IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 23, 2020, accepted November 9, 2020, date of publication November 16, 2020,
date of current version November 25, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3037799

Asymptotic Analysis of Blind Reconstruction of BCH Codes Based on Consecutive Roots of Generator Polynomials

MINKI SONG, (Member, IEEE), AND DONG-JOON SHIN, (Senior Member, IEEE)
Department of Electronic Engineering, Hanyang University, Seoul 04763, South Korea

Corresponding author: Dong-Joon Shin (djshin@hanyang.ac.kr)

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.

ABSTRACT In the military surveillance and security information systems, correct blind reconstruction of signal parameters from unknown signals is very important. Especially, many blind reconstruction methods of error-correcting codes have been proposed, and their theoretical performance analysis is essential for both the defender who wants to prevent information leakage and the challenger who wants to extract information from the intercepted signals. However, a proper performance analysis of most blind reconstruction methods has not been performed yet. Among many blind reconstruction methods of BCH codes proposed so far, the blind reconstruction method based on consecutive roots of generator polynomials proposed by Jo, Kwon, and Shin, called the JKS method, shows the best performance under the unknown channel information. However, the performance of the JKS method is only evaluated through simulation without performing theoretical analysis. In this paper, the JKS method is asymptotically analyzed under the binary symmetric channel with the cross-over probability p. Since the blind reconstruction performance heavily depends on how many and which received codewords are used even for the same channel environment, sufficiently many codewords are assumed to perform asymptotic analysis. More specifically, an asymptotic threshold on p, up to which blind reconstruction is successful, is derived when the number of received codewords is sufficiently large, which can be used as a new performance metric for blind reconstruction methods. Finally, the validity of the asymptotic analysis is confirmed through simulation.

INDEX TERMS Asymptotic analysis, BCH codes, blind reconstruction, consecutive roots, generator polynomial, military surveillance system, security information system.

I. INTRODUCTION

In the current digital communication systems, an error-correcting code (ECC) is essential to achieve reliable information communication [1]. By sharing the parameters of ECC at both transmitter and receiver, a receiver can correct channel errors. However, if the receiver does not know the parameters of ECC used by the transmitter, it is very hard for the receiver to communicate with the transmitter as well as to correct the errors in the received signals. In such a case, the receiver must blindly reconstruct the parameters of ECC to correctly recover the information from the received signals. Such blind reconstruction of ECCs is very important in various areas such as military surveillance and security information systems [2]–[5]. For these reasons, blind reconstruction of ECCs has been actively studied [2]–[15].

Especially, blind reconstruction of cyclic codes, one of the most widely used ECCs, has been investigated in many ways [2]–[9] and most of the proposed methods focus on recovering generator polynomials of cyclic codes. In [2], a blind reconstruction method of Bose-Chaudhuri-Hocquenghem (BCH) codes is proposed, which uses the property that t-error correcting BCH codewords are divisible by the generator polynomial having $2t$ consecutive roots, but there is a problem that random data polynomials can also be divisible by other minimal polynomial with non-negligible probability. To resolve this problem, a probability compensation is used in [2] to improve the blind

The associate editor coordinating the review of this manuscript and approving it for publication was Shadi Aljawarneh.

reconstruction performance. In [3], a generator polynomial of binary cyclic code of length n is reconstructed by deriving the syndrome distribution of the received codewords for all possible factors of $x^n - 1$. In more general situations, a codeword synchronization scheme for the received bitstream, in addition to a blind reconstruction of generator polynomial, is proposed in [4]. Even if the above-mentioned blind reconstruction methods show good performance, unfortunately, clear performance analysis has not been performed.

In [5], a blind reconstruction method of BCH codes based on Galois field Fourier transform (GFFT) is proposed for the first time. All the codeword polynomials of BCH code share the roots of generator polynomial and the roots of the received codeword polynomials can be easily verified by performing GFFT to them. Therefore, by checking the roots of the received codeword polynomials through GFFT, the method in [5] estimates the roots of generator polynomial. In [6], a blind reconstruction method of BCH codes is proposed, which uses the property that all the codeword polynomials of BCH code with the error-correcting capability t share the same $2t$ consecutive roots which are roots of generator polynomial. This blind reconstruction method in [6] is performed as follows. Initially, find the maximum length of consecutive roots (MLCR) and the corresponding starting value of consecutive roots (SVCR) for each of the received codeword polynomials. Then, the most frequent values of SVCR and MLCR are used to reconstruct the generator polynomials of BCH codes. Note that this blind reconstruction method in [6] outperforms the other blind reconstruction methods and does not even utilize channel information. However, the blind reconstruction performance of this blind reconstruction method has been evaluated only by simulation, and since theoretical performance analysis has not been performed, it is hard to estimate the exact performance or the performance limit for various cases. Therefore, such lack of analysis makes it difficult to properly apply this method to various systems such as military surveillance and security information systems.

It is clear that theoretical performance analysis of blind reconstruction methods is required for both a defender and a challenger. Specifically, a defender needs to guarantee security in communication and a challenger wants to blindly extract correct signal information with high probability. Moreover, without general performance analysis, very extensive simulation is required to confirm the performance of the blind reconstruction methods even for a limited situation. However, most of the blind reconstruction methods have not been theoretically analyzed and only a lower bound on the reconstruction performance was derived for the method in [9].

In this paper, we analyze the performance of the blind reconstruction method proposed by Jo, Kwon, and Shin [6], called the JKS method, which shows the best performance among the blind reconstruction methods of BCH codes. The analysis of the JKS method is asymptotically performed under the assumption that the number of received codewords is sufficiently large because the blind reconstruction performance heavily depends on how many and which received codewords are used even for the same channel environment. The blind reconstruction performance of the JKS method is estimated by calculating the probability that the correct generator polynomial of BCH code is reconstructed. Based on this asymptotic analysis, an asymptotic threshold on the cross-over probability of binary symmetric channel (BSC) is derived, up to which correct reconstruction of the generator polynomial of BCH code is guaranteed with probability 1. Since various blind reconstruction methods have been proposed without clear analysis [2], [3], [5], [6], [14], it is expected that an asymptotic analysis proposed in this paper can be applied to other methods for deriving their performance limit. Moreover, this asymptotic analysis will provide a new performance metric for blind reconstruction methods and will give intuition to the development of blind reconstruction method or the modification of existing methods.

The rest of the paper is organized as follows. In Section II, BCH codes and the JKS method are briefly introduced. In Section III, asymptotic analysis of the JKS method is performed. The simulation results in Section IV confirm that the asymptotic analysis of the JKS method is valid. Finally, conclusions are given in Section V.

II. PRELIMINARIES

A. BCH CODES

A BCH code of code length n, dimension k, and error-correcting capability t is denoted by BCH(n, k, t) and the Galois field of q elements is denoted by $GF(q)$. The generator polynomial $g(x)$ of BCH(n, k, t) over $GF(q)$ is defined as follows [1].

$$g(x) = LCM\left\{\phi_{\alpha^b}(x), \phi_{\alpha^{b+1}}(x), \cdots, \phi_{\alpha^{b+2t-1}}(x)\right\}, \quad (1)$$

where LCM is the least common multiple, α is a primitive n-th root of unity in $GF(q^m)$, and $\phi_{\alpha^i}(x)$, $0 < i \leq n$, is the minimal polynomial of α^i over $GF(q)$. Note that m is the smallest integer such that n divides $q^m - 1$, b is a positive integer, and $g(x)$ has $2t$ consecutive roots α^b, α^{b+1}, $\cdots$, and α^{b+2t-1}.

The BCH codeword polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ is generated by the product of $m(x) = m_0 + m_1x + \cdots + m_{k-1}x^{k-1}$ and $g(x)$, where $c_i,\ m_i \in GF(q)$. The received codeword polynomial $r(x) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1}$ is the sum of the BCH codeword polynomial $c(x)$ and the error polynomial $e(x) = e_0 + e_1x + \cdots + e_{n-1}x^{n-1}$, where $r_i,\ e_i \in GF(q)$.

B. JKS METHOD FOR BLIND RECONSTRUCTION OF BCH CODES

In the JKS method for blindly reconstructing the generator polynomials of BCH codes [6], it is assumed that the receiver knows the code length n and $GF(q)$ over which the BCH code is defined, and the receiver does not know the channel information. Also, the transmitter sequentially transmits BCH codewords, a perfect codeword synchronization is guaranteed

at the receiver, and M codewords are received through BSC with the cross-over probability $p < 0.5$.

A brief explanation of the JKS method in [6] is given as follows. Let S denote the set of M received codeword polynomials. First, the GFFT is carried out for each of the received codeword polynomials in S to identify the SVCR and MLCR of each received codeword polynomial. Note that the roots of the received codeword polynomial are searched in the order of $\{\alpha^1, \alpha^2, \cdots, \alpha^{n-1}, \alpha^n\}$ and when calculating the MLCR of the received codeword polynomial, the cyclic shift of the roots is not considered as explained in [6]. For example, when $f(\alpha^{n-1}) = f(\alpha^n) = f(\alpha^1) = f(\alpha^2) = f(\alpha^3) = 0$, the MLCR value of this polynomial $f(x)$ is calculated as 3 by only considering $f(\alpha^1) = f(\alpha^2) = f(\alpha^3) = 0$.

Moreover, the MLCR value should be larger than or equal to 2 and if the MLCR value of a received codeword polynomial is less than 2, this received codeword polynomial is excluded from S. Then, the JKS method carries out two majority votes on SVCR and MLCR, respectively. The first majority vote is done for the SVCR values of the received codeword polynomials in S to obtain the most frequent SVCR which is called a reference SVCR s_{ref}. If a SVCR value of a received codeword polynomial in S is different from s_{ref}, this received codeword polynomial is excluded from S to form a new set S'. The second majority vote is done for the MLCR values of the received codeword polynomials in S' to obtain the most frequent MLCR which is called a reference MLCR l_{ref}. Finally, the generator polynomial $\hat{g}(x)$ is reconstructed by using the s_{ref} and l_{ref} as follows:

$$\hat{g}(x) = LCM\left\{\phi_{\alpha^{s_{ref}}}(x), \cdots, \phi_{\alpha^{s_{ref}+l_{ref}-1}}(x)\right\}. \tag{2}$$

In other words, the JKS method determines b and $2t$ in (1) by deriving s_{ref} in the first majority vote and l_{ref} in the second majority vote, respectively, and if both $s_{ref} = b$ and $l_{ref} = 2t$ are satisfied, then the correct generator polynomial is successfully reconstructed by using the JKS method. Since the JKS method determines the most frequent SVCR and then the most frequent MLCR from the received codeword polynomials in this order, an asymptotic analysis will be performed by calculating the probability that s_{ref} and l_{ref} are equal to b and $2t$ of the generator polynomial, respectively, in this order.

III. ASYMPTOTIC ANALYSIS OF THE JKS METHOD

Since a blind reconstruction performance heavily depends on how many and which received codewords are used even for the same channel environment, an asymptotic analysis of the JKS method is performed under the assumption that the number of received codewords is sufficiently large. Under this assumption, the reconstruction performance of the JKS method is analyzed to derive the maximum cross-over probability, which is called an asymptotic threshold, up to which the correct generator polynomial is successfully reconstructed.

An asymptotic analysis of the JKS method is performed for each majority vote since the first majority vote and the second majority vote in the JKS method are done for the SVCR values and MLCR values of the received codeword polynomials, respectively. To succeed in the blind reconstruction, the correct SVCR b should be selected as s_{ref} in the first majority vote, and then the correct MLCR $2t$ must be selected as l_{ref} in the second majority vote. As will be explained in detail in the next section, in order to select correct MLCR, more conditions must be satisfied compared with the case of selecting correct SVCR. Thus, the channel conditions for selecting correct MLCR should be better than the channel conditions for selecting correct SVCR. In this section, an asymptotic threshold is obtained by deriving an asymptotic threshold in the first majority vote and then by deriving an asymptotic threshold in the second majority vote.

A. NOTATIONS

Let C_i be the conjugacy class including $\alpha^i \in GF(q^m)$ and let $R \subset GF(q^m)$ be the set of the roots of generator polynomial $g(x)$. For example, if $g(x)$ has consecutive roots $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+2t-1} \in GF(q^m)$, then $R = \bigcup_{i=b}^{b+2t-1} C_i$.

Let $S^{q,n}_{(b,l)}$ denote the set of all polynomials having the SVCR b and the MLCR greater than or equal to l over $GF(q)[x]/(x^n - 1)$ where $n|q^m - 1$. For example, all the narrow-sense binary BCH codes of length n are included in $S^{2,n}_{(1,2)}$ because they are generated by the generator polynomials having the SVCR 1 and the MLCR $2t$ which is greater than or equal to 2 over $GF(2)[x]/(x^n - 1)$. Additionally, let $S^{q,n}_{(b,l)^*}$ denote the set of polynomials having the SVCR b and the MLCR l over $GF(q)[x]/(x^n - 1)$, i.e., the polynomials in $S^{q,n}_{(b,l)^*}$ do not have α^{b+l} as their root. Note that since all the polynomials in $S^{q,n}_{(b,l)}$ may have α^{b+l} as their root, $S^{q,n}_{(b,l)^*} \subset S^{q,n}_{(b,l)}$.

Let $\lambda^{q,n}_{(b,l)}$ denote the maximum length of consecutive elements starting from α^b in a union of all conjugacy classes of $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+l-1}$ with respect to $GF(q)$, where $n|q^m - 1$. For example, $\lambda^{2,15}_{(1,3)}$ is 4 because a union of conjugacy classes of α^1, α^2, and α^3 with respect to $GF(2)$ is $\{\alpha^1, \alpha^2, \alpha^4, \alpha^8\} \cup \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$and the maximum length of consecutive elements in this union is 4, i.e., $\alpha^1, \alpha^2, \alpha^3$, and α^4. Additionally, let $\lambda^{q,n,+}_{(b,l)}$ denote $\lambda^{q,n}_{(b,\lambda^{q,n}_{(b,l)}+1)}$. Note that the correct MLCR is exactly $\lambda^{q,n}_{(b,2t)}$, not $2t$.

B. ASYMPTOTIC ANALYSIS FOR THE FIRST MAJORITY VOTE

Suppose that q-ary BCH(n, k, t) codeword polynomials, which are included in $S^{q,n}_{(b,\lambda^{q,n}_{(b,2t)})}$, are transmitted over BSC with the cross-over probability p. Let suppose that the correct SVCR and MLCR of q-ary BCH(n, k, t) are b and $\lambda^{q,n}_{(b,2t)}$, respectively. After performing GFFT to the received codeword polynomials in S, the first majority vote is carried out to the SVCR values of the received codeword polynomials with at least MLCR value 2 in S to result in s_{ref} which is an estimate of b. In order to succeed in the blind reconstruction, the largest number of received codeword polynomials must

have the correct SVCR b (i.e., $s_{ref} = b$), which is statistically expressed as:

$$\Pr\left(r(x) \in S_{(b,2)}^{q,n}\right) \underset{Failure}{\overset{Success}{\gtrless}} \Pr\left(r(x) \in S_{(b',2)}^{q,n}\right), \tag{3}$$

where $b' \neq b$ and b' is an incorrect SVCR. Note that to simplify the expression we omit the given condition that the codeword polynomials $c(x)$ generated by a generator polynomial $g(x)$ having $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+2t-1}$ as its roots are transmitted. We will derive the probabilities that the received codeword polynomials show the correct SVCR b or an incorrect SVCR b', respectively, and then calculate the asymptotic threshold T_1 of the first majority vote of JKS method.

1) DERIVATION OF THE OCCURRING PROBABILITY THAT RECEIVED CODEWORD POLYNOMIALS SHOW THE CORRECT SVCR b

In order for the received codeword polynomial $r(x)$ to be included in $S_{(b,2)}^{q,n}$, the two conditions $r(\alpha^{b-1}) \neq 0$ and $r(\alpha^b) = r(\alpha^{b+1}) = 0$ should be satisfied. Note that, in this case, α^{b-1} is not included in a union of C_b and C_{b+1} because if so, $r(\alpha^{b-1}) = 0$ and hence $r(x)$ is not included in $S_{(b,2)}^{q,n}$. In other words, C_{b-1} and a union of C_b and C_{b+1} must be disjoint. Thus, the two conditions $r(\alpha^{b-1}) \neq 0$ and $r(\alpha^b) = r(\alpha^{b+1}) = 0$ are independent, and hence $\Pr(r(x) \in S_{(b,2)}^{q,n})$ can be calculated as follows:

$$\begin{aligned}&\Pr\left(r(x) \in S_{(b,2)}^{q,n}\right)\\ &\quad= \Pr\left(r(\alpha^{b-1}) \neq 0\right) \Pr\left(r(\alpha^b) = r(\alpha^{b+1}) = 0\right).\end{aligned} \tag{4}$$

The derivation of $\Pr(r(x) \in S_{(b,2)}^{q,n})$ will be explained by deriving $\Pr(r(\alpha^b) = r(\alpha^{b+1}) = 0)$ and $\Pr(r(\alpha^{b-1}) \neq 0)$ separately.

In order for the received codeword polynomial $r(x)$ to have α^b and α^{b+1} as its roots, since the codeword polynomials $c(x)$ already have α^b and α^{b+1} as their roots, the error polynomial $e(x)$ must have α^b and α^{b+1} as its roots. Therefore, to calculate the probability $\Pr(r(\alpha^b) = r(\alpha^{b+1}) = 0)$ in (4), the consecutive roots of error polynomials $e(x)$ are analyzed as follows.

The consecutive roots of error polynomial $e(x)$ definitely depend on the number of non-zero coefficients of $e(x)$, which is denoted as $wt(e(x))$. Then, the error polynomials can be classified into three types according to the number of non-zero coefficients. The first type is the error polynomial $e_1(x)$ having $wt(e_1(x)) = 0$, i.e., error-free case. Since the first-type error polynomial $e_1(x)$ has all the elements α^i as its roots, i.e., $e_1(\alpha^i) = 0$ for $0 \leq i < n$, the received codeword polynomials $r(x)$ with the first-type error polynomial $e_1(x)$ have α^b and α^{b+1} as their roots, i.e., $r(\alpha^b) = 0$ and $r(\alpha^{b+1}) = 0$. Therefore, we have $\Pr(r(\alpha^b) = r(\alpha^{b+1}) = 0 | e_1(x)) = 1$ and if $c(\alpha^{b-1}) \neq 0$, the condition $r(\alpha^{b-1}) = c(\alpha^{b-1}) + e_1(\alpha^{b-1}) \neq 0$ is satisfied. Note that the number of distinct values which $c(\alpha^{b-1})$ can take for $\alpha^{b-1} \in R^c$ is $q^{|C_{b-1}|}$ because α^{b-1} is not included in R, and α^b and α^{b+1} are included in R [12]. Since messages are randomly generated, $\Pr(c(\alpha^{b-1}) = u_{C_{b-1}}) = 1/q^{|C_{b-1}|}$, where $u_{C_{b-1}} \in U_{C_{b-1}}$ for the set $U_{C_{b-1}}$ of values which $c(\alpha^{b-1})$ can take. Thus, we have $\Pr(c(\alpha^{b-1}) \neq 0) = 1 - 1/q^{|C_{b-1}|}$.

In conclusion, the probability that the received codeword polynomial $r(x)$ with the first-type error $e_1(x)$ shows the correct SVCR b is derived as follows:

$$\begin{aligned}&\Pr\left(r(x) \in S_{(b,2)}^{q,n} \middle| e_1(x)\right)\\ &= \Pr\left(r(\alpha^{b-1}) \neq 0 \middle| e_1(x)\right) \Pr\left(r(\alpha^b) = r(\alpha^{b+1}) = 0 \middle| e_1(x)\right)\\ &= 1 - \frac{1}{q^{|C_{b-1}|}} = Q_1(b-1),\end{aligned} \tag{5}$$

where $Q_1(i) = 1 - \frac{1}{q^{|C_i|}}$ for $0 < i < n$. Since, in the JKS method, the roots of the received codeword polynomial $r(x)$ are searched in the order of $\{\alpha^1, \alpha^2, \cdots, \alpha^{n-1}, \alpha^n\}$ without considering the cyclic shift of the roots, the expression in (5) is valid for $2 \leq b \leq n$, i.e., $Q_1(i)$ is defined for $1 \leq i < n$ as given in (5). However, for the narrow-sense BCH codes, $b = 1$ and hence the value of $Q_1(0)$ should be defined. Since, in this case, the probability in (5) is definitely 1, $Q_1(0)$ should be set as 1. Therefore, $Q_1(i)$ is defined as follows:

$$Q_1(i) \triangleq \begin{cases} 1, & i = 0 \\ 1 - \dfrac{1}{q^{|C_i|}}, & 1 \leq i < n. \end{cases} \tag{6}$$

The second type is the error polynomial $e_2(x)$ having $wt(e_2(x)) = 1$ or 2. It will be shown that the second-type error polynomials do not have consecutive roots over $GF^*(q^m) = GF(q^m)/\{0\}$ by Lemma 1. Thus, the received codeword polynomials $r(x)$ with the second-type error polynomials $e_2(x)$ do not have roots α^b and α^{b+1}, i.e., $\Pr(r(\alpha^b) = r(\alpha^{b+1}) = 0 | e_2(x)) = 0$ Therefore, the received codeword polynomials $r(x)$ with the second-type error polynomials $e_2(x)$ do not show the correct SVCR b, i.e., $\Pr\left(r(x) \in S_{(b,2)}^{q,n} \middle| e_2(x)\right) = 0$. Note that the received codeword polynomials with the second-type error polynomials may show an incorrect SVCR b' for $b' \neq b$.

Lemma 1: Any polynomials $f(x)$ having $wt(f(x)) = 1$ or 2 in $GF(q)[x]/(x^n - 1)$ do not have consecutive roots over $GF^*(q^m)$, where $n | q^m - 1$.

Proof: Let $f_1(x) = f_i x^i$ be the polynomial having $wt(f_1(x)) = 1$, where $f_i \neq 0$ and $0 \leq i < n$. Then $f(x) \neq 0$ for $x \in GF^*(q^m)$. Then, it is clear that $f_1(x) = f_i x^i \neq 0$ for any $x \in GF^*(q^m)$.

Let $f_2(x) = f_i x^i + f_j x^j$ be the polynomial having $wt(f_2(x)) = 2$, where $f_i, f_j \neq 0$ and $0 \leq i < j < n$. Suppose that $f_2(x)$ has two consecutive roots $\alpha^b, \alpha^{b+1} \in GF^*(q^m)$. The two equations $f_2(\alpha^b) = 0$ and $f_2(\alpha^{b+1}) = 0$ can be expressed in matrix form as follows:

$$\underbrace{\begin{bmatrix} \alpha^{bi} & \alpha^{bj} \\ \alpha^{(b+1)i} & \alpha^{(b+1)j} \end{bmatrix}}_{A} \begin{bmatrix} f_i \\ f_j \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \tag{7}$$

Note that the determinant of matrix A is $\det(A) = \alpha^{bi+bj}(\alpha^j - \alpha^i)$. Since $\alpha^{bi+bj} \neq 0$ and $\alpha^j - \alpha^i \neq 0$, $\det(A) \neq 0$. Therefore, in order to satisfy (7), both f_i and f_j must be zeros, which is a contradiction.

In conclusion, any polynomials $f(x)$ having $wt(f(x)) = 1$ or 2 in $GF(q)[x]/(x^n - 1)$ do not have consecutive roots over $GF^*(q^m)$, where $n|q^m - 1$. □

Lastly, the third type is the error polynomial $e_3(x)$ having $wt(e_3(x)) \geq 3$. The received codeword polynomials $r(x)$ with the third-type error polynomials $e_3(x)$ may or may not have consecutive roots. If the third-type error polynomial $e_3(x)$ has α^b and α^{b+1} as its roots, the received codeword polynomial $r(x)$ has α^b and α^{b+1} as its roots. Therefore, the occurring probability that the received codeword polynomial $r(x)$ with the third-type error polynomial $e_3(x)$ has the roots α^b and α^{b+1} is calculated as follows:

$$\begin{aligned}&\Pr\left(r(\alpha^b) = r(\alpha^{b+1}) = 0 \middle| wt(e_3(x)) = i\right)\\ &= \Pr\left(e(\alpha^b) = e(\alpha^{b+1}) = 0 \middle| wt(e_3(x)) = i\right)\\ &= \frac{w^{q,n}_{(b,2)}(i)}{\binom{n}{i}},\end{aligned} \tag{8}$$

where $3 \leq i \leq n$. Also, $w^{q,n}_{(b,2)} = \{w^{q,n}_{(b,2)}(0), w^{q,n}_{(b,2)}(1), \cdots, w^{q,n}_{(b,2)}(n)\}$ denotes the weight distribution of q-ary BCH code of the code length n whose generator polynomial has consecutive roots α^b and α^{b+1}, i.e., $w^{q,n}_{(b,2)}(i)$ denotes the number of this BCH codewords having the Hamming weight i. At the same time, the condition $c(\alpha^{b-1}) \neq -e_3(\alpha^{b-1})$ should be satisfied while the condition $e_3(\alpha^b) = e_3(\alpha^{b+1}) = 0$ is satisfied. In fact, such third-type error polynomials $e_3(x)$ are the codeword polynomials that do not have α^{b-1} as a root among the codeword polynomials generated by a generator polynomial $g'(x)$ with consecutive roots α^b and α^{b+1}. Note that this generator polynomial $g'(x)$ does not have α^{b-1} as a root. Thus, the number of distinct values which $e_3(\alpha^{b-1})$ can take for $\alpha^{b-1} \in R^c$ is $q^{|C_{b-1}|}$ [12]. Because an error occurs uniformly at random, $\Pr(e_3(\alpha^{b-1}) = u_{E_{b-1}}) = 1/q^{|C_{b-1}|}$, where $u_{E_{b-1}} \in U_{E_{b-1}}$ for the set $U_{E_{b-1}}$ of values which $e_3(\alpha^{b-1})$ can take. Therefore, since $\Pr(c(\alpha^{b-1}) = u_{C_{b-1}}) = 1/q^{|C_{b-1}|}$, we obtain the following probability: $\Pr(c(\alpha^{b-1}) \neq -e_3(\alpha^{b-1})) = Q_1(b-1)$. In conclusion, the occurring probability that the received codeword polynomial $r(x)$ with the third-type error polynomial $e_3(x)$ shows the correct SVCR b is derived as follows:

$$\Pr\left(r(x) \in S^{q,n}_{(b,2)} \middle| wt(e_3(x)) = i\right) = Q_1(b-1)\frac{w^{q,n}_{(b,2)}(i)}{\binom{n}{i}}, \tag{9}$$

where $3 \leq i \leq n$.

By using the results for three types of error polynomials, the occurring probability $\Pr\left(r(x) \in S^{q,n}_{(b,2)}\right)$ that the received codeword polynomial $r(x)$ shows the correct SVCR b is derived as:

$$\begin{aligned}&\Pr\left(r(x) \in S^{q,n}_{(b,2)}\right)\\ &= \Pr\left(r(x) \in S^{q,n}_{(b,2)} \middle| e_1(x)\right)\Pr\left(e_1(x)\right)\\ &\quad + \sum_{i=3}^{n} \Pr\left(r(x) \in S^{q,n}_{(b,2)} \middle| wt(e_3(x)) = i\right)\\ &\quad \cdot \Pr\left(wt(e_3(x)) = i\right)\\ &= Q_1(b-1)\sum_{i=0}^{n} w^{q,n}_{(b,2)}(i)p^i(1-p)^{n-i},\end{aligned} \tag{10}$$

where $\Pr(e_1(x)) = (1-p)^n$, $\Pr(wt(e_3(x)) = i) = \binom{n}{i} p^i(1-p)^{n-i}$, and p is the cross-over probability of BSC. Note that $w^{q,n}_{(b,2)}(0) = 1$ and $w^{q,n}_{(b,2)}(1) = w^{q,n}_{(b,2)}(2) = 0$ by the BCH bound [1].

2) DERIVATION OF THE OCCURRING PROBABILITY THAT THE RECEIVED CODEWORD POLYNOMIALS SHOW AN INCORRECT SVCR b'

The received codeword polynomial with the second-type or the third-type error polynomial can show an incorrect SVCR b', which may degrade the blind reconstruction performance by increasing $\Pr(r(x) \in S^{q,n}_{(b',2)})$. Specifically, in order for the received codeword polynomial $r(x)$ with the second-type error polynomial $e_2(x)$ to be included in $S^{q,n}_{(b',2)}$, the conditions $r(\alpha^{b'-1}) \neq 0$ and $r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0$ should be satisfied. Note that since $\alpha^{b'-1}$ is not included in a union of $C_{b'}$ and $C_{b'+1}$, the conditions $r(\alpha^{b'-1}) \neq 0$ and $r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0$ must be independent. Thus, the probability $\Pr(r(x) \in S^{q,n}_{(b',2)})$ in (3) can be calculated as follows:

$$\begin{aligned}&\Pr\left(r(x) \in S^{q,n}_{(b',2)}\right)\\ &= \Pr\left(r(\alpha^{b'-1}) \neq 0\right)\Pr\left(r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0\right).\end{aligned} \tag{11}$$

The probability $\Pr(r(x) \in S^{q,n}_{(b',2)})$ will be derived by calculating $\Pr(r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0)$ and $\Pr(r(\alpha^{b'-1}) \neq 0)$ separately.

In order for the received codeword polynomial $r(x)$ with the second-type error polynomial $e_2(x)$ to have consecutive roots $\alpha^{b'}$ and $\alpha^{b'+1}$, the conditions $c(\alpha^{b'}) = -e_2(\alpha^{b'})$ and $c(\alpha^{b'+1}) = -e_2(\alpha^{b'+1})$ should be satisfied. Note that $e_2(x)$ cannot have both $\alpha^{b'}$ and $\alpha^{b'+1}$ as its roots by Lemma 1. There are two cases which satisfy these conditions. The first case is that $\alpha^{b'}$ and $\alpha^{b'+1}$ are included in the same conjugacy class. In this case, if the condition $c(\alpha^{b'}) = -e_2(\alpha^{b'})$ is satisfied, the condition $c(\alpha^{b'+1}) = -e_2(\alpha^{b'+1})$ is automatically satisfied. The second case is that $\alpha^{b'}$ and $\alpha^{b'+1}$ are included in the different conjugacy classes. In this case, in order for the received codeword polynomial to have consecutive roots, the conditions $c(\alpha^{b'}) = -e_2(\alpha^{b'})$ and $c(\alpha^{b'+1}) = -e_2(\alpha^{b'+1})$ should be separately satisfied. Thus, the first case occurs much more frequently than the second case. Since the JKS method is based on the majority vote, the first case affects the

blind reconstruction performance more than the second case. Therefore, we will only derive the occurring probability of the first case for analyzing the first majority vote of the JKS method.

Consider the first case such that $\alpha^{b'}$ and $\alpha^{b'+1}$ are included in the same conjugacy class $C_{b'}$. Note that the number of distinct values which $c(\alpha^{b'})$ can take for $\alpha^{b'} \in R^c$ is $q^{|C_{b'}|}$. Since it is assumed that messages are randomly generated, $\Pr(c(\alpha^{b'}) = u_{C_{b'}}) = 1/q^{|C_{b'}|}$, where $u_{C_{b'}} \in U_{C_{b'}}$ for the set $U_{C_{b'}}$ of values which $c(\alpha^{b'})$ can take [12]. Moreover, it will be confirmed that $\Pr(c(\alpha^{b'}) = u_{C_{b'}}) = 1/q^m$ by Theorems 1 and 2.

Theorem 1: The size of the conjugacy class including consecutive elements in $GF(q^m)$ with respect to $GF(q)$ is m.

Proof: Let C_i be the conjugacy class including the two consecutive elements $\beta^i, \beta^{i+1} \in GF(q^m)$. Suppose that the size $|C_i|$ of C_i is d which clearly divides m. Then, $\beta^{iq^d} = \beta^i$ and $\beta^{(i+1)q^d} = \beta^{i+1}$. Thus, $iq^d = i \mod (q^m - 1)$ and $(i+1)q^d = i+1 \mod (q^m - 1)$, and these equations can be expressed as:

$$A_1(q^m - 1) + i = iq^d \tag{12}$$

$$A_2(q^m - 1) + i + 1 = (i+1)q^d, \tag{13}$$

where A_1 and A_2 are integers making i and $i+1$ be in $[0, q^m - 2]$, respectively. From (12) and (13), we obtain

$$A_2 - A_1 = \frac{q^d - 1}{q^m - 1}.$$

Since $A_2 - A_1$ is an integer, d should be m for $(q^d - 1)/(q^m - 1)$ to be an integer. Therefore, $|C_i|$ is m. □

Theorem 2: The order of the elements in the conjugacy class including consecutive elements in $GF(q^m)$ with respect to $GF(q)$ is $q^m - 1$.

Proof: Suppose that the two consecutive elements $\beta^i, \beta^{i+1} \in GF(q^m)$ are included in the same conjugacy class. Then, the orders of β^i and β^{i+1} are the same, which is denoted as s with $s|q^m - 1$. Because $(\beta^i)^s = 1$ and $(\beta^{i+1})^s = 1$, $is = 0 \mod (q^m - 1)$ and $(i+1)s = 0 \mod (q^m - 1)$. Thus,

$$is = B_1(q^m - 1) \tag{14}$$

$$(i+1)s = B_2(q^m - 1), \tag{15}$$

where B_1 and B_2 are integers. From (14) and (15), we obtain

$$B_1 - B_2 = \frac{s}{q^m - 1}.$$

Since B_1 and B_2 are integers, s should be $q^m - 1$ for $s/(q^m - 1)$ to be an integer. Therefore, the order s of β^i and β^{i+1} is $q^m - 1$. Moreover, since all the elements in the conjugacy class have the same order, the order of all elements of the conjugacy class including consecutive elements is $q^m - 1$ in $GF(q^m)$ with respect to $GF(q)$. □

By Theorem 2, we know that the number of distinct values which $e_2(\alpha^{b'})$ can take for $\alpha^{b'} \in C_{b'}$ is $q^m - 1$, where $b' \neq b$ and $\alpha^{b'}, \alpha^{b'+1} \in C_{b'}$. Because an error occurs uniformly at random, $\Pr(e_2(\alpha^{b'}) = u_{E_{b'}}) = 1/(q^m - 1)$, where $u_{E_{b'}} \in U_{E_{b'}}$ for the set $U_{E_{b'}}$ of the values which $e_2(\alpha^{b'})$ can have. Since the numbers of distinct values which $c(\alpha^{b'})$ and $e_2(\alpha^{b'})$ can take are q^m and $q^m - 1$, respectively, in order for the received codeword polynomial to show an incorrect SVCR b', the number of cases where the condition $c(\alpha^{b'}) = -e_2(\alpha^{b'})$ is satisfied is $q^m - 1$. Thus, the occurring probability that the received codeword polynomial $r(x)$ with the second-type error polynomial $e_2(x)$ shows consecutive roots $\alpha^{b'}$ and $\alpha^{b'+1}$ is calculated as follows:

$$\begin{aligned}
&\Pr\left(r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0 \middle| wt(e_2(x)) = i\right) \\
&= (q^m - 1)\Pr\left(c(\alpha^{b'}) = u_{C_{b'}} \middle| wt(e_2(x)) = i\right) \\
&\quad \cdot \Pr\left(e_2(\alpha^{b'}) = u_{E_{b'}} \middle| wt(e_2(x)) = i\right) \\
&= (q^m - 1)\frac{1}{q^m}\frac{1}{q^m - 1} \\
&= \frac{1}{q^m},
\end{aligned} \tag{16}$$

where $i = 1$ or 2, and $b' \neq b$.

In order for the received codeword polynomial $r(x)$ with the second-type polynomial $e_2(x)$ to show an incorrect SVCR b', the condition $r(\alpha^{b'-1}) \neq 0$, i.e., $c(\alpha^{b'-1}) \neq -e_2(\alpha^{b'-1})$, should be also satisfied. However, unlike α^b and α^{b+1}, $\alpha^{b'-1}$ may or may not be the root of the generator polynomial $g(x)$ because it is determined by q, n, b, and t of the transmitted BCH code, i.e., we do not know whether $\alpha^{b'-1} \in R$ or $\alpha^{b'-1} \in R^c$. Note that in a case where $\alpha^{b'-1} \in R$, $c(\alpha^{b'-1}) = 0$ and in a case where of distinct values which $c(\alpha^{b'-1})$ can take is $|C_{b'-1}|$ [12]. Thus, we explain separately a case where $\alpha^{b'-1} \in R$ and a case where $\alpha^{b'-1} \in R^c$.

The numbers of distinct values which both the single-error polynomials and the double-error polynomials can take vary depending on q and m. In case of the single-error polynomial, since the single-error polynomials do not have a non-zero root, if $|C_{b'-1}| = m$, the number of distinct values which the single-error polynomial can take is $q^m - 1$, otherwise, it is $q^{|C_{b'-1}|}$. In case of the double-error polynomial, if $q^m - 1$ is the prime and $q = 2$, the double-error polynomial does not have a root, otherwise it has a root. Thus, when $q^m - 1$ is the prime and $q = 2$, the number of distinct values which the double-error polynomial can take is $q^m - 1$, otherwise it is $q^{|C_{b'-1}|}$. Note that when $q^m - 1$ is the prime, the size of all conjugacy classes is m [1].

In conclusion, when $\alpha^{b'-1} \in R^c$, the probability that the received codeword polynomial $r(x)$ with the second-type polynomial $e_2(x)$ shows an incorrect SVCR b' is calculated as follows:

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b',2)} \middle| wt(e_2(x)) = 1\right) \\
&= \Pr\left(r(\alpha^{b'-1}) \neq 0 \middle| wt(e_2(x)) = 1\right) \\
&\quad \cdot \Pr\left(r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0 \middle| wt(e_2(x)) = 1\right) \\
&= Q_2(b' - 1)\frac{1}{q^m},
\end{aligned} \tag{17}$$

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b',2)} \middle| wt(e_2(x)) = 2\right) \\
&= \Pr\left(r(\alpha^{b'-1}) \neq 0 \middle| wt(e_2(x)) = 2\right) \\
&\quad \cdot \Pr\left(r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0 \middle| wt(e_2(x)) = 2\right) \\
&= Q_3(b'-1)\frac{1}{q^m}, \qquad (18)
\end{aligned}$$

where if $|C_{b'-1}| = m$, $Q_2(b'-1) = 1 - 1/(q^{|C_{b'-1}|} - 1)$, otherwise, $Q_2(b'-1) = Q_1(b'-1)$. Also, if $q^m - 1$ is the prime and $q = 2$, $Q_3(b'-1) = 1 - 1/(q^{|C_{b'-1}|} - 1)$, otherwise, $Q_3(b'-1) = Q_1(b'-1)$. Note that it is defined as $Q_2(0) = 1$ and $Q_3(0) = 1$ for the same reason as $Q_1(0)$.

When $\alpha^{b'-1} \in R$, because $c(\alpha^{b'-1}) = 0$, the received codeword polynomials $r(x)$ with a single-error polynomial always satisfies the condition $r(\alpha^{b'-1}) \neq 0$. Thus, we have $\Pr(r(\alpha^{b'-1}) \neq 0 | wt(e_2(x)) = 1) = 1$. When $\alpha^{b'-1} \in R$, $q^m - 1$ is the prime, and $q = 2$, the received codeword polynomial $r(x)$ with the double-errors polynomial always satisfies the condition $r(\alpha^{b'-1}) \neq 0$. Also, when $\alpha^{b'-1} \in R$, either $q^m - 1$ is not the prime or $q \neq 2$, the number of non-zero values which the double-error polynomial can take is $q^{|C_{b'-1}|} - 1$. Since the error occurs uniformly at random, the occurring probability of such a case is $\Pr(r(\alpha^{b'-1}) \neq 0 | wt(e_2(x)) = 2) = Q_1(b'-1)$.

In conclusion, when $\alpha^{b'-1} \in R$, the probability that the received codeword polynomial $r(x)$ with the second-type polynomial $e_2(x)$ shows an incorrect SVCR b' is calculated as follows:

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b',2)} \middle| wt(e_2(x)) = 1\right) \\
&= \Pr\left(r(\alpha^{b'-1}) \neq 0 \middle| wt(e_2(x)) = 1\right) \\
&\quad \cdot \Pr\left(r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0 \middle| wt(e_2(x)) = 1\right) \\
&= \frac{1}{q^m}, \qquad (19) \\
&\Pr\left(r(x) \in S^{q,n}_{(b',2)} \middle| wt(e_2(x)) = 2\right) \\
&= \Pr\left(r(\alpha^{b'-1}) \neq 0 \middle| wt(e_2(x)) = 2\right) \\
&\quad \cdot \Pr\left(r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0 \middle| wt(e_2(x)) = 2\right) \\
&= Q_4(b'-1)\frac{1}{q^m}, \qquad (20)
\end{aligned}$$

where if $q^m - 1$ is the prime and $q = 2$, $Q_4(b'-1) = 1$, otherwise, $Q_4(b'-1) = Q_1(b'-1)$.

The occurring probability that the received codeword polynomial $r(x)$ with the third-type error polynomial $e_3(x)$ shows an incorrect SVCR $b'(\neq b)$ is calculated similar to the second-type error polynomial case, and the difference is that the third-type error polynomial, unlike the second-type error polynomial, can have consecutive roots. Therefore, the number of distinct values which $e_3(\alpha^{b'})$ can take for $\alpha^{b'} \in GF(q^m)$ and $\alpha^{b'} \in C_{b'}$ is q^m by Theorems 1 and 2, and the occurring probability that the received codeword polynomial $r(x)$ with the third-type error polynomial $e_3(x)$ having $wt(e_3(x)) = i$ for $3 \leq i \leq n$ is calculated as $\Pr(r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0 | wt(e_3(x)) = i) = 1/q^m$. Also, the condition $r(\alpha^{b'-1}) \neq 0$ should be satisfied. When $\alpha^{b'-1} \in R^c$, similar to the second-type error polynomial case, the numbers of distinct values which each of $c(\alpha^{b'-1})$ and $e_3(\alpha^{b'-1})$ can take are $q^{|C_{b'-1}|}$. Since the messages are generated randomly and errors occur uniformly at random, $\Pr(r(\alpha^{b'-1}) \neq 0 | wt(e_3(x)) = i) = Q_1(b'-1)$.

In conclusion, when $\alpha^{b'-1} \in R^c$, the probability that the received codeword polynomial $r(x)$ with the third-type polynomial $e_3(x)$ shows an incorrect SVCR b' is calculated as follows:

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b',2)} \middle| wt(e_3(x)) = i\right) \\
&= \Pr\left(r(\alpha^{b'-1}) \middle| wt(e_3(x)) = i\right) \\
&\quad \cdot \Pr\left(r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0 \middle| wt(e_3(x)) = i\right) \\
&= Q_1(b'-1)\frac{1}{q^m}. \qquad (21)
\end{aligned}$$

When $\alpha^{b'-1} \in R$, $c(\alpha^{b'-1}) = 0$ and the number of distinct values which $e_3(\alpha^{b'-1})$ can take is $q^{|C_{b'-1}|}$. Since the errors occur uniformly at random, $\Pr(r(\alpha^{b'-1}) \neq 0 | wt(e_3(x)) = i) = Q_1(b'-1)$. Thus, when $\alpha^{b'-1} \in R$, the probability that the received codeword polynomial $r(x)$ with the third-type polynomial $e_3(x)$ shows an incorrect SVCR b' is calculated as follows:

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b',2)} \middle| wt(e_3(x)) = i\right) \\
&= \Pr\left(r(\alpha^{b'-1}) \middle| wt(e_3(x)) = i\right) \\
&\quad \cdot \Pr\left(r(\alpha^{b'}) = r(\alpha^{b'+1}) = 0 \middle| wt(e_3(x)) = i\right) \\
&= Q_1(b'-1)\frac{1}{q^m}. \qquad (22)
\end{aligned}$$

In conclusion, when $\alpha^{b'-1} \in R^c$, the occurring probability that the received codeword polynomial $r(x)$ shows an incorrect SVCR b' is calculated as follows:

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b',2)}\right) \\
&= \sum_{i=1}^{2} \Pr\left(r(x) \in S^{q,n}_{(b',2)} \middle| wt(e_2(x)) = i\right) \\
&\quad \cdot \Pr\left(wt(e_2(x)) = i\right) \\
&\quad + \sum_{i=3}^{n} \Pr\left(r(x) \in S^{q,n}_{(b',2)} \middle| wt(e_3(x)) = i\right) \\
&\quad \cdot \Pr\left(wt(e_3(x)) = i\right) \\
&= \sum_{i=0}^{n} w^{q,n,R^c}(i) p^i (1-p)^{n-i}, \qquad (23)
\end{aligned}$$

where $\Pr(wt(e_2(x)) = i) = \binom{n}{i} p^i (1-p)^{n-i}$ for $i = 1$ or 2, and $w^{q,n,R^c}(0) = 0$, $w^{q,n,R^c}(1) = Q_2(b'-1)1/q^m \binom{n}{1}$, $w^{q,n,R^c}(2) = Q_3(b'-1)1/q^m \binom{n}{2}$, and $w^{q,n,R^c}(j) = Q_1(b'-1)1/q^m \binom{n}{j}$ for

$3 \le j \le n$. When $\alpha^{b'-1} \in R$, the occurring probability that the received codeword polynomial $r(x)$ shows an incorrect SVCR b' is calculated as follows:

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b',2)}\right) \\
&= \sum_{i=1}^{2} \Pr\left(r(x) \in S^{q,n}_{(b',2)} \middle| wt\left(e_2(x)\right) = i\right) \\
&\quad \cdot \Pr\left(wt\left(e_2(x)\right) = i\right) \\
&\quad + \sum_{i=3}^{n} \Pr\left(r(x) \in S^{q,n}_{(b',2)} \middle| wt\left(e_3(x)\right) = i\right) \\
&\quad \cdot \Pr\left(wt\left(e_3(x)\right) = i\right) \\
&= \sum_{i=0}^{n} w^{q,n,R}(i) p^i (1-p)^{n-i}, \qquad (24)
\end{aligned}$$

where $w^{q,n,R}(0) = 0$, $w^{q,n,R}(1) = 1/q^m \binom{n}{1}$, $w^{q,n,R}(2) = Q_4(b'-1)1/q^m \binom{n}{2}$, and $w^{q,n,R}(j) = Q_1(b'-1)1/q^m \binom{n}{j}$ for $3 \le j \le n$.

3) DERIVATION OF ASYMPTOTIC THRESHOLD OF THE FIRST MAJORITY VOTE

Finally, when $\alpha^{b'-1} \in R^c$, by using (3), (10), and (23), the decision criterion of the first majority vote in the JKS method is derived as follows.

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b,2)}\right) \underset{Fail}{\overset{Success}{\gtrless}} \Pr\left(r(x) \in S^{q,n}_{(b',2)}\right) \\
&\Leftrightarrow \Pr\left(r(x) \in S^{q,n}_{(b,2)}\right) - \Pr\left(r(x) \in S^{q,n}_{(b',2)}\right) \underset{Fail}{\overset{Success}{\gtrless}} 0 \\
&\Leftrightarrow \sum_{i=0}^{n} \left(w'^{q,n}_{(b,2)}(i) - w^{q,n,R^c}(i)\right) p^i (1-p)^{n-i} \underset{Fail}{\overset{Success}{\gtrless}} 0, \qquad (25)
\end{aligned}$$

where $w'^{q,n}_{(b,2)}(i) = Q_1(b-1) w^{q,n}_{(b,2)}(i)$. When $\alpha^{b'-1} \in R$, by using (3), (10), and (24), the decision criterion of the first majority vote in the JKS method is derived as follows.

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b,2)}\right) \underset{Fail}{\overset{Success}{\gtrless}} \Pr\left(r(x) \in S^{q,n}_{(b',2)}\right) \\
&\Leftrightarrow \sum_{i=0}^{n} \left(w'^{q,n}_{(b,2)}(i) - w^{q,n,R}(i)\right) p^i (1-p)^{n-i} \underset{Fail}{\overset{Success}{\gtrless}} 0. \qquad (26)
\end{aligned}$$

The asymptotic threshold T_1 of the first majority vote is the maximum p that leads (25) and (26) to the success. From (25) and (26), it is confirmed that the asymptotic threshold T_1 of the first majority vote is affected by the code length n of BCH codes but not the error-correcting capability t of BCH code. For the various narrow-sense BCH codes, Table 1 shows the asymptotic thresholds T_1 of the first majority vote in the JKS method, which is calculated by using the weight distribution of narrow-sense BCH codes [1]. When the narrow-sense BCH code of the code length $n = 31$ is used, there exists the case that $\alpha^{b'-1} \in R$ unlike the narrow-sense BCH codes of the code length $n = 63$ and $n = 127$. Thus, only for the narrow-sense BCH code of the code length $n = 31$, the asymptotic threshold T_1 is derived by selecting a smaller value between the asymptotic threshold which is calculated by using (25) and (26) as shown in Table 1.

TABLE 1. T_1 for the various narrow-sense binary BCH codes.

n	31	63	127
T_1	0.1786	0.1148	0.0703

C. ASYMPTOTIC ANALYSIS FOR THE SECOND MAJORITY VOTE

Through the first majority vote of the JKS method, all received codeword polynomials in S' have the same SVCR. Note that it is assumed that the correct SVCR b is selected in the first majority vote, i.e., $s_{ref} = b$ and all received codeword polynomials in S' are included in $S^{q,n}_{(b,2)}$, To succeed in the second majority vote, the correct MLCR $\lambda^{q,n}_{(b,2t)}$ should be selected. Note that $\lambda^{q,n}_{(b,2t)}$ will be denoted by l_t for simplicity. From an asymptotic point of view, the occurring probability of the received codeword polynomial showing the correct MLCR l_t in S' should be higher than that of the received codeword polynomial showing an incorrect MLCR. Thus, to derive an asymptotic threshold of the second majority vote, it should be compared that the occurring probability of the received codeword polynomial showing the correct MLCR and the highest occurring probability of the received codeword polynomial showing an incorrect MLCR. Note that the codeword polynomial showing an incorrect MLCR with the highest occurring probability changes according to the error-correcting capability of BCH code. Thus, we analyze the second majority vote of the JKS method by considering two cases, the first case is when the error-correcting capability of BCH code is 1, and the other case is when the error-correcting capability of BCH code is more than 1. The difference in these two cases will be explained in the next section. For the convenience of explanation, the case when the error-correcting capability is more than 1 will be explained first.

1) ASYMPTOTIC ANALYSIS FOR BCH CODES WITH MULTIPLE-ERROR CORRECTING CAPABILITY

When BCH code with multiple-error-correcting capability is used, it will be confirmed through Lemma 2 that the received codeword polynomial with the smallest incorrect MLCR value shows the highest occurring probability among those with incorrect MLCR values.

Lemma 2: Let's divide the polynomials showing the same SVCR in $GF(q)[x]/(x^n - 1)$ into the sets based on the MLCR value such that each set consists of the polynomials showing the same MLCR value and different sets show different MLCR value. Then, among these sets, a set of polynomials having the smallest MLCR value shows the highest occurring probability.

Proof: Let $S_{(b,l)}^{q,n}$ be the set of polynomials showing SVCR b and MLCR l in $GF(q)[x]/(x^n-1)$, and let $S_{(b,l')}^{q,n}$ be the set of polynomials showing SVCR b and MLCR $l' > l$ in $GF(q)[x]/(x^n-1)$. Since all polynomials in $S_{(b,l')}^{q,n}$ are included in $S_{(b,l)}^{q,n}$, i.e., $S_{(b,l)}^{q,n} \supset S_{(b,l')}^{q,n}$, $\Pr\left(S_{(b,l)}^{q,n}\right) \geq \Pr\left(S_{(b,l')}^{q,n}\right)$. Therefore, among the sets of polynomials showing the same SVCR $S_{(b,l)}^{q,n}$, the set of polynomials with the smallest MLCR l shows the highest occurring probability. □

Since l_{ref} is determined by the majority vote, in order to succeed in the second majority vote, the largest number of received codeword polynomials must show the correct MLCR value l_t (i.e., $l_{ref} = l_t$), which is statistically expressed as:

$$\Pr\left(r(x) \in S_{(b,l_t)^*}^{q,n}\right) \underset{Failure}{\overset{Success}{\gtrless}} \Pr\left(r(x) \in S_{(b,l_1)^*}^{q,n}\right), \quad (27)$$

where $l_1 = \lambda_{(b,2)}^{q,n}$. Note that to simplify the expression we omit the given condition that the codeword polynomials $c(x)$ generated by a generator polynomial $g(x)$ having $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+l_t-1}$ as its roots are transmitted.

In order for the received codeword polynomials $r(x)$ to show the correct MLCR l_t, the conditions $r(\alpha^b) = r(\alpha^{b+1}) = \cdots = r(\alpha^{b+l_t-1}) = 0$, $r(\alpha^{b-1}) \neq 0$, and $r(\alpha^{b+l_t}) \neq 0$ should be satisfied. Note that because $r(\alpha^{b-1}) \neq 0$ and $r(\alpha^{b+l_t}) \neq 0$, it can be seen that a union of C_{b-1} and C_{b+l_t} and a union of C_b, C_{b+1}, $\cdots$, C_{b+l_t-1} are disjoint, i.e., $\alpha^{b-1}, \alpha^{b+l_t} \in R^c$. Since $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+l_t-1} \in R$ and $\alpha^{b-1}, \alpha^{b+l_t} \in R^c$, these conditions such that $r(\alpha^b) = r(\alpha^{b+1}) = \cdots = r(\alpha^{b+l_t-1}) = 0$ and $r(\alpha^{b-1}), r(\alpha^{b+l_t}) \neq 0$ must be independent. However, we do not exactly know whether the condition $r(\alpha^{b-1}) \neq 0$ and the condition $r(\alpha^{b+l_t}) \neq 0$ are independent or not because it is determined by the transmitted BCH code. Specifically, we do not know whether α^{b-1} and α^{b+l_t} are included in the different conjugacy classes or the same conjugacy class. Note that if α^{b-1} and α^{b+l_t} are included in the different conjugacy classes, $\Pr(r(\alpha^{b-1}) \neq 0, r(\alpha^{b+l_t}) \neq 0) = \Pr(r(\alpha^{b-1}) \neq 0)\Pr(r(\alpha^{b+l_t}) \neq 0)$, otherwise, $\Pr(r(\alpha^{b-1}) \neq 0, r(\alpha^{b+l_t}) \neq 0) = \Pr(r(\alpha^{b+l_t}) \neq 0)$. Hence, we consider both cases where α^{b-1} and α^{b+l_t} are included in the same conjugacy class and ones are included in the different conjugacy classes. Note that when α^{b-1} and α^{b+l_t} are included in the same conjugacy class, if the condition $r(\alpha^{b-1}) \neq 0$ is satisfied, then the condition $r(\alpha^{b+l_t}) \neq 0$ is satisfied automatically. When α^{b-1} and α^{b+l_t} are included in the different conjugacy classes, the conditions $r(\alpha^{b-1}) \neq 0$ and $r(\alpha^{b+l_t}) \neq 0$ must be independent. Thus, when α^{b-1} and α^{b+l_t} are included in the different conjugacy classes, $\Pr(r(x) \in S_{(b,l_t)^*}^{q,n})$ can be calculated as follows:

$$\begin{aligned}&\Pr\left(r(x) \in S_{(b,l_t)^*}^{q,n}\right)\\ &= \Pr\left(r(\alpha^{b-1}) \neq 0\right)\Pr\left(r(\alpha^b) = \cdots = r(\alpha^{b+l_t-1}) = 0\right)\\ &\quad \cdot \Pr\left(r(\alpha^{b+l_t}) \neq 0\right), \end{aligned} \quad (28)$$

where $\Pr(r(\alpha^{b-1}) \neq 0)$ and $\Pr(r(\alpha^{b+l_t}) \neq 0)$ are calculated as $Q_1(b-1)$ and $Q_1(b+l_t)$, respectively. When α^{b-1} and α^{b+l_t} are included in the same conjugacy class, $\Pr(r(x) \in S_{(b,l_t)^*}^{q,n})$ can be calculated as follows:

$$\begin{aligned}&\Pr\left(r(x) \in S_{(b,l_t)^*}^{q,n}\right)\\ &= \Pr\left(r(\alpha^b) = \cdots = r(\alpha^{b+l_t-1}) = 0\right)\Pr\left(r(\alpha^{b+l_t}) \neq 0\right). \end{aligned} \quad (29)$$

Since $c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+l_t-1}) = 0$, $\Pr(r(\alpha^b) = r(\alpha^{b+1}) = \cdots = r(\alpha^{b+l_t-1}) = 0)$ is recalculated as $\Pr(e(\alpha^b) = e(\alpha^{b+1}) = \cdots = e(\alpha^{b+l_t-1}) = 0)$, and then $\Pr(e(\alpha^b) = \cdots = e(\alpha^{b+l_t-1}) = 0)$ is calculated by using (8) as follows:

$$\begin{aligned}&\Pr\left(e(\alpha^b) = \cdots = e(\alpha^{b+l_t-1}) = 0\right)\\ &= \sum_{i=0}^{n} w_{(b,l_t)}^{q,n}(i)p^i(1-p)^{n-i}. \end{aligned} \quad (30)$$

In conclusion, when α^{b-1} and α^{b+l_t} are included in the different conjugacy classes, the occurring probability that the received codeword polynomial $r(x)$ shows the correct MLCR l_t is calculated by using (28) and (30) as follows:

$$\begin{aligned}&\Pr\left(r(x) \in S_{(b,l_t)^*}^{q,n}\right)\\ &= Q_1(b-1)Q_1(b+l_t)\sum_{i=0}^{n} w_{(b,l_t)}^{q,n}(i)p^i(1-p)^{n-i}. \end{aligned} \quad (31)$$

When α^{b-1} and α^{b+l_t} are included in the same conjugacy class, the occurring probability that the received codeword polynomial $r(x)$ shows the correct MLCR l_t is calculated by using (29) and (30) as follows:

$$\begin{aligned}&\Pr\left(r(x) \in S_{(b,l_t)^*}^{q,n}\right)\\ &= Q_1(b+l_t)\sum_{i=0}^{n} w_{(b,l_t)}^{q,n}(i)p^i(1-p)^{n-i}. \end{aligned} \quad (32)$$

In order for the received codeword polynomials $r(x)$ to show an incorrect MLCR l_1, the conditions $r(\alpha^b) = r(\alpha^{b+1}) = \cdots = r(\alpha^{b+l_1-1}) = 0$, $r(\alpha^{b-1}) \neq 0$, and $r(\alpha^{b+l_1}) \neq 0$ should be satisfied. Because a union of C_{b-1} and C_{b+l_1} and a union of $C_b, C_{b+1}, \cdots, C_{b+l_1-1}$ are disjoint, the conditions $r(\alpha^{b+1}), r(\alpha^{b+l_1}) \neq 0$ and $r(\alpha^b) = r(\alpha^{b+1}) = \cdots = r(\alpha^{b+l_1-1}) = 0$ must be independent. Note that since whether α^{b-1} and α^{b+l_1} are included in the same conjugacy class or not is determined by the transmitted BCH code, we do not exactly know. Hence, we consider both cases where α^{b-1} and α^{b+l_1} are included in the different conjugacy classes and ones are included in the same conjugacy class.

Since $c(\alpha^b) = \cdots = c(\alpha^{b+l_1-1}) = \cdots = c(\alpha^{b+l_t-1}) = 0$, $\Pr(r(x) \in S_{(b,l_1)^*}^{q,n})$ can be recalculated

as follows:

$$\Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right) = \Pr\left(r(\alpha^{b-1}) \neq 0\right) \Pr\left(e(\alpha^b) = \cdots = e(\alpha^{b+l_1-1}) = 0\right) \cdot \Pr\left(e(\alpha^{b+l_1}) \neq 0\right), \quad (33)$$

where α^{b-1} and α^{b+l_1} are included in the different conjugacy classes. When α^{b-1} and α^{b+l_1} are included in the same conjugacy class, the occurring probability that the received codeword polynomial $r(x)$ shows an incorrect MLCR l_1 is calculated as follows:

$$\Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right) = \Pr\left(e(\alpha^b) = \cdots = e(\alpha^{b+l_1-1}) = 0\right) \Pr\left(e(\alpha^{b+l_1}) \neq 0\right). \quad (34)$$

Because $\alpha^{b-1} \in R^c$, $\Pr(r(\alpha^{b-1}) \neq 0) = Q_1(b-1)$. In order to satisfy the two conditions $e(\alpha^b) = e(\alpha^{b+1}) = \cdots = e(\alpha^{b+l_1-1}) = 0$ and $e(\alpha^{b+l_1}) \neq 0$, the error polynomial $e(x)$ must have consecutive roots $\alpha^b, \cdots, \alpha^{b+l_1-1}$ and not α^{b+l_1}. Thus, the occurring probability of these two conditions is calculated by using (30) and $w^{q,n}_{(b,l_1)^*}(i) = w^{q,n}_{(b,l_1)}(i) - w^{q,n}_{(b,l_1^+)}(i)$ as follows:

$$\Pr\left(e(\alpha^b) = \cdots = e(\alpha^{b+l_1-1}) = 0\right) \Pr\left(e(\alpha^{b+l_1}) \neq 0\right) = \sum_{i=0}^{n} w^{q,n}_{(b,l_1)^*}(i) p^i (1-p)^{n-i}. \quad (35)$$

In conclusion, when α^{b-1} and α^{b+l_1} are included in the different conjugacy classes, the occurring probability that the received codeword polynomial $r(x)$ shows an incorrect MLCR l_1 is calculated as follows:

$$\Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right) = Q_1(b-1) \sum_{i=0}^{n} w^{q,n}_{(b,l_1)^*}(i) p^i (1-p)^{n-i}. \quad (36)$$

When α^{b-1} and α^{b+l_1} are included in the same conjugacy class, the occurring probability that the received codeword polynomial $r(x)$ shows an incorrect MLCR l_1 is calculated as follows:

$$\Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right) = \sum_{i=0}^{n} w^{q,n}_{(b,l_1)^*}(i) p^i (1-p)^{n-i}. \quad (37)$$

In conclusion, when α^{b-1}, α^{b+l_1}, and α^{b+l_t} are included in the different conjugacy classes, for BCH code with multiple-error-correcting capability, by using (27), (31), and (36), the decision criterion of the second majority vote in the JKS method is derived as follows:

$$\Pr\left(r(x) \in S^{q,n}_{(b,l_t)^*}\right) \underset{Failure}{\overset{Success}{\gtrless}} \Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right)$$
$$\Leftrightarrow \Pr\left(r(x) \in S^{q,n}_{(b,l_t)^*}\right) - \Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right) \underset{Fail}{\overset{Success}{\gtrless}} 0$$
$$\Leftrightarrow Q_1(b-1) \sum_{i=0}^{n} \left\{Q_1(b+l_t) w^{q,n}_{(b,l_t)}(i) - w^{q,n}_{(b,l_1)^*}(i)\right\} \cdot p^i (1-p)^{n-i} \underset{Failure}{\overset{Success}{\gtrless}} 0. \quad (38)$$

When α^{b-1}, α^{b+l_1}, and α^{b+l_t} are included in the same conjugacy class, for BCH code with multiple-error-correcting capability, by using (27), (32), and (37), the decision criterion of the second majority vote in the JKS method is derived as follows:

$$\Pr\left(r(x) \in S^{q,n}_{(b,l_t)^*}\right) \underset{Failure}{\overset{Success}{\gtrless}} \Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right)$$
$$\Leftrightarrow \Pr\left(r(x) \in S^{q,n}_{(b,l_t)^*}\right) - \Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right) \underset{Fail}{\overset{Success}{\gtrless}} 0$$
$$\Leftrightarrow \sum_{i=0}^{n} \left\{Q_1(b+l_t) w^{q,n}_{(b,l_t)}(i) - w^{q,n}_{(b,l_1)^*}(i)\right\} \cdot p^i (1-p)^{n-i} \underset{Failure}{\overset{Success}{\gtrless}} 0. \quad (39)$$

The asymptotic threshold T_2 of the second majority vote in the JKS method is the maximum p that leads the decision by (39) to the success. For various narrow-sense BCH codes, Table 2 shows the asymptotic threshold T_2 of JKS method, which is calculated by using the weight distributions of BCH codes [1].

2) ASYMPTOTIC ANALYSIS FOR BCH CODES WITH ONE-ERROR-CORRECTING CAPABILITY

When BCH code with multiple-error-correcting capability is used, the error polynomial included in $S^{q,n}_{(b,l_1)^*}$ leads to the

TABLE 2. T_2 and T for various narrow-sense binary BCH codes.

t \ n	31		63		127	
	T_2	T	T_2	T	T_2	T
1	0.5000	0.1786	0.5000	0.1148	0.5000	0.0703
2	0.1141	0.1141	0.0668	0.0668	0.0384	0.0384
3	0.1138	0.1138	0.0667	0.0667	0.0384	0.0384
4	0.1138	0.1138	0.0652	0.0652	0.0384	0.0384
5	-	-	0.0667	0.0667	0.0384	0.0384
6	-	-	0.0667	0.0667	0.0384	0.0384
7	-	-	0.0667	0.0667	0.0384	0.0384
8	-	-	0.0632	0.0667	0.0384	0.0384
9	-	-	0.0667	0.0667	0.0384	0.0384
10	-	-	0.0632	0.0667	0.0384	0.0384
11	-	-	-	-	0.0384	0.0384
12	-	-	-	-	0.0384	0.0384
13	-	-	-	-	0.0384	0.0384
14	-	-	-	-	0.0384	0.0384
15	-	-	-	-	0.0384	0.0384
16	-	-	-	-	0.0384	0.0384

failure of the JKS method, where $l_1 = \lambda^{q,n}_{(b,2)}$. However, when BCH code with one-error-correcting capability is used, the JKS method succeeds even with the error polynomial included in $S^{q,n}_{(b,l_1)^*}$. Hence, the error polynomial that leads the blind reconstruction of the JKS method to fail should be redefined. According to Lemma 2, among the sets of polynomials showing the same SVCR, a set of polynomials having the smaller MLCR value shows the higher occurring probability than the other sets of polynomial having the larger MLCR value. Thus, it is clear that the received codeword polynomial showing the second smallest MLCR value leads the JKS method to fail when BCH code with one-error-correcting capability is used. Therefore, when BCH code with one-error-correcting capability is used, in order to succeed in the second majority vote, the largest number of received codeword polynomials must show the correct MLCR value l_1 (i.e., $l_{ref} = l_1$), which is statistically expressed as:

$$\Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right) \underset{Failure}{\overset{Success}{\gtrless}} \Pr\left(r(x) \in S^{q,n}_{(b,l_1^+)^*}\right), \quad (40)$$

where $l_1^+ = \lambda^{q,n,+}_{(b,2)}$. Note that to simplify the expression we omit the given condition that the codeword polynomials $c(x)$ generated by a generator polynomial $g(x)$ having $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+l_t-1}$ as its roots are transmitted.

In the left-hand side (LHS) of (40), in order for the received codeword polynomial to be included in $S^{q,n}_{(b,l_1)^*}$, it is needed that the error polynomial $e(x)$ is included in $S^{q,n}_{(b,l_1)^*}$ and the conditions $r(\alpha^{b-1}) \neq 0$ and $r(\alpha^{b+l_1}) \neq 0$ are satisfied. Note that $\alpha^{b-1}, \alpha^{b+l_1} \in R^c$, but it is not known whether α^{b-1} and α^{b+l_1} are included in the different conjugacy classes or not, and hence we consider both cases where α^{b-1} and α^{b+l_1} are included in the different conjugacy classes and ones are included in the same conjugacy class. When α^{b-1} and α^{b+l_1} are included in the different conjugacy classes, the probability $\Pr(r(x) \in S^{q,n}_{(b,l_1)^*})$ in the LHS of (40) can be calculated as follows:

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right) \\
&= \Pr\left(r(\alpha^{b-1}) \neq 0, r(\alpha^b) = \cdots = r(\alpha^{b+l_1-1}) = 0, \right. \\
&\qquad \left. r(\alpha^{b+l_1}) \neq 0\right) \\
&= \Pr\left(r(\alpha^{b-1}) \neq 0\right) \Pr\left(r(\alpha^b) = \cdots = r(\alpha^{b+l_1-1}) = 0\right) \\
&\quad \cdot \Pr\left(r(\alpha^{b+l_1}) \neq 0\right) \\
&= Q_1(b-1) \Pr\left(e(\alpha^b) = \cdots = e(\alpha^{b+l_1-1}) = 0\right) \\
&\quad \cdot Q_1(b+l_1) \\
&= Q_1(b-1)Q_1(b+l_1) \sum_{i=0}^{n} w^{q,n}_{(b,l_1)}(i) p^i (1-p)^{n-i}, \quad (41)
\end{aligned}$$

where $\Pr(r(\alpha^{b-1}) \neq 0) = Q_1(b-1)$ and $\Pr(r(\alpha^{b+l_1}) \neq 0) = Q_1(b+l_1)$ because $\alpha^{b-1}, \alpha^{b+l_1} \in R^c$. Also, $\Pr(e(\alpha^b) = \cdots = e(\alpha^{b+l_1-1}) = 0) = \sum_{i=0}^{n} w^{q,n}_{(b,l_1)}(i) p^i (1-p)^{n-i}$ is calculated as (8). When α^{b-1} and α^{b+l_1} are included in the same conjugacy class, the probability $\Pr(r(x) \in S^{q,n}_{(b,l_1)^*})$ in the LHS of (40) can be calculated as follows:

$$\begin{aligned}
&\Pr\left(r(x) \in S^{q,n}_{(b,l_1)^*}\right) \\
&= \Pr\left(r(\alpha^{b-1}) \neq 0, r(\alpha^b) = \cdots = r(\alpha^{b+l_1-1}) = 0, \right. \\
&\qquad \left. r(\alpha^{b+l_1}) \neq 0\right) \\
&= \Pr\left(r(\alpha^b) = \cdots = r(\alpha^{b+l_1-1}) = 0\right) \Pr\left(r(\alpha^{b+l_1}) \neq 0\right) \\
&= \Pr\left(e(\alpha^b) = \cdots = e(\alpha^{b+l_1-1}) = 0\right) Q_1(b+l_1) \\
&= Q_1(b+l_1) \sum_{i=0}^{n} w^{q,n}_{(b,l_1)}(i) p^i (1-p)^{n-i}. \quad (42)
\end{aligned}$$

Note that because α^{b-1} and α^{b+l_1} are included in the same conjugacy class, if the condition $r(\alpha^{b+l_1}) \neq 0$ is satisfied, the condition $r(\alpha^{b-1}) \neq 0$ is satisfied automatically.

In the RHS of (40), in order for the received codeword polynomials $r(x)$ to be included in $S^{q,n}_{(b,l_1^+)^*}$, the conditions $r(\alpha^b) = r(\alpha^{b+1}) = \cdots = r(\alpha^{b+l_1^+-1}) = 0$, $r(\alpha^{b-1}) \neq 0$, and $r(\alpha^{b+l_1^+}) \neq 0$ should be satisfied. Because $\alpha^{b-1}, \alpha^{b+l_1^+} \in R^c$, the occurring probabilities of the conditions $r(\alpha^{b-1}) \neq 0$ and $r(\alpha^{b+l_1^+}) \neq 0$ are calculated as $Q_1(b-1)$ and $Q_1(b+l_1^+)$, respectively. However, it is not known whether α^{b-1} and $\alpha^{b+l_1^+}$ are included in the different conjugacy classes or not since it is determined by the transmitted BCH code. Thus, we consider both cases where α^{b-1} and $\alpha^{b+l_1^+}$ are included in the different conjugacy classes and ones are included in the same conjugacy class.

Since $c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+l_1-1}) = 0$, the condition $r(\alpha^b) = r(\alpha^{b+1}) = \cdots = r(\alpha^{b+l_1^+-1}) = 0$ can be divided into the two conditions $r(\alpha^b) = r(\alpha^{b+1}) = \cdots = r(\alpha^{b+l_1-1}) = 0$ and $r(\alpha^{b+l_1}) = 0$. Note that since a union of $C_b, C_{b+1}, \cdots, C_{b+l_1}$ is the same as a union of $C_b, C_{b+1}, \cdots, C_{b+l_1^+-1}$, the condition $r(\alpha^b) = r(\alpha^{b+1}) = \cdots = r(\alpha^{b+l_1^+-1}) = 0$ is satisfied if the two conditions divided are satisfied. Also, because C_{b+l_1} and a union of $C_b, C_{b+1}, \cdots, C_{b+l_1-1}$ are disjoint, the two conditions divided must be independent. The first condition $r(\alpha^b) = r(\alpha^{b+1}) = \cdots = r(\alpha^{b+l_1-1}) = 0$ can be calculated as $e(\alpha^b) = e(\alpha^{b+1}) = \cdots = e(\alpha^{b+l_1-1}) = 0$ because $c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+l_1-1}) = 0$. Thus, the occurring probability of the first condition is calculated as $\sum_{i=0}^{n} w^{q,n}_{(b,l_1)}(i) p^i (1-p)^{n-i}$ by using (8). Because $\alpha^{b+l_1} \in R^c$, the occurring probability of the second condition $r(\alpha^{b+l_1}) = 0$ is calculated as $1 - Q_1(b+l_1)$, i.e., $\Pr(r(\alpha^{b+l_1}) = 0) = 1 - \Pr(r(\alpha^{b+l_1}) \neq 0)$.

In conclusion, when α^{b-1} and $\alpha^{b+l_1^+}$ are included in the different conjugacy classes, the occurring probability that the received codeword polynomial $r(x)$ shows an incorrect

MLCR l_1^+ is calculated as follows:

$$\Pr\left(r(x) \in S^{q,n}_{(b,l_1^+)^*}\right) = Q_1(b-1)Q_1(b+l_1)Q_1(b+l_1^+) \cdot \sum_{i=0}^{n} w^{q,n}_{(b,l_1)}(i)p^i(1-p)^{n-i}. \quad (43)$$

When α^{b-1} and $\alpha^{b+l_1^+}$ are included in the same conjugacy class, the occurring probability that the received codeword polynomial $r(x)$ shows an incorrect MLCR l_1^+ is calculated as follows:

$$\Pr\left(r(x) \in S^{q,n}_{(b,l_1^+)^*}\right) = Q_1(b+l_1)Q_1(b+l_1^+) \cdot \sum_{i=0}^{n} w^{q,n}_{(b,l_1)}(i)p^i(1-p)^{n-i}. \quad (44)$$

In conclusion, for BCH code with one-error-correcting capability, like (39), when α^{b-1} and $\alpha^{b+l_1^+}$ are included in the different conjugacy classes, the decision criterion of the second majority vote in the JKS method is derived by using (40), (41), and (43) as follows:

$$Q_1(b-1)Q_1(b+l_1)\sum_{i=0}^{n}\left\{w^{q,n}_{(b,l_1)}(i) - Q_1(b+l_1^+)w^{q,n}_{(b,l_1)}(i)\right\}p^i(1-p)^{n-i} \underset{Failure}{\overset{Success}{\gtrless}} 0. \quad (45)$$

When α^{b-1} and $\alpha^{b+l_1^+}$ are included in the same conjugacy class, the decision criterion of the second majority vote in the JKS method is derived by using (40), (42), and (44) as follows:

$$Q_1(b+l_1)\sum_{i=0}^{n}\left\{w^{q,n}_{(b,l_1)}(i) - Q_1(b+l_1^+)w^{q,n}_{(b,l_1)}(i)\right\}p^i(1-p)^{n-i} \underset{Failure}{\overset{Success}{\gtrless}} 0. \quad (46)$$

The asymptotic threshold T_2 of the second majority vote in the JKS method is the maximum p that leads the decision by (46) to the success. Because $0 < Q_1(b+l_1^+) < 1$, the decision criterion of the second majority vote in the JKS method in (46) always succeeds. This is because in order for the received codeword polynomial $r(x)$ to show larger than the MLCR of the codeword polynomial $c(x)$, it is necessary to be satisfied with many conditions for the codeword polynomial $c(x)$ and the error polynomials $e(x)$ as explained in this section.

Moreover, since the one-error-correcting BCH codes have a smaller MLCR than other BCH codes of the same code length, when they are used, T_2 is larger than T_1, unlike when multiple-error-correcting BCH codes of the same code length are used. Note that a small MLCR value of the BCH code means that the size of the null spectrum is small of the corresponding BCH code. Since the one-error-correcting BCH codes have the smallest size of null spectrum, the number of cases where the received codeword polynomial of the corresponding BCH codes has an incorrect SVCR is the largest.

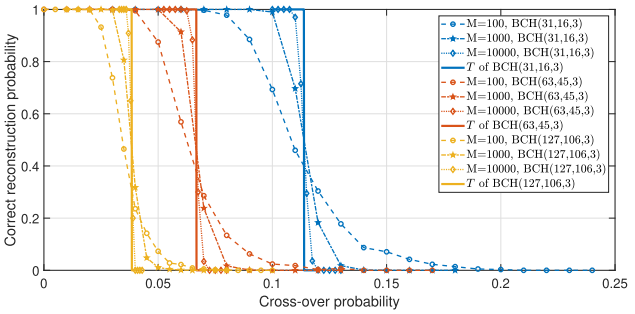


FIGURE 1. Comparison of correct reconstruction probability for three-error-correcting narrow-sense BCH codes according to the number of received codewords.

Finally, in order to succeed in the blind reconstruction using the JKS method, it must be selected as both the correct SVCR in the first majority vote and correct MLCR in the second majority vote. Therefore, we derive the asymptotic threshold T of blind reconstruction of the JKS method by $T = \min(T_1, T_2)$, and such results are shown in Table 2 for various BCH codes.

IV. SIMULATION RESULTS

To verify the validity of the asymptotic threshold derived in Section III, the JKS method is performed for various narrow-sense BCH codes. Specifically, we obtain the correct reconstruction probability according to the number of received codewords for various narrow-sense BCH codes whose weight distributions are known [1]. Note that the correct reconstruction means to correctly estimate the SVCR and MLCR values of the generator polynomial of transmitted BCH code. Also, because the decision criterion for the second majority vote changes depending on whether the BCH code is one-error-correcting or multiple-error correcting, simulations are performed for BCH codes with the one-error-correcting capability and with the three-error-correcting capability to verify the asymptotic threshold, respectively.

Fig. 1 shows the correct reconstruction probability of the JKS method for the three-error-correcting narrow-sense BCH codes of the code lengths 31, 63, and 127 according to the number of received codewords. Note that 1000 simulations are performed to obtain each correct reconstruction probability of the JKS method. Even if the asymptotic threshold T is derived under the assumption that the number of received codewords is sufficiently large, Fig. 1 shows that the cross-over probability for successful blind reconstruction approaches the asymptotic threshold T, as the number of received codeword increases. Therefore, it is positively expected that the cross-over probability for successful blind reconstruction converges to the asymptotic threshold T as the number of received codewords increases, which implies that the analysis and the asymptotic threshold are valid. In other words, it is shown that the transition region, which denotes the region between the maximum cross-over probability for the

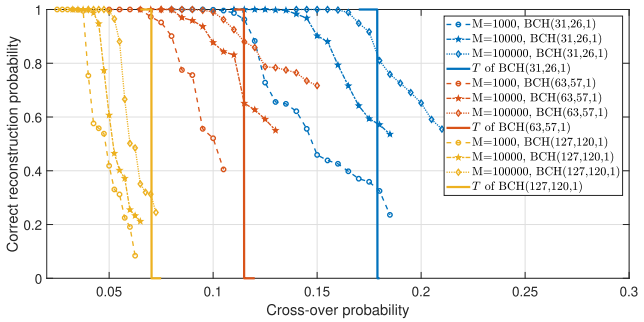


FIGURE 2. Comparison of correct reconstruction probability for one-error-correcting narrow-sense BCH codes according to the number of received codewords.

100% successful reconstruction and the minimum cross-over probability for the 100% failed reconstruction in the JKS method, decreases as the number of received codewords increases until there appears the asymptotic threshold. Thus, it can be seen that as the number of received codewords increases, the correct reconstruction probability of the JKS method converges to the step function in the cross-over probability domain as shown in Fig. 1.

Fig. 2 compares the correct reconstruction probability of the JKS method for various one-error-correcting narrow-sense BCH codes of the code lengths 31, 63, and 127 according to the number of received codewords. Similar to the case of three-error-correcting BCH codes, 1000 simulations are performed to obtain each correct reconstruction probability of the JKS method. Since one-error-correcting narrow-sense binary BCH codes have the smallest null spectrum, the received codeword polynomials showing an incorrect SVCR occur the more frequently compared with the multiple-error-correcting BCH codes. For this reason, the simulation curves for one-error-correcting BCH codes in Fig. 2 are not smooth and the error floor phenomenon is incurred. Nevertheless, Fig. 2 shows a tendency that the cross-over probability for successful blind reconstruction approaches the asymptotic threshold T as the number of received codewords increases. As a result, it is expected that the cross-over probability of successful blind reconstruction will asymptotically approach to the asymptotic threshold. From Figs. 1 and 2, we can see that a defender should not use more than a certain number of codewords of the same BCH code to prevent information leakage and that the challenger needs more than a certain number of codewords to succeed in blind information extraction.

V. DISCUSSION AND CONCLUSION

In this paper, asymptotic analysis of the JKS method [6] is performed, which shows the best blind reconstruction performance of BCH codes, under the assumption that the number of received codewords is sufficiently large. The reason for this assumption is that the blind reconstruction performance heavily depends on how many and which received codewords are used even for the same channel environment. Through asymptotic analysis, an asymptotic threshold is derived, which is the maximum cross-over probability p of BSC for which the generator polynomials of BCH codes are successfully reconstructed by the JKS method. Specifically, asymptotic analysis of the JKS method is performed for each of the two majority votes. Since the JKS method is based on each majority vote on SVCR and MLCR, the occurring probability of the received codeword polynomials showing the correct SVCR and MLCR and the occurring probability of the received codeword polynomials showing the incorrect SVCR and MLCR are derived based on the analysis of consecutive roots of error polynomial according to the number of errors. In other words, the occurring probability of the received codeword polynomial showing the correct SVCR and MLCR is derived, and they are compared with the occurring probability of the received codeword polynomial showing the incorrect SVCR and MLCR. For each majority vote, statistical decision criteria of the JKS method are derived and then used to obtain an asymptotic threshold. Finally, the validity of the derived asymptotic threshold is verified through simulation.

This asymptotic analysis will provide a new performance metric for blind reconstruction methods and give an intuition to the development of blind reconstruction method and the modification of the existing methods. Also, to the defender who wants to prevent information leakage and to the challenger who wants to blindly extract information from the intercepted signals, this asymptotic analysis provides a baseline of the cross-over probability of BSC and the number of received codewords for the successful blind reconstruction. Furthermore, it is expected that the asymptotic analysis proposed in this paper can be applied to other methods for deriving their performance limit. Also, it may be a good future work to derive an asymptotic threshold of the existing or future blind reconstruction methods of various cyclic codes.

REFERENCES

[1] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1995.

[2] H. Lee, C.-S. Park, J.-h. Lee, and Y. Joon Song, "Reconstruction of BCH codes using probability compensation," in *Proc. 18th Asia–Pacific Conf. Commun. (APCC)*, Jeju, South Korea, Oct. 2012, pp. 591–594.

[3] A. D. Yardi, S. Vijayakumaran, and A. Kumar, "Blind reconstruction of binary cyclic codes," in *Proc. Eur. Wireless*, Barcelona, Spain, May 2014, pp. 849–854.

[4] A. D. Yardi, S. Vijayakumaran, and A. Kumar, "Blind reconstruction of binary cyclic codes from unsynchronized bitstream," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 2693–2706, Jul. 2016.

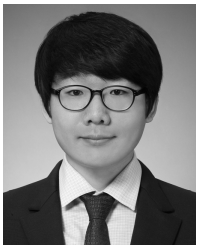
[5] G. Wu, B. Zhang, X. Wen, and D. Guo, "Blind recognition of BCH code based on galois field Fourier transform," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nanjing, China, Oct. 2015, pp. 1–4.

[6] D. Jo, S. Kwon, and D.-J. Shin, "Blind reconstruction of BCH codes based on consecutive roots of generator polynomials," *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 894–897, May 2018.

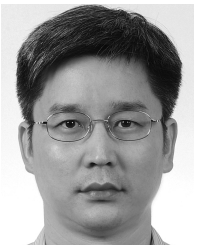
[7] E. Filiol, "Reconstruction of convolutional encoders over GF(q)," in *Proc. Int. Conf. Cryptogr. Coding*, Berlin, Germany, vol. 1335, 1997, pp. 101–109.

[8] A. Valembois, "Detection and recognition of a binary linear code," *Discrete Appl. Math.*, vol. 111, nos. 1–2, pp. 199–218, Jul. 2001.

[9] A. D. Yardi, "Blind reconstruction of binary cyclic codes over binary erasure channel," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Singapore, Oct. 2018, pp. 301–305.
[10] M. Marazin, R. Gautier, and G. Burel, "Blind recovery of k/n rate convolutional encoders in a noisy environment," *EURASIP J. Wireless Commun. Netw.*, vol. 2011, no. 1, pp. 1–9, Dec. 2011.
[11] R. Moosavi and E. G. Larsson, "Fast blind recognition of channel codes," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1393–1405, May 2014.
[12] Z. Jing, H. Zhiping, S. Shaojing, and Y. Shaowu, "Blind recognition of binary cyclic codes," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, pp. 1–17, Dec. 2013.
[13] A. D. Yardi, A. Kumar, and S. Vijayakumaran, "Channel-code detection by a third-parity receiver via the likelihood ratio test," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jun./Jul. 2014, pp. 1051–1055.
[14] M. Cluzeau, "Block code reconstruction using iterative decoding techniques," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 2269–2273.
[15] M. Marazin, R. Gautier, and G. Burel, "Dual code method for blind identification of convolutional encoder for cognitive radio receiver design," in *Proc. IEEE Globecom Workshops*, Honolulu, HI, USA, Nov. 2009, pp. 1–6.



MINKI SONG (Member, IEEE) received the B.S. degree in electronics and communication engineering and the M.S. degree in electronics and computer engineering from Hanyang University, Seoul, South Korea, in 2013 and 2015, respectively, where he is currently pursuing the Ph.D. degree in electronics and computer engineering. His research interests include signal processing, error-correcting codes, and cryptography.



DONG-JOON SHIN (Senior Member, IEEE) received the B.S. degree in electronics engineering from Seoul National University, Seoul, South Korea, the M.S. degree in electrical engineering from Northwestern University, Evanston, USA, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, USA. From 1999 to 2000, he was a Member of Technical Staff with the Wireless Network Division and the Satellite Network Division, Hughes Network Systems, MD, USA. Since 2000, he has been with the Department of Electronic Engineering, Hanyang University, Seoul. His current research interests include signal processing, machine learning, error-correcting codes, sequences, discrete mathematics, and cryptography.