Serdica J. Computing **12** (2018), No 4, 219–226

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

NEW LOWER BOUNDS FOR THE NUMBER OF ACG CODES OVER $\mathbb{F}_4$

Zlatko Varbanov, Maya Hristova

Abstract. In this paper we consider additive circulant graph (ACG) codes over $\mathbb{F}_4$ of length $n \geq 34$ and we present some new results for the number of these codes. The most important result is that there exists a unique ACG code over $\mathbb{F}_4$ of length 36 and minimum weight 11.

1. Introduction. Additive self-orthogonal codes over $\mathbb{F}_{q^2}$ are objects of interest because of their representation as a class of quantum error-correcting codes [3]. Several papers (see [3, 5, 6]) were devoted to classifying or constructing additive self-dual codes over $\mathbb{F}_4$. Additive self-dual codes over $\mathbb{F}_9$, $\mathbb{F}_{16}$ and $\mathbb{F}_{25}$ were classified in [4]. Moreover, it was shown in [10] that certain vectors in some

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

Key words: additive self-dual codes, circulant codes, graph codes.

*This research of the authors was supported by Bulgarian Science Fund under Contract DN-02-2/13.12.2016. Some of the results were announced at the 8th International Conference *Optimal codes and related topics*, 10–14.07, Sofia, Bulgaria.

additive self-dual codes over $\mathbb{F}_4$ hold generalized t-designs as well as classical t-designs with possibly repeated blocks. These facts motivate the construction of additive self-dual codes over $\mathbb{F}_4$.

A naturally arising problem is to classify all nonequivalent codes of given length and minimum weight. All additive self-dual codes over $\mathbb{F}_4$ of length n have previously been classified (up to equivalence) by Calderbank et al. [3] for $n \leq 5$, and by Höhn [9] for $n \leq 7$. Gaborit et al. [6] classified all extremal codes of length 8, 9, 11, and 12. Gulliver and Kim [8] classified many circulant and 4-circulant codes of length $n \leq 27$. Using graph representation, Danielsen and Parker [5] gave a full classification of the codes of length $n \leq 12$. Varbanov [14] classified all extremal (optimal) codes of length 13 and 14, and constructed many extremal codes of length $15 \leq n \leq 21$. Further some constructive and classification results about additive codes from circulant graphs were obtained. Danielsen [4] gave some results about these codes over $\mathbb{F}_4$, $\mathbb{F}_9$, $\mathbb{F}_{16}$ and $\mathbb{F}_{25}$. Varbanov [15] gave a full classification of codes over $\mathbb{F}_4$ for lengths $13 \leq n \leq 33$ and some results for $34 \leq n \leq 36$. This class of codes was also considered in [11]. The last known results were published by Grassl and Harada [7]. They presented many obtained results for codes over $\mathbb{F}_4$ for lengths $36 \leq n \leq 100$.

The purpose of this paper is to present some new classification results about additive self-dual codes from circulant graphs, called *additive circulant graph (ACG)* codes below. The paper is structured in the following way. Section 2 contains basic definitions and preliminary results. In Section 3 we give some notations about circulant codes and a short description of the algorithm for constructing ACG codes. The last section contains the obtained classification results.

2. Preliminaries. Let $\mathbb{F}_4 = GF(4) = \{0, 1, \omega, \bar{\omega}\}$ where $\bar{\omega} = \omega^2 = 1+\omega$. We recall some definitions on additive codes over $\mathbb{F}_4$ from [3, 6].

An *additive code C over $\mathbb{F}_4$ of length n* is an additive subgroup of $\mathbb{F}_4^n$. Such a code C has 2^k codewords for some $0 \leq k \leq 2n$ and we call C an $(n, 2^k)$ code. It has a basis, consisting of k basis vectors; a generator matrix of C is a $k \times n$ matrix with entries in $\mathbb{F}_4$ whose rows are a basis of C.

About additive codes, a natural inner product arising from the trace map is used. The trace map $Tr : \mathbb{F}_4 \to \mathbb{F}_2$ is given by $Tr(x) = x + x^2$ (therefore $Tr(0) = Tr(1) = 0$ and $Tr(\omega) = Tr(\bar{\omega}) = 1$). The *conjugate* of $x \in \mathbb{F}_4$, denoted $\bar{x}$, is the following image: $\bar{0} = 0, \bar{1} = 1$, and $\bar{\bar{\omega}} = \omega$.

Then the *trace inner product* of two vectors $x = (x_1, x_2, \ldots, x_n)$, $y =$

$(y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_4^n$ is defined as

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

If C is an additive code, its *dual* code with respect to (1) is the code $C^{\perp} = \{x \in \mathbb{F}_4^n | x \star c = 0 \text{ for all } c \in C\}$. If C is an $(n, 2^k)$ code, then $C^{\perp}$ is an $(n, 2^{2n-k})$ code. A code C is called *self-orthogonal* (with respect to (1)) if $C \subseteq C^{\perp}$, and *self-dual* if $C = C^{\perp}$. If C is self-dual, then C is an $(n, 2^n)$ code.

The *weight* of a codeword $c \in C$) is the number of nonzero entries of c. The minimum weight d of a code C is the smallest weight among all nonzero codewords of C. If C is an additive $(n, 2^k)$ code with minimum weight d then C is an $(n, 2^k, d)$ code. A self-dual code C is called *Type II* if all codewords have even weight; otherwise it is *Type I*. It is known that *Type II* codes of length n exist only if n is even [6]. There is a bound on the minimum weight of an additive self-dual code ([12], 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

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

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

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, a scaling of coordinates by elements of $\mathbb{F}_4$, and a conjugation of some of the coordinates.

A *graph code* is an additive self-dual code over $\mathbb{F}_4$ with generator matrix $G = \Gamma + \omega I$ where I is the identity matrix and Γ is the adjacency matrix of a simple undirected graph, which must be symmetric with 0's along the diagonal.

Example:

$$\Gamma = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad G = \begin{pmatrix} \omega & 0 & 1 \\ 0 & \omega & 1 \\ 1 & 1 & \omega \end{pmatrix}$$

Schlingemann [13] first proved (in terms of *quantum stabilizer states*) that for any self-dual quantum code, there is an equivalent graph code. This means that there is a one-to-one correspondence between the set of simple undirected graphs and the set of additive self-dual codes over $\mathbb{F}_4$.

3. Additive circulant graph (ACG) codes. A matrix B of the form:

$$B = \begin{pmatrix} b_0 & b_1 & \dots & b_{n-2} & b_{n-1} \\ b_{n-1} & b_0 & b_1 & \dots & b_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ b_2 & \dots & b_{n-1} & b_0 & b_1 \\ b_1 & b_2 & \dots & b_{n-1} & b_0 \end{pmatrix}$$

is called a *circulant matrix*. The vector $(b_0, b_1, \dots, b_{n-1})$ is called a *generator vector* for the matrix B. An additive code with circulant generator matrix is called *circulant* code (see [8]).

An *additive circulant graph code* is a code corresponding to a graph with circulant adjacency matrix. Circulant graphs must be regular, i.e., all vertices must have the same number of neighbours. The generator vector of such matrix has the following property: $b_i = b_{n-i}, \forall\ i = 1, \dots, n-1$, and $b_0 = \omega$. Then, the entries in the generator matrix of ACG code depend on the coordinates $(b_1, b_2, \dots, b_{\lfloor n/2 \rfloor})$ only. The search space can be restricted to the $2^{\lfloor n/2 \rfloor}$ codes over $\mathbb{F}_4$ of length n corresponding to graphs with adjacency matrices that are circulant.

In the current work we use the constructive algorithm described in detail in [15]. Shortly, by this algorithm we construct ACG codes of length n and minimum weight $\geq d$ using the property that a given generator vector (without its first coordinate) is binary and it is symmetric with respect to its central coordinate. We use a bit-wise representation of this binary vector and from an arbitrary step it is easy to get the next possible vector (in lexicographical order) just increasing by 1. After the construction part we use the special form of the generator matrix of a graph code. This form makes it easier to determine the minimum weight, since any codeword obtained as a linear combination of i rows of the generator matrix has weight at least i (there is just one entry in any row and column that is not 0 neither 1). Also, to calculate the weight of a given quaternary vector we do not need to check every coordinate position of the vector (we use the bit-wise representation of the codewords and faster algorithm [2]).

The description of the used algorithm is given below.

INPUT: positive integers n and d $(1 < d < n)$.

OUTPUT: all possible ACG codes of length n with minimum weight $\geq d$.

Step 1. If n is even, take a binary vector $g^{(0)} = (g_1, g_2, \dots g_{\frac{n}{2}})$ and extend it to a vector $g = (\omega, g_1, g_2, \dots, g_{\frac{n}{2}-1}, g_{\frac{n}{2}}, g_{\frac{n}{2}-1}, \dots, g_2, g_1)$. If n is odd then $g^{(0)} = (g_1, g_2, \dots g_{\frac{n-1}{2}})$, and $g = (\omega, g_1, g_2, \dots, g_{\frac{n-1}{2}}, g_{\frac{n-1}{2}}, \dots, g_2, g_1)$

Step 2. Construct a circulant matrix G (a generator matrix of an ACG code) with generator vector g.

Step 3. Compute all linear combinations of $1, 2, ..., d-1$ rows of G and check the weights. If all weights are $\geq d$ then the minimum distance is at least d.

Step 4. If g is not all-one vector then $g = g + 1$, Step 1.

END.

To obtain the nonequivalent codes among the constructed codes of given length we use a transformation into linear binary codes shown in [3] ($0 \to 000$, $1 \to 011$, $\omega \to 101, \bar{\omega} \to 110$) and we check for equivalence the obtained binary images by the program package Q-Extension [1].

4. Results. In this section we construct some ACG codes of lengths $34 \leq n \leq 39$ with maximum d that the codes of this type can reach. Grassl and Harada [7] performed a computer search of ACG codes over $\mathbb{F}_4$ of length up to 100 and obtained a lot of new results. One of their results is the constructed code of length 36 with minimum weight $d = 11$. Here we prove the uniqueness of this code. Also, we improve the lower bounds of the number of codes for lengths 34, 35, 37, 38, and 39. In [7] by exhaustive search was found that the maximum possible minimum weight for ACG codes is: $d = 10$ (for $n = 34, 35$), $d = 11$ (for $n = 36, 37, 39$), and $d = 12$ (for $n = 38$).

The obtained classification results are the following:

- $n = 34$: For $d = 10$, we construct 295 nonequivalent codes.
- $n = 35$: For $d = 10$, we construct 81 nonequivalent codes.
- $n = 36$: In [7] a code with $d = 11$ was constructed. By exhaustive search we construct 6 ACG codes with $d = 11$. Practically, in this case only the exhaustive search is possible because of the small number of ACG codes with these parameters. After check for equivalence, we obtain that all of them are equivalent to the code constructed in [7]. Theferore, there exists a unique ACG code of length 36 with minimum weight 11.
- $n = 37$: For $d = 11$, we construct 10 nonequivalent codes.

- $n = 38$: For $d = 12$, we construct 7 nonequivalent codes. It is known [7] that a code with these parameters can be only of *Type II*.
- $n = 39$: For $d = 11$, we construct 5 nonequivalent codes.

In Table 1 we summarize the obtained results.

Table 1. ACG codes of length $34 \leq n \leq 39$ for the maximum reached d

n	d	old number	new number	*Type I*	*Type II*
34	10	≥ 144 [15]	≥ 295	≥ 36	≥ 259
35	10	≥ 12 [15]	≥ 81	≥ 81	–
36	11	≥ 1 [7]	**1**	1	–
37	11	≥ 1 [7]	≥ 10	≥ 10	–
38	12	≥ 1 [7]	≥ 7	–	≥ 7
39	11	≥ 1 [7]	≥ 5	≥ 5	–

5. Conclusions. Here we considered a special class of additive self-dual codes over $\mathbb{F}_4$. By exhaustive computer search we proved the uniqueness of the ACG code of length 36 with minimum weight 11. Also, we constructed new ACG codes of length 34, 35, 37, 38 and 39 for the maximum reached minimum weight and in this way we improved the lower bounds for the number of codes with these parameters.

REFERENCES

[1] Bouyukliev I. What is Q-extension? *Serdica J. Computing*, **1** (2007), 115–130.

[2] Bouyukliev I., V. Bakoev. Efficient computing of some vector operations over $GF(3)$ and $GF(4)$. *Serdica J. Computing*, **2** (2008), 101–108.

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

[4] Danielsen L. Graph-Based Classification of Self-Dual Additive Codes over Finite Fields. *Adv. Math. Commun.*, **3** (2009), No 4, 329–348.

[5] Danielsen L., M. Parker. On the classification of all self-dual additive codes over GF(4) of length up to 12. *J. Combin. Theory*, Series A, **113** (2006), No 7, 1351–1367.

[6] Gaborit P., W. C. Huffman, J. L. Kim, V. Pless. On additive GF(4)-codes. In: DIMACS Workshop on Codes and Association Schemes. *DIMACS Series in Discrete Math. and Theoret. Computer Science*, Amer. Math. Society, **56** (2001), 135–149.

[7] Grassl M., M. Harada. New self-dual additive F_4-codes constructed from circulant graphs. *Discrete Mathematics*, **340** (2017), No 3, 399–403.

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

[9] Höhn G. Self-dual codes over the Kleinian four group. *Math. Ann.*, **327** (2003), No 2, 227–255. arXiv:math.CO/0005266.

[10] Kim J. L., V. Pless. Designs in additive codes over GF(4). *Design, Codes, and Cryptography*, **30** (2003), 187–199.

[11] Li R., X. Li, Y. Mao, M. Wei. Searching for (near) optimal codes. In: Proc. of 9^{th} International Conference on Combinatorial Optimization and Applications, Houston, USA, 2015, 521–536.

[12] Rains E. M., N. Sloane. Self–dual codes. In: V. S. Pless and W. C. Huffman (eds). Handbook of Coding Theory. Amsterdam, Elsevier, 1998, 177–294.

[13] Schlingemann D. Stabilizer codes can be realized as graph codes. *Quantum Inf. Comput.*, **2** (2002), No 4, 307–323. arXiv:quant-ph/0111080.

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

[15] Varbanov Z. Additive circulant graph codes over GF(4). In: Proc. of 6^{th} International Workshop on Optimal Codes and Related Topics, Varna, Bulgaria, 2009, 189–195.

Zlatko Varbanov
Department of Information Technologies
Faculty of Mathematics and Informatics
University of Veliko Tarnovo
5000 V. Tarnovo, Bulgaria
e-mail: `vtgold@yahoo.com`

Maya Hristova
Department of Information Technologies
Faculty of Mathematics and Informatics
University of Veliko Tarnovo
5000 V. Tarnovo, Bulgaria
e-mail: `maqhristova@gmail.com`

Received August 29, 2017
Final Accepted February 24, 2018