Construction of Optimal Codes in Two Element Field

Dong Yuhao1, Zhao Xuejun1*, Yuan Xiujiu1, Li Jialin1, Li Jiang1, Sun Haoxiang1
1Graduate School of Air Force Engineering University, Xi’an, Shanxi, 710038

Abstract. Some definitions, theorems and lemmas related to optimal codes on binary field have been proposed in this paper. Optimal codes with different dimensions have been gotten by directly constructing, combinating and deleting. Relevant proofs have also been given. We work on how to gain optimal codes when $2 \leq k \leq 5$. Generator matrices of these optimal codes can be constructed, and codes that reaches the Griesmer bound can be furthermore determined. Method adopted in this paper is based on check matrices and designed to construct optimal codes which have low dimensions, it provides a theoretical basis for codes with higher dimensions.

1. Introduction

Since 1950s, computer technology and digital communication technology have made great progress. This development has a profound impact on human work and life style. Many subjects such as discrete mathematics, graph theory, number theory, algebra and algebraic geometry have been applied in digital communication and computer science. Due to the actual needs of communication reliability, the classical error correcting code theory came into being. There are many different types of codes in different application scenes. The optimal code and related theories have also been greatly developed. This development is not only widely discussed and studied, but also promotes the production of new mathematical ideas and the application of the coding theory.

Since the Griesmer boundary was proposed by Griesmer J H in 1960, the optimal code has been widely and deeply discussed to the Griesmer boundary. The construction of the generation matrix of the low dimensional optimal code in the two yuan domain has been basically solved, and the optimal code with large distance can also be realized by programming. Starting from the parity check matrix of linear codes, we explore the matrix method for constructing optimal codes over two variables and discuss the construction process when $k = 2, 3, 4, 5$.

2. Basic knowledge

This section will introduce several bounds on linear codes. These bounds give the mutual restriction between three parameters of linear codes.

Theorem 2.1 [1] (Ham min g boundary) If there is an error correcting code $(n, K, d)$, then

$$q^n \geq K \sum_{j=0}^{k-1} (q - 1) \binom{n}{k},$$

where $q = 2$.
where $\binom{n}{k}$ is a combination, $K$ is the number of codewords of a linear code, dimension $k = \log K$. The codes which reach the Hammin g boundary are called Hamming codes.

**Theorem 2.2** (Griesmer bound)

If $C$ is a linear code with positions of $[n,k,d]$ in $q$ element field, and it meets the requirement of $n \geq g = \sum_{i=0}^{k-1} \left\lfloor \frac{d}{q^i} \right\rfloor$, it is called $k$-dimensional optimal code, where $g$ is Griesmer boundary.

3. Construction of optimal codes

The code table of 4-dimentional optimal codes is listed in appendix 1.

According to the construction of low-dimentional optimal codes ($k = 2, 3$), we can conclude that the identity matric $I_k$ and the generation matrix of Simplex code should be find firstly. Then $G_{k,l}$ ($l \leq 2n$) will be constructed by expansion and deletion. In the end, we can make a predictation of the cods when $2n \geq k$.

When $k = 4$, the matric is constructed as

$$I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad S_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$  

The method used is same as that of the previous one. Special column vectors in $S_4$ are graded as

$$X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8, X_9, X_{10}, X_{11} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$  

The principle of the extension method is to find a column vector in the above matrix and gradually expand the column. The extension is based on the code distance of the new code (the new code reaches the Griesmer boundary) or the constant (the new code has not reached the Griesmer boundary). When constructing the optimal code with the dimention $k = 2, 3$, the column vector needed to extend in the generating matrix can be seen directly. But as the dimensions increase, this work is becoming more and more complex (of course, if the process is not difficult to achieve), so I have a new approach to the basis of the extension based on my own knowledge.

In order to get a new generation matrix $G'$ from the original generation matrix $G$, we should take the change of the code distance as an extended constraint. In order to reduce the complexity, I use the check matrices $H$ and $H'$ here.

The generation matrix before the extension is recorded as $G = [I_4 : P]$, thus the check matrix $H = [P^T : I_{n-4}]$. According the properties of generating matrices and check matrices, code length $d$ of $G$ depends on the minimum correlation group of column vectors in $H$, it depends on the minimum correlation group of column vectors in $P^T$ when $d \leq k + 1$. In order to better reflect the function of the check matrix, I divide the column by column into two categories according to the result,
optimal codes which reach Griesmer boundary and optimal codes which don’t reach Griesmer boundary.

(1) When generator matrices obtained generate an optimal code reaching Griesmer boundary, code lengths will be up to $n^* = n + c$ after expanding, and code distances will be $d^* = d + c(c = 1, 2, \ldots)$. The basis for the column extension at this time is adding $c$ line vectors for $H$ so as to exchange it into $H^*$, in this time, $d + c$ column vectors are included in the minimum correlating group.

**Example 3.1** $[7, 4, 3]_2 \rightarrow [8, 4, 4]_2$. The generator matrix of $[7, 4, 3]_2$ code can be obtained by the check matrix of $[7, 3, 4]_2$ code.

$$G_{4,7} = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}.$$  

The check matrix corresponding is

$$H_{4,7} = \begin{bmatrix}
1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1
\end{bmatrix}.$$  

We can see that

$$P^T = \begin{bmatrix}
1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1
\end{bmatrix}.$$  

There is only one minimum correlating group, it is

$$\begin{bmatrix}
1 \\
1 \\
0
\end{bmatrix}, \begin{bmatrix}
1 \\
0 \\
1
\end{bmatrix}, \begin{bmatrix}
0 \\
1 \\
1
\end{bmatrix}.$$  

Some elements will be added at the end of the three column vectors. They should be linearly independent. Thus, these elements added can only be “1”. These three vectors after being operated will be

$$\begin{bmatrix}
1 \\
1 \\
1
\end{bmatrix}, \begin{bmatrix}
1 \\
0 \\
1
\end{bmatrix}, \begin{bmatrix}
0 \\
1 \\
1
\end{bmatrix}.$$  

Both of “0” or “1” are acceptable in the end of the last vector. Assuming it as “0”, can be chosen as the expanding column vector according to $(X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8, X_9, X_{10}, X_{11})$. So we can conclude that

$$G_{4,8} = [G_{4,7} : X_7] = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1
\end{bmatrix}.$$
\( G_{4,8} \) will generate the \([8,4,4]_2\) code.

(2) When generator matrices obtained generate a optimal code reaching Griesmer boundary, code lengths will be up to \( n^* = n + c \) after expanding, and code distances will be \( d^* = d + c(e = 1, 2, \ldots) \). The basis for the column extension at this time is adding \( c \) line vectors for \( H \) so as to exchange it into \( H^* \), and the minimum correlation of the minimum correlating group will not be changed.

**Example 3.2** \([5,4,2]_2 \to [6,4,2]_2\). The generator of \([5,4,2]_2\) code is

\[
G_{4,5} = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1
\end{bmatrix},
\]

The check matrix corresponding is

\[
H_{4,5} = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix},
\]

We can see that

\[
P^T = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix},
\]

A minimum correlating group is

\((1), (1)\).

Considering the method in (2), \( \chi_1 \) can be chosen to be added into \( G_{4,5} \) according to \((\chi_1, \chi_2, \chi_3, \chi_4, \chi_5, \chi_6, \chi_7, \chi_8, \chi_9, \chi_{10}, \chi_{11})\) as

\[
G_{4,6} = \begin{bmatrix} G_{4,5} : \chi_1 \end{bmatrix} = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0
\end{bmatrix}.
\]

\( G_{4,6} \) will generates the \([6,4,2]_2\) code.

As can be seen from the two examples above, the core of this method is to add a row vector to its generator matrix according to the minimum correlation group of the column vectors in the checksum matrix (mainly \( P^T \)). In (1) all minimum correlation groups need to be extracted, while in (2) we only need to consider one of the smallest correlation groups. Compared with the process of calculating code distance in programming, this method greatly reduces the computational complexity. It is important to note that when \( d < 5 \), we can only study on \( P^T \), and the check matric \( H \) should be considered as a whole when \( d > 5 \) so that we can obtain the column vector \( \chi_i (1 \leq i \leq 11) \).

We can easily construct generator matrices of optimal codes when \( k = 4, 5 \leq n \leq 15 \) as

\[
G_{4,5} = \begin{bmatrix} G_{4,4} : \chi_{11} \end{bmatrix}, \ G_{4,6} = \begin{bmatrix} G_{4,5} : \chi_1 \end{bmatrix}; \\
G_{4,7} = \begin{bmatrix} I_4 : \chi_9, \chi_9, \chi_{10} \end{bmatrix}, \ G_{4,8} = \begin{bmatrix} G_{4,7} : \chi_7 \end{bmatrix}; \\
G_{4,9} = \begin{bmatrix} G_{4,8} : \chi_1 \end{bmatrix}, \ G_{4,10} = \begin{bmatrix} G_{4,9} : \chi_2 \end{bmatrix}, \ G_{4,11} = \begin{bmatrix} G_{4,10} : \chi_5 \end{bmatrix}; \\
G_{4,12} = \begin{bmatrix} G_{4,11} : \chi_5 \end{bmatrix}, \ G_{4,13} = \begin{bmatrix} G_{4,12} : \chi_4 \end{bmatrix}, \ G_{4,14} = \begin{bmatrix} G_{4,13} : \chi_6 \end{bmatrix}, \ G_{4,15} = S_4.
\]
4. Conclusion
In this paper, the relevant definitions and theorems of linear codes are integrated, and the construction process of low dimensional optimal codes on two element domains is discussed. A new method of matrix construction is proposed from the check matrix of linear codes. We have solved the construction problem of the generation matrix of the optimal code when \( k = 2, 3, 4, 5 \), and obtained a series of generating matrices of the optimal codes, which opened up a new idea for the construction of the optimal code on the two element domain. Next, we will further analyze and study optimal codes and MacDonald codes when \( k \geq 6 \), and discuss the feasibility of other methods.

Appendices

| d | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| g | 4 | 5 | 7 | 8 | 11| 12| 14| 15|
| n | 4 | 5,6| 7 | 8,9,10| 11| 12,13| 14| 15,16,17,18|
| d | 9 | 10| 11| 12| 13| 14| 15| 16|
| g | 19 | 20| 22| 23| 26| 27| 29| 30|
| n | 19 | 20,21| 22| 23,24,25| 26| 27,28| 29| 30|

References
[1] Griesmer J H. A bound for error-correcting codes[M]. IBM Corp. 1960.
[2] André Neubauer, Jürgen Freudenberger, Volker Kühn, etc. Coding Theory [M]. Posts & Telecom Press, 2009.
[3] SanLing, ChaopingXing. Coding theory [M]. Cambridge University Press, 2004. Appendix 1
[4] Shannon C E. A mathematical theory of communication[J]. Bell System Technical Journal, 1997, 14(4):306.
[5] Hamming R W. Error detecting and error correcting codes[J]. Bell System Technical Journal, 1950, 29(2):147-160.