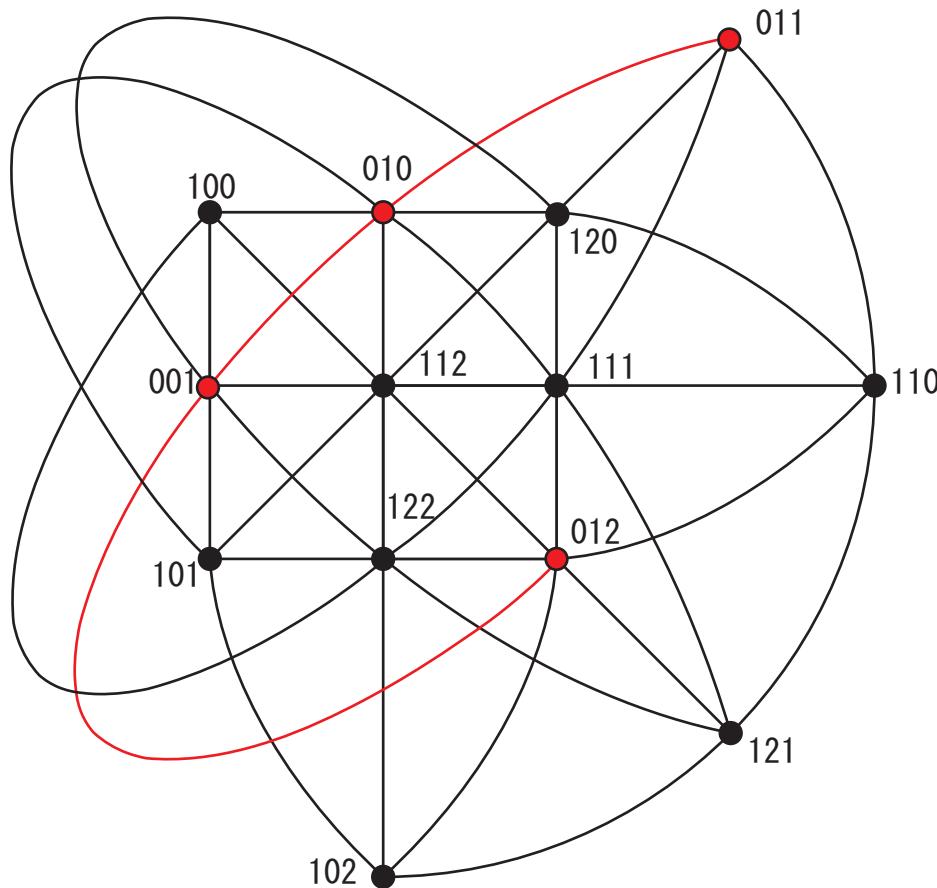
Ex. $\text{PG}(2, 3)$



$[13, 3, 9]_3$ simplex code

$$\left[\begin{array}{cccccccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{array} \right]$$

Ex. $\text{PG}(2, 3)$



(9, 3)-arc in $\text{PG}(2, 3)$
at most three points
of which are collinear

$[9, 3, 6]_3$ code

0	0	0	0	1	1	1	1	1	1	1	1
0	1	1	1	0	0	0	1	1	1	2	2
1	0	1	2	0	1	2	0	1	2	0	1

Lemma 1.

\mathcal{C} : projective $[n, k, d]_q$ code with generator matrix G .

\overline{G} : $(n, n-d)$ -arc of $\Sigma = \text{PG}(k-1, q)$ obtained from G .

If \overline{G} contains a t -flat Δ s.t. $\overline{G} - \Delta$ spans Σ

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

Proof. Let \mathcal{C}' be an $[n' = n - \theta_t, k, d']_q$ code obtained from $K = \overline{G} - \Delta$.

For $\forall H \in \mathcal{F}_{k-2}$, $H \cap \Delta = \theta_{t-1}$ or θ_t . So,

$$|K \cap H| \leq n' - d' \leq n - d - \theta_{t-1},$$

giving $d' \geq d - q^t$.

Lemma 1.

\mathcal{C} : projective $[n, k, d]_q$ code with generator matrix G .

\overline{G} : $(n, n-d)$ -arc of $\Sigma = \text{PG}(k-1, q)$ obtained from G .

If \overline{G} contains a t -flat Δ s.t. $\overline{G} - \Delta$ spans Σ

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

Example.

\mathcal{C} : simplex $[\theta_{k-1}, k, q^{k-1}]_q$ code

Δ : a hp of Σ

$\Rightarrow \mathcal{C}'$: Griesmer $[q^{k-1}, k, q^{k-1} - q^{k-2}]_q$ code

Lemma 2.

\mathcal{C} : s -fold simplex $[s\theta_{k-1}, k, sq^{k-1}]_q$ code, $s \geq 1$,

i.e. every point of $\Sigma = \text{PG}(k-1, q)$ is an s -point.

If there exist F_1, \dots, F_t ($F_j \in \mathcal{F}_{m_j}$, $0 \leq m_j \leq k-2$) s.t.

$$\bigcap_{i \in I} F_i = \emptyset \text{ for any } (s+1)\text{-set } I \subset \{1, \dots, t\}$$

$$\Rightarrow \exists [g_q(k, d), k, d]_q \text{ code for } d = sq^{k-1} - \sum_{i=1}^t q^{m_i}.$$

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

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

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

Thm 1 was first proved by Belov, Logachev, Sandimirov (1974) for binary codes, and generalized to non-binary codes by Hill (1992). For $q = 2$, see

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

Thm 1. $\exists \mathcal{C}: [g_q(k, d), k, d]_q$ code of Belov type iff

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

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

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

4. Optimal 4-dimensional linear codes

$[k = 4, q = 2]$

d	$g_2(4, d)$	$n_2(4, d)$	d	$g_2(4, d)$	$n_2(4, d)$
1	4	4	9	19	19
2	5	5	10	20	20
3	7	7	11	22	22
4	8	8	12	23	23
5	11	11	13	26	26
6	12	12	14	27	27
7	14	14	15	29	29
8	15	15	16	30	30

- $n_2(4, d) = g_2(4, d)$ for all $d \geq 3$ by Thm 1.

$[k = 4, q = 2]$

d	$g_2(4, d)$	construction
1	4	\mathbb{F}_2^4 : $[4, 4, 1]_2$
2	5	extension of \mathbb{F}_2^4
3	7	$S_1 - \Pi_2 - \Pi_0$
4	8	$S_1 - \Pi_2$
5	11	$S_1 - \Pi_1 - \Pi_0$
6	12	$S_1 - \Pi_1$
7	14	$S_1 - \Pi_0$
8	15	S_1

- $S_1 = \text{PG}(3, 2)$ (simplex code), $\Pi_i \in \mathcal{F}_i$
- $n_2(4, d) = g_2(4, d)$ for all $d \geq 3$ by Thm 1.

$[k = 4, q = 2]$

d	$g_2(4, d)$	construction
9	19	$S_2 - \Pi_2 - \Pi_1 - \Pi_0$
10	20	$S_2 - \Pi_2 - \Pi_1$
11	22	$S_2 - \Pi_2 - \Pi_0$
12	23	$S_2 - \Pi_2$
13	26	$S_2 - \Pi_1 - \Pi_0$
14	27	$S_2 - \Pi_1$
15	29	$S_2 - \Pi_0$
16	30	S_2

- S_2 : 2-fold simplex, $\Pi_i \in \mathcal{F}_i$

$$[k = 4, q = 4] \quad g = g_4(4, d), n = n_4(4, d)$$

d	g	n
1	4	4
2	5	5
3	6	7
4	7	8
5	9	9
6	10	10
7	11	12
8	12	13
9	14	14
10	15	15
11	16	16
12	17	17
13	19	20
14	20	21
15	21	22
16	22	23
17	25	25
18	26	26
19	27	27
20	28	28

d	g	n
21	30	30
22	31	31
23	32	33
24	33	34
25	35	36
26	36	37
27	37	38
28	38	39
29	40	41
30	41	42
31	42	43
32	43	44
33	46	46
34	47	47
35	48	48
36	49	49
37	51	52
38	52	53
39	53	54
40	54	55

d	g	n
41	56	57
42	57	58
43	58	59
44	59	60
45	61	61
46	62	62
47	63	63
48	64	64
49	67	67
50	68	68
51	69	69
52	70	70
53	72	72
54	73	73
55	74	74
56	75	75
57	77	77
58	78	78
59	79	79
60	80	80

d	g	n
61	82	82
62	83	83
63	84	84
64	85	85
65	89	89
66	90	90
67	91	91
68	92	92
69	94	94
70	95	95
71	96	96
72	97	97
73	99	99
74	100	100
75	101	101
76	102	102
77	104	105
78	105	106
79	106	107
80	107	108

- $n_4(4, d) = g_4(4, d)$ for all $d \geq 81$.

Known results [M 1999]

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

Ex. $n_4(4, d)$ ($g = g_4(4, d)$, $n = n_4(4, d)$).

d	1, 2	9-12	33-36	45-76	81-
n	g	g	g	g	g
cf.	(1)	(2)	(3)	(4)	(5)

How to construct a $[g_q(4, d), 4, q^3 - 2q^2 + q]_q$ code

Let $\mathcal{H} = \mathbf{V}(x_0x_1 + x_2x_3)$: hyperbolic quadric in

$\Sigma = \text{PG}(3, q)$. Take

$P(0010) \in \mathcal{H}$ and $\pi = \mathbf{V}(x_3)$ (tangent plane at P).

Putting

$$C_0 = (\mathcal{H} \cup \pi) \setminus \{P\} \text{ and } C_1 = \Sigma \setminus C_0$$

we get a Griesmer $[q^3 - q^2 + 1, 4, q^3 - 2q^2 + q]_q$ code.

Known results ([M 1999], [M-Landjev-Rousseva 2005])

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

Ex. $n_4(4, d)$ ($g = g_4(4, d)$, $n = n_4(4, d)$).

d	13-15	16	23, 24	37-44	77-80
n	$g + 1$				
cf.	(1)	(2)	(3)	(4)	(5)

$$[k = 4, q = 4] \quad g = g_4(4, d), n = n_4(4, d)$$

d	g	n									
1	4	4	21	30	30	41	56	57	61	82	82
2	5	5	22	31	31	42	57	58	62	83	83
3	6	7	23	32	33	43	58	59	63	84	84
4	7	8	24	33	34	44	59	60	64	85	85
5	9	9	25	35	36	45	61	61	65	89	89
6	10	10	26	36	37	46	62	62	66	90	90
7	11	12	27	37	38	47	63	63	67	91	91
8	12	13	28	38	39	48	64	64	68	92	92
9	14	14	29	40	41	49	67	67	69	94	94
10	15	15	30	41	42	50	68	68	70	95	95
11	16	16	31	42	43	51	69	69	71	96	96
12	17	17	32	43	44	52	70	70	72	97	97
13	19	20	33	46	46	53	72	72	73	99	99
14	20	21	34	47	47	54	73	73	74	100	100
15	21	22	35	48	48	55	74	74	75	101	101
16	22	23	36	49	49	56	75	75	76	102	102
17	25	25	37	51	52	57	77	77	77	104	105
18	26	26	38	52	53	58	78	78	78	105	106
19	27	27	39	53	54	59	79	79	79	106	107
20	28	28	40	54	55	60	80	80	80	107	108

- $n_4(4, d) = g_4(4, d)$ for all $d \geq 81$.

$$[k = 4, q = 4] \quad g = g_4(4, d), n = n_4(4, d)$$

d	g	n
1	4	4
2	5	5
3	6	7
4	7	8
5	9	9
6	10	10
7	11	12
8	12	13
9	14	14
10	15	15
11	16	16
12	17	17
13	19	20
14	20	21
15	21	22
16	22	23
17	25	25
18	26	26
19	27	27
20	28	28

d	g	n
21	30	30
22	31	31
23	32	33
24	33	34
25	35	36
26	36	37
27	37	38
28	38	39
29	40	41
30	41	42
31	42	43
32	43	44
33	46	46
34	47	47
35	48	48
36	49	49
37	51	52
38	52	53
39	53	54
40	54	55

Known results (M 1999)

- $n_4(4, d) \geq g_4(4, d) + 1$ for
 - (1) $d = q - 1, q$ for $q \geq 4$
 - (2) $d = 2q - 1, 2q$ for $q \geq 4$
 - (3) $2q^2 - 2q + 1 \leq d \leq 2q^2$ for $q \geq 4$

$$[k = 4, q = 4] \quad g = g_4(4, d), n = n_4(4, d)$$

d	g	n
1	4	4
2	5	5
3	6	7
4	7	8
5	9	9
6	10	10
7	11	12
8	12	13
9	14	14
10	15	15
11	16	16
12	17	17
13	19	20
14	20	21
15	21	22
16	22	23
17	25	25
18	26	26
19	27	27
20	28	28

d	g	n
21	30	30
22	31	31
23	32	33
24	33	34
25	35	36
26	36	37
27	37	38
28	38	39
29	40	41
30	41	42
31	42	43
32	43	44
33	46	46
34	47	47
35	48	48
36	49	49
37	51	52
38	52	53
39	53	54
40	54	55

Known results (M 1999)

- $n_4(4, d) \geq g_4(4, d) + 1$ for
 - (1) $d = q - 1, q$ for $q \geq 4$
 - (2) $d = 2q - 1, 2q$ for $q \geq 4$
 - (3) $2q^2 - 2q + 1 \leq d \leq 2q^2$ for $q \geq 4$

Problem 3.

Generalize the existence of

- [10, 4, 6]₄ ($n = g$)
- [28, 4, 20]₄ ($n = g$)
- [31, 4, 22]₄ ($n = g$)
- [39, 4, 28]₄ ($n = g + 1$)
- [44, 4, 32]₄ ($n = g + 1$).

- We can generalize the existence of [7, 4, 3]₄ and [42, 4, 30]₄ ($n = g + 1$).

Problem 3.

Generalize the existence of

$[10, 4, 6]_4$, $[28, 4, 20]_4$, $[31, 4, 22]_4$ ($n = g$) and
 $[39, 4, 28]_4$, $[44, 4, 32]_4$ ($n = g + 1$).

As for the original construction of the above codes,
see

P.P. Greenough, R. Hill, Optimal linear codes over
 $\text{GF}(4)$, Discrete Math. 125 (1994) 187–199.

The fact $n_4(4, d) = g_4(4, d) + 1$ for $29 \leq d \leq 32$ can
be generalized to the following conjecture.

Conjecture. $n_q(4, d) = g_q(4, d) + 1$ for $q \geq 3$ for
 $q^3 - 2q^2 - q + 1 \leq d \leq q^3 - 2q^2$.

Note. (1) Conjecture is true for $q = 3, 4, 5$.
(2) It is known that $n_q(4, d) \geq g_q(4, d) + 1$ for $q \geq 7$.

Problem 4. (1) Does a $[287, 4, 245]_7$ code exist?
(2) Does a $[440, 4, 384]_8$ code exist?

Theorem 2. $n_q(4, d) = g_q(4, d) + 1$ for
(a) $q^3 - 2q^2 - q + 1 \leq d \leq q^3 - 2q^2 - \frac{q+1}{2}$ for odd $q \geq 7$,
(b) $q^3 - 2q^2 - q + 1 \leq d \leq q^3 - 2q^2 - \frac{q}{2}$ for even $q \geq 8$.

Lemma 1 can be generalized as follows.

Lemma 3 ([Geometric Puncturing](#)).

\mathcal{C} : $[n, k, d]_q$ code with generator matrix G .

$\Sigma = \cup_{i=0}^{\gamma_0} C_i$: the partition obtained from \overline{G} .

$\cup_{i>0} C_i \supset \mathcal{F}$: (f, m) -minihyper s.t. $\langle \cup_{i>0} C_i - \mathcal{F} \rangle = \Sigma$

$\Rightarrow \exists \mathcal{C}'$: $[n - f, k, d + m - f]_q$ code

An f -set F in $\text{PG}(k - 1, q)$ is an [\$\(f, m\)\$ -minihyper](#) if

$$m = \min\{|F \cap \pi| \mid \pi \in \mathcal{F}_{k-2}\}.$$

Ex. A line is a $(q + 1, 1)$ -minihyper.

A blocking b -set in some plane is a $(b, 1)$ -minihyper.

5. Proof of Theorem 2.

Theorem 2. $n_q(4, d) = g_q(4, d) + 1$ for

- (a) $q^3 - 2q^2 - q + 1 \leq d \leq q^3 - 2q^2 - \frac{q+1}{2}$ for odd $q \geq 7$,
- (b) $q^3 - 2q^2 - q + 1 \leq d \leq q^3 - 2q^2 - \frac{q}{2}$ for even $q \geq 8$.

To prove the above theorem, it suffices to construct a $[g_q(4, d) + 1, 4, d]_q$ code for

- (a) $d = q^3 - 2q^2 - \frac{q+1}{2}$ for odd $q \geq 7$,
- (b) $d = q^3 - 2q^2 - \frac{q}{2}$ for even $q \geq 8$,

since $\exists[n, k, d]_q \Rightarrow \exists[n - 1, k, d - 1]_q$.

5. Proof of Theorem 2.

Let $\mathcal{H} = V(x_0x_1 + x_2x_3)$: hyperbolic quadric in $\Sigma = PG(3, q)$. Take

$P(0010) \in \mathcal{H}$ and $\pi = V(x_3)$ (tangent plane at P).

Putting $C_0 = (\mathcal{H} \cup \pi) \setminus \{P\}$ and $C_1 = \Sigma \setminus C_0$, we get a Griesmer $[q^3 - q^2 + 1, 4, q^3 - 2q^2 + q]_q$ code, say \mathcal{C} .

Note that K contains no line, for $\gamma_1 = q$.

Instead, we take a blocking set \mathcal{B} in the plane

$\delta = V(x_0 + x_1)$ through P as \mathcal{F} in Lemma 3 so that

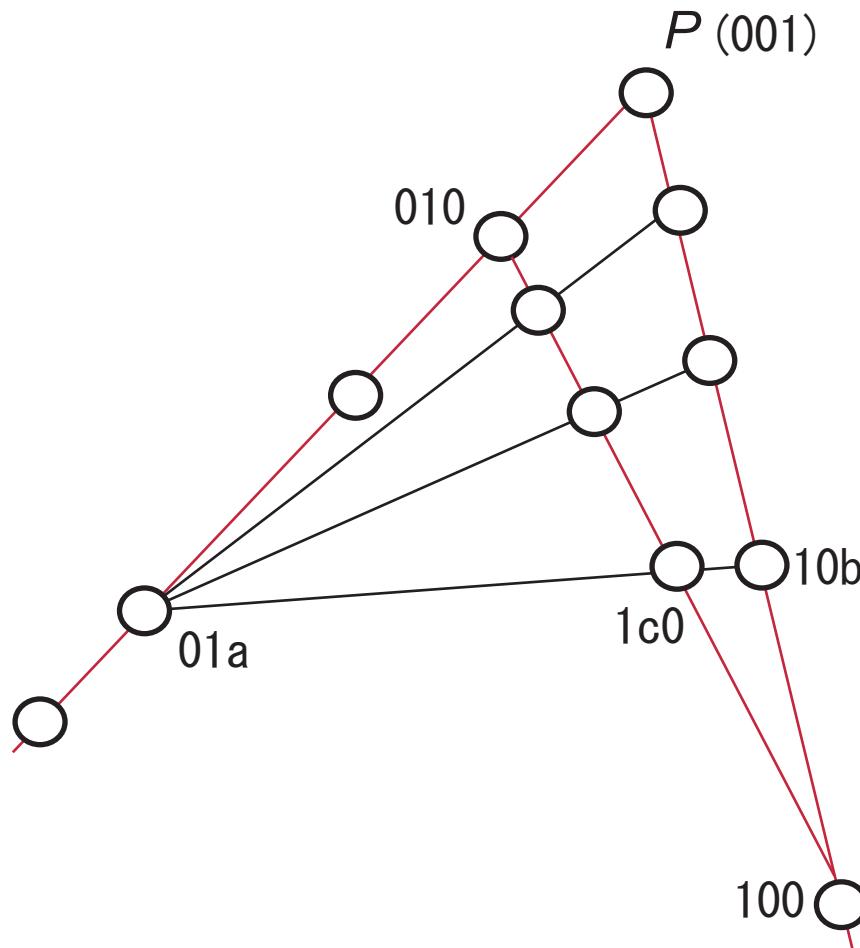
\mathcal{B} : projective triad of side $\frac{q+2}{2}$ for even q ,

\mathcal{B} : projective triangle of side $\frac{q+3}{2}$ for odd q .

Then we get the desired codes with length $g_q(4, d) + 1$.

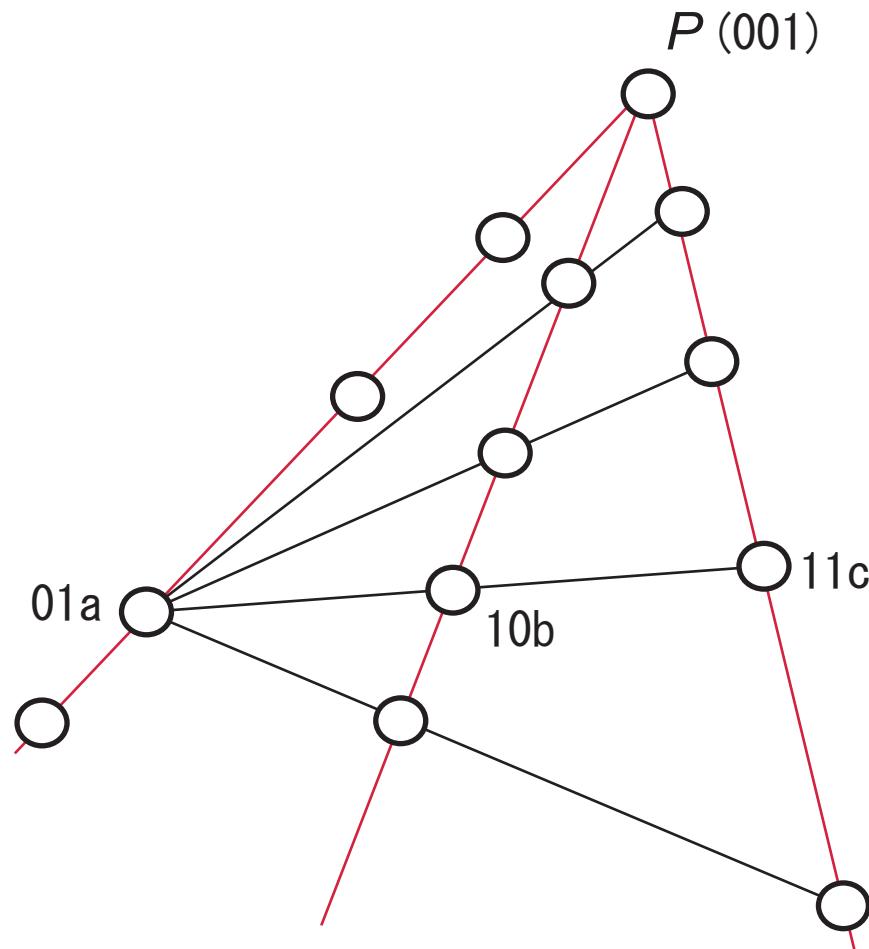
A projective triangle of side 5 in $\text{PG}(2, 7)$

a and b are non-zero squares in \mathbb{F}_7 , $c = -a^{-1}b$



A projective triad of side 5 in $\text{PG}(2,8)$

$a, b, c \in \mathbb{F}_8$ with $\text{tr}(a) = \text{tr}(b) = 0$, $c = a + b$



5. Proof of Theorem 2.

Let $\mathcal{H} = V(x_0x_1 + x_2x_3)$: hyperbolic quadric in $\Sigma = PG(3, q)$. Take

$P(0010) \in \mathcal{H}$ and $\pi = V(x_3)$ (tangent plane at P).

Putting $C_0 = (\mathcal{H} \cup \pi) \setminus \{P\}$ and $C_1 = \Sigma \setminus C_0$, we get a Griesmer $[q^3 - q^2 + 1, 4, q^3 - 2q^2 + q]_q$ code, say \mathcal{C} .

Note that K contains no line, for $\gamma_1 = q$.

Instead, we take a blocking set \mathcal{B} in the plane

$\delta = V(x_0 + x_1)$ through P as \mathcal{F} in Lemma 3 so that

\mathcal{B} : projective triad of side $\frac{q+2}{2}$ for even q ,

\mathcal{B} : projective triangle of side $\frac{q+3}{2}$ for odd q .

Then we get the desired codes with length $g_q(4, d) + 1$.

More new results.

- $n_q(4, d) = g_q(4, d) + 1$ for
$$2q^3 - 3q^2 - 2q + 1 \leq d \leq 2q^3 - 3q^2 - q, \quad q \geq 11$$
- $n_q(4, d) = g_q(4, d)$ for
$$2q^3 - 5q^2 + 1 \leq d \leq 2q^3 - 5q^2 + 3q, \quad q \geq 7$$
- $n_q(4, d) \leq g_q(4, d) + 1$ for
$$2q^3 - 6q^2 + 3q + 1 \leq d \leq 2q^3 - 5q^2, \quad q \geq 7$$
- $n_p(4, d) \geq g_p(4, d) + 1$ for
$$2p^3 - sp^2 - p + 1 \leq d \leq 2p^3 - sp^2, \quad p > s \geq 5, \quad p \text{ prime}$$

More problems.

- The only known case s.t. $n_q(4, d) > g_q(4, d) + 1$ holds is $n_5(4, 25) = g_5(4, 25) + 2$.

How about $n_7(4, 49)$?

($n_q(4, q^2) \geq g_q(4, q^2) + 1$ is known)

- Construct the $n_9(4, d)$ -table for all d .

($n_9(4, d) = g_9(4, d)$ for $d \geq 1216$)

Thank you for your attention!