IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 10, 2020, accepted August 29, 2020, date of publication September 7, 2020, date of current version September 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3022460

New Two-Stage Automorphism Group Decoders for Cyclic Codes

CHANKI KIM[1], (Member, IEEE), AND JONG-SEON NO[2], (Fellow, IEEE)
[1]Division of National Supercomputing, Korea Institute of Science and Technology Information (KISTI), Daejeon 34141, South Korea
[2]Department of Electrical and Computer Engineering, INMC, Seoul National University, Seoul 08826, South Korea

Corresponding author: Chanki Kim (carisis@kisti.re.kr)

This work was supported by Institute for Information & Communications Technology Promotion (IITP) Grant funded by the Korea Government, Ministry of Science and ICT (MSIT) (R-20160229-002941, Research on Lightweight Post-Quantum Crypto-Systems for IoT and Cloud Computing).

ABSTRACT Recently, error correcting codes in the erasure channel have drawn great attention for various applications such as distributed storage systems and wireless sensor networks, but many of their decoding algorithms are not practical because they have higher decoding complexity and longer delay. Thus, the automorphism group decoder (AGD) for cyclic codes in the erasure channel was introduced, which has good erasure decoding performance with low decoding complexity. In this paper, we propose new two-stage AGDs (TS-AGDs) for cyclic codes in the erasure channel by modifying the parity-check matrix and introducing the preprocessing stage to the AGD scheme. The proposed TS-AGD is analyzed for binary extended Golay and BCH codes. Also, TS-AGD can be used in the error channel using ordered statistics. Through numerical analysis, it is shown that the proposed decoding algorithm has good erasure decoding performance with lower decoding complexity than the conventional AGD. For some cyclic codes, it is shown that the proposed TS-AGD achieves the performance nearly identical to the maximum likelihood (ML) decoder in the erasure channel and the ordered statistics decoder (OSD) in the error channel.

INDEX TERMS Automorphism group decoder (AGD), Bose-Chaudhuri-Hocquenghem (BCH) codes, cyclic codes, erasure channel, error correcting codes, iterative erasure decoder (IED), ordered statistics decoder (OSD).

I. INTRODUCTION

Research on error correcting codes in the erasure channel is one of the major subjects in information theory. Erasure channel is a typical channel model for distributed storage systems and wireless sensor networks, where the locations of symbol errors are known.

Algebraic codes have a long history from Hamming codes to algebraic geometry codes. The decoders of algebraic codes are designed using the mathematical properties of the codes and thus it is difficult to implement practical decoders for algebraic codes. However, lots of research works for their decoding algorithms have been done to reduce the decoding complexity and delay. In cyclic codes, one-step majority decoding [3] and permutation decoding [4] schemes are exemplary methods which can be practically implemented using their cyclic property in the error channel.

A low complexity iterative decoder can be one of the solution as an implementable decoder and thus, the iterative decoding algorithms and error correcting codes with iterative decoder such as turbo and low-density parity-check (LDPC) codes have been widely studied. In addition, low-complexity iterative erasure decoder (IED) for algebraic codes has also been studied [7]. However, IED has inherently inferior decoding performance compared to the maximum likelihood (ML) decoder and the gap between the decoding performances becomes larger for the algebraic codes, because the sparseness of their parity check matrices is not guaranteed contrary to the LDPC codes. Thus, a possible solution for decoding of algebraic codes is to modify the structure of the decoder in the erasure channel.

Recently, one approach to overcome the inferior decoding performance of IED for the algebraic codes in the erasure channel was proposed, called the automorphism group decoder (AGD) for cyclic codes [8]. AGD uses the permutations of the automorphism group in the middle of the IED procedure. For cyclic codes, the permutation operation can be substituted by the cyclic shift operation for codewords, which are also codewords. It was shown that for some cyclic codes, AGD improves the decoding performance but it requires higher decoding complexity and delay due to repeated decoding process. In addition, many similar concepts have been

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

proposed for cyclic LDPC codes in the error channel such as multiple-bases belief-propagation (MBBP) [9] and revolving iterative decoding (RID) [10], [11].

In order to operate AGD efficiently, it is important to design the appropriate parity-check matrix. However, the conventional design method in [8] includes the problem to find codewords with minimum Hamming weight which is known as NP-hard problem in general. In this paper, we propose a new decoding algorithm, referred to as a two-stage AGD (TS-AGD) which includes a construction algorithm of good parity-check matrix with polynomial-time complexity and also has excellent decoding performance with low decoding complexity for cyclic codes. The proposed decoding process is done in two decoding stages. That is, the first decoding stage finds the cyclic shift values of the received vector for the successful erasure decoding while in the second decoding stage, the erasure decoding process is done for the received vectors cyclically shifted by the cyclic shift values found in the first decoding stage. Further, the proposed TS-AGD algorithm can be implemented by the modified parity-check matrix for the (n, k) cyclic code such that some of the $(n-k)$-tuple column vectors in the parity-check matrix are standard vectors in the appropriate column indices and Hamming weight of the row vectors in the parity-check matrix becomes as low as possible, which requires polynomial-time complexity. The numerical analysis shows that the proposed algorithms are advantageous for extended Golay codes and high-rate BCH codes, where they achieve near-ML decoding performance.

Interestingly, TS-AGD can also be applied to the error channel such as additive Gaussian channel using the motivation of ordered statistics decoding (OSD) [12]. In OSD, k most reliable bits are considered not to be erroneous and declare a decoded word as the codeword which has the same hard-decisioned bits as the received vector in the k most reliable bits, where k is code dimension. It is known that OSD outperforms hard-decision decoding (HDD) such as Euclidean decoder. For codelength n, most reliable k bits and the other $n-k$ bits in OSD are considered as non-erasures and erasures in the erasure channel. respectively and thus, TS-AGD for erasure channel can also decode the errors as OSD can decode. Numerical analysis shows that TS-AGD has near-ML performance in the error channel as well as in the erasure channel.

This paper is organized as follows. In Section II, AGD, IED, and OSD are reviewed. In Section III, the proposed TS-AGD for the binary cyclic codes in the erasure and error channels is introduced by modifying the parity-check matrix and the AGD algorithm, referred to as TS-AGD. In Section IV, numerical analysis of the proposed TS-AGD schemes verifies the performance improvement for the extended Golay and high-rate BCH codes. Finally, the conclusion is given in Section V.

II. PRELIMINARY

In this section, several mathematical notations and abbreviations are defined. For a vector $\boldsymbol{v}$, wt($\boldsymbol{v}$) denotes Hamming weight of vector $\boldsymbol{v}$ and supp($\boldsymbol{v}$) denotes the set of indices of the nonzero components in $\boldsymbol{v}$. The i-th standard vector $\boldsymbol{u}_i$ is the basis vector, where the i-th component of $\boldsymbol{u}_i$ is equal to 1 and the other components are equal to 0. Let $\mathbf{0}$ and $\mathbf{1}$ denote the all-zero and all-one vectors. The decoding procedures of IED and AGD are explained and compared and several definitions are presented in the next subsection. Also suppose that (n, k) linear binary code $\mathcal{C}$ with codelength n and dimension k has an $(n-k) \times n$ parity-check matrix H.

A. ERASURE DECODER: IED AND AGD

1) IED FOR ERASURE CHANNEL

In IED, H can be represented by a bipartite graph $\mathcal{G}$ with n variable nodes (VNs) and $n-k$ check nodes (CNs). Let V and U be sets of variable nodes and check nodes and let d_{v_i} and d_{u_j} be degrees of a variable node $v_i \in V$ and check node $u_j \in U$, respectively, for $0 \le i \le n-1$ and $0 \le j \le n-k-1$. The bipartite graph is then denoted by $\mathcal{G}=(V, U, H)$. In the erasure channel, the variable nodes have two different states, i.e., erasure and non-erasure states, while the check nodes have three states, i.e., decodable, non-decodable, and non-erasure states. The decoding procedure of IED consists of several iterations, where each iteration performs check node update (CNU) and variable node update (VNU) operations sequentially.

The CNU operation is the procedure that each CN finds its state by counting the number of the erasure states of the variable nodes connected to itself. A decodable state of a CN is declared when the number of the connected VNs in the erasure state is 1. If the CN is connected to two or more VNs in the erasure state, then a non-decodable state is declared for the CN. The CNs which are not connected with VNs in the erasure state are called non-erasure states. The VNU operation is a procedure by which VNs in the erasure state are decoded using their connected decodable CNs.

2) AGD FOR ERASURE CHANNEL [8]

AGD can be applied to cyclic codes, where AGD consists of the repeated IED and cyclic shift operations for the received vectors. That is, if there is no decodable check node, then the received vector is cyclically shifted until decodable check nodes are found. If it is found, the IED algorithm is repeatedly applied to the cyclically shifted received vectors.

It is known that the cyclic shift operation is easy to implement with negligible complexity and delay. In the AGD, IED should be performed for each cyclically shifted received vector until the decoding is successful or the number of cyclic shifts is equal to the length of codeword. Although the decoding complexity and delay of the AGD are much higher than those of the IED, the decoding performance of the AGD is much better than that of the IED.

The decoding performance and complexity of IED and AGD can be improved by using an optimized parity-check matrix. For binary case, Hehn uses cyclic orbit generator (cog) and cog family to construct parity-check matrix [8]. Two vectors $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ are said to be cyclically indistinguishable if the cyclic shift of $\boldsymbol{v}_1$ is identical to $\boldsymbol{v}_2$, and otherwise,

cyclically distinguishable. Then, the cog is defined as the cyclically distinguishable binary codeword of a dual code with minimum Hamming weight, which can be used as a row of the parity-check matrix. Cog family is the set of cogs that have the same Hamming autocorrelation property, where the Hamming autocorrelations of cog's are defined as

$$|OO_\tau| = \boldsymbol{cog} \cdot \boldsymbol{cog}^{(\tau)}, |ZO_\tau| = (\mathbf{1} - \boldsymbol{cog}) \cdot \boldsymbol{cog}^{(\tau)},$$
$$|OZ_\tau| = \boldsymbol{cog} \cdot (\mathbf{1} - \boldsymbol{cog}^{(\tau)}), |ZZ_\tau| = (\mathbf{1} - \boldsymbol{cog}) \cdot (\mathbf{1} - \boldsymbol{cog}^{(\tau)}) \quad (1)$$

where $\boldsymbol{cog}^{(\tau)}$ is right cyclic shift of $\boldsymbol{cog}$ by τ and $\cdot$ denotes the inner product. Then, the parity-check matrix is constructed by $n-k$ cogs, where it is desirable to select the $n-k$ cogs from cog families minimizing the upper bounds of Theorem 3.9 in [8].

B. ERROR DECODER: OSD

Let $\boldsymbol{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$ be a binary codeword in a code $\mathcal{C}$ and binary phase shift keying (BPSK) modulation is assumed. Then, a received vector $\boldsymbol{r} = (r_0, \ldots, r_{n-1})$ is denoted as $r_i = (-1)^{c_i} + z_i$, where $z_i \sim \mathcal{N}(0, \frac{N_0}{2})$. Then, we select the k most reliable information (MRI) elements from the received vector, that is, the k elements with the largest values in $|\boldsymbol{r}| = (|r_0|, \ldots, |r_{n-1}|)$ that are linearly independent. Declare a decoded codeword as the codeword which has the same hard-decisioned bits as the received vector in the indices of the k MRI elements.

Procedure of OSD requires the following operations. In order to find the decoded codeword with the same elements as the hard-decisioned k MRI elements, matrix inversion of $(n-k) \times (n-k)$ submatrix with columns except the indices of k MRI bits from H is used. In fact, many of the $n-k$ columns are linearly dependent actually and thus it is needed to reiterate the following procedure for k new MRI bits by removing the column with minimum reliability and adding the dependent column with maximum reliability among the columns except the indices of the k MRI bits. Thus, OSD requires high decoding complexity from these operations. In order to reduce the complexity, locality-aware OSD was introduced recently [16]. Similarly, we will show that low-complexity TS-AGD will be proposed in the error channel using the approach of OSD.

C. SOME DEFINITIONS

In this subsection, some definitions for the proposed TS-AGD algorithms are presented as follows. First, several definitions of binary sequences are presented. Let $s_D(t)$ denote a characteristic sequence of index set D such that $s_D(t) = 1$ if $t \in D$ and $s_D(t) = 0$, otherwise. Two binary sequences frequently used in this paper are defined as follows.

Definition 1 (Erasure Sequence): Erasure sequence $s_e(t)$ is defined as a characteristic sequence of the erasure set S_e, which is the set of indices of erasure symbols in the vector received over the erasure channel.

Definition 2 (Parity Check Sequence): Parity check sequence $s_p(t)$ of the $(n-k) \times n$ parity-check matrix H of the (n, k) cyclic code is a binary sequence of length n defined as

$$s_p(t) = \begin{cases} 1, & \text{if } \mathrm{wt}(\boldsymbol{h}_t) = 1 \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

where $\boldsymbol{h}_t$ is the t-th column of H. Furthermore, let S_p denote the support set of $s_p(t)$, i.e., the set of indices of column vectors with Hamming weight 1.

For column indices of the parity-check matrix H, the components of S_p are called standard indices and otherwise, non-standard indices. Thus, the number of 1's in a length of $s_p(t)$ is smaller than or equal to $n-k$. The Hamming cross-correlation of two binary $\{0, 1\}$ sequences, $s_e(t)$ and $s_p(t)$, is defined as

$$R_H(\tau) = \sum_{t=0}^{n-1} s_e(t) s_p(t+\tau) \quad (3)$$

where $R_H(\tau)$ takes values in $\{0, 1, \ldots, n-k\}$.

In the next section, we propose a modification of parity-check matrix, TS-AGD algorithm, and their analysis.

III. MODIFICATION OF PARITY-CHECK MATRIX AND TWO-STAGE AGD

In this section, we propose a new modification method of the parity-check matrix and a two-stage decoding algorithm, and the result of a numerical analysis for the proposed decoding algorithm is discussed.

A. MODIFICATION OF THE PARITY-CHECK MATRIX

First, we propose a method to modify the parity-check matrix for the proposed two-stage decoding algorithm because the decoding performance of the proposed two-stage decoding algorithm depends on the structure of the parity-check matrix. Here, the following criteria are used for the modification of the parity-check matrix using Definition 2.

⟨*Three criteria for modification of parity-check matrix*⟩

(i) Modify the parity-check matrix such that as many of its column vectors as possible are the standard vectors.
(ii) The parity check sequence of the parity-check matrix has Hamming autocorrelation values as low as possible.
(iii) Each row of the parity-check matrix has as low Hamming weight as possible.

In fact, the best criteria for the parity-check matrix of (n, k) cyclic codes can be described as:

(i) $n-k$ columns of the parity-check matrix are standard vectors.
(ii) All Hamming autocorrelation values of the parity check sequence of the parity-check matrix are equal.
(iii) The Hamming weights of all rows of the parity-check matrix are equal to the minimum Hamming weight of its dual code.

It is easy to check that in order for the parity check sequences to satisfy the second criterion, they should be the characteristic sequences of cyclic difference sets D_C with parameters (n, k, λ) for (n, k) cyclic codes, if their parameters are allowed for the cyclic difference sets. Note that k-subset D_C of a cyclic group G with order n is an (n, k, λ) cyclic difference set if every nonzero component of G has exactly λ representations as a difference $d_c - d_c'$ with components from d_c,

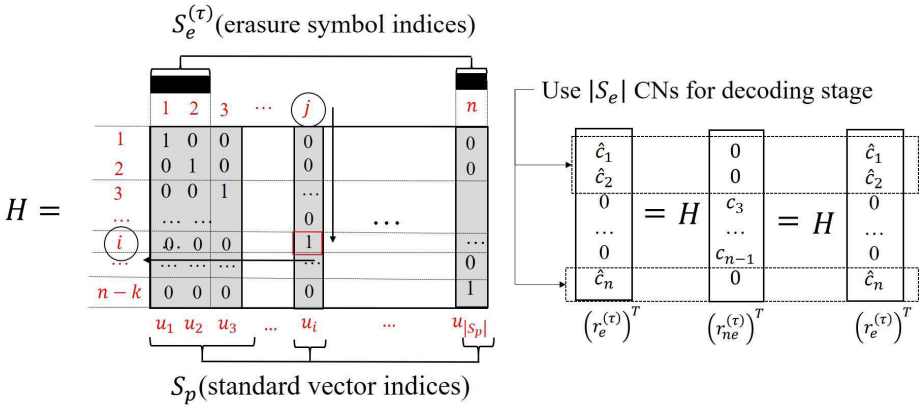

FIGURE 1. The second stage decoding procedure of the TS-AGD of τ such that $R_H(\tau) = |S_e|$.

$d'_c \in D_C$ [13]. It is known that some cyclic codes satisfy the above best criteria. The other criteria can be compromised if one criterion cannot be achieved due to the other criteria. The proposed decoding algorithms together with the proposed modification of the parity-check matrix will be explained in the next subsection.

B. A NEW TWO-STAGE AGD IN THE ERASURE CHANNEL

Using AGD algorithm, we propose a new two-stage AGD of (n, k) cyclic codes in the erasure channel as follows.

1) FIRST DECODING STAGE (PREPROCESSING STAGE)

Find a $\{0, 1\}$ parity check sequence $s_p(t)$ of length n from the parity-check matrix H of an (n, k) cyclic code. Find a $\{0, 1\}$ erasure sequence $s_e(t)$ of length n from the received vector $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1})$. Then, calculate a Hamming cross-correlation as

$$R_H(\tau) = \sum_{t=0}^{n-1} s_p(t)s_e(t+\tau), \ 0 \le \tau \le n-1. \tag{4}$$

Clearly, $R_H(\tau)$ takes values of the nonnegative integers less than or equal to $\min\{|S_e|, |S_p|\}$ because $|S_e|$ is the number of erasure symbols and $|S_p|$ is the number of standard vectors of the parity-check matrix. It can be assumed that the decoding complexity of the preprocessing stage for each τ is analogous to the CNU of one check node. If there exists τ such that $R_H(\tau) = |S_e|$, then proceed to the second decoding stage. If not found, cyclically shift the received vector and proceed to the second decoding stage for $\mathbf{r}^{(\tau)}$ in the order of τ's such that values of $R_H(\tau)$ are decreasing, where $\mathbf{r}^{(\tau)}$ is a cyclic shift of $\mathbf{r}$ by τ.

2) SECOND DECODING STAGE (IED Stage)

In the second decoding stage, the IED algorithm is used for decoding of the cyclically shifted received vector according to the values of $R_H(\tau)$. Recall that S_p is the support set of $s_p(t)$. Let $\mathbf{r}^{(\tau)} = (r_{n-\tau}, r_{n-\tau+1}, \ldots, r_{n-1}, r_0, \ldots, r_{n-\tau-1})$ be a received vector cyclically shifted by τ, where erasure symbols are located in the indices in $S_e^{(\tau)} = \{t | s_e(t-\tau) = 1, 0 \le t \le n-1\}$.

(i) For τ such that $R_H(\tau) = |S_e|$: It is clear that $S_e^{(\tau)} \subseteq S_p$, that is, all of the erasure symbols in $\mathbf{r}^{(\tau)}$ are located in the indices of standard vectors. Note that the i-th component of the received vector $\mathbf{r}$ is expressed as the transmitted symbol c_i for a non-erasure symbol and $\hat{c}_i$ for an erasure symbol. Suppose that $\mathbf{r}^{(\tau)}$ can be split into two n-tuple vectors as

$$\mathbf{r}^{(\tau)} = \mathbf{r}_e^{(\tau)} + \mathbf{r}_{ne}^{(\tau)} \tag{5}$$

where the j-th component of $\mathbf{r}_e^{(\tau)}$ is denoted as $\hat{c}_j$ for $j \in S_e^{(\tau)}$ and otherwise, 0 and the j-th component of $\mathbf{r}_{ne}^{(\tau)}$ is equal to the j-th component of $\mathbf{r}^{(\tau)}$ for $j \notin S_e^{(\tau)}$ and otherwise, 0. In general, the syndrome vector should be zero as

$$S = H(\mathbf{r}^{(\tau)})^\top = H(\mathbf{r}_e^{(\tau)})^\top + H(\mathbf{r}_{ne}^{(\tau)})^\top = 0 \tag{6}$$

where $\top$ is a transpose of a vector and thus

$$(\mathbf{r}_e^{(\tau)})^\top = H(\mathbf{r}_e^{(\tau)})^\top = H(\mathbf{r}_{ne}^{(\tau)})^\top. \tag{7}$$

If the j-th column vector of H is the i-th standard vector $\boldsymbol{u}_i$, $\hat{c}_j$ is equal to the i-th component of $H(\mathbf{r}_{ne}^{(\tau)})^\top$ because $R_H(\tau) = |S_e|$. Clearly, each j-th column for $j \in S_e \subset S_p$ has a different standard vector $\boldsymbol{u}_i$. In this case, we can recover all of the erasure symbols by $H(\mathbf{r}_{ne}^{(\tau)})^\top$ in one iteration, which is described in Fig. 1.

(ii) For τ such that $R_H(\tau) = |S_e| - 1$: In this case, we have one erasure symbol in the non-standard vector of H and the other erasure symbols are located in the column indices in S_p. Here, the decoding process is done in two steps, that is, one for one erasure symbol in the non-standard vector of H and the other for the other erasure symbols with indices in S_p. Suppose that the set of erasure symbol indices is given as $\{e_0, e_1, \ldots, e_{z-1}\}$, where z is the number of erasure symbols. Suppose that the e_j-th column is the i_j-th standard vector $\boldsymbol{u}_{i_j}$, $0 \le j \le z-2$, and the e_{z-1}-th column of H is a non-standard vector. We also have $|S_p| - z + 1$ standard vectors in H, where non-erasure symbols are located. In the first decoding step, assume that for $z \le i_j \le |S_p|$, some i_j-th component of the e_{z-1}-th column of H is equal to 1. Then, using the

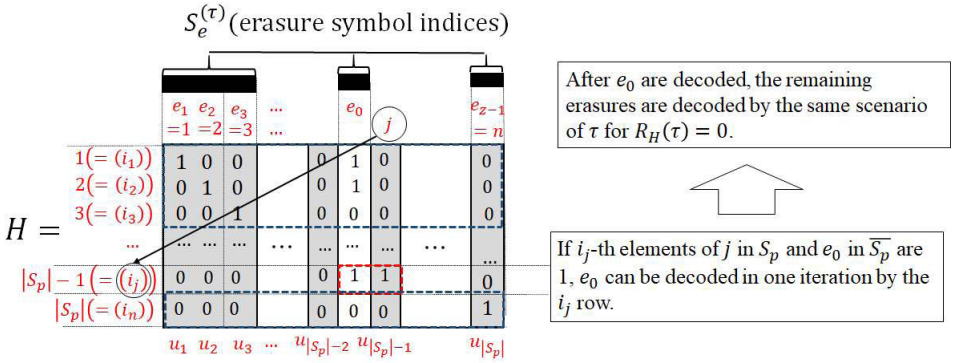

FIGURE 2. The second stage decoding procedure of the TS-AGD of τ such that $R_H(\tau) = |S_e| - 1$.

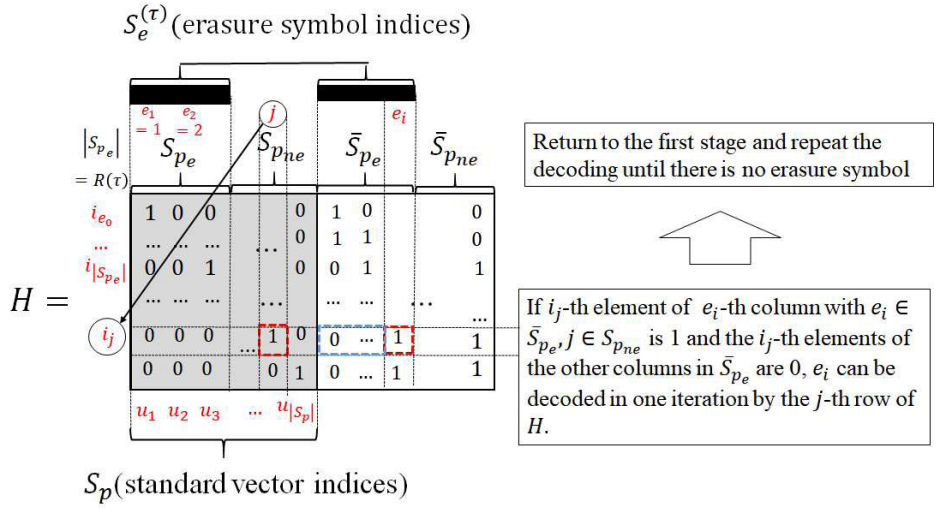

FIGURE 3. The second stage decoding procedure of the TS-AGD of τ such that $R_H(\tau) \leq |S_e| - 2$.

i_j-th row of H, the erasure symbol $\hat{c}_{e_{z-1}}$ can be recovered because there is no erasure symbol except for $\hat{c}_{e_{z-1}}$ at the positions of component 1 in the i_j-th row of H. Then, we go to the second decoding stage, which is the same as that of $R(\tau) = |S_e|$. If the i_j-th component of the e_{z-1}-th column of H is 0, decoding of the first step cannot be successful because e_{z-1} disappears in the IED procedure. If the first decoding step is not successful, then we try to decode it for other τ values such that $R_H(\tau) = |S_e| - 1$. The second decoding procedure is described in Fig. 2.

(iii) For τ such that $R_H(\tau) \leq |S_e|-2$: Let $\bar{S}_p = \{t | s_p(t) = 0\}$, i.e., the complement of S_p. Let $S_p = S_{p_e} \cup S_{p_{ne}}$, where S_{p_e} is a subset of indices such that the erasure symbols exist and $S_{p_{ne}} = S_p \backslash S_{p_e}$. Similarly, let $\bar{S}_p = \bar{S}_{p_e} \cup \bar{S}_{p_{ne}}$ and then clearly, $|S_{p_e}| = R_H(\tau)$. For $j \in S_{p_{ne}}$, suppose that the j-th component of the e_i-th column of H with $e_i \in \bar{S}_{p_e}$ is 1 and that the j-th components of the other columns with indices in $\bar{S}_{p_e} \setminus \{e_j\}$ of H are all zero and further, there exists $\boldsymbol{u}_j$ in the columns with indices in $S_{p_{ne}}$. Then, we can recover the erasure symbol with index e_i. That is, all erasure symbols except for $\hat{c}_{e_i}$ are disappeared in the inner product of the j-th row of H and the received vector cyclically shifted by τ and thus $\hat{c}_{e_i}$ can be recovered.

To decode the remaining erasure symbols, it is needed to return to the preprocessing stage to find the values of τ's with higher values of $R_H(\tau)$. The second decoding stage of the proposed two-stage decoding algorithm is described in Fig. 3.

Overall, the decoding procedure of TS-AGD is described in the flowchart of Fig. 4.

C. ANALYSIS OF MODIFICATION CRITERIA FOR THE PARITY-CHECK MATRIX

This subsection analyzes the modification criteria of H for (n, k) cyclic codes. The first criterion is related to the number of standard vectors, that is, the number of t's such that $s_p(t) = 1$, which is less than or equal to $n - k$. As described in the previous subsection, the proposed TS-AGD procedure can be done for the cyclically shifted received vector $\mathbf{r}^{(\tau)}$ such that $R_H(\tau)$ has higher values. As the number of 1's in $s_p(t)$ increases, it is more probable for $R_H(\tau)$ to have higher values.

The second criterion is how to locate the standard vectors in the parity-check matrix. It is not easy to prove the second criterion and thus the following theorem replaces the proof of the second criterion. First, we need a lemma to prove the following theorem.

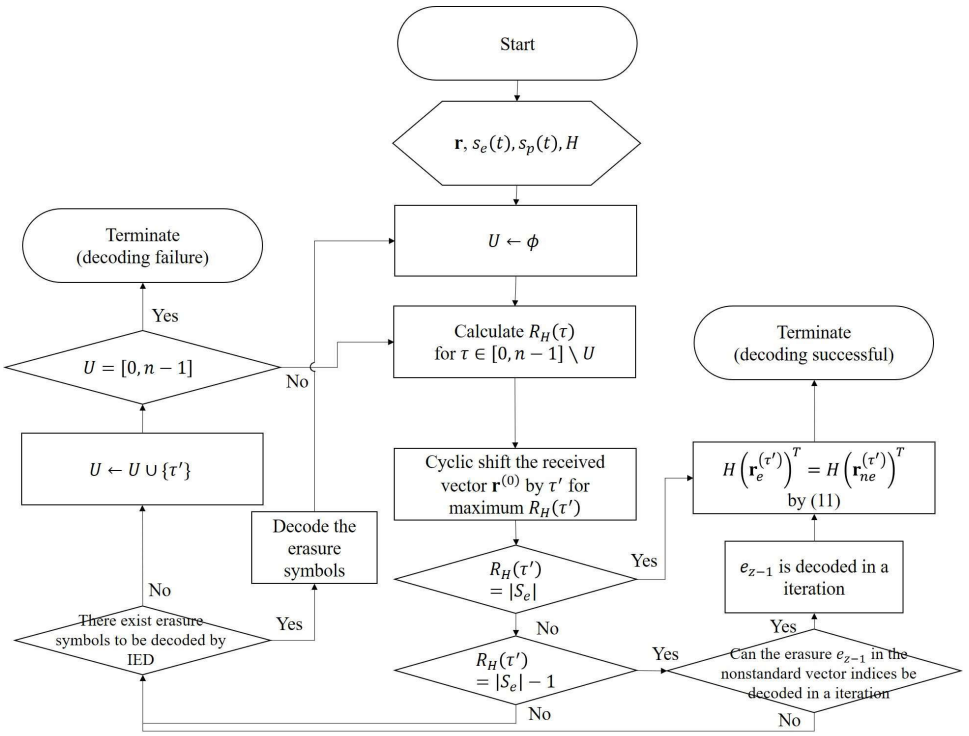

FIGURE 4. Flowchart of the TS-AGD algorithm.

Lemma 1 (Bonferroni Inequality [15]): Let E_i, $i \in A$, be sets of components. Then we have the following inequality as

$$\sum_{I\subset A,|I|=1} |E_i| - \sum_{I\subset A,|I|=2} \left|\bigcap_{i\in I} E_i\right| \leq \left|\bigcup_{i\in A} E_i\right| \leq \sum_{I\subset A,|I|=1} |E_i| - \frac{2}{|A|} \sum_{I\subset A,|I|=2} \left|\bigcap_{i\in I} E_i\right|. \quad (8)$$

Theorem 1: In the upper bound of Lemma 1, the number of occurrences of $R_H(\tau) \geq |S_e| - 1$ for $0 \leq \tau \leq n-1$ is maximized if the parity check sequence of the modified parity-check matrix has a particular constant dependent on $|S_e|$ autocorrelation values.

Proof: First, it is desirable for the proposed decoding algorithm to successfully decode more erasure patterns, which is possible if $R_H(\tau) \geq |S_e| - 1$. Thus, we have to modify the parity-check matrix, for which $R_H(\tau) \geq |S_e| - 1$ is most common for as many shift values τ as possible. The following two cases are considered.

(i) $R_H(\tau) = |S_e|$:
This means that $S_e^{(\tau)} \subseteq S_p$. It is easy to check that in $R_H(\tau)$, it is equivalent to cyclically shift $s_p(t)$ instead of $s_e(t)$. Let $S_p^{(\tau)}$ be the support set of $s_p(t+\tau)$. Let E_τ be the set of erasure patterns which can be successfully recovered by $s_p(t+\tau)$. Then, we have $|E_\tau| = \binom{|S_p|}{|S_e|}$, which leads to

$$\sum_{\tau=0}^{n-1} |E_\tau| \leq n\binom{|S_p|}{|S_e|}. \quad (9)$$

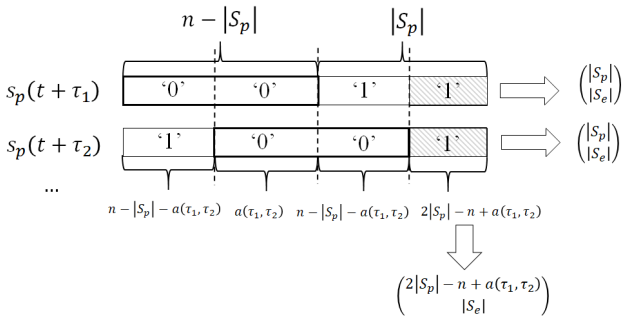

FIGURE 5. The number of doubly counted erasure patterns for τ such that $R_H(\tau) = |S_e|$.

It is easy to check that doubly counted erasure patterns are included in (9), which should be excluded. If the shaded parts in Fig. 5 include all the erasure symbols, those erasure patterns are doubly counted, where $a(\tau_1, \tau_2)$ denotes the number of pairs $\left(s_p(t+\tau_1), s_p(t+\tau_2)\right) = (1,1)$. Thus we have $\binom{2|S_p|+a(\tau_1,\tau_2)-n}{|S_e|}$ doubly counted erasure patterns. Using Lemma 1, the number of erasure patterns which are successfully decoded by $s_p(t)$ is bounded as

$$\left|\bigcup_{\tau=0}^{n-1} E_\tau\right| \leq \sum_{\tau=0}^{n-1} |E_\tau| - \frac{2}{n}\sum_{\tau_1,\tau_2} \left|E_{\tau_1} \cap E_{\tau_2}\right| \leq n\binom{|S_p|}{|S_e|} - \frac{2}{n}\sum_{\tau_1,\tau_2} \binom{2|S_p| + a(\tau_1,\tau_2) - n}{|S_e|}. \quad (10)$$

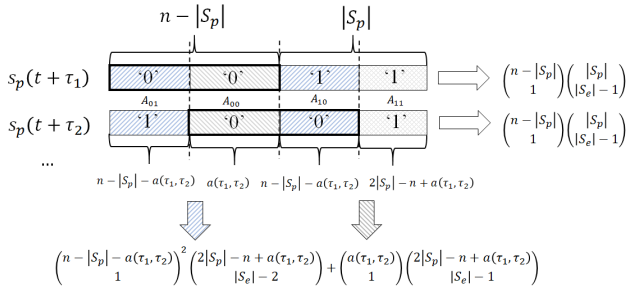

FIGURE 6. The number of doubly counted erasure patterns for τ such that $R_H(\tau) = |S_e| - 1$.

(ii) $R_H(\tau) = |S_e| - 1$:
In this case, the index of one erasure symbol is in $\bar{S}_p$ and the indices of the other erasure symbols are in S_p. Thus, the total number of such erasure patterns is $\binom{n-|S_p|}{1}\binom{|S_p|}{|S_e|-1}$, where doubly counted erasure patterns are included. There are two cases of doubly counted erasure patterns as shown in Fig. 6.

a) Each of two erasure symbols is located in A_{10} and A_{01}, respectively and the other erasure symbols are located in A_{00}, which are counted as $\binom{n-|S_p|-a(\tau_1,\tau_2)}{1}^2\binom{2|S_p|-n+a(\tau_1,\tau_2)}{|S_e|-2}$.

b) One erasure symbol is located in A_{11} and the other erasure symbols are located in A_{00}, which are counted as $\binom{a(\tau_1,\tau_2)}{1}\binom{2|S_p|+a(\tau_1,\tau_2)-n}{|S_e|-1}$. Similarly, from Lemma 1, the number of erasure patterns which are successfully decoded by $s_p(t)$ is given as

$$\begin{aligned}\left|\bigcup_{\tau=0}^{n-1} E_\tau\right| &\le \sum_{\tau=0}^{n-1}|E_\tau| - \frac{2}{n}\sum_{\tau_1,\tau_2}\left|E_{\tau_1}\cap E_{\tau_2}\right| \\ &\le n\binom{n-|S_p|}{1}\binom{|S_p|}{|S_e|-1} \\ &\quad - \frac{2}{n}\sum_{\tau_1,\tau_2\in[0,n-1]}\left(\binom{n-|S_p|-a(\tau_1,\tau_2)}{1}^2\right. \\ &\quad \times\binom{2|S_p|+a(\tau_1,\tau_2)-n}{|S_e|-2}+\binom{a(\tau_1,\tau_2)}{1} \\ &\quad \left.\times\binom{2|S_p|+a(\tau_1,\tau_2)-n}{|S_e|-1}\right). \qquad (11)\end{aligned}$$

In order to maximize the upper bounds in (10) and (11), the second terms of the right hand sides should be minimized, which can be solved by the convex optimization as described in Appendix. That is, it is derived in Appendix that maximizing the upper bound on the number of occurrences of $R_H(\tau) \ge |S_e| - 1$ for $0 \le \tau \le n-1$ by convex optimization occurs when the autocorrelation values of $s_p(t)$ are constant. Thus, we prove the theorem. ■

The third criterion is related to the performance of the decoder, that is, H with the minimum Hamming weight of rows can have better decoding performance in IED as mentioned in [8] as cog, because more erasure symbols are removed in the inner product of the received vector and the rows with the minimum Hamming weight of H.

D. ANALYSIS OF DECODING COMPLEXITY OF TS-AGD IN THE ERASURE CHANNEL

Decoding complexity of TS-AGD in the erasure channel is analyzed as follows. In the decoding stage, it requires a large number of iterations and high decoding complexity. In the preprocessing stage, TS-AGD derives the order of decoding by computing cross-correlation of the parity check sequence and erasure sequence. TS-AGD decodes in order of more successful decoding cases of cyclic shift values τ but the conventional AGD decodes for all the possible τ without considering the decoding order.

We analyze the decoding complexity using integer addition and XOR operation. Complexities of each integer addition and each XOR operation between two binary integer values are considered as 1, respectively and then integer additions and XOR operations among l values are done by $l-1$ serialized operations between two integers in the binary form. The complexity of preprocessing stage will be counted by occurrence of integer additions as in Fig. 7 and the complexity for search of $\tau's$ with high correlation values is ignored because it has low complexity. For each iteration of decoding process, both CNU and VNU operations are performed, where CNU operation requires $(d_c-1)(n-k)$ integer additions as in Fig. 8 and VNU operation requires (d_c-2) XOR for each decodable erasure symbol as in Fig. 9. In order to compute the decoding complexity by the numerical analysis, we consider XOR and integer addition operations as 1, respectively, where numerical approach will be used for the following discussions including Figs. 11, 13, and 16 in Section IV.

E. TS-AGD IN THE ERROR CHANNEL

In this subsection, we propose a new method of low-complexity TS-AGD in the error channel motivated by OSD. In order to use TS-AGD in the erasure channel, we treat $n-k$ bits except MRI bits as erasures regardless of their linearly independent columns. Then, TS-AGD decodes the codeword until decoding successfully or reaching a stopping set. If stopping set is found, the decoder treats one of the remaining erasures with the maximum reliability as non-erasure and it can proceed to erasure decoding. In this way, the decoder always obtain a decoded codeword.

Generally, many of the $n-k$ columns are linearly dependent and thus, linearly independent $n-k$ columns after many iterations in OSD should contain several less reliable bits as MRI bits. Instead, we consider an alternative method to decode the received codewords using the $n-k$ bits as erasures and change the erasure bit to non-erasure bit only when stopping set exists after iterations.

For complexity of TS-AGD, it is definitely lower than OSD. As aforementioned in Section II-B, the operations related with high decoding complexity of OSD are matrix inversion and the iterations by searching $n-k$ linearly independent columns. For the matrix inversion with $\mathcal{O}(n^3)$, TS-AGD is lower because it is based on the iterative decoding with $\mathcal{O}(n)$ for iterations. Also, the iterated operation by searching $n-k$ linearly independent columns for matrix

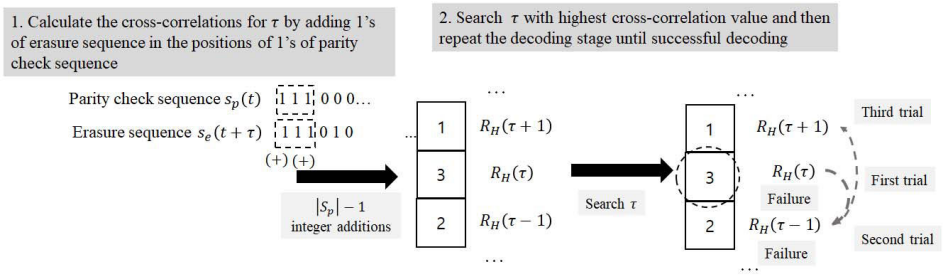

FIGURE 7. Complexity analysis of preprocessing operation for TS-AGD.

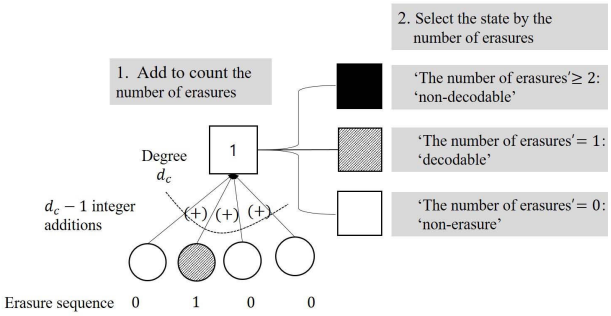

FIGURE 8. Complexity analysis of CNU operation for AGD and TS-AGD.

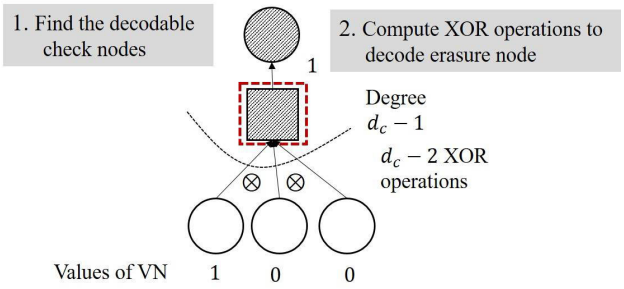

FIGURE 9. Complexity analysis of VNU operation for AGD and TS-AGD.

inversion is not required in the TS-AGD. For FER performance in the error channel, TS-AGD has comparable performance to OSD for the codes that TS-AGD has near-ML performance such as extended Golay and high-rate BCH codes, which will be given in the numerical analysis of the next section.

IV. NUMERICAL ANALYSIS FOR TS-AGD

In this section, the proposed TS-AGD is shown to be near-ML performance for some cyclic codes in the erasure channel such as extended Golay codes and double and triple-error correcting BCH codes. For extended Golay codes, the proposed modification of parity-check matrix can achieve the decoding performance identical to that of the ML decoder. For double- and triple-error correcting BCH codes, AGD and TS-AGD have the near-ML decoding performances. Regarding decoding complexity, additional complexity by preprocessing stage for TS-AGD may increase the decoding complexity but for long codelength, overall decoding complexity of TS-AGD becomes lower than that of AGD.

A. (24, 12, 8) EXTENDED GOLAY CODE

Extended Golay code is not a cyclic code, but it is cyclic except for the last parity bit. Thus, we can apply the AGD and the proposed TS-AGD. For comparison, we will use parity-check matrix $H_{[24,12],*}$ in [8].

A systematic parity-check matrix H_{sys} is constructed where the 12×12 submatrix by the first 12 columns is identity matrix, i.e., parity check sequence of H_{sys} is $s_p(t) = (111111111111000000000000)$. The modified parity-check matrix based on the three proposed criteria can be given as

$$H_m = \begin{pmatrix} 100010000000011000111010 \\ 010010100100001010100010 \\ 001000000010011010100110 \\ 000100100110011000010010 \\ 000011100010001000001110 \\ 000010110000010010010110 \\ 000010001110000000110110 \\ 000000100101010000101110 \\ 000000100010100010111010 \\ 000010000110010110001010 \\ 000000000100001011011110 \\ 000010100110011010111101 \end{pmatrix} \tag{12}$$

where the first 11 standard column vector indices are determined by the cyclic difference set with parameters (23, 12, 5) and the last standard vector is located in the extended bit. The last row of H_m has the Hamming weight of 12, which is larger than the minimum Hamming weight 8. Thus, we can further modify it by replacing the last row by sum of the first row and the last row as

$$H_A = \begin{pmatrix} 100010000000011000111010 \\ 010010100100001010100010 \\ 001000000010011010100110 \\ 000100100110011000010010 \\ 000011100010001000001110 \\ 000010110000010010010110 \\ 000010001110000000110110 \\ 000000100101010000101110 \\ 000000100010100010111010 \\ 000010000110010110001010 \\ 000000000100001011011110 \\ 100000100110000010000111 \end{pmatrix} \tag{13}$$

where the last row has the minimum Hamming weight 8 but the first column is not a standard vector. The further modifi-

TABLE 1. The undecodable erasure patterns by the modified H for the (24, 12, 8) binary extended Golay code.

The number of erasures	Total number of erasure patterns	TS-AGD and AGD of H_{sys}	TS-AGD and AGD of H_m	TS-AGD and AGD of H_A	TS-AGD and AGD of H_B and H_{Hehn}	TS-AGD and AGD of H_C and ML
≤ 7		0	0	0	0	0
8	735471	759	759	759	759	759
9	1307504	12144	12144	12144	12144	12144
10	1961256	92000	91080	91080	91080	91080
11	2496144	460253	426581	425178	425040	425040
12	2704156	1515792	1344005	1325536	1322179	1313116

cation is done by replacing the i-th row with the sum of the i-th row and the last row of H_m, $1 \leq i \leq 11$ and the last row with the first row of H_m as

$$H_B = \begin{pmatrix} 100000100110000010000111 \\ 010000000010010000011111 \\ 001010100100000000011011 \\ 000110000000000010101111 \\ 000001000100010010110011 \\ 000000010110001000101011 \\ 000000101000011010001011 \\ 000010000011001010010011 \\ 000010000100111000000111 \\ 000000100000001100110111 \\ 000010100010010001100011 \\ 100010000000011000111010 \end{pmatrix}. \quad (14)$$

In fact, the first columns of H_A and H_B have Hamming weight 2. Then the parity check sequences of H_p, H_A, and H_B are given as

$$s_{p,H_m}(t) = \left(111101011001100101000001\right) \quad (15)$$
$$s_{p,H_A}(t) = \left(011101011001100101000001\right) \quad (16)$$
$$s_{p,H_B}(t) = \left(011101011001100101000000\right). \quad (17)$$

In the (24, 12, 8) extended Golay code, any of the modified parity check matrices cannot achieve the same performance as that of the ML decoder. However, the TS-AGD by adding redundant check equations to H_B can give us the same decoding performance as the ML decoder, which is given as

$$H_C = \begin{pmatrix} H_B \\ H'_A \end{pmatrix} \quad (18)$$

where H'_A is a submatrix composed of nine rows out of the first 11 rows of H_A. Fig. 10 shows the relationship among the various modified parity check matrices. Table 1 shows the decoding performance of the proposed TS-AGD and AGD with H_{sys}, H_m, H_A, H_B, H_{Hehn}, and H_C, where H_C shows decoding performance identical to that of the ML decoder and better decoding performance than the decoding algorithm by Hehn. In AGD, decoding complexity of the modified H's is lower than H_{Hehn} except H_c as in Fig. 11, where H_C is the highest decoding complexity due to additional rows of the parity-check matrix. For the number of iterations of TS-AGD, H_m and H_A are lower than others because $|S_p| = n-k$, which

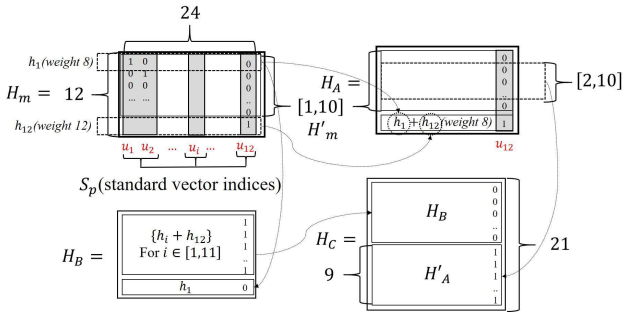

FIGURE 10. Modifications of the parity-check matrix in the (24, 12, 8) extended binary Golay code.

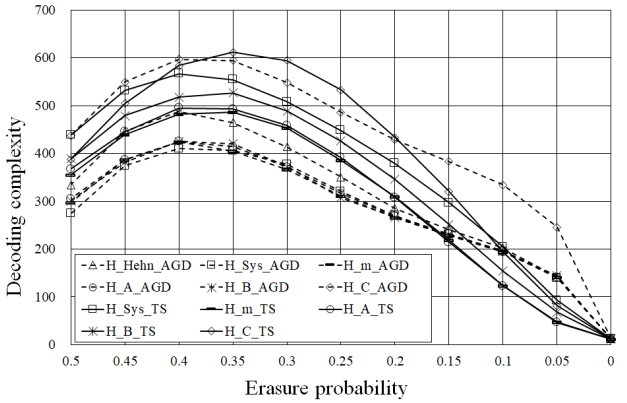

FIGURE 11. Decoding complexity of AGD and TS-AGD for (24, 12, 8) extended Golay code.

is larger than the others. For decoding complexity, decoding complexity of TS-AGD is lower than that of AGD for low erasure probabilities. Among the modified H's of TS-AGD, the decoding complexity is proportional to the number of iterations except H_C.

B. HIGH-RATE BINARY BCH CODES

Binary primitive BCH codes are widely used due to large designed distance and guaranteed decoding performance for certain number of errors and erasures. However, BCH codes require inherently high decoding complexity and their performance is degraded for large n and k.

The proposed TS-AGD can overcome the disadvantages of BCH codes by the low-complexity decoding with improved performance compared to AGD. Here, the proposed TS-AGD for the double-error correcting $(n, k, d) = (63, 51, 5), (127, 113, 5), (255, 239, 5)$ and triple-error correcting $(63, 45, 7), (127, 106, 7), (255, 231, 7)$ BCH codes is numerically analyzed in the erasure and error channel.

In general, $s_p(t)$ of the BCH code is generated by the cyclic difference set but there are some cases that the cyclic difference set does not exist for the parameters of the BCH code. Instead S_p can be constructed using the union of cyclotomic cosets of the finite field as an alternative construction method. In this case, $s_p(t)$ does not have constant but relatively low values of autocorrelation. Thus, this construction method of $s_p(t)$ also results in good decoding performance. For $(63, 51, 5)$ and $(63, 45, 7)$ BCH codes, S_p is constructed using cyclotomic cosets whose coset leaders are $\{\alpha, \alpha^3\}$ and $\{\alpha, \alpha^3, \alpha^{11}\}$, where α is a primitive element of F_{2^6}. Similarly, S_p's of $(127, 113, 5)$ and $(127, 106, 7)$ BCH codes use cyclotomic cosets whose coset leaders are $\{\alpha^3, \alpha^5\}$ and $\{\alpha^3, \alpha^5, \alpha^{11}\}$, where α is a primitive element of F_{2^7}. Lastly, S_p's of $(255, 239, 5)$ and $(255, 231, 7)$ BCH codes use cyclotomic cosets whose coset leaders are $\{\alpha^7, \alpha^{11}\}$, and $\{\alpha^7, \alpha^{11}, \alpha^{13}\}$, where α is a primitive element of F_{2^8}.

For comparison of the codes with $n = 63, 127$, FER performance of ML is used as a numerical calculated values by Monte-Carlo method. However, we use a $(260, 234)$ regular LDPC code for comparison of $n = 255$ because it requires high complexity to induce the FER performance of ML using Monte-Carlo method.

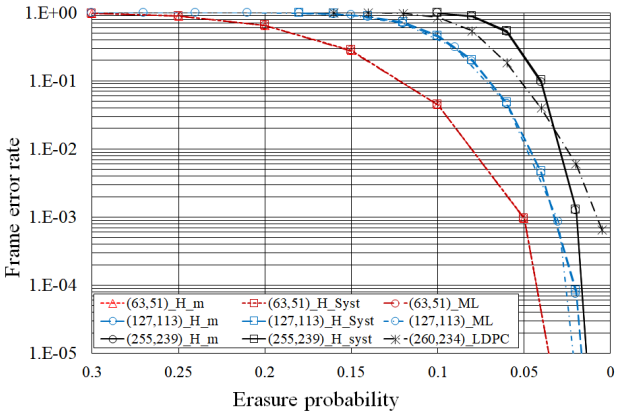

FIGURE 12. Frame error rate of (63, 51), (127, 113), (255, 239) double-error correcting BCH codes by AGD and TS-AGD for H_m and H_{sys}.

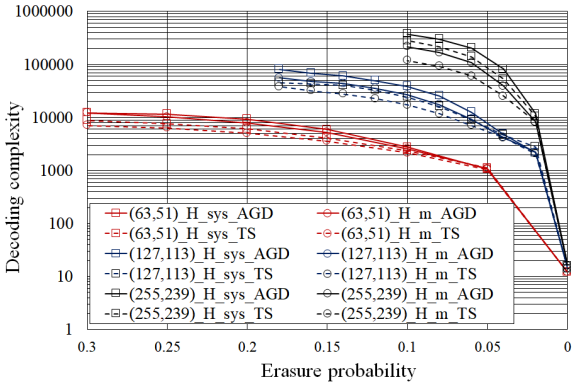

FIGURE 13. Decoding complexity of (63, 51), (127, 113), (255, 239) double-error correcting BCH code by AGD and TS-AGD for H_m and H_{sys}.

little difference among H_m, H_{sys}, and ML. Note that FER performance of AGD and TS-AGD are identical because both of them try all the cyclic shifted cases before they declare decoding failure. However, decoding complexity in Fig. 13 shows that H_m has lower decoding complexity than H_{sys} and their gap becomes larger for long codelength. For the decoding complexity of AGD and TS-AGD, TS-AGD has lower complexity than AGD and their gap becomes larger for long codelength. Therefore, the proposed TS-AGD with H_m has lowest decoding complexity for these codes.

In the error channel, FER performance of OSD, TS-AGD, and HDD of $(127, 113)$ BCH code is given in Fig.14, where TS-AGD has better performance than HDD but little degraded performance than OSD. However, TS-AGD can decode the code with lower complexity and thus, TS-AGD can be used for the lower complexity applications.

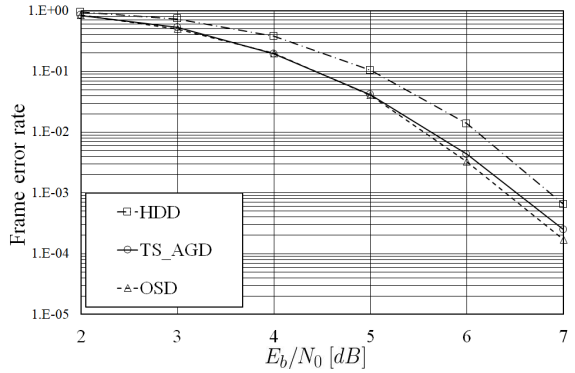

FIGURE 14. FER performance of OSD, TS-AGD, and HDD of (127, 113) double-error correcting BCH codes in the error channel.

1) DOUBLE-ERROR CORRECTING BCH CODES

Here, we analyze FER performance and decoding complexity of AGD and TS-AGD for double error correcting BCH codes in the erasure channel. For the modification of parity-check matrix, H_m and H_{sys} are compared, where the optimization of the upper bound by the second criterion leads to improve the decoding performance for these codes. First, FER performance is given in Fig. 12 showing that there is

2) TRIPLE-ERROR CORRECTING BCH CODES

For FER performance of the triple-error correcting BCH codes, Fig. 15 shows that there is little difference among H_m, H_{sys}, and ML, but their gap is larger than that of the double-error correcting BCH codes. Note that FER performance of AGD and TS-AGD is identical because both of them try to all the cyclic shifted cases before they declare decoding failure. However, decoding complexity in Fig. 16

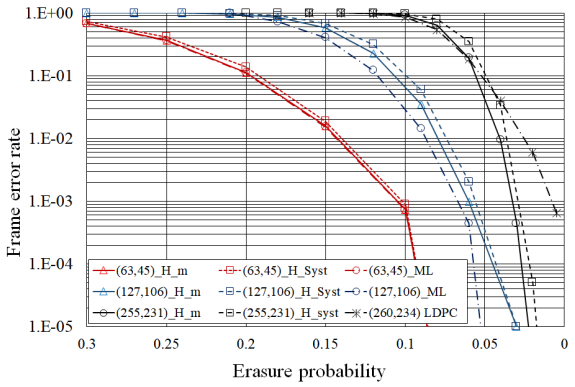

FIGURE 15. Frame error rate of (63, 45), (127, 106), (255, 231) triple-error correcting BCH codes by AGD and TS-AGD for H_m and H_{sys}.

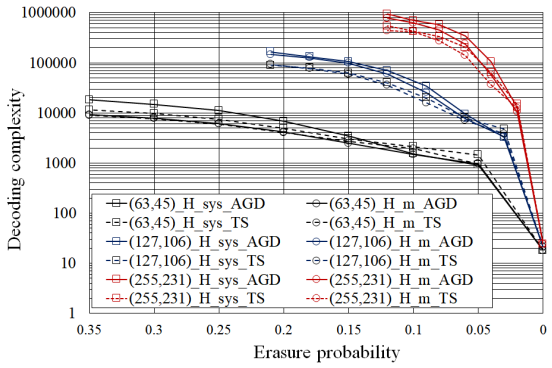

FIGURE 16. Decoding complexity of (63, 45), (127, 106), (255, 231) triple-error correcting BCH codes by AGD and TS-AGD for H_m and H_{sys}.

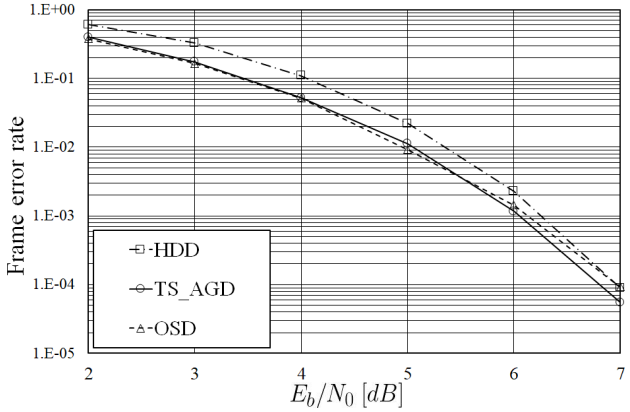

FIGURE 17. FER performance of OSD, TS-AGD, and HDD of (63, 45) triple-error correcting BCH code in the error channel.

shows that H_m has lower decoding complexity than H_{sys} and their gap becomes larger for long codelength. For the decoding complexity of AGD and TS-AGD, TS-AGD has lower complexity than AGD and their gap becomes larger for long codelength. Therefore, the proposed TS-AGD with H_m has lowest decoding complexity for these codes.

In the error channel, FER performance of OSD, TS-AGD, and HDD of (63, 45) BCH code is given in Fig. 17. TS-AGD has better performance than HDD but worse performance than OSD in low E_b/N_0. However, FER performance of HDD and TS-AGD outperforms that of OSD in high E_b/N_0 contrary to (127, 113) BCH code because less reliable bits are included in k MRI bits in order to satisfy linear independence of the corresponding columns as $n - k$ is larger. On the average, OSDs of (127, 113) and (63, 45) BCH codes treat $(k + 1.588)$-th and $(k + 1.76)$-th reliable bit as least reliable MRI bit. In contrary, TS-AGD firstly uses most reliable k bits and substitute other bits only when the stopping set exists and thus, TS-AGD is less influenced by less reliable bits. Also, TS-AGD can decode the code with lower complexity and thus, TS-AGD can be used for the lower complexity applications.

V. CONCLUSION

In this paper, a new TS-AGD for binary cyclic codes was proposed by modifying their parity-check matrix. Modification criteria of the parity-check matrix was proposed and the proposed TS-AGD algorithms were shown to be able to reduce the average number of iterations and the decoding complexity. The extended Golay and BCH codes were considered for the proposed TS-AGD algorithms, where they achieve the near-ML and OSD performances with low decoding complexity in the erasure and error channels.

APPENDIX
PROOF OF MAXIMIZATION OF THE UPPER BOUNDS IN (10) AND (11)

The objective functions to be minimized are as follows:

1) For $R_H(\tau) = |S_e|$, the objective function is $\sum_{\tau_1,\tau_2} \binom{2|S_p|+a(\tau_1,\tau_2)-n}{|S_e|}$.
2) For $R_H(\tau) = |S_e| - 1$, the objective function is

$$\sum_{\tau_1,\tau_2} \binom{n-|S_p|-a(\tau_1,\tau_2)}{1}^2 \binom{2|S_p|+a(\tau_1,\tau_2)-n}{|S_e|-2} + \binom{a(\tau_1,\tau_2)}{1}\binom{2|S_p|+a(\tau_1,\tau_2)-n}{|S_e|-1}. \quad (19)$$

It is easy to check that the following constraints are used for optimization:

(i) For all τ_1 and τ_2, $0 \le a(\tau_1, \tau_2) \le n - |S_p|$.
(ii) For any τ_2, $\sum_{\tau_1=0}^{n-1} a(\tau_1, \tau_2) = (n - |S_p|)^2$.
(iii) For any τ, $a(\tau, \tau) = n - |S_p|$.
(iv) $|S_e| \le |S_p|$.

Let $g(x, y)$ be a function defined by

$$g(x,y) = \begin{cases} \prod_{i=0}^{y-1} \frac{x-i}{i+1}, & \text{if } x \ge y+1 \\ 0, & \text{otherwise} \end{cases} \quad (20)$$

where x and y are real numbers. In fact, we have that $g(x, y) = \binom{x}{y}$ for $x, y \in Z^+$. It is easy to check that $g(x, y)$ is a convex function. First, the objective function for $R_H(\tau) = 0$ is convex because $g(2|S_p| - n + a(\tau_1, \tau_2), |S_e|) = \binom{2|S_p|-n+a(\tau_1,\tau_2)}{|S_e|}$.

At this point, we will prove that the objective function for $R_H(\tau) = 1$ is convex for $\frac{1}{9} < \frac{|S_p|}{n} \le 1$ and $|S_e| \ge 3$ but it does not mean that the case of $\frac{|S_p|}{n} \le \frac{1}{9}$ is not a convex.

Clearly, the convexity of (19) can be proved by the convexity of summands. Then, the summand of (19) can be rewritten as

$$a(\tau_1,\tau_2)g(2|S_p|-n+a(\tau_1,\tau_2),|S_e|-1) + (n-|S_p|-a(\tau_1,\tau_2))^2 g(2|S_p|-n+a(\tau_1,\tau_2),|S_e|-2). \quad (21)$$

Using $g(x,y)=\frac{x-y+1}{y}g(x,y-1)$ for $x\geq y-1$, (21) can be modified as

$$(a(\tau_1,\tau_2)(2|S_p|+a(\tau_1,\tau_2)-n-|S_e|+2) + (|S_e|-1)(n-|S_p|-a(\tau_1,\tau_2))^2)g(2|S_p|-n + a(\tau_1,\tau_2),|S_e|-2). \quad (22)$$

The convexity of (22) can be proved by its second derivative. Let

$$f(a)=a(\tau_1,\tau_2)(2|S_p|+a(\tau_1,\tau_2)-n-|S_e|+2) + (|S_e|-1)(n-|S_p|-a(\tau_1,\tau_2))^2. \quad (23)$$

Then, (22) can be expressed as the product of f and g. Then the convexity of (22) can be proved by deriving the following inequality

$$(fg)''=f''g+2f'g'+fg''\geq 0. \quad (24)$$

It is not difficult to derive the s-derivative of $g(x,y)$ in terms of x as

$$g^{(s)}(x,y)=\sum_{S,|S|=s}\prod_{i\in[0,y-1]\setminus[S]}\frac{x-i}{i+1}. \quad (25)$$

Using the geometric-harmonic mean inequality

$$(x_1x_2\ldots x_n)^{\frac{1}{n}}\geq\frac{n}{\frac{1}{x_1}+\frac{1}{x_2}+\ldots+\frac{1}{x_n}} \quad (26)$$

with $x_i=(x-i+1)$ and $n=y$, we have

$$(g(x,y))^{\frac{1}{y}}\geq\frac{bg(x,y)}{g'(x,y)} \quad (27)$$

$$\frac{y}{(g(x,y))^{\frac{1}{y}}}g(x,y)\leq g'(x,y). \quad (28)$$

In general, $g^{(s)}(x,y)$ is the summation of polynomials factored into $y-s+1$ polynomials of degree one. Using (27) and (28), (22) can be modified as

$$\frac{b-s+1}{(g(a,b-s+1))^{\frac{1}{b-s+1}}}g^{(s-1)}(a,b)\leq g^{(s)}(a,b). \quad (29)$$

Using (29), we have

$$\begin{aligned}(fg)''&=f''g+2f'g'+fg''\\&\geq\frac{(|S_e|-3)^2}{g(2|S_p|-n+a(\tau_1,\tau_2),|S_e|-3)^{\frac{2}{|S_e|-3}}}f\\&\quad+\frac{2(|S_e|-3)}{g(2|S_p|-n+a(\tau_1,\tau_2),|S_e|-3)^{\frac{1}{|S_e|-3}}}f'+f''g\\&\geq\left(\frac{(|S_e|-3)^2}{g(|S_p|,|S_e|-3)^{\frac{2}{|S_e|-3}}}f\right.\\&\quad\left.+\frac{2(|S_e|-3)}{g(|S_p|,|S_e|-3)^{\frac{1}{|S_e|-3}}}f'+f''\right)g. \quad (30)\end{aligned}$$

Let $w=\frac{2(|S_e|-3)}{g(|S_p|,|S_e|-3)^{\frac{1}{|S_e|-3}}}$. Then, it is enough to show that

$$w^2f+2wf'+f''\geq 0. \quad (31)$$

It is easy to check that w is an increasing function for $|S_e|$ and $\frac{|S_e|}{|S_p|}$ and a decreasing function for $|S_p|$. Then, left hand side of (31) can be rewritten as

$$\begin{aligned}L(a)&=w^2\Big((|S_e|-1)\left(n-|S_p|-a(\tau_1,\tau_2)\right)^2\\&\quad+a(\tau_1,\tau_2)(-n+2|S_p|-|S_e|+a(\tau_1,\tau_2)+2)\Big)\\&\quad+2w(-2n|S_e|+n+|S_e|(2|S_p|+2a(\tau_1,\tau_2)-1)+2)\\&\quad+2|S_e|. \quad (32)\end{aligned}$$

At this stage, it is necessary to prove that $L(0)>0$ and that its discriminant is negative in terms of a. It is easy to check that $L(a)$ is linear in terms of $|S_e|$ with a negative slope. Thus, $L(a)$ has its minimum value at the maximum value of $|S_e|$. If $|S_e|=|S_p|$, we have

$$\begin{aligned}L(0)&=w^2(|S_p|-1)(n-|S_p|)^2+w(n(2-4|S_p|)\\&\quad+4|S_p|^2-2|S_p|+4)+2|S_p|\geq 0. \quad (33)\end{aligned}$$

Let $z=\frac{|S_p|}{n}$. Then for sufficiently large values of n and p, (33) can be written as

$$\begin{aligned}\frac{L(0)}{n^2w}&=w(|S_p|-1)(1-z)^2-4|S_p|+4|S_p|^2\\&\geq\left((w(|S_p|-1)+4)z-w(|S_p|-1)\right)(z-1)\\&=(w(|S_p|-1)+4)\left(z-\frac{w(|S_p|-1)}{w(|S_p|-1)+4}\right)(z-1). \quad (34)\end{aligned}$$

Clearly, (34) is positive for a sufficiently large p. Thus, we have $L(0)\geq 0$. Next, the discriminant is written as

$$\begin{aligned}D&=w^4n^2-10w^4n|S_p|+4w^4n+9w^4|S_p|^2\\&\quad-4w^4|S_p|+4w^4+8w^2|S_p|^2<0. \quad (35)\end{aligned}$$

It can also be reduced with sufficiently large values of n and p, whose simplified inequality is given as

$$(9w^4+8w^2)z^2-10w^4z+w^4<0. \quad (36)$$

For $\frac{1}{9}<z<1$, it is easy to derive $D<0$ for a large value of w. Thus we prove the convexity of (22) for the proposed convexity region.

Using the solution of the optimization program cvx for (22), its minimum value occurs at

$$a(\tau_1,\tau_2)=\frac{(n-|S_e|+1)^2-n-|S_e|+1}{n-1}\text{ for all }\tau_1\text{ and }\tau_2, \quad (37)$$

which means that the autocorrelation values of $s_p(t)$ are constant.

REFERENCES

[1] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4539–4551, Sep. 2010.

[2] D. S. Papailiopoulos and A. G. Dimakis, "Locally repairable codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2012, pp. 2771–2775.

[3] I. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *IRE Trans. Inf. Theory*, vol. 4, no. 4, pp. 38–49, Sep. 1954.

[4] J. Macwilliams, "Permutation decoding of systematic codes," *Bell Syst. Tech. J.*, vol. 43, no. 1, pp. 485–505, Jan. 1964.

[5] J. Bellorado and A. Kavcic, "Low-complexity soft-decoding algorithms for Reed–Solomon codes—Part I: An algebraic soft-in hard-out chase decoder," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 945–959, Mar. 2010.

[6] J. Bellorado, A. Kavcic, M. Marrow, and L. Ping, "Low-complexity soft-decoding algorithms for Reed–Solomon codes—Part II: Soft-input soft-output iterative decoding," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 960–967, Mar. 2010.

[7] H. D. L. Hollmann and L. M. G. M. Tolhuizen, "On parity-check collections for iterative erasure decoding that correct all correctable erasure patterns of a given size," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 823–828, Feb. 2007.

[8] T. Hehn, O. Milenkovic, S. Laendner, and J. B. Huber, "Permutation decoding and the stopping redundancy hierarchy of cyclic and extended cyclic codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5308–5331, Dec. 2008.

[9] T. Hehn, J. Huber, O. Milenkovic, and S. Laendner, "Multiple-bases belief-propagation decoding of high-density cyclic codes," *IEEE Trans. Commun.*, vol. 58, no. 1, pp. 1–8, Jan. 2010.

[10] C. Chen, B. Bai, X. Yang, L. Li, and Y. Yang, "Enhancing iterative decoding of cyclic LDPC codes using their automorphism groups," *IEEE Trans. Commun.*, vol. 61, no. 6, pp. 2128–2137, Jun. 2013.

[11] K. Liu, S. Lin, and K. Abdel-Ghaffar, "A revolving iterative algorithm for decoding algebraic cyclic and quasi-cyclic LDPC codes," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4816–4827, Dec. 2013.

[12] M. P. C. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inf. Theory*, vol. 41, no. 5, pp. 1379–1396, Sep. 1995.

[13] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*. New York, NY, USA: CRC Press, 2006.

[14] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 922–932, Mar. 2006.

[15] K. Dohmen, *Improved Bonferroni Inequalities Via Abstract Tubes*. Berlin, Germany: Springer-Verlag, 2003.

[16] M. N. Krishnan, B. Puranik, P. V. Kumar, I. Tamo, and A. Barg, "Exploiting locality for improved decoding of binary cyclic codes," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2346–2358, Jun. 2018.

CHANKI KIM (Member, IEEE) received the B.S. and Ph.D. degrees in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2013 and 2019, respectively. He was a Senior Engineer with Samsung Electronics Company Ltd., Hwaseong, Gyeonggi, South Korea, in 2019. He is currently a Senior Researcher with the Division of National Supercomputing, Korea Institute of Science and Technology Information (KISTI), Daejeon, South Korea. His current research interests include error-correcting codes, fault-tolerant systems for wireless communication, distributed memory and storage and edge, and high-performance and quantum computing.

JONG-SEON NO (Fellow, IEEE) received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, South Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1988. He was a Senior MTS with Hughes Network Systems from 1988 to 1990. He was an Associate Professor with the Department of Electronic Engineering, Konkuk University, Seoul, from 1990 to 1999. He joined the Department of Electrical and Computer Engineering, Seoul National University, as a Faculty Member, in 1999. He was a member with the National Academy of Engineering of Korea (NAEK) in 2015, where he is currently the Division Chair of electrical, electronic, and information engineering. He is also a Professor with Seoul National University. His research interests include error-correcting codes, cryptography, sequences, LDPC codes, interference alignment, and wireless communication systems. He was with the IEEE Information Theory Society in 2012. He was a recipient of the IEEE Information Theory Society Chapter of the Year Award in 2007. From 1996 to 2008, he served as the Founding Chair for the Seoul Chapter, the IEEE Information Theory Society. He served as the General Chair for the Sequence and Their Applications (SETA2004), Seoul, in 2004. He also served as the General Co-Chair for the International Symposium on Information Theory and Its Applications (ISITA2006) in 2006 and the International Symposium on Information Theory (ISIT2009), Seoul, in 2009. He served as a Co-Editor-in-Chief for the IEEE JOURNAL OF COMMUNICATIONS AND NETWORKS from 2012 to 2013.