

On Construction of Good Quaternary Additive Codes

Luo-Bin Guo, Yang Liu, Liang-Dong Lu and Rui-Hu Li

School of Science, Air Force Engineering University, Xi'an, shaanxi 710051, China

Abstract. In this paper we present construction of some additive codes with very good parameters over the four elements finite field, each of these quaternary additive codes has double code words than its corresponding optimal linear code of the same length and minimum distance.

1. Introduction

Additive codes are generalizations of linear codes over finite fields, they have close relations with quantum error-correcting codes, for a general introduction of additive codes and a theory of quantum codes, please see [1] and [2]. In [3-7], some authors discussed the parameters of optimal additive codes and explicit construction of short length additive codes with length $n \leq 15$ and leaves several cases unsolved. The results of [3-5] shows that, for length $n \leq 15$, there are quaternary additive codes have double codewords than their corresponding optimal linear code of the same length and minimum distance. As for larger length additive codes, little are known on their parameters, let alone on construction of additive codes with good parameters and compare them with their counterpart linear codes. Thus, it is an interesting topic to discuss construction of additive codes with good parameters.

Here we concentrate on the construction of good quaternary additive codes. Before give our discussion, let us introduce some basic knowledge on quaternary field, quaternary additive codes and make some notations.

Let $F_4 = \{0, 1, \omega, \bar{\omega}\}$ be the Galois field with four elements such that $\bar{\omega} = 1 + \omega = \omega^2$, $\omega^3 = 1$, and the conjugation is defined by $\bar{x} = x^2$. An additive subgroup C of F_4 is called an additive code over F_4 . If C contains 2^m vectors, C is called an $(n, 2^m)$ additive code. A matrix whose rows form a base of C over F_2 is called an additive generator matrix of C . Especially, if C is a k -dimensional subspace of F_4^n over F_4 , C is called a linear code over F_4 and is denoted as $[n, k]_4$. It is easy to see that an $[n, k]_4$ code is an additive $(n, 2^m) = [n, 2^{2k}]$ code. However, generally, an

$[n, 2^{2k}]$ additive code is not a linear code, for details please see [1].

An $[n, k, d]_4$ linear code is called an optimal linear code if there is no $[n, k, d+1]_4$ code, neither $[n, k+1, \geq d]_4$ code. For details on parameters of optimal linear code over F_4 , please see [8].

Notation: In the following of this paper, we use $G = (a_{ij})_{m \times n}$ to denote an additive generator matrix of an additive $(n, 2^m)$ code C , in order to present the matrices in compact form, we use '2' to denote ω and use '3' to denote $\bar{\omega}$ in the remain of this paper.

2. Construction of Additive Code

In this subsection, we construct generator matrices of some additive codes by combinational method, our discussion is presented in two cases.

Case I: construction of $(n, 2^5, d)$ additive codes.

To save space, we need some special matrices as follows.

Let

$$0_3 = (0, 0, 0), 1_3 = (1, 1, 1), 2_3 = (2, 2, 2),$$

$$0_4 = (0, 0, 0, 0), 1_4 = (1, 1, 1, 1),$$

$$2_4 = (2, 2, 2, 2), 3_4 = (3, 3, 3, 3),$$

$$X = (0, 1, 2, 3), Y = (1, 3, 2, 0),$$

$$G_{5,31} = \begin{pmatrix} 0_4 & 1_4 & 1_4 & 1_4 & 1_4 & 1_4 & 1_4 & 1_4 & 0_3 \\ 1_4 & 0_4 & 1_4 & 2_4 & 2_4 & 2_4 & 2_4 & 2_4 & 0_3 \\ 3_4 & 2_4 & 3_4 & 0_4 & 1_4 & 2_4 & 3_4 & 0_3 & \\ X & X & X & X & X & X & X & X & 1_3 \\ Y & Y & Y & Y & Y & Y & Y & Y & 2_3 \end{pmatrix}.$$

It is not difficult to check that $G_{5,31}$ generates an additive code $C_{5,31}$ with parameters $(31, 2^5, 24)$, and the weight polynomial of this code is $1 + 31z^{24}$.

Puncturing $C_{5,31}$ on coordinate 1, 2, 3, 4, 29, one can obtain an additive code $C_{5,26}$ with parameters $(26, 2^5, 20)$, and the weight polynomial of this code is $1 + 30z^{20} + z^{24}$.

CaseII: construction of $(n, 2^7, d)$ additive codes.

In this case, we use combinational and inductive methods to construct additive codes. Firstly, define

$$A_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 3 & 1 & 1 & 3 & 2 & 0 \\ 3 & 1 & 2 & 1 & 2 & 0 & 3 \\ 3 & 2 & 1 & 3 & 0 & 1 & 2 \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 3 & 1 & 1 & 3 & 2 & 0 \\ 3 & 1 & 2 & 1 & 2 & 0 & 3 \\ 3 & 2 & 1 & 3 & 0 & 1 & 2 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 2 & 3 & 1 & 1 & 3 & 2 & 0 \\ 3 & 1 & 2 & 1 & 2 & 0 & 3 \\ 3 & 2 & 1 & 3 & 0 & 1 & 2 \end{pmatrix}$$

$$A_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 3 & 1 & 1 & 3 & 2 & 0 \\ 3 & 1 & 2 & 1 & 2 & 0 & 3 \\ 3 & 2 & 1 & 3 & 0 & 1 & 2 \end{pmatrix}$$

$$A_5 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 3 & 1 & 1 & 3 & 2 & 0 \\ 3 & 1 & 2 & 1 & 2 & 0 & 3 \\ 3 & 2 & 1 & 3 & 0 & 1 & 2 \end{pmatrix}$$

$$B_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 3 & 1 & 1 & 3 & 2 & 0 \\ 3 & 1 & 2 & 1 & 2 & 0 & 3 \\ 3 & 2 & 1 & 3 & 0 & 1 & 2 \end{pmatrix}$$

$$B_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 3 & 1 & 1 & 3 & 2 & 0 \\ 3 & 1 & 2 & 1 & 2 & 0 & 3 \\ 3 & 2 & 1 & 3 & 0 & 1 & 2 \end{pmatrix}$$

$$B_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 2 & 3 & 1 & 1 & 3 & 2 & 0 \\ 3 & 1 & 2 & 1 & 2 & 0 & 3 \\ 3 & 2 & 1 & 3 & 0 & 1 & 2 \end{pmatrix}$$

$$B_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 3 & 1 & 1 & 3 & 2 & 0 & 0 \\ 3 & 1 & 2 & 1 & 2 & 0 & 3 & 0 \\ 3 & 2 & 1 & 3 & 0 & 1 & 2 & 0 \end{pmatrix}$$

$$B_5 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 3 & 1 & 1 & 3 & 2 & 0 & 0 \\ 3 & 1 & 2 & 1 & 2 & 0 & 3 & 0 \\ 3 & 2 & 1 & 3 & 0 & 1 & 2 & 0 \end{pmatrix}$$

$$G_{7,31} = \begin{pmatrix} 0_{31} \\ 0_{31} \\ G_{5,31} \end{pmatrix}$$

Using the above matrices as blocks, we can construction four matrices as follows:

$$G_{7,35} = (A_1, A_2, A_3, A_4, A_5)$$

$$G_{7,72} = (B_1, B_2, B_2, B_3, B_3, B_4, B_4, B_4, B_5)$$

$$G_{7,96} = (B_1, B_1, G_{7,72}, B_5)$$

$$G_{7,127} = (B_1, B_1, B_1, \dots, B_4, G_{7,31})$$

It is not difficult to check that $G_{7,35}$ generates an additive code $C_{7,35}$ with parameters $(35, 2^7, 26)$, and the weight polynomial of this code is $1 + 105z^{26} + 15z^{28} + 7z^{30}$. Puncturing $C_{7,35}$ on any one coordinate of $G_{7,35}$, one can obtain an additive code $C_{7,34}$ with parameters $(34, 2^7, 25)$, and it is not difficult to calculate the weight polynomial of this code $C_{7,34}$ is $1 + 78z^{25} + 27z^{26} + 12z^{27} + 3z^{28} + 6z^{29} + z^{30}$.

Similarly, we can check that $G_{7,72}$ generates an additive code $C_{7,72}$ with parameters $(72, 2^7, 54)$, and the weight polynomial of this code $C_{7,72}$ is $1 + 112z^{54} + 12z^{56} + 3z^{64}$.

Puncturing $C_{7,72}$ on the first coordinate, one can obtain an additive code $C_{7,71}$ with parameters $(71, 2^7, 53)$, and the weight polynomial of this code is $1 + 84z^{53} + 28z^{54} + 12z^{55} + 3z^{64}$. Puncturing $C_{7,72}$ on the ninth coordinate, one can obtain another additive code $C'_{7,71}$ with parameters $(71, 2^7, 53)$, and the weight polynomial of this new code is $1 + 84z^{53} + 28z^{54} + 9z^{55} + 3z^{56} + 3z^{64}$. Hence, we know there are at least two non equivalent additive codes with parameters $(71, 2^7, 53)$.

The matrix $G_{7,96}$ generates an additive code $C_{7,96}$ with parameters $(96, 2^7, 72)$, and the weight polynomial of this code is $1 + 118z^{72} + 9z^{80}$.

Puncturing $C_{7,96}$ on the first coordinate, one can obtain an additive code $C_{7,95}$ with parameters $(95, 2^7, 71)$, and the weight polynomial of this code is $1 + 87z^{71} + 31z^{72} + 9z^{79}$. Puncturing $C_{7,96}$ on the twenty-fifth coordinate, one can obtain another additive code $C'_{7,95}$ with parameters $(95, 2^7, 71)$, and the weight polynomial of this new code is $1 + 90z^{71} + 38z^{72} + 6z^{79} + 3z^{80}$. Hence, we know there are at least two non equivalent additive codes with parameters $(95, 2^7, 71)$.

The matrix $G_{7,127}$ generates an additive code $C_{7,127}$ with parameters $(127, 2^7, 96)$, and the weight polynomial of this code is $1 + 127z^{96}$.

3. Discussion and Conclusion

According to Ref.[8], for $n=34,35,72,71,96,95,127$ and $k=3,4$, optimal $[n, k, d]_4$ linear code has parameters as follows:

$$[35, 3, 26]_4, [35, 3, 25]_4;$$

$$[35, 4, 24]_4, [34, 4, 24]_4;$$

$$[72, 3, 54]_4, [71, 3, 53]_4;$$

$$[72, 4, 53]_4, [71, 4, 52]_4;$$

$$[96, 3, 72]_4, [95, 3, 71]_4;$$

$$[96, 4, 71]_4, [95, 4, 70]_4;$$

$$[127, 3, 96]_4, [127, 4, 95]_4.$$

Comparing the above linear codes with our additive codes given in last section, we can obtain the following fact hold:

(1) The additive code $(35, 2^7, 26)$ has double codewords than the optimal linear $[35, 3, 26]_4 = (35, 2^6, 26)$ code; the additive code $(34, 2^7, 25)$ has double codewords than the optimal linear $[34, 3, 25]_4 = (34, 2^6, 25)$ code.

(2) The additive code $(72, 2^7, 54)$ has double codewords than the optimal linear $[72, 3, 54]_4 = (72, 2^6, 54)$ code; the additive code $(71, 2^7, 53)$ has double codewords than the optimal linear $[71, 3, 53]_4 = (71, 2^6, 53)$ code.

(3) The additive code $(96, 2^7, 72)$ has double codewords than the optimal linear $[96, 3, 72]_4 = (96, 2^6, 72)$ code; the additive code $(95, 2^7, 71)$ has double codewords than the optimal linear $[95, 3, 71]_4 = (95, 2^6, 71)$ code.

(4) The additive code $(127, 2^7, 96)$ has double codewords than the optimal linear $[127, 3, 96]_4 = (127, 2^6, 96)$ code.

From [9]-[12], we know that additive codes have many new applications, we wish that using our method one can construct much more additive codes for other usage.

Whether one can further construct new good additive codes from the above $(n, 2^7, d)$ codes given in Cases II, by puncturing on several coordinates? This need further study in the future.

Acknowledgement

This work is supported by National Natural Science Foundation of China under Grant No.11471011 and Natural Science Foundation of Shaanxi under Grant No. 2017JQ1032.

References

1. A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, IEEE. T. Inform. Theory, 44, 1369-1387(1998).
2. V.Tonchev, Discrete Math., 257, 549-557(2002).
3. A.Blokhuis, A.E. Brouwer, Eur. J. Combin. 25, 161-167(2004).
4. J.Bierbrauer, G.Faina, S.Marcugini, F. Pambianco, Proc. 10th Int. Workshop Algebraic Combin. Coding Theory, Zvenigorod, Russia, 15- 18 (2006).

5. J. Bierbrauer, Y. Edel, G. Faina, S. Marcugini, F. Pambianco, IEEE. T. Inf. Theory, 55, 952-954(2009).
6. J. Bierbrauer, D. Bartoli, G. Faina, S. Marcugini F. Pambianco, Finite Fields Th. App., 26, 29-40(2015).
7. J. Bierbrauer, Introduction to Coding Theory (Chapman & Hall/CRC Press, London, 2004).
8. M. Grassl., <http://www.codetables.de>.
9. P. Gaborit, W. C. Huffman, J. L. Kim, V. Pless, DIMACS Ser. Discrete Math. Theor. Comput. Sci., Amer. Math. Soc., Providence, 56, 135-149 (2001)
10. T. A. Gulliver, J. L. Kim, IEEE. T. Inf. Theory, 50, 359-366 (2004),.
11. G. Hohn, Math. Ann., 327, 227-255 (2003).
12. W. C. Huffman, V. S. Pless, Fundamentals of Error-correcting Codes, (Cambridge University Press, Cambridge, 2003).