New 4-dimensional linear codes over  $\mathbb{F}_9$ 

Tsukasa Okazaki (Joint work with Tatsuya Maruta)

Department of Mathematics and Information Sciences Osaka Prefecture University

#### Contents

- 1. Optimal linear codes problem
- 2. Geometric method
- 3. Projective dual
- 4. Geometric puncturing
- 5. Quasi-cyclic codes
- 6. Construction of new codes
- 7. New results on  $n_9(4, d)$

#### 1. Optimal linear codes problem

$$\mathbb{F}_q$$
: the field of  $q$  elements  
 $\mathbb{F}_q^n = \{(a_1, \cdots, a_n) \mid a_i \in \mathbb{F}_q\}$   
The weight of  $a = (a_1, \cdots, a_n) \in \mathbb{F}_q^n$  is  
 $wt(a) = |\{i \mid a_i \neq 0\}|$ 

An  $[n, k, d]_q$  code C means a k-dimensional subspace of  $\mathbb{F}_q^n$  with minimum weight d,  $d = \min\{wt(a) \mid a \in C, a \neq 0\}.$ A vector  $a \in C$  is called a codeword.

For an  $[n, k, d]_q$  code C, a  $k \times n$  matrix G whose rows form a basis of C is a generator matrix. The weight distribution (w.d.) of C is the list of numbers  $A_i > 0$ , where

$$A_i = |\{c \in \mathcal{C} \mid wt(c) = i\}| > 0.$$

The weight distribution

$$(A_0, A_d, \ldots) = (1, \alpha, \ldots)$$

is also expressed as

$$0^1 d^{\alpha} \cdots$$
.

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, and large d to correct many errors.

The problem to optimize one of the parameters n, k, d for given the other two is called "optimal linear codes problem" (Hill 1992). **Problem 1.** Find  $n_q(k, d)$ , the smallest value of *n* for which an  $[n, k, d]_q$  code exists.

**Problem 2.** Find  $d_q(n,k)$ , the largest value of d for which an  $[n,k,d]_q$  code exists.

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

We deal with Problem 1 for q = 9, k = 4.

#### The Griesmer bound

$$n \ge g_q(k,d) := \sum_{i=0}^{k-1} \left[ \frac{d}{q^i} \right]$$

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

An  $[n, k, d]_q$  code attaining the Griesmer bound is called a Griesmer code. Griesmer codes are optimal. Known results for q = 9, k = 4

The exact values of  $n_9(4, d)$  are determined for all d for  $d \ge 1216$ . For  $1 \le d \le 1215$ ,  $n_9(4, d)$  is detemined for

276 values of d but not for 939 values of d.

#### 2. The geometric method

 $\begin{array}{ll} \mathsf{PG}(r,q) \colon \text{projective space of dim. } r \text{ over } \mathbb{F}_q \\ j\text{-flat: } j\text{-dim. projective subspace of } \mathsf{PG}(r,q) \\ & 0\text{-flat: point } 1\text{-flat: line} \\ & 2\text{-flat: plane } (r-1)\text{-flat: hyperplane} \\ \theta_j \mathrel{\mathop:}= (q^{j+1}-1)/(q-1) = q^j + q^{j-1} + \dots + q + 1 \end{array}$ 

C: an  $[n, k, d]_q$  code generated by G.

Since we would like to find  $n_q(k,d)$ , we assume that G contains no all-zero-columns. Then the columns of G can be considered as a multiset of n points in  $\Sigma = PG(k-1,q)$ denoted also by C.

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

*i*-point: a point of  $\Sigma$  with multiplicity *i* in *C*.  $\gamma_0$ : the maximum multiplicity of a point from  $\Sigma$  in *C* 

 $\begin{array}{l} C_i: \text{ the set of } i\text{-points in } \Sigma, \ 0 \leq i \leq \gamma_0. \\ \lambda_i:= |C_i|, \ 0 \leq i \leq \gamma_0. \end{array}$ 

For  $\forall S \subset \Sigma$ , the multiplicity of S w.r.t. C, denoted by  $m_{\mathcal{C}}(S)$ , is defined by

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

Then we obtain the partition  $\Sigma = C_0 \cup C_1 \cup \cdots \cup C_{\gamma_0} \text{ such that}$   $n = m_{\mathcal{C}}(\Sigma),$   $n - d = \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}.$ 

Conversely such a partition of  $\Sigma$  as above gives an  $[n, k, d]_q$  code in the natural manner. *i*-hyperplane: a hyperplane  $\pi$  with  $i = m_{\mathcal{C}}(\pi)$ .  $a_i := |\{\pi \in \mathcal{F}_{k-2} \mid m_{\mathcal{C}}(\pi) = i\}|.$ 

The list of  $a_i$ 's is the spectrum of C.

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

#### 3. Projective dual

An  $[n, k, d]_q$  code is *m*-divisible (or *m*-div) if  $\exists m > 1$  s.t.  $A_i > 0 \Rightarrow m | i$ .

**Ex. 1.** There exists a 3-div  $[41, 4, 33]_9$  code with w.d.  $0^133^{984}36^{3608}39^{1968}$ .

The spectrum is  $(a_2, a_5, a_8) = (246, 451, 123)$ .

Lemma 1. (Projective dual) C: m-div  $[n, k, d]_q$  code,  $q = p^h$ , p prime.  $m = p^r$  for some  $1 \le r < h(k - 2)$ ,  $\lambda_0 > 0$ .  $\Rightarrow \exists C^*: t$ -div  $[n^*, k, d^*]_q$  code with

$$t = q^{k-2}/m,$$
  

$$n^* = ntq - \frac{d}{m}\theta_{k-1},$$
  

$$d^* = ((n-d)q - n)t.$$

A generator matrix for  $C^*$  is given by considering (n - d - jm)-hyperplanes as *j*-points in the dual space  $\Sigma^*$  of  $\Sigma$  for  $0 \le j \le w - 1$ .

Ex. 2.

- C: 3-div  $[41, 4, 33]_9$ with spec.  $(a_2, a_5, a_8) = (246, 451, 123)$ 
  - $\downarrow$  projective dual
- C\*: 27-div [943, 4, 837]<sub>9</sub>  $(n^* = 2a_2 + a_5)$ with spec.  $(a_{79}^*, a_{106}^*) = (41, 779)$

#### 4. Geometric puncturing

The puncturing from a given  $[n, k, d]_q$  code by deleting the coordinates corresponding to some geometric object in  $\Sigma = PG(k-1, q)$  is geometric puncturing.

**Lemma 2.** C:  $[n, k, d]_q$  code  $\cup_{i=0}^{\gamma_0} C_i$ : the partition of  $\Sigma$  obtained from C. If  $\cup_{i\geq 1} C_i$  contains a *t*-flat  $\Pi$  and if  $d > q^t$  $\Rightarrow \exists C'$ :  $[n - \theta_t, k, d']_q$  code, for  $d' \geq d - q^t$ .

#### 5. Quasi-cyclic codes

$$\begin{split} R &= \mathbb{F}_q[x]/(x^N - 1): \text{ ring of polynomials} \\ & \text{ over } \mathbb{F}_q \text{ modulo } x^N - 1. \\ \text{We associate } (a_0, a_1, ..., a_{N-1}) \in \mathbb{F}_q^N \\ & \text{ with } a_0 + a_1 x + \dots + a_{N-1} x^{N-1} \in R. \end{split}$$

For  $g = (g_1(x), \dots, g_m(x)) \in R^m$ , an ideal  $C_g$ of  $R^m$  defined by

$$C_{\mathbf{g}} = \{ (r(x)g_1(x), \cdots, r(x)g_m(x)) \mid r(x) \in R \}$$

is called the 1-generator quasi-cyclic (QC) code with generator g.

When m = 1,  $C = C_g$  is called cyclic satisfying that  $c(x) \in C$  implies  $x \cdot c(x) \in C$ , i.e.,  $(c_0, c_1, ..., c_{N-1}) \in C$  $\Rightarrow (c_{N-1}, c_0, c_1, ..., c_{N-2}) \in C$ .

Let 
$$g(x) = x^k - \sum_{i=0}^{k-1} g_i x^i \in \mathbb{F}_q[x]$$
 dividing  $x^N - 1$ .  
We denote by  $[g^N]$  or by  $[g_0g_1 \cdots g_{k-1}^N]$  the  $k \times N$  matrix

$$[P, TP, T^2P, ..., T^{N-1}P]$$
,

where

$$T = \begin{bmatrix} 0 & 0 & \dots & \dots & 0 & g_0 \\ 1 & 0 & \dots & \dots & 0 & g_1 \\ 0 & 1 & 0 & \dots & 0 & g_2 \\ 0 & 0 & \ddots & 0 & \vdots & \vdots \\ 0 & \dots & 0 & \ddots & 0 & g_{k-2} \\ 0 & \dots & 0 & 1 & g_{k-1} \end{bmatrix}, P = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

i.e., T is the companion matrix of g(x).

 $\tau : \mathsf{PG}(k-1,q) \longrightarrow \mathsf{PG}(k-1,q)$ defined by  $\tau(\mathsf{P}(x_0,\cdots,x_{k-1})) = \mathsf{P}(T(x_0,\cdots,x_{k-1})^{\mathsf{T}}).$ 

Then the columns of  $[g^N]$  can be considered as an orbit of  $\tau$ .

Now, take m orbits  $\mathcal{O}_1, \mathcal{O}_2, \cdots, \mathcal{O}_m$  of  $\tau$  with length N, and select a point  $P_i$  from each  $\mathcal{O}_i$ . We take  $P_1, P_2, \cdots, P_m$  as non-zero column vectors in  $\mathbb{F}_q^k$ . We always take  $P_1$  as  $P = (1, 0, 0, \dots, 0)^{\top}$ . We denote the matrix  $[P_1, TP_1, T^2P_1, ..., T^{n_1-1}P_1; P_2, TP_2, \cdots$  $\cdots$  ;  $P_m, TP_m, T^2 P_m, ..., T^{n_m-1} P_m$ ] by  $[q^{n_1}] + P_2^{n_2} + \cdots + P_m^{n_m}$ . Then, the matrix  $[g^N] + P_2^N + \cdots + P_m^N$  defined from m orbits  $\mathcal{O}_1, \mathcal{O}_2, \cdots, \mathcal{O}_m$  of  $\tau$  generates a QC code.

 $\mathbb{F}_9 = \{0, 1, \alpha, \dots, \alpha^7\} \text{ ,with } \alpha^2 = \alpha + 1.$ we denote  $\alpha, \alpha^2, \dots, \alpha^7$  by  $2, 3, \dots, 8$  so that  $\mathbb{F}_9 = \{0, 1, 2, \dots, 8\}.$ 

addition table

+	0	1	2	3	4	5	6	7	8	×	C
0	0	1	2	3	4	5	6	7	8	0	С
1	1	5	3	8	7	0	4	6	2	1	C
2	2	3	6	4	1	8	0	5	7	2	C
3	3	8	4	7	5	2	1	0	6	3	C
4	4	7	1	5	8	6	3	2	0	4	C
5	5	0	8	2	6	1	7	4	3	5	C
6	6	4	0	1	3	7	2	8	5	6	C
7	7	6	5	0	2	4	8	3	1	7	C
8	8	2	7	6	0	3	5	1	4	8	C

multiplication table

Х	0	Τ	2	3	4	5	6	(	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	3	4	5	6	7	8	1
3	0	3	4	5	6	7	8	1	2
4	0	4	5	6	7	8	1	2	3
5	0	5	6	7	8	1	2	3	4
6	0	6	7	8	1	2	3	4	5
7	0	7	8	1	2	3	4	5	6
8	0	8	1	2	3	4	5	6	7

### **Ex. 3.** $P_1 = (1, 0, 0, 0)^{\top}, P_2 = (1, 0, 1, 7)^{\top} \in \mathbb{F}_9^4$

$$g(x) = x^4 - 5x^3 - 5x^2 - 5x - 5 \in \mathbb{F}_9[x]$$

$$\Rightarrow T = \begin{bmatrix} 0 & 0 & 0 & 5 \\ 1 & 0 & 0 & 5 \\ 0 & 1 & 0 & 5 \\ 0 & 0 & 1 & 5 \end{bmatrix}$$

 $P_1 = (1, 0, 0, 0)^{\top}$ ,  $TP_1 = (0, 1, 0, 0)^{\top}$ ,  $T^2 P_1 = (0, 0, 1, 0)^{\top}$ ,  $T^3 P_1 = (0, 0, 0, 1)^{\top}$ ,  $T^4 P_1 = (5, 5, 5, 5)^{\top}$ ,  $T^5 P_1 = (1, 0, 0, 0)^{\top}$ 

 $\mathcal{O}_1 = \{P_1, TP_1, T^2P_1, T^3P_1, T^4P_1\}$ 

$$\Rightarrow [1 \ 2 \ 3 \ 4^{5}] = \begin{bmatrix} 1 \ 0 \ 0 \ 0 \ 5 \\ 0 \ 1 \ 0 \ 0 \ 5 \\ 0 \ 0 \ 1 \ 0 \ 5 \\ 0 \ 0 \ 1 \ 5 \end{bmatrix}$$
$$\Rightarrow [5, 4, 2]_{9} \text{ code}$$

 $P_2 = (1,0,1,7)^{\top}$ ,  $TP_2 = (3,8,3,8)^{\top}$ ,  $T^2P_2 = (4,5,0,5)^{\top}$ ,  $T^3P_2 = (1,7,0,1)^{\top}$ ,  $T^4P_2 = (5,0,4,5)^{\top}$ ,  $T^5P_2 = (1,0,1,7)^{\top}$ 

 $\mathcal{O}_2 = \{P_2, TP_2, T^2P_2, T^3P_2, T^4P_2\}$ 

$$\Rightarrow 1017^{5} = \begin{bmatrix} 1 & 3 & 4 & 1 & 5 \\ 0 & 8 & 5 & 7 & 0 \\ 1 & 3 & 0 & 0 & 4 \\ 7 & 8 & 5 & 1 & 5 \end{bmatrix}$$
$$\Rightarrow [5, 4, 2]_{9} \text{ code}$$

$$\begin{bmatrix} 1 \ 2 \ 3 \ 4^{5} \end{bmatrix} = \begin{bmatrix} 1 \ 0 \ 0 \ 0 \ 5 \\ 0 \ 1 \ 0 \ 0 \ 5 \\ 0 \ 0 \ 1 \ 0 \ 5 \\ 0 \ 0 \ 0 \ 1 \ 5 \end{bmatrix}, \ 1 \ 0 \ 1 \ 7^{5} = \begin{bmatrix} 1 \ 3 \ 4 \ 1 \ 5 \\ 0 \ 8 \ 5 \ 7 \ 0 \\ 1 \ 3 \ 0 \ 4 \\ 7 \ 8 \ 5 \ 1 \ 5 \end{bmatrix}$$
$$\Rightarrow \ \begin{bmatrix} 1 \ 2 \ 3 \ 4^{5} \end{bmatrix} + 1 \ 0 \ 1 \ 7^{5} = \begin{bmatrix} 1 \ 0 \ 0 \ 0 \ 1 \\ 0 \ 1 \ 0 \ 0 \ 2 \\ 0 \ 8 \ 5 \ 7 \ 0 \\ 1 \ 3 \ 0 \ 4 \\ 7 \ 8 \ 5 \ 1 \ 5 \end{bmatrix}$$

 $\Rightarrow$  QC [10, 4, 5]<sub>9</sub> code

6. Construction of new codes

**Lemma 3.** There exists  $[1227, 4, 1089]_9$ ,  $[1237, 4, 1098]_9$ ,  $[1247, 4, 1107]_9$  codes.

#### Proof.

C: QC code with generator matrix  $[5214^7] + 1402^7 + 1371^7 + 1706^7 + 1243^7 + 1377^7 + 1718^7$ .

Then C is a 3-div  $[49, 4, 39]_9$  code with spectrum  $(a_1, a_4, a_7, a_{10}) = (28, 448, 267, 77).$ 

As projective dual, we get a  $[1247, 4, 1107]_9$ code  $C^*$  with w.d.  $0^1 1107^{6168} 1134^{392}$ . The multiset for  $\mathcal{C}^*$  has two skew lines  $l_1 = \langle 1000, 1111 \rangle, \ l_2 = \langle 1002, 1121 \rangle.$ Hence, we get  $[1227, 4, 1089]_9$ ,  $[1237, 4, 1098]_9$  codes by geometric puncturing.

Lemma 4. There exist

 $[913, 4, 810]_9$ ,  $[923, 4, 819]_9$ ,  $[933, 4, 828]_9$ and  $[943, 4, 837]_9$  codes.

#### Proof.

C: extended QC code with generator matrix  $[1000^4] + 7211^4 + 1116^4 + 1574^4 + 1376^4 + 1507^4$  $+1247^4 + 1426^4 + 1237^4 + 1860^4 + 1515^1$ .

⇒ C: 3-div [41, 4, 33]<sub>9</sub> code with spectrum  $(a_2, a_5, a_8) = (246, 451, 123).$  C: 3-div [41, 4, 33]<sub>9</sub>

 $\downarrow$  projective dual

 $C^*$ : 27-div [943, 4, 837]<sub>9</sub>

The multiset for  $\mathcal{C}^*$  contains three skew lines

 $l_1 = \langle 1000, 1018 \rangle, \ l_2 = \langle 1002, 1102 \rangle, \ l_3 = \langle 1003, 1114 \rangle.$ 

Hence, we get

 $[913, 4, 810]_9$ ,  $[923, 4, 819]_9$  and  $[933, 4, 828]_9$  codes by geometric puncturing.

There are 200 orbits of length 4, 8 orbits of length 2 and 4 fixed points under the projectivity defined by the companion matrix of  $x^4 - 1$ .

We give three other 3-divisible codes constructed from these orbits.

# Lemma 5. There exist $[1034 - 10t, 4, 918 - 9t]_9$ codes for t = 0, 1, 2, 3, 4, 5, 6, 7, 8.

#### Proof.

C:  $[38, 4, 30]_9$  code with generator matrix  $G = [1000^4] + 1721^4 + 1215^4 + 1056^4 + 1574^4$  $+ 1542^4 + 1761^4 + 1065^4 + 1168^4 + 1515^1 + 1357^1$ , where the columns of G consist of nine orbits of length 4 and two fixed points under the projectivity defined by the companion matrix of  $x^4 - 1$ .

⇒ C: 3-div [38, 4, 30]<sub>9</sub> code with spectrum  $(a_2, a_5, a_8) = (298, 438, 84).$ 

C: 3-div [38, 4, 30]<sub>9</sub>

 $\downarrow$  projective dual

 $C^*$ : 27-div [1034, 4, 918]<sub>9</sub>

The multiset for  $C^*$  contains eight skew lines  $\langle 1000, 1103 \rangle$ ,  $\langle 1002, 1111 \rangle$ ,  $\langle 1003, 1017 \rangle$ ,  $\langle 1005, 1121 \rangle$ ,  $\langle 1006, 1132 \rangle$ ,  $\langle 1007, 1140 \rangle$ ,  $\langle 1008, 1150 \rangle$ ,  $\langle 1010, 1105 \rangle$ . Hence, we get  $[1034 - 10t, 4, 918 - 9t]_9$  codes for  $1 \le t \le 8$ 

by geometric puncturing.

# Lemma 6. There exist $[1125 - 10t, 4, 999 - 9t]_9$ codes for t = 0, 1, 2, 3, 4, 5, 6, 7, 8.

#### Proof.

C:  $[35, 4, 27]_9$  code with generator matrix  $G = 1018^4 + 1077^4 + 1220^4 + 1550^4 + 1034^4 + 1566^4$  $+ 1356^4 + 1313^2 + 1652^2 + 1357^1 + 1111^1 + 1753^1$ , where the columns of G consist of seven orbits of length 4, two orbits of length 2 and three fixed points under the projectivity defined by the companion matrix of  $x^4 - 1$ .

⇒ C: 3-div [35, 4, 27]<sub>9</sub> code with spectrum  $(a_2, a_5, a_8) = (360, 405, 55).$  C: 3-div [35, 4, 27]<sub>9</sub>

 $\downarrow$  projective dual

 $C^*$ : 27-div [1125, 4, 999]<sub>9</sub>

The multiset for  $C^*$  contains eight skew lines  $\langle 1000, 1001 \rangle$ ,  $\langle 1011, 1100 \rangle$ ,  $\langle 1012, 1114 \rangle$ ,  $\langle 1013, 1120 \rangle$ ,  $\langle 1014, 1130 \rangle$ ,  $\langle 1015, 1140 \rangle$ ,  $\langle 1016, 1150 \rangle$ ,  $\langle 1017, 1161 \rangle$ . Hence, we get  $[1125 - 10t, 4, 999 - 9t]_9$  codes for  $1 \le t \le 8$ 

by geometric puncturing.

### Lemma 7. There exist $[1186-10t, 4, 1053-9t]_9$ for t = 0, 1, 2, 3, 4, 5 and $[1277, 4, 1134]_9$ codes.

#### Proof.

C:  $[39, 4, 30]_9$  code with generator matrix  $G = [1000^4] + 1721^4 + 1846^4 + 1473^4 + 1300^4 + 1851^4 + 1574^4 + 1281^4 + 1405^4 + 1256^2 + 1515^1$ , where the columns of G consist of nine orbits of length 4, **one orbit of length 2 and one fixed point** under the projectivity defined by the companion matrix of  $x^4 - 1$ .

⇒ C: 3-div [39, 4, 30]<sub>9</sub> code with spectrum  $(a_0, a_3, a_6, a_9) = (32, 427, 327, 34).$ 

```
C: 3-div [39, 4, 30]<sub>9</sub>
    \downarrow projective dual
    C^*: 27-div [1277, 4, 1134]<sub>9</sub>
The multiset for \mathcal{C}^* contains one plane
                  (1004, 1018, 1118)
and five skew lines
(1000, 1015), (1002, 1103), (1003, 1110), (1005, 1120),
(1006, 1140).
 Hence, we get
[1186 - 10t, 4, 1053 - 9t]_9 codes for 0 < t < 5
```

by geometric puncturing.

7. New results on  $n_9(4, d)$ We determined  $n_9(4, d)$  for 115 values of d. (1)  $n_9(4, d) = g_9(4, d)$  for  $d \in \{811-837, 892-918, 973-999\}$ 

(2)  $n_9(4,d) = g_9(4,d) + 1$  for  $d \in \{964-972, 1045-1053, 1114-1116, 1122-1134\}$ 

(3)  $n_9(4, d) \le g_9(4, d) + 1$  for  $d \in \{802-810, 838-891, 919-963, 1000-1044, 1081-1113, 1117-1121\}$ 

Still  $n_9(4, d)$  is not determined for 824 values of d.

### Thank you for your attention!

#### References

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

R. Hill, Optimal linear codes, in *Cryptography and Coding* II, C. Mitchell, Ed., Oxford Univ. Press, Oxford, 1992, 75–104.

R. Hill, D.E. Newton, Optimal ternary linear codes, *Des. Codes Cryptogr.* 2, 137–157, 1992.

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

T. Maruta, Griesmer bound for linear codes over finite fields, http://www.mi.s.osakafu-u.ac.jp/~maruta/griesmer.htm.

T. Maruta, Y. Oya, On optimal ternary linear codes of dimension 6, *Adv. Math. Commun.* **5**, 505–520, 2011.

T. Maruta, M. Shinohara, A. Kikui, On optimal linear codes over  $\mathbb{F}_5$ , *Discrete Math.* **309**, 1255–1272, 2009.

T. Maruta, M. Shinohara, M. Takenaka, Constructing linear codes from some orbits of projectivities, *Discrete Math.* **308** 832–841, 2008.