Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 107-112*

New 5-dimensional linear codes over $\mathbb{F}_5$ [1]

Yuuki Kageyama st301011@mi.s.osakafu-u.ac.jp
Tatsuya Maruta maruta@mi.s.osakafu-u.ac.jp
Department of Mathematics and Information Sciences
Osaka Prefecture University, Sakai, Osaka 599-8531, Japan

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. We construct a lot of new $[n, 5, d]_5$ codes to determine the exact value of $n_5(5, d)$ or to improve the known upper bound on $n_5(5, d)$, where $n_q(k, d)$ is the minimum length n for which an $[n, k, d]_q$ code exists.

1 Introduction

Let $\mathbb{F}_q^n$ denote the vector space of n-tuples over $\mathbb{F}_q$, the field of q elements. An $[n, k, d]_q$ code $\mathcal{C}$ is a linear code of length n, dimension k and minimum Hamming distance d over $\mathbb{F}_q$. The weight distribution of $\mathcal{C}$ is the list of numbers A_i which is the number of codewords of $\mathcal{C}$ with weight i. The weight distribution with $(A_0, A_d, ...) = (1, \alpha, ...)$ is also expressed as $0^1 d^\alpha \cdots$. A fundamental problem in coding theory is to find $n_q(k, d)$, the minimum length n for which an $[n, k, d]_q$ code exists ([2]). There is a natural lower bound on $n_q(k, d)$, the so-called Griesmer bound: $n_q(k, d) \geq g_q(k, d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$, where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. The values of $n_q(k, d)$ are determined for all d only for some small values of q and k. For linear codes over $\mathbb{F}_5$, $n_5(k, d)$ is known for $k \leq 4$ for all d except the four cases $d = 81, 82, 161, 162$ for $k = 4$. As for the case $k = 5$, the value of $n_5(5, d)$ is unknown for many integer d, see [5] and [7]. In this paper, we construct new codes to determine $n_5(5, d)$ for some open cases for $d \leq 625$.

Theorem 1. (1) *There exist* $[g_5(5, d)+1, 5, d]_5$ *codes for* $d = 300, 350, 380, 385, 390, 395, 400, 430, 435, 440, 445, 450, 455, 460, 465, 470, 475.$
(2) *There exist* $[g_5(5, d) + 2, 5, d]_5$ *codes for* $d = 131, 155, 281, 287, 305, 310, 315, 320, 330, 335, 340, 355, 360, 365, 370, 375, 405, 410, 415, 420, 425, 485.$

Corollary 2. (1) $n_5(5, d) = g_5(5, d)+1$ *for* $d \in \{296\text{-}300, 346\text{-}350, 394, 395, 398\text{-}400, 426\text{-}475\}$.
(2) $n_5(5, d) = g_5(5, d) + 2$ *for* $373 \leq d \leq 375$.

[1] This research is partially supported by Grant-in-Aid for Scientific Research of Japan Society for the Promotion of Science under Contract Number 24540138.

(3) $n_5(5,d) = g_5(5,d)$ *or* $g_5(5,d)+1$ *for* $376 \le d \le 393$.
(4) $n_5(5,d) = g_5(5,d)+1$ *or* $g_5(5,d)+2$ *for* $d \in \{151\text{-}155, 301\text{-}320, 326\text{-}340, 351\text{-}372, 411\text{-}425, 481\text{-}485\}$.

2 Construction methods

We denote by $\mathrm{PG}(r,q)$ the projective geometry of dimension r over $\mathbb{F}_q$. The 0-flats, 1-flats, 2-flats, 3-flats, $(r-2)$-flats and $(r-1)$-flats are called *points, lines, planes, solids, secundums* and *hyperplanes* respectively. We denote by $\mathcal{F}_j$ the set of j-flats of $\mathrm{PG}(r,q)$ and by θ_j the number of points in a j-flat, i.e. $\theta_j = (q^{j+1}-1)/(q-1)$.

Let $\mathcal{C}$ be an $[n,k,d]_q$ code having no coordinate which is identically zero. The columns of a generator matrix of $\mathcal{C}$ can be considered as a multiset of n points in $\Sigma = \mathrm{PG}(k-1,q)$ denoted also by $\mathcal{C}$. We see linear codes from this geometrical point of view. An *i-point* is a point of Σ which has multiplicity i in $\mathcal{C}$. Denote by γ_0 the maximum multiplicity of a point from Σ in $\mathcal{C}$ and let C_i be the set of i-points in Σ, $0 \le i \le \gamma_0$. For any subset S of Σ we define *the multiplicity of S with respect to* $\mathcal{C}$, denoted by $m_{\mathcal{C}}(S)$, as $m_{\mathcal{C}}(S) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|$, where $|T|$ denotes the number of elements in a set T. A line l with $t = m_{\mathcal{C}}(l)$ is called a *t-line*. A *t-plane*, a *t-solid* and so on are defined similarly. Then we obtain the partition $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ such that $n = m_{\mathcal{C}}(\Sigma)$ and $n-d = \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}$. Such a partition of Σ is called an $(n,n-d)$-*arc* of Σ. Conversely an $(n,n-d)$-arc of Σ gives an $[n,k,d]_q$ code in the natural manner. Denote by a_i the number of i-hyperplanes in Σ. The list of the values a_i is called the *spectrum* of $\mathcal{C}$. Note that $a_i = A_{n-i}/(q-1)$ for $0 \le i \le n-d$.

For a non-zero element $\alpha \in \mathbb{F}_q$, let $R = \mathbb{F}_q[x]/(x^N - \alpha)$ be the ring of polynomials over $\mathbb{F}_q$ modulo $x^N - \alpha$. We associate the vector $(a_0, a_1, ..., a_{N-1}) \in \mathbb{F}_q^N$ with polynomial $a(x) = \sum_{i=0}^{N-1} a_i x^i \in R$. For $\mathbf{g} = (g_1(x), \cdots, g_s(x)) \in R^s$,

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

is called the 1-*generator quasi-twisted* (QT) *code* with generator $\mathbf{g}$. $C_{\mathbf{g}}$ is usually called *quasi-cyclic* (QC) when $\alpha = 1$. $C_{\mathbf{g}}$ is also called *degenerate* if $g_1(x), \cdots, g_s(x)$ have a common factor dividing $x^N - \alpha$. When $s = 1$, $C_{\mathbf{g}}$ is called *pseudo-cyclic* or *constacyclic*. All of these codes are generalizations of cyclic codes ($\alpha = 1$, $s = 1$). Take a monic polynomial $g(x) = x^k - \sum_{i=0}^{k-1} a_i x^i$ in $\mathbb{F}_q[x]$ dividing $x^N - \alpha$ with non-zero $\alpha \in \mathbb{F}_q$, and let T be the companion matrix of $g(x)$. Let τ be the projectivity of $\mathrm{PG}(k-1,q)$ defined by T. We denote by $[g^n]$ or by $[a_0 a_1 \cdots a_{k-1}^n]$ the $k \times n$ matrix $[P, TP, T^2P, ..., T^{n-1}P]$, where P is the column vector $(1,0,0,\cdots,0)^{\mathrm{T}}$ (h^{T} stands for the transpose of a row vector h). Then $[g^N]$ generates an α^{-1}-cyclic code. Hence one can construct a cyclic or pseudo-cyclic code from an orbit of τ. We denote the matrix

$$[P, TP, T^2P, ..., T^{n_1-1}P; P_2, TP_2, ..., T^{n_2-1}P_2; \cdots; P_s, TP_s, ..., T^{n_s-1}P_s]$$

by $[g^{n_1}] + P_2^{n_2} + \cdots + P_s^{n_s}$. Then, the matrix $[g^N] + P_2^N + \cdots + P_s^N$ defined from s orbits of τ of length N generates a QC or QT code, see [8]. It is shown in [8] that many good codes can be constructed from orbits of projectivities.

An $[n,k,d]_q$ code is called *m-divisible* if all codewords have weights divisible by an integer $m > 1$. It sometimes happens that QC or QT codes are divisible or can be extended to divisible codes.

Lemma 1 ([9]). *Let $\mathcal{C}$ be an m-divisible $[n,k,d]_q$ code with $q = p^h$, p prime, whose spectrum is*

$$(a_{n-d-(w-1)m}, a_{n-d-(w-2)m}, \cdots, a_{n-d-m}, a_{n-d}) = (\alpha_{w-1}, \alpha_{w-2}, \cdots, \alpha_1, \alpha_0),$$

where $m = p^r$ for some $1 \le r < h(k-2)$ satisfying $\lambda_0 > 0$. Then there exists a t-divisible $[n^*, k, d^*]_q$ code $\mathcal{C}^*$ with $t = q^{k-2}/m$, $n^* = \sum_{j=0}^{w-1} j\alpha_j = ntq - \frac{d}{m}\theta_{k-1}$, $d^* = n^* - nt + \frac{d}{m}\theta_{k-2} = ((n-d)q - n)t$ whose spectrum is

$$(a_{n^*-d^*-\gamma_0 t}, a_{n^*-d^*-(\gamma_0-1)t}, \cdots, a_{n^*-d^*-t}, a_{n^*-d^*}) = (\lambda_{\gamma_0}, \lambda_{\gamma_0-1}, \cdots, \lambda_1, \lambda_0).$$

Note that 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 $0 \le j \le w-1$ [9]. $\mathcal{C}^*$ is called the *projective dual* of $\mathcal{C}$, see also [1].

Lemma 2 ([6]). *Let $\mathcal{C}$ be an $[n,k,d]_q$ code and let $\cup_{i=0}^{\gamma_0} C_i$ be the partition of $\Sigma = \mathrm{PG}(k-1,q)$ obtained from $\mathcal{C}$. If $\cup_{i\ge 1} C_i$ contains a t-flat Π and if $d > q^t$, then there exists an $[n-\theta_t, k, d-q^t]_q$ code $\mathcal{C}'$.*

$\mathcal{C}'$ in Lemma 2 can be constructed from $\mathcal{C}$ by removing the t-flat Π from the multiset for $\mathcal{C}$. In general, the method to construct new codes from a given $[n,k,d]_q$ code by deleting the coordinates corresponding to some geometric object in $\mathrm{PG}(k-1,q)$ is called *geometric puncturing*, see [4].

3 Proof of Theorem 1

Lemma 3. *There exist QC codes with parameters* $[169,5,131]_5$ *and* $[198,5,155]_5$.

Proof. See Table 1. □

Table 1. Generator matrices of QC codes in Lemma 3

parameters	generator matrix
$[169,5,131]_5$	$[10320^{13}] + 11000^{13} + 31000^{13} + 21100^{13} + 23100^{13} + 34100^{13}$ $+32010^{13} + 31110^{13} + 12110^{13} + 42110^{13} + 12210^{13} + 22210^{13}$ $+21310^{13}$
$[198,5,155]_5$	$[12411^{11}] + 11000^{11} + 31000^{11} + 10100^{11} + 31100^{11} + 30010^{11}$ $+31010^{11} + 22010^{11} + 14010^{11} + 44110^{11} + 30210^{11} + 43210^{11}$ $+34210^{11} + 12310^{11} + 13310^{11} + 41101^{11} + 32201^{11} + 33011^{11}$

Lemma 4. *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. Let $\mathcal{C}_1$ be the $[53,5,40]_5$ code with generator matrix

$$G_1 = \begin{bmatrix} 00011111110001111111001111111100111111110011111111110 \\ 11111133441111113344111233333441111114444111233333344000 \\ 01101304040240141234241013340413114400220323011401241 \\ 00110100440100110044444421213333333332222444411223300 0 \\ 40444310243122104020113200044010132404343303431121042 \end{bmatrix},$$

which is from [3]. Then $\mathcal{C}_1$ has weight distribution $0^1 40^{1720} 45^{1300} 50^{104}$. Applying Lemma 1, as the projective dual of $\mathcal{C}_1$, one can get a $[377,5,300]_5$ code $\mathcal{C}_1^*$ with generator matrix G_1^* whose weight distribution is $0^1 300^{2912} 325^{212}$.
Let $\mathcal{C}_2$ be the $[26,4,20]_5$ code with generator matrix

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

Then $\mathcal{C}_2$ has weight distribution $0^1 20^{520} 25^{104}$. Now, let Π be the hyperplane $\langle 10000, 00100, 00010, 02001 \rangle = V(3x_1 - x_4)$, where $x_0 x_1 \cdots x_4$ stands for the point $\mathbf{P}(x_0, x_1 \cdots, x_4)$ of $\Sigma = \mathrm{PG}(4,5)$ represented by a vector $(x_0, x_1 \cdots, x_4)$. 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

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

Let $\bar{G}_2$ be the 26-set in PG(3,5) defined by the columns of G_2, and let $G_2^{'}$ be the matrix whose columns consist of the image of $\bar{G}_2$ by φ. Then

$$G_2^{'} = \begin{bmatrix} 00142332410014014410232332 \\ 00002222222222222222002222 \\ 10111144444231113322444332 2 \\ 01111144221433211443112233 \\ 00001111111111111111001111 \end{bmatrix}.$$

Let $\mathcal{C}_2^{'}$ and $\mathcal{C}$ be the codes generated by $[G_2^{'}]$ and $[G_1^*, G_2^{'}]$, respectively. Then $\mathcal{C}$ is a $[403,5,d]_5$ code. Since $m_{\mathcal{C}_1^*}(\Pi) = 52$ and $m_{\mathcal{C}_2^{'}}(\Pi) = 26$, we have $m_{\mathcal{C}}(\Pi) = 78$. It follows from $\max\{m_{\mathcal{C}_1^*}(\pi) \mid \pi \in \mathcal{F}_{k-2} \setminus \Pi\} = 77$ and $\max\{m_{\mathcal{C}_2^{'}}(\pi) \mid \pi \in \mathcal{F}_{k-2} \setminus \Pi\} = 6$ that $\max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2} \setminus \Pi\} = 83$. Thus $d = n - \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\} = 403 - 83 = 320$. Hence, $\mathcal{C}$ is a $[403,5,320]_5$ code. It can be checked that the multiset for $\mathcal{C}$ has mutually disjoint three lines $\langle 12100, 31011 \rangle$, $\langle 42100, 01021 \rangle$, $\langle 23100, 23021 \rangle$. Hence, we get $[385,5,305]_5$, $[391,5,310]_5$, $[397,5,315]_5$ codes by deleting the lines (Lemma 2). □

Lemma 5. *There exist* $[416, 5, 330]_5$*,* $[422, 5, 335]_5$ *and* $[428, 5, 340]_5$ *codes.*

Proof. Let $\mathcal{C}$ be the $[66, 5, 50]_5$ code with generator matrix $G = [12411^{11}] + 11000^{11} + 41100^{11} + 21010^{11} + 30210^{11} + 22310^{11}$. Then $\mathcal{C}$ has weight distribution $0^1 50^{1584} 55^{1320} 60^{220}$. Applying Lemma 1, as the projective dual of $\mathcal{C}$, one can get a $[440, 5, 350]_5$ code $\mathcal{C}^*$ with weight distribution $0^1 350^{2860} 375^{264}$. It can be checked that the multiset for $\mathcal{C}^*$ has mutually disjoint four lines

$$\langle 20100, 21011\rangle, \ \langle 31100, 43021\rangle, \ \langle 13100, 11011\rangle, \ \langle 02010, 40201\rangle.$$

Hence, we get $[416, 5, 330]_5$, $[422, 5, 335]_5$, $[428, 5, 340]_5$ codes by Lemma 2. □

Table 2. Projective duals

$\mathcal{C}$	$\mathcal{C}^*$
5-divisible $[41, 5, 30]_5$	25-divisible $[439, 5, 350]_5$
5-divisible $[60, 5, 45]_5$	25-divisible $[471, 5, 375]_5$
5-divisible $[54, 5, 40]_5$	25-divisible $[502, 5, 400]_5$
5-divisible $[73, 5, 55]_5$	25-divisible $[534, 5, 425]_5$
5-divisible $[42, 5, 30]_5$	25-divisible $[564, 5, 450]_5$

A $[439, 5, 350]_5$ code can be constructed as the projective dual of a known 5-divisible $[41, 5, 30]_5$ code (Table 2). The following four lemmas can be obtained from the $[471, 5, 375]_5$, $[502, 5, 400]_5$, $[534, 5, 425]_5$ and $[564, 5, 450]_5$ codes in Table 2, respectively, by deleting some lines from the multiset for $\mathcal{C}^*$ as puncturing. The codes for $\mathcal{C}$ in Table 2 are from [3].

Lemma 6. *There exist* $[g_5(5, d) + 2, 5, d]_5$ *codes for* $d = 355, 360, 365, 370$.

Lemma 7. *There exist* $[g_5(5, d) + 1, 5, d]_5$ *codes for* $d = 380, 385, 390, 395$.

Lemma 8. *There exist* $[g_5(5, d) + 2, 5, d]_5$ *codes for* $d = 405, 410, 415, 420$.

Lemma 9. *There exist* $[g_5(5, d) + 1, 5, d]_5$ *codes for* $d = 430, 435, 440, 445$.

Lemma 10. *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. Let $\mathcal{C}$ be the $[36, 5, 25]_5$ code with generator matrix $G = [10000^5] + 11000^5 + 34100^5 + 11310^5 + 33410^5 + 31411^5 + 24121^5 + 11111$. Then $\mathcal{C}$ has weight distribution $0^1 25^{804} 30^{2260} 35^{60}$. Applying Lemma 1, as the projective dual of $\mathcal{C}$, one can get a $[595, 5, 475]_5$ code $\mathcal{C}^*$ with weight distribution $0^1 475^{2980} 500^{144}$. It can be checked that the multiset for $\mathcal{C}^*$ has mutually disjoint four lines

$$\langle 10100, 22011\rangle, \ \langle 30100, 23011\rangle, \ \langle 21100, 20011\rangle, \ \langle 31100, 11011\rangle.$$

Hence, we get $[571, 5, 455]_5$, $[577, 5, 460]_5$, $[583, 5, 465]_5$, $[589, 5, 470]_5$ codes by deleting the lines from the multiset for $\mathcal{C}^*$ as puncturing. □

Lemma 11. *There exist* $[609, 5, 485]_5$ *code.*

Proof. Let $\mathcal{C}$ be the $[55, 5, 40]_5$ code with generator matrix $G = [12411^{11}] + 11000^{11} + 20100^{11} + 31100^{11} + 40010^{11}$. Then $\mathcal{C}$ has weight distribution $0^1 40^{880} 45^{1980} 50^{264}$. Applying Lemma 1, as the projective dual of $\mathcal{C}$, one can get a $[627, 5, 500]_5$ code $\mathcal{C}^*$ with weight distribution $0^1 500^{2904} 525^{220}$. It can be checked that the multiset for $\mathcal{C}^*$ has mutually disjoint three lines

$$\langle 30100, 33010\rangle,\ \langle 11100, 30010\rangle,\ \langle 21100, 31001\rangle.$$

Hence, we get $[609, 5, 485]_5$ codes by deleting the three lines from the multiset for $\mathcal{C}^*$ as puncturing. □

References

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

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

[3] A. Kohnert, Best linear codes, `http://www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/Linear_Codes_BKW/index.html`.

[4] T. Maruta, Construction of optimal linear codes by geometric puncturing, *Serdica J. Computing*, to appear.

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

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

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

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

[9] M. Takenaka, K. Okamoto, T. Maruta, On optimal non-projective ternary linear codes, *Discrete Math.,* **308**, 842–854, 2008.