New Constructions of Binary and Ternary Locally Repairable Codes Using Cyclic Codes

Chanki Kim, *Student Member, IEEE*, and Jong-Seon No, *Fellow, IEEE*

***Abstract*— New constructions of binary and ternary locally repairable codes (LRCs) using cyclic codes and their concatenation are proposed. The proposed binary LRCs with $d = 4$ and some r and with $d \geq 5$ and some n are shown to be optimal in terms of the upper bounds. In addition, the similar method of the binary case is applied to construct the ternary LRCs with good parameters.**

***Index Terms*— Cyclic codes, distributed storage systems (DSSs), locally repairable codes (LRCs).**

I. Introduction

FOR a decade, coding for distributed storage systems (DSSs) has attracted a considerable amount of attention from researchers as the demand for data centers based on DSS grows exponentially. In particular, regenerating codes and locally repairable codes (LRCs) are mostly studied. LRC is designed to minimize the number of storage nodes to be accessed during the repair process, called the locality r.

For practical usefulness, attempts to construct the optimal binary LRCs have also been made, some of which achieve the optimality [1], [2]. Similarly, ternary LRCs were studied [3], where several constructions were proposed. Moreover, cyclic LRCs were introduced in [4]. In this paper, new constructions of binary and ternary LRCs are proposed. For the binary case, it is shown that the proposed LRCs with $d = 4$ and some r and with $d \geq 5$ and some n are shown to be optimal in terms of the upper bounds in [5] and [7]. The similar construction of binary case is applied to the ternary ones, where ternary LRCs with good parameters are constructed.

II. Preliminary

In this section, the mathematical notations and definitions as well as some bounds on LRCs are summarized. All operations are based on the finite field F_q, where q is a prime power. Let $\mathbf{v}$ be a row vector and v_i be the i-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 by $\text{supp}(\mathbf{v}) = \{i; v_i \neq 0\}$ and the Hamming weight of $\mathbf{v}$ by $\text{wt}(\mathbf{v}) = |\text{supp}(\mathbf{v})|$. Let $[a, b] = \{i \in Z^+;\ a \leq i \leq b\}$ and $[i] = [0, i]$ for the set of nonnegative integers Z^+.

Let $\mathcal{C}$ be a code with the parameters (n, k, d), where n is the codelength, k the dimension, and d the minimum distance. Then, $\mathcal{C}$ has a $k \times n$ generator matrix G and $(n-k) \times n$ parity check matrix H. Let $\mathbf{h}_i, i \in [n-k-1]$ be the row vector of H, which is called a *check*.

In general, LRC has the parameters (n, k, d, r), where r is locality. It is clear that LRC with locality r should satisfy the condition that the union of supports of checks whose Hamming weights are less than or equal to $(r+1)$ is equal to $[n-1]$. The trade-off between d and r has been studied, where (n, k, d, r) LRC is said to be r-optimal if (n, k, d, r') LRC does not exist for $r' < r$. Similarly, (n, k, d, r) LRC is said to be d-optimal and k-optimal if (n, k, d', r) and (n, k', d, r) LRCs do not exist for $d' > d$ and $k' > k$, respectively. LRC is said to be optimal if LRC is r-optimal, d-optimal, and k-optimal. Moreover, the well-known bounds for LRCs are listed as follows.

Proposition 1 Singleton-Like Bound [5]: For an (n, k, d, r) LRC,

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2. \tag{1}$$

Proposition 2 Cadambe-Mazumda (C-M) Bound [6]: For an (n, k, d, r) linear LRC,

$$k \leq \min_{x \in Z^+} \{xr + k_{\text{opt}}^{(q)}(n - x(r+1), d)\} \tag{2}$$

where $k_{\text{opt}}^{(q)}(a, b)$ is the largest possible code dimension for codelength a and minimum distance b of the linear code over F_q.

Recently, more explicit bound for binary LRCs with $d \geq 5$ was proposed as follows.

Proposition 3 LRC Bound [7]: For an (n, k, d, r) linear binary LRC with $d \geq 5$ and $2 \leq r \leq \frac{n}{2} - 2$, it holds

$$k \leq \frac{rn}{r+1} - \min\left\{\log_2\left(1 + \frac{rn}{2}\right), \frac{rn}{(r+1)(r+2)}\right\}. \tag{3}$$

III. Constructions of Binary LRCs Using Cyclic Codes

In this section, new binary LRCs are proposed by using cyclic codes, where some of them are optimal in terms of bounds in (1), (2), and (3).

Construction 1 (Cyclic Binary LRCs With $d = 4$): For $(r+1)|n$, let $v = \frac{n}{r+1}$ and $u = r + 1$, where $\gcd(u, v) = 1$ and $u, v \geq 2$. Let $g(x)$ be a generator polynomial of the cyclic binary LRC and β' be an u-th root of unity. Then, $(uv, uv - \deg(g(x)), 4, u-1)$ binary LRCs can be constructed by the following generator polynomials:

1) For $2|r$, $g(x) = (x^v + 1)g_1(x)$, where $g_1(x)$ is the minimal polynomial of β' over F_2.
2) For $r = 2^m - 1$, $g(x) = (x^v + 1)(x+1)^{2^m - 1}$, where m is a positive integer.

Proof: First, we have to prove that they are LRCs, that is, there are at least one check with Hamming weight $r + 1$.

Manuscript received October 10, 2017; accepted November 9, 2017. Date of publication November 21, 2017; date of current version February 9, 2018. This work was supported by the Samsung Electronics Co., Ltd., in Korea and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. NRF-2016R1A2B2012960). The associate editor coordinating the review of this paper and approving it for publication was N. Tran. *(Corresponding author: Jong-Seon No.)*

The authors are with the Department of Electrical and Computer Engineering, Institute of New Media and Communications, Seoul National University, Seoul 08826, South Korea (e-mail: carisis@ccl.snu.ac.kr; jsno@snu.ac.kr).

Digital Object Identifier 10.1109/LCOMM.2017.2776141

Since $(x^{\upsilon}+1)|g(x)$, $1+x^{\upsilon}+\ldots+x^{(u-1)\upsilon}$ can be a check of H. Thus, the proposed codes are LRC with $r=u-1$.

Next, it is necessary to prove that the minimum distance of the proposed LRCs is 4. It is easy to check that there is no codeword with odd Hamming weight for both cases of $g(x)$. Subsequently, we have to prove the nonexistence of codewords with Hamming weight 2 and the existence of codewords with Hamming weight 4.

For $2|r$, suppose that we have a codeword $c(x)$ with Hamming weight 2. Since $(x^{\upsilon}+1)|c(x)$, $c(x)=1+x^{\upsilon l}, l\in[u-1]$. Further, $c(\beta')=0$, that is, $(\beta')^{\upsilon l}=1$ and $u|(\upsilon l)$ and thus, $l=0$ from $\gcd(u,\upsilon)=1$. Then, $c(x)=1+1=0$, which contradicts the assumption. Thus, there is no codeword with Hamming weight 2. It is easy to check that $g(x)$ divides $(1+x^{u})(1+x^{\upsilon})$, which is a codeword with Hamming weight 4.

For $r=2^m-1$, suppose that there exists a codeword $c(x)$ with Hamming weight 2. Since $(x^{2^{m-1}}+1)|c(x)$, $c(x)=x^{l2^{m-1}}+1, l\in[2\upsilon-1]$. Since $c(x)=(x^{2^{m-1}}+1)(x^{(l-1)2^{m-1}}+x^{(l-2)2^{m-1}}+\ldots+x^{2^{m-1}}+1)$, $(x+1)$ should divide $(x^{(l-1)2^{m-1}}+x^{(l-2)2^{m-1}}+\ldots+x^{2^{m-1}}+1)$ and thus l should be even. Let $l=2l'$. Then, $c(x)=x^{l'2^m}+1$, which satisfies $c(\beta'')=0$, where β'' is a υ-th root of unity. Then, $(\beta'')^{l'2^m}=1$. Given that $u=2^m$, $\gcd(u,\upsilon)=1$, and $l'\in[\upsilon-1]$, we have $l=0$ and $c(x)=1+1=0$, which contradicts the assumption. Thus, there is no codeword with Hamming weight 2. Since $g(x)=x^{2^{m-1}+\upsilon}+x^{2^{m-1}}+x^{\upsilon}+1$, there exists a codeword with Hamming weight 4. ∎

Some classes in Construction 1 are optimal or r-optimal as in the following proposition.

Proposition 4 (Optimality of Construction 1): For LRCs in Construction 1, two classes of $(2l, l-1, 4, 1)$ and $(4l, 3l-2, 4, 3)$ cyclic binary LRCs are optimal for $l\geq 3$, $\gcd(2,l)=1$ and one class of $(3l, 2l-2, 4, 2)$ proposed cyclic binary LRC is r-optimal by (1) for $l\geq 4$, $\gcd(3,l)=1$.

Proof: Two classes of the proposed $(2l, l-1, 4, 1)$ and $(4l, 3l-2, 4, 3)$ LRCs have the same parameters as the optimal binary LRCs in [8, Construction 1]. If the class of proposed $(3l, 2l-2, 4, 2)$ LRC is not r-optimal, the inequality $\frac{k}{n}\leq\frac{n-2}{2n}$ derived from (1) for LRC with $r=1$ should be satisfied but it does not hold for $l\geq 4$, which tells that the class of proposed $(3l, 2l-2, 4, 2)$ LRC is r-optimal. ∎

Optimal or r-optimal LRCs with the same parameters were also introduced in [8] and [9], but they were not cyclic.

Noncyclic binary LRCs with larger minimum distance are also proposed as in the following construction.

Construction 2 (Linear Binary LRC With $d\geq 6$ and $r=2$): Let β be a primitive element of the finite field F_{2^m} and n a positive integer larger than or equal to 9 and divisible by 3 such that $\frac{2n}{3}\leq 2^m-1$. Let $\mathcal{C}_E$ be a $(2^m-1, 2^m-m-2, 4)$ expurgated Hamming code with generator polynomial $g(x)=(x+1)g_1(x)$, where $g_1(x)$ is the minimal polynomial of β over F_2. A $(\frac{2n}{3}, \frac{2n}{3}-m-1, \geq 4)$ shortened expurgated Hamming code $\mathcal{C}_S$ can be generated by shortening the first $(2^m-\frac{2n}{3}-1)$ information bits of $\mathcal{C}_E$. Then, concatenation of $\mathcal{C}_S$ and an $(n, \frac{2n}{3})$ cyclic code with parity check polynomial $x^{\frac{2n}{3}}+x^{\frac{n}{3}}+1$ as an inner code makes an $(n, \frac{2n}{3}-\lceil\log_2(\frac{2n}{3}+1)\rceil-1, d\geq 6, 2)$ LRC $\mathcal{C}_C$.

TABLE I

THE OPTIMALITY OF THE EXISTING BINARY LRCS WITH $d=6$ AND $r=2$

	(n,k), conditions	r-opt	k-opt	d-opt
Thm. 1 in [1]	$(2^m-1, \frac{2n}{3}-m), 2\|m$	O	O	O
Cor. 1 in [10]	$(3s, 2s-4), 4\leq s\leq 5$	O	O	O

Proof: Let H_E and H_S be the parity check matrices of $\mathcal{C}_E$ and $\mathcal{C}_S$, respectively. Let $H_E=[H_1'\ H_2'\ H_3']$ and $H_S=[H_2'\ H_3']$, where H_1' is the $(m+1)\times(2^m-1-\frac{2n}{3})$ matrix and H_2' and H_3' are the $(m+1)\times\frac{n}{3}$ matrices. The parity check matrix of the cyclic inner code can be given as $H_I=[I_{\frac{n}{3}}\ I_{\frac{n}{3}}\ I_{\frac{n}{3}}]$. The parity check matrix of the proposed LRC is then given as

$$H=\begin{bmatrix}H_O\\ H_I\end{bmatrix}=\begin{bmatrix}H_2' & H_3' & O\\ I_{\frac{n}{3}} & I_{\frac{n}{3}} & I_{\frac{n}{3}}\end{bmatrix} \tag{4}$$

where O denotes the $(m+1)\times\frac{n}{3}$ zero matrix. It is easily verified that the locality of LRC is 2 from the lower part of H, H_I. Adding all of the rows of H_I makes an all-one vector and thus, there is no codeword with odd Hamming weight. At this stage, we have to prove that there is no codeword with Hamming weight 4. Suppose that there is a codeword with Hamming weight 4. Since the minimum distance of $\mathcal{C}_S$ is larger than or equal to 4, the nonzero elements of the codeword with Hamming weight 4 should be located in the first $\frac{2n}{3}$ elements of the codeword. In order to satisfy H_I, the codeword polynomial should be a form of $c(x)=x^i+x^j+x^{i+\frac{n}{3}}+x^{j+\frac{n}{3}}=(x^i+x^j)(1+x^{\frac{n}{3}})$, $0\leq i<j<\frac{n}{3}$. Clearly, $g_1(x)|c(x)$ and thus $c(\beta)=0$ but $\beta^{\frac{n}{3}}\neq 1$ and $\beta^i+\beta^j\neq 0$. Thus, there is no codeword with Hamming weight 4. ∎

Using (3), the optimality of the LRCs in Construction 2 can be stated as follows:

Proposition 5 (Optimality of Construction 2): Let k_{opt} and k be the dimensions of the LRCs satisfying the equality in (3) and the proposed LRCs in Construction 2, respectively. If $n\geq 33$, the proposed LRCs are r-optimal. Further, if $n\geq 33$ and $\lceil\log_2(\frac{2n}{3}+1)\rceil+1=\lceil\log_2(1+n)\rceil$, the proposed LRCs are r-optimal and k-optimal.

Proof: If $n=33$ or 36, $k=k_{opt}$ by (3) and thus LRC is r- and k-optimal. For $n\geq 39$, the proposed LRC is also r-optimal by (1), because (1) is rewritten as $\frac{k}{n}\leq\frac{k_{opt}}{n}=\frac{2}{3}-\frac{\lceil\log_2(n+1)\rceil}{n}\leq\frac{n-2}{2n}\leq\frac{1}{2}$ for $r=1$, that is, $\frac{n}{6}\leq\lceil\log_2(n+1)\rceil$. Thus it does not hold for $n\geq 39$ and $r=1$, which tells that the proposed LRC with $n\geq 33$ is r-optimal. Also, $k_{opt}=\frac{2n}{3}-\lceil\log_2(n+1)\rceil$ and $k=\frac{2n}{3}-\lceil\log_2(\frac{2n}{3}+1)\rceil-1$ and thus if $\lceil\log_2(\frac{2n}{3}+1)\rceil+1=\lceil\log_2(1+n)\rceil$, the proposed LRCs are r-optimal and k-optimal, i.e., $k=k_{opt}$. ∎

Note that (3) does not gaurantee d-optimal because (3) is valid for $d\geq 5$. Table I shows the parameters of optimal LRCs with $d=6$ and $r=2$ from the existing works [1], [10]. Thus, Construction 2 gives us new binary r- and k-optimal LRCs.

For $r\geq 3$, there is a construction of LRC based on nonlinear codes as in the following construction.

Construction 3 (Nonlinear Binary LRC With $d\geq 5$ and $r\geq 3$): Let β be a primitive element of the finite field F_{2^m} and n a positive integer such that $n+1$ is divisible by $r+1$.

Let υ be $\frac{n+1}{r+1}$ and m should satisfy $r\upsilon \leq 2^m - 1$. Let $\mathcal{C}_E$ be a $(2^m - 1, 2^m - m - 2, 4)$ expurgated Hamming code as defined in the previous construction. An $(r\upsilon, r\upsilon - m - 1, \geq 4)$ shortened expurgated Hamming code $\mathcal{C}_S$ can be generated by shortening the first $(2^m - r\upsilon - 1)$ information bits of $\mathcal{C}_E$. Then, the $(n+1, r\upsilon - m - 1, \geq 4, r)$ linear LRC $\mathcal{C}_C$ can be constructed by concatenating $\mathcal{C}_S$ and an $(n+1, r\upsilon)$ cyclic code with parity check polynomial $x^{r\upsilon} + x^{(r-1)\upsilon} + \ldots + x^{\upsilon} + 1$. By selecting all codewords with the i-th element 1 for a fixed $i \in [r\upsilon, n]$ and deleting the i-th elements from the selected codewords, an $(n, 2^{r\upsilon - m - 2}, \geq 5, r)$ nonlinear binary LRC can be constructed.

Proof: Let H_S be a parity check matrix of $\mathcal{C}_S$. A parity check matrix of the $(n, r\upsilon)$ cyclic code can be given as $H_I = [I_\upsilon \ \ldots \ I_\upsilon] = [H'_L \ I_\upsilon]$, where H'_L is a $\upsilon \times r\upsilon$ matrix consisting of r I_υ's. Then, the parity check matrix of the proposed LRC is given as

$$H = \begin{bmatrix} H_O \\ H_I \end{bmatrix} = \begin{bmatrix} H_S & O \\ H'_L & I_\upsilon \end{bmatrix}$$

where O denotes the $(m+1) \times \upsilon$ zero matrix. It is easily checked that the locality of LRC is r from the lower part of H, H_I. Adding all of the rows of H_I makes an all-one vector and thus, there is no codeword with odd Hamming weight. Now, we have to prove that there is no codeword with Hamming weight 4. Suppose that there is a codeword with Hamming weight 4. Since the minimum distance of $\mathcal{C}_S$ is larger than or equal to four, the nonzero elements of the codeword with Hamming weight 4 should be located in the first $r\upsilon$ elements of the codeword. If the codewords with nonzero elements in the index $[r\upsilon, n]$ exist, their Hamming weights are larger than or equal to six. Since we select the codewords with the i-th element 1 for a fixed $i \in [r\upsilon, n]$, the selected code has the minimum Hamming weight larger than or equal to six. By deleting the i-th elements from all selected codewords, their minimum Hamming weight is larger than or equal to five. At this point, we have to prove the number of codewords of the proposed LRCs. First, we can decompose $\mathcal{C}_C$ into two classes, that is, a set of codewords with the i-th element 1, $\mathcal{C}_1^{(i)}$ and a set of the remaining codewords, $\mathcal{C}_0^{(i)}$. Let $\mathbf{c}_i$ be a codeword of $\mathcal{C}_1^{(i)}$. Then for any $\mathbf{c}_j$ in $\mathcal{C}_1^{(i)}$, $\mathbf{c}_i \bigoplus \mathbf{c}_j$ belongs to $\mathcal{C}_0^{(i)}$ and thus $|\mathcal{C}_1^{(i)}| \leq |\mathcal{C}_0^{(i)}|$. Further, for any $\mathbf{c}_k$ in $\mathcal{C}_0^{(i)}$, $\mathbf{c}_i \bigoplus \mathbf{c}_k$ belongs to $\mathcal{C}_1^{(i)}$ and thus $|\mathcal{C}_0^{(i)}| \leq |\mathcal{C}_1^{(i)}|$. Accordingly, $|\mathcal{C}_0^{(i)}| = |\mathcal{C}_1^{(i)}| = 2^{r\upsilon - m - 2}$, which is the number of codewords of the proposed LRCs. ∎

In order to encode the proposed LRCs in Construction 3, the parity check matrix of $\mathcal{C}_C$ in Fig. 1 is used, where $m + 1 < \upsilon$. Assume that index i is set to $r\upsilon$, whose element will be 'deleted' from all codewords of $\mathcal{C}_1^{(i)}$ later. For the message vector $\mathbf{m} = (m_1, m_2, \ldots, m_{r\upsilon - m - 2})$, the codeword can be given as $\mathbf{c} = (p_0, m_1, m_2, \ldots, m_{r\upsilon - m - 2}, p_1, p_2, \ldots, p_{(r+1)\upsilon - 1})$, where $p_{m+2} = 1$ will be deleted for the proposed LRCs. First, the value of p_0 is computed by the $(m+1)$-th row of H_C, $\mathbf{m}$, and $p_{m+2} = 1$. Then, the values of $p_1, p_2, \ldots, p_{m+1}$ are computed using H_S and the values of $p_{m+3}, p_{m+4}, \ldots, p_{m+\upsilon+1}$ can also be computed by H_I. The codeword of the proposed LRC is then given as $(p_0, m_1, m_2, \ldots, m_{r\upsilon - m - 2}, p_1, p_2, \ldots, p_{m+1}, p_{m+3}, p_{m+4}, \ldots, p_{m+\upsilon+1})$. Thus, the encoding procedure of the proposed LRCs is identical to that of the linear code C_C.

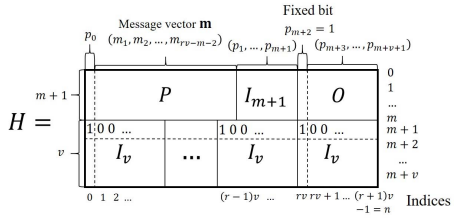

Fig. 1. Parity check matrix of the LRC in Construction 3 with $i = r\upsilon$.

TABLE II
CODELENGTH OF r-OPTIMAL LRCS IN CONSTRUCTION 3 WITH $r \in [3, 8]$

r	3	4	5	6	7	8
n	≥ 67	≥ 124	≥ 209	≥ 286	≥ 431	≥ 620

TABLE III
THE OPTIMALITY OF THE PROPOSED BINARY LRCS

	Conditions	r-opt	k-opt	d-opt
Const.1	Class with $d = 4$, $r = 2$ of Prop. 4	O	?	?
Const.1	Classes with $d = 4$, $r = 1, 3$ of Prop. 4	O	O	O
Const.2	$d \geq 6$, $r = 2$, $n \geq 33$, $3 \mid n$	O	?	?
Const.2	$d \geq 6$, $r = 2$, $n \geq 33$, $3 \mid n$ $\lceil \log_2(\frac{2n}{3} + 1) \rceil + 1 = \lceil \log_2(1+n) \rceil$	O	O	?
Const.3	$d \geq 5$, $(r+1) \mid (n+1)$, Prop. 6	O	?	?
Exam.1	$(n, k, d, r) = (20, 10, 6, 3)$	O	O	O

Using (1), the optimality of the LRCs in Construction 3 can be stated as follows:

Proposition 6 (Optimality of Construction 3): For some n, the proposed binary LRCs in Construction 3 is r-optimal.

Similar to the proof of the previous cases, it can be easily checked that (1) does not hold for $(n, k, d, r-1)$ LRC in Construction 3. Table II lists the codelength of r-optimal LRCs for $r \in [3, 8]$ in Construction 3.

As a special case for the short codelength, we can modify Constructions 3 as in the following example to construct binary LRC.

Example 1 (Construction of Linear Binary LRC With $r = 3$): Linear binary LRC with $d = 6$ and $r = 3$ can be constructed for short codelength without deleting the i-th bit in Construction 3. A (20, 10, 6, 3) LRC is constructed by using a (15, 10, 3) binary cyclic code with $g(x) = (x^4 + x + 1)(x + 1)$, which is optimal by (2) and better than dimension 9 from [2] and [10].

Table III summarizes the optimality of the proposed binary LRCs.

IV. CONSTRUCTIONS OF LINEAR TERNARY LRCS USING CYCLIC CODES

Using the construction method of the binary LRCs, two linear ternary LRCs are proposed in the following constructions.

Construction 4 (Linear Ternary LRCs of $d \geq 5$ and $r = 2$): Let β be a primitive element of the finite field F_{3^m} and n a positive integer divisible by 3 such that $\frac{2n}{3} \leq 3^m - 1$. Let $\mathcal{C}_E$ be a $(3^m - 1, 3^m - m - 2, 3)$ cyclic code with generator polynomial $g(x) = (x - 1)g_1(x)$, where $g_1(x)$ is the minimal polynomial

of β over F_3. A $(\frac{2n}{3}, \frac{2n}{3} - m - 1, \geq 3)$ shortened code $\mathcal{C}_S$ can be generated by shortening the first $3^m - 1 - \frac{2n}{3}$ information bits of $\mathcal{C}_E$. Then, concatenation of $\mathcal{C}_S$ and an $(n, \frac{2n}{3})$ cyclic code $\mathcal{C}_C$ with parity check polynomial $x^{\frac{2n}{3}} + x^{\frac{n}{3}} + 1$ as an inner code makes an $(n, \frac{2n}{3} - \lceil \log_3(\frac{2n}{3} + 1) \rceil - 1, d \geq 5, 2)$ linear ternary LRC.

Proof: It is easy to check that $\mathcal{C}_E$ has $d \geq 3$ by BCH bound and two consecutive zeros $\{1, \beta\}$. Let H_E and H_S be parity check matrices of $\mathcal{C}_E$ and $\mathcal{C}_S$, respectively. Similarly to Construciton 2, the parity check matrix of the proposed LRCs is given as (4).

Then, the locality of the proposed LRC is 2 and we have to prove that there is no codeword with Hamming weights of 3 and 4. Suppose that there is a codeword with Hamming weight 3. Since the minimum Hamming weight of $\mathcal{C}_S$ is larger than or equal to 3, the nonzero elements of the codeword with Hamming weight 3 should be located in the first $\frac{2n}{3}$ elements of the codeword. Then, the codeword polynomial should be $c_1(x) = a_1x^i + a_2x^j + a_3x^{i+\frac{n}{3}}$ or $c_2(x) = a_1x^i + a_2x^j + a_3x^k$, $0 \leq i < j < k < \frac{n}{3}$ and $a_1, a_2, a_3 \in \{-1, 1\}$. It is easy to check that the checksum of H_I cannot be satisfied for the both cases. If the codeword with Hamming weight 4 has three nonzero elements located in $[\frac{2n}{3} - 1]$ and the other in $[\frac{2n}{3}, n - 1]$, it cannot be a codeword because the check $[\mathbf{0}_{\frac{2n}{3}}, \mathbf{1}_{\frac{n}{3}}]$ can be obtained by subtracting $[\mathbf{1}_{\frac{2n}{3}}, \mathbf{0}_{\frac{n}{3}}]$ by $(x-1)$ in $g(x)$ from $[\mathbf{1}_n]$ by H_I. Thus, the codeword with Hamming weight 4 has four nonzero elements in $[\frac{2n}{3} - 1]$, which can be represented as $c(x) = (a_1x^i + a_2x^j)(1 - x^{\frac{n}{3}})$, $0 \leq i < j < \frac{n}{3}$, $a_1, a_2 \in \{-1, 1\}$ because it should satisfy H_I. Then, $c(\beta) \neq 0$ because $\beta^{\frac{n}{3}} \neq 1$ and $\beta^{(j-i)} \neq \pm 1$. Thus, there is no codeword with Hamming weight 4. ■

Note that the $(12, 5, 6, 2)$ ternary LRC constructed in Construction 4 has the same parameters as those of the eight classes of the optimal ternary LRCs in [3] by (1).

In addition, the linear ternary LRC of $r = 3$ can also be constructed as follows.

Construction 5 (Linear Ternary LRC of $d \geq 5$ and $r = 3$): Let β be a primitive element of the finite field F_{3^m} and n a positive integer divisible by 4 such that $\frac{3n}{4} \leq 3^m - 1$. Let $\mathcal{C}_E$ be a $(3^m - 1, 3^m - 1 - 2m, 4)$ ternary BCH code with $g(x) = g_1(x)g_2(x)$, where $g_1(x)$ and $g_2(x)$ are the minimal polynomials of β and β^2 over F_3, respectively. A $(\frac{3n}{4}, \frac{3n}{4} - 2m, \geq 5)$ shortened code $\mathcal{C}_S$ can be generated by shortening the first $3^m - 1 - \frac{3n}{4}$ information bits of $\mathcal{C}_E$. Then, concatenation of $\mathcal{C}_S$ and an $(n, \frac{3n}{4})$ cyclic code $\mathcal{C}_C$ with parity check polynomial $x^{\frac{3n}{4}} + x^{\frac{2n}{4}} + x^{\frac{n}{4}} + 1$ as an inner code makes an $(n, \frac{3n}{4} - 2\lceil \log_3(\frac{3n}{4} + 1) \rceil, d \geq 5, 3)$ linear ternary LRC.

Proof: It is easily checked that the locality of the proposed LRC is 3 by the parity check polynomial of $\mathcal{C}_S$. Then, we have to prove that there is no codeword with Hamming weight 4. If there is a codeword with Hamming weight 4, its nonzero element should be located in $[\frac{3n}{4} - 1]$ because C_S has the minimum Hamming weight 4 by BCH bound and the three consecutive zeros. For $a_1, a_2 \in \{-1, 1\}$ and $i \neq j \in [\frac{n}{4} - 1]$, the codewords with Hamming weight 4 can be expressed as in the following five cases;

1) $c_1(x) = x^l(a_1x^i + a_2x^j - a_1x^{i+\frac{n}{4}} - a_2x^{j+\frac{n}{4}}) = x^l(1 - x^{\frac{n}{4}})(a_1x^i + a_2x^j)$ for $l \in \{0, \frac{n}{4}\}$.
2) $c_2(x) = a_1x^i + a_2x^j - a_1x^{i+\frac{2n}{4}} - a_2x^{j+\frac{2n}{4}} = (1 - x^{\frac{2n}{4}})(a_1x^i + a_2x^j)$.
3) $c_3(x) = a_1x^i + a_2x^j - a_1x^{i+\frac{n}{4}} - a_2x^{j+\frac{2n}{4}} = (1 - x^{\frac{n}{4}})(a_1x^i + a_2x^j(1 + x^{\frac{n}{4}}))$.
4) $c_4(x) = a_1x^i + a_2x^{j+\frac{n}{4}} - a_1x^{i+\frac{2n}{4}} - a_2x^{j+\frac{2n}{4}} = -x^{\frac{2n}{4}}(1 - x^{-\frac{n}{4}})(a_1x^i + a_2x^j(1 + x^{-\frac{n}{4}}))$.
5) $c_5(x) = a_1x^i + a_2x^{j+\frac{n}{4}} - a_1x^{i+\frac{n}{4}} - a_2x^{j+\frac{2n}{4}} = (1 - x^{\frac{n}{4}})(a_1x^i - a_2x^{j+\frac{n}{4}})$.

For the proofs of 1) and 2), it is easy to check that $c_1(\beta) \neq 0$ because $\beta^{\frac{n}{4}} \neq 1$ and $\beta^{j-i} \neq \pm 1$ and $c_2(\beta) \neq 0$ because $\beta^{\frac{2n}{4}} \neq 1$. For 3), we have to prove $c_3(\beta^k) \neq 0$ for at least one $k \in [1, 3]$. Suppose $\beta^{\frac{n}{4}}, \beta^{\frac{2n}{4}}, \beta^{\frac{3n}{4}} \neq -1$. Clearly, $\beta^{\frac{kn}{4}} \neq 1$ for $k \in [1, 3]$ and we have $a_1\beta^i + a_2\beta^j(\beta^{\frac{n}{4}} + 1) = a_1\beta^{2i} + a_2\beta^{2j}(\beta^{\frac{2n}{4}} + 1) = a_1\beta^{3i} + a_2\beta^{3j}(\beta^{\frac{3n}{4}} + 1) = 0$ by $c_3(\beta) = c_3(\beta^2) = c_3(\beta^3) = 0$. Then, $\beta^i = \frac{a_1\beta^{2i}}{a_1\beta^i} = \frac{-a_2\beta^{2j}(\beta^{\frac{2n}{4}}+1)}{-a_2\beta^j(\beta^{\frac{n}{4}}+1)}$ and also $\beta^i = \frac{a_1\beta^{3i}}{a_1\beta^{2i}} = \frac{-a_2\beta^{3j}(\beta^{\frac{3n}{4}}+1)}{-a_2\beta^{2j}(\beta^{\frac{2n}{4}}+1)}$. Thus, we have $(\beta^{\frac{2n}{4}} + 1)^2 = (\beta^{\frac{n}{4}} + 1)(\beta^{\frac{3n}{4}} + 1)$, which can be rewritten as $\beta^{\frac{n}{4}}(\beta^{\frac{n}{4}} - 1)^2 = 0$ and it contradicts. If $\beta^{\frac{kn}{4}} = -1$ for some $k \in [1, 3]$, $c_3(\beta^k) = (1 + 1)(a_1\beta^{ki}) \neq 0$. Similarly, 4) can be proved. For 5), $\beta^{j-i+\frac{n}{4}} = 1$ by $\beta^i = \frac{a_1\beta^{2i}}{a_1\beta^i} = \beta^{j+\frac{n}{4}}$ and $c_5(\beta) = c_5(\beta^2) = 0$, but there is a contradiction. Thus, there is no codeword with Hamming weight 4. ■

V. Conclusion

In this paper, several binary and ternary constructions of LRCs by cyclic codes are proposed. Some of the proposed binary LRCs are optimal. As a future work, it is necessary to verify the optimality of the other proposed LRCs.

References

[1] S. Goparaju and R. Calderbank, "Binary cyclic codes that are locally repairable," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Honolulu, HI, USA, Jun./Jul. 2014, pp. 676–680.

[2] P. Huang, E. Yaakobi, H. Uchikawa, and P. H. Siegel, "Binary linear locally repairable codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6268–6283, Nov. 2016.

[3] J. Hao, S.-T. Xia, and B. Chen, "On optimal ternary locally repairable codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 171–175.

[4] I. Tamo, A. Barg, S. Goparaju, and R. Calderbank, "Cyclic LRC codes and their subfield subcodes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, Jun. 2015, pp. 1262–1266.

[5] I. Tamo and A. Barg, "A family of optimal locally recoverable codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4661–4676, Aug. 2014.

[6] V. R. Cadambe and A. Mazumdar, "Bounds on the size of locally recoverable codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 5785–5794, Nov. 2015.

[7] A. Wang, Z. Zhang, and D. Lin, "Bounds and constructions for linear locally repairable codes over binary fields," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 2033–2037.

[8] J. Hao, S.-T. Xia, and B. Chen, "Some results on optimal locally repairable codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 440–444.

[9] M. Shahabinejad, M. Khabbazian, and M. Ardakani, "A class of binary locally repairable codes," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3182–3193, Aug. 2016.

[10] M.-Y. Nam and H.-Y. Song, "Binary locally repairable codes with minimum distance at least six based on partial t-spreads," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1683–1686, Aug. 2017.