SELF-DUAL ADDITIVE $\mathbb{F}_4$-CODES OF LENGTHS UP TO 40 REPRESENTED BY CIRCULANT GRAPHS

KEN SAITO
Research Center for Pure and Applied Mathematics
Graduate School of Information Sciences
Tohoku University, Sendai 980–8579, Japan
(Communicated by Markus Grassl)

ABSTRACT. In this paper, we consider additive circulant graph codes which are self-dual additive $\mathbb{F}_4$-codes. We classify all additive circulant graph codes of length $n = 30, 31$ and $34 \leq n \leq 40$ having the largest minimum weight. We also classify bordered circulant graph codes of lengths up to 40 having the largest minimum weight.

1. Introduction

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field of two elements and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ be the finite field of four elements where $\omega^2 = \omega + 1$. An additive $\mathbb{F}_4$-code $C$ of length $n$ is an additive subgroup of $\mathbb{F}_4^n$. An additive $(n, 2^k)$ $\mathbb{F}_4$-code $C$ is a code of length $n$ which contains $2^k$ codewords. A generator matrix of an additive $(n, 2^k)$ $\mathbb{F}_4$-code $C$ is a $k \times n$ matrix whose rows are a basis of $C$. The weight of a vector $c$ is the number of nonzero components of $c$. The minimum weight of a code $C$ is the smallest weight among all nonzero codewords of $C$. An additive $(n, 2^k)$ $\mathbb{F}_4$-code having minimum weight $d$ is called an additive $(n, 2^k, d)$ $\mathbb{F}_4$-code.

Two additive $\mathbb{F}_4$-codes $C_1$ and $C_2$ are called 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 multiplication of coordinates by nonzero elements of $\mathbb{F}_4$, followed by possible conjugation of the coordinates. The conjugation of $x \in \mathbb{F}_4$ is defined by $\bar{x} = x^2$. All self-dual additive $\mathbb{F}_4$-codes of length $n$ were classified by Calderbank, Rains, Shor and Sloane [3] for $n \leq 5$. All self-dual additive $\mathbb{F}_4$-codes can be applied to designing DNA codes for use in DNA computing and solving problems of DNA codes which satisfy some constraints [11]. A self-dual additive $(n, 2^n, d)$ $\mathbb{F}_4$-code gives a quantum $[[n, 0, d]]$ code (see [3] for a description of quantum codes). These are motivations for our study of self-dual additive $\mathbb{F}_4$-codes.

Two additive $\mathbb{F}_4$-codes $C_1$ and $C_2$ are called 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 multiplication of coordinates by nonzero elements of $\mathbb{F}_4$, followed by possible conjugation of the coordinates. The conjugation of $x \in \mathbb{F}_4$ is defined by $\bar{x} = x^2$. All self-dual additive $\mathbb{F}_4$-codes of length $n$ were classified by Calderbank, Rains, Shor and Sloane [3] for $n \leq 5$. All self-dual...
additive $\mathbb{F}_4$-codes of length $n$ were classified by using $n \times n$ adjacency matrices of graphs for $1 \leq n \leq 12$, by Danielsen and Parker [5]. Varbanov [10] constructed some self-dual additive $\mathbb{F}_4$-codes from adjacency matrices of circulant graphs. All additive circulant graph codes of length $13 \leq n \leq 29$ and $31 \leq n \leq 33$ having the largest minimum weight were classified by Varbanov [10]. All bordered circulant graph codes of length $n = 2, 3, 6, 8, 9, 14, 15, 18, 20, 22$ having the largest minimum weight were classified by Danielsen and Parker [6].

A graph code is an additive $\mathbb{F}_4$-code with generator matrix $\Gamma + \omega I$ where $\Gamma$ is the adjacency matrix of a graph and $I$ is the identity matrix. In this paper, we classify all additive circulant graph codes having the largest minimum weight for length $n = 30$ and $34 \leq n \leq 40$, and classify all bordered circulant graph codes having the largest minimum weight for length $n = 4, 5, 7, 10, 11, 12, 13, 16, 17, 18, 19, 21, 23, \ldots, 40$. All computer calculations were done using Magma [2].

### 2. Self-dual additive $\mathbb{F}_4$-codes from graphs

A self-dual additive $\mathbb{F}_4$-code is called Type II if all codewords have even weights, it is called Type I otherwise. It is known that there is a Type II additive $\mathbb{F}_4$-code of length $n$ if and only if $n$ is even.

A (simple) graph is a pair $(V, E)$ where $V = \{v_1, \ldots, v_n\}$ is a finite set of vertices, and $E$ is a set of edges. Here, an edge is a 2-subset of $V$. The adjacency matrix of a graph $(V, E)$ is an $n \times n$ $\mathbb{F}_2$-matrix $(a_{ij})$ where $a_{ij} = a_{ji} = 1$ if $\{v_i, v_j\} \in E$, and $a_{ij} = a_{ji} = 0$ otherwise. Let $\Gamma$ denote the adjacency matrix of a graph. Then $\Gamma$ is a symmetric matrix with the diagonal elements all zero.

Any graph code is self-dual [5]. It was shown that for any self-dual additive $\mathbb{F}_4$-code $C$, there is a graph code $C(\Gamma)$ such that $C$ and $C(\Gamma)$ are equivalent [5]. This means that self-dual additive $\mathbb{F}_4$-codes can be represented by the adjacency matrices of some graphs. We can restrict our study to self-dual additive $\mathbb{F}_4$-codes with generator matrices of the form $\Gamma + \omega I$. In [5], all self-dual additive $\mathbb{F}_4$-codes of length $n$ were classified by classifying graphs with $n$ vertices for $n \leq 12$.

It seems to be hard to give a classification and determine the largest minimum weight for all self-dual additive $\mathbb{F}_4$-codes of length 13 or more. We consider only a special form of an adjacency matrix of a graph. An $n \times n$ matrix of the form

$$
\begin{pmatrix}
    b_0 & b_1 & \cdots & b_{n-2} & b_{n-1} \\
    b_{n-1} & b_0 & b_1 & \cdots & b_{n-2} \\
    b_{n-2} & b_{n-1} & b_0 & \cdots & b_{n-3} \\
    \vdots & \ddots & \ddots & \ddots & \vdots \\
    b_1 & \cdots & b_{n-2} & b_{n-1} & b_0
\end{pmatrix}
$$

(1)

is called a circulant matrix. A graph $G$ is called a circulant graph if the adjacency matrix of $G$ is circulant. Circulant graphs have been studied widely (see e.g., [1, 4, 7]). Varbanov [10] focused on constructing additive $\mathbb{F}_4$-codes from circulant graphs to restrict the search space. A graph code $C(\Gamma)$ is called an additive circulant graph code if $\Gamma$ is circulant. A symmetric matrix of the form (1) has the property that $b_i = b_{n-i}$ ($i = 1, \ldots, \lfloor n/2 \rfloor$). Thus, an additive circulant graph code $C(\Gamma)$ depends on the first $\lfloor n/2 \rfloor$ coordinates $(b_1, \ldots, b_{\lfloor n/2 \rfloor})$.

Danielsen and Parker [6] considered graphs with the following $n \times n$ adjacency matrices:
where $\Gamma$ are the adjacency matrices of graphs with $n - 1$ vertices (more generally, Danielsen and Parker [6] considered additive $\mathbb{F}_4$-codes $C(\Gamma^*)$ with generator matrices $\Gamma^* + \omega I$ where $\Gamma^*$ are the adjacency matrices of directed graphs). Let $C(\Gamma)$ denote the additive $\mathbb{F}_4$-code with generator matrix $\Gamma + \omega I$. We call $C(\Gamma)$ a bordered circulant graph code. Any bordered circulant graph code is self-dual since it is a graph code.

**Proposition 1.** A bordered circulant graph code of even length is always Type II.

**Proof.** Consider a bordered circulant graph code $C(\Gamma)$ of length $n$ where $\Gamma$ is the adjacency matrix of a graph with $n - 1$ vertices. Suppose that $n$ is even. Then the first row $(b_0, b_1, \ldots, b_{n-2})$ of $\Gamma$ has even weight since $\Gamma$ is symmetric and the first row satisfies the property $b_i = b_{n-1-i}$ $(i = 1, \ldots, n-2)$. Thus, each row of $\Gamma + \omega I$ has even weight. It is shown that a graph code $C(\Gamma')$ is Type II if and only if all the vertices of a graph with adjacency matrix $\Gamma'$ have odd degrees, in other words, each row of $\Gamma' + \omega I$ has even weight [5]. Therefore, $C(\Gamma)$ is Type II. \hfill $\square$

To obtain all inequivalent codes among the constructed additive circulant graph codes, we use the following method, by Calderbank, Rains, Shor and Sloane [3]. We map the additive $(n, 2^k) \mathbb{F}_4$-code $C$ to the binary $[3n, k]$ code $C(\beta(C))$ by applying the map $\beta : 0 \mapsto (000), 1 \mapsto (011), \omega \mapsto (101), \omega^2 \mapsto (110)$ to the coordinates of $C$. Then, two self-dual additive $\mathbb{F}_4$-codes $C$ and $C'$ are equivalent if and only if the two binary codes $\beta(C)$ and $\beta(C')$ are equivalent.

3. ADDITIVE CIRCULANT GRAPH CODES OF LENGTHS UP TO 40

Let $d_{\max}^A(n)$ denote the largest integer $d$ such that a circulant graph code $C(\Gamma)$ of length $n$ which has minimum weight $d$ exists. In this section, we give a classification of additive circulant graph codes of length $n$ having the largest minimum weight $d_{\max}^A(n)$ for $1 \leq n \leq 12$, $n = 30, 31$ and $34 \leq n \leq 40$.

Varbanov [10] determined $d_{\max}^A(n)$ for $n \leq 33$. Grassl and Harada [8] determined $d_{\max}^A(n)$ for $34 \leq n \leq 50$. All additive circulant graph codes of length $13 \leq n \leq 29$ and $31 \leq n \leq 33$ having the largest minimum weight $d_{\max}^A(n)$ were classified, up to equivalence, by Varbanov [10].

By exhaustive computer search, we found all distinct Type I and Type II additive circulant graph codes $C(\Gamma)$ having the largest minimum weight $d_{\max}^A(n)$ for length $1 \leq n \leq 12$, $n = 30$ and $34 \leq n \leq 40$. Then, by the method described in Section 2, we determined by MAGMA [2] whether two additive circulant graph codes are equivalent or not. Then we have a classification of the additive circulant graph codes of length $n$ having minimum weight $d_{\max}^A(n)$ for $1 \leq n \leq 12$, $n = 30, 31$ and $34 \leq n \leq 40$ where $d_{\max}^A(n)$ is listed in Table 1. Let $\text{num}_I^A(n)$ and $\text{num}_{III}^A(n)$ denote the numbers of inequivalent Type I and Type II additive circulant graph codes of length $n$ having the minimum weight $d_{\max}^A(n)$, respectively. To save space, we only list $\text{num}_I^A(n)$ and $\text{num}_{II}^A(n)$ in Table 1. The fifth and tenth columns of Table 1 provide references for $\text{num}_I^A(n)$ and $\text{num}_{II}^A(n)$. We remark that $\text{num}_{III}^A(36) = 0$ since $d_{\max}^A(36)$ is odd. For the additive circulant graph codes $C(\Gamma)$ in Table 1, the
first rows of $\Gamma$ can be obtained from http://www.ims.is.tohoku.ac.jp/~ksaito/codes/acgf4.html.

| $n$ | $d_{\text{max}}^{A}(n)$ | num$_{A}^{I}(n)$ | num$_{A}^{II}(n)$ | Ref. | $n$ | $d_{\text{max}}^{A}(n)$ | num$_{A}^{I}(n)$ | num$_{A}^{II}(n)$ | Ref. |
|-----|--------------------------|------------------|------------------|------|-----|--------------------------|------------------|------------------|------|
| 1   | 1                        | 1                | -                |      | 21 | 7                        | 11               | -                | [10] |
| 2   | 2                        | 0                | 1                |      | 22 | 8                        | 0                | 14               | [10] |
| 3   | 2                        | 1                | -                |      | 23 | 8                        | 2                | -                | [10] |
| 4   | 2                        | 1                | 2                |      | 24 | 8                        | 5                | 46               | [10] |
| 5   | 3                        | 1                | -                |      | 25 | 8                        | 31               | -                | [10] |
| 6   | 4                        | 0                | 1                |      | 26 | 8                        | 49               | 161              | [10] |
| 7   | 3                        | 1                | -                |      | 27 | 8                        | 140              | -                | [10] |
| 8   | 4                        | 0                | 1                |      | 28 | 10                       | 0                | 1                | [10] |
| 9   | 4                        | 1                | -                |      | 29 | 11                       | 1                | -                | [10] |
| 10  | 4                        | 3                | 5                |      | 30 | 12                       | 0                | 1                |      |
| 11  | 4                        | 2                | -                |      | 31 | 10                       | 5                | -                |      |
| 12  | 6                        | 0                | 1                |      | 32 | 10                       | 2                | 106              | [10] |
| 13  | 5                        | 2                | -                | [10] | 33 | 10                       | 76               | -                | [10] |
| 14  | 6                        | 0                | 3                | [10] | 34 | 10                       | 115              | 851              |      |
| 15  | 6                        | 2                | -                | [10] | 35 | 10                       | 595              | -                |      |
| 16  | 6                        | 1                | 5                | [10] | 36 | 11                       | 1                | 0                |      |
| 17  | 7                        | 1                | -                | [10] | 37 | 11                       | 17               | -                |      |
| 18  | 6                        | 16               | 36               | [10] | 38 | 12                       | 0                | 22               |      |
| 19  | 7                        | 4                | -                | [10] | 39 | 11                       | 276              | -                |      |
| 20  | 8                        | 0                | 2                | [10] | 40 | 12                       | 0                | 213              |      |

Table 1. Additive circulant graph codes

Note that num$_{A}^{I}(31)$ is incorrectly reported in [10] as 62. We claim that num$_{A}^{I}(31)$ is 5.

**Proposition 2.** There are five Type I additive circulant graph codes of length 31 having minimum weight 10, up to equivalence.

We give an observation of some codes given in Table 1. The five inequivalent Type I additive circulant graph codes with parameters $(31, 2^{31}, 10)$ in Table 1 are constructed as the codes $C(\Gamma_{31}^{(i)})$ $(i = 1, \ldots, 5)$ where $\Gamma_{31}^{(i)}$ are the $31 \times 31$ circulant matrices with the following first rows $r_{31}^{(i)}$:

\[
\begin{align*}
    r_{31}^{(1)} &= (010111110001110011000111111101), \\
    r_{31}^{(2)} &= (010111110100011001100010111101), \\
    r_{31}^{(3)} &= (0011000011011001100110101000110), \\
    r_{31}^{(4)} &= (011010000111011011011000011011), \\
    r_{31}^{(5)} &= (000111011011011001101010111100).
\end{align*}
\]

We calculated by MAGMA [2] the weight distribution of each code $C(\Gamma_{31}^{(i)})$ $(i = 1, \ldots, 5)$. The weight distributions are listed in Table 2 where $A_{i}$ denotes the number of codewords of weight $i$. The weight distributions also yield that these codes are inequivalent. The unique additive circulant graph code with parameters $(30, 2^{30}, 12)$ in Table 1 is constructed as the code $C(\Gamma_{30})$ where $\Gamma_{30}$ is the $30 \times 30$ circulant matrix with the following first row:

\[
(001110110100111100101101110110111100).
\]
We verified by Magma [2] that the code $C(\Gamma_{30})$ is equivalent to the extended quadratic residue code $Q_{30}$ described in [9]. The weight distribution of $Q_{30}$ is given in [9, Table I]. The weight distribution of the unique additive circulant graph code with parameters $(36, 2^{36}, 11)$ in Table 1 is given in [8, Table 2].

4. Bordered circulant graph codes of lengths up to 40

Let $d_{\text{max}}(n)$ denote the largest integer $d$ such that a bordered circulant graph code $C(\Gamma)$ of length $n$ which has minimum weight $d$ exists. In this section, we give a classification of bordered circulant graph codes of length $n$ having the largest minimum weight $d_{\text{max}}(n)$ for $n = 4, 5, 7, 10, 11, 12, 13, 16, 17, 18, 19, 21, 23, \ldots, 40$.

As described above, Danielsen and Parker [6] considered additive $\mathbb{F}_4$-codes constructed from not only graphs but also directed graphs. It follows that all bordered circulant graph codes for length $n = 2, 3, 6, 8, 9, 14, 15, 18, 20, 22$ having the largest minimum weight $d_{\text{max}}(n)$ were classified.
By exhaustive computer search, we determined the largest minimum weight $d_{B_{\text{max}}}^B(n)$ of bordered circulant graph codes of length $n$ while we found all distinct bordered circulant graph codes of length $n$ having the largest minimum weight $d_{B_{\text{max}}}^B(n)$ for $n = 4, 5, 7, 10, 11, 12, 13, 16, 17, 18, 19, 21, 23, \ldots, 40$. Then, by the method described in Section 2, we classified all the bordered circulant graph codes of length $n$ having minimum weight $d_{B_{\text{max}}}^B(n)$ where $d_{B_{\text{max}}}^B(n)$ is listed in Table 3. Let $\text{num}^B_B(n)$ denote the number of inequivalent bordered circulant graph codes of length $n$ having the minimum weight $d_{B_{\text{max}}}^B(n)$. To save space, we only list $\text{num}^B_B(n)$ for $2 \leq n \leq 40$ in Table 3. The fourth and eighth columns of Table 3 provide references for $d_{B_{\text{max}}}^B(n)$ and $\text{num}^B_B(n)$. For the bordered circulant graph codes $C(\Gamma)$ in Table 3, the first rows of $\Gamma$ can be obtained from http://www.ims.is.tohoku.ac.jp/~ksaito/codes/bcfg4.html.

| $n$ | $d_{B_{\text{max}}}^B(n)$ | $\text{num}^B_B(n)$ | Ref. | $n$ | $d_{B_{\text{max}}}^B(n)$ | $\text{num}^B_B(n)$ | Ref. |
|-----|-----------------|------------------|------|-----|-----------------|------------------|------|
| -   | -               | -                | -    | 21  | 6               | 34               | -    |
| 2   | 2               | 1                | [6]  | 22  | 8               | 3                | [6]  |
| 3   | 2               | 1                | [6]  | 23  | 7               | 20               |      |
| 4   | 2               | 1                |      | 24  | 8               | 11               |      |
| 5   | 2               | 2                |      | 25  | 8               | 18               |      |
| 6   | 4               | 1                | [6]  | 26  | 8               | 14               |      |
| 7   | 3               | 1                |      | 27  | 8               | 70               |      |
| 8   | 4               | 1                | [6]  | 28  | 8               | 102              |      |
| 9   | 4               | 1                | [6]  | 29  | 9               | 1                |      |
| 10  | 4               | 1                |      | 30  | 12              | 1                |      |
| 11  | 4               | 3                |      | 31  | 10              | 1                |      |
| 12  | 4               | 1                |      | 32  | 10              | 41               |      |
| 13  | 5               | 1                |      | 33  | 10              | 31               |      |
| 14  | 6               | 2                | [6]  | 34  | 10              | 368              |      |
| 15  | 6               | 1                | [6]  | 35  | 10              | 381              |      |
| 16  | 6               | 3                |      | 36  | 10              | 249              |      |
| 17  | 6               | 4                |      | 37  | 11              | 1                |      |
| 18  | 8               | 1                | [6]  | 38  | 12              | 4                |      |
| 19  | 6               | 25               |      | 39  | 11              | 22               |      |
| 20  | 8               | 2                | [6]  | 40  | 12              | 27               |      |

Table 3. Bordered circulant graph codes

We give an observation of some codes given in Table 3. We verified by Magma [2] that the unique bordered circulant graph code with parameters $(18, 2^{18}, 8)$ in Table 3 is equivalent to the extended quadratic residue code $S_{18}$ described in [9]. Danielsen and Parker [6] constructed a self-dual additive $F_4$-code with parameters $(30, 2^{30}, 12)$ by bordering a quadratic residue code. The unique bordered circulant graph codes with parameters $(29, 2^{29}, 9), (30, 2^{30}, 12), (31, 2^{31}, 10)$ and $(37, 2^{37}, 11)$ in Table 3 are constructed as the codes $C(\Gamma_{28}), C(\Gamma_{29}), C(\Gamma_{30})$ and $C(\Gamma_{36})$, respectively, where $\Gamma_{n-1}$ are the $(n-1) \times (n-1)$ circulant matrices with the following first rows $r_{n-1}$ ($n = 29, 30, 31, 37$):

$r_{28} = (011111101101110011001011111111),$

$r_{29} = (01001110100001000100011111111111),$

$r_{30} = (0110101111111001001111111101011),$
We verified by Magma [2] that the code $C(\Gamma_{29})$ is equivalent to $Q_{30}$. We calculated by Magma [2] the weight distribution of each code $C(\Gamma_{n-1})$ ($n = 29, 30, 31, 37$). The weight distributions are listed in Table 4.

![Table 4](image)

### Acknowledgments

The author would like to thank supervisor Professor Masaaki Harada for introducing the problem, and his helpful advice and encouragement.

### References

[1] B. Alspach and T. D. Parsons, Isomorphism of circulant graphs and digraphs, *Discrete Math.*, 25 (1979), 97–108.

[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.*, 24 (1997), 235–265.

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

[4] S. Cichacz and D. Froncek, Distance magic circulant graphs, *Discrete Math.*, 339 (2016), 84–94.

[5] L. E. Danielsen and M. G. Parker, On the classification of all self-dual additive codes over $GF(4)$ of length up to 12, *J. Combin. Theory Ser. A*, 113 (2006), 1351–1367.

[6] L. E. Danielsen and M. G. Parker, Directed graph representation of half-rate additive codes over $GF(4)$, *Des. Codes Cryptogr.*, 59 (2011), 119–130.

[7] B. Elspas and J. Turner, Graphs with circulant adjacency matrices, *J. Combinatorial Theory*, 9 (1970), 297–307.
[8] M. Grassl and M. Harada, New self-dual additive $\mathbb{F}_4$-codes constructed from circulant graphs, *Discrete Math.*, **340** (2017), 399–403.

[9] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane and H. N. Ward, Self-dual codes over $\mathbb{GF}(4)$, *J. Combin. Theory Ser. A*, **25** (1978), 288–318.

[10] Z. Varbanov, Additive circulant graph codes over $\mathbb{GF}(4)$, *Math. Maced.*, **6** (2008), 73–79.

[11] Z. Varbanov, T. Todorov and M. Hristova, A method for constructing DNA codes from additive self-dual codes over $\mathbb{GF}(4)$, *ROMAI J.*, **10** (2014), 203–211.

Received for publication January 2017.

*E-mail address:* kensaito@ims.is.tohoku.ac.jp