New 5-dimensional linear codes over $\mathbb{F}_5$

Yuuki Kageyama

(Joint work with Tatsuya Maruta)

Department of Mathematics

and Information Sciences

Osaka Prefecture University

Contents

1. Optimal linear codes problem

$\mathbb{F}_q$: the field of q elements

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

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

the (Hamming) distance between $\boldsymbol{a}$ and $\boldsymbol{b}$ is

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

The weight of $\boldsymbol{a} = (a_1, \cdots, a_n) \in \mathbb{F}_q^n$ is

$$\begin{aligned} wt(\boldsymbol{a}) &= |\{i \mid a_i \neq 0\}| \\ &= d(\boldsymbol{a}, \boldsymbol{0}) \end{aligned}$$

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

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

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

The weight distribution (w.d.) of $\mathcal{C}$ is the list of numbers $A_i > 0$, where

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

The weight distribution

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

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

$$n = n_q(k,d) \text{ or } d = d_q(n,k).$$

We deal with Problem 1 for $q=5$, $k=5$.

The Griesmer bound

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

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

An $[n,k,d]_q$ code attaining the Griesmer bound is called a Griesmer code.

Griesmer codes are optimal.

Known results for $q = 5$

The exact values of $n_5(k, d)$ are determined for all d for $k \leq 3$.

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

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

$n_5(5, d)$ is not determined yet for many d, see Maruta's website:

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

2. The geometric method

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

j-flat: j-dim. projective subspace of PG(r, q)

0-flat: point 1-flat: line

2-flat: plane $(r-1)$-flat: hyperplane

$\theta_j := (q^{j+1} - 1)/(q - 1)$

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

The columns of G can be considered as a multiset of n points in $\Sigma = \mathrm{PG}(k-1, q)$ denoted also by $\mathcal{C}$.

$\mathcal{F}_j$:= the set of j-flats of $\mathrm{PG}(k-1, q)$

i-point: a point of Σ with multiplicity i in $\mathcal{C}$.

γ_0: the maximum multiplicity of a point from Σ in $\mathcal{C}$

C_i: the set of i-points in Σ, $0 \leq i \leq \gamma_0$.

$\lambda_i := |C_i|$, $0 \leq i \leq \gamma_0$.

For ${}^\forall S \subset \Sigma$, the multiplicity of S w.r.t. $\mathcal{C}$, 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

$\Sigma = C_0 \cup C_1 \cup \cdots \cup C_{\gamma_0}$ such 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 such a partition of Σ as above gives an $[n,k,d]_q$ code in the natural manner.

i-hyperplane: a hyperplane π 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 $\mathcal{C}$.

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

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 5-div $[36, 5, 25]_5$ code with w.d. $0^1 25^{804} 30^{2260} 35^{60}$. The spectrum is $(a_1, a_6, a_{11}) = (15, 565, 201)$.

Lemma 1. (Projective dual)

$\mathcal{C}$: m-div $[n,k,d]_q$ code, $q=p^h$, p prime.

$m=p^r$ for some $1\le r<h(k-2)$, $\lambda_0>0$.

$\Rightarrow \exists\mathcal{C}^*$: t-div $[n^*,k,d^*]_q$ code with

$$t\ = q^{k-2}/m,$$
$$n^* = ntq - \tfrac{d}{m}\theta_{k-1},$$
$$d^* = n^* - nt + \tfrac{d}{m}\theta_{k-2} = ((n-d)q-n)t.$$

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

Ex. 2.

$\mathcal{C}$ 5-div $[36, 5, 25]_5$

with spec. $(a_1, a_6, a_{11}) = (15, 565, 201)$

$\downarrow$ projetive dual

$\mathcal{C}^*$ 25-div $[595, 5, 475]_5$ $(n^* = 2a_1 + a_6)$

with spec. $(a^*_{95}, a^*_{120}) = (36, 745)$

4. Geometric puncturing

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

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

5. Quasi-cyclic codes

$R = \mathbb{F}_q[x]/(x^N - 1)$: ring of polynomials over $\mathbb{F}_q$ modulo $x^N - 1$.

We associate $(a_0, a_1, ..., a_{N-1}) \in \mathbb{F}_q^N$ with $a_0 + a_1 x + \cdots + a_{N-1} x^{N-1} \in R$.

For $\mathbf{g} = (g_1(x), \cdots, g_m(x)) \in R^m$, an ideal $C_{\mathbf{g}}$ 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 $\mathbf{g}$.

When $m = 1$, $\mathcal{C} = C_{\mathbf{g}}$ is called cyclic satisfying that $c(x) \in \mathcal{C}$ implies $x \cdot c(x) \in \mathcal{C}$,

i.e., $\quad (c_0, c_1, ..., c_{N-1}) \in \mathcal{C}$

$\Rightarrow \quad (c_{N-1}, c_0, c_1, ..., c_{N-2}) \in \mathcal{C}$.

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 $[g_0 g_1 \cdots g_{k-1}^N]$ the $k \times N$ matrix

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

where

$$T = \left[\begin{array}{ccccc|c} 0 & 0 & \ldots & \ldots & 0 & g_0 \\ \hline 1 & 0 & \ldots & \ldots & 0 & g_1 \\ 0 & 1 & 0 & \ldots & 0 & g_2 \\ 0 & 0 & \ddots & 0 & \vdots & \vdots \\ 0 & \ldots & 0 & \ddots & 0 & g_{k-2} \\ 0 & \ldots & \ldots & 0 & 1 & g_{k-1} \end{array}\right], P = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}$$

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

$$\tau : \mathsf{PG}(k-1,q) \longrightarrow \mathsf{PG}(k-1,q)$$

defined by

$$\tau(\mathbf{P}(x_0,\cdots,x_{k-1})) = \mathbf{P}(T(x_0,\cdots,x_{k-1})^{\mathsf{T}}).$$

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

Now, take m orbits $\mathcal{O}_1, \mathcal{O}_2, \cdots, \mathcal{O}_m$ of τ 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 $P = (1, 0, 0, \cdots, 0)^{\mathsf{T}}$.

We denote the matrix

$$[P_1, TP_1, T^2P_1, ..., T^{n_1-1}P_1; P_2, TP_2, \cdots$$
$$\cdots; P_m, TP_m, T^2P_m, ..., T^{n_m-1}P_m]$$

by $[g^{n_1}] + P_2^{n_2} + \cdots + P_m^{n_m}$.

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 τ generates a QC code.

Ex. 3.

S: companion matrix of $x^4 + x + 1 \in \mathbb{F}_2[x]$.

Label the points of PG(3,2) as

$$Q_0 = P = 1000,\ Q_i = S^i P \text{ for } 1 \le i \le 14.$$

$g(x) = 1 + x + x^2 + x^4$ which divides $x^7 - 1$.

Let τ be the projectivity defined by $g(x)$.

Then τ has three orbits:

$$\mathcal{O}_1 = \{Q_0, Q_1, Q_2, Q_3, Q_{10}, Q_{11}, Q_7\},$$
$$\mathcal{O}_2 = \{Q_8, Q_9, Q_4, Q_5, Q_6, Q_{12}, Q_{14}\},$$
$$\mathcal{O}_3 = \{Q_{13} = 1011\}.$$

$$[g^7] + Q_8^7 = [1110^7] + 1010^7$$

$$= \left[\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{array}\right]$$

generates a QC $[14, 4, 7]_2$ code.

6. Construction of new codes

Lemma 3. There exists a $[169, 5, 131]_5$ code.

Proof.

$\mathcal{C}$: QC code with generator matrix

$$[10320^{13}] + 11000^{13} + 31000^{13} + 21100^{13} + 23100^{13}$$
$$+34100^{13} + 32010^{13} + 31110^{13} + 12110^{13} + 42110^{13}$$
$$+12210^{13} + 22210^{13} + 21310^{13}.$$

Then $\mathcal{C}$ is a $[169, 5, 131]_5$ code. $\square$

Lemma 4. There exists a $[609, 5, 485]_5$ code.

Proof.

$\mathcal{C}$: QC code with generator matrix

$[12411^{11}] + 11000^{11} + 20100^{11} + 31100^{11} + 40010^{11}$.

Then $\mathcal{C}$ is a 5-div $[55, 5, 40]_5$ code with spectrum $(a_5, a_{10}, a_{15}) = (66, 495, 220)$.

As projective dual, we get a $[627, 5, 500]_5$ code $\mathcal{C}^*$ with w.d. $0^1 500^{2904} 525^{220}$.

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

$l_1 = \langle 30100, 33010 \rangle$, $l_2 = \langle 11100, 30010 \rangle$,

$l_3 = \langle 21100, 31001 \rangle$.

The geometric puncturing $\mathcal{C}^* - (l_1 \cup l_2 \cup l_3)$ yields a $[609, 5, 485]_5$ code. $\square$

Lemma 5. There exist $[571, 5, 455]_5$, $[577, 5, 460]_5$, $[583, 5, 465]_5$, $[589, 5, 470]_5$ and $[595, 5, 475]_5$ codes.

Proof.

$\mathcal{C}$: extended QC code with generator matrix

$$[10000^5] + 11000^5 + 34100^5 + 11310^5$$

$$+33410^5 + 31411^5 + 24121^5 + 11111.$$

$\Rightarrow$ $\mathcal{C}$: 5-div $[36, 5, 25]_5$ code with spectrum

$$(a_1, a_6, a_{11}) = (15, 565, 201).$$

$\mathcal{C}$ 5-div $[36, 5, 25]_5$

$\downarrow$ projetive dual

$\mathcal{C}^*$ 25-div $[595, 5, 475]_5$

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

$$l_1 = \langle 10100, 22011 \rangle,\ l_2 = \langle 30100, 23011 \rangle,$$

$$l_3 = \langle 21100, 20011 \rangle,\ l_4 = \langle 31100, 11011 \rangle.$$

Hence, we get

$[595 - 6t, 5, 475 - 5t]_5$ codes for $t = 1, 2, 3, 4$

by geometric puncturing. $\square$

Lemma 6. (Hill-Newton, 1992)

$\mathcal{C}_1$: $[n_1, k, d_1]_q$ code

$\mathcal{C}_2$: $[n_2, k-1, d_2]_q$ code

$\exists c_1 \in \mathcal{C}_1$ with $wt(c_1) \geq d_1 + d_2$

$\Rightarrow \exists \mathcal{C}$: $[n_1 + n_2, k, d_1 + d_2]_q$ code

Lemma 7. There exist $[377, 5, 300]_5$, $[385, 5, 305]_5$, $[391, 5, 310]_5$, $[397, 5, 315]_5$ and $[403, 5, 320]_5$ codes.

Proof.

$\mathcal{C}_1$:5-div $[53, 5, 40]_5$ code generated by

$$G_1 = \begin{bmatrix} 00011111110001111111001111111100111111110011111111110 \\ 11111133441111113344111233334411111144441112333344000 \\ 01101304040240141234241013340413114400220323011401241 \\ 00110100440100110044444421213333333322224444112233000 \\ 40444310243122104020113200044010132404343303431121042 \end{bmatrix}$$

$\mathcal{C}_1$ 5-div $[53, 5, 40]_5$

$\downarrow$ projetive dual

$\mathcal{C}_1^*$ 25-div $[377, 5, 300]_5$

generator matrix: G_1^*

spectrum: $(a_{52}, a_{77}) = (53, 728)$

$\mathcal{C}_2$: $[26, 4, 20]_5$ code with generator matrix

$$G_2 = \begin{bmatrix} 00142323230023014140231414 \\ 00002233112344122334001144 \\ 10111111222222333333444444 \\ 01111111111111111111111111 \end{bmatrix}$$

Then $\mathcal{C}_2$ has spectrum $(a_1, a_6) = (26, 130)$.

Π: hyperplane ($V(3x_1 - x_4)$)

$$m_{\mathcal{C}_1^*}(\Pi) = 52$$

Define the mapping

$$\varphi: \ \mathrm{PG}(3,5) \to \Pi$$

for $\mathbf{P}(x_0, x_1, x_2, x_3) \in \mathrm{PG}(3,5)$ by

$$\varphi(\mathbf{P}(x_0, x_1, x_2, x_3)) = \mathbf{P}(x_0, x_1, x_2, x_3, 3x_1).$$

$$G_2 = \begin{bmatrix} 00142323230023014140231414 \\ 00002233112344122334001144 \\ 10111111222222333333444444 \\ 01111111111111111111111111 \end{bmatrix}$$

$$\Big\downarrow \; \varphi$$

$$G_2' = \begin{bmatrix} 00142332410014014410232332 \\ 00002222222222222222002222 \\ 10111144442311133224443322 \\ 01111144221433211443112233 \\ 00001111111111111111001111 \end{bmatrix}$$

$\mathcal{C}$: a code generated by $[G_1^*, G_2']$

Then $\mathcal{C}$ is a $[403, 5, 320]_5$ code by Lemma 6.

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

$$l_1 = \langle 12100, 31011 \rangle,\ l_2 = \langle 42100, 01021 \rangle,$$

$$l_3 = \langle 23100, 23021 \rangle.$$

Hence, we get

$[403 - 6t, 5, 320 - 5t]_5$ codes for $t = 1, 2, 3$ by

geometric puncturing. $\square$

7. New results on $n_5(5, d)$

We determined $n_5(5, d)$ for 68 values of d.

(1) $n_5(5, d) = g_5(5, d) + 1$ for

$d \in \{$296-300, 346-350,394,395,398-400,426-475$\}$

(2) $n_5(5, d) = g_5(5, d) + 2$ for $373 \leq d \leq 375$

(3) $n_5(5,d)$=$g_5(5,d)$ or $g_5(5,d)+1$ for

$d \in \{$376-393,396,397$\}$

(4) $n_5(5,d) \leq g_5(5,d)+2$ for $d \in \{$131,401-410$\}$

(5) $n_5(5,d)$=$g_5(5,d)+1$ or $g_5(5,d)+2$ for

$d \in \{$151-155,301-320,326-345,351-372,411-425,

481-485$\}$.

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*, to appear.

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.

Thank you for your attention!