Scientific Research Publishing

Communications and Network, 2022, 14, 23-35
https://www.scirp.org/journal/cn
ISSN Online: 1947-3826
ISSN Print: 1949-2421

On the Construction of the Kernel Matrix by Primitive BCH Codes for Polar Codes

Liping Lin

College of Cyber Security, Jinan University, Guangzhou, China
Email: 505416760@qq.com

How to cite this paper: Lin, L.P. (2022) On the Construction of the Kernel Matrix by Primitive BCH Codes for Polar Codes. *Communications and Network*, **14**, 23-35.
https://doi.org/10.4236/cn.2022.141003

Received: December 10, 2021
Accepted: January 18, 2022
Published: January 21, 2022

Abstract

The polar codes defined by the kernel matrix are a class of codes with low coding-decoding complexity and can achieve the Shannon limit. In this paper, a novel method to construct the 2^n-dimensional kernel matrix is proposed, that is based on primitive BCH codes that make use of the interception, the direct sum and adding a row and a column. For ensuring polarization of the kernel matrix, a solution is also put forward when the partial distances of the constructed kernel matrix exceed their upper bound. And the lower bound of exponent of the 2^n-dimensional kernel matrix is obtained. The lower bound of exponent of our constructed kernel matrix is tighter than Gilbert-Varshamov (G-V) type, and the scaling exponent is better in the case of 16-dimensional.

Keywords

Polar Code, Kernel Matrix, Matrix Interception, Partial Distance, Exponent, Scaling Exponent

1. Introduction

Polar codes can achieve the Shannon limit for binary-input discrete memoryless channels (BI-DMC) in theory and with low encoding and decoding complexity [1]. Polar codes employ the n-th Kronecker power of the matrix $G_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ to encode 2^n channels, where G_2 is called the polarizing matrix or kernel matrix. As the number of channels grows, sub-channel becomes either a noiseless channel or a pure-noise channel, the proportion of the noiseless channels is close to the original channel capacity, and the noiseless channels transmit the information bits without error.

The kernel matrix is an important part of polar codes, which determines the polarization property of polar codes. The kernel matrix G_2 is also called 2-dimensional kernel matrix, there are other kernel matrices, and different kernel matrices will have different polarization effects. In order to improve the polarization of the polarization code, many researchers have done a lot of research on the kernel matrix.

There are two extended research directions for the construction of the kernel matrix, one is to expand the field of the kernel matrix, the other is to increase the dimension of the kernel matrix. Generally speaking, the larger the field or the higher the dimension of the kernel matrix, the better the polarization effect of the polar codes. Şaşoğlu *et al.* [2] [3] [4] generalized the polar code to any discrete memoryless channel and q-ary field, which expanded the field of the kernel matrix. Korada [5] proposed to construct a $\left(2^n-1\right)$-dimensional kernel matrix with BCH codes, which increased the dimension of kernel matrix. E. Moskovskaya *et al.* [6], based on [5] [7], put forward a method to construct a 2^n-dimensional kernel matrix with extended BCH codes, which further increased the dimension of kernel matrix. E. Moskovskaya *et al.* stacked the matrix blocks to construct a $2^n\times\left(2^n-1\right)$ matrix, and then added a column of parity bits to construct a 2^n-dimensional kernel matrix. Although the 2^n-dimensional kernel matrix had a higher dimension and exponent, it did not consider the problem of partial distance's upper bound.

Therefore, based on [5] [6], we take advantage of the primitive BCH codes to design a higher-dimensional kernel matrix which meets the upper bound of partial distance. Compared with the work in [5], the proposed construction enjoys two advantages, one is that the kernel matrix has a higher dimension, and the other is that the obtained kernel matrix is naturally lower triangular, guaranteeing the polarization property of kernel matrix. And compared with the work in [6], a solution is given to adjust these rows whose partial distances are beyond their upper bounds. The comparison result shows that the proposed 2^n-dimensional kernel matrix has a tighter lower bound of the exponent than the Gilbert-Varshamov (G-V) type construction in [5], the scaling exponent is not very different from [6], and 16-dimensional kernel matrix is even slightly better than [6].

2. Preliminaries

This section reviews the knowledge of primitive BCH codes and background of polar codes, including the polarization condition, the scaling exponent, the partial distance, and the exponent.

2.1. Primitive BCH Codes

Definition 1 (Primitive BCH Codes [8]). Let α be the primitive element, and $g(x)$ be the lowest degree polynomial with $\alpha,\alpha^2,\cdots,\alpha^{2t}$ as the roots in finite field $GF(2)$. The code generated by $g(x)$ is called a primitive BCH code, denoted as $BCH(N,k,t)$. It has a code length $N=2^n-1$, encodes k symbols and corrects at most t errors.

For example, if α is the primitive element of polynomial $g(x)=x^4+x+1$, the finite field $GF\left(2^4\right)$ can be generated by $g\left(x\right)$, the minimum polynomial of all elements can be obtained as follows:

$$\alpha,\alpha^2,\alpha^4,\alpha^8 --- x^4+x+1=\phi_1\left(x\right). \tag{1}$$

$$\alpha^3,\alpha^6,\alpha^9,\alpha^{12} --- x^4+x^3+x^2+x+1=\phi_3\left(x\right). \tag{2}$$

$$\alpha^5,\alpha^{10} --- x^2+x+1=\phi_5\left(x\right). \tag{3}$$

$$\alpha^7,\alpha^{11},\alpha^{13},\alpha^{14} --- x^4+x^3+1. \tag{4}$$

If $t=1$ and $n=15$, then the generator polynomial of $BCH\left(15,11,1\right)$ is

$$g\left(x\right)=\phi_1\left(x\right)=x^4+x+1. \tag{5}$$

If $t=2$ and $n=15$, then the generator polynomial of $BCH\left(15,7,2\right)$ is

$$\begin{aligned} g\left(x\right) &= LCM\left(\phi_1\left(x\right),\phi_3\left(x\right)\right) \\ &= \left(x^4+x+1\right)\left(x^4+x^3+x^2+x+1\right) \\ &= x^8+x^7+x^6+x^4+1. \end{aligned} \tag{6}$$

where $LCM\left(\cdot\right)$ denotes the Least Common Multiple of its inputs.

If $t=3$ and $n=15$, then the generator polynomial of $BCH\left(15,5,3\right)$ is

$$g\left(x\right)=LCM\left(\phi_1\left(x\right),\phi_3\left(x\right),\phi_5\left(x\right)\right)=x^{10}+x^8+x^5+x^4+x^2+x+1. \tag{7}$$

Lemma 1 (Minimum Distance [8]). For any positive integer $n,t\left(n\geq 3,t\leq 2^{n-1}\right)$, if there is a cyclic code of length 2^n-1, the number of parity bits is $N-k\leq nt$, and the minimum distance $d_{\min}\geq 2t+1$.

2.2. The Performance and Property of Polar Code

Polar code can produce polarization phenomena, which can polarize channel into pure noise channel or noise-free channel. These matrices that can produce polarization phenomena are polarization matrices, and the kernel matrix actually is a polarization matrix. Given a $l\times l$ matrix G_l, the necessary and sufficient condition for judging whether it is a polarization matrix is that the matrix is non-singular, and the upper triangular matrix is not formed after any column transformation [3]. Therefore, kernel matrix G_l is non-singular, and G_l also can be called *l*-dimensional kernel matrix.

The polar code polarizes the sub-channels capacity $I\left(W\right)$ to 0 or 1, but there are some sub-channels whose channel capacity is between 0 and 1, these sub-channels are called unpolarized channels. The speed of unpolarized channel's channel capacity tends to 1 is called the polarization speed. Fazeli *et al.* [9] [10] applied the scaling exponent to measure the polarization speed of polar code. The scaling exponent was proposed on the basis of the scaling assumption. The definition of the scaling assumption is as follows:

Definition 2 (scaling assumption [11]). Given a kernel matrix G_l and binary discrete memoryless channel *W*, there exists

$$\lim_{n\to\infty}\frac{\text{number of unpolarized channels}}{\text{number of total channels}}N^{\frac{1}{\mu}}\in\left(0,+\infty\right). \tag{8}$$

where μ denotes the scaling exponent, and $N = 2^l \left(l \geq 2 \right)$ denotes the length of polar code.

The optimal value of scaling exponent is 2, the closer the scaling exponent of kernel matrix is to 2, the better the polarization effect. Most of the scaling exponents of kernel matrices are between 3 and 5, but Yao *et al.* [12] proved that when the dimension of kernel matrix is 64, the scaling exponent can be less than 2.9603. The scaling exponent can be calculated by

$$N^{1/\mu} \left(C - R \right) = \beta , \tag{9}$$

where $\beta = \left(1 + 2P_e^{-0.01} \right)^3$, p_e, R and C denote block error rate, ratio and channel capacity [9], respectively.

The exponent is also an index to measure the speed of polarization. The value of the exponent is between 0 and 1. The larger the exponent, the better the polarization of polar code. The exponent is determined by the partial distance sequence, which is defined as follows:

Definition 3 (partial distance [5]). For the kernel matrix $G_l = \left[g_1^{\mathrm{T}}, g_2^{\mathrm{T}}, \cdots, g_l^{\mathrm{T}} \right]^{\mathrm{T}}$, its *i*-th partial distance D_i is

$$D_i = d_H \left(g_i, \left\langle g_{i+1}, \cdots, g_l \right\rangle \right), i = 1, 2, \cdots, l - 1 , \tag{10}$$

$$D_l = d_H \left(g_l, \mathbf{0} \right) . \tag{11}$$

where $g_i \left(i = 1, 2, \cdots, l \right)$ denotes the row vector of length *l*, $d_H \left(a, b \right)$ denotes the Hamming distance of the vector *a* and *b*, $d_H \left(a, C \right) = \min_{c \in C} d_H \left(a, c \right)$, $\left\langle g_1, \cdots, g_k \right\rangle$ denotes the linear space generated by $g_1, \cdots, g_k$, 0 denotes the zero vector of length *l*.

According to the partial distance sequence, the definition of the exponent is as follows:

Definition 4 (exponent [5]). The exponent of kernel matrix G_l is defined as

$$E \left(G_l \right) = \frac{1}{l} \sum_{i=1}^{l} \log_l^{D_i} . \tag{12}$$

In this paper, all operations on matrix elements are XOR on $GF \left(2 \right)$, *i.e.*, $1 + 0 = 1 \bmod \left(2 \right) = 1$, $1 + 1 = 2 \bmod \left(2 \right) = 0$.

The size of the square matrix in this paper is described by the concept of order and dimension. For example, a 3*3 matrix can be expressed as a 3-dimensional matrix or a 3-order matrix in this paper. The 3-dimensional matrix indicates that the matrix is non-singular, and the 3-order matrix only indicates the size of the matrix.

3. The Construction of 2^n-Dimensional Kernel Matrix

In this section, we employ the classification formula to construct a $\left(2^n - 1 \right)$-order matrix, adding a column vector and a row vector of all 1s before the first column and below the last row of the $\left(2^n - 1 \right)$-order matrix, and the 2^n-dimensional kernel matrix can be obtained.

3.1. The Construction of the $\left(2^n - 1 \right)$-Order Matrix

Definition 5 (Classification Formula [13]). According to the classification formula of cyclotomic coset, the integer set $\{0,1,\cdots,2^n-1\}$ is classified as

$$S=\bigcup_{i=0}^{2^n-2}\left\{2^k\cdot i\bmod\left(2^n-1\right):k\in N\right\}=\bigcup_{j=1}^{c}v(j). \tag{13}$$

where $v(i)$ denotes the elements in the *i*-th partitioned set with $i(1\le i\le c)$, and *c* denotes the number of cyclotomic cosets in *S*.

According to the Definition 5, we can obtain the following theorem 1:

Theorem 1. Let $l(i)$ denotes the number of elements in $v(i)$, and $l(1)=1$, $l(2)=l(3)=n$ can be obtained.

Proof. $v(1)=\left\{0\cdot 2^k \bmod\left(2^n-1\right),k\in N\right\}=\{0\}$, $v(2)=\left\{1\cdot 2^k \bmod\left(2^n-1\right),k\in N\right\}$, $v(3)=\left\{3\cdot 2^k \bmod\left(2^n-1\right),k\in N\right\}$ can be known from Equation (13), therefore $l(1)=1$. for $v(2)$, when $k=n$, $\left(2^n-1\right)=1=1\cdot 2^0 \bmod\left(2^n-1\right)$, therefore $v(2)=\left\{1,2,4,\cdots,2^{n-1}\right\}$ and $l(2)=n$. Similarly, $v(3)=\left\{3,6,12,\cdots,3\cdot 2^{n-1}\right\}$ and $l(3)=n$ can be obtained.□

For example, $n=4$ and $S=\{0,1,\cdots,14\}=\{\{0\},\{1,2,4,8\},\{3,6,9,12\}\}$, therefore, $c=5$, $l(1)=1$, $l(2)=l(3)=4$, $l(4)=2$, $l(5)=4$, $v(1)=\{0\}$, $v(2)=\{1,2,4,8\}$, $v(3)=\{3,6,9,12\}$, $v(4)=\{5,10\}$, $v(5)=\{7,11,13,14\}$.

According to the classification formula (13), we use *c* different sub-matrices to construct a $\left(2^n-1\right)$-order matrix by stacking the matrix blocks from top to bottom. The specific construction process is as follows:

1) The first layer sub-matrix is a zero matrix of dimension $l(1)$.

2) The second layer sub-matrix is a unit matrix with dimension $l(2)$.

3) The third layer sub-matrix is intercepting from the generator matrix of the primitive BCH code with dimension $l(3)$ and 1 error correction capability. The interception criterion is that the rows of intercepted matrix are continuous, and the intercepted matrix can form a sub-lower triangular matrix with the previous two layers.

4) If $c>3$, looking for other generating matrices of the primitive BCH codes with length $\left(2^n-1\right)$ and error correction capability $t(t=2,3,\cdots,c-2)$ in turn, then intercepting the matrix according to the $l(i)(i=4,5,\cdots,c)$ and interception criterion.

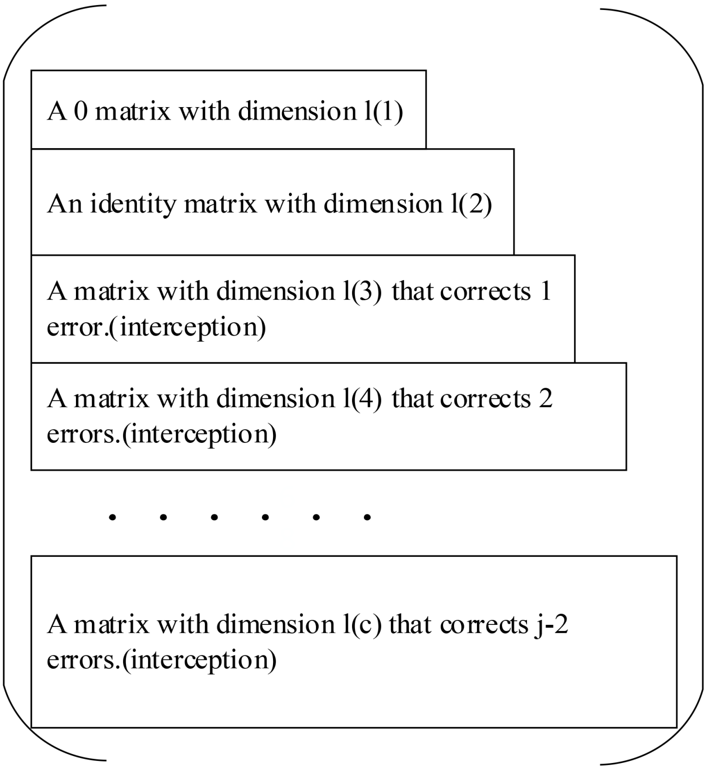
The above construction of the $\left(2^n-1\right)$-order matrix is summarized in Figure 1.

3.2. A Row and Column Addition

Through adding a column and a row vector of all 1s before the first column and below the last row of the $\left(2^n-1\right)$-order matrix, the 2^n-dimensional kernel matrix is obtained. The 2^n-dimensional kernel matrix is a lower triangular matrix, which guarantees the polarization.

For example, in order to construct the 16-dimensional matrix, the 15-order matrix should be constructed firstly. When $n=4,t=1$, the generator polynomial of the primitive BCH code is Equation(5), and $c=5$, $l(1)=1$, $l(2)=l(3)=4$, $l(4)=2$, $l(5)=4$.

15-order matrix can be constructed with 5 layers sub-matrices, and the dimension of theses sub-matrices are 1, 4, 4, 2 and 4, and the construction of the



A 0 matrix with dimension l(1)
An identity matrix with dimension l(2)
A matrix with dimension l(3) that corrects 1 error.(interception)
A matrix with dimension l(4) that corrects 2 errors.(interception)
• • • • • •
A matrix with dimension l(c) that corrects j-2 errors.(interception)

Figure 1. The construction of $\left(2^n-1\right)$-order matrix.

16-dimensional kernel matrix is as follows:

$$\begin{pmatrix} 0 &&&& \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{t=1} \begin{pmatrix} 0 &&&&&&&& \\ 1 & 0 & 0 & 0 & 0 &&&& \\ 0 & 1 & 0 & 0 & 0 &&&& \\ 0 & 0 & 1 & 0 & 0 &&&& \\ 0 & 0 & 0 & 1 & 0 &&&& \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\xrightarrow{t=2} \begin{pmatrix} 0 &&&&&&&&&& \\ 1 & 0 & 0 & 0 & 0 &&&&&& \\ 0 & 1 & 0 & 0 & 0 &&&&&& \\ 0 & 0 & 1 & 0 & 0 &&&&&& \\ 0 & 0 & 0 & 1 & 0 &&&&&& \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 && \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 && \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 && \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 && \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$$\xrightarrow{t=3}\begin{pmatrix}
0 &&&&&&&&&&&&&& \\
1 & 0 & 0 & 0 &&&&&&&&&&& \\
0 & 1 & 0 & 0 &&&&&&&&&&& \\
0 & 0 & 1 & 0 &&&&&&&&&&& \\
0 & 0 & 0 & 1 &&&&&&&&&&& \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 &&&&&&& \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 &&&&&&& \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 &&&&&&& \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 &&&&&&& \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 &&&&& \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 &&&&& \\
1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0
\end{pmatrix}$$

$$\xrightarrow{\text{a row and column addition}}\begin{pmatrix}
1 & 0 &&&&&&&&&&&&&& \\
1 & 1 & 0 & 0 & 0 &&&&&&&&&&& \\
1 & 0 & 1 & 0 & 0 &&&&&&&&&&& \\
1 & 0 & 0 & 1 & 0 &&&&&&&&&&& \\
1 & 0 & 0 & 0 & 1 &&&&&&&&&&& \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 &&&&&&& \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 &&&&&&& \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 &&&&&&& \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 &&&&&&& \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 &&&&& \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 &&&&& \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}$$

Filling 0 in the remaining blank positions, and 16-dimension kernel matrix can be obtained.

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}. \tag{14}$$

3.3. The Analysis of Construction

From Lemma 1, $(N-k)_{\min}=n$ and the lowest degree of the generator polynomial $\partial(g(x))_{\min}=n$ can be obtained. If α is the primitive of $g(x)$, then $GF(2^n)$ is the *n*-th extension of $GF(2)$ and $\forall\beta\in GF(2^n)$, $\beta=a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{n-1}\alpha^{n-1}$, ($a_0,\cdots,a_{n-1}\in F_2$) [14]. Because $GF(2^n-1)=GF(2^n)/\{0\}$, the element in $GF(2^n-1)$ also can be expressed linearly by $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$. If the above process is extended to the matrix, a similar conclusion can be obtained.

Marking $0,1,\alpha,\alpha^2,\cdots,\alpha^{2^n-1}$ above each column of the 2^n-dimensional kernel matrix, and the construction analysis of the (2^n-1)-order matrix is as follows:

1) For the first layer sub-matrix, $l(1)=1$ and the field is $GF(2)$, therefore the first sub-matrix is zero matrix.

2) For the second layer sub-matrix, $l(2)=n$ can be obtained from Theorem 2, therefore, the second sub-matrix is a unit matrix, and row vectors correspond to $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$.

3) For the *i*-th layer sub-matrix, $3\le i\le c$. Because the *i*-th sub-matrix is composed of primitive BCH code, it is connected by the generator polynomial $g(x)$, and $g(\alpha)=0$, the column indicators corresponding to non-zero elements add up to 0.

4) For the 2^n-dimensional kernel matrix. Because the 2^n-dimensional kernel matrix is a lower triangular matrix and the first column's indicator is marked as 0, the column indicators corresponding to the diagonal elements are the sum of the non-zero element before the diagonal elements

Therefore, the diagonal elements of 2^n-dimensional kernel matrix can be expressed linearly by $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$, The sub-diagonal elements of (2^n-1)-order matrix are equivalent to $GF(2^n-1)$, and the diagonal elements of 2^n-dimensional matrix are equivalent to $GF(2^n)$.

For example, the 7-th row vector in Equation (14), Since the 16-dimensional kernel matrix is a lower triangular matrix, only the elements before the diagonal are listed, it is $\begin{array}{c}\begin{array}{ccccccc}0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5\end{array}\\ \begin{pmatrix}1 & 0 & 1 & 1 & 0 & 0 & 1\end{pmatrix}\end{array}$, $g(\alpha)=\alpha^4+\alpha+1=0$, and $\alpha^4=\alpha+1$, therefore, $\alpha^5=\alpha^2+\alpha$ or $\alpha+\alpha^2+\alpha^5=0$ can be obtained.

4. The Partial Distance and Exponent

4.1. The Upper of Partial Distance

Equation (10) can infer

$$D_i=d_H\left(g_i,\langle g_{i+1},\cdots,g_l\rangle\right)=\min_{j\ge i}D_j=d_{\min}\left(\langle g_i,\cdots,g_l\rangle\right)\le d_{\max}[l,l-i+1]. \quad (15)$$

where $d_{\min}(\langle a,b\rangle)$ denotes the minimum distance for generating codeword from vector *a* and *b*, $d_{\max}[l,k],1\le k\le l$ denotes the maximum minimum Hamming distance attained by a code of length *l* and size *k* [15].

Therefore, the partial distance of kernel matrix cannot exceed its upper bound. Because [5] constructed a (2^n-1)-dimensional kernel matrix from bottom to top according to the definition of partial distance, the $\left(2^n-1\right)$-dimensional kernel matrix in [5] met the upper bound of partial distance. [6] also used a similar method to construct a matrix, but [6] obtained a $2^n\times\left(2^n-1\right)$ matrix, not a $\left(2^n-1\right)$-dimensional kernel matrix. Through adding a column of parity bits, [6] obtained a 2^n-dimensional kernel matrix, but the added column vector would affect the partial distance, and which may cause the partial distance exceeded its upper bound. When $l=32, D_{25}=14$, for example, D_{25} exceeds its upper bound 13 [15].

We take the opposite approach, through constructing $\left(2^n-1\right)$-order matrix from top to bottom, and then adds a column vector and a row vector of all 1 s before the first column and below the last row of the $\left(2^n-1\right)$-order matrix, and the 2^n-dimensional kernel matrix can be obtained. Therefore, we only need to analyze the partial distance of $\left(2^n-1\right)$-order matrix. The Definition of partial distance is proposed for the kernel matrix, but it can be applied to other square matrices, In order to analyze the partial distance of the 2^n-dimensional kernel matrix, We use the definition of partial distance to analyze the $\left(2^n-1\right)$-order matrix. because according to the Definition 3, the first column of 2^n-dimensional matrix is all 1, and it will not affect the partial distance. The 2^n-dimensional kernel matrix can meet its partial distance by appropriately adjusting the $\left(2^n-1\right)$-order matrix, the specific adjustment process is as follows:

1) If D_i exceeds its upper bound, adjusting the codeword in the *i*-th row to the $(i-1)$-th row by shifting one bit to the right.

2) If D_i still exceeds its upper bound after a right cyclic shift., both the *i*-th row and the $(i-1)$-th row are adjusted to the right cyclic shift of the $(i-2)$-th row. this cycle continues until D_i meets its upper bound.

This method can not only ensure that the $\left(2^n-1\right)$-order matrix is composed of the primitive BCH codes, but also can ensure that it is still a sub-lower triangular matrix, thereby ensuring the polarization of the 2^n-dimensional kernel matrix. The process is demonstrated in Figure 2.

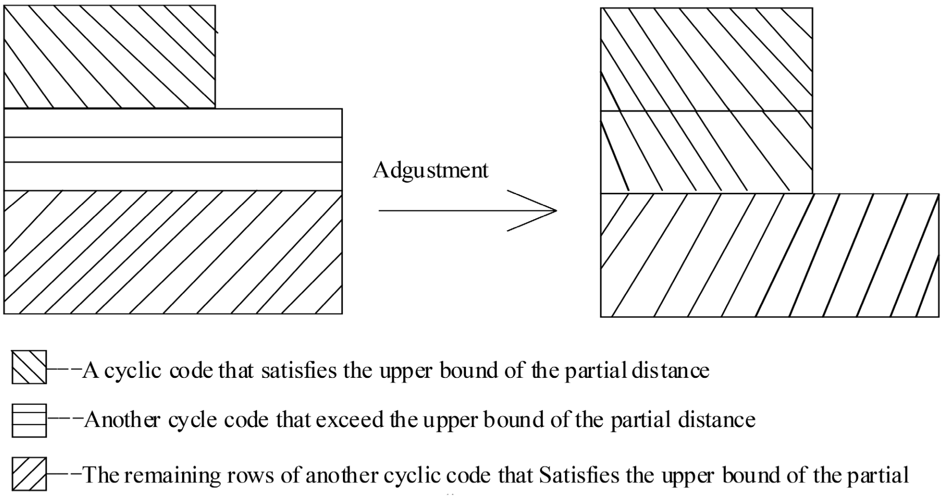

Adgustment
▧—A cyclic code that satisfies the upper bound of the partial distance
☰—Another cycle code that exceed the upper bound of the partial distance
▨—The remaining rows of another cyclic code that Satisfies the upper bound of the partial

Figure 2. Adjust the row exceeds the upper bound of the partial distance.

Through the above adjustment method, the 32-dimensional kernel matrix can be obtained as follows:

$$G_{32}=\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0& &0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&0&1&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&1&0&1&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&1&0&0&1&0&1&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&1&0&1&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&0&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&1&1&1&0&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&1&1&1&1&0&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&1&1&1&0&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&1&1&1&1&0&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&1&1&1&1&0&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&1&1&1&0&0&0&1&0&0&0&0&0&0\\
1&1&1&1&0&0&1&0&0&0&1&0&1&0&1&1&1&1&0&1&1&0&0&1&0&1&1&0&0&0&0&0\\
1&0&1&1&1&0&0&1&0&0&0&1&0&1&0&1&1&1&1&0&1&1&0&0&1&0&1&1&0&0&0&0\\
1&0&0&1&1&1&0&0&1&0&0&0&1&0&1&0&1&1&1&1&0&1&1&0&0&1&0&1&1&0&0&0\\
1&0&0&0&1&1&1&0&0&1&0&0&0&1&0&1&0&1&1&1&1&0&1&1&0&0&1&0&1&1&0&0\\
1&0&0&0&0&1&1&1&0&0&1&0&0&0&1&0&1&0&1&1&1&1&0&1&1&0&0&1&0&1&1&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix} \tag{16}$$

4.2. The Lower Bound of Exponent

Definition 6 (Direct-Sum). Let C_1 be a $[n,k_1,d_1]_q$ linear code, C_2 be a $[n,k_2,d_2]_q$ linear code, and $C_1 \cap C_2=\{0\}$, if $C_1 \oplus C_2=\{x+y \mid x\in C_1, y\in C_2\}$, then $C_1 \oplus C_2$ is called the direct-sum of C_1 and C_2.

The construction of the $\left(2^n-1\right)$-order matrix is direct-sum construction. Therefore, the relevant properties of the direct-sum construction can be used to analyze the partial distance of the 2^n-dimensional kernel matrix. The minimum distance of direct-sum has the following relationship:

Lemma 2 (Minimum distance [16]). The minimum distance of $C_1 \oplus C_2$ is *d*. where

$$d \le \min\{d_1, d_2\}.$$

Theorem 2. If the *i*-th row vector belongs to the *j*-th layer, then $D_i \ge 2j-3$.

Proof. From Lemma 2 and Definition 3, D_i is only related to the layer where it belongs with and has nothing to do with the subsequent layers. Because the *j*-th layer is capable of correcting $j-2$ errors, $D_i \ge 2(j-2)+1 = 2j-3$ can be obtained.□

Remark. The primitive BCH codes with different error correction capabilities may have the same generator polynomial. For example, when constructing a 31-order matrix, the generator polynomials of $t=5$ and $t=6$ are same, so the 6-th and 7-th layers matrix are intercepted from different rows of the same generator matrix. However, in order to construct a kernel matrix with larger exponent, the sub-matrices of each layer should be intercepted from different generator matrices, because as the number of primitive BCH code error corrections increases, the minimum distance of these sub-matrices increases, the partial distance of the 2^n-dimensional kernel matrix will increases, therefore the exponent will also increases.

The partial distance lower bound sequence of 2^n-dimensional kernel matrix can be obtained from Theorem 2, the partial distance lower bound sequence is

$$\{D_i\}_{i=1,2,\cdots,2^n} = \left\{1, \underbrace{2,\cdots,2}_{n}, \underbrace{3,\cdots,3}_{l(3)}, \underbrace{5,\cdots,5}_{l(4)}, \cdots, \underbrace{2c-3,\cdots,2c-3}_{l(c)}, 2^n\right\}. \tag{17}$$

Therefore,

$$\begin{aligned} E(G) &= \frac{1}{2^n}\sum_{i=1}^{2^n}\log_{2^n}^{(D_i)} \\ &\ge \frac{1}{2^n}\left[0+1+l(3)\log_{2^n}^{3}+l(4)\log_{2^n}^{5}+\cdots+l(c)\log_{2^n}^{2c-3}+1\right] \\ &= \frac{1}{2^n}\left[2+\frac{1}{n}\cdot\sum_{i=3}^{c} l(i)\log_2^{(2i-3)}\right]. \end{aligned}$$

Namely

$$E(G) \ge \frac{1}{2^n}\left[2+\frac{1}{n}\cdot\sum_{i=3}^{c} l(i)\log_2^{(2i-3)}\right]. \tag{18}$$

5. Comparative Analysis

Table 1 compares the scaling exponent of we proposed and [6], and the scaling index can be obtained according to Equation (9). Table 1 shows that the scaling exponent of the 32-dimensional kernel matrix is higher than that of [6], this is because we adjust these rows exceeding the upper bound of partial distance which has impact on the scaling exponent. The scaling exponent of 16-dimensional kernel matrix is slightly lower than [6]. Therefore, the 16-dimensional kernel matrix constructed by this paper is slightly better than [6] in terms of polarization speed.

Table 1. The sacling exponent of kernel matrix

dimension	8	16	32
The proposed	3.577	3.365	3.417
Method used in [6]	3.577	3.396	3.122

Table 2. The lower bound of kernel matrix's exponent.

dimension	8	16	32	64
The proposed	0.4481	0.4721	0.4795	0.5265
G-V construction [5]	0.3577	0.3888	0.4311	0.4792

Table 2 compares the lower bounds of the exponent of the proposed and G-V construction. G-V construction takes advantage of $\tilde{D}_i = \max\left\{ D : \sum_{j=0}^{D-1} \binom{l}{j} < 2^i \right\}$ to obtain the lower bound sequence of the partial distance, and the lower bound of the exponent can be obtained by definition 4. Due to the difficulty of calculation, Table 2 only gives the lower bounds of the exponent of 8, 16, 32, and 64-dimensional kernel matrices. Table 2 shows that the lower bound of the exponent of the kernel matrix is higher than that of the G-V construction in these examples.

6. Conclusions

We use the primitive BCH codes to construct a 2^n-dimensional kernel matrix. Firstly, the generator matrix of primitive BCH codes with different error correction capabilities is intercepted to construct a $\left(2^n - 1\right)$-order matrix, these submatrices are stacked from top to bottom, and then adding a column and row vector of all 1 s to form a 2^n-dimensional kernel matrix. Aiming at the problem of partial distance, a solution is proposed to solve the problem of partial distance exceeding the upper bound, through right cyclic shifting, it becomes the right cyclic shift vector of the previous row, which makes the sub-matrix still a lower triangular cyclic structure, ensuring the polarization of 2^n-dimensional kernel matrix, and the lower bound of 2^n-dimensional kernel matrix's exponent is obtained.

The comparison result shows that the lower bound of 2^n-dimensional kernel matrix constructed in this paper is tighter than G-V construction, and the scaling exponent is better than [6] in 16-dimensional kernel matrix.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Arikan, E. (2009) Channel Polarization: A Method for Constructing Capacity-Achie-

ving Codes for Symmetric Binary-Input Memoryless Channels. *IEEE Transactions on Information Theory*, **55**, 3051-3073. https://doi.org/10.1109/TIT.2009.2021379

[2] Şaşoğlu, E. (2011) Polar Coding Theorems for Discrete Systems. École Polytechnique Fédérale de Lausanne, Lausanne.

[3] Şaşoğlu, E., Telatar, E. and Arikan, E. (2009) Polarization for Arbitrary Discrete Memoryless Channels. *Proceedings of* 2009 *IEEE Information Theory Workshop*, Taormina, 11-16 October 2009, 144-148. https://doi.org/10.1109/ITW.2009.5351487

[4] Mori, R. and Tanaka, T. (2010) Channel Polarization on q-ary Discrete Memoryless Channels by Arbitrary Kernels. *Proceedings of* 2010 *IEEE International Symposium on Information Theory*, Austin, 13-18 June 2010, 894-898. https://doi.org/10.1109/ISIT.2010.5513568

[5] Korada, S.B., Şaşoğlu, E. and Urbanke, R. (2010) Polar Codes: Characterization of Exponent, Bounds, and Constructions. *IEEE Transactions on Information Theory*, **56**, 6253-6264. https://doi.org/10.1109/TIT.2010.2080990

[6] Moskovskaya, E. and Trifonov, P. (2020) Design of BCH Polarization Kernels with Reduced Processing Complexity. *IEEE Communications Letters*, **24**, 1383-1386. https://doi.org/10.1109/LCOMM.2020.2984382

[7] Miloslavskaya, V. and Trifonov, P. (2012) Design of Binary Polar Codes with Arbitrary Kernel. *Proceedings of* 2012 *IEEE Information Theory Workshop*, Lausanne, 3-7 September 2012, 119-123. https://doi.org/10.1109/ITW.2012.6404639

[8] Shen, L.F. and Ye, Z.H. (2004) Information Theory and Coding. Science Press, Beijing.

[9] Fazeli, A., Hassani, H., Mondelli, M. and Vardy, A. (2020) Binary Linear Codes with Optimal Scaling: Polar Codes with Large Kernels. *IEEE Transactions on Information Theory*, **67**, 5693-5710. https://doi.org/10.1109/TIT.2020.3038806

[10] Hassani, S.H., Alishahi, K. and Urbanke, R.L. (2014) Finite-Length Scaling for Polar Codes. *IEEE Transactions on Information Theory*, **60**, 5875-5898. https://doi.org/10.1109/TIT.2014.2341919

[11] Fazeli, A. and Vardy, A. (2014) On the Scaling Exponent of Binary Polarization Kernels. *Proceedings of* 2014 52*nd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, 30 September-3 October 2014, 797-804. https://doi.org/10.1109/ALLERTON.2014.7028536

[12] Yao, H., Fazeli, A. and Vardy, A. (2019) Explicit Polar Codes with Small Scaling Exponent. *Proceedings of* 2019 *IEEE International Symposium on Information Theory* (*ISIT*), Paris, 7-12 July 2019, 1757-1761. https://doi.org/10.1109/ISIT.2019.8849741

[13] Huffman, W.C. (2003) Fundamentals of Error correcting Codes. Cambridge University Press, New York. https://doi.org/10.1017/CBO9780511807077

[14] Feng, K.Q. (2005) The Algebraic Theory of Error Correcting Codes. Tsinghua University Press, Beijing.

[15] Lin, H.P., Lin, S. and Abdel-Ghaffar, K.A.S. (2015) Linear and Nonlinear Binary Kernels of Polar Codes of Small Dimensions with Maximum Exponents. *IEEE Transactions on Information Theory*, **61**, 5253-5270. https://doi.org/10.1109/TIT.2015.2469298

[16] Xu, Y.C. and Ma, S.Y. (2013) Algebraic Coding and Cryptography. Higher Education Press, Beijing.