Serdica J. Computing **1** (2007), 185–192

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

SOME MDS CODES OVER *GF*(64) CONNECTED WITH THE BINARY DOUBLY-EVEN [72,36,16] CODE

Stefka Bouyuklieva*

Abstract. MDS [8,4,5] codes over a field with 64 elements are constructed. All such codes which are self-dual under a Hermitian type inner product are classified. The connection between these codes and a putative binary self-dual [72,36,16] code is considered.

1. Introduction. A linear q-ary $[n, k]$ code C is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the finite field of q elements. The elements of C are called codewords and the (Hamming) weight of a codeword is the number of its non-zero coordinates. The minimum weight d of C is the smallest weight among all non-zero codewords of C, and C is called an $[n, k, d]$ code. For these three parameters, the following bound holds:

Theorem 1 (Singleton bound) [9]. *Given an* $[n, k, d]$ *code,* $d \leq n-k+1$.

A code for which equality holds in the Singleton bound is called *maximum distance separable*, abbreviated MDS code. If C is an MDS code, then every k

ACM Computing Classification System (1998): E.4.

Key words: Self-dual codes, Automorphisms, MDS codes.

*The author is supported by a Return Fellowship from the Alexander von Humboldt Foundation.

coordinates are an information set for C. The weight distribution of an MDS code over $\mathbb{F}_q$ is determined by its parameters n, k and q. In this paper, we construct MDS [8,4,5] codes over $GF(64)$. The codes we consider have to be not only MDS but also self-dual under a Hermitian type inner product.

Let $(u, v) : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be an inner product in the linear space $\mathbb{F}_q^n$. The dual code of C is $C^\perp = \{u \in \mathbb{F}_q^n : (u, v) = 0 \text{ for all } v \in C\}$. $C^\perp$ is a linear $[n, n-k]$ code. If $C \subseteq C^\perp$, C is termed self-orthogonal and if $C = C^\perp$, C is self-dual. For the self-dual codes $k = \frac{1}{2}n$.

In this paper, we consider the following two families of self-dual codes:

1. Binary self-dual codes with inner product

$$(u, v) = u \cdot v = \sum_{i=1}^{n} u_i v_i$$

Obviously, all weights in a binary self-dual code are even. If all weights are divisible by four, the code is doubly-even. Self-dual doubly-even codes exist only when n is a multiple of 8. Rains [12] proved that the minimum distance d of a binary self-dual $[n, k, d]$ code satisfies the following bound:

$$d \le 4\lfloor n/24 \rfloor + 4, \quad \text{if } n \not\equiv 22 \pmod{24},$$

$$d \le 4\lfloor n/24 \rfloor + 6, \quad \text{if } n \equiv 22 \pmod{24}.$$

Codes achieving this bound are called extremal. If n is a multiple of 24, then a self-dual code meeting the bound must be doubly-even [12]. Moreover, for any nonzero weight w in such a code, the codewords of weight w form a 5-design [1]. Therefore the extremal binary doubly-even self-dual codes of length a multiple of 24 are of particular interest. The extended Golay code g_{24} is the unique [24,12,8] code and the extended quadratic residue code q_{48} is the unique extremal doubly-even code of length 48. The smallest length for which the existence of an extremal code is not known is 72. That's why many papers are devoted to the problem of existence of such codes. Many properties of the putative doubly-even [72,36,16] codes have been proved but the main question still remains open.

Recall that $\sigma \in S_n$ is an automorphism of a binary linear code C if $C = \sigma(C)$. We say that σ is of type $p-(c, f)$ if σ has a prime order p, can be presented as a product of c independent cycles and fixes f points. The set of all automorphisms of C form its automorphism group $Aut(C)$. Of course, knowledge of the existence of a non-trivial automorphism group is very useful in constructing a code. The automorphism group of the extended

Golay code is the 5-transitive Mathieu group M_{24} of order $2^{10}\cdot 3^3\cdot 5\cdot 7\cdot 11\cdot 23$ [9]. The automorphism group of q_{48} is only 2-transitive. It is isomorphic to the projective special linear group $PSL(2,47)$ and has order $2^4\cdot 3\cdot 23\cdot 47$ [9].

What can we say about the automorphism group of a putative self-dual doubly-even [72,36,16] code C? The investigations on this group have been started by Conway and Pless in [5] where they have proved that the primes dividing its order, are from the set $\{2,3,5,7,11,17,23\}$. Further, Pless [10], Pless and Thompson [11], Huffman and Yorgov [8], have excluded 11, 17 and 23 from this set. Moreover, following [5], the possible types of the corresponding automorphisms are 7-(10,2), 5-(14,2), 3-(24,0), 3-(22,6), 3-(20,12) and 3-(18,18). Dontcheva, van Zanten and Dodunekov in [6] have proved that if a doubly-even [72,36,16] code has an automorphism of odd order $r > 1$, then $r = 35$, 27, 15, 9, 7, 5, or 3. The possibility $r = 35$ is excluded in [14], $r = 27$ and $r = 15$ – in [2]. Hence $r \leq 9$. Moreover, we have proved in [2] that automorphisms of types 3-(22,6), 3-(20,12) and 3-(18,18) are not possible. Recently, it is shown in [3], that the automorphism group of a binary self-dual doubly-even $[72,36,16]$ code is a solvable group of order $5,7,10,14,56$, or a divisor of 72.

In this paper we consider the structure of a putative self-dual doubly-even [72,36,16] code having an automorphism of order 9 and its connection with Hermitian self-dual [8,4,5] codes over a field with 64 elements.

2. Hermitian self-dual codes over $\mathbb{F}_q$, where $q = 2^s$ for an even integer $s \geq 2$ with

$$(u,v) = \sum_{i=1}^{n} u_i\overline{v_i},$$

where $\overline{a} = a^{\sqrt{q}}$ for $a \in \mathbb{F}_q$. Note that for $a, b \in \mathbb{F}_q$, $(a+b)^{\sqrt{q}} = a^{\sqrt{q}} + b^{\sqrt{q}}$ and $a^q = a$.

In Section 2, we consider the structure of the binary self-dual codes having an automorphism of order 9. Eventually, we discuss the self-dual [72,36,16] codes with such an automorphism. Section 3 is devoted to the [8,4,5] MDS codes over a field with 64 elements.

2. Binary self-dual codes with an automorphism of order 9.

Let C be a binary self-dual code with an automorphism σ of order 9, where

$$\sigma = \Omega_1 \dots \Omega_c \Omega_{c+1} \dots \Omega_{c+f}, \tag{1}$$

$\Omega_i = (9i-8,\dots,9i), i=1,\dots,c$, and $\Omega_{c+i} = (9c+i), i=1,\dots,f$. So σ has c 9-cycles and f fixed points and does not have cycles of length 3. Let

$$F = F_\sigma(C) = \{v \in C : v\sigma = v\},$$

$$E = E_\sigma(C) = \{v \in C : wt(v|\Omega_i) \equiv 0 \pmod 2, \quad i = 1,\dots,c+f\},$$

where $v|\Omega_i$ is the restriction of v on Ω_i. Then the following Lemma holds

Lemma 2. [7]. *The code C is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$.*

Clearly $v \in F_\sigma(C)$ iff $v \in C$ and v is constant on each cycle. Let $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$ be the projection map where if $v \in F_\sigma(C)$, $(\pi(v))_i = v_j$ for some $j \in \Omega_i, i = 1,2,\dots,c+f$.

Lemma 3 [4]. *If C is a binary self-dual code having an automorphism σ of type* (1) *then $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual code of length $c+f$.*

Denote by E^* the code E with the last f coordinates deleted. So E^* is a self-orthogonal binary code of length cp^2 and $\dim E^* = \dim C - \dim F = \frac{c(p^2-1)}{2}$. For $v \in E^*$ we identify $v|\Omega_i = (v_0, v_1, \cdots, v_{p^2-1})$ with the polynomial $v_0 + v_1 x + \cdots + v_{p^2-1}x^{p^2-1}$ from $\mathcal{T}$ for $i = 1,\dots,c$, where $\mathcal{T}$ is the ring of even-weight polynomials in $\mathbb{F}_2[x]/(x^{p^2}-1)$. Thus we obtain the map $\phi : E^* \to \mathcal{T}^c$. In order to learn more about the code $C_\phi = \phi(E^*)$, we need to investigate the structure of the ring $\mathcal{T}$. In our work [4] we have proved that $\mathcal{T} = I_1 \oplus I_2$ where $I_1 = \{0, x^s e_1, s = 0,1,2\}$ is a field of 4 elements with identity $e_1 = x^8 + x^7 + x^5 + x^4 + x^2 + x$, and I_2 is a field of 2^6 elements with identity $e_2 = x^6 + x^3$. The element $\alpha = (x+1)e_2$ is a primitive element of I_2. We consider the element $\delta = \alpha^9 = x^2 + x^4 + x^5 + x^7$ of multiplicative order 7 in I_2 and $I_2 = \{0, x^s\delta^k$, for $0 \le s \le 8$ and $0 \le k \le 6\}$. Following Lemma 5 and Corollary 1 from [4], we have the theorem:

Theorem 4. $C_\phi = \phi(E^*) = M_1 \oplus M_2$, *where $M_j = \{u \in E^* | u_i \in I_j, i = 1,\dots,c\}, j = 1,2$. Moreover, M_1 and M_2 are Hermitian self-dual codes over the fields I_1 and I_2, respectively.*

Corollary 5. *If C is a binary self-dual code having an automorphism σ of type (1) then*

$$C = E_1 \oplus E_2 \oplus F$$

where $E_1 \oplus E_2 = E$, $M_1 = \phi(E_1^*)$, $M_2 = \phi(E_2^*)$.

Let us now consider the extremal binary self-dual codes of length 72 having an automorphism of order 9. We discuss the possibilities for such an automorphism in the next lemma.

Lemma 6. *If C is a binary doubly even self-dual $[72, 36, 16]$ code and $\sigma \in Aut(C)$ is an automorphism of order 9, then*

$$\sigma = \Omega_1 \Omega_2 \dots \Omega_8$$

where Ω_1, Ω_2, $\dots$, Ω_8 are independent cycles of length 9.

Proof. As it is proved in [2], if C has an automorphism of order 3, this automorphism does not fix any coordinate of C. Let σ has c 9-cycles, t 3-cycles, and f fixed points in its presentation as a product of independent cycles. Then σ^3 is an automorphism of C of order 3 with $3t + f$ fixed points. It turns out that $3t + f = 0$, hence $t = f = 0$ and $c = 8$. □

Theorem 7. *If C is a binary doubly even self-dual $[72, 36, 16]$ code and $\sigma \in Aut(C)$ is an automorphism of order 9, then*

$$C = E_1 \oplus E_2 \oplus F$$

where E_1, E_2, and F are doubly-even $[72, 8, \geq 16]$, $[72, 24, \geq 16]$, and $[72, 4, \geq 16]$ codes, respectively. Moreover, $M_1 = \phi(E_1)$ is a Hermitian quaternary self-dual $[8, 4, 4]$ code, $M_2 = \phi(E_2)$ is a Hermitian self-dual code over $I_2 \cong GF(64)$, and $\pi(F)$ is a binary self-dual $[8, 4, 4]$ code.

Proof. Since F is a doubly even code, so should be $\pi(F)$. The only self-dual doubly even code of length 8 is the extended Hamming code e_8 with parameters [8,4,4] [13]. If M_1 is a Hermitian quaternary self-dual $[8, 4, d_1]$ code, then E_1 will be a binary self-orthogonal $[72, 8, 6d_1]$. Hence $d_1 \geq 4$. The only Hermitian quaternary self-dual code of length 8 with such minimum weight is e_8 considered as a code over $\mathbb{F}_4$ [13]. □

It turns out that we know the subcodes E_1 and F up to equivalence. In the next Section we consider the possibilities for E_2 and its image M_2.

3. MDS [8,4,5] codes over $GF(64)$.

In classifying mathematical objects, one should carefully define the concept of isomorphism or – depending on the conventional terminology – equivalence. For self-dual and self-orthogonal codes, the definition of equivalence depends on the inner product.

The transformations that we allow in defining equivalence for the Hermitian self-dual codes over the field I_2 are the following:

1. permutation of the coordinates,
2. multiplication of the elements in a given coordinate by x^t for $0 \leq t \leq 8$,

3. application of the substitution $x \to x^2$ to the elements in all coordinates simultaneously.

Two linear codes over I_2, C_1 and C_2, are said to be *equivalent* if the codewords of C_2 can be obtained from the codewords of C_1 via a sequence of these three transformations.

Theorem 8. *If C is a binary doubly even self-dual $[72,36,16]$ code and $\sigma \in Aut(C)$ is an automorphism of order 9, then the code M_2 is a Hermitian self-dual $[8,4,d_2 \geq 4]$ code over $I_2 \cong GF(64)$.*

Proof. Let $v \in M_2$ is a codeword with minimum weight d_2. Up to equivalence

$$v = (e_2, \delta^{a_2}, \ldots, \delta^{a_{d_2}}, 0, \ldots, 0), \quad 0 \leq a_2 \leq \cdots \leq a_{d_2} \leq 6.$$

It is easy to check that $e_2 + \delta = \delta^3$. Using the orthogonality condition and the above transformations, we have:

- If $d_2 = 2$ then $v = (e_2, e_2, 0, \ldots, 0) \Rightarrow wt(\phi^{-1}(v)) = 4$;
- If $d_2 = 3$ then $v = (e_2, \delta, \delta^3, 0, \ldots, 0) \Rightarrow wt(\phi^{-1}(v)) = 12$;
- If $d_2 = 4$ then

$$v = (e_2, e_2, e_2, e_2, 0, 0, 0, 0) \Rightarrow wt(\phi^{-1}(v)) = 8 \text{ or}$$

$$v = (e_2, e_2, \delta, \delta, 0, 0, 0, 0) \Rightarrow wt(\phi^{-1}(v)) = 12 \text{ or}$$

$$v = (e_2, \delta, \delta^2, \delta^5, 0, 0, 0, 0) \Rightarrow wt(\phi^{-1}(v)) = 16$$

Hence $d_2 \geq 4$. According to the Singleton bound, $d_2 \leq 5$ and therefore $d_2 = 4$ or 5. □

Here we consider only the case $d_2 = 5$. Up to equivalence, we can take a generator matrix of the [8,4,5] MDS code in the form:

$$G = \begin{pmatrix} e_2 & 0 & 0 & 0 & \delta^{a_{11}} & \delta^{a_{12}} & \delta^{a_{13}} & \delta^{a_{14}} \\ 0 & e_2 & 0 & 0 & \delta^{a_{21}} & x^{b_{22}}\delta^{a_{22}} & x^{b_{23}}\delta^{a_{23}} & x^{b_{24}}\delta^{a_{24}} \\ 0 & 0 & e_2 & 0 & \delta^{a_{31}} & x^{b_{32}}\delta^{a_{32}} & x^{b_{33}}\delta^{a_{33}} & x^{b_{34}}\delta^{a_{34}} \\ 0 & 0 & 0 & e_2 & \delta^{a_{41}} & x^{b_{42}}\delta^{a_{42}} & x^{b_{43}}\delta^{a_{43}} & x^{b_{44}}\delta^{a_{44}} \end{pmatrix}$$

where $0 \leq a_{11} \leq a_{12} \leq a_{13} \leq a_{14} \leq 6$, $0 \leq a_{11} \leq a_{21} \leq a_{31} \leq a_{41} \leq 6$. Using the orthogonality conditions, we have

$$e_2 + \delta^{9a_{11}} + \delta^{9a_{12}} + \delta^{9a_{13}} + \delta^{9a_{14}} = e_2 + \delta^{2a_{11}} + \delta^{2a_{12}} + \delta^{2a_{13}} + \delta^{2a_{14}} = 0$$

$$\Rightarrow e_2 + \delta^{a_{11}} + \delta^{a_{12}} + \delta^{a_{13}} + \delta^{a_{14}} = 0$$

So up to equivalence

$$(a_{11}, a_{12}, a_{13}, a_{14}) = (0,0,1,3),\ (0,1,2,4) \text{ or } (0,1,5,6)$$

To obtain all inequivalent MDS [8,4,5] codes, we use a computer program with the following constrains:

- $e_2 + \delta^{a_{i1}} + \delta^{a_{i2}} + \delta^{a_{i3}} + \delta^{a_{i4}} = 0$ for $i = 1,2,3,4$;
- $\delta^{a_{j1}+a_{i1}} + x^{b_{j2}-b_{i2}}\delta^{a_{j2}+a_{i2}} + x^{b_{j3}-b_{i3}}\delta^{a_{j3}+a_{i3}} + x^{b_{j4}-b_{i4}}\delta^{a_{j4}+a_{i4}} = 0$ for $1 \le i < j \le 4$;
- $(b_{ij}, a_{ij}) \neq (b_{is}, a_{is})$ for $j \neq s$, $i = 1,2,3,4$.

Additionally, we check the minimum weight of the constructed subcodes in any step. In this way we obtain 96 Hermitian self-dual [8,4,5] codes over the field I_2 which lead to 96 inequivalent binary doubly-even [72,24,16] codes. All these binary codes have the same weight enumerator

$$\begin{aligned} W(y) = \quad & 1 + 513y^{16} + 14112y^{20} + 170856y^{24} + 1118880y^{28} + 3772467y^{32} \\ & +6219360y^{36} + 4413528y^{40} + 1034208y^{44} + 33291y^{48} \end{aligned}$$

Nevertheless we have only one possibility for E_1 and again one possibility for F up to equivalence, it is computationally difficult to construct all inequivalent binary codes which have an automorphism σ and to check if some of them are extremal. To do that, we have to fix one of these codes, say E_2, and to consider all different, even equivalent, codes E_1 and F. So the possibilities are too many and we have not succeeded to check all of them.

REFERENCES

[1] Assmus E. F., H. F. Mattson. New 5-designs. *J. Combin. Theory* **6** (1969), 122–151.

[2] Bouyuklieva S. On the automorphism group of a doubly-even [72,36,16] code. *IEEE Trans. Inform. Theory* **50** (2004), 544–547.

[3] Bouyuklieva S., E. A. O'Brien, W. Willems. The automorphism group of a binary self-dual doubly-even [72,36,16] code is solvable. *IEEE Trans. Inform. Theory* **52** (2006), 4244–4248.

[4] Bouyuklieva S., R. Russeva, N. Yankov. On the structure of binary self-dual codes having an automorphism of order a square of an odd prime. *IEEE Trans. Inform. Theory* **51** (2005), 3678–3686.

[5] Conway J. H., V. Pless. On primes dividing the group order of a doubly-even (72,36,16) code and the group order of a quaternary (24,12,10) code. *Discrete Math.* **38** (1982), 143–156.

[6] Dontcheva R., A. J. van Zanten, S. Dodunekov. Binary self-dual codes with automorphisms of composite order. *IEEE Trans. Inform. Theory* **50** (2004), 311–318.

[7] Huffman W. C. Decomposing and shortening codes using automorphisms. *IEEE Trans. Inform. Theory* **32** (1986), 833–836.

[8] Huffman W. C., V. Yorgov. A [72,36,16] doubly-even code does not have an automorphism of order 11. *IEEE Trans. Inform. Theory* **33** (1987), 749–752.

[9] MacWilliams F. J., N. J. A. Sloane. The Theory of Error-Correcting Codes. North-Holland, Amsterdam, 1977.

[10] Pless V. 23 does not divide the order of the group of a (72,36,16) doubly-even code. *IEEE Trans. Inform. Theory* **28** (1982), 113–117.

[11] Pless V., J. G. Thompson. 17 does not divide the order of the group of a (72,36,16) doubly-even code. *IEEE Trans. Inform. Theory* **28** (1982), 537–541.

[12] Rains E. M. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory* **44** (1998), 134–139.

[13] Rains E., N. J. A. Sloane. Self-dual codes. In: Handbook of Coding Theory (Eds V. Pless, W. C. Huffman). Elsevier, Amsterdam, 1998, 177–294.

[14] Yorgov V. On the automorphism group of a putative code. *IEEE Trans. Inform. Theory* **52** (2006), 1724–1726.

Veliko Tarnovo University
5000 Veliko Tarnovo, Bulgaria
e-mail: `stefka@uni-vt.bg`

Received October 23, 2006
Final Accepted June 27, 2007