Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 277–282*

New 4-dimensional linear codes over $\mathbb{F}_9$ [1]

TSUKASA OKAZAKI su301006@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

Abstract. We construct a lot of new $[n, 4, d]_9$ codes to determine the exact value of $n_9(4, d)$ or to give new upper bounds on $n_9(4, d)$, where $n_q(k, d)$ is the minimum length n for which an $[n, k, d]_q$ code exists. Some 3-divisible codes over $\mathbb{F}_9$ are constructed from some orbits of a projectivity.

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 ([4]). There is a natural lower bound on $n_q(k, d)$ called the 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, see [11]. For linear codes over $\mathbb{F}_9$, $n_9(k, d)$ is known for all d for $k \leq 3$. As for the case $k = 4$, the value of $n_9(4, d)$ is unknown for many integer d. It is already known that $n_9(4, d) = g_9(4, d)$ for $d \in \{1\text{-}7, 10\text{-}12, 19, 28\text{-}30, 64\text{-}72, 568\text{-}576, 640\text{-}801, 1054\text{-}1080\}$ and for all $d > 1215$, and that $n_9(4, d) = g_9(4, d) + 1$ for $\in \{8, 9, 17, 18, 25\text{-}27, 34, 61\text{-}63, 73\text{-}80, 141\text{-}144, 559\text{-}562, 593, 594, 602, 603, 622\text{-}639, 1194\text{-}1215\}$, see [1], [3], [7], [8], [10]. We note that $n_9(4, d) \leq g_9(4, d) + 1$ for $577 \leq d \leq 621$ and $1135 \leq d \leq 1193$, see Lemma 3.5 in [7] and Corollary 11 in [5]. See also [9] and [6] for the nonexistence of Griesmer codes of dimension 4. In this paper, we construct new codes to determine $n_9(4, d)$ for $d \leq 1193$.

Theorem 1. (1) *There exist $[g_9(4, d), 4, d]_9$ codes for $d = 819$, 828, 837, 900, 909, 918, 981, 990, 999.*

[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.

(2) *There exist* $[g_9(4,d)+1,4,d]_9$ *codes for* $d =$ 180, 810, 846, 855, 864, 873, 882, 891, 927, 936, 945, 954, 963, 972, 1008, 1017, 1026, 1035, 1044, 1053, 1089, 1098, 1107, 1116, 1125, 1134.

Corollary 2. (1) $n_9(4,d) = g_9(4,d)$ *for* $d \in \{811\text{-}837, 892\text{-}918, 973\text{-}999\}$.

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

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

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 and $(r-1)$-flats are called *points, lines, planes* 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* 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 $(a_0,a_1,\ldots,a_{N-1}) \in \mathbb{F}_q^N$ 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 $[a_0a_1\cdots a_{k-1}^n]$ 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 [13]. It is shown in [13] 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 codes defined by some orbits of a projectivity like QC or QT codes are divisible codes.

Lemma 3 ([14]). *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

$$(a_{n^*-d^*-\gamma_0t},a_{n^*-d^*-(\gamma_0-1)t},\cdots,a_{n^*-d^*-t},a_{n^*-d^*})=(\lambda_{\gamma_0},\lambda_{\gamma_0-1},\cdots,\lambda_1,\lambda_0).$$

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 $0\le j\le w-1$ [14]. $\mathcal{C}^*$ is called the *projective dual* of $\mathcal{C}$, see also [2].

Lemma 4 ([12]). *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 $\cup_{i\ge1}C_i$ contains a t-flat Π and if $d>q^t$, then an $[n-\theta_t,k,d']_q$ code $\mathcal{C}'$ with $d'\ge d-q^t$ exists.*

The code $\mathcal{C}'$ in Lemma 4 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 [10].

3 Proof of Theorem 1

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

Lemma 5. *There exists a QT $[205,4,180]_9$ code.*

Proof. Let $\mathcal{C}$ be the QT $[205,4,180]_9$ code with generator matrix $G=[1218^{41}]+6100^{41}+3210^{41}+3310^{41}+7310^{41}$, where 1218 defines the polynomial $x^4-(1+2x+x^2+8x^3)$ and 6100 stands for the point $\mathbf{P}(6,1,0,0)$ in $\mathrm{PG}(3,9)$. Then $\mathcal{C}$ has weight distribution $0^1 180^{4920} 189^{1640}$. □

Lemma 6. *There exist* $[913,4,810]_9$*,* $[923,4,819]_9$*,* $[933,4,828]_9$ *and* $[943,4,837]_9$ *codes.*

Proof. Let $\mathcal{C}$ be the extended QC $[41,4,33]_9$ code with generator matrix $G=[1000^4]+7211^4+1116^4+1574^4+1376^4+1507^4+1247^4+1426^4+1237^4+1860^4+1515^1$. Then $\mathcal{C}$ has weight distribution $0^1 33^{984} 36^{3608} 39^{1968}$. Applying Lemma 3, as the projective dual of $\mathcal{C}$, one can get a $[943,4,837]_9$ code $\mathcal{C}^*$ with weight distribution $0^1 837^{6232} 864^{328}$. It can be checked that the multiset for $\mathcal{C}^*$ has three mutually disjoint lines $\langle 1000,1018\rangle$, $\langle 1002,1102\rangle$, $\langle 1003,1114\rangle$, where $x_0x_1\cdots x_3$ stands for the point $\mathbf{P}(x_0,x_1\cdots,x_3)$ of $\Sigma=\mathrm{PG}(3,9)$ and $\langle P,Q\rangle$ stands for the line through the points P and Q in Σ. Hence, we get $[913,4,810]_9$, $[923,4,819]_9$ and $[933,4,828]_9$ codes by Lemma 4. □

Lemma 7. *There exist* $[954,4,846]_9$*,* $[964,4,855]_9$*,* $[974,4,864]_9$*,* $[984,4,873]_9$*,* $[994,4,882]_9$*,* $[1004,4,891]_9$*,* $[1014,4,900]_9$*,* $[1024,4,909]_9$ *and* $[1034,4,918]_9$ *codes.*

Proof. Let $\mathcal{C}$ be the $[38,4,30]_9$ 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 $\mathbf{P}(1,5,1,5)$ and $\mathbf{P}(1,3,5,7)$ are fixed points under the projectivity defined by the companion matrix of x^4-1. Then $\mathcal{C}$ has weight distribution $0^1 30^{672} 33^{3504} 36^{2384}$. Applying Lemma 3, as the projective dual of $\mathcal{C}$, one can get a $[1034,4,918]_9$ code $\mathcal{C}^*$ with weight distribution $0^1 918^{6256} 945^{304}$. It can be checked that the multiset for $\mathcal{C}^*$ has eight mutually disjoint lines $\langle 1000,1103\rangle$, $\langle 1002,1111\rangle$, $\langle 1003,1017\rangle$, $\langle 1005,1121\rangle$, $\langle 1006,1132\rangle$, $\langle 1007,1140\rangle$, $\langle 1008,1150\rangle$, $\langle 1010,1105\rangle$. So, we get $[954,4,846]_9$, $[964,4,855]_9$, $[974,4,864]_9$, $[984,4,873]_9$, $[994,4,882]_9$, $[1004,4,891]_9$, $[1014,4,900]_9$ and $[1024,4,909]_9$ codes by Lemma 4. □

Lemma 8. *There exist* $[1045,4,927]_9$*,* $[1055,4,936]_9$*,* $[1065,4,945]_9$*,* $[1075,4,954]_9$*,* $[1085,4,963]_9$*,* $[1095,4,972]_9$*,* $[1105,4,981]_9$*,* $[1115,4,990]_9$ *and* $[1125,4,999]_9$ *codes.*

Proof. Let $\mathcal{C}$ be the $[35,4,27]_9$ 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. Then $\mathcal{C}$ has weight distribution $0^1 27^{440} 30^{3240} 33^{2880}$. Applying Lemma 3, as the projective dual of $\mathcal{C}$, one can get a $[1125,4,999]_9$ code $\mathcal{C}^*$ with weight distribution $0^1 999^{6280} 1026^{280}$. It can be checked that the multiset for $\mathcal{C}^*$ has eight mutually disjoint 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 $[1045, 4, 927]_9$, $[1055, 4, 936]_9$, $[1065, 4, 945]_9$, $[1075, 4, 954]_9$, $[1085, 4, 963]_9$, $[1095, 4, 972]_9$, $[1105, 4, 981]_9$ and $[1115, 4, 990]_9$ codes by Lemma 4. □

Lemma 9. *There exist* $[1136, 4, 1008]_9$, $[1146, 4, 1017]_9$, $[1156, 4, 1026]_9$, $[1166, 4, 1035]_9$, $[1176, 4, 1044]_9$, $[1186, 4, 1053]_9$, $[1257, 4, 1116]_9$, $[1267, 4, 1125]_9$ *and* $[1277, 4, 1134]_9$ *codes.*

Proof. Let $\mathcal{C}$ be the $[39, 4, 30]_9$ 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 a fixed point under the projectivity defined by the companion matrix of $x^4 - 1$. Then $\mathcal{C}$ has weight distribution $0^1 30^{272} 33^{2616} 36^{3416} 39^{256}$. Applying Lemma 3, as the projective dual of $\mathcal{C}$, one can get a $[1277, 4, 1134]_9$ code $\mathcal{C}^*$ with weight distribution $0^1 1134^{6248} 1161^{312}$. It can be checked that the multiset for $\mathcal{C}^*$ contains one plane $\delta = \langle 1004, 1018, 1118\rangle$, which is a 143-plane. Moreover, $\mathcal{C}^*$ contains five mutually disjoint lines $\langle 1000, 1015\rangle$, $\langle 1002, 1103\rangle$, $\langle 1003, 1110\rangle$, $\langle 1005, 1120\rangle$, $\langle 1006, 1140\rangle$, each of which meets δ in a 2-point. Hence, we get $[1136, 4, 1008]_9$, $[1146, 4, 1017]_9$, $[1156, 4, 1026]_9$, $[1166, 4, 1035]_9$, $[1176, 4, 1044]_9$, $[1186, 4, 1053]_9$ codes by Lemma 4. On the other hand, $\mathcal{C}^*$ has two mutually disjoint lines $\langle 1000, 1015\rangle$ and $\langle 1002, 1102\rangle$. Hence, we also get $[1257, 4, 1116]_9$ and $[1267, 4, 1125]_9$ codes by Lemma 4. □

Lemma 10. *There exist* $[1227, 4, 1089]_9$, $[1237, 4, 1098]_9$ *and* $[1247, 4, 1107]_9$ *codes.*

Proof. Let $\mathcal{C}$ be the QT $[49, 4, 39]_9$ code with generator matrix $G = [1131^7] + 1000^7 + 1402^7 + 1846^7 + 1407^7 + 1445^7 + 1705^7$. Then $\mathcal{C}$ has weight distribution $0^1 39^{784} 42^{2136} 45^{3080} 48^{560}$. Applying Lemma 3, as the projective dual of $\mathcal{C}$, one can get a $[1247, 4, 1107]_9$ code $\mathcal{C}^*$ with weight distribution $0^1 1107^{6224} 1134^{280} 1161^{56}$. It can be checked that the multiset for $\mathcal{C}^*$ has two mutually disjoint lines $\langle 1000, 1111\rangle$, $\langle 1003, 1126\rangle$. Hence, we get $[1227, 4, 1089]_9$ and $[1237, 4, 1098]_9$ codes by Lemma 4. □

References

[1] Bayreuth Research Group, Best linear codes, `http://www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/Linear_Codes_BKW/index.html`.

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

[3] M. Grassl, Linear code bound [electronic table; online], `http://www.codetables.de/`.

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

[5] Y. Kageyama and T. Maruta, On the construction of optimal codes over $\mathbb{F}_q$, preprint.

[6] R. Kanazawa, On the minimum length of linear codes of dimension 4, MSc Thesis, Osaka Prefecture Univ., 57pp, 2011.

[7] R. Kanazawa, T. Maruta, On optimal linear codes over $\mathbb{F}_8$, *Electron. J. Combin.*, **18**, #P34, 27pp, 2011.

[8] K. Kumegawa and T. Maruta, Nonexistence of some Griesmer codes of dimension 4 over $\mathbb{F}_q$, Proc. 14th International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk, Russia, 2014, submitted.

[9] T. Maruta, On the minimum length of q-ary linear codes of dimension four, *Discrete Math.* **208/209**, 427–435, 1999.

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

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

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

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

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