On the Construction of LCD Codes over F_5

Qian Song, Rui-Hu Li, Qiang Fu and Luo-Bin Guo

School of Science, Air Force Engineering University, Xi'an, Shaanxi 710051, P. R. China

Abstract. Recently, linear codes with complementary dual (LCD codes) are employed in direct-sum-masking technique for prevention of side channel attacks, which is another application on LCD codes out of data storage, communication system and consumer electronics. Follow on, they are also used to construct maximal entanglement entanglement-assisted quantum codes for protecting quantum information from noise. In this paper, by transforming known codes, some optimal LCD codes of short length with dimension 3 or 4 over F_5 are constructed, respectively.

1. Introduction

Let F_5^n be the n-dimensional row vector space over F_5, the finite field with five elements. A linear $[n,k]$ code C is a k-dimensional subspace of F_5^n. The weight $w(x)$ of $x \in C$ is the number of its nonzero coordinates, if the minimum weight of nonzero codewords in C is d, then C is denoted as $C=[n,k,d]$. The dual code $C^{\perp}$ of a linear code C is defined as

$$C^{\perp} = \{x \in F_5^n \mid x \cdot y = xy^T = \mathbf{0} \text{ for all } \mathbf{y} \in C\}. \quad (1)$$

Two codes C and C' are equivalent if one can be obtained from the other by permuting the coordinates and multiplying an monomial matrix, see [1]. A permutation matrix is a square matrix with exactly one 1 in each row and column and 0s elsewhere. A monomial matrix is a square matrix with exactly one non-zero entry in each row and column [1].

Cyclic LCD codes, called originally as reversible codes, were first introduced by Massey in 1964 [2]. After 28 years, Massey [3] then gave generalized definition of a linear LCD code as: C is said to be complementary dual if $C \cap C^{\perp} = \{\mathbf{0}\}$. He also showed that asymptotically good LCD codes exist and LCD codes can provide an optimum linear coding solution for the two-user binary adder channel.

In 2014, LCD codes were found to have an application against side-channel attacks in cryptography [4]. Since then, construction and applications on LCD codes were deeply and investigated [5-15] widely. For example, many maximal entanglement entanglement-assisted quantum codes were derived from good LCD codes [5-8]. Some optimal LCD codes are studied and constructed in the Refs. [6-15].

Ref. [2] gave equivalent conditions for an LCD code as follows:

Proposition 1.1. Let C be a linear code. Let G be a generator matrix of C and H a parity-check matrix. Then the three following properties are equivalent:

1. C is LCD.
2. The matrix HH^T is invertible.
3. The matrix GG^T is invertible.

Definition 1.2. An $[n,k]$ code C is called optimal if it has the highest weight among all the $[n,k]$ codes, such a code is denoted as $C=[n,k,d_o(n,k)]$, where $d_o = d_o(n,k) = max\{d \mid there\ is\ an\ [n,k,d]_q\ code\}$. Denote $d_l =$ $d_l(n,k)=max\{d \mid$ there is an $[n,k,d]_q$ *LCD code*$\}$. If there is a $C=[n,k,d_l(n,k)]_q$ LCD code, we call C an optimal LCD code. If there is a $C=[n,k,d_l(n,k)-1]_q$ LCD code, C is called a near optimal LCD code.

In [15], for a given linear code C, the authors showed that there is an LCD code C' which is equivalent to C. Hence to construct optimal LCD codes one needs to give optimal linear codes and construct suitable equivalent transformations formed by coordinates permutation and monomial matrix.

The objective of this paper is to study construction of optimal LCD codes over F_5. In Section 2, we give will construct LCD $[n,k]$ codes with k=3, 4 from known codes obtained in the Database of Magma [16]. Section 3 gives discussions and the conclusion.

2. Construction of 3 and 4 Dimensional LCD Codes

In this section, we discuss construction of LCD codes from known linear codes, the results are provided in two subsections.

2.1 Construction of [*n*,3] LCD Codes

In this subsection, for length n with $3 \le n \le 62$, we present optimal $[n,3,d_o]$ linear codes and construct LCD $[n,3,d_l]$ codes with $d_o = d_l$.

The Database in Magma [16-18] give $[n,3,d_o]$ code for length n satisfies $3 \le n \le 62$, denote the generator matrix of the $[n,3,d_o]$ code as $G_{n,3}$. We check these 60 optimal codes and find that 33 of them are LCD codes. These 33 codes have the following lengths n, where $n =$ 3, 4, 7, 8, 10, 11, 14, 18, 19, 20-24, 26, 33, 34, 36-40, 42, 45, 47-49, 52-57. The remaining 27 codes can be used to construct optimal LCD codes by the following steps.

Step 1.1: If $n =$ 6, 12, 13, 15, 17, 28, 35, 41, 43, 46, 59, 60, for each $G_{n,3}$, we can change $G_{n,3}$ into $G'_{n,3}$ by diagonal transformation, where the columns of $G'_{n,3}$ are all monic vectors. Then $G' = G'_{n,3}$ satisfies

$$rank(G'(G')^T) = 3.$$

Hence $G'_{n,3}$ generate optimal LCD $[n,3]$ codes. Thus we can construct 13 optimal LCD codes.

For example, the matrix

$$G_{6,3} = \begin{pmatrix} 100223 \\ 010324 \\ 001434 \end{pmatrix}$$

We denote $G_{n,k}G_{n,k}^T = T_{n,k}$, where

$$T_{6,3} = \begin{pmatrix} 321 \\ 204 \\ 142 \end{pmatrix}$$

satisfies

$$rank\left(T_{6,3}\right) = 2$$

which implies $G_{6,3}$ generates a non-LCD code; using monomial matrix, we can change $G_{6,3}$ into a monic matrix $G'_{6,3}$, which generates LCD [6,3] codes as

$$G'_{6,3} = \begin{pmatrix} 100111 \\ 010413 \\ 001243 \end{pmatrix}$$

$$T'_{6,3} = \begin{pmatrix} 434 \\ 321 \\ 410 \end{pmatrix}$$

and

$$rank(T'_{6,3}) = 3.$$

Step 1.2: If $n =$ 5,9,25,27,29,30,50,58 for each $G_{n,3}$, we can permute one or two columns of $G_{n,3}$ and change it into $G''_{n,3} = (I_3 \mid P_{n-3})$. If $G_{n,3}$ has the form of

$$G''_{n,3} = (I_3 \mid P_{n-3}) \ ,$$

then no permutation is need. Now, let

$$\mathrm{I}_3 = (\alpha_1, \alpha_2, \alpha_3),$$

for

$$\alpha_1 = (1,0,0)^T, \ \alpha_2 = (0,1,0)^T, \ \alpha_3 = (0,0,1)^T,$$

then it is not difficult to check that

$$(3\alpha_1, 3\alpha_2, \alpha_3 \mid P_2),$$

$$(3\alpha_1, 3\alpha_2, 3\alpha_3 \mid P_6),$$

$$(3\alpha_1, \alpha_2, \alpha_3 \mid P_{22}),$$

…,

$$(\alpha_1, 3\alpha_2, \alpha_3 \mid P_{55})$$

generate optimal LCD codes.
For example, the matrix

$$G_{5,3} = \begin{pmatrix} 10031 \\ 01013 \\ 00122 \end{pmatrix}$$

and

$$T_{5,3}=\begin{pmatrix}113\\113\\334\end{pmatrix}$$

satisfying

$$rank\left(T_{5,3}\right)=2,$$

which implies $G_{5,3}$ generates a non LCD code; using monomial matrix, we can change $G'_{5,3}$ into a monic matrix $G''_{5,3}$ which generates LCD $[5,3]$ code, the reason is that

$$G_{5,3}=\begin{pmatrix}10031\\01013\\00122\end{pmatrix},$$

$$G''_{5,3}=(3\alpha_1 3\alpha_2\alpha_3|\ P_2),$$

$$T''_{5,3}=\begin{pmatrix}101\\024\\141\end{pmatrix},$$

and

$$rank(G''_{5,3}G''^{T}_{5,3})=3.$$

Step 1.3: If $n=$ 31, 32, 44, 51, 61, 62, for each $G_{n,3}$,we first change $G_{n,3}$ into $G'_{n,3}$ as we did in step 1.1, then permutation one or two columns of $G'_{n,3}$ as we did in step 1.2 and transform $G'_{n,3}$ into the form

$$G''_{n,3}=(I_3\mid P_{n-3})$$

at last multiply the first three columns by suitable invertible diagonal matrix D, denote

$$G'''_{n,3}=(D\mid P_{n-3}),$$

then G''' gives an optimal LCD code. Thus we obtain 6 optimal LCD codes in this step.

For example, we first change $G_{31,3}$ into

$$G'_{31,3}=\begin{pmatrix}1001111111100001111111111111111\\0101324000011111324214334124231\\0010000132413241324132413241324\end{pmatrix}$$

then perform invertible diagonal matrix D, $G''_{31,3}$ is changed into $G'''_{31,3}=(3\alpha_1 3\alpha_2\alpha_3|\ P_{28})$,

$$T'''_{31,3}=\begin{pmatrix}300\\030\\001\end{pmatrix}$$

and $rank(T'''_{31,3})=3$.

Summarizing the previous discussion, the following theorem holds.

Theorem 2.1 If $3\le n\le 62$, there exists an optimal LCD $[n,3,d]$ code.

2.2 Construction of [n,4] LCD Codes

In this subsection, for length n with $4\le n\le 156$, we present optimal $[n,4,d_o]$ linear codes and construct LCD $[n,4,d_l]$ codes with $d_o=d_l$.

The Database in Magma [16-18] give $[n,4,d_o]$ code for length n with $4\le n\le 156$. We checked these 153 optimal codes and found that 111 of them are LCD codes. These 111 codes have the following length n, where $n=$ 4, 6-9, 12-13, 17-27, 29-31, 34-38, 41-45, 47-48, 51-57, 59-61, 63-64, 66-67, 71-73, 77-81, 84, 86-88, 90, 93-97, 99, 103-105, 107, 109-113, 115-119, 123, 127-131, 133-138, 140-147, 149-153, 156. The remaining 42 codes can be used to construct optimal LCD codes by the following steps.

Step 2.1: If $n=$ 5, 10, 11, 14-16, 28, 32, 33, 39, 40, 46, 49, 50, 62, 65, 68-70, 74, 85, 91, 92, 98, 100-102, 106, 108, 114, 120-122, 124-126, 132, 139, 148, 154, 155, for each $G_{n,4}$, we can change $G_{n,4}$ into $G'_{n,4}$, where the columns of $G'_{n,4}$ are all monic factors. Then $G'=G'_{n,4}$ satisfies $rank(G'(G')^T)=4$. Hence we can construct 36 optimal LCD codes in this way.

Step 2.2: If $n=$ 58, 75, 76, 82, 83, 89, for each $G_{n,4}$, we can permute one or two columns of $G_{n,4}$ and change it into $G''_{n,4}=(I_4\mid P_{n-4})$.

Let

$$\mathrm{I}_4=(\beta_1,\beta_2,\beta_3,\beta_4),$$

where

$$\beta_1=(1,0,0,0)^T,$$

$$\beta_2=(0,1,0,0)^T,$$

$$\beta_3=(0,0,1,0)^T,$$

$$\beta_4 = (0,0,0,1)^T.$$

Then, similar to that we did in subsection A, it is not difficult to check that

$$(\beta_1, \beta_2, \beta_3, 3\beta_4 \mid P_{54}),$$

$$(\beta_1, \beta_2, 3\beta_3, \beta_4 \mid P_{71}),$$

$$(\beta_1, 3\beta_2, \beta_3, 3\beta_4 \mid P_{72}),$$

$$\cdots$$

$$(\beta_1, \beta_2, \beta_3, 3\beta_4 \mid P_{85})$$

generate optimal LCD codes.

For example, we change $G_{58,4}$ into $G'_{58,4} = (A \mid B)$, where

$$A = \begin{pmatrix} 10003213442034314243312420321013003132 03 \\ 01003404341310241434021024230110341323 03 \\ 00100111111111000000000111111111122222 22 \\ 00030000000000111111111111111111111111 11 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 011142140233212002 \\ 212302410434032411 \\ 222333333333344444 \\ 111111111111111111 \end{pmatrix}.$$

Then

$$T_{58,4} = \begin{pmatrix} 0230 \\ 2300 \\ 3000 \\ 0003 \end{pmatrix},$$

we have $rank(T_{58,4}) = 4$. Hence, we have constructed an optimal LCD $[58,4,45]$ code.

Summarizing the previous discussion, the following theorem holds.

Theorem **2.2** If $4 \le n \le 156$, there exists an optimal LCD $[n,4,d]$ code.

3. Discussion and Conclusion

In this paper, we have studied the construction of LCD codes over F_5 from known linear codes by special transformations. Many $[n,3]$ and $[n,4]$ optimal LCD codes have been obtained from the Database of Magma and constructed via transformation technique. By the technique in this paper, one can construct many LCD codes with good parameters for some applications.

From [17-21], we know that existence of many optimal linear codes over F_5 are determined. Yet, it is not known whether these codes are LCD codes. Our future work concerns the constructions of LCD codes with larger lengths and higher dimensions. Hence, much work is needed in the future. The reader is thus cordially invited to uncover the world of LCD codes over F_5.

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. W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, (Cambridge University Press, Cambridge, 2003).
2. J. L. Massey, Inform. Cont., 7, 369-380(1964).
3. J. L. Massey, Discrete Math., 106/107, 337-342(1992).
4. C. Carlet, S. Guilley, *Coding Theory and Applications, CIM Series in Mathematical Sciences*(Springer Verlag, 3, 97-105, 2014). See also : Adv. Math. Commun., 10, 131-150(2016).
5. J. Qian, L. Zhang, Design code. cryptogr.,77,193-202(2015).
6. L. Lu, R. Li, L. Guo, Q. Fu, Quantum Inf. Process, 14, 165–182 (2015).
7. K. Guenda, S. Jitman, T. A. Gulliver, Design code. cryptogr., (1-16) 2016. see also : arXiv: 1606.00134v1.
8. L. Lu, R. Li, L. Guo, Int.J. Quantum Inf., 14, 1750017 (2017) .
9. X. Hou, and F. Oggier, *IEEE International Symposium on Information Theory*, (1501-1505) 2016.
10. E. R. Lina, Jr. ,E. G. Nocon, *the DLSU Research Congress*, 4(2016).
11. K. Boonniyoma, S. Jitman, https: //arxiv. org/pdf/1605.06827.pdf.
12. S. Zhu, B. Pang,Z. Sun, arXiv:1610.08206v1 [cs. IT] 26 Oct 2016.
13. L. Jin, IEEE T. Inform. Theory, Doi 10.1109/TIT. 2016. 2644660, 2016.
14. B. Chen, H. Liu, arxiv.org/abs/1705.00770v1.
15. C. Carlet, S. Mesnager, C. Tang, Y. Qi, arXiv:1703.04346v2.
16. http://magma.maths.usyd.edu.au/magma/download/db/
17. M. Grassl, http: //www. codetables.de.
18. W. Bosma, J. Cannon, *Handbook of Magma functions*, (Sydney,1995).

19. Iliya Boukliev, Stoyan Kapralov, Tatsuya Maruta, Masaharu Fukui, IEEE T. Inform. Theory, 43,308-313(1997).
20. Tatsuya Maruta, Maori Shinohara, Ayako Kikui, Discrete Math., 309, 1255-1272 (2009).
21. Yuuki Kageyama, Tatsuya Maruta, *Seventh International Workshop on Optimal Codes and Related Topics*(Albena, Bulgaria, 2013).