Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 286-291*

New results on s-extremal additive codes over $\mathbb{F}_4$

Zlatko Varbanov vtgold@yahoo.com
Department of Mathematics and Informatics,
Veliko Tarnovo University, 5000 Veliko Tarnovo, BULGARIA

Abstract. The purpose of this paper is to study s-extremal additive codes over F_4. The concept of s-extremality was introduced in [2] and the s-extremal additive codes with minimum distance up to 4 were classified. In this paper, our goal is to construct (or to classify if possible) new s-extremal codes with minimum distance $d = 5$ or 6. For $d = 5$ we classify the codes of length 13, and we construct 1075 new codes of length 14. For $d = 6$ we obtain that there is a unique code of length 14.

1 Introduction

The shadow of a binary self-dual code was introduced by Conway and Sloane [5] in order to get additional constraints in the weight enumerator of a singly-even binary self-dual code. Let C be a singly-even binary self-dual code. The shadow S of C is

$$S = \{w \in \mathbb{F}_2^n | (v, w) \equiv \tfrac{1}{2}wt(v) \ (mod\ 2) \text{ for all } v \in C\},$$

where (v, w) is an Euclidean inner product in $\mathbb{F}_2^n$.

Let d be the minimum distance of C and s be the minimum weight of S. It is known [1] that $2d + s \leq n/2 + 4$ except in the case $n \equiv 22 \pmod{24}$ and $d = 4[n/24] + 6$ where $2d + s = n/2 + 8$. Binary codes attaining these bounds are called s-extremal.

After the introduction of s-extremal binary self-dual codes, it is natural to ask whether there exists a concept of s-extremal additive F_4 codes. If so, can we classify them? This concept was introduced by Bautista, Gaborit, Kim, and Walker [2]. They gave a bound on the possible lengths of such codes related to their distances for even d and classified them up to $d = 4$. Also, they gave possible lengths (only strongly conjectured for odd d) and (shadow) weight enumerators for which there exist s-extremal codes with $5 \leq d \leq 11$.

In this paper, we investigate a s-extremal codes with minimum distance 5 and 6. For $d = 5$ we give a full classification of the codes of length 13 and we construct 1075 new codes of length 14. For $d = 6$ we obtain that there is a unique code (up to equivalence) of length 14.

2 Preliminaries

Let $F_4 = \{0, 1, \omega, \bar{\omega}\}$ with convention that $\bar{\omega} = \omega^2 = 1 + \omega$. We recall some definitions on additive codes over F_4 from [4], [6].

Definition 2.1 *An **additive code** C **over** F_4 **of length n** is an additive subgroup of F_4^n. As C is a free F_2-module, it has size 2^k for some $0 \leq k \leq 2n$. We call C an $(n, 2^k)$ code. It has a basis, as a F_2-module, consisting of k basis vectors; a **generator matrix** of C is any $k \times n$ matrix with entries in F_4 whose rows are a basis of C.*

Definition 2.2 *The **weight** of a codeword $c \in C$ (denoted by $wt(c)$) is the number of nonzero components of c and the **minimum weight** (or **minimum distance**) d of C is the smallest weight among all nonzero codewords in C. We call C an $(n, 2^k, d)$ code.*

There is an inner product arising from the trace map. The trace map $Tr : F_4 \to F_2$ is given by $Tr(x) = x + x^2$. The *conjugate* of $x \in F_4$, denoted $\bar{x}$, is the following image: $\bar{0} = 0, \bar{1} = 1$, and $\bar{\omega} = \omega$.

Definition 2.3 ***Trace inner product*** *of two vectors $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ in F_4^n is*

$$x \star y = \sum_{i=1}^{n} Tr(x_i \bar{y_i}) \tag{1}$$

Definition 2.4 *If C is an additive code, its **dual**, denoted $C^{\perp}$, is the additive code $\{x \in F_4^n | x \star c = 0$ for all $c \in C\}$. If C is an $(n, 2^k)$ code, then $C^{\perp}$ is an $(n, 2^{2n-k})$ code. As usual, C is **self-orthogonal** if $C \subseteq C^{\perp}$, and **self-dual** if $C = C^{\perp}$.*

In particular, if C is self-dual, then C is an $(n, 2^n)$ code. C is *Type II* code if C is self-dual and all codewords have even weight; *Type II* codes of length n exist only if n is even [6]. If C is self-dual but some codeword has odd weight (in which case the code cannot be F_4-linear), the code is *Type I*. There is a bound on the minimum weight of an additive self-dual code ([10], Theorem 33). If d_I and d_{II} are the minimum weights of additive self-dual *Type I* and *Type II* codes, respectively, of length $n > 1$, then

$$d_I \leq \begin{cases} 2\lfloor n/6 \rfloor + 1, & n \equiv 0 \ (mod\ 6); \\ 2\lfloor n/6 \rfloor + 3, & n \equiv 5 \ (mod\ 6); \\ 2\lfloor n/6 \rfloor + 2, & \text{otherwise} \end{cases} \tag{2}$$

$$d_{II} \leq \ 2\lfloor n/6 \rfloor + 2$$

A code that meets the appropriate bound is called *extremal*.

Definition 2.5 *Two additive codes C_1 and C_2 are **equivalent** if there is a map sending the codewords of C_1 onto the codewords of C_2 where the map consists of a permutation of coordinates, followed by a scaling of coordinates by elements of F_4, followed by conjugation of some of the coordinates.*

Definition 2.6 *Let C be an additive F_4-code of length n which is self-dual with respect to the trace inner product. The* ***shadow*** *$S = S(C)$ of C is given by*

$$S = \{w \in \mathbb{F}_4^n | v \star w \equiv wt(v) \ (mod\ 2) \text{ for all } v \in C\}.$$

If C is *Type II* $S(C) = C$, while if C is *Type I* $S(C)$ is a coset of C.
The next theorem is the F_4-analog of Theorem 1 in [1].

Theorem 2.7 [2] *Let C be a Type I additive code over F_4 of length n, let $d = d_{min}(C)$ be the minimum distance of C, let $S = S(C)$ be the shadow of C, and let $s = wt_{min}(S)$ be the minimum weight of S. Then $2d + s \leq n + 2$ unless $n = 6m + 5$ and $d = 2m + 3$, in which case $2d + s = n + 4$.*

This theorem motivates the following definition.

Definition 2.8 *Let C be a Type I additive code over F_4 of length n, let $d = d_{min}(C)$ be the minimum distance of C, let $S = S(C)$ be the shadow of C, and let $s = wt_{min}(S)$ be the minimum weight of S. We call C* ***s-extremal*** *if the bound of Theorem 7 is met, i.e., if $2d + s = n + 2$ except $n = 6m + 5$ and $d = 2m + 3$, in which case $2d + s = n + 4$.*

There are some known bounds for the length of s-extremal codes.

Theorem 2.9 [9] *Let C be an $(n, 2^n, d)$ s-extremal code. Then $n \geq 3d - 4$. If d is even, then $3d - 4 \leq n \leq 3d - 2$.*

For odd $d > 3$, there are the following bounds [9]:
$d = 5 \ : \ 11 \leq n \leq 15$ $\qquad$ $d = 7 \ : \ 17 \leq n \leq 21$
$d = 9 \ : \ 23 \leq n \leq 27$ $\qquad$ $d = 11 \ : \ 29 \leq n \leq 33$

3 Lengthening of graph codes

We recall the lengthening of graph codes from [12]. A *graph* is a pair $G = (V, E)$, where $V = \{v_0, v_1, \ldots, v_n\}$ is a set of n *vertices* (or *nodes*), and E is a set of distinct pairs of elements from V, i.e., $E \subseteq V \times V$. A pair $\{v_i, v_j\} \in E$ is called *edge*. We will only consider *undirected* graphs, which are graphs where E is a set of distinct unordered pairs of elements from V, and no self-loops ($\{v_i, v_i\} \notin E$). A graph may be represented by an *adjacency matrix* Γ. This is a $|V| \times |V|$ matrix where $\Gamma_{i,j} = 1$ if $\{v_i, v_j\} \in E$ and $\Gamma_{i,j} = 0$ otherwise. The adjacency matrix of an undirected graph will be symmetric, i.e., $\Gamma_{i,j} = \Gamma_{j,i}$, and $\Gamma_{i,i} = 0$ (because no self-loops).

A *graph code* is an additive self-dual code over F_4 with generator matrix $C = \Gamma + \omega I$ where I is the identity matrix and Γ is the adjacency matrix of a undirected graph, which must be symmetric with 0's along the diagonal.

Example: $\Gamma = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, $C = \Gamma + \omega I = \begin{pmatrix} \omega & 1 & 1 \\ 1 & \omega & 1 \\ 1 & 1 & \omega \end{pmatrix}$.

Schlingemann [11] first proved the following theorem in terms of *quantum stabilizer states.*

Theorem 3.1 ([11], [7]) *For any additive self-dual code, there is an equivalent graph code. This means that there is a one-to-one correspondence between the set of undirected graphs and the set of additive self-dual codes over* F_4.

We have seen that every graph represents an additive self-dual code over F_4, and that every additive self-dual code over F_4 can be represented by a graph. It follows from Theorem 3.1 that, without loss of generality, we can restrict our study of additive self-dual codes over F_4 to those with generator matrices of the form $\Gamma + \omega I$ (graph form).

The lengthening of graph codes is based on the following theorem.

Theorem 3.2 [12] *If* G *is a generator matrix of a graph code* C *of length* n*, and* x *is a binary vector, then*

$$G' = \left(\begin{array}{c|c} G & x^t \\ \hline x & \omega \end{array}\right)$$

is a generator matrix of a graph code of length $n+1$.

Using this construction we obtain new results described in the following section.

4 Results

To obtain new s-extremal additive codes we use some preliminary results.

Theorem 4.1 (Theorem 4.1 [12]) *There are* 85845 *nonequivalent additive self-dual* $(13, 2^{13}, 5)$ *codes,* 2 *nonequivalent* $(14, 2^{14}, 6)$ *Type I codes, and* 1020 *nonequivalent* $(14, 2^{14}, 6)$ *Type II codes.*

These codes were obtained by lengthening of graph codes. Then, their generator matrices are given in graph form and we can use the same method to get new results.

It is known that the weight enumerator of the s-extremal codes of length 13 is $C(z) = 1 + 39z^5 + 156z^6 + 468z^7 + 1053z^8 + 1690z^9 + 2028z^{10} + 1716z^{11} + 858z^{12} + 183z^{13}$ and the number of these codes is ≥ 9 [2]. Using the results in Theorem 4.1 by computer check we obtain the following classification.

Theorem 4.2 *There are exactly* 33428 *nonequivalent* s*-extremal codes of length* 13.

In Table 1 we give full classification (by group order) of the s-extremal codes of length 13.

Table 1 Number of s-extremal codes of length 13 with group order α

α	1	2	3	4	6	8	12	52	156
Number	32134	1228	5	49	7	1	2	1	1

In our work we use the program package $Q - Extension$ [3] to obtain the number of nonequivalent codes and their group orders.

We use the generator matrices of the codes of length 13 to obtain new codes of length 14 with $d = 5$. By lengthening of graph codes we construct 1075 new codes with these parameters (one code is already known [8]). Therefore

Theorem 4.3 *There are at least* 1076 *nonequivalent s-extremal codes of length* 14 *with* $d = 5$.

In Table 2 we give a group order of the constructed s-extremal codes of length 14. It is known [2] that these codes have weight enumerator $C(z) = 1 + 42z^5 + 119z^6 + 408z^7 + 1281z^8 + 2492z^9 + 3486z^{10} + 3864z^{11} + 3038z^{12} + 1386z^{13} + 267z^{14}$, and shadow enumerator $S(z) = 308z^6 + 2352z^8 + 7224z^{10} + 5936z^{12} + 564z^{14}$.

Table 2 Number of s-extremal codes of length 14 with group order α

α	1	2	3	4	6	8	24	28
Number	≥ 915	≥ 125	≥ 8	≥ 16	≥ 5	≥ 5	≥ 1	≥ 1

By results in Theorem 4.1 we obtain that there is a unique s-extremal code of length 14. This code has weight enumerator $C(z) = 1 + 161z^6 + 576z^7 + 1113z^8 + 2240z^9 + 3738z^{10} + 4032z^{11} + 2870z^{12} + 1344z^{13} + 309z^{14}$, shadow enumerator $S(z) = 21z^4 + 203z^6 + 2562z^8 + 7014z^{10} + 6041z^{12} + 543z^{14}$, and group order 48. The generator matrix G_{14} of this code is

$$G_{14} = \begin{pmatrix}
\omega & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & \omega & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & \omega & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & \omega & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & \omega & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & \omega & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & \omega & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & \omega & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & \omega & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & \omega & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \omega & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & \omega
\end{pmatrix}$$

References

[1] C. Bachoc, P. Gaborit, Designs and self-dual codes with long shadows, *J. Combin. Theory* Ser.A 105, 2004, 15-34.

[2] E. Bautista, P. Gaborit, J.-L. Kim, J. Walker, s-extremal additive $\mathbb{F}_4$ codes, *Adv. Math. Commun.* 1, 2007, 111-130.

[3] I. Bouyukliev, What is Q-extension?, *Serdica J. Comput.* 1, 2007, 115-130.

[4] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inform. Theory.* 44, 1998, 1369-1387.

[5] J. H. Conway, N. J. A. Sloane, A new upper bound on the minimal distance of selfdual codes, *IEEE Trans. Inform. Theory* 36, 1990, 1319-1333.

[6] P. Gaborit, W. C. Huffman, J.-L. Kim, V. Pless, On additive GF(4)-codes, *DIMACS Workshop Codes Assoc. Schemes*, DIMACS Series Discr. Math. Theoret. Comp. Sci., AMS 56, 2001, 135-149.

[7] D. G. Glynn, On self-dual quantum codes and graphs, submitted to Electr. J. Combin.
http://homepage.mac.com/dglynn/.cv/dglynn/Public/SD-G3.pdf-link.pdf

[8] T. A. Gulliver, J.-L. Kim, Circulant based extremal additive self-dual codes over $GF(4)$, *IEEE Trans. Inform. Theory* 40, 2004, 359-366.

[9] S. Han, J.-L. Kim, Upper bounds for the length of s-extremal codes over $\mathbb{F}_2, \mathbb{F}_4$, and $\mathbb{F}_2 + u\mathbb{F}_2$, submitted, 2007.

[10] E. M. Rains, N. J. A. Sloane, Selfdual codes, in Handbook of Coding Theory, ed. V. S. Pless and W. C. Huffman, Amsterdam: Elsevier (1998), 177-294.

[11] D. Schlingemann, Stabilizer codes can be realized as graph codes, *Quantum Inf. Comput.* 2, 2002, 307-323, arXiv:quant-ph/0111080.

[12] Z. Varbanov, Some new results for additive self-dual codes over $GF(4)$, *Serdica J. Comput.* 1, 2007, 213-227.