Scientific Research Publishing

Applied Mathematics, 2023, 14, 684-695
https://www.scirp.org/journal/am
ISSN Online: 2152-7393
ISSN Print: 2152-7385

Construction and Weight Distributions of Binary Linear Codes Based on Deep Holes

Yong Yang, Wenwei Qiu

School of Mathematics and Information, China West Normal University, Nanchong, China
Email: yangyong111752@163.com

How to cite this paper: Yang, Y. and Qiu, W.W. (2023) Construction and Weight Distributions of Binary Linear Codes Based on Deep Holes. *Applied Mathematics*, **14**, 684-695.
https://doi.org/10.4236/am.2023.1410040

Received: September 7, 2023
Accepted: October 9, 2023
Published: October 12, 2023

Abstract

Deep holes are very important in the decoding of generalized RS codes, and deep holes of RS codes have been widely studied, but there are few works on constructing general linear codes based on deep holes. Therefore, we consider constructing binary linear codes by combining deep holes with binary BCH codes. In this article, we consider the 2-error-correcting binary primitive BCH codes and the extended codes to construct new binary linear codes by combining them with deep holes, respectively. Furthermore, three classes of binary linear codes are constructed, and then we determine the parameters and the weight distributions of these new binary linear codes.

Keywords

Linear Codes, MacWilliams Equations, Weight Distribution, Dual Codes, Deep Holes, Covering Radius

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements, where q is an odd prime. An $[n,k,d]$ linear code $\mathcal{C}$ is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$ with minimum distance d, where $1 \le k \le n$. The weight of code x is denoted by $wt(x)$. The dual code of $\mathcal{C}$, denoted by $\mathcal{C}^{\perp}$, is defined by

$$\mathcal{C}^{\perp} = \left\{ x \in \mathbb{F}_q^n \mid xc = 0, \text{ for all } c \in \mathcal{C} \right\}.$$

Clearly, $\dim(\mathcal{C}) + \dim(\mathcal{C}^{\perp}) = n$.

For the linear code $\mathcal{C}$ with length n, the number of codewords of weight i denotes $A_i(\mathcal{C})$ with $0 \le i \le n$. The *weight enumerator* of $\mathcal{C}$ is defined by

$$1 + l_1 z + l_2 z^2 + l_3 z^3 + \cdots + l_n z^n,$$

and the sequence $(1, l_1, l_2, \cdots, l_n)$ is said to be the weight distribution of $\mathcal{C}$. If the number of non-zeros in the sequence is t, then we say that the linear code is a t-weight code. The weight distributions of linear codes not only give the important information of linear codes in practice and theory, but also reflect the error-correcting ability of linear codes and the probability of error information occurring during transmission. In general, it is not effortless to determine the weight distributions of linear codes.

The coset of $\mathcal{C}$, denoted by Q, is defined by

$$Q=\{x+c \mid c\in\mathcal{C}\}\subset\mathbb{F}_q^n,$$

where $x\in Q$ is a vector fixed for the given representation. The *weight of Q* is the smallest Hamming weight of the codewords of Q.

For any vector (codeword) $u\in\mathbb{F}_q^n$, the error distance to code $\mathcal{C}$ of a received codeword u is defined by

$$d(u,\mathcal{C})=\min\{d(u,c) \mid c\in\mathcal{C}\},$$

where the minimum Hamming distance between vectors u and c is defined to be

$$d(u,c)=\left|\{i \mid u_i\neq c_i, 1\leq i\leq n\}\right|.$$

The maximum error distance is defined by

$$\rho(\mathcal{C})=\max\{d(u,\mathcal{C}) \mid u\in\mathbb{F}_q^n\},$$

where ρ is called the covering radius of the linear code $\mathcal{C}$. If the error distance to code $\mathcal{C}$ of a received word $u\in\mathbb{F}_q^n$ reaches the covering radius of linear code $\mathcal{C}$, the vector u is called the deep hole.

Deep holes have been widely studied in RS codes, and the deep holes of standard RS codes are given in [1]. In addition, Zhang *et al.* also gave deep holes for several classes of special codes in [2] [3] [4]. Therefore, most scholars are keen on studying the deep holes of some special codes. However, there is little work on constructing general linear codes from deep holes. Thus, we further consider the use of deep holes to construct some binary linear codes.

Around the 1960s, BCH codes were proposed by Hocquenghem [5] and Bose and Ray-Chaudhuri [6], and the error-correcting codes were studied by Gorenstein and Zierler [7] over finite fields. In 1960, Gorenstein *et al.* [8] showed that the covering radius of binary 2-error-correcting BCH codes was 3, and further, the covering radius of the extended codes was 4. The study of 2-error-correcting BCH codes is very thorough, including covering radius, weight distribution, coset weight distribution and so on. The covering radius of the 2-error-correcting binary primitive BCH codes is known. From the definition of deep holes, we know that the deep holes of these BCH codes exist. Since linear codes play an important role in the fields of data storage, information security and secret sharing, the construction of linear codes is one of the important contents in the current cryptography and coding research. Therefore, it is very meaningful to construct binary linear codes.

In this paper, our main work is to construct some binary linear codes by combining deep holes with BCH codes. Furthermore, we can determine the parameters and the weight distributions of the binary linear codes. Finally, some examples are presented by Magma experiments, which support the weight distributions of these binary linear codes. These experimental results coincide with the theoretical results.

The rest of this paper is outlined as follows. Section 2 states some notations and results about narrow-sense binary primitive BCH codes and linear codes. In Section 3, three classes of binary linear codes are constructed and their parameters are determined. In Section 4, the weight distributions of these binary linear codes are obtained. Finally, the conclusion of this paper is given.

2. Preliminaries

In this section, we state some basic facts and known results about linear codes and narrow-sense binary primitive BCH codes.

2.1. The Weight Distributions of the Linear Code and Its Dual Code

For an $[n,k]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$, and denote its dual by $\mathcal{C}^{\perp}$. The weight distribution of $\mathcal{C}$ can be uniquely determined by the weight distribution of $\mathcal{C}^{\perp}$ and vice versa. This linear relationship is crucial for investigating and calculating weight distribution, and we call it the MacWilliams identity.

Let A_j and $A_j^{\perp}$ be the number of codewords of weight j in $\mathcal{C}$ and $\mathcal{C}^{\perp}$, respectively. The *MacWilliams identity* is defined by

$$\sum_{i=0}^{n-j}\binom{n-i}{j}A_i^{\perp}=q^{k-j}\sum_{i=0}^{j}\binom{n-i}{n-j}A_i,\ \text{for all } j\in[0,n]. \tag{1}$$

Equivalently, we have

$$\sum_{j=0}^{n} j^r A_j=\sum_{j=0}^{\min\{n,r\}}(-1)^j A_j^{\perp}\left[\sum_{t=j}^{r} t!S(r,t)q^{k-t}(q-1)^{t-j}\binom{n-j}{n-t}\right]\ \text{for } r\geq 0, \tag{2}$$

and it is more convenient for us to calculate. But it involves the Stirling numbers $S(r,t)$ of the second kind, where $S(r,t)$ is defined by

$$S(r,t)=\frac{1}{t!}\sum_{i=0}^{t}(-1)^{t-i}\binom{t}{i}i^r\ \text{ for } r,t\geq 0. \tag{3}$$

In particular, $S(r,t)=0$ if $r<t$ and $S(r,r)=1$.

In binary codes, from (2), we deduce

$$\sum_{j=0}^{n}A_j j^r=\sum_{j=0}^{\min\{n,r\}}(-1)^j A_j^{\perp}\left[\sum_{t=j}^{r}\left(\sum_{i=1}^{t}(-1)^{t-i}\binom{t}{i}i^r\right)2^{k-t}\binom{n-j}{n-t}\right]\ \text{for } r\geq 0. \tag{4}$$

From (2), the first four Pless power moments are listed as follows ([9], p. 259):

$$\sum_{j=0}^{n}A_j=q^k;$$

$$\sum_{j=0}^{n}jA_j=q^{k-1}\left(qn-n-A_1^{\perp}\right);$$

$$\sum_{j=0}^{n}j^2A_j=q^{k-2}\left[(q-1)n(qn-n+1)-(2qn-q-2n+2)A_1^{\perp}+2A_2^{\perp}\right];$$

$$\begin{aligned}\sum_{j=0}^{n} j^3 A_j = q^{k-3}\Big[&(q-1)n\left(q^2n^2-2qn^2+3qn-q+n^2-3n+2\right)\\ &-\left(3q^2n^2-3q^2n-6qn^2+12qn+q^2-6q+3n^2-9n+6\right)A_1^{\perp}\\ &+6(qn-q-n+2)A_2^{\perp}-6A_3^{\perp}\Big].\end{aligned}$$

2.2. Cyclic Codes and Narrow-Sense BCH Codes

An $[n,k,d]$ linear code $\mathcal{C}$ over the finite field $\mathbb{F}_q$, it is said to be cyclic if the codeword $(c_{n-1},c_0,\cdots,c_{n-2})\in\mathcal{C}$ implies $c=(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$. For each vector $(c_0,c_1,\cdots,c_{n-1})\in\mathbb{F}_q^n$, define $c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in\mathbb{F}_q[x]/(x^n-1)$, any code $\mathcal{C}$ corresponds to a subset of quotient ring $\mathbb{F}_q[x]/(x^n-1)$. Note that a linear code $\mathcal{C}$ is cyclic if and only if the corresponding subset is an ideal of the quotient ring $\mathbb{F}_q[x]/(x^n-1)$. Besides, every ideal of $\mathbb{F}_q[x]/(x^n-1)$ is principal. Thus, every code $\mathcal{C}$ can be expressed as $\mathcal{C}=\langle g(x)\rangle$, where $g(x)$ is monic and has the smallest degree. $g(x)$ is said the generator polynomial, and $h(x)=(x^n-1)/g(x)$ is referred to as the check polynomial of $\mathcal{C}$.

Let $n=q^m-1$, where m is an integer with $m>1$. Let α be a primitive element of $\mathbb{F}_{q^m}^*$. In addition, let $m_i(x)$ be the minimal polynomial of α^i with $1\le i\le q^m-2$ over $\mathbb{F}_q$. For any $2\le\eta\le n$, define

$$g_{(q,m,\eta)}(x)=lcm\left(m_1(x),m_2(x),\cdots,m_{\eta-1}(x)\right),$$

where lcm denotes the least common multiple of these minimal polynomials.

Let $\mathcal{C}_{(q,m,\eta)}$ denote the cyclic code with generator polynomial $g_{(q,m,\eta)}(x)$, then we know $\mathcal{C}_{(q,m,\eta)}=\langle g_{(q,m,\eta)}(x)\rangle$. The set $\mathcal{C}_{(q,m,\eta)}$ is described as a narrow-sense primitive BCH code with design distance η. An $[n,k,d]$ linear code $\mathcal{C}$ is said e-error-correcting if $e=\left\lfloor\frac{d-1}{2}\right\rfloor$.

Let E denote the 2-error-correcting binary primitive BCH codes, and denote its dual by $E^{\perp}$. The code E is an $[n=2^m-1,k_E=2^m-2m-1,5]$ linear code, for $m\ge3$. The code E has parity-check matrix H_E defined by

$$H_E=\begin{bmatrix}1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1}\\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)}\end{bmatrix}.$$

The code E consists of all binary codewords $x=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$ such that $H_Ex^{\mathrm{T}}=0$. The extended code of B denote $\hat{E}$ and denote its duals by $\hat{E}^{\perp}$. A vector r of $\hat{E}$ is $r=(x_\infty,x_0,x_1,\cdots,x_{n-1})$ where $x_\infty=\sum_{i=0}^{n-1}x_i$. The code $\hat{E}$ has parameters $[N=2^m,k_{\hat{E}}=2^m-2m-1,6]$ for $m\ge3$. The parity-check matrix $H_{\hat{E}}$ is defined by

$$H_{\hat{E}}=\begin{bmatrix}1 & 1 & 1 & 1 & \cdots & 1\\ 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1}\\ 0 & 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)}\end{bmatrix},$$

where α is an element of order $n=2^m-1$ in $\mathbb{F}_2^n$. The code $\hat{E}$ consists of all binary codewords $r=(x_\infty,x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^N$ such that $H_{\hat{E}}r^{\mathrm{T}}=0$.

2.3. The Weight Distributions of 2-Error-Correcting Binary Primitive BCH Codes and the Extended Codes

In this subsection, we introduce the weight distributions of the 2-error-correcting binary narrow-sense BCH codes and of their extensions, whose length are respectively 2^m-1 and 2^m.

The code $E^{\perp}$ is an $\left[n=2^m-1, 2m, 2^{m-1}-2^{(m-1)/2}\right]$ linear code in [10], for odd $m \geq 3$. The code $E^{\perp}$ is a binary linear code with the weight distribution in Table 1.

The code $\hat{E}^{\perp}$ is an $\left[N=2^m, 2m+1, 2^{m-1}-2^{m/2}\right]$ linear code in ([11], Table 16.5), for odd $m \geq 3$. The code $\hat{E}^{\perp}$ is a binary linear code with the weight distribution in Table 2.

The code $\hat{E}^{\perp}$ is an $\left[N=2^m, 2m+1, 2^{m-1}-2^{(m-1)/2}\right]$ linear code, for even $m \geq 4$. The code $\hat{E}^{\perp}$ is a binary linear code with the weight distribution in Table 3.

Lemma 1. ([9], *Lemma* 7.5.1) *Let* $\mathcal{C}$ *be an* $[n,k]$ *linear code over* $\mathbb{F}_q$. *Suppose u is a vector in* $\mathbb{F}_q^n$ *but not in* $\mathcal{C}$. *The linear code is generated by* $\mathcal{C}$ *and u, which is an* $[n,k+1]$ *linear code. Let D be this linear code, then we have*

$$A_j(u+C)=A_j(D\setminus C)/(q-1) \text{ for } 0 \leq j \leq n.$$

Table 1. The weight distribution of $E^{\perp}$, for odd $m \geq 3$.

Weights	The number of codewords
0	1
$(n+1)/2-\sqrt{(n+1)/2}$	$n\left((n+1)/4+\sqrt{(n+1)/8}\right)$
$(n+1)/2$	$n\left((n+1)/2+1\right)$
$(n+1)/2+\sqrt{(n+1)/2}$	$n\left((n+1)/4-\sqrt{(n+1)/8}\right)$

Table 2. The weight distribution of $\hat{E}^{\perp}$, for odd $m \geq 3$.

Weights	The number of codewords
0, N	1
$N/2-\sqrt{N/2}$	$N(N-1)/2$
$N/2$	$N(N-1)(N+2)$
$N/2+\sqrt{N/2}$	$N(N-1)/2$

Table 3. The weight distribution of $\hat{E}^{\perp}$, for even $m \geq 4$.

Weights	The number of codewords
0, N	1
$N/2 \pm \sqrt{N}$	$N(N-1)/12$
$N/2$	$(N-1)(N+4)/2$
$N/2 \pm \sqrt{N/4}$	$2N(N-1)/3$

DOI: 10.4236/am.2023.1410040

In binary codes, it is clear that we have

$$A_j(u+C)=A_j(D\setminus C) \text{ for } 0\le j\le n.$$

In other words, we have

$$A_j(u+C)=A_j(D)-A_j(C) \text{ for } 0\le j\le n.$$

Theorem 2. ([9], *Th.* 7.3.1) *Let T be a set $\{1,2,3,\cdots,d\}$ with $|T|=d$. The weight distribution of $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are determined by $A_1^{\perp},A_2^{\perp},\cdots,A_{d-1}^{\perp}$ and the A_i with $i\notin T$.*

It is very convenient for us to calculate the weight distribution. The following corollary can be deduced from Theorem 2.

Corollary 3. *Let $\mathcal{C}$ be an $[n,k,d]$ linear code over $\mathbb{F}_q$, and denote its dual by $\mathcal{C}^{\perp}$. Then the dual code $\mathcal{C}^{\perp}$ is a linear code of length n and dimension $n-k$. Let T be a set $\{1,2,3,\cdots,d\}$ with $|T|=d$ and $A_1=A_2=\cdots=A_{d-1}=0$, so the weight distribution of $\mathcal{C}^{\perp}$ is uniquely determined. If $r<d$, (4) is equivalent to*

$$\sum_{j=0}^{n}A_j^{\perp}j^r=\sum_{d=0}^{r}\left(\sum_{i=1}^{d}(-1)^{d-i}\binom{d}{i}i^r\right)2^{n-k-d}\binom{n}{d} \text{ for } 0\le r<d. \tag{5}$$

It is very convenient to calculate the weight distribution of the dual code $\mathcal{C}^{\perp}$. If $r\ge d$, we use (4).

Theorem 4. ([9], *Th.* 1.4.5) *Let $\mathcal{C}$ be an $[n,k,d]$ linear code over $\mathbb{F}_q$, then we have*

- $A_0(\mathcal{C})+A_1(\mathcal{C})+A_2(\mathcal{C})+\cdots+A_n(\mathcal{C})=q^k$.
- $A_0(\mathcal{C})=1$, and $A_1(\mathcal{C})=A_2(\mathcal{C})=\cdots=A_{d-1}(\mathcal{C})=0$.
- If $\mathcal{C}$ is a binary code, which contains the codeword $\mathbf{1}=11\cdots1$. We know $A_j(\mathcal{C})=A_{n-j}(\mathcal{C})$ for $0\le j\le n$.

Thus, for a 2-ary linear code $\mathcal{C}$, if $\mathcal{C}$ contains the codeword $\mathbf{1}=11\cdots1$, then the weight distribution of $\mathcal{C}$ is symmetric.

3. The Parameters of Three Classes of Binary Linear Codes

In this chapter, we construct three classes of binary linear codes based on deep holes, then determine the parameters of these binary linear codes.

Let $\mathcal{C}$ be an $[n,k,d]$ linear code over the finite field $\mathbb{F}_q$, let u be a deep hole of the linear code $\mathcal{C}$, then we construct general linear code $\mathcal{C}_u=\{c+\lambda u\mid c\in\mathcal{C},\lambda\in\mathbb{F}_q\}$. We consider binary BCH codes combined with deep holes to construct general linear codes.

Three classes of binary linear codes are constructed by deep holes combined with the 2-error-correcting binary primitive BCH code and their extended codes, respectively.

Lemma 5. *The code E is an $[n=2^m-1,k_E=2^m-2m-1,5]$ linear code. Suppose u is a deep hole of the code E, and construct general binary linear code $E_u=\{c+\lambda u\mid c\in E,\lambda\in\mathbb{F}_2\}$. Then the code E_u is an $[n=2^m-1,2^m-2m,3]$ linear code, and the dual code $E_u^{\perp}$ is an $[n=2^m-1,K_E=2^m-1,2^{m-1}-2^{(m-1)/2}]$*

linear code, where m is odd and $m \geq 3$.

Proof. Let $\alpha_1, \alpha_2, \cdots, \alpha_{k_E}$ be a basis for a k_E-dimensional subspace of $\mathbb{F}_q^n$, and the code E is a vector space $span\left(\alpha_1, \alpha_2, \cdots, \alpha_{k_E}\right)$. Since the covering radius of code E is 3, from the definition of deep hole, the maximum error distance $d(u, E) = 3$. Moreover, the minimum distance of E is 5, it is easy to know that $u \notin E$. The binary linear code E_u is constructed, we have

$$u \in E_u \text{ and } E \subset E_u.$$

Furthermore, we obtain

$$d(u, E) = d(u, E_u) = 3,$$

so the minimum distance of the linear code E_u is 3. The binary code E_u is the vector space $span\left(\alpha_1, \alpha_2, \cdots, \alpha_{k_E}, u\right)$. Since $u \notin E$, so the dimension of the linear code E_u is $k_E + 1$. Namely, the code E_u has parameters $\left[n = 2^m - 1, 2^m - 2m, 3\right]$.

Let set $S = \left\{i > 0 \mid A_i\left(E^{\perp}\right) \neq 0\right\}$ for $0 < i \leq n$. As $E_u^{\perp} \subset E^{\perp}$, we get

$$A_i\left(E_u^{\perp}\right) = 0 \text{ for } i \neq 0$$

and $i \notin S$. We denote the minimum Hamming distance of the code $E_u^{\perp}$ by $d^{\perp}$, from the weight distribution in Table 1, we have

$$d^{\perp} = 2^{m-1} - 2^{(m-1)/2} \text{ for odd } m \geq 3.$$

Then the dual code $E_u^{\perp}$ has parameters $\left[n = 2^m - 1, K_E = 2m - 1, 2^{m-1} - 2^{(m-1)/2}\right]$, for odd $m \geq 3$. Therefore, the parameters of the code E_u and of its dual code $E_u^{\perp}$ are determined separately. □

We similarly construct several classes of binary linear codes and determine their parameters. The proof is similar to that of Lemma 5 and is omitted here. These binary linear codes are as follows.

Lemma 6. *The code* $\hat{E}$ *is an* $\left[N = 2^m, k_{\hat{E}} = 2^m - 2m - 1, 6\right]$ *linear code. Suppose u is a deep hole of the code* $\hat{E}$. *We construct general binary linear code* $\hat{E}_u = \left\{c + \lambda u \mid c \in \hat{E}, \lambda \in \mathbb{F}_2\right\}$. *Then the code* $\hat{E}_u$ *is an* $\left[N = 2^m, 2^m - 2m, 4\right]$ *linear code, and the dual code* $\hat{E}_u^{\perp}$ *is an* $\left[N = 2^m, K_{\hat{E}} = 2^m, 2^{m-1} - 2^{(m-1)/2}\right]$ *linear code, where m is odd and* $m \geq 3$.

Lemma 7. *The code* $\hat{E}$ *is an* $\left[N = 2^m, k_{\hat{E}} = 2^m - 2m - 1, 6\right]$ *linear code, suppose* u_1 *is a deep hole of the code* $\hat{E}$. *We construct general binary linear code* $\hat{E}_{u_1} = \left\{c + \lambda u_1 \mid c \in \hat{E}, \lambda \in \mathbb{F}_2\right\}$. *Then the code* $\hat{E}_{u_1}$ *has parameters* $\left[N = 2^m, 2^m - 2m, 4\right]$, *and the dual code* $\hat{E}_{u_1}^{\perp}$ *has parameters* $\left[N = 2^m, K_{\hat{E}} = 2^m, 2^{m-1} - 2^{m/2}\right]$, *for even* $m \geq 4$.

4. The Weight Distributions of Three Classes of Binary Linear Codes

In this part, we determine the weight distributions of these binary linear codes. From the general linear code $\mathcal{C}_u = \left\{c + \lambda u \mid c \in \mathcal{C}, \lambda \in \mathbb{F}_q\right\}$, the weight distributions of these binary linear codes are related to the coset weight distributions of

BCH codes. The coset weight distributions of BCH codes have been studied in the literature [12] [13].

To facilitate the computation of the weight distribution of the dual code, the following lemma can be deduced.

Lemma 8. *Let* $\mathcal{C}$ *be an* $[n,k,d]$ *linear code, and denote its dual by* $\mathcal{C}^{\perp}$. *Then* $A_1(\mathcal{C})=A_2(\mathcal{C})=\cdots=A_{d-1}(\mathcal{C})=0$ *and* $A_0(\mathcal{C})=1$. *Thus by Corollary* 3, *the weight distribution of* $\mathcal{C}^{\perp}$ *can be determined by the first d Pless power moments, we obtain*

$$\begin{cases}\sum_{i=0}^{n} A_i^{\perp}=2^{n-k},\\ \sum_{i=0}^{n} iA_i^{\perp}=2^{n-k-1}n,\\ \sum_{i=0}^{n} i^2A_i^{\perp}=2^{n-k-2}n(n+1),\\ \sum_{i=0}^{n} i^3A_i^{\perp}=2^{n-k-3}n^2(n+3),\\ \sum_{i=1}^{n} i^4A_i^{\perp}=2^{n-k-4}n(n+1)(n^2+5n-2),\\ \sum_{i=1}^{n} i^5A_i^{\perp}=2^{n-k-5}n^2(n^3+10n^2+15n-10),\\ \sum_{i=1}^{n} i^6A_i^{\perp}=2^{n-k-6}n(n+1)(n^4+14n^3+31n-46n+16),\\ \cdots,\end{cases} \tag{6}$$

where $A_i^{\perp}$ is the number of codewords of weight i in $\mathcal{C}^{\perp}$.

Theorem 9. *The binary code* E_u *is an* $\left[n=2^m-1,2^m-2m,3\right]$ *linear code, and the dual code* $E_u^{\perp}$ *is an* $\left[n=2^m-1,K_E=2m-1,2^{m-1}-2^{(m-1)/2}\right]$ *linear code, where m is odd and* $m\geq 3$. *Moreover, the weight distribution of* $E_u^{\perp}$ *is shown in* **Table 4**.

Proof. Let $U=\left\{w_i>0 \mid A_{w_i}\left(E^{\perp}\right)\neq 0\right\}$, as $E_u^{\perp}\subset E^{\perp}$, we have $A_{w_i}\left(E_u^{\perp}\right)=0$ if $w_i\neq 0$ and $w_i\notin U$. From **Table 1**, it is easily seen that the minimum weight distribution of $E_u^{\perp}$ is at least 3. Thus, there are three nonzero weights of $E_u^{\perp}$ as follows:

$$w_1=(n+1)/2-\sqrt{(n+1)/2},\ w_2=(n+1)/2,\ w_3=(n+1)/2+\sqrt{(n+1)/2}.$$

So the weight of the code $E_u^{\perp}$ contains $\{w_1,w_2,w_3\}$. Let $A_{w_i}^{\perp}$ be the total number of codewords with weight w_i in $E_u^{\perp}$. In addition, let $A_i=A_i(E_u)$ and $A_i^{\perp}=A_i\left(E_u^{\perp}\right)$, where $0\leq i\leq n$. For binary linear codes, then the first three Pless power moments from Lemma 8, we obtain

$$\begin{cases}\sum_{j=1}^{3} A_{w_j}^{\perp}=2^{K_E}-1,\\ \sum_{j=1}^{3} w_jA_{w_j}^{\perp}=2^{K_E-1}n,\\ \sum_{j=1}^{3} w_j^2A_{w_j}^{\perp}=2^{K_E-2}n(n+1),\end{cases} \tag{7}$$

where $2^{K_E}=2^{2m-1}$ and $n=2^m-1$.

By solving this system of equations, we obtain the results in **Table 4**. The proof is complete. □

Two examples are presented by Magma experiments, which support Theorem 9.

Table 4. The weight distribution of $E_u^{\perp}$, for odd $m \geq 3$.

Weights	The number of codewords
0	1
$(n+1)/2-\sqrt{(n+1)/2}$	$(n-1)\left((n+1)/2+\sqrt{(n+1)/2}\right)/4$
$(n+1)/2+\sqrt{(n+1)/2}$	$(n-1)\left((n+1)/2-\sqrt{(n+1)/2}\right)/4$
$(n+1)/2$	$\left(3n^2+8n-3\right)/8$

Example 1. *Let* $m=3$ *and let the deep hole vector* $u=(1,1,1,0,\cdots,0)$, *the binary code* E_u *has parameters* $[7,2,3]$. *In Theorem* 9, *the code* $E_u^{\perp}$ *is a* $[7,5,2]$ *binary linear code with the weight enumerator* $1+9z^2+19z^4+3z^6$.

Example 2. *Let* $m=5$ *and let the deep hole vector* $u=(1,1,1,0,\cdots,0)$, *the binary linear code* E_u *has parameters* $[31,22,3]$. *In Theorem* 9, *the code* $E_u^{\perp}$ *is a* $[31,9,12]$ *binary linear code with the weight enumerator* $1+150z^{12}+271z^{16}+90z^{20}$.

Theorem 10. *The binary code* $\hat{E}_u$ *is an* $\left[N=2^m,2^m-2m,4\right]$ *linear code, and the dual code* $\hat{E}_u^{\perp}$ *is an* $\left[N=2^m,K_{\hat{E}}=2m,2^{m-1}-2^{(m-1)/2}\right]$ *linear code, where m is odd and* $m\geq 3$. *Moreover, the weight distribution of* $\hat{E}_u^{\perp}$ *is shown in* Table 5.

Proof. Let $U_1=\left\{w_j>0 \mid A_{w_j}\left(\hat{E}^{\perp}\right)\neq 0\right\}$, as $\hat{E}_u^{\perp}\subset\hat{E}^{\perp}$, we have $A_{w_j}\left(\hat{E}_u^{\perp}\right)=0$ if $w_j\neq 0$ and $w_j\notin U_1$. From Table 2, it is easily seen that the minimum weight distribution of $\hat{E}_u^{\perp}$ is at least 4. Therefore, we know that the code $\hat{E}_u^{\perp}$ has the following four nonzero weights:

$$w_1=N/2-\sqrt{N/2},\ w_2=N/2,\ w_3=N/2+\sqrt{N/2},\ w_4=N.$$

The weight of the code $\hat{E}_u^{\perp}$ contains $\{w_1,w_2,w_3,w_4\}$. Let $A_{w_j}^{\perp}$ be the total number of codewords with Hamming weight w_j in $\hat{E}_u^{\perp}$, and let $A_i=A_i\left(\hat{E}_u\right)$ and $A_i^{\perp}=A_i\left(\hat{E}_u^{\perp}\right)$ for $0\leq i\leq N$. Since $\hat{E}$ is even and contains the codeword $1=111\cdots 1$. From Theorem 4, we have $A_{w_j}^{\perp}=A_{N-w_j}^{\perp}$ and $A_0^{\perp}=A_N^{\perp}=1$ for $w_j\in U_1$. For the binary linear code, then the first and the third Pless power moments from Lemma 8, we obtain

$$\begin{cases}\sum_{j=1}^{4}A_{w_j}^{\perp}=2^{K_{\hat{E}}}-1,\\ \sum_{j=1}^{4}w_j^2A_{w_j}^{\perp}=2^{K_{\hat{E}}-2}N(N+1),\end{cases} \tag{8}$$

where $2^{K_{\hat{E}}}=2^{2m}$ and $N=2^m$.

By solving this system of equations, we obtain the results in Table 5. The proof is complete. □

Two examples are presented by Magma experiments, which support Theorem 10.

Example 3. *Let* $m=3$ *and let the deep hole vector* $u=(1,1,1,1,0,\cdots,0)$, *the binary linear code* $\hat{E}_u$ *has parameters* $[8,2,4]$. *In Theorem* 10, *the code* $\hat{E}_u^{\perp}$ *is a* $[8,6,2]$ *binary linear code with the weight enumerator* $1+12z^2+38z^4+12z^6+z^8$.

Table 5. The weight distribution of $\hat{E}_u^{\perp}$, for odd $m \ge 3$.

Weights	The number of codewords
$0, N$	1
$N/2-\sqrt{N/2}$	$N^2/4-N/2$
$N/2+\sqrt{N/2}$	$N^2/4-N/2$
$N/2$	$N^2/2+N-2$

Example 4 *Let* $m=5$ *and let the deep hole vector* $u=(1,1,1,0,1,0,\cdots,0)$, *the binary linear code* $\hat{E}_u$ *has parameters* $[32,22,4]$. *In Theorem* 10, *the code* $\hat{E}_u^{\perp}$ *is a* $[32,10,12]$ *binary linear code with the weight enumerator* $1+240z^{12}+542z^{16}+240z^{20}+z^{32}$.

Theorem 11. *The binary code* $\hat{E}_{u_1}$ *is an* $[N=2^m, 2^m-2m, 4]$ *linear code, and the dual code* $\hat{E}_{u_1}^{\perp}$ *is an* $[N=2^m, K_{\hat{E}}=2m, 2^{m-1}-2^{m/2}]$, *where m is even and* $m \ge 4$. *Moreover, the weight distribution of* $\hat{E}_{u_1}^{\perp}$ *is shown in* Table 6.

Proof. Let $U_2=\{w_i>0 \mid A_{w_i}(\hat{E}^{\perp})\ne 0\}$, as $\hat{E}_{u_1}^{\perp}\subset \hat{E}^{\perp}$, we have $A_{w_i}(\hat{E}_{u_1}^{\perp})=0$ if $w_i \ne 0$ and $w_i \notin U_2$. From Table 3, it is easily seen that the minimum weight distribution of $\hat{E}_{u_1}^{\perp}$ is at least 6. Thus, there are six nonzero weights of $\hat{E}_{u_1}^{\perp}$ as follows:

$$w_1=N/2-\sqrt{N},\ w_2=N/2-\sqrt{N/4},\ w_3=N/2,$$

$$w_4=N/2+\sqrt{N/4},\ w_5=N/2-\sqrt{N},\ w_6=N.$$

The weight of the code $\hat{E}_{u_1}^{\perp}$ contains $\{w_1,w_2,w_3,w_4,w_5,w_6\}$. Let $A_{w_i}^{\perp}$ be the total number of codewords with Hamming weight w_i in $\hat{E}_{u_1}^{\perp}$, and let $A_i=A_i(\hat{E}_{u_1})$ and $A_i^{\perp}=A_i(\hat{E}_{u_1}^{\perp})$ for $0\le i\le N$. Since $\hat{E}$ is even and contains the code word $1=111\cdots 1$. From theorem 4, we know that $A_{w_j}^{\perp}=A_{N-w_j}^{\perp}$ and $A_0^{\perp}=A_N^{\perp}=1$ for $w_j\in U_2$. For this binary linear code, then the first, the third and the fifth Pless power moments from Lemma 8 and Corollary 3, we obtain

$$\begin{cases}\sum_{j=1}^{6} A_{w_j}^{\perp}=2^{K_{\hat{E}}}-1,\\ \sum_{j=1}^{6} w_j^2 A_{w_j}^{\perp}=2^{K_{\hat{E}}-2}N(N+1),\\ \sum_{j=1}^{6} w_j^4 A_{w_j}^{\perp}=2^{K_{\hat{E}}-4}\left(N(N+1)(N^2+5N-2)+24A_4\right),\end{cases} \tag{9}$$

where $2^{K_{\hat{E}}}=2^{2m}$ and $N=2^m$. Since $\hat{E}_{u_1}$ has parameters $[N=2^m,2^m-2m,4]$, the minimum Hamming distance is 4, so $A_1=A_2=A_3=0$. We need to determine the number of codewords of weight 4 in $\hat{E}_{u_1}$. Since u_1 is a vector in $\mathbb{F}_2^N$ but not in $\hat{E}$. From Lemma 1, we have

$$A_4(\hat{E}_{u_1})=A_4(\hat{E})+A_4(\hat{E}+u_1).$$

The minimum distance of $\hat{E}$ is 6, thus we have $A_4(\hat{E})=0$, so

$$A_4(\hat{E}_{u_1})=A_4(\hat{E}+u_1).$$

The number of codewords of weight 4 in the coset $\hat{E}+u_1$ is determined in the literature ([13], Remark 4), then we obtain

Table 6. The weight distribution of $\hat{E}_{u_1}^{\perp}$, for even $m \geq 4$.

Weights	The number of codewords
0, N	1
$N/2 \pm \sqrt{N}$	$\left(N^2 - 4N\right)/24$
$N/2$	$N^2/4 + N - 2$
$N/2 \pm \sqrt{N/4}$	$\left(N^2 - N\right)/3$

$$A_4\left(\hat{E} + u_1\right) = N\left(N - 4\right)/24.$$

Thus, we have

$$A_4\left(\hat{E}_{u_1}\right) = N\left(N - 4\right)/24.$$

By solving this system of equations, we obtain the results in Table 6. The proof is complete. □

Two examples are presented by Magma experiments, which support Theorem 11.

Example 5. *Let* $m = 4$ *and let the deep hole vector* $u_1 = (1,1,1,0,1,0,\cdots,0)$, *the binary linear code* $\hat{E}_{u_1}$ *has parameters* $[16,8,4]$. *In Theorem* 11, *the code* $\hat{E}_{u_1}^{\perp}$ *is a* $[16,8,4]$ *binary linear code with the weight enumerator* $1 + 8z^4 + 80z^6 + 78z^8 + 80z^{10} + 8z^{12} + z^{16}$.

Example 6. *Let* $m = 6$ *and let the deep hole vector* $u_1 = (1,1,1,0,1,0,\cdots,0)$, *the binary linear code* $\hat{E}_{u_1}$ *has parameters* $[64,48,4]$. *In Theorem* 11, *the code* $\hat{E}_{u_1}^{\perp}$ *is a* $[64,12,24]$ *binary linear code with the weight enumerator* $1 + 160z^{24} + 1344z^{28} + 1086z^{32} + 1344z^{36} + 160z^{40} + z^{64}$.

5. Concluding Remarks

In this paper, we consider binary 2-error-correcting BCH codes combined with deep holes to construct general linear codes $\mathcal{C}_u = \{c + \lambda u \mid c \in \mathcal{C}, \lambda \in \mathbb{F}_2\}$, where u is a deep hole of the codes $\mathcal{C}$. Therefore, we not only construct three classes of binary linear codes, but also determine the parameters and the weight distributions of these binary linear codes. Furthermore, we wish to construct more general linear codes related to deep holes.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Wu, R.J. and Hong, S.F. (2012) On Deep Holes of Standard Reed-Solomon Codes. *Science China Mathematics*, **55**, 2447-2455. https://doi.org/10.1007/s11425-012-4499-3

[2] Zhang, J., Fu, F.W. and Liao, Q.Y. (2013) Deep Holes of Generalized Reed-Solomon Codes. *Scientia Sinica Mathematica*, **43**, 727-740. (In Chinese)

https://doi.org/10.1360/012012-30

[3] Zhang, J., Wan, D.Q. and Kaipa, K. (2019) Deep Holes of Projective Reed-Solomon Codes. *IEEE Transactions on Information Theory*, **66**, 2392-2401. https://doi.org/10.1109/TIT.2019.2940962

[4] Zhang, J. and Wan, D.Q. (2023) On Deep Holes of Elliptic Curve Codes. *IEEE Transactions on Information Theory*, **69**, 4498-4506. https://doi.org/10.1109/TIT.2023.3257320

[5] Hocquenghem, A. (1959) Codes correcteurs d'rreurs. *Chiffres* (*Paris*), **2**, 147-156.

[6] Bose, R.C. and Ray-Chaudhuri, D.K. (1960) On a Class of Error Correcting Binary Group Codes. *Information and Control*, **3**, 68-79. https://doi.org/10.1016/S0019-9958(60)90287-4

[7] Gorenstein, D. and Zierler, N. (1961) A Class of Error-Correcting Codes in p^m Symbols. *Journal of the Society for Industrial and Applied Mathematics*, **9**, 207-214. https://doi.org/10.1137/0109020

[8] Gorenstein, D., Peterson, W.W. and Zierler, N. (1960) Two-Error Correcting Bose-Chaudhuri Codes Are Quasi-Perfect. *Information and Control*, **3**, 291-294. https://doi.org/10.1016/S0019-9958(60)90877-9

[9] Huffman, W.C. and Pless, V. (2003) Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9780511807077

[10] MacWilliams, F.J. and Sloane, N.J.A. (1977) The Theory of Error-Correcting Codes (I and II). North-Holland Publishing Company, Amsterdam.

[11] Berlekamp, E.R. (1968) Algebraic Coding Theory. McGraw-Hill, New York.

[12] Assmus, E. and Mattson, H. (1978) The Weight-Distribution of a Coset of a Linear Code (Corresp.). *IEEE Transactions on Information Theory*, **24**, 497-497. https://doi.org/10.1109/TIT.1978.1055903

[13] Charpin, P. (1994) Weight Distributions of Cosets of Two-Error-Correcting Binary BCH Codes, Extended or Not. *IEEE Transactions on Information Theory*, **40**, 1425-1442. https://doi.org/10.1109/18.333859