

RESEARCH ARTICLE

New Design of Error Control Codes Resilient to Single Burst Error or Two Random Bit Errors Using Constacyclic Codes

CHANKI KIM¹, (Member, IEEE), JAE-WON KIM², (Member, IEEE),
AND JONG-SEON NO³, (Fellow, IEEE)

¹Department of Information and Communication Engineering, Chosun University, Gwangju 61452, South Korea

²Department of Electronic Engineering, Engineering Research Institute (ERI), Gyeongsang National University, Jinju 52828, South Korea

³Department of Electrical and Computer Engineering, Institute of New Media and Communications (INMC), Seoul National University, Seoul 08826, South Korea

Corresponding author: Jae-Won Kim (jaewon07.kim@gnu.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korean Government [Ministry of Science and ICT (MSIT)] under Grant 2021R1G1A1091369; and in part by Samsung Electronics Company Ltd., under Contract MEM210728_0001.

ABSTRACT In this paper, we introduce a new design method of burst error control codes (BECCs), which can correct single burst error or two random bit errors by using the maximum likelihood syndrome decoder (MLSD), where the proposed BECCs are designed by a modification of the well-known Fire codes using constacyclic codes. Also, for the existing low-latency burst error-correcting decoder, it is shown that the proposed BECCs have the single burst error correction capability together with two random bit error detection capability with no additional parity bits and comparable complexity with the existing BECCs. For this, the complexity and latency is numerically analyzed by register-transfer level (RTL) synthesis.

INDEX TERMS Burst error control codes (BECCs), burst errors, error control codes, fire codes, low-latency decoder.

I. INTRODUCTION

Error control codes (ECCs) have been widely used for the reliable communication and memory systems. For emerging state-of-art applications of the high-performance memory and interconnect systems, the low-latency property for the decoders of ECCs was introduced as a key requirement to meet industrial demand [1]. For the corresponding error model, burst errors and burst ECCs (BECCs) are commonly considered in the two-dimensional array bit and symbol placement [2]. To this end, cyclic product and Fire codes with the low-latency burst decoder (BD) were proposed in [3] and [4] and adopted for the 10G ethernet standard [5].

In addition, it is known that multi-bit errors become prevalent for recent memory devices, where the existing single burst error correction code is not sufficient for covering multi-bit errors [6], [7], [8]. Thus, a modified class of BECC, called Hsu-Kasami-Chien (HKC) codes with multi-bit error

correction was proposed by expurgating the cyclic Fire codes [9], [10], [11] for a compound channel model with random bit errors and single burst error. However, known classes of HKC codes exists only for limited parameters found by exhaustive computer search and required to have additional parity bits compared to the Fire codes. Although the BECC with random bit error control capability is necessary in many applications, general constructions and optimalities of the BECC are still unknown.

For the implementation of ECC, a digital signal processor (DSP) or field programmable gate array (FPGA) is known to be more faster and energy-efficient than software-based implementation [12]. For the low-latency applications, the BECC is often implemented as a DSP or logic modules in the transceiver for the physical layer. In addition, the BECC can be implemented as the smart network interface card (NIC) with a FPGA for scalability and compatibility of the communication system [13], [14].

In this paper, we introduce a new design of BECCs by modifying the binary cyclic Fire codes without additional

The associate editor coordinating the review of this manuscript and approving it for publication was Oussama Habachi¹.

parity bits. The proposed BECC is constructed using the constacyclic code [15], [16], [17] in order to correct single burst error or two random bit errors for the maximum likelihood syndrome decoder (MLSD). Also, we investigate the performance of the proposed BECC for the existing low-latency BD and it is shown that the proposed BECCs have the single burst error correction capability or two random bit error detection capability. In order to analyze the performance under the hardware implementation of BECCs in the low latency applications, the existing and proposed BECCs are synthesized and compared by the numerical analysis in register-transfer level (RTL).

The paper is organized as follows. In Section II, some preliminaries are introduced including the mathematical notation, system model, Fire code as a BECC, and decoding algorithms. In Section III, new BECCs using constacyclic codes with single burst or two random bit error control capabilities are proposed. In Section IV, the error control capability, decoder latency, and decoder complexity are analyzed using the theoretical and numerical approaches. Finally, the paper is concluded in Section V.

II. PRELIMINARIES

A. NOTATIONS AND DEFINITIONS

In this section, we first summarize some mathematical expressions. Let \mathbf{v} be a binary row vector and v_i be the i -th element of \mathbf{v} . Let $\mathbf{1}$ and $\mathbf{0}$ be all-one and all-zero vectors, respectively. The support set of \mathbf{v} is denoted as $\text{supp}(\mathbf{v}) = \{i; v_i \neq 0\}$ and the Hamming weight of vector \mathbf{v} is given as $\text{wt}(\mathbf{v}) = |\text{supp}(\mathbf{v})|$. Let $[a, b] = \{i \in \mathbb{Z}; a \leq i \leq b\}$, $i \geq 1$ for the set of integers \mathbb{Z} . Also, a linear code \mathcal{C} over the finite field with characteristic two has parameters (n, k, d) , where n and k denote the codelength and message length with the minimum Hamming distance $d = \min_{\mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}} \text{wt}(\mathbf{c})$.

Code operations are based on the $a \times b$ matrix A over the binary finite field \mathbb{F}_2 or its extended fields \mathbb{F}_{2^l} , \mathbb{F}_{2^m} , $\mathbb{F}_{2^{2m}}$, and $\mathbb{F}_{2^{2l}}$ for a positive integer m and an even integer l . Also, let α , β , ξ , and γ be primitive elements of \mathbb{F}_{2^l} , \mathbb{F}_{2^m} , $\mathbb{F}_{2^{2m}}$, and $\mathbb{F}_{2^{2l}}$, respectively. It is easy to check that \mathbb{F}_{2^m} is a subfield of $\mathbb{F}_{2^{2m}}$, where $\mathbb{F}_{2^{2m}}$ is also a subfield of $\mathbb{F}_{2^{4m}}$. Then, the corresponding primitive elements should satisfy

$$\beta = \xi^{2^m+1} = \gamma^{(\sum_{i \in [0, l-1]} 2^{mi})}, \quad \xi = \gamma^{(\sum_{i \in [0, \frac{l}{2}-1]} 2^{2mi})}. \quad (1)$$

Let \mathcal{F} be a linear map from \mathbb{F}_{2^m} to $\mathbb{F}_{2^{2m}}$, that is, $\mathcal{F}(\beta^i) = \xi^{i(2^m+1)}$, $i \in [0, 2^m - 2]$ and $\mathcal{F}(0) = 0$.

Let B be an incidence matrix of A over \mathbb{F}_{2^m} , denoted as $B = M(A)$, that is, $b_{i,j} = 1$ if $a_{i,j} \neq 0$ and $b_{i,j} = 0$, otherwise, where $a_{i,j}$ and $b_{i,j}$ are the (i, j) -th elements of A and B , respectively. Also, let T^i be a companion matrix denoted by

$$T^i =: [[\xi^i], [\xi^{i+1}], \dots, [\xi^{i+2m-1}]] \in \mathbb{F}_2[T] \subseteq \mathbb{F}_2^{2m \times 2m},$$

where $[\xi^i]$ is denoted as a $2m \times 1$ column vector derived from the additive $2m$ -tuple representation of a finite field with basis $\{1, \xi, \dots, \xi^{2m-1}\}$ for an arbitrary integer i and $\mathbb{F}_2[T] = \{T^0, T^1, \dots, T^{2^m-2}\}$. Then, it is easy to check that there

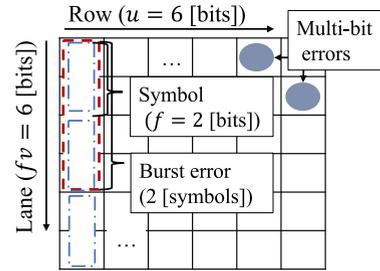


FIGURE 1. Compound error model with single burst error and two random bit errors with $u = 6$, $v = 3$, and $f = 2$.

exists a field-isomorphic map \mathcal{I} from $\{0, \xi^0, \xi^1, \dots, \xi^{2^m-2}\}$ to $\{O, T^0, T^1, \dots, T^{2^m-2}\}$, where O denotes an all-zero matrix [22].

B. ERROR MODEL AND ERROR CONTROL CAPABILITY

In this subsection, we introduce the error model for the state-of-art application such as memory and interconnects [1]. For positive integers f , v , and u , the data and error patterns are represented as an $fv \times u$ two dimensional bit-wise array, where a column is called as a lane. Here, each element of the lane, called a symbol is denoted by the column vector of size f and thus, each lane is composed of v symbols from each pin of the memory chip. Thus, burst errors in lanes are assumed to be independently occurred. Then, the compound error model with both single burst error of several symbols, called a burst error and random bit errors is represented as follows. First, a burst error is occurred for adjacent symbols in a lane, and it should be detected or corrected by the decoder. Here, we only consider single burst error for BECC. In addition, random bit errors can be occurred for any lane and any row locations, where some possible cases should be detected and thus do not be mis-corrected. The error control capability of BECCs is represented by the following four parameters $t_{s,c}$, $t_{s,d}$, $t_{b,c}$, and $t_{b,d}$ as;

- i) Upto $t_{s,c}$ and $t_{s,d}$ symbols in a burst error in a lane are correctable and detectable;
- ii) Upto $t_{b,c}$ and $t_{b,d}$ bits in the random bit errors are correctable and detectable,

where the expressions of correctable and detectable are used when all the errors in the specified pattern can be corrected and detected. For the next subsection, we introduce well-known design types of the existing cyclic BECCs. Fig. 1 describes the compound error model with single burst error and two random bit errors with $u = 6$, $v = 3$, and $f = 2$.

C. THE EXISTING BINARY CYCLIC BECCS

In this subsection, we introduce the well-known class of binary cyclic BECCs, called as Fire codes [3]. Note that the introduced BECCs were rediscovered as an optimal binary locally repairable codes (BLRCs) for bit erasures in the distributed storage systems (DSSs) [18]. In this paper, the parameters of the existing BECCs (Fire codes) can be modified as $(n, k, t_{s,c}, t_{s,d}, t_{b,c}, t_{b,d})$. Thus, the binary cyclic BECCs in [3] are modified as follows.

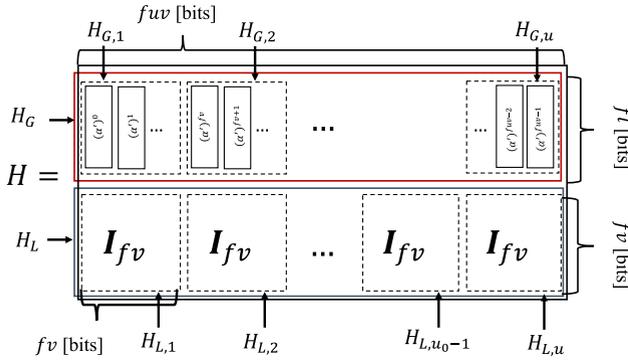


FIGURE 2. Parity check matrix of the modified BECC (Fire code) in Construction 1.

Construction 1 (Modified BECC in [3]): For code length $n = fuv$ with $v > l$, let δ be a $(2^l - 1)$ -th root of unity over the finite field \mathbb{F}_{2^l} , where $u_0 = 2^l - 1$ and $u \leq u_0$. Here, suppose a cyclic code with a generator polynomial $g(x) = (x^{fv} + 1)p_{\alpha'}(x)$, where $p_{\alpha'}(x)$ is a minimal polynomial of $\alpha' \in \mathbb{F}_{2^l}$ over \mathbb{F}_2 . Then, a parity check matrix $H_o = \begin{bmatrix} H_{G_o} \\ H_{L_o} \end{bmatrix}$ is composed of two submatrices, an $fl \times fu_0v$ submatrix $H_{G_o} = [H_{G,1}, H_{G,2}, \dots, H_{G,u_0}]$ and an $fv \times fu_0v$ submatrix $H_{L_o} = [H_{L,1}, H_{L,2}, \dots, H_{L,u_0}] = [I_{fv}, I_{fv}, \dots, I_{fv}]$ for an $fl \times fv$ submatrix $H_{G,i}, i \in [u_0]$ and an $fv \times fv$ identity matrix I_{fv} . Here, H_{G_o} and H_{L_o} are constructed by check equations with roots in $p_{\alpha'}(x)$ and $(x^{fv} + 1)$, respectively.

Then, let C_{BC} be a BECC, whose codeword $\mathbf{c} = (\mathbf{c}_1, \dots, \mathbf{c}_u)$ can be defined by shortening $f(u_0 - u)v$ information bits as in Fig. 2 and its parity check matrix consists of two submatrices H_G and H_L as $H_{BC} = \begin{bmatrix} H_G \\ H_L \end{bmatrix}$ with $H_G = [H_{G,1}, \dots, H_{G,u_0}]$ and $H_L = [H_{L,1}, \dots, H_{L,u_0}]$. Then, the BECC C_{BC} has the following properties;

- i) A burst error of at least $t_{s,c} \geq l$ and $t_{s,d} \geq v$ symbols is correctable and detectable [3].
- ii) Random bit errors for $t_{b,c} \geq 1$ and $t_{b,d} \geq 1$ are correctable and detectable (Theorem 4 in [10]).

In fact, Construction 1 with $f = 1$ and $u_0 = u$ corresponds to the binary cyclic BECC (Fire code) in [3]. Also, note that shortening the cyclic BECC offers the modified parameters while shortening preserves the error control capability of the original cyclic code. However, burst error control capability in this paper is not identical to that in [3] and [10] from the difference of the channel model such that each burst error is only located in a lane.

In order to improve $t_{b,c}$ and $t_{b,d}$, HKC codes were proposed by multiplying additional polynomials into $g(x)$ in the cyclic Fire codes. However, only some classes of HKC codes with good selection of additional roots were analyzed requiring additional parity bits [9], [10], [11].

For the low-latency applications, BECC operations are designed as a hardware module. Conventionally, encoding and decoding implementation of the cyclic BECCs such as the existing Fire and HKC codes consist of linear feedback shift

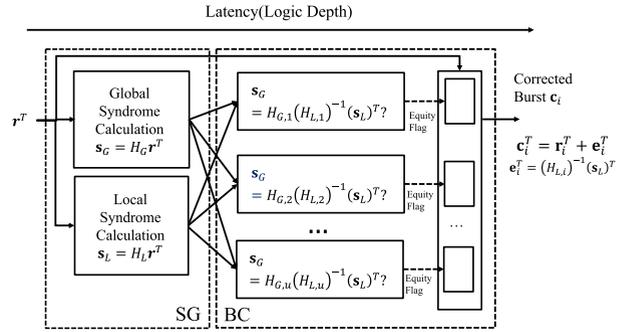


FIGURE 3. BD implementation logic architecture.

registers (LFSRs) for the finite field arithmetic [19]. First, the encoding operation can be represented as multiplication of binary polynomials and consumes at least k cycle to complete. In addition, decoding operation of burst trapping process is known to require at least $fv + l$ cycles to proceed [20], where the required latency becomes prohibitive for BECCs with long code length and low-latency applications.

In order to improve the latency for the burst error correction, the MLSD and low-latency BD for BECC are introduced.

D. MLSD AND LOW-LATENCY BD FOR BECC

Here, concepts of the MLSD and low-latency BD are introduced for the existing and proposed BECCs. In fact, both decoders have an advantage of using combinatorial logics and thus, low latency can be achieved by removing processing cycles by LFSRs. Also, both decoders use syndrome values which can be obtained from the following procedures. First, suppose that an fu_0v -length codeword $\mathbf{c} = (\mathbf{c}_1, \dots, \mathbf{c}_u) \in C_{BC}$ in the BECC experiences the compound channel. A burst error in the i -th lane is assumed to be occurred, which is represented by a nonzero $1 \times fv$ error subvector \mathbf{e}_i in the $1 \times fu_0v$ received and error vectors \mathbf{r} and \mathbf{e} such that $\mathbf{r} = \mathbf{c} + \mathbf{e}$. Then, the syndrome \mathbf{s} is defined as $\mathbf{s}^T = H\mathbf{r}^T = H\mathbf{e}^T$.

Here, the MLSD can correct single burst or multi-bit errors for BECC if all the corresponding error vectors upto single burst error of $t_{s,c}$ symbols or $t_{b,c}$ random bit errors have different syndromes. However, its naive implementation requires comparing all the possible correctable cases, which results in the high decoding complexity for BECCs with the single burst or bit error control capability.

In order to achieve low-latency design from the MLSD, the parallel decoder architecture for cyclic BECCs was introduced [21], where the global syndrome \mathbf{s}_G and local syndromes \mathbf{s}_L were derived as;

- i) $(\mathbf{s}_L)^T := H_L \mathbf{r}^T$,
- ii) $(\mathbf{e}_i)^T := (H_{L,i})^{-1}(\mathbf{s}_L)^T$,
- iii) $(\mathbf{s}_G)^T := H_{G,i} \mathbf{e}_i^T = H_G \mathbf{r}^T$.

Then BD can be implemented by combinatorial logic using the following two phases;

- i) Syndrome generator (SG): Calculate $(\mathbf{s}_G)^T = H_G \mathbf{r}^T$ and $(\mathbf{s}_L)^T = H_L \mathbf{r}^T$.

- ii) Burst error corrector (BC): If $\mathbf{s}_G \neq \mathbf{0}$ and $\mathbf{s}_L \neq \mathbf{0}$, find a unique i satisfying

$$(\mathbf{s}_G)^\top = H_{G,i}(H_{L,i})^{-1}(\mathbf{s}_L)^\top. \quad (2)$$

If there exists a unique $i \in [u]$, we can recover $\mathbf{c}_i = \mathbf{r}_i + \mathbf{e}_i$. If there does not exist a unique i , error detection is declared.

For low-latency property, BD can parallelize the BC operation for all possible u lanes. Fig. 3 shows the BD implementation logic architecture with parallelized BC.

As complexity and latency measures of the proposed BD logic architecture, the gate count and logic depth of SG and BC are presented. First, gate count is the total number of used gates for operating hardware modules. In addition, logic depth is the maximum number of processed gates for critical paths. Generally, gate count and logic depth show the level of complexity and latency of combinatorial logics for the BD architecture [19], [21]. Also, two measures can be analyzed by either estimation from the constructed parity check matrix H or synthesis on the FPGA using the Verilog codes for RTL.

Note that the BD is sub-optimal compared with the MLSD because it can only correct single burst error, not multi-bit errors in the multiple lanes. Also, for the compound channel with multi-bit errors, there exists mis-correction to single burst error if they have the same syndrome. In the next section, concepts of constacyclic codes and new design for low-latency BECCs are introduced.

III. NEW DESIGN OF PROPOSED LOW-LATENCY BECCS USING CONSTACYCLIC CODES

In this section, we first introduce the concept of the existing constacyclic codes. Then, the new design of low-latency BECCs is proposed using the constacyclic codes.

A. CONSTACYCLIC CODES

Before introducing the constacyclic codes, we first remind cyclic codes. For the cyclic codes with codeword length $n = 2^l - 1$, encoding and decoding operations are defined over an isomorphic mapping from the algebraic operation over the principal ring $\mathbb{F}_2[x]/\langle x^n + 1 \rangle$, where $\langle \cdot \rangle$ is a generator. Denote $\alpha \in \mathbb{F}_{2^l}$ as a primitive element satisfying $\alpha^{2^l-1} = 1$. For the set of root exponents $C = [0, 2^l - 2]$, let $C_i = \{\alpha^i, \alpha^{2i}, \dots, \alpha^{2^{l-1}i}\}$, $|C_i| \leq l$ be a coset, a partition of C . Let $p_i(x)$ be a minimal polynomial of α^i over \mathbb{F}_2 . Then, we have

$$x^n + 1 = (x + 1) \left(\sum_{i \in [0, n-1]} x^i \right) = \prod_{i \in I \setminus \{0\}} (x + 1)p_i(x), \quad (3)$$

where I is a subset of $[0, 2^l - 2]$ satisfying $C = \cup_{i \in I} C_i$ with the minimum cardinality.

Then, a special class of non-binary constacyclic codes was proposed as a generalization of cyclic codes, which is defined as follows.

Definition 1 (Constacyclic codes, [15], [17]): For integers m, l and an element $\lambda \in \mathbb{F}_{2^m}$, a 2^m -ary linear code \mathcal{C} with codeword length $n = 2^l - 1$ is denoted as λ -constacyclic if $(\lambda c_n, c_1, \dots, c_{n-1}) \in \mathcal{C}$ for all $(c_1, c_2, \dots, c_n) \in \mathcal{C}$.

Similarly, a constacyclic code is defined over an isomorphic mapping to the principal ring $\mathbb{F}_{2^m}[x]/\langle x^n + \lambda \rangle$. Note that the authors in [15] and [17] only considered the case with $l = m$, but this isomorphism generally holds for any l and m . Here, suppose an element $\delta \in \mathbb{F}_{2^m}$ satisfying $\delta^n = \lambda$, where the coset $C'_i = \{\delta \cdot \alpha^i, \delta \cdot \alpha^{2i}, \dots, \delta \cdot \alpha^{2^{l-1}i}\}$ and $\beta^j \cdot \alpha^k$ returns $\gamma^{j(\sum_{i \in [0, l-1]} 2^{mi}) + k(\sum_{i \in [0, m-1]} 2^{li})} \in \mathbb{F}_{2^{lm}}$ for $\alpha^k \in \mathbb{F}_{2^l}$ and $\beta^j \in \mathbb{F}_{2^m}, j, k \in \mathbb{Z}$. Then, we use the following lemma.

Lemma 1: For a principal ring $\mathbb{F}_{2^m}[x]/\langle x^n + \lambda \rangle$, with $n = 2^l - 1$ and relatively prime l and m , the following statements are valid;

- 1) There exists an element δ satisfying $\delta^n + \lambda = 0$ and $\delta = \beta^e$, where $\beta \in \mathbb{F}_{2^m}$.
- 2) Let $p'_i(x)$ be a minimal polynomial of $\delta \cdot \alpha^i$ over \mathbb{F}_{2^m} mapped from $p_i(x) \in \mathbb{F}_2[x]/\langle x^n + 1 \rangle$, where the map converts the coefficients of zero and one of the binary coefficients to zero and one over \mathbb{F}_{2^m} , respectively. Then, $x^n + \lambda$ is factored into

$$\begin{aligned} x^n + \lambda &= \delta^n(\delta^{-n}x^n + 1) \\ &= \delta^n(\delta^{-1}x + 1) \prod_{i \in I \setminus \{0\}} p'_i(\delta^{-1}x). \end{aligned} \quad (4)$$

Proof: For the first part, note that $n = 2^l - 1$ and $2^m - 1$ are relatively prime. By the well-known Chinese remainder theorem, we can always find a unique value satisfying $i' = 0 \pmod{2^m - 1}$ and $i' = e(\sum_{i \in [0, l-1]} 2^{mi}) \pmod{2^l - 1}$ for $i' \in [(2^m - 1)(2^l - 1)]$. Let $i'' = \frac{(2^{ml} - 1)i'}{(2^m - 1)(2^l - 1)} \in [2^{ml} - 1]$. Then, $\delta = \gamma^{i''}$ is an element of \mathbb{F}_{2^m} because $\gamma \in \mathbb{F}_{2^{lm}}$ and $\delta^{2^m-1} = \gamma^{\frac{(2^{ml}-1)i''}{(2^l-1)}} = (\gamma^{\frac{(2^{ml}-1)}{(2^l-1)}})^{i''} = 1$. Also, $\delta = \beta^e$ in that $\delta^{2^l-1} = \left(\gamma^{\frac{(2^{ml}-1)}{(2^m-1)}}\right)^{i''} = \gamma^{e(\sum_{i \in [0, l-1]} 2^{mi})} = \beta^e = \lambda$.

For the second part, it is easy to check that (4) is satisfied using (3). Also, $p'_i(\delta^{-1}x)$ is a minimal polynomial of $\delta \cdot \alpha^i$ because $p'_i(\delta^{-1}x)$ is an irreducible polynomial with roots C'_i , which concludes the proof. ■

Also, the constacyclic codes preserve some useful properties of the cyclic codes [15]. Let Z and Z' be defining sets, that is, sets of roots in the generator polynomial of cyclic and constacyclic codes, respectively. Then, Z and Z' are represented as the unions of some cosets of the finite field denoted as $Z = \cup_i C_i = \cup_i \{\alpha^i\}$ and $Z' = \cup_i C'_i = \cup_i \{\delta \cdot \alpha^i\}$ for cyclic and constacyclic codes. Accordingly, the well-known BCH bound for constacyclic codes is represented as follows.

Lemma 2 (Constacyclic BCH Bound [15], [17]): For $\delta \in \mathbb{F}_{2^m}$ and $\alpha \in \mathbb{F}_{2^l}$, suppose a constacyclic code \mathcal{C}_{cc} over \mathbb{F}_{2^m} with a defining set $Z' = \cup_i \{\delta \cdot \alpha^i\}$ including the consecutive roots $\{\delta \cdot \alpha^l, \delta \cdot \alpha^{l+1}, \dots, \delta \cdot \alpha^{l+d'-2}\}$. Then, \mathcal{C}_{cc} has the minimum Hamming distance at least d' .

Proof: See the proof in [15] and [17]. ■

Using this property, we can generalize the class of cyclic BECCs as the constacyclic codes while preserving error control capability and parity bits for single burst errors. In the next subsection, we propose the new design of low-latency BECCs using the constacyclic codes.

B. NEW DESIGN OF BECCs USING CONSTACYCLIC CODES

In this subsection, the proposed BECCs can be constructed as follows.

Construction 2 (Construction of the Proposed Binary BECCs): Suppose the primitive roots β and ξ over \mathbb{F}_{2^m} and $\mathbb{F}_{2^{2m}}$, satisfying $l < v$ and $\beta = \xi^{2^{m+1}}$, where l and m are relatively prime. For the principal ring of $\langle x^{uv} + \lambda^v \rangle$, let $b = 2^m + 1$ and $\delta = \beta^e = \xi^{e(2^{m+1})} = \xi^{eb}$ be a root of $x^u + \lambda$ over \mathbb{F}_{2^m} for $u = 2^l - 1$ and some integer e . From an $(n, k) = (uv, uv - l - v)$ constacyclic code C_P , a linear binary BECC C_{prop} with $(n, k) = (fuv, f(uv - l - v))$ for a symbol size $f = 2m$ has a $2m(l + v) \times 2muv$ parity check matrix $H_{C_{prop}} = \begin{bmatrix} H_G \\ H_L \end{bmatrix}$, where $H_G = [H_{G,1}, \dots, H_{G,u}]$ and $H_L = [H_{L,1}, \dots, H_{L,u}]$ are constructed as following procedures.

- i) Let C_1 be a constacyclic code over \mathbb{F}_{2^m} with the parity check polynomial $h(x)$ as

$$h(x) = \frac{x^u + \lambda}{p'_i(\delta^{-1}x)} = \prod_{j \in I \setminus \{i\}} p'_j(\delta^{-1}x) = \sum_{i \in [0, u-1]} h_i x^i, \quad h_i \in \mathbb{F}_{2^m}.$$

- ii) Generate an $l \times uv$ $P_G = [P'_U, \delta^v P'_U, \dots, \delta^{v(u-1)} P'_U]$, where an $l \times uv$ P'_U is represented as shown at the bottom of the page, using the coefficient of check polynomial $h(x)$ and $h_i \in \mathbb{F}_{2^m}$.
- iii) Construct a $v \times uv$ submatrix $P_L = [P_{L,1}, \dots, P_{L,u}]$ with

$$P_{L,i} = \begin{bmatrix} \delta^{v(i-1)} & 0 & \dots & 0 \\ 0 & \delta^{v(i-1)} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \delta^{v(i-1)} \end{bmatrix},$$

and thus, an $(l + v) \times uv$ matrix $P = \begin{bmatrix} P_G \\ P_L \end{bmatrix}$ is generated from P_G and P_L . Then, P is a parity check matrix of the constacyclic code C_P with the generator polynomial $g(x) = (\delta^{-v}x^v + 1)p'_i(\delta^{-1}x)$ over \mathbb{F}_{2^m} .

- iv) From C_P , convert all the elements by two sequential maps $\mathcal{I} \circ \mathcal{F}$ to binary elements. First, the map \mathcal{F} converts β^i to ξ^{bi} and $\delta^i = \beta^{ei}$ to ξ^{bei} . Then, the elements of ξ^i are mapped into $2m \times 2m$ companion matrices by $\mathcal{I}(\xi^i) = T^i$, which finally construct the proposed binary BECC with a $2m(l + v) \times 2muv$ parity check matrix $H_{C_{prop}}$.

For the encoding of the proposed BECCs, encoding of the constacyclic codes can be implemented as a multiplication of

two polynomials over $\mathbb{F}_2[x]/\langle x^n + \lambda \rangle$, where the required complexity is similar to the existing one. Also, the MLSD and low-latency BD can be used for the low-latency decoding of the proposed codes.

Note that the parity bits for the proposed BECC are the same as the cyclic Fire BECCs, which maintains high code rates for low-latency applications. Nevertheless, the proposed BECC and BD have additional two bit error detection capability with the same burst error correction capability as Fire codes. For the existing HKC codes, they requires the additional parity bits for multi-bit error control capability. In the next section, theoretical approach is introduced in order to show it.

IV. ANALYSES OF THE PROPOSED BINARY BECC

In this section, single burst and two random bit error control capability of the proposed binary BECC is analyzed via the theoretical approach. Also, its decoding latency and complexity are numerically derived by nonzero values on parity check matrix and RTL synthesis.

A. THEORETICAL ANALYSIS FOR ERROR CONTROL CAPABILITY ON THE PROPOSED BECC

In this subsection, the single burst and two random bit error control capability is derived. The first theorem shows that the proposed BECC has the same burst error control capability as the Fire code for $f = 2m$.

Theorem 1 (Burst Error Control Capability of the Proposed Binary BECC): The proposed BECC can correct $t_{s,c}$ symbols and detect $t_{s,d}$ symbols of single burst error by both the MLSD and BD, where $t_{s,c} \geq l$ and $t_{s,d} \geq v$.

Proof: It is known that the BD calculates the syndrome in parallel by a lane, where the BD corrects the single burst error only when the corresponding syndrome uniquely exists for one lane. Let $b(x) = \sum_{i \in [0, l-1]} b_i x^i$ be a burst error polynomial of degree $l - 1$ over \mathbb{F}_{2^m} . If there exists another burst error polynomial $x^{j_1} b'(x)$, $j_1 \in \{v, 2v, \dots, (u-1)v\}$ with $b'(x) = \sum_{i \in [0, l-1]} b'_i x^i$, which returns the same syndrome value as $b(x)$, $b(x)$ is not correctable. Provided that $x^{j_1} b'(x) + b(x) = 0 \pmod{g(x)} = (\delta^{-v}x^v + 1)p'_i(\delta^{-1}x)$, the following equations should be satisfied as;

- i) From $(\delta^{-v}x^v + 1)|(x^{j_1} b'(x) + b(x))$, $b'(x) = \delta^{j_2-j_1} x^{-j_2} b(x)$ for $j_1 - j_2 \in \{0, v, 2v, \dots, (u-1)v\}$.
- ii) From $p'_i(\delta^{-1}x)|(x^{j_1} b'(x) + b(x)) = (\delta^{j_2-j_1} x^{j_1-j_2} + 1)b(x)$, $p'_i(\delta^{-1}x)|b(x)$.

However, the condition $p'_i(\delta^{-1}x)|b(x)$ is not satisfied because degree of $b(x)$ is less than l and $p'_i(\delta^{-1}x)$ of degree l is irreducible. It contradicts the assumption and thus single burst

$$P'_U = \begin{bmatrix} h_0 & h_1 & \dots & h_{u-l} & 0 & \dots & 0 \\ 0 & h_0 & \dots & h_{u-l-1} & h_{u-l} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & h_{u-2l+1} & h_{u-2l+2} & \dots & h_{u-l} \end{bmatrix}$$

error less than l symbols in a lane is correctable for the proposed BECC.

For the single burst error of v symbols in the lane, the index of lane i satisfying (2) either uniquely exists in the erroneous lane or coexists both in the erroneous lane and other lanes.

In either case, the BD can know their error occurrence and thus detect the burst error. Similar to the BD, the MLSD can correct and detect the errors by the syndrome, which concludes the proof. ■

In order to show the additional random bit error control capability for the proposed BECC, the following lemma and theorem are introduced.

Lemma 3: The Hamming distance of a constacyclic code C_P over \mathbb{F}_{2^m} is at least four. Also, for the parity check matrix P , $M(P)$ is a parity check matrix of the binary BECC (Fire code) in Construction 1 with $g(x) = (x^v + 1)p_i(x)$.

Proof: For C_P with $g(x) = (\delta^{-v}x^v + 1)p_i'(\delta^{-1}x)$, its corresponding defining set is $Z = \{\delta \cdot \alpha^0, \delta \cdot \alpha^i, \dots, \delta \cdot \alpha^{2^{l-1}i}\}$. By three subsequent roots of $\{\delta \cdot \alpha^0, \delta \cdot \alpha^i, \delta \cdot \alpha^{2^i}\}$, the Hamming distance of C_P over \mathbb{F}_{2^m} is at least four from Lemma 2. ■

Theorem 2: For the proposed binary BECC C_{prop} with $v = \sum_{i \in [0, \lceil \frac{l}{2} \rceil - 1]} 2^{2im}$, the BD can detect the two random bit errors. Also, the MLSD can correct the two random bit errors.

Proof: Suppose a constacyclic code over $\mathbb{F}_{2^{2m}}$ from $\mathcal{F}(C_P)$. For the proof, it is sufficient to show that all the corresponding syndromes for upto single burst error of $t_{s,c} = l$ symbols and two random bit errors are different. For two random bit errors, the corresponding error polynomial can be represented as $e(x) = \xi^{i_1}x^{d_1}$ for one symbol error or $e(x) = \xi^{i_1}x^{d_1} + \xi^{i_2}x^{d_2}$ for two symbol errors over $\mathbb{F}_{2^{2m}}$. However, we only focus on the case of $e(x) = \xi^{i_1}x^{d_1} + \xi^{i_2}x^{d_2}$. Also, note that $\xi^{i_1}, \xi^{i_2} \in [\xi^0, \dots, \xi^{2^m-1}]$, whose binary representation has the Hamming weight one. Then, what we have to show can be divided into two parts.

- i) The syndrome by two random bit errors in the proposed code is different from that of all the other two random bit error cases.
- ii) All the syndromes from single burst error less than or equal to $t_{s,c}$ symbols are different from those of all two random bit errors.

First, suppose that a two random bit error polynomial $e_1(x) = \xi^{i_{1,1}}x^{d_{1,1}} + \xi^{i_{1,2}}x^{d_{1,2}}$ returns the syndrome value, which is not unique and thus, another two bit error polynomial $e_2(x) = \xi^{i_{2,1}}x^{d_{2,1}} + \xi^{i_{2,2}}x^{d_{2,2}}$ returns the same syndrome. For MLSD, recall that different syndromes between two random bits errors guarantee the correction and detection. However, BD only guarantees detection because there is no correction algorithm for two random bit errors, which can only detect error by checking that there does not exist a case satisfying (2) in BD. Also, it is known that the cases with not guaranteeing correction and detection are possible in the decoding of Fire codes, which shows the superiority of the proposed BECC.

Then, the syndrome polynomial is $s(x) = h(x)e_1(x) = h(x)e_2(x) \pmod{g(x)}$ and equivalently, $h(x)(e_1(x) + e_2(x)) \pmod{g(x)}$ with the Hamming weight less than or equal to four. However, there is no codeword with the Hamming weight less than four by Lemma 3. Also, suppose that there exists a weight-4 codeword polynomial $\xi^{i_{1,1}}x^{d_{1,1}} + \xi^{i_{1,2}}x^{d_{1,2}} + \xi^{i_{2,1}}x^{d_{2,1}} + \xi^{i_{2,2}}x^{d_{2,2}} = \xi^{i_{1,1}}x^{d_{2,2}}(x^{d_{1,1}-d_{2,2}} + \xi^{i_{1,2}-i_{1,1}}x^{d_{1,2}-d_{2,2}} + \xi^{i_{2,1}-i_{1,1}}x^{d_{2,1}-d_{2,2}} + \xi^{i_{2,2}-i_{1,1}})$.

Then, the binary representation of each coefficient $[\xi^{i_{1,2}-i_{1,1}}], [\xi^{i_{2,1}-i_{1,1}}], [\xi^{i_{2,2}-i_{1,1}}]$ should be in $\{[1], [\xi^1], [\xi^2], \dots, [\xi^{2^m-1}]\}$. However, encoding operation by $g(x)$ is defined over \mathbb{F}_{2^m} with a primitive element $\beta = \xi^b$, $b|(i_{1,2} - i_{1,1})$, $b|(i_{2,1} - i_{1,1})$, and $b|(i_{2,2} - i_{1,1})$. By $b = 2^m + 1 > 2m$, the only possible case is $i_{1,1} = i_{1,2} = i_{2,1} = i_{2,2}$, which means that there exists a codeword whose nonzero coefficients are one. Then, we have a codeword $c(x) = x^{d_1}(x^{l_1v} + 1) + x^{d_2}(x^{l_2v} + 1)$, where $d_{1,1} = d_{1,1} + l_{1,1}v$ and $d_{1,2} = d_{1,2} + l_{1,2}v$ for $d_{1,1}, d_{1,2} \in [0, v - 1]$. From $(\delta^{-v}x^v + 1)|c(x)$, we have $(\delta^{-v}x^v + 1)|(x^{l_1v} + 1)$ and $(\delta^{-v}x^v + 1)|(x^{l_2v} + 1)$. Then, $c(x)$ should be factored into $c(x) = (\delta^{-v}x^v + 1)(x^{d_1} \sum_{i=0}^{l_1-1} \delta^{vi}x^{vi} + x^{d_2} \sum_{i=0}^{l_2-1} \delta^{vi}x^{vi})$ and $\delta^{vl_1} = \delta^{vl_2} = 1$. Also, from $c(1) = 0$, l_1 should be equal to l_2 for all-one weight-4 codeword $c(x)$ because $\delta^v \neq 1$ and $\sum_{i=l_{1,1}}^{l_{1,2}-1} \xi^{ibev} \neq 0$ for $l_1 \neq l_2$. However, $\delta^{(\sum_{i \in [0, \lceil \frac{l}{2} \rceil - 1]} 2^{2mi})l} \neq 1$ because $2^m - 1$ does not divide $\sum_{i \in [0, \lceil \frac{l}{2} \rceil - 1]} 2^{2mi}$. Therefore, there is no weight-4 codeword polynomial, which proves the first part.

For the second part, suppose that there correctable exists single burst error polynomial in the first lane $e_2(x) = \sum_{j \in [t_{s,c}]} \xi_{d_2+j}x^{d_2+j}$ for $\xi_{d_2+j} \in \{0, 1, \xi, \dots, \xi^{2^{2m}-2}\}$ and $t_{s,c} + b < bv$, together with a two random bit error polynomial $e_1(x) = \xi^{i_{1,1}}x^{d_{1,1}} + \xi^{i_{1,2}}x^{d_{1,2}}$. If $e_1(x) + e_2(x)$ becomes a codeword $c(x)$, then $g(x)|c(x)$ and $(\delta^{-v}x^v + 1)|c(x)$. In order to satisfy it, $e_2(x)$ should be reduced to $e_2(x) = \delta^{l_{1,1}v}\xi^{i_{1,1}}x^{d_{1,1}} + \delta^{l_{1,2}v}\xi^{i_{1,2}}x^{d_{1,2}}$ and $c(x)$ is represented as

$$c(x) = \xi^{i_{1,1}}x^{d'_{1,1}}(x^{l_{1,1}v} + \delta^{l_{1,1}v}) + \xi^{i_{1,2}}x^{d'_{1,2}}(x^{l_{1,2}v} + \delta^{l_{1,2}v}), \quad (5)$$

where $d_{1,1} = d'_{1,1} + l_{1,1}v$, $d_{1,2} = d'_{1,2} + l_{1,2}v$, and $\xi^{i_{1,1}}, \xi^{i_{1,2}} \in [\xi^0, \xi^1, \dots, \xi^{2^m-1}]$ similar to the first procedure without loss of generality. From (5) and $c(\delta \cdot \alpha) = 0$, we have

$$\begin{aligned} (\xi)^{i_{1,1}-i_{1,2}}(\delta \cdot \alpha)^{d'_{1,1}-d'_{1,2}} &= \frac{(\delta \cdot \alpha)^{l_{1,2}v} + \delta^{l_{1,2}v}}{(\delta \cdot \alpha)^{l_{1,1}v} + \delta^{l_{1,1}v}} \\ &= \frac{(\delta^{l_{1,2}v} \cdot \alpha^{l_{1,2}v}) + (\delta^v)^{l_{1,2}}}{(\delta^{l_{1,1}v} \cdot \alpha^{l_{1,1}v}) + (\delta^v)^{l_{1,1}}}, \quad (6) \end{aligned}$$

where $v = \sum_{i \in [0, \lceil \frac{l}{2} \rceil - 1]} 2^{2mi}$. Here, the left-hand side in (6) is in $\mathbb{F}_{2^{2m}}$ but not \mathbb{F}_{2^m} from $(\delta \cdot \alpha)^{d'_{1,1}-d'_{1,2}} = \gamma^{(d'_{1,1}-d'_{1,2})(e^{(\sum_{i \in [0, l-1]} 2^{2mi}) + (\sum_{i \in [0, m-1]} 2^{li})})}$, where all the factors of the exponents are not divided by $\sum_{i \in [0, \lceil \frac{l}{2} \rceil - 1]} 2^{2mi}$ for $|d'_{1,1} - d'_{1,2}| < v$. On the contrary, the right-hand side is in $\mathbb{F}_{2^{2m}}$ because the field operation is conducted only using the elements of $\mathbb{F}_{2^{2m}}$, $(\delta^v)^i, (\alpha^v)^i \in \mathbb{F}_{2^{2m}}$ by $\gamma^v = \xi \in \mathbb{F}_{2^{2m}}$

TABLE 1. Complexity and latency analysis for the proposed and existing BECCs with BD.

(n, k)	Analysis method		Estimation on H			RTL Synthesis		
	Decoding procedure		SG	BC	Total	SG	BC	Total
(476, 396)	Proposed BECC	Gate number	2567	1807	4375	366	200	566
		Logic depth	8	10	18	4	6	10
(476, 396)	Existing Fire codes	Gate number	3176	2856	6032	476	500	976
		Logic depth	8	10	18	5	8	13
(340, 256)	Existing HKC codes	Gate number	3028	2688	5716	460	233	693
		Logic depth	6	9	15	3	8	11

and (1), which results in contradiction and the theorem is proved. ■

Note that in the existing Fire code in Construction 1, at least one case such that the same syndrome between different types of two random bit errors always exists from a codeword $c'(x) = x^{fv}(x^{fu} + 1) + x^{fu} + 1$ and thus, the improved multi-bit error control capability for the proposed code is clearly shown by the above theorem.

In order to discuss the decoder latency, the next section focuses on numerical analysis for the existing and proposed BECCs using the FPGA.

B. NUMERICAL ANALYSIS OF COMPLEXITY AND LATENCY FOR BD IN THE PROPOSED BECC

In this subsection, the complexity and latency of proposed BECC is numerically analyzed and compared with the existing BECCs under the compound channel and BD. For this, we consider a $(n, t_{s,c}, t_{s,d}) = (476, 3, 17)$ BECC under the compound channel with $f = 4$, $u = 7$, and $v = 2^m + 1 = 17$. By Construction 2, $(n, k, t_{s,c}, t_{s,d}) = (476, 396, 3, 17)$ binary BECCs with $m = 2$ are considered. Also, the existing $(n, k, t_{s,c}, t_{s,d}) = (476, 396, 3, 17)$ binary Fire codes and $(n, k, t_{s,c}, t_{s,d}) = (340, 256, 3, 5)$ HKC codes with $t_{b,c} = t_{b,d} = 2$ are generated from cyclic Fire codes by Construction 1 and a primitive polynomial $g_1(x) = x^{12} + x^{10} + x^2 + x + 1$ with degree $fl = 12$. Also, HKC codes with lower code rate can be generated by repeating four $(n, k) = (85, 64)$ HKC codes $g(x) = (1 + x^5) \prod_{i=1}^2 g_i(x)$ from the second class of $(n, k) = (85, 64)$ HKC codes in Table 3 of [11], where $g_i(x)$ is a minimal polynomial with root α^{6i-3} . Note that only some classes of HKC codes are known to have a good parameter approaching the theoretical bound and thus, (85,64) HKC code with the same burst error correction capability is selected as comparison among the HKC codes with known parameters. For generator polynomials, two 8-degree polynomials are selected as $g_1(x) = x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$ and $g_2(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$. Equivalently, HKC codes can be generated by the repeated-root cyclic codes with a generator polynomial $g^4(x)$ over $\mathbb{F}_2[x]/\langle x^{340} + 1 \rangle$.

For estimation of complexity and latency based on H , the gate numbers of SG and BC are counted by the number of ones in H and $H_{G,i}(H_{L,i})^{-1}$ based on only 2-input XOR gates. Accordingly, logic depth of SG and BC amounts to the base-2 logarithm of the maximum number of ones in each row

in H and $H_{G,i}(H_{L,i})^{-1}$. Also, BC consumes extra cycles to construct 1-bit equity flag of (2) from the syndrome, which requires additional logic depth $\lceil \log_2 fl \rceil$ from the syndrome calculation.

In the RTL synthesis on FPGA, Intel Quartus Prime version 19.2 synthesis tool for Intel Arria 10 GT FPGA is used. By synthesis, gate number and logic depth are further reduced from the estimation by logic optimization process using depth-reducing gates from 2-input to 6-input gate operations. Note that logic optimization process does not change the error control capability of the BECCs.

Table 1 shows that the logic depth and the gate number of the proposed and existing BECCs. Due to the short code-length and sparsity in H_G , the processing complexity and latency are small compared to the (476, 396) proposed and existing Fire BECCs. Similarly, the simulation results show that the proposed BECC by Construction 2 has the lower gate number and logic number with the existing BECCs but shows the enhanced error control capability without additional parities from the existing Fire codes. Note that optimized results also consider various aspects of the FPGA such as the number and placement of arithmetic logic units (ALUs) and the level of gate reduction is not constant by the code parameters. Nevertheless, reduction on complexity and latency for the proposed BECC is shown both in the synthesis result and estimation on H .

V. CONCLUSION

In this paper, we proposed the BECCs with the single burst error or two random bit error control capability using the constacyclic codes while preserving the low latency and low complexity. In the theoretical approach, the algebraic theory of constacyclic codes was used to show its error control capability. Also, numerical analysis showed that the proposed BECCs can also have the similar or lower latency and complexity properties compared to the conventional BECCs for the existing BD.

As a future work, the low-latency decoder achieving performance of the MLSD will be researched. Also, new design for different classes of integrated BECCs with burst and bit error control capability are possible considerations.

REFERENCES

- [1] D. D. Sharma, "PCI express 6.0 specification: A low-latency, high-bandwidth, high-reliability, and cost-effective interconnect with 64.0 GT/s PAM-4 signaling," *IEEE Micro*, vol. 41, no. 1, pp. 23–29, Jan./Feb. 2021.

- [2] M. Yang, S. Shahramian, H. Shakiba, H. Wong, P. Krotnev, and A. C. Carusone, "Statistical BER analysis of wireline links with non-binary linear block codes subject to DFE error propagation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 1, pp. 284–297, Jan. 2020.
- [3] P. Fire, "A class of multiple-error-correcting binary codes for non independent errors," Sylvania Reconnaissance Syst. Lab., Mountain View, CA, USA, Tech. Rep., RSL-E-2, 1959.
- [4] H. Burton and E. Weldon, "Cyclic product codes," *IEEE Trans. Inf. Theory*, vol. IT-11, no. 3, pp. 433–439, Jul. 1965.
- [5] A. Szczepanek, I. Ganga, C. Li, and M. Valliappan, "10GBASE-KR FEC tutorial," IEEE 802 Plenary, San Diego, CA, USA, Tech. Rep., Jul. 2006.
- [6] S. Cha, O. Seongil, H. Shin, S. Hwang, K. Park, S. J. Jang, J. S. Choi, G. Y. Jin, Y. H. Son, H. Cho, J. H. Ahn, and N. S. Kim, "Defect analysis and cost-effective resilience architecture for future DRAM devices," in *Proc. IEEE Int. Symp. High Perform. Comput. Archit. (HPCA)*, Austin, TX, USA, Feb. 2017, pp. 61–71.
- [7] K. C. Chun, Y. K. Kim, Y. Ryu, J. Park, C. S. Oh, Y. Y. Byun, and S. Y. Kim, "A 16-GB 640-GB/s HBM2E DRAM with a data-bus window extension technique and a synergetic on-die ECC scheme," *IEEE J. Solid-State Circuits*, vol. 56, no. 1, pp. 199–211, Jan. 2021.
- [8] K. Criss, K. Bains, R. Agarwal, T. Bennett, T. Grunzke, J. K. Kim, H. Chung, and M. Jang, "Improving memory reliability by bounding DRAM faults: DDR5 improved reliability features," in *Proc. Int. Symp. Memory Syst.*, Washington, DC, USA, Sep. 2020, pp. 317–322.
- [9] H. Hsu, T. Kasami, and R. Chien, "Error-correcting codes for a compound channel," *IEEE Trans. Inf. Theory*, vol. IR-14, no. 1, pp. 135–139, Jan. 1968.
- [10] W. Zhou, S. Lin, and K. Abdel-Ghaffar, "Burst or random error correction based on fire and BCH codes," in *Proc. Inf. Theory Appl. Workshop (ITA)*, San Diego, CA, USA, Feb. 2014, pp. 61–71.
- [11] W. Zhou, "On the maximum burst-correcting capability of cyclic HSU–Kasami–Chien codes," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2352–2355, Nov. 2017.
- [12] V. Pignoly, B. Le Gal, C. Jeco, B. Gadat, and L. Barthe, "Fair comparison of hardware and software LDPC decoder implementations for SDR space links," in *Proc. 27th IEEE Int. Conf. Electron., Circuits Syst. (ICECS)*, Glasgow, U.K., Nov. 2020, pp. 1–4.
- [13] R. Farjadrad, M. Kuemerle, and B. Vinnakota, "A bunch-of-wires (BoW) interface for interchiplet communication," *IEEE Micro*, vol. 40, no. 1, pp. 15–24, Jan. 2020.
- [14] J. S. Panchal, S. Subramanian, and R. Cavatur, "Enabling and scaling of URLLC verticals on 5G vRAN running on COTS hardware," *IEEE Commun. Mag.*, vol. 59, no. 9, pp. 105–111, Sep. 2021.
- [15] A. Krishna and D. V. Sarwate, "Pseudocyclic maximum-distance-separable codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 4, pp. 880–884, Jul. 1990.
- [16] J. M. Jensen, "A class of constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 3, pp. 951–954, May 1994.
- [17] B. Chen, W. Fang, S.-T. Xia, and F.-W. Fu, "Constructions of optimal (r, δ) locally repairable codes via constacyclic codes," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5253–5263, Aug. 2019.
- [18] C. Kim and J.-S. No, "New constructions of binary and ternary locally repairable codes using cyclic codes," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 228–231, Feb. 2018.
- [19] X. Zhang, *VLSI Architecture for Modern Error-Correcting Codes*. Boca Raton, FL, USA: CRC Press, 2016.
- [20] W. Adi, "Fast burst error-correction scheme with fire code," *IEEE Trans. Comput.*, vol. C-33, no. 7, pp. 613–618, Jul. 1984.
- [21] G. Umanesan and E. Fujiwara, "Parallel decoding cyclic burst error correcting codes," *IEEE Trans. Comput.*, vol. 54, no. 1, pp. 87–92, Jan. 2005.
- [22] R. Horn and C. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1985.



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-do, South Korea, in 2019. He was a Senior Researcher with the Division of National Supercomputing, Korea Institute of Science and Technology Information (KISTI), Daejeon, South Korea, until March 2021. He is currently an Assistant Professor with the Department of Information and Communication, Chosun University, Gwangju, South Korea. His current research interests include error-correcting codes and fault-tolerant systems for wireless communication, distributed memory and storage, and code-based post-quantum cryptography.



JAE-WON KIM (Member, IEEE) received the B.S. and Ph.D. degrees in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2014 and 2020, respectively. From 2020 to 2021, he was a Staff Engineer with Samsung Electronics Company Ltd., South Korea. In 2021, he joined Gyeongsang National University, Jinju, South Korea, where he is currently an Assistant Professor with the Department of Electronic Engineering. His research interests include error-correcting codes, coding theory, index coding, and DNA storage.



JONG-SEON NO (Fellow, IEEE) received the B.S. and M.S. 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. In 1999, he joined the Department of Electrical and Computer Engineering, Seoul National University, as a Faculty Member, where he is currently a Professor. His research interests include error-correcting codes, cryptography, sequences, LDPC codes, interference alignment, and wireless communication systems. He became a fellow of IEEE through the IEEE Information Theory Society, in 2012, and a member of the National Academy of Engineering of Korea (NAEK), in 2015, where he has served as the Division Chair of Electrical, Electronic, and Information Engineering, from 2019 to 2020. He was a recipient of the IEEE Information Theory Society Chapter of the Year Award, in 2007. From 1996 to 2008, he has served as the Founding Chair for the Seoul Chapter of the IEEE Information Theory Society. He was the General Chair of Sequence and Their Applications 2004 (SETA2004), Seoul. He has also served as the General Co-Chair for the International Symposium on Information Theory and Its Applications 2006 (ISITA2006) and the International Symposium on Information Theory 2009 (ISIT2009), Seoul, and the Co-Editor-in-Chief for the IEEE JOURNAL OF COMMUNICATIONS AND NETWORKS, from 2012 to 2013.

• • •