



Article

Analysis of Blind Reconstruction of BCH Codes

Soonhee Kwon  and Dong-Joon Shin * 

Department of Electronics and Computer Engineering, Hanyang University, Seoul 04763, Korea; tnsqml1991@hanyang.ac.kr

* Correspondence: djshin@hanyang.ac.kr

Received: 16 October 2020; Accepted: 4 November 2020; Published: 5 November 2020



Abstract: In this paper, the theoretical lower-bound on the success probability of blind reconstruction of Bose–Chaudhuri–Hocquenghem (BCH) codes is derived. In particular, the blind reconstruction method of BCH codes based on the consecutive roots of generator polynomials is mainly analyzed because this method shows the best blind reconstruction performance. In order to derive a performance lower-bound, the theoretical analysis of BCH codes on the aspects of blind reconstruction is performed. Furthermore, the analysis results can be applied not only to the binary BCH codes but also to the non-binary BCH codes including Reed–Solomon (RS) codes. By comparing the derived lower-bound with the simulation results, it is confirmed that the success probability of the blind reconstruction of BCH codes based on the consecutive roots of generator polynomials is well bounded by the proposed lower-bound.

Keywords: blind reconstruction; BCH codes; galois field; galois field fourier transform; lower-bound; RS codes

1. Introduction

In order to achieve reliable information transmission through noisy communication channels, the use of error-correcting codes (ECCs) in data-stream is indispensable [1]. By sharing the parameters of ECCs between the transmitter and the receiver, the errors occurred by communication channels can be detected or corrected at the receiver in a cooperative way. However, in a non-cooperative context, it is necessary to decode received (or intercepted) data without the knowledge of parameters of the used ECC. In other words, a blind reconstruction of the parameters of the used ECC should be performed by the receiver.

A blind reconstruction of ECCs has been studied in various ways [2–19]. The blind reconstruction schemes of linear block codes are studied in [2–9], the blind reconstruction schemes of Bose–Chaudhuri–Hocquenghem (BCH) codes are studied in [10–15], and the blind reconstruction schemes of convolutional codes are studied in [16–19]. Most of the blind reconstruction schemes of ECCs take the dual code approach to reconstruct the dual code space of the used code by using the received codewords. Valembois [2] proposed a detection and recognition algorithm for binary linear codes by using the dual code property and Cluzeau [3] proposed a blind reconstruction method based on iterative decoding techniques by using the dual code property. Moreover, most of the blind detection methods of BCH codes are also based on the dual code approach. By using the properties of BCH codes, their parity-check matrices can be constructed through applying Galois field Fourier transform (GFFT) on the received codewords and many of the blind reconstruction methods of BCH codes are based on GFFT [10–15]. In the same manner, most of the blind reconstruction methods of convolutional codes are also based on the dual code approach [16–19]. To reconstruct the generator polynomial or generator matrix of convolutional code, its dual code is recognized preferentially.

An analysis of the blind reconstruction of cyclic codes over binary erasure channel (BEC) is performed in [20]. Note that for BEC, the number and the locations of error bits in the received

data-stream are known to the receiver. By using this property of BEC, a blind reconstruction scheme of binary cyclic codes is proposed and a lower-bound on the detection probability of this scheme is analyzed in [20]. However, many blind reconstruction schemes consider the binary symmetric channel (BSC) where the number and the locations of error bits in the received data-stream are not unavailable. Therefore, the analysis in [20] is not directly applicable to the blind reconstruction schemes considering the BSC.

In this paper, the blind reconstruction of BCH codes over q -ary symmetric channel is mainly considered because BCH codes are a most widely used class of cyclic codes, especially in communication and storage systems and q -ary symmetric channel is a general form of BSC. Especially, the method in [15] shows the best blind reconstruction performance among the existing blind reconstruction methods of BCH codes, but the theoretical analysis of this method has not been performed yet. Therefore, by analyzing the properties of BCH codes on the aspects of blind reconstruction, a lower-bound on the success probability of the blind reconstruction method in [15] is derived. More specifically, the distribution of GFFT values of the received codewords is analyzed and the blind reconstruction method is formulated by using the conjugacy classes. By comparing the derived lower-bound with the simulation results, it is confirmed that the success probability of the blind reconstruction is well lower-bounded. Furthermore, the analysis of BCH codes on the aspects of blind reconstruction may lay a foundation for an analysis of other blind reconstruction methods of BCH codes based on GFFT.

In Section 2, definitions and properties of BCH codes and GFFT are briefly explained. In Section 3, the theoretic analysis of the properties of BCH codes on the aspects of blind reconstruction is performed. In Section 4, the blind reconstruction method in [15] is explained, and a lower-bound on the success probability of this blind reconstruction method is derived. The simulation results confirm that the success probability of the blind reconstruction method is well-bounded by the derived lower-bound. In Section 5, conclusions are provided.

2. BCH Codes and Galois Field Fourier Transform

In this section, the BCH codes and the Galois field Fourier transform (GFFT) are briefly described.

2.1. BCH Codes

BCH codes is a class of linear block codes for forward error correction. Let $GF(q)$ denote the Galois field (or finite field) of q elements and let $BCH_q(n, k)$ denote the BCH code with length n and dimension k over $GF(q)$. Note that the dimension k is the same as the length of random message which also implies the number of codewords. Then, the generator polynomial of $BCH_q(n, k)$ is defined as follows:

$$g(x) = LCM[M_{\alpha^b}(x), M_{\alpha^{b+1}}(x), \dots, M_{\alpha^{b+d-2}}(x)] \quad (1)$$

where LCM denotes the least common multiple function, α is a primitive n -th root of unity in $GF(q^m)$, $M_{\alpha^i}(x)$ is a minimal polynomial of α^i over $GF(q)$, b is an arbitrary positive integer smaller than n , and d is a designed distance. Note that m is the smallest integer such that n divides $q^m - 1$. By the definition of generator polynomial $g(x)$, $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+d-2}$ are the roots of $g(x)$, i.e., $g(\alpha^b) = g(\alpha^{b+1}) = \dots = g(\alpha^{b+d-2}) = 0$. Let S_r be the set of the exponents of all roots of $g(x)$ as follows:

$$S_r = \{i \mid g(\alpha^i) = 0, i \in \{0, 1, \dots, n-1\}\}. \quad (2)$$

A message can be expressed in polynomial form as $m(x) = m_0 + m_1x + \dots + m_{k-1}x^{k-1}$ and in vector form as $\mathbf{m} = (m_0, m_1, \dots, m_{k-1})$, where $m_i \in GF(q)$ for $i \in \{0, 1, \dots, k-1\}$. A codeword of $BCH_q(n, k)$ can be expressed in polynomial form as $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ and in vector form as $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$, where $c_i \in GF(q)$ for $i \in \{0, 1, \dots, n-1\}$. Then, $c(x)$ can be obtained as follows:

$$c(x) = m(x)g(x). \quad (3)$$

Since a codeword $c(x)$ has $g(x)$ as a factor, all roots of $g(x)$ are also roots of $c(x)$, i.e., $c(\alpha^i) = 0$ for all $i \in S_r$. In this paper, the q -ary symmetric channel with error probability ϵ is considered. Channel error can be expressed in polynomial form as $e(x) = e_0 + e_1x + \dots + e_{n-1}x^{n-1}$ and in vector form as $\mathbf{e} = (e_0, e_1, \dots, e_{n-1})$, where $e_i \in GF(q)$ for $i \in \{0, 1, \dots, n-1\}$. Note that by the definition of q -ary symmetric channel, $\Pr(e_i = 0) = 1 - \epsilon$ and $\Pr(e_i = x) = \epsilon/(q-1)$ for $i \in \{0, 1, \dots, n-1\}$ and $x \in GF^*(q)$ where $GF^*(q) = GF(q) \setminus \{0\}$. Then, a received codeword at the receiver is expressed in polynomial form as

$$r(x) = c(x) + e(x), \quad (4)$$

or in vector form as follows:

$$\mathbf{r} = \mathbf{c} + \mathbf{e}. \quad (5)$$

Throughout the paper, the polynomial form and the vector form will be used interchangeably.

If there is no error (i.e., $e(x) = 0$), $r(\alpha^i) = 0$ for all $i \in S_r$ because $r(x) = c(x)$. However, if $e(x) \neq 0$, we may have $r(\alpha^i) \neq 0$ for some $i \in S_r$ because it can be $e(\alpha^i) \neq 0$ for some $i \in S_r$.

2.2. Conjugacy Classes and Cyclotomic Cosets

Let U_β denote a conjugacy class of $\beta \in GF(q^m)$. Then, U_β consists of β and its conjugates $\beta^q, \beta^{q^2}, \beta^{q^3}, \dots$. Note that the conjugacy classes of the elements in the same conjugacy class are the same. The minimal polynomial of $\alpha^i \in GF(q^m)$ over $GF(q)$, $M_{\alpha^i}(x)$, can be obtained by using the conjugacy classes as follows:

$$M_{\alpha^i}(x) = \prod_{z \in U_{\alpha^i}} (x - z). \quad (6)$$

The degree of $M_{\alpha^i}(x)$ is equal to $|U_{\alpha^i}|$, where $|S|$ is the cardinality of a set S . Note that since $M_{\alpha^i}(x)$ has all the elements in U_{α^i} as its roots, $g(x)$ in (1) has all the elements in $U_{\alpha^b}, U_{\alpha^{b+1}}, \dots, U_{\alpha^{b+d-2}}$ as its roots. Let S_N denote the null spectrum of the $BCH_q(n, k)$ which has the generator polynomial in (1). Then S_N is obtained as follows:

$$S_N = \bigcup_{i=b}^{b+d-2} U_{\alpha^i}. \quad (7)$$

S_r in (2) is also expressed as the set of the exponents of the elements in S_N such as $S_r = \{i \mid \alpha^i \in S_N\}$. Then, the complement of S_r , denoted by S_r^c , is obtained as follows:

$$S_r^c = \{i \mid \alpha^i \in GF^*(q^m) \setminus S_N\}. \quad (8)$$

It is clear that $S_r^c = \mathbb{Z}_n \setminus S_r$ where $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$.

Let \mathcal{C}_i denote the cyclotomic coset of i modulo n with respect to $GF(q)$. Then, the exponents of all the elements in U_{α^i} make up \mathcal{C}_i and $S_r = \bigcup_{i=b}^{b+d-2} \mathcal{C}_i$ by (2) and (7).

2.3. Galois Field Fourier Transform

The roots of a received codeword $r(x)$ can also be obtained by performing the Galois field Fourier transform (GFFT) on $r(x)$. The GFFT of $c(x)$, denoted as $C(X)$, can be expressed in polynomial form as follows:

$$C(X) = c(\alpha^0) + c(\alpha^1)X + \dots + c(\alpha^{n-1})X^{n-1}, \quad (9)$$

where $c(\alpha^i) \in GF(q^m)$ for $i \in \{0, 1, \dots, n-1\}$. It is also expressed in vector form as follows:

$$\mathbf{C} = (C_0, C_1, \dots, C_{n-1}) = (c(\alpha^0), c(\alpha^1), \dots, c(\alpha^{n-1})). \quad (10)$$

The GFFT matrix M_G is defined as follows:

$$M_G = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 & \dots & \alpha^0 \\ \alpha^0 & \alpha^1 & \alpha^2 & \dots & \alpha^{n-1} \\ \alpha^0 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^0 & \alpha^{n-1} & \alpha^{2(n-1)} & \dots & \alpha^{(n-1)^2} \end{bmatrix}. \quad (11)$$

Then, the GFFT of c is simply obtained by $C = c \times M_G$. By the definition of $g(x)$ in (1), $C_b = C_{b+1} = \dots = C_{b+d-2} = 0$.

The GFFT of $r(x)$, denoted as $R(X)$, can be expressed in polynomial form as follows:

$$R(X) = r(\alpha^0) + r(\alpha^1)X + \dots + r(\alpha^{n-1})X^{n-1}, \quad (12)$$

where $r(\alpha^i) \in GF(q^m)$ for $i \in \{0, 1, \dots, n-1\}$. The vector form of $R(X)$ is expressed as follows:

$$R = (R_0, R_1, \dots, R_{n-1}) = (r(\alpha^0), r(\alpha^1), \dots, r(\alpha^{n-1})). \quad (13)$$

By using M_G in (11), the GFFT of r is simply obtained by $R = r \times M_G$. In the error-free case (i.e., $e(x) = 0$), $R_b = R_{b+1} = \dots = R_{b+d-2} = 0$. However, if $e(x) \neq 0$, we may have $R_i \neq 0$ for some $i \in \{b, b+1, \dots, b+d-2\}$.

The GFFT of $e(x)$, denoted as $E(X)$, can be expressed in polynomial form as follows:

$$E(X) = e(\alpha^0) + e(\alpha^1)X + \dots + e(\alpha^{n-1})X^{n-1}, \quad (14)$$

where $e(\alpha^i) \in GF(q^m)$ for $i \in \{0, 1, \dots, n-1\}$. The vector form of $E(X)$ is expressed as follows:

$$E = (E_0, E_1, \dots, E_{n-1}) = (e(\alpha^0), e(\alpha^1), \dots, e(\alpha^{n-1})). \quad (15)$$

By using (5), (10) and (13), it is clear that $R = C + E = (c + e)M_G$.

3. Theoretical Analysis of BCH Codes on the Aspects of Blind Reconstruction

3.1. GFFT of a Single Symbol Error

In this subsection, the GFFT values of a single symbol error is investigated. Let $wt(\mathbf{a})$ denote the Hamming weight of a vector \mathbf{a} , i.e., $wt(\mathbf{a})$ is the number of non-zero elements in \mathbf{a} . Note that a single symbol error $e(x)$ satisfies $wt(\mathbf{e}) = 1$.

Lemma 1. *If a received codeword $r(x)$ of $BCH_q(n, k)$ contains a single symbol error, then*

$$r(\alpha^i) \neq 0, \forall i \in S_r. \quad (16)$$

Proof. Let $e(x) = e_j x^j$ for some $j \in \{0, 1, \dots, n-1\}$ and $e_j \in GF^*(q)$. Since the GFFT value of $e(x)$ with respect to α^i is $E_i = e(\alpha^i) = e_j \alpha^{ij} \neq 0$ for all $i \in \{0, 1, \dots, n-1\}$ and $C_i = 0$ for $i \in S_r$, $R_i = C_i + E_i \neq 0$ for $i \in S_r$. \square

Lemma 1 shows that if $r(x)$ contains a single symbol error, any root of $g(x)$ cannot be a root of $r(x)$. In the next subsection, the distribution of GFFT values of $c(x)$ is analyzed.

3.2. GFFT of Codewords

Let $S_{c(\alpha^i)}$ denote the set of the GFFT values taken by all the codewords $c(x)$ of $BCH_q(n, k)$ for $x = \alpha^i$ as follows:

$$S_{c(\alpha^i)} \triangleq \{c(\alpha^i) \mid c(x) \in BCH_q(n, k)\}. \tag{17}$$

Suppose that the minimal polynomial $M_\alpha(x)$ of a primitive n -th root of unity $\alpha \in GF(q^m)$ over $GF(q)$ has a degree m' where $m' \mid m$. Then, any $\alpha^i \in GF(q^m)$ can be expressed by a linear combination of $\alpha^0, \alpha^1, \dots, \alpha^{m'-1}$ as follows:

$$\alpha^i = h_0 + h_1\alpha + \dots + h_{m'-1}\alpha^{m'-1}, \tag{18}$$

where $h_i \in GF(q)$ for $i \in \{0, 1, \dots, m' - 1\}$. Moreover, based on (18), any $\alpha^i \in GF(q^m)$ can be expressed in vector form, denoted as v_{α^i} , as follows:

$$v_{\alpha^i} = (h_0, h_1, \dots, h_{m'-1}). \tag{19}$$

Note that v_{α^i} is a row vector. Let $V_{\alpha^i} \in GF(q)^{n \times m'}$ be a matrix with $v_{(\alpha^i)0}, v_{(\alpha^i)1}, \dots, v_{(\alpha^i)n-1}$ as its rows, and $rk(\alpha^i)$ denote the rank of V_{α^i} over $GF(q)$.

Lemma 2. Suppose that a message $m(x)$ is generated uniformly at random, a codeword $c(x)$ of $BCH_q(n, k)$ is encoded by $g(x)$ as in (3), and $k \geq rk(\alpha^i)$. Then, it is satisfied that

$$S_{c(\alpha^i)} = \{0\}, \forall i \in S_r, \tag{20}$$

$$|S_{c(\alpha^i)}| = q^{rk(\alpha^i)}, \forall i \in S_r^c, \tag{21}$$

$$\Pr(c(\alpha^i) = x) = \frac{1}{|S_{c(\alpha^i)}|}, \forall x \in S_{c(\alpha^i)}. \tag{22}$$

Proof. First of all, for any $i \in S_r$, it is always true that $c(\alpha^i) = 0$ due to the definition of S_r . Therefore, $S_{c(\alpha^i)} = \{0\}$ and $\Pr(c(\alpha^i) = 0) = 1/|S_{c(\alpha^i)}| = 1$ for any $i \in S_r$.

Second, in order to prove (21), let $\Gamma \in GF(q)^{q^k \times n}$ denote a matrix having all the q^k codewords of $BCH_q(n, k)$ as its rows. Then, the GFFT values of q^k codewords can be expressed in vector form as follows:

$$\Lambda = \Gamma \times V_{\alpha^i}, \tag{23}$$

where $\Lambda \in GF(q)^{q^k \times m'}$ is a matrix with the vector forms of all GFFT values of q^k codewords with respect to α^i as its rows. Note that the rank of Γ is k because all the rows of Γ are the codewords of $BCH_q(n, k)$, and the rank of V_{α^i} is $rk(\alpha^i)$ by the definition. The matrix Γ can be decomposed as $\Gamma = \Delta \times G$ where Δ has all the elements of $GF(q)^k$ as its rows and G is the generator matrix of $BCH_q(n, k)$. Note that the rank of Λ , $rank(\Lambda)$, is equal to $rank(\Gamma \times V_{\alpha^i}) = rank(\Delta \times G \times V_{\alpha^i})$. Since the size of Δ is $q^k \times k$ and $rank(\Delta) = k$, $rank(\Delta \times G \times V_{\alpha^i}) = rank(G \times V_{\alpha^i})$. The j -th row of $G \times V_{\alpha^i}$ is expressed as $g_j \times V_{\alpha^i}$ where g_j is the j -th row of G , $j \in \{1, 2, \dots, k\}$. Since $g_j \times V_{\alpha^i} \neq 0$ for $i \in S_r^c$ and $j \in \{1, 2, \dots, k\}$, g_1, g_2, \dots, g_k are linearly independent, and $k \geq rk(\alpha^i)$, it is clear that $rank(G \times V_{\alpha^i})$ is equal to $rk(\alpha^i)$. Therefore, the rank of Λ is also equal to $rk(\alpha^i)$, which implies that there are $q^{rk(\alpha^i)}$ distinct rows in Λ and $|S_{c(\alpha^i)}| = q^{rk(\alpha^i)}$ for any $i \in S_r^c$.

Lastly, in order to show (22), let $x_0, x_1, \dots, x_{n_1-1} \in GF(q)^n$ be all distinct codewords such that $x_0(\alpha^i) = x_1(\alpha^i) = \dots = x_{n_1-1}(\alpha^i) = x$ for given i and $x \in GF(q^m)$. Also, let $y_0, y_1, \dots, y_{n_2-1} \in GF(q)^n$ be all distinct codewords such that $y_0(\alpha^i) = y_1(\alpha^i) = \dots = y_{n_2-1}(\alpha^i) = y$ for the same i and $y \in GF(q^m)$. These relations can be expressed in matrix multiplication as follows:

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n_1-1} \end{bmatrix} \times M_G^{(i+1)} = \begin{bmatrix} x \\ x \\ \vdots \\ x \end{bmatrix}, \tag{24}$$

$$\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n_2-1} \end{bmatrix} \times M_G^{(i+1)} = \begin{bmatrix} y \\ y \\ \vdots \\ y \end{bmatrix}, \tag{25}$$

where $M_G^{(i+1)}$ is the $(i + 1)$ -st column of M_G in (11). In order to show $\Pr(c(\alpha^i) = x) = 1/|S_{c(\alpha^i)}|$, it is enough to show $n_1 = n_2$. Without loss of generality, suppose that $n_1 > n_2$. From (24), we can obtain

$$\begin{bmatrix} x_0 - x_0 \\ x_1 - x_0 \\ \vdots \\ x_{n_1-1} - x_0 \end{bmatrix} \times M_G^{(i+1)} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{26}$$

Note that n_1 vectors $x_i - x_0$ are all distinct. By adding y_0 to each row of the first matrix in LHS of (26), we obtain

$$\begin{bmatrix} y_0 + x_0 - x_0 \\ y_0 + x_1 - x_0 \\ \vdots \\ y_0 + x_{n_1-1} - x_0 \end{bmatrix} \times M_G^{(i+1)} = \begin{bmatrix} y \\ y \\ \vdots \\ y \end{bmatrix}. \tag{27}$$

Note that n_1 vectors $y_0 + x_i - x_0$ are still all distinct and they are valid codewords. According to (27), the number of codewords which have y as the GFFT value with respect to α^i is n_1 , which is a contradiction to the assumption $n_1 > n_2$ and hence $n_1 = n_2$. Therefore, if GFFT is performed on all the codewords of $BCH_q(n, k)$ with respect to α^i , all the elements of $S_{c(\alpha^i)}$ occur uniformly at random for the random message $m(x)$, which implies $\Pr(c(\alpha^i) = x) = 1/|S_{c(\alpha^i)}|$ for any $i \in S_r^c$. \square

By Lemma 2, it is clear that $c(\alpha^i) = 0$ for $i \in S_r$ and $c(\alpha^i)$ for $i \in S_r^c$ takes a value from $S_{c(\alpha^i)}$ uniformly at random. In the next subsection, the distribution of GFFT values of $r(x)$ is analyzed.

3.3. GFFT of Received Codewords

Consider a received codeword $r(x) = c(x) + e(x)$ having a single symbol error, i.e., $e(x) = e_j x^j$ with $e_j \neq 0$. Let $S_{e(\alpha^i)}$ be the set of all GFFT values of a single symbol error $e(x)$ with respect to α^i as follows:

$$S_{e(\alpha^i)} \triangleq \{e(\alpha^i) \mid e(x) = e_j x^j, e_j \in GF^*(q), j \in \{0, 1, \dots, n - 1\}\}. \tag{28}$$

By using Lemma 2, the distribution of GFFT values of $r(x)$ with a single symbol error is analyzed as follows.

Corollary 1. Suppose that a message $m(x)$ is generated uniformly at random, a codeword $c(x)$ of $BCH_q(n, k)$ is encoded by $g(x)$ as (3), $e(x)$ is a single symbol error, and $k \geq rk(\alpha^i)$. Then, it is satisfied that

$$S_{e(\alpha^i)} \subset S_{c(\alpha^i)}, \forall i \in S_r^c. \tag{29}$$

Proof. By Lemma 2, if $k \geq rk(\alpha^i)$, it is clear that $|S_{c(\alpha^i)}| = q^{rk(\alpha^i)}$ for $i \in S_r^c$, which means that $S_{c(\alpha^i)}$ contains all the linear combinations of $(\alpha^i)^0, (\alpha^i)^1, \dots, (\alpha^i)^{n-1}$ over $GF(q)$. Therefore, $S_{c(\alpha^i)}$ contains $S_{e(\alpha^i)}$ for any $i \in S_r^c$ and (29) holds. \square

Let $S_{r(\alpha^i)}$ be the set of all GFFT values of $r(x)$ with a single symbol error $e_j x^j$ with respect to α^i as follows:

$$S_{r(\alpha^i)} \triangleq \{r(\alpha^i) \mid r(x) = c(x) + e_j x^j, e_j \in GF^*(q), c(x) \in BCH_q(n, k), j \in \{0, 1, \dots, n-1\}\}. \tag{30}$$

Lemma 3. Suppose that a message $m(x)$ is generated uniformly at random, a codeword $c(x)$ of $BCH_q(n, k)$ is encoded by $g(x)$ as (3), $e(x)$ is a single symbol error, and $k \geq rk(\alpha^i)$. Then, it is satisfied that

$$S_{r(\alpha^i)} = S_{c(\alpha^i)}, \forall i \in S_r^c, \tag{31}$$

$$\Pr(r(\alpha^i) = x) = \frac{1}{q^{rk(\alpha^i)}}, \forall x \in S_{r(\alpha^i)}, \forall i \in S_r^c. \tag{32}$$

Proof. Based on (30), $S_{r(\alpha^i)}$ can be expressed as follows:

$$S_{r(\alpha^i)} = \{c(\alpha^i) + e(\alpha^i) \mid c(\alpha^i) \in S_{c(\alpha^i)}, e(\alpha^i) \in S_{e(\alpha^i)}\}. \tag{33}$$

As shown in Corollary 1, if $e(x)$ is a single symbol error and $k \geq rk(\alpha^i)$, $S_{e(\alpha^i)} \subset S_{c(\alpha^i)}$ for any $i \in S_r^c$. Therefore, $S_{r(\alpha^i)}$ is equal to $S_{c(\alpha^i)}$ for any $i \in S_r^c$.

The probability in (32) is derived as follows:

$$\begin{aligned} \Pr(r(\alpha^i) = x) &= \Pr(c(\alpha^i) + e(\alpha^i) = x) \\ &= \sum_{y \in S_{e(\alpha^i)}} \Pr(c(\alpha^i) = x - y) \Pr(e(\alpha^i) = y) \\ &\stackrel{(a)}{=} \frac{1}{|S_{c(\alpha^i)}|} \sum_{y \in S_{e(\alpha^i)}} \Pr(e(\alpha^i) = y) \\ &= \frac{1}{|S_{c(\alpha^i)}|} \\ &= \frac{1}{q^{rk(\alpha^i)}} \end{aligned} \tag{34}$$

for $x \in S_{r(\alpha^i)}$ and $i \in S_r^c$. The equality (a) holds by Lemma 2. \square

Lemma 3 assumes $wt(e) = 1$, however, in practice, multiple errors also occur. If $wt(e) > 1$, Lemma 1 does not hold because $r(\alpha^i)$ can be 0 for some $i \in S_r$ even though $e(x) \neq 0$. Note that $\Pr(e(\alpha^i) = 0, e(x) \neq 0, i \in S_r)$ is equal to the undetectable error probability of the BCH code which has $\{\alpha^i \mid i \in S_r\}$ as its null spectrum.

Lemma 4. Suppose that a message $m(x)$ is generated uniformly at random, a codeword $c(x)$ of $BCH_q(n, k)$ is encoded by $g(x)$ as (3), $e(x)$ is generated by q -ary symmetric channel with error probability ϵ , and $k \geq rk(\alpha^i)$. Then, it is satisfied that

$$S_{r(\alpha^i)} = S_{c(\alpha^i)}, \forall i \in S_r^c, \tag{35}$$

$$\Pr(r(\alpha^i) = x) = \frac{1}{q^{rk(\alpha^i)}}, \forall x \in S_{r(\alpha^i)}, \forall i \in S_r^c. \tag{36}$$

Proof. For $i \in S_r^c$, $S_{c(\alpha^i)}$ contains all the linear combinations of $(\alpha^i)^0, (\alpha^i)^1, \dots, (\alpha^i)^{n-1}$ over $GF(q)$. Since the error $e(x)$ is not a single symbol error anymore, $S_{e(\alpha^i)}$ is defined as follows:

$$S_{e(\alpha^i)} = \left\{ e(\alpha^i) \mid e(x) = \sum_{j=0}^{n-1} e_j x^j, e_j \in GF(q) \right\}. \tag{37}$$

$S_{e(\alpha^i)}$ also contains all the linear combinations of $(\alpha^i)^0, (\alpha^i)^1, \dots, (\alpha^i)^{n-1}$ over $GF(q)$ and hence $S_{r(\alpha^i)} = S_{c(\alpha^i)}$ for any $i \in S_r^c$ because $r(\alpha^i) = c(\alpha^i) + e(\alpha^i)$.

The probability in (36) is derived as follows:

$$\begin{aligned} & \Pr(r(\alpha^i) = x) \\ &= \Pr(c(\alpha^i) + e(\alpha^i) = x) \\ &= \sum_{y \in S_{e(\alpha^i)}} \Pr(c(\alpha^i) = x - y) \Pr(e(\alpha^i) = y) \\ &= \frac{1}{|S_{c(\alpha^i)}|} \sum_{y \in S_{e(\alpha^i)}} \Pr(e(\alpha^i) = y) \\ &= \frac{1}{|S_{c(\alpha^i)}|} \\ &= \frac{1}{q^{rk(\alpha^i)}} \end{aligned} \tag{38}$$

for $x \in S_{r(\alpha^i)}$ and $i \in S_r^c$. □

As you can see from Lemmas 3 and 4, the conclusions (31) and (32) and (35) and (36) are the same. It implies that if the encoded message $m(x)$ is generated uniformly at random, the GFFT of $r(x)$ with respect to α^i takes a value in $S_{r(\alpha^i)}$ uniformly at random regardless of the distribution of $e(x)$ for $i \in S_r^c$. By Lemma 4, the probability that $r(x)$ has α^i as its root for $i \in S_r^c$ is $1/q^{rk(\alpha^i)}$. Based on Lemma 4, the performance of blind reconstruction method of BCH codes [15] is analyzed in the next section.

4. Analysis of Blind Reconstruction Method of BCH Codes

4.1. Blind Reconstruction Method of BCH Codes

In this subsection, the blind reconstruction method of BCH codes based on consecutive roots of generator polynomials [15] is described. In order to perform this method, it is assumed that the codeword synchronization is perfectly done and the code length n is known to the receiver. Suppose that M codewords are received. The j -th received codeword is expressed in polynomial form as $r_j(x) = r_{j,0} + r_{j,1}x + \dots + r_{j,n-1}x^{n-1}$ and in vector form as $\mathbf{r}_j = (r_{j,0}, r_{j,1}, \dots, r_{j,n-1})$ for $j \in \{1, 2, \dots, M\}$. Let L_j denote the set of pairs consisting of the length l of the consecutive roots and the starting value s of these consecutive roots of $r_j(x)$ defined as follows:

$$L_j \triangleq \left\{ (s, l) \mid s \in \{1, 2, \dots, n-1\}, 2 \leq l \in \mathbb{N}, r_j(\alpha^i) = 0, \forall i \in \mathcal{C}_s^l \right\}, \tag{39}$$

where $\mathcal{C}_s^l \triangleq \cup_{i=s}^{s+l-1} \mathcal{C}_i$. For example, if $\mathbf{r}_j = (0, 0, 1, 0, 1, 1, 0)$ is received, then the GFFT of \mathbf{r}_j is $\mathbf{R}_j = (1, 0, 0, 1, 0, 1, 1)$, and therefore $L_j = \{(5, 2)\}$. Note that $0 < s < n$ and $2 \leq l$ of the elements in L_j . By using (39), for $r_j(x)$, the maximum length of consecutive roots (MLCR) l_j^{max} and the corresponding starting value of consecutive roots (SVCR) s_j^{max} are obtained as follows:

$$(s_j^{max}, l_j^{max}) = \arg \max_{(s_j, l_j) \in L_j} l_j. \tag{40}$$

Let S_{max} denote the set of (s_j^{max}, l_j^{max}) for $j \in \{1, 2, \dots, M\}$ as follows:

$$S_{max} \triangleq \{(s_j^{max}, l_j^{max}) \mid j \in \{1, 2, \dots, M\}\} \tag{41}$$

The blind reconstruction method of BCH codes in [15] has two-stage processes.

1. First stage: The most frequent s_j^{max} in S_{max} is selected and called a reference SVCR (R-SVCR), denoted as s_{ref} .
2. Second stage: The most frequent l_j^{max} among the pairs having $s_j^{max} = s_{ref}$ in S_{max} is selected and called a reference MLCR (R-MLCR), denoted as l_{ref} .

By setting $b = s_{ref}$ and $d = l_{ref} + 1$ in (1), the generator polynomial of the used BCH code is reconstructed.

4.2. Performance Analysis of Blind Reconstruction Method of BCH Codes

In this subsection, the performance of blind reconstruction method in [15] is analyzed. Suppose that $BCH_q(n, k)$ is used and M codewords are received. The generator polynomial $g_0(x)$ is set as in (1) with $b = s_0$ and $d = l_0 + 1$. In order to succeed in blind reconstruction of this BCH code, s_{ref} and l_{ref} should be correctly determined as $s_{ref} = s_0$ and $l_{ref} = l_0$. Define the sets of received codewords, $M(s, l)$, $M^m(s, l)$, $M^*(s, l)$, and $M^e(s, l)$ as follows:

$$M(s, l) = \{r_j(x) \mid (s, l) \in L_j\}, \tag{42}$$

$$M^m(s, l) = \{r_j(x) \mid (s_j^{max}, l_j^{max}) = (s, l)\}, \tag{43}$$

$$M^*(s, l) = \left\{ r_j(x) \mid r_j(x) \in M^m(s, l), r_j(\alpha^i) \neq 0, \forall i \in \{1, 2, \dots, n-1\} \setminus \mathcal{C}_s^l \right\}, \tag{44}$$

$$M^e(s, l) = \{r_j(x) \mid e_j(x) \neq 0, r_j(x) \in M(s, l)\}. \tag{45}$$

Note that $M^*(s, l) \subseteq M^m(s, l) \subseteq M(s, l)$. In order to succeed in the first stage of the blind reconstruction method, the following relation should be satisfied,

$$\sum_{l=2}^{n-1} |M^m(s_0, l)| > \sum_{l=2}^{n-1} |M^m(s, l)|, \forall s \neq s_0. \tag{46}$$

The relation (46) can be simplified as in the following Lemma 5.

Lemma 5. *If the following inequality is satisfied, then the first stage of the blind reconstruction of BCH codes in [15] always succeeds,*

$$|M^*(s_0, l_0)| > |M(s, 2)|, \forall s \neq s_0, \tag{47}$$

and the success probability of the first stage is lower-bounded as

$$\Pr \left(\sum_{l=2}^{n-1} |M^m(s_0, l)| > \sum_{l=2}^{n-1} |M^m(s, l)|, \forall s \neq s_0 \right) \geq \Pr \left(|M^*(s_0, l_0)| > |M(s, 2)|, \forall s \neq s_0 \right). \tag{48}$$

Proof. In order to succeed in the first stage of the blind reconstruction method in [15], the relation (46) should be satisfied. The LHS in (46) satisfies the following inequalities,

$$\begin{aligned} \sum_{l=2}^{n-1} |M^m(s_0, l)| &\stackrel{(a)}{\geq} \sum_{l=2}^{n-1} |M^*(s_0, l)| \\ &\stackrel{(b)}{\geq} |M^*(s_0, l_0)|. \end{aligned} \tag{49}$$

The first inequality (a) is derived by using $M^*(s_0, l) \subseteq M^m(s_0, l)$, and the second inequality (b) is trivial. The RHS in (46) satisfies the following inequality,

$$\begin{aligned} \sum_{l=2}^{n-1} |M^m(s, l)| &\stackrel{(a)}{=} \left| \bigcup_{l=2}^{n-1} M^m(s, l) \right| \\ &\stackrel{(b)}{\leq} \left| \bigcup_{l=2}^{n-1} M(s, l) \right| \\ &\stackrel{(c)}{=} |M(s, 2)|. \end{aligned} \tag{50}$$

The first equality (a) in (50) is derived by using $M^m(s, l) \cap M^m(s, l') = \emptyset$ for all $l \neq l'$. The second inequality (b) is derived by using $M^m(s, l) \subseteq M(s, l)$. The third equality (c) is derived by using $M(s, l') \subseteq M(s, l)$ for all $l' > l$.

Therefore, if $|M^*(s_0, l_0)| > |M(s, 2)|$ for any $s \neq s_0$, the first stage of the blind reconstruction method of BCH codes in [15] always succeeds. Furthermore, by the Equations (49) and (50), the inequality (48) clearly holds. \square

If the first stage succeeds, in order for the second stage to succeed, the following relation should be satisfied,

$$|M^m(s_0, l_0)| > |M^m(s_0, l)|, \forall l \neq l_0. \tag{51}$$

The relation (51) can be simplified as in the following Lemma 6.

Lemma 6. *If $|M^*(s_0, l_0)| > |M(s, 2)|, \forall s \neq s_0$, holds and the following inequality is satisfied, then the second stage of the blind reconstruction of BCH codes in [15] always succeeds,*

$$|M^*(s_0, l_0)| > |M^e(s_0, 2)|, \tag{52}$$

and the success probability of the second stage is lower-bounded as

$$\Pr \left(|M^m(s_0, l_0)| > |M^m(s_0, l)|, \forall l \neq l_0 \right) \geq \Pr \left(|M^*(s_0, l_0)| > |M^e(s_0, 2)| \right), \tag{53}$$

where, for better readability, the given condition that $|M^*(s_0, l_0)| > |M(s, 2)|, \forall s \neq s_0$, is omitted in the probability.

Proof. Since $|M^*(s_0, l_0)| > |M(s, 2)|$ for any $s \neq s_0$, $|M^m(s_0, l_0)| > |M^m(s_0, l)|$ holds for $l > l_0$ as follows:

$$\begin{aligned} |M^m(s_0, l)| &\stackrel{(a)}{\leq} |M(s_0 + 1, l - 1)| \\ &\stackrel{(b)}{<} |M^*(s_0, l_0)| \\ &\stackrel{(c)}{\leq} |M^m(s_0, l_0)|. \end{aligned} \tag{54}$$

The inequality (a) in (54) is derived by using $M^m(s_0, l) \subseteq M(s_0 + 1, l - 1)$. The inequality (b) is derived by using $|M^*(s_0, l_0)| > |M(s, 2)|$ for $s \neq s_0$ and $|M(s_0 + 1, 2)| \geq |M(s_0 + 1, l - 1)|$. The inequality (c) is derived by using $M^*(s_0, l_0) \subseteq M^m(s_0, l_0)$. Therefore, it remains to prove that our assumption implies $|M^m(s_0, l_0)| > |M^m(s_0, l)|$ for $l < l_0$.

If the j -th received codeword $r_j(x)$ is error-free (i.e., $e_j(x) = 0$), then $r_j(x) \notin M^m(s_0, l)$ for all $l < l_0$ because $r_j(x) \in M(s_0, l_0)$ always holds. Therefore, $e_j(x) \neq 0$ for $r_j(x) \in M^m(s_0, l), l < l_0$ and then, the relation (51) can be simplified as $|M^m(s_0, l_0)| > |M^m(s_0, l) \cap \{r_j(x) \mid e_j(x) \neq 0\}|$ for $l < l_0$. Since it is always satisfied that $|M^m(s_0, l) \cap \{r_j(x) \mid e_j(x) \neq 0\}| \leq |M(s_0, l) \cap \{r_j(x) \mid$

$e_j(x) \neq 0\}$ $= |M^e(s_0, l)|$, if $|M^m(s_0, l_0)| > |M^e(s_0, l)|$ for $l < l_0$, the second stage succeeds. Furthermore, since $|M^e(s_0, l)| > |M^e(s_0, l')|$ for $l < l'$, if $|M^m(s_0, l_0)| > |M^e(s_0, 2)|$ is satisfied, then the second stage also succeeds. Note that the LHS in (51) satisfies that $|M^m(s_0, l_0)| \geq |M^*(s_0, l_0)|$. Therefore, if $|M^*(s_0, l_0)| \geq |M^e(s_0, 2)|$ is satisfied, then the second stage always succeeds.

The lower-bound on the success probability of the second stage is derived as follows:

$$\begin{aligned}
 & \Pr \left(|M^m(s_0, l_0)| > |M^m(s_0, l)|, \forall l \neq l_0 \right) \\
 &= \Pr \left(|M^m(s_0, l_0)| > |M^m(s_0, l)|, \forall l \leq l_0 \right) \\
 &= \Pr \left(|M^m(s_0, l_0)| > |M^m(s_0, l) \cap \{r_j(x) \mid e_j(x) \neq 0\}|, \forall l \leq l_0 \right) \\
 &\geq \Pr \left(|M^m(s_0, l_0)| > |M(s_0, l) \cap \{r_j(x) \mid e_j(x) \neq 0\}|, \forall l \leq l_0 \right) \tag{55} \\
 &= \Pr \left(|M^m(s_0, l_0)| > |M^e(s_0, l)|, \forall l \leq l_0 \right) \\
 &= \Pr \left(|M^m(s_0, l_0)| > |M^e(s_0, 2)| \right) \\
 &\geq \Pr \left(|M^*(s_0, l_0)| > |M^e(s_0, 2)| \right).
 \end{aligned}$$

Note that, for better readability, the given condition that $|M^*(s_0, l_0)| > |M(s, 2)|, \forall s \neq s_0$, is omitted in the probability. \square

By Lemmas 5 and 6, if $|M^*(s_0, l_0)| > \max_{s \neq s_0} |M(s, 2)|$ and $|M^*(s_0, l_0)| > |M^e(s_0, 2)|$, then the blind reconstruction method of BCH code in [15] always succeeds. Moreover, the success probability of the blind reconstruction method of BCH code in [15] is lower-bounded, as in the following Theorem 1.

Theorem 1. Suppose that randomly generated M codewords of $BCH_q(n, k)$, which uses the generator polynomial $g(x)$ as in (1) with $b = s_0$ and $d = l_0 + 1$, are received after passing through q -ary symmetric channel with error probability ϵ . Then, the success probability of the blind reconstruction method of BCH codes in [15], denoted as P_s , is lower-bounded as follows:

$$P_s \geq \sum_{x=1}^M B(M, x, p_0) \prod_{C_i \subseteq C_{s_0}^{l_0^c}} \left\{ \sum_{y=0}^{x-1} B \left(M, y, \frac{1}{q^{rk(\alpha^i)}} \right) \right\} \prod_{C_j \subseteq C_{s_0}^{l_0^c}} \left\{ \sum_{y=0}^{x-1} B \left(M, y, P_{ue}(C_j) \right) \right\}, \tag{56}$$

where $B(M, x, p) = \binom{M}{x} p^x (1-p)^{M-x}$, $p_0 = \{(1-\epsilon)^n + P_{ue}(C_{s_0}^{l_0})\} \prod_{z \in C_{s_0}^{l_0^c}} (1 - 1/q^{rk(\alpha^z)})$, $C_{s_0}^{l_0^c} = \{1, 2, \dots, n-1\} \setminus C_{s_0}^{l_0}$, and $P_{ue}(C)$ is the undetectable error probability of BCH code having $\{\alpha^i \mid i \in C\}$ as its null spectrum.

Proof. By Lemmas 5 and 6, if $|M^*(s_0, l_0)| > \max_{s \neq s_0} |M(s, 2)|$ and $|M^*(s_0, l_0)| > |M^e(s_0, 2)|$, then the blind reconstruction of BCH codes in [15] always succeeds. In order to calculate the probability that $|M^*(s_0, l_0)| > \max_{s \neq s_0} |M(s, 2)|$ and $|M^*(s_0, l_0)| > |M^e(s_0, 2)|$, the probabilities that $r_j(x) \in M^*(s_0, l_0)$, $r_j(x) \in M(s, 2)$, and $r_j(x) \in M^e(s_0, 2)$ should be calculated, respectively.

If the j -th received codeword $r_j(x)$ is error-free or has an undetectable error, it is always true that $r_j(x) \in M(s_0, l_0)$. Furthermore, if $r_j(\alpha^i) \neq 0$ for $i \in \mathcal{C}_{s_0}^{l_0^c}$, it is also true that $r_j(x) \in M^*(s_0, l_0)$, where $\mathcal{C}_{s_0}^{l_0^c} = \{1, 2, \dots, n - 1\} \setminus \mathcal{C}_{s_0}^{l_0}$. Then, $\Pr(r_j(x) \in M^*(s_0, l_0))$ is derived as follows:

$$\begin{aligned} \Pr(r_j(x) \in M^*(s_0, l_0)) &= \Pr(r_j(\alpha^i) = 0, \forall i \in \mathcal{C}_{s_0}^{l_0}, r_j(\alpha^z) \neq 0, \forall z \in \mathcal{C}_{s_0}^{l_0^c}) \\ &\stackrel{(a)}{=} \Pr(r_j(\alpha^i) = 0, \forall i \in \mathcal{C}_{s_0}^{l_0}) \prod_{z \in \mathcal{C}_{s_0}^{l_0^c}} \Pr(r_j(\alpha^z) \neq 0) \\ &\stackrel{(b)}{=} \{(1 - \epsilon)^n + P_{ue}(\mathcal{C}_{s_0}^{l_0})\} \prod_{z \in \mathcal{C}_{s_0}^{l_0^c}} \left(1 - \frac{1}{q^{rk(\alpha^z)}}\right) \\ &\triangleq p_0, \end{aligned} \tag{57}$$

where $P_{ue}(\mathcal{C}_{s_0}^{l_0})$ is the undetectable error probability of BCH code having $\{\alpha^i \mid i \in \mathcal{C}_{s_0}^{l_0}\}$ as its null spectrum. In the equality (a) in (57), $r_j(\alpha^i)$ for $i \in \mathcal{C}_{s_0}^{l_0}$ occurs uniformly at random because the message is generated uniformly at random. Therefore, the event that $r_j(\alpha^i) = 0$ for any $i \in \mathcal{C}_{s_0}^{l_0}$ and the event that $r_j(\alpha^z) = 0$ for any $z \in \mathcal{C}_{s_0}^{l_0^c}$ are independent and hence the equality (a) holds. The equality (b) is derived by using $\Pr(r_j(\alpha^i) = 0, \forall i \in \mathcal{C}_{s_0}^{l_0}) = \{(1 - \epsilon)^n + P_{ue}(\mathcal{C}_{s_0}^{l_0})\}$ and Lemma 4.

The probability that $r_j(x) \in M(s, 2)$ for $s \neq s_0$ is calculated by using Lemma 4 as follows:

$$\begin{aligned} \Pr(r_j(x) \in M(s, 2)) &= \Pr(r_j(\alpha^i) = 0, \forall i \in \mathcal{C}_s^2) \\ &= \Pr(r_j(\alpha^i) = 0, \forall i \in \mathcal{C}_s^2 \cap \mathcal{C}_{s_0}^{l_0}) \Pr(r_j(\alpha^z) = 0, \forall z \in \mathcal{C}_s^2 \setminus \mathcal{C}_{s_0}^{l_0}) \\ &= \Pr(r_j(\alpha^i) = 0, \forall i \in \mathcal{C}_s^2 \cap \mathcal{C}_{s_0}^{l_0}) \prod_{z \in \mathcal{C}_s^2 \setminus \mathcal{C}_{s_0}^{l_0}} \Pr(r_j(\alpha^z) = 0) \\ &= P_{ue}(\mathcal{C}_s^2 \cap \mathcal{C}_{s_0}^{l_0}) \prod_{z \in \mathcal{C}_s^2 \setminus \mathcal{C}_{s_0}^{l_0}} \frac{1}{q^{rk(\alpha^z)}}. \end{aligned} \tag{58}$$

For better readability, $s \neq s_0$ is omitted in the probability.

Let $M_1(\mathcal{C}_i)$ be $\{r_j(x) \mid r_j(\alpha^z) = 0, \forall z \in \mathcal{C}_i\}$ and $M_2(\mathcal{C}_i)$ be $\{r_j(x) \mid r_j(\alpha^z) = c_j(\alpha^z) + e_j(\alpha^z) = 0, \forall z \in \mathcal{C}_i, e_j(x) \neq 0\}$. If $|M^*(s_0, l_0)|$ is greater than $|M_1(\mathcal{C}_i)|$ for any $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0^c}$ and also greater than $|M_2(\mathcal{C}_i)|$ for any $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0}$, it is also satisfied that $|M^*(s_0, l_0)| > |M(s, 2)|$ for any $s \neq s_0$. It is because if there exists $\mathcal{C}_i \subseteq \mathcal{C}_s^2$ such that $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0^c}$, it is true that $|M^*(s_0, l_0)| > |M(s, 2)|$ due to $|M^*(s_0, l_0)| > |M_1(\mathcal{C}_i)| \geq |M(s, 2)|$ for any $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0^c}$. Furthermore, if there exists $\mathcal{C}_i \subseteq \mathcal{C}_s^2$ such that $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0}$, then it is also true that $|M^*(s_0, l_0)| > |M(s, 2)|$ due to $|M^*(s_0, l_0)| > |M_2(\mathcal{C}_i)| \geq |M(s, 2)|$ for any $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0}$. Then, the condition for the success of the first stage of blind reconstruction method is simplified as follows:

$$|M^*(s_0, l_0)| > |M_1(\mathcal{C}_i)|, |M^*(s_0, l_0)| > |M_2(\mathcal{C}_j)|, \forall \mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0^c}, \forall \mathcal{C}_j \subseteq \mathcal{C}_{s_0}^{l_0}. \tag{59}$$

Moreover, $\Pr(r_j(\alpha^z) = 0, \forall z \in \mathcal{C}_i)$ for $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0^c}$ is simplified as follows:

$$\begin{aligned} \Pr\left(r_j(\alpha^z) = 0, \forall z \in \mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0^c}\right) &= \Pr\left(r_j(x) \in M(i, 1), \mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0^c}\right) \\ &\stackrel{(a)}{=} P_{ue}(\mathcal{C}_i \cap \mathcal{C}_{s_0}^{l_0}) \prod_{\mathcal{C}_j \subseteq \mathcal{C}_i \setminus \mathcal{C}_{s_0}^{l_0}} \frac{1}{q^{rk(\alpha^j)}} \\ &\stackrel{(b)}{=} \frac{1}{q^{rk(\alpha^i)}}. \end{aligned} \tag{60}$$

The equality (a) is derived by using (58) and (b) is derived by using $\mathcal{C}_i \cap \mathcal{C}_{s_0}^{l_0} = \emptyset$ and $\mathcal{C}_i \setminus \mathcal{C}_{s_0}^{l_0} = \mathcal{C}_i$. Furthermore, $\Pr(r_j(\alpha^z) = 0, \forall z \in \mathcal{C}_i, e_j(x) \neq 0)$ for $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0}$, is also simplified as follows:

$$\begin{aligned} \Pr\left(r_j(\alpha^z) = 0, \forall z \in \mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0}, e_j(x) \neq 0\right) &= \Pr\left(r_j(x) \in M(i, 1), \mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0}\right) \\ &= P_{ue}(\mathcal{C}_i \cap \mathcal{C}_{s_0}^{l_0}) \prod_{\mathcal{C}_j \subseteq \mathcal{C}_i \setminus \mathcal{C}_{s_0}^{l_0}} \frac{1}{q^{rk(\alpha^j)}} \\ &\stackrel{(a)}{=} P_{ue}(\mathcal{C}_i). \end{aligned} \tag{61}$$

The equality (a) is derived by using $\mathcal{C}_i \cap \mathcal{C}_{s_0}^{l_0} = \mathcal{C}_i$ and $\mathcal{C}_i \setminus \mathcal{C}_{s_0}^{l_0} = \emptyset$

The probability that $r_j(x) \in M^e(s_0, 2)$ is the same as the undetectable error probability of a BCH code having $\{\alpha^i \mid i \in \mathcal{C}_{s_0}^2\}$ as its null spectrum as follows:

$$\Pr\left(r_j(x) \in M^e(s_0, 2)\right) = P_{ue}(\mathcal{C}_{s_0}^2). \tag{62}$$

If $|M^*(s_0, l_0)| > |M_2(\mathcal{C}_i)|$ for $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^2$, then the second stage of the blind reconstruction method succeeds. Therefore, $\Pr(|M^*(s_0, l_0)| > |M^e(s_0, 2)|) \geq \Pr(|M^*(s_0, l_0)| > |M_2(\mathcal{C}_i)|)$ for $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^2$.

Finally, by using (57)–(62), P_s is lower-bounded as

$$\begin{aligned} P_s &\geq \Pr\left(|M^*(s_0, l_0)| > \max_{s \neq s_0} |M(s, 2)|, |M^*(s_0, l_0)| > |M^e(s_0, 2)|\right) \\ &= \sum_{x=1}^M \Pr\left(|M^*(s_0, l_0)| = x\right) \Pr\left(\max_{s \neq s_0} |M(s, 2)| < x, |M^e(s_0, 2)| < x \mid |M^*(s_0, l_0)| = x\right) \\ &\stackrel{(a)}{\geq} \sum_{x=1}^M \Pr\left(|M^*(s_0, l_0)| = x\right) \prod_{\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0^c}} \Pr\left(|M_1(\mathcal{C}_i)| < x\right) \prod_{\mathcal{C}_j \subseteq \mathcal{C}_{s_0}^{l_0}} \Pr\left(|M_2(\mathcal{C}_j)| < x\right) \\ &= \sum_{x=1}^M B(M, x, p_0) \prod_{\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0^c}} \left\{ \sum_{y=0}^{x-1} B\left(M, y, \frac{1}{q^{rk(\alpha^i)}}\right) \right\} \prod_{\mathcal{C}_j \subseteq \mathcal{C}_{s_0}^{l_0}} \left\{ \sum_{y=0}^{x-1} B\left(M, y, P_{ue}(\mathcal{C}_j)\right) \right\}. \end{aligned} \tag{63}$$

The inequality (a) in (63) is derived by using $\Pr(|M^*(s_0, l_0)| > |M^e(s_0, 2)|) \geq \Pr(|M^*(s_0, l_0)| > |M_2(\mathcal{C}_i)|)$ for $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^2$. Note that the event of $|M_z(\mathcal{C}_i)| < x$ is independent with the event of $|M_z(\mathcal{C}_j)| < x$ for $i \neq j$ and $z \in \{1, 2\}$ because $\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$ for $i \neq j$. Furthermore, the event of $|M_1(\mathcal{C}_i)| < x$ and the event of $|M_2(\mathcal{C}_j)| < x$ for $i \neq j$ are also independent because $\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$ for $i \neq j$. \square

In Theorem 1, a lower-bound on the success probability of the blind reconstruction method of BCH codes in [15] is obtained. In order to confirm the validity of this lower-bound, simulations are performed by using the following BCH codes.

- $BCH_2(31, 21)$, $BCH_2(63, 51)$, $BCH_2(127, 113)$: These are binary BCH codes having $\{\alpha^i \mid i \in \mathcal{C}_1^4\}$ as their null spectrum.
- $BCH_{32}(31, 29)$, $BCH_{64}(63, 59)$: These are Reed–Solomon (RS) codes having $\{\alpha^i \mid i \in \mathcal{C}_1^4\}$ as their null spectrum.

As you can see from Figure 1, the success probability of the blind reconstruction of binary BCH codes is well bounded by the lower-bound in (56). However, for $BCH_2(63, 51)$, the gap between the simulation result and the lower-bound is larger than the others because $BCH_2(63, 51)$ has a cyclotomic coset of cardinality 2, while all the cyclotomic cosets of $BCH_2(31, 21)$ and $BCH_2(127, 113)$ have the cardinality 5 and 7, respectively. In (56), if a cyclotomic coset $\mathcal{C}_i \subseteq \mathcal{C}_{s_0}^{l_0^c}$ has small cardinality, $1/q^{rk(\alpha^i)}$ becomes bigger and then, $B(M, y, 1/q^{rk(\alpha^i)})$ becomes smaller. Therefore, the lower-bounds of the blind reconstruction performance of $BCH_2(31, 21)$ and $BCH_2(127, 113)$ is much tighter than $BCH_2(63, 51)$.

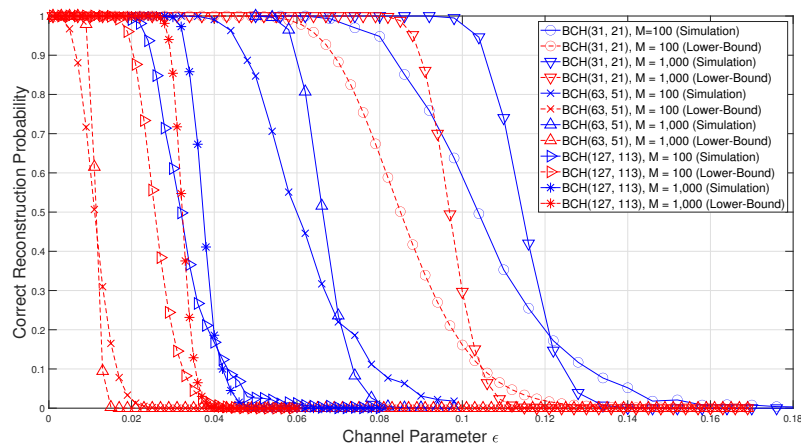


Figure 1. Comparison of the correct reconstruction probability with the proposed lower-bound for binary Bose–Chaudhuri–Hocquenghem (BCH) codes.

As you can see from Figure 2, the success probability of the blind reconstruction of RS codes is also well bounded by the lower-bound in (56). Moreover, as the code length increase, the proposed lower-bound of RS codes becomes tighter and therefore this lower-bound can be a good estimation of blind reconstruction performance for practical RS codes. Furthermore, since the proposed lower-bound can estimate the blind reconstruction performance without the extensive simulation, the proposed lower-bound is suitable for practical use.

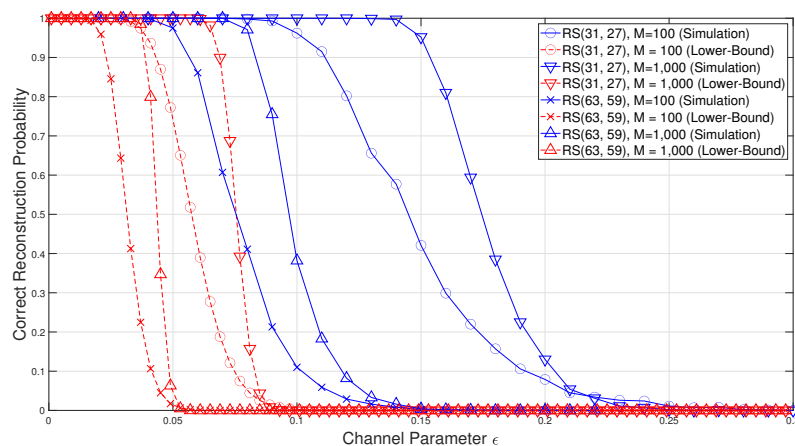


Figure 2. Comparison of the correct reconstruction probability with the proposed lower-bound for Reed–Solomon (RS) codes.

5. Conclusions

The blind reconstruction method of BCH codes in [15] shows the best performance, but the theoretical analysis of this method has not been performed. In this paper, by analyzing the properties of BCH codes on the aspects of blind reconstruction, a lower-bound on the success probability of the blind reconstruction method in [15] is derived. Especially, the distribution of GFFT values of the received codewords are analyzed and the blind reconstruction method is formalized based on the conjugacy classes. Furthermore, the analysis results can be applied not only to the binary BCH codes, but also to the non-binary BCH codes, including RS codes. By comparing the derived lower-bound with the simulation results, it is confirmed that the success probability of the blind reconstruction is well bounded by the proposed lower-bound.

Author Contributions: S.K. and D.-J.S. developed the main idea, conducted simulations and wrote the manuscript. S.K. played a leading role in the analysis and simulation and D.-J.S. played a leading role in fixing research direction and procedures. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the research fund of Signal Intelligence Research Center supervised by Defense Acquisition Program Administration and Agency for Defense Development of Korea.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References

1. Wicker, S. Error control coding for digital communication systems In *Error Control Systems for Digital Communication and Storage*; Prentice-Hall: Englewood Cliffs, NJ, USA, 1995; pp. 1–16.
2. Valembois, A. Detection and recognition of a binary linear code. *Discret. Appl. Math.* **2001**, *111*, 199–218. [[CrossRef](#)]
3. Cluzeau, M. Block code reconstruction using iterative decoding techniques. In Proceedings of the 2006 IEEE International Symposium on Information Theory (ISIT 2006), Seattle, DC, USA, 9–14 July 2006; pp. 2269–2273.
4. Burel, G.; Gautier, R. Blind estimation of encoder and interleaver characteristics in a non cooperative context. In Proceedings of the IASTED International Conference on Communications, Internet and Information Technology (CIIT 2003), Scottsdale, AZ, USA, 17–19 November 2003.
5. Moosavi, R.; Larsson, E. Fast blind recognition of channel codes. *IEEE Trans. Commun.* **2014**, *62*, 1393–1405. [[CrossRef](#)]
6. Chabot, C. Recognition of a code in a noisy environment. In Proceedings of the 2007 IEEE International Symposium on Information Theory (ISIT 2007), Nice, France, 24–29 June 2007; pp. 2211–2215.
7. Yardi, A.; Kumar, A.; Vijayakumaran, S. Channel-code detection by a third-party receiver via the likelihood ratio test. In Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT 2014), Honolulu, HI, USA, 24 June–4 July 2014; pp. 1051–1055.
8. Yardi, A.; Vijayakumaran, S.; Kumar, A. Blind reconstruction of binary cyclic codes. In Proceedings of the 20th European Wireless Conference, Barcelona, Spain, 14–16 May 2014; pp. 849–854.
9. Yardi, A.; Vijayakumaran, S.; Kumar, A. Blind reconstruction of binary cyclic codes from unsynchronized bitstream. *IEEE Trans. Commun.* **2016**, *64*, 2693–2706. [[CrossRef](#)]
10. Wu, G.; Zhang, B.; Wen, X.; Guo, D. Blind recognition of BCH code based on Galois field Fourier transform. In Proceedings of the 2015 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 15–17 October 2015; pp. 1–4.
11. Wang, J.; Yue, Y.; Yao, J. Statistical recognition method of binary BCH code. *Commun. Netw.* **2011**, *3*, 17–22. [[CrossRef](#)]
12. Jing, Z.; Zhiping, H. Blind recognition of binary BCH codes for cognitive radios. *Math. Probl. Eng.* **2016**, *2016*, 1–6.
13. Lee, H.; Park, C.; Lee, J.; Song, Y. Reconstruction of BCH codes using probability compensation. In Proceedings of the 18th Asia-Pacific Conference on Communications (APCC), Jeju, Korea, 15–17 October 2012; pp. 591–594.

14. Li, C.; Zhang, T.; Lin, Y. Blind recognition of RS codes based on Galois field columns Gaussian elimination. In Proceedings of the 7th International Congress on Image and Signal Processing, Dalian, China, 14–16 October 2014; pp. 836–841.
15. Jo, D.; Kwon, S.; Shin, D. Blind reconstruction of BCH codes based on consecutive roots of generator polynomials. *IEEE Commun. Lett.* **2018**, *22*, 894–897. [[CrossRef](#)]
16. Filiol, E. Reconstruction of convolutional encoders over GF(q). In *IMA International Conference on Cryptography and Coding*; Springer: Berlin/Heidelberg, Germany, 1997; Volume 1355, pp. 101–109. [[CrossRef](#)]
17. Lu, P.; Li, S.; Luo, X.; Zou, Y. Blind recognition of punctured convolutional codes. In Proceedings of the 2004 International Symposium on Information Theory (ISIT 2004), Chicago, IL, USA, 27 June–2 July 2004; p. 457.
18. Barbier, J. Reconstruction of turbo-code encoder. In *Digital Wireless Communications VII and Space Communication Technologies*; International Society for Optics and Photonics: Bellingham, WA, USA, 2005; pp. 463–473.
19. Marazin, M.; Gautier, R.; Burel, G. Blind recovery of k/n rate convolutional encoders in a noisy environment. *EURASIP J. Wirel. Commun. Netw.* **2011**, *2011*, 1–9. [[CrossRef](#)]
20. Yardi, A. Blind reconstruction of binary cyclic codes over binary erasure channel. In Proceedings of the 2018 International Symposium on Information Theory and Its Applications (ISITA), Singapore, 28–31 October 2018; pp. 301–305.

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).