Constructing new linear codes over the field of order five

Yuto Inoue
(Joint work with Tatsuya Maruta)

Department of Mathematical Sciences
Osaka Prefecture University

Contents

1. Optimal linear codes problem

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

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

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

$$wt(\boldsymbol{a}) = |\{i \mid a_i \neq 0\}|$$

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

$$d = \min\{wt(a) \mid a \in \mathcal{C},\ a \neq \mathbf{0}\}.$$

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 of $\mathcal{C}$.

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

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

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

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

Known results for $q = 5$, $k = 5$

It is known that

$$n_5(5, d) = g_5(5, d) \text{ for } d \geq 1376.$$

For $1 \leq d \leq 1375$, $n_5(5, d)$ is detemined for 655 values of d but not for 725 values of d, see

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

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

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

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

Assume that G contains no all-zero-column.

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 Σ

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 $\mathcal{C}$.

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

3. Projective dual

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

Ex. 1. There exists a 3-div $[41, 4, 33]_9$ code with w.d. $0^1 33^{984} 36^{3608} 39^{1968}$. The spectrum is $(a_2, a_5, a_8) = (246, 451, 123)$.

Lemma 1. (Projective dual)

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

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

$$\bigcap_{H:\ i\text{-hyperplane},\ i<n-d} H = \emptyset$$

$\Rightarrow {}^{\exists}\mathcal{C}^*$: 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 $\mathcal{C}^*$ 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.

$\mathcal{C}$ 3-div $[41, 4, 33]_9$

with spec. $(a_2, a_5, a_8) = (246, 451, 123)$

$\downarrow$ projetive dual

$\mathcal{C}^*$ 27-div $[943, 4, 837]_9$ $(n^* = 2a_2 + a_5)$

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 $\Sigma = \mathrm{PG}(k-1, q)$ 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 $d > q^t$
$\Rightarrow$ $\exists \mathcal{C}'$: $[n - \theta_t, k, d']_q$ code, for $d' \geq d - q^t$.

5. Construction of new codes

Lemma 3. There exist $[1126, 5, 900]_5$, $[1120, 5, 895]_5$, $[1114, 5, 890]_5$, $[1108, 5, 885]_5$, $[1102, 5, 880]_5$ codes.

Proof.

$\mathcal{C}_1$: the code with generator matrix

$$G_1 = \begin{bmatrix} 1111000003342334222344243011111 \\ 0000100024033413331433322111111 \\ 0000010022404243443421414411111 \\ 0000001001220122414222332111111 \\ 0000000110111111111111111411111 \end{bmatrix}$$

Then $\mathcal{C}_1$ is a 5-div $[34, 5, 20]_5$ code with spectrum $(a_4, a_9, a_{14}) = (410, 306, 65)$.

As a projective dual, we get a $[1126, 5, 900]_5$ code $\mathcal{C}_1^*$ with w.d. $0^1 900^{3016} 925^{100} 1000^4 1025^4$.

The multiset for $\mathcal{C}_1^*$ has four lines

$$l_1 = \langle 10000, 00110 \rangle,\ l_2 = \langle 11000, 10110 \rangle,$$

$$l_3 = \langle 31000, 00210 \rangle,\ l_4 = \langle 41000, 10210 \rangle.$$

Hence, we get

$$[1120, 5, 895]_5,\ [1114, 5, 890]_5,$$

$$[1108, 5, 885]_5,\ [1102, 5, 880]_5$$

codes by geometric puncturing. □

Lemma 4. There exist $[1626, 5, 1300]_5$, $[1620, 5, 1295]_5$, $[1614, 5, 1290]_5$, $[1608, 5, 1285]_5$, $[1602, 5, 1280]_5$ codes.

Proof.

$\mathcal{C}_2$: the code with generator matrix

$$G_2 = \begin{bmatrix} 11110000111311132213331322220000100000 \\ 00001000200320134033102311112222011111 \\ 00000100120012032404310111114444044444 \\ 00000010012011201220132011113333011111 \\ 00000001001101110111011111111111044444 \end{bmatrix}$$

Then $\mathcal{C}_2$ is a 5-div $[38, 5, 20]_5$ code with spectrum $(a_3, a_8, a_{13}, a_{18}) = (256, 362, 134, 29)$.

As a projective dual, we get a $[1626, 5, 1300]_5$ code $\mathcal{C}_2^*$ with w.d. $0^1 1300^{3028} 1325^{80} 1400^8 1425^8$.

The multiset for $\mathcal{C}_2^*$ has four lines

$$l_1 = \langle 10000, 01000 \rangle,\ l_2 = \langle 00100, 00010 \rangle,$$

$$l_3 = \langle 10100, 11010 \rangle, l_4 = \langle 20100, 02010 \rangle.$$

Hence, we get

$$[1620, 5, 1295]_5,\ [1614, 5, 1290]_5,$$

$$[1608, 5, 1285]_5,\ [1602, 5, 1280]_5$$

codes by geometric puncturing. □

Remark.

The matrices G_1 and G_2 are found as multsets in PG$(4, 5)$ by prescribing the group generated by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

i.e., the multiset consisting of the columns of G_i is the union of some orbits of the projectivity τ on PG$(4, 5)$ with $\tau : (x_1, x_2, x_3, x_4, x_5) \rightarrow (x_1, x_5, x_2, x_3, x_4)$.

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

We determined $n_5(5, d)$ for 50 values of d.

Theorem 5. $n_5(5, d) = g_5(5, d)$
for $876 \leq d \leq 900$ and $1276 \leq d \leq 1300$.

Note.
The problem to determine $n_5(5, d)$ for all d is still open for 675 values of d, some of which are solved in the next talk by Kuranaka.

References

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

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.

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/`

Thank you for your attention!