Available online at www.sciencedirect.com
SCIENCE DIRECT®
Discrete Mathematics 282 (2004) 233–237
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Note

MDS codes over $\mathbb{F}_9$ related to the ternary Golay code

Makoto Araya[a], Masaaki Harada[b,*]

[a] Department of Computer Science, Shizuoka University, Hamamatsu 432-8011, Japan
[b] Department of Mathematical Sciences, Yamagata University, Yamagata 990-8560, Japan

Received 13 November 2002; received in revised form 31 October 2003; accepted 5 November 2003

Abstract

Goldberg constructed an MDS code over $\mathbb{F}_9$ whose ternary image is the ternary Golay [12, 6, 6] code. Motivated by the work, in this paper, we found all such MDS codes over $\mathbb{F}_9$ under some equivalence.
© 2004 Elsevier B.V. All rights reserved.

Keywords: MDS code; Ternary Golay code; Code over $\mathbb{F}_9$

1. Introduction

An $[n, k]$ code C over $\mathbb{F}_q$ is a k-dimensional vector subspace of $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the finite field of order q and q is a prime power. The elements of C are called codewords. The Hamming weight $\mathrm{wt}_{\mathrm{H}}(x)$ of a codeword x is the number of non-zero coordinates in x. The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0 \text{ for all } y \in C\}$, where $x \cdot y$ denotes the usual inner-product.

Let $\mathbb{F}_3 = \{0, 1, 2\}$ be the finite field of order 3 and let $\mathbb{F}_9 = \mathbb{F}_3[\alpha]/(\alpha^2 + 1)$ be the finite field of order 9. In this paper, we consider codes over $\mathbb{F}_3$ and $\mathbb{F}_9$. Let Q be the set of nonzero squares in $\mathbb{F}_9$, that is, $Q = \{1, 2, \alpha, 2\alpha\}$, and let $N = \{1 + \alpha, 1 + 2\alpha, 2 + \alpha, 2 + 2\alpha\}$. The *Lee weight* $\mathrm{wt}_{\mathrm{L}}(x)$ of a codeword $x = (x_1, x_2, \ldots, x_n)$ is defined as $\#\{i \mid x_i \in Q\} + 2\#\{i \mid x_i \in N\}$. As defined in [4], we consider a map ϕ from $\mathbb{F}_9^n$ to $\mathbb{F}_3^{2n}$ where $\phi(x + \alpha y) = (x, y)$ for $x, y \in \mathbb{F}_3^n$. We say that the image $\phi(C)$ of a code C over $\mathbb{F}_9$ is the *ternary image* of C. The minimum Hamming weight d_{H} (resp. Lee weight d_{L}) of C is the smallest Hamming weight (resp. Lee weight) among all nonzero codewords in C. It is obvious that $\mathrm{wt}_{\mathrm{L}}(x) = \mathrm{wt}_{\mathrm{H}}(\phi(x))$, in addition, if C is an $[n, k]$ code over $\mathbb{F}_9$ with minimum Lee weight d_{L} then $\phi(C)$ is a ternary $[2n, 2k, d_{\mathrm{L}}]$ code where an $[n, k, d]$ code is an $[n, k]$ code with minimum Hamming weight d. An $[n, k, n-k+1]$ code is called MDS (cf. [5]).

It is well-known that the ternary Golay [12, 6, 6] code G_{12} is the unique ternary code with these parameters, under the usual equivalence (see e.g. [5, Chapter 20, Theorem 20]). Goldberg [4] constructed a [6, 3] code $\mathscr{C}$ such that its ternary image $\phi(\mathscr{C})$ is the Golay code G_{12} (see also [1] for other ternary images of larger codes over $\mathbb{F}_9$). This motivates us to consider a classification of such codes, that is, codes C over $\mathbb{F}_9$ with $\phi(C) = G_{12}$. To do this, we consider the following definitions of equivalence of codes over $\mathbb{F}_9$. Let C and C' be codes over $\mathbb{F}_9$. If there is a monomial matrix P over $\mathbb{F}_3$ such that $C = C' \cdot P = \{x \cdot P \mid x \in C'\}$, we say that two codes C and C' are *signed-permutation equivalent* and a monomial matrix P such that $C = C \cdot P$ is called a *signed-permutation automorphism*. The set of signed-permutation automorphisms is called the signed-permutation automorphism group of C. Moreover, if there is a monomial matrix P over $\mathbb{F}_9$ with entries in $\{0, 1, 2, \alpha, 2\alpha\}$ such that $C = C' \cdot P$, we say that C and C' are *α-equivalent* and a monomial matrix P such that $C = C \cdot P$ is said to be an *α-automorphism*. The set of α-automorphisms is said to be the α-automorphism group of C. Obviously, if two codes C and C' are signed-permutation equivalent then they are α-equivalent. Note that the Lee weight of a codeword x is invariant under the α-equivalence.

* Corresponding author. Tel.: +81-236-28-4533; fax: +81-236-28-4538.
E-mail addresses: araya@cs.inf.shizuoka.ac.jp (M. Araya), mharada@sci.kj.yamagata-u.ac.jp, harada@kdw.kj.yamagata-u.ac.jp (M. Harada).

0012-365X/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2003.11.012

In this paper, we give two classifications of codes over $\mathbb{F}_9$ whose ternary images are the Golay codes under the signed-permutation equivalence and the α-equivalence. There are four such $[6,3]$ codes over $\mathbb{F}_9$ under the signed-permutation equivalence and there is a unique such $[6,3]$ code over $\mathbb{F}_9$ under the α-equivalence.

2. Results

Lemma 1. *If C is a code over* $\mathbb{F}_9$ *whose ternary image is the ternary Golay* $[12,6,6]$ *code then C is an MDS* $[6,3,4]$ *code.*

Proof. Let C be a $[6,3,d \leqslant 3]$ code and x be a codeword of Hamming weight at most 3. Then a codeword γx contains 1 in at least one of its coordinates for some $\gamma \in \mathbb{F}_9$. Hence the Lee weight of γx is at most five. □

The converse assertion is not true in general. Consider the code with the following generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 2\alpha+2 & 2\alpha+2 \\ 0 & 1 & 0 & 1 & \alpha+2 & \alpha+1 \\ 0 & 0 & 1 & 1 & \alpha+1 & \alpha+2 \end{pmatrix}.$$

This code is MDS but the ternary image is not the Golay code since it contains a codeword of Lee weight $\leqslant 5$, for example, $\mathrm{wt}_{\mathrm{L}}(r_1+2r_2)=5$ where r_i is the ith row of the generator matrix.

Let C be a $[6,3]$ code over $\mathbb{F}_9$ with $d_{\mathrm{L}}=6$ and generator matrix of the following form

$$\begin{pmatrix} 1 & 0 & 0 & a_1 & a_2 & a_3 \\ 0 & 1 & 0 & a_4 & a_5 & a_6 \\ 0 & 0 & 1 & a_7 & a_8 & a_9 \end{pmatrix}.$$

By Lemma 1, C is a $[6,3,4]$ code. Hence $a_i \neq 0$ for each i. Without loss of generality, we may assume that $(\mathrm{wt}_{\mathrm{L}}(a_1), \mathrm{wt}_{\mathrm{L}}(a_2), \mathrm{wt}_{\mathrm{L}}(a_3)) = (1,2,2)$ and $(\mathrm{wt}_{\mathrm{L}}(a_4), \mathrm{wt}_{\mathrm{L}}(a_5), \mathrm{wt}_{\mathrm{L}}(a_6), \mathrm{wt}_{\mathrm{L}}(a_7), \mathrm{wt}_{\mathrm{L}}(a_8), \mathrm{wt}_{\mathrm{L}}(a_9))=$

(A) $(2,1,2,2,2,1)$,
(B) $(1,2,2,1,2,2)$ or
(C) $(1,2,2,2,1,2)$.

Lemma 2. *Let C be a* $[6,3]$ *code over* $\mathbb{F}_9$ *with generator matrix of type* (B) *or* (C). *Then C has minimum Lee weight* $d_{\mathrm{L}} \leqslant 5$.

Proof. Suppose that C has minimum Lee weight 6. Let r_1 and r_2 be the first and second rows in the generator matrix of C. From our equivalence, we may assume that either $r_1=(1,0,0,1,g_1,g_2)$ and $r_2=(0,1,0,1,g_3,g_4)$ or $r_1=(1,0,0,1,g_1,g_2)$ and $r_2=(0,1,0,\alpha,g_3,g_4)$ where $\mathrm{wt}_{\mathrm{L}}(g_i)=2$ for $i=1,2,3,4$. Consider the first case. Since the codeword $r_1+2r_2=(1,2,0,0,g_1+2g_3,g_2+2g_4)$ has weight $\geqslant 6$, we have $\mathrm{wt}_{\mathrm{L}}(g_1+2g_3)\geqslant 2$ and $\mathrm{wt}_{\mathrm{L}}(g_2+2g_4)\geqslant 2$. Hence $\mathrm{wt}_{\mathrm{L}}(g_1+2g_3)=\mathrm{wt}_{\mathrm{L}}(g_2+2g_4)=2$. Since $\{g_1,g_3\}=\{1+\alpha,2+2\alpha\}$ or $\{1+2\alpha,2+\alpha\}$, the codeword r_1+r_2 has Lee weight at most 5. The later case is similar and $wt_{\mathrm{L}}(r_1+2\alpha r_2)\leqslant 5$. □

Our classification of codes whose ternary images are the Golay code under the signed-permutation equivalence was done as follows. All the computations in this paper were done using GAP [3] or MAGMA [2]. In particular, the computations by GAP were done by considering codes as vector spaces over a finite field. By Lemma 2, we can assume that $(a_1,a_2,a_3)=(1,2+2\alpha,2+2\alpha)$, $(1,2+2\alpha,1+2\alpha)$, $(1,1+2\alpha,1+2\alpha)$, $(\alpha,2+2\alpha,2+2\alpha)$, $(\alpha,2+2\alpha,1+2\alpha)$ or $(\alpha,1+2\alpha,1+2\alpha)$. Then the possibilities of generator matrices are at most 6×4^6 from $a_5,a_9\in Q$ and $a_4,a_6,a_7,a_8\in N$. From the condition that its ternary image is the Golay code, we have found 32 distinct codes for each (a_1,a_2,a_3). So there are 192 distinct codes which must be checked further for signed-permutation equivalence. Then by only permutations of the coordinates, the 32 codes are reduced to twelve for each (a_1,a_2,a_3). Now we have verified that the twelve codes for each (a_1,a_2,a_3) are divided into $4,3,4,3,2$ and 3 codes under the signed-permutation equivalence. Finally, we have verified that each of the 15 codes with $(a_1,a_2,a_3)\neq(1,2+2\alpha,2+2\alpha)$ is equivalent to one of the four codes with $(a_1,a_2,a_3)=(1,2+2\alpha,2+2\alpha)$. Therefore we obtain the following result.

Theorem 3. *There are four codes over $\mathbb{F}_9$ whose ternary images are the ternary Golay code, up to signed-permutation equivalence.*

Let C_i $(i = 1,2,3,4)$ be the code with the generator matrix (I, A_i), where

$$A_1 = \begin{pmatrix} 1 & 2+2\alpha & 2+2\alpha \\ 2+2\alpha & 1 & 2+2\alpha \\ 2+2\alpha & 2+2\alpha & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 2+2\alpha & 2+2\alpha \\ 2+2\alpha & 1 & 2+2\alpha \\ 2+\alpha & 2+\alpha & 2\alpha \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 1 & 2+2\alpha & 2+2\alpha \\ 2+2\alpha & 2 & 1+2\alpha \\ 2+2\alpha & 1+2\alpha & 2 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 1 & 2+2\alpha & 2+2\alpha \\ 2+2\alpha & 2 & 1+2\alpha \\ 2+\alpha & 2+2\alpha & \alpha \end{pmatrix}.$$

Then these four codes C_1, C_2, C_3 and C_4 form the set of the four codes given in the above theorem. Note that C_1 is the same as the code given in [4].

By Theorem in [4], $C_1 \cap C_1^{\perp} = \{0\}$. We have verified that $C_2 \cap C_2^{\perp}$ is a one-dimensional code generated by (111221) and $C_i \cap C_i^{\perp} = \{0\}$ for $i = 3,4$. The orders of the signed-permutation automorphism groups of C_1, C_2, C_3 and C_4 are 120, 20, 8 and 12, respectively. It is easily checked that C_i is signed-permutation equivalent to its dual code $C_i^{\perp}$ for each i.

Permutation-equivalent codes have the identical complete weight enumerators but equivalent codes under the signed-permutation may have different complete weight enumerators. The appropriate weight enumerator for such equivalent codes is the *symmetrized weight enumerator* defined as

$$swe_C(a,b,c,d,e) = \sum_{x \in C} a^{n_0(x)} b^{n_1(x)} c^{n_2(x)} d^{n_3(x)} e^{n_4(x)},$$

where $n_0(x)$ is the number of components 0 of x, $n_1(x)$ is the number of components 1 and 2, $n_2(x)$ is the number of components α and 2α, $n_3(x)$ is the number of components $1+\alpha$ and $2+2\alpha$ and $n_4(x)$ is the number of components $2+\alpha$ and $1+2\alpha$.

We give the symmetrized weight enumerators swe_i of C_i:

$$\begin{aligned} swe_1 = {} & 12de^5 + 12d^5e + 20c^3e^3 + 20c^3d^3 + 60bc^2de^2 + 60bc^2d^2e \\ & + 12bc^5 + 60b^2cde^2 + 60b^2cd^2e + 20b^3e^3 + 20b^3d^3 + 12b^5c \\ & + 60acd^2e^2 + 60abd^2e^2 + 60ab^2c^2e + 60ab^2c^2d + 30a^2c^2e^2 \\ & + 30a^2c^2d^2 + 30a^2b^2e^2 + 30a^2b^2d^2 + a^6, \end{aligned}$$

$$\begin{aligned} swe_2 = {} & 2e^6 + 10d^2e^4 + 10d^4e^2 + 2d^6 + 20c^3de^2 + 20c^3d^2e + 2c^6 \\ & + 20bc^2e^3 + 40bc^2de^2 + 40bc^2d^2e + 20bc^2d^3 + 20b^2ce^3 \\ & + 40b^2cde^2 + 40b^2cd^2e + 20b^2cd^3 + 10b^2c^4 + 20b^3de^2 \\ & + 20b^3d^2e + 10b^4c^2 + 2b^6 + 20acde^3 + 20acd^2e^2 + 20acd^3e \\ & + 20abde^3 + 20abd^2e^2 + 20abd^3e + 20abc^3e + 20abc^3d + 20ab^2c^2e \\ & + 20ab^2c^2d + 20ab^3ce + 20ab^3cd + 10a^2c^2e^2 + 20a^2c^2de \\ & + 10a^2c^2d^2 + 20a^2bce^2 + 20a^2bcd^2 + 10a^2b^2e^2 + 20a^2b^2de \\ & + 10a^2b^2d^2 + a^6, \end{aligned}$$

$$\begin{aligned} swe_3 = {} & 4de^5 + 16d^3e^3 + 4d^5e + 4c^3e^3 + 16c^3de^2 + 16c^3d^2e + 4c^3d^3 \\ & + 16bc^2e^3 + 44bc^2de^2 + 44bc^2d^2e + 16bc^2d^3 + 4bc^5 \\ & + 16b^2ce^3 + 44b^2cde^2 + 44b^2cd^2e + 16b^2cd^3 + 4b^3e^3 \end{aligned}$$

$$+16b^3de^2+16b^3d^2e+4b^3d^3+16b^3c^3+4b^5c+4ace^4$$
$$+16acde^3+20acd^2e^2+16acd^3e+4acd^4+4ac^4e+4ac^4d$$
$$+4abe^4+16abde^3+20abd^2e^2+16abd^3e+4abd^4+16abc^3e$$
$$+16abc^3d+20ab^2c^2e+20ab^2c^2d+16ab^3ce+16ab^3cd$$
$$+4ab^4e+4ab^4d+6a^2c^2e^2+16a^2c^2de+6a^2c^2d^2$$
$$+16a^2bce^2+32a^2bcde+16a^2bcd^2+6a^2b^2e^2+16a^2b^2de+6a^2b^2d^2+a^6,$$

$$\begin{aligned}swe_4 = {} & 12d^2e^4+12d^4e^2+8c^3e^3+12c^3de^2+12c^3d^2e+8c^3d^3\\ & +12bc^2e^3+48bc^2de^2+48bc^2d^2e+12bc^2d^3+12b^2ce^3\\ & +48b^2cde^2+48b^2cd^2e+12b^2cd^3+12b^2c^4+8b^3e^3\\ & +12b^3de^2+12b^3d^2e+8b^3d^3+12b^4c^2+6ace^4+12acde^3\\ & +24acd^2e^2+12acd^3e+6acd^4+6ac^4e+6ac^4d+6abe^4\\ & +12abde^3+24abd^2e^2+12abd^3e+6abd^4+12abc^3e\\ & +12abc^3d+24ab^2c^2e+24ab^2c^2d+12ab^3ce+12ab^3cd\\ & +6ab^4e+6ab^4d+6a^2c^2e^2+12a^2c^2de+6a^2c^2d^2\\ & +12a^2bce^2+48a^2bcde+12a^2bcd^2+6a^2b^2e^2+12a^2b^2de\\ & +6a^2b^2d^2+a^6.\end{aligned}$$

Of course, it holds that $swe_{C_i}(1,y,y,y^2,y^2)=1+264y^6+440y^9+24y^{12}$ for $i=1,2,3,4$.

Now we are in a position to complete the classification of codes given in the above theorem under the α-equivalence. Define the following monomial matrices over $\mathbb{F}_9$:

$$P_2=\begin{pmatrix}1&0&0&0&0&0\\0&0&0&1&0&0\\0&0&0&0&\alpha&0\\0&1&0&0&0&0\\0&0&2&0&0&0\\0&0&0&0&0&1\end{pmatrix},\quad P_3=\begin{pmatrix}0&0&0&1&0&0\\0&\alpha&0&0&0&0\\0&0&0&0&0&\alpha\\0&0&1&0&0&0\\0&0&0&0&\alpha&0\\2\alpha&0&0&0&0&0\end{pmatrix}\quad\text{and}$$

$$P_4=\begin{pmatrix}0&0&0&1&0&0\\0&\alpha&0&0&0&0\\0&0&0&0&0&1\\0&0&1&0&0&0\\0&0&0&0&\alpha&0\\2\alpha&0&0&0&0&0\end{pmatrix}.$$

Then we have

$$C_1=C_2\cdot P_2=C_3\cdot P_3=C_4\cdot P_4.$$

Hence we obtain the following theorem.

Theorem 4. *The code $\mathscr{C}$ given in* [4, Theorem] *is the unique code over $\mathbb{F}_9$ whose ternary image is the ternary Golay code, up to α-equivalence.*

Let H and G be the set of all monomial matrices over $\mathbb{F}_3$ and all monomial matrices over $\mathbb{F}_9$ with entries in $\{0, 1, 2, \alpha, 2\alpha\}$, respectively. It is clear that G forms a group and H is a subgroup of G. Let A be the set of all $[6, 3, 4]$ codes over $\mathbb{F}_9$ whose ternary images are the ternary Golay code. Then the two groups G and H act on A by a left multiplication. We already calculate the order of the stabilizers H_{C_1}, H_{C_2}, H_{C_3} and H_{C_4}, that is, the signed-permutation automorphism groups. By Theorem 3, we have

$$\begin{aligned}|A| &= |C_1^H| + |C_2^H| + |C_3^H| + |C_4^H| \\ &= |H : H_{C_1}| + |H : H_{C_2}| + |H : H_{C_3}| + |H : H_{C_4}| \\ &= 6! \times 2^6/120 + 6! \times 2^6/20 + 6! \times 2^6/8 + 6! \times 2^6/12 = 12288,\end{aligned}$$

where $C_i^H = \{C_i \cdot P \mid P \in H\}$. Hence we obtain the order of the α-automorphism group $G_{\mathscr{C}}$ of $\mathscr{C}$ from Theorem 4 as follows:

$$|G_{\mathscr{C}}| = |G|/|A| = 6! \times 4^6/12288 = 240.$$

Finally, we consider other ternary self-dual codes of lengths up to 12. The numbers of inequivalent ternary self-dual codes of lengths 4,8 and 12 are 1,1 and 3, respectively (cf. [6, Table 1]). The unique code of length 4 (resp. 8) is denoted by E_4 (resp. $2E_4$). The other two codes of length 12 are denoted by $3E_4$ and $4C_3(12)$. Let A be the code over $\mathbb{F}_9$ with generator matrix $(1, 1+\alpha)$. The ternary image of A is E_4. Thus the ternary images of $A \oplus A$ and $A \oplus A \oplus A$ are $2E_4$ and $3E_4$, respectively. In addition, the ternary image of the code with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & \alpha & \alpha & 0 \\ 0 & 1 & 0 & 1+2\alpha & 2+\alpha & 1 \\ 0 & 0 & 1 & 1+2\alpha & 2+\alpha & 2 \end{pmatrix}$$

is $4C_3(12)$. Therefore we have the following:

Proposition 5. *Every ternary self-dual code of length up to* 12 *can be constructed as a ternary image of some code over $\mathbb{F}_9$.*

Acknowledgements

The authors would like to thank the anonymous referees for reading carefully the manuscript and suggesting several improvements.

References

[1] G.F.M. Beenker, A note on extended quadratic residue codes over $GF(9)$ and their ternary images, IEEE Trans. Inform. Theory 30 (1984) 403–405.
[2] W. Bosma, J. Cannon, Handbook of Magma Functions, Version 2.9, Sydney, July, 2002.
[3] The GAP Group, GAP–Groups, Algorithms, and Programming, Version 4.3; 2002, http://www.gap-system.org.
[4] D.Y. Goldberg, Reconstructing the ternary Golay code, J. Combin. Theory Ser. A 42 (1986) 296–299.
[5] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[6] C.L. Mallows, V. Pless, N.J.A. Sloane, Self-dual codes over $GF(3)$, SIAM. J. Appl. Math. 31 (1976) 649–666.