A Bound on the Minimal Field Size of LRCs, and Cyclic MR Codes That Attain It

Han Cai⬚, *Member, IEEE*, and Moshe Schwartz⬚, *Senior Member, IEEE*

Abstract—We prove a new lower bound on the field size of locally repairable codes (LRCs). Additionally, we construct maximally recoverable (MR) codes which are cyclic. While a known construction for MR codes has the same parameters, it produces non-cyclic codes. Furthermore, we prove both necessary conditions and sufficient conditions that specify when the known non-cyclic MR codes may be permuted to become cyclic, thus proving our construction produces cyclic MR codes with new parameters. Furthermore, using our new bound on the field size, we show that the new cyclic MR codes have optimal field size in certain cases. Other known LRCs are also shown to have optimal field size in certain cases.

Index Terms—Distributed storage, locally repairable codes, maximally recoverable codes, cyclic codes.

I. INTRODUCTION

IN LARGE-SCALE cloud storage and distributed file systems, such as Amazon Elastic Block Store (EBS) and Google File System (GoogleFS), disk failures are the norm and not the exception, due to the sheer scale of the system. To protect the data integrity, coding theory is used to recover from data loss due to disk failures. The simplest solution for those systems is a straightforward replication of data packets across different disks. However, this solution is costly especially for large-scale systems since it suffers from a large storage overhead. As an alternative solution, erasure codes such as $[n, k]$ maximum distance separable (MDS) codes, may be employed as storage codes. These codes encode k information symbols to n symbols and store them across n disks, and they can recover from the loss of any $n - k$ symbols. This scheme achieves a dramatic improvement in redundancy compared with replication. However, for MDS codes, even if one disk fails, the system needs to access k surviving disks in order to recover the lost symbol, which makes the repair process costly.

One method to improve the repair efficiently, suggested in [17], is endow the code with a locality property. This property allows a failed symbol to be recovered by accessing only $r \ll k$ other symbols. Erasure codes with locality are also called locally repairable codes (LRCs). The original concept of locality only works when exactly one erasure occurs (that is, one disk fails). In the past decade, the notion of locality further generalized in several directions. For example, LRCs with (r, δ)-locality [31] allow an erased symbol to be recovered by reading r other symbols, even if the repair set suffered $\delta - 1$ more erasures. Other examples include: locality which guarantees disjoint multiple repairable sets (also named as availability) [6], [8], [35], [40], locality which has a hierarchical structure [14], [36], and unequal localities [22], [26], [44].

Other code properties are also desirable. For a given code length n and dimension k, we would like the Hamming distance to be as large as possible, in order to maximize erasure-correcting capabilities. Additionally, we would like the field size (or alphabet size) to be as small as possible, in order to reduce the computation complexity for coding and decoding. Other desirable properties may include a cyclic structure for the code, since it allows for fast encoding algorithms. Finally, even if the code has optimal distance, we would like to be able to correct some pre-determined erasure patterns beyond the minimum Hamming distance.

In the past a few years, many results have been obtained for LRCs. Upper bounds on the minimum Hamming distance were proved, e.g., Singleton-type bounds [7], [17], [31], [41], and bounds related with the alphabet size [1], [5]. Optimal LRCs (with respect to these bounds), were constructed, e.g., [13], [24], [28], [34], [37], [38], [42]. In [21] and [9], lower bounds on the field size of optimal LRCs were derived for $\delta = 2$ [21], and $\delta \geqslant 2$ [9]. Among the known optimal LRCs, some of them also achieve order-optimal field size [2], [12], [25], [43] when $\delta = 2$, and [9] when $\delta \geqslant 2$. Otherwise, constructions of optimal cyclic LRCs were introduced in [13], [14], [32], [39], and [33]. When considering pre-determined recoverable erasure patterns beyond the minimum Hamming distance, codes that can recover from all information-theoretically recoverable erasure patterns are called maximally recoverable (MR) codes [17], also known as partial MDS codes [3]. In [19], lower bounds on the field size requirement for MR codes were introduced. For explicit constructions of MR codes, the reader may refer to [3], [10], [15], [16], [20], [28], and [18]. Notably, there are MR codes have order-optimal field size (with respect to the bound in [19]): [3] for a single global parity check

($h = 1$), [4], [19] for $h = 2$, [16] for $h = 3$ and $\delta = 2$, and [10], [18] for $h \leqslant \delta + 1$ a constant, and $n = \Theta(r^2)$.

The above summary shows how subsets of the mentioned desired properties may be obtained simultaneously. However, to the best of our knowledge, there are no explicit constructions that achieve all them, namely, cyclic MR codes with optimal field size. In this paper, our motivation is to construct cyclic MR codes with optimal field size, or order-optimal field size. To this end, we work both on constructions for cyclic MR codes, and a theoretic bound on the field size of optimal LRCs (containing MR codes as special cases). In the first part of the paper we prove a new general bound for optimal LRCs. We compare our new bound with the known bounds, and show that it is tighter for some parameters. In the second part of the paper, we introduce a new construction for cyclic MR codes. Our construction produces cyclic MR codes that share the same parameters as one of the known non-cyclic constructions in [19]. We also show that under certain conditions, the non-cyclic construction from [19] can be permuted to become a cyclic code, whereas in other cases it cannot, thus proving our construction produces cyclic MR codes with new parameters. As a byproduct of the proof, we characterize the algebraic structure of repair sets for optimal cyclic LRCs, which results in strong new restrictions on the parameters of optimal cyclic LRCs. Finally, we return to review our bound on optimal LRCs, and show that our construction has an optimal field size when $r = 2$. Since the bound is for general LRCs, as a consequence we get that some known constructions have optimal field size when $r = 2$, a result which has not been claimed before.

The remainder of this paper is organized as follows. Section II introduces some preliminaries about LRCs. Section III proves a new bound on the field size of LRCs. Section IV describes a construction of cyclic MR codes, as well as sufficient and necessary conditions under which a known non-cyclic construction from [19] may be permuted to become cyclic. Section V concludes this paper with some remarks.

II. PRELIMINARIES

In this section, we present notation and some necessary known results, which are used throughout the paper. For a positive integer $n \in \mathbb{N}$, we define $[n] = \{0, 1, \ldots, n-1\}$. If $m|n$ is a positive integer, we denote

$$\langle m \rangle \triangleq m\mathbb{Z} \cap [n] = \{0, m, 2m, \ldots, n-m\}.$$

Thus, $\langle m \rangle$ implicitly depends on n, whose value should be understood from the context.

For any prime power q, let $\mathbb{F}_q$ denote the finite field of size q, let $\mathbb{F}_q^m$ denote the set of vectors of length m over $\mathbb{F}_q$, and let $\mathbb{F}_q^{m \times n}$ denote the set of all possible $m \times n$ matrices over $\mathbb{F}_q$.

An $[n, k]_q$ linear code, $\mathcal{C}$, over $\mathbb{F}_q$, is a k-dimensional subspace of $\mathbb{F}_q^n$. Such a code may be specified as the row-space of a $k \times n$ generator matrix $G = (g_0, g_1, \ldots, g_{n-1})$, where g_i is a column vector of length k for all $i \in [n]$. Specifically, it is called an $[n, k, d]_q$ linear code if the minimum Hamming

distance of the code is d. For a subset $S \subseteq [n]$, we define

$$\operatorname{span}(S) \triangleq \operatorname{span}\{g_i \; : \; i \in S\},$$
$$\operatorname{rank}(S) \triangleq \operatorname{rank}(\operatorname{span}(S)).$$

The code $\mathcal{C}$ can also be specified by a parity-check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$, i.e., $\mathcal{C} = \{c \in \mathbb{F}_q^n \; : \; Hc^\intercal = 0\}$, where $\operatorname{rank}(H) = n - k$. Given a non-empty set of coordinates, $S \subseteq [n]$, the punctured code $\mathcal{C}|_S$ is the code obtained from $\mathcal{C}$ by deleting the code symbols at positions $[n] \setminus S$. Thus, $\mathcal{C}|_S$ is generated by $G|_S$ which is obtained from G by deleting the columns at $[n] \setminus S$. Similarly, the shortened code $\mathcal{C}|^S$ is the code whose parity matrix is $H|_S$, namely, the matrix obtained from H by deleting the columns at $[n] \setminus S$.

An $[n, k]_q$ linear code, $\mathcal{C}$, is said to be a cyclic code if $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ implies that $\sigma(c) \triangleq (c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in \mathcal{C}$, where σ is the cyclic shift operator by one place. It is well known (see [27]) that a cyclic code with length n over $\mathbb{F}_q$ corresponds to a principal ideal of $\mathbb{F}_q[x]/(x^n - 1)$. Thus, let $\mathcal{C}$ be generated by a monic polynomial $g(x)|(x^n - 1)$, which is called the generator polynomial of $\mathcal{C}$. When $n|(q^m - 1)$, assume α is a primitive nth root of unity of $\mathbb{F}_{q^m}$, then the cyclic code $\mathcal{C}$ can be also be determined by the roots of $g(x)$, i.e., $R_{\mathcal{C}} = \{\alpha^i \; : \; g(\alpha^i) = 0\}$.

We shall encounter many Vandermonde matrices in the following section. Since we use a broader-than-usual definition for such matrices, we give it here explicitly. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be n distinct elements. We say the following $m \times n$ matrix is a Vandermonde matrix,

$$\Pi \cdot D \cdot \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_0 & \alpha_1 & \ldots & \alpha_{n-1} \\ \vdots & \vdots & & \vdots \\ \alpha_0^{m-1} & \alpha_1^{m-1} & \ldots & \alpha_{n-1}^{m-1} \end{pmatrix} D',$$

where Π is a permutation matrix, and where D and D' are invertible diagonal matrices. It is well known that the rank of such a matrix is $\min\{m, n\}$.

A. Locally Repairable Codes

In [17], Gopalan et al. introduced a definition for the locality of code symbols. For $j \in [n]$, the jth code symbol, c_j, of an $[n, k, d]_q$ linear code, $\mathcal{C}$, is said to have locality r if it can be recovered by accessing at most r other symbols of $\mathcal{C}$. This has been generalized in [31] to the following definition:

Definition 1: Let $\mathcal{C}$ be an $[n, k, d]_q$ linear code, and let G be a generator matrix for it. For $j \in [n]$, the jth code symbol, c_j, of $\mathcal{C}$, is said to have (r, δ)-locality if there exists a subset $S_j \subseteq [n]$ such that:

- $j \in S_j$ and $|S_j| \leqslant r + \delta - 1$; and
- the minimum Hamming distance of the punctured code $\mathcal{C}|_{S_j}$ is at least δ.

In that case, the set S_j is also called a repair set of c_j. The code $\mathcal{C}$ is said to have information (r, δ)-locality if there exists $S \subseteq [n]$ with $\operatorname{rank}(S) = k$ such that for each $j \in S$, c_j has (r, δ)-locality. Furthermore, the code $\mathcal{C}$ is said to have all-symbol (r, δ)-locality if all the code symbols have (r, δ)-locality.

Thus, the definition of symbol locality from [17] is the special case of $\delta = 2$ in the definition from [31]. In [31] (and for the case $\delta = 2$, originally [17]), the following upper bound on the minimum Hamming distance of linear codes with information (r, δ)-locality is derived.

Theorem 1 [31]: For an $[n, k, d]_q$ linear code with information (r, δ)-locality,

$$d \leqslant n - k + 1 - \left(\left\lceil \frac{k}{r} \right\rceil - 1 \right)(\delta - 1).$$

Codes with information (r, δ)-locality are said to be *optimal locally repairable codes (optimal LRCs)* if their minimum Hamming distance attains the bound of Theorem 1 with equality. We note that all-symbol (r, δ)-locality is a special case of information (r, δ)-locality. Thus, the bound of Theorem 1 also applies to codes with all-symbol (r, δ)-locality. While Theorem 1 may be further improved for all-symbol (r, δ)-locality, it is already tight when $(r + \delta - 1)|n$, which is the case we shall be interested in throughout the paper. From now on, we shall also use the term *optimal LRCs* to refer to all-symbol (r, δ)-LRCs, with $(r + \delta - 1)|n$, that attain the bound of Theorem 1 with equality. For the current state of improvements on Theorem 1 when $(r + \delta - 1) \nmid n$, the reader is referred to the recent [7] and the references therein.

Theorem 2 ([9], [37]): Let $\mathcal{C}$ be an optimal $[n, k, d]_q$ LRC with all-symbol (r, δ)-locality. Let $\Gamma \subseteq 2^{[n]}$ be the set of all possible repair sets. Write $k = ru + v$, for integers u and v, and $0 \leqslant v \leqslant r - 1$. If $(r + \delta - 1)|n$, $k > r$, and additionally, $u \geqslant 2(r - v + 1)$ or $v = 0$, then there exists a subset $\mathcal{S} \subseteq \Gamma$, such that:

- All $S \in \mathcal{S}$ are of cardinality $|S| = r + \delta - 1$, and $\mathcal{S}$ is a partition of $[n]$.
- For any $S \in \mathcal{S}$, $\mathcal{C}|_S$ is an $[r + \delta - 1, r, \delta]_q$ MDS code.

Remark: The partitioning of $[n]$ by repair sets was first proved in [37] only for the case $r|k$, i.e., $v = 0$. Recently, this property was proved in [9] also for the case $u \geqslant 2(r - v + 1)$.

In [21], Guruswami et al. asked a fundamental interesting question: How long can an optimal LRC with $(r, \delta = 2)$-locality be? They derived the following upper bound on the code length.

Theorem 3 [21]: Let $\mathcal{C}$ be an optimal $[n, k, d]_q$ LRC with all-symbol $(r, 2)$-locality. If $d \geqslant 5$, $k > r$, $(r + 1)|n$, and additionally, $r|k$ or $k \geqslant 2r^2 + 2r - (2r - 1)(k \bmod r)$, then

$$n = \begin{cases} O\left(dq^{\frac{4(d-2)}{d-a} - 1}\right), & \text{if } a = 1, 2, \\ O\left(dq^{\frac{4(d-3)}{d-a} - 1}\right), & \text{if } a = 3, 4, \end{cases} \quad (1)$$

where $a \in \{1, 2, 3, 4\}$, and $a \equiv d \pmod 4$.

In [9], this problem is further considered for optimal LRCs with all-symbol (r, δ)-locality, $\delta \geqslant 2$.

Theorem 4 [9]: Let $n = w(r + \delta - 1)$, $\delta > 2$, $k = ur + v$, $0 \leqslant v \leqslant r - 1$, and additionally, $u \geqslant 2(r - v + 1)$ or $v = 0$, where all parameters are integers. Assume that there exists an optimal $[n, k, d]_q$ linear code $\mathcal{C}$ with all-symbol (r, δ)-locality, and define $t = \lfloor (d - 1)/\delta \rfloor$. If $t \geqslant 2$, then

$$n \leqslant \begin{cases} \frac{(t-1)(r+\delta-1)}{2r(q-1)} q^{\frac{2(w-u)r-2v}{t-1}} & \text{if } t \text{ is odd} \\ \frac{t(r+\delta-1)}{2r(q-1)} q^{\frac{2(w-u)r-2v}{t}} & \text{if } t \text{ is even} \end{cases}$$

$$= O\left(\frac{t(r + \delta)}{r} q^{\frac{(w-u)r-v}{\lfloor t/2 \rfloor} - 1}\right),$$

where $w - u$ can also be rewritten as $w - u = \lfloor (d - 1 + v)/ (r + \delta - 1) \rfloor$.

B. Maximally Recoverable Codes

Maximally recoverable (MR) codes are an extremal case of LRCs, that maximize the erasure-repair capability.

Definition 2: Let $\mathcal{C}$ be an $[n, k, d]_q$ code with all-symbol (r, δ)-locality, and define $\mathcal{S} \triangleq \{S_i : i \in [n]\}$, where S_i is a repair set for coordinate i. The code $\mathcal{C}$ is said to be a *maximally recoverable (MR) code* if $\mathcal{S}$ is a partition of $[n]$, and for any $R_i \subseteq S_i$ such that $|S_i \setminus R_i| = \delta - 1$, the punctured code $\mathcal{C}|_{\cup_{i \in [n]} R_i}$ is an MDS code.

In general, S_i for $i \in [n]$, are not required to be of the same size. However, from an application point of view, equal-sized repair sets simplify the implementation, bringing us to the following definition:

Definition 3: Let $\mathcal{C}$ be an $[n, k, d]_q$ MR code, as in Definition 2. If each $S_i \in \mathcal{S}$ is of size $|S_i| = r + \delta - 1$ (implying $r + \delta - 1|n$), we define

$$m \triangleq \frac{n}{r + \delta - 1}, \qquad h \triangleq mr - k.$$

Then $\mathcal{C}$ is said to be an (n, r, h, δ, q)-MR code.

We first note that it is easy to verify that (n, r, h, δ, q)-MR codes are optimal $[n, k, d]_q$ LRCs with all-symbol (r, δ)-locality. We can regard each codeword of an (n, r, h, δ, q)-MR code, as an $m \times (r + \delta - 1)$ array, by placing each repair set in $\mathcal{S}$ as a row, when $\mathcal{S}$ forms a partition of $[n]$. In this way, (n, r, h, δ, q)-MR codes match the definition of partial MDS (PMDS) codes, as defined in [3]. When implemented in a distributed-storage setting, each entry of a codeword array corresponds to a sector, each column of the array corresponds to a disk, and each row to a stripe. Thus, an (n, r, h, δ, q)-MR code can recover from $\delta - 1$ sector erasures in each stripe, and additional h erased sectors anywhere. We mention in passing that a more restricted type of codes, called sector-disk (SD) codes, are capable of recovering from $\delta - 1$ disk erasures, and additional h erased sectors (see [11], [30]).

Paralleling the general case of optimal LRCs, it is interesting to ask what is the minimum alphabet size required by MR codes.

Lemma 1 ([19, Theorem I.1]): Let $\mathcal{C}$ be an (n, r, h, δ, q)-MR code, $h \geqslant 2$. If $m \triangleq \frac{n}{r+\delta-1} \geqslant 2$, then

$$q = \Omega(nr^\varepsilon),$$

where $\varepsilon = \min\{\delta - 1, h - 2\lceil \frac{h}{m} \rceil\}/\lceil \frac{h}{m} \rceil$, and where h and δ are regarded as constants. Additionally,

1) If $m \geqslant h$:

$$q = \Omega\left(nr^{\min\{\delta-1, h-2\}}\right).$$

2) If $m \leqslant h$, $m|h$, and $\delta - 1 \leqslant h - \frac{2h}{m}$:

$$q = \Omega\left(n^{1 + \frac{m(\delta-1)}{h}}\right).$$

3) If $m \leqslant h$, $m|h$, and $\delta - 1 > h - \frac{2h}{m}$:

$$q = \Omega\left(n^{m-1}\right).$$

Remark: For the case $h = 1$, the field size requirement of an (n, r, h, δ, q)-MR code may be as small as $q = \Theta(r + \delta - 1)$. This is attainable since the punctured code over any repair set together with the single global parity check is an $[r + \delta, r, \delta + 1]_q$ MDS code when $(r + \delta - 1)|k$ or $u \geqslant 2(r - v + 1)$, where $k = ur + v$ with $0 \leqslant v \leqslant r - 1$ (see [9]).

Definition 4: A family of (n, r, h, δ, q)-MR codes has *order-optimal field size* if it attains one of the bounds of Lemma 1 asymptotically for $h \geqslant 2$, or if it has $q = \Theta(r + \delta - 1)$ for $h = 1$.

III. A NEW BOUND ON OPTIMAL LRCs

In this section we present a new bound on the parameters of optimal LRCs with all-symbol (r, δ)-locality. To that end, we first prove bounds for optimal LRCs with small minimum Hamming distance, distinguishing between the two cases of $2 \mid r$ and $2 \nmid r$. The proof strategy of both bounds is showing that the existence of such codes forces the existence of many subspaces, any two of which intersect only trivially. We then recall a parameter-reduction lemma, which reduces optimal LRCs with a large minimum Hamming distance into optimal LRCs with a smaller one. Combining these together results in the main bound. We note that the new bound is not specific to MR codes or to cyclic codes, but instead applies to optimal LRCs. The bound does, however, require certain divisibility conditions, which are common to several constructions of optimal LRCs, among them, MR codes.

Lemma 2: Let $\mathcal{C}$ be an optimal $[n = (u + 1)(r + \delta - 1), ur, r + 2\delta - 1]_q$ LRC with all-symbol (r, δ)-locality. If $2|r$, then

$$u + 1 \leqslant (q^{r/2} + 1) \Big/ \left\lfloor \frac{2r + 2\delta - 2}{r} \right\rfloor.$$

Proof: Denote $t \triangleq \lceil (2r + 2\delta - 2)/r \rceil$ and $t' \triangleq \lfloor (2r + 2\delta - 2)/r \rfloor$. By Theorem 2, the code $\mathcal{C}$ has a parity-check matrix of the following form,

$P =$

$$\begin{pmatrix} V_{0,0} & V_{0,1} & \cdots & V_{0,t-1} & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & V_{1,0} & V_{1,1} & \cdots & V_{1,t-1} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & V_{u,0} & V_{u,1} & \cdots & V_{u,t-1} \\ W_{0,0} & W_{0,1} & \cdots & W_{0,t-1} & W_{1,0} & W_{1,1} & \cdots & W_{1,t-1} & \cdots & W_{u,0} & W_{u,1} & \cdots & W_{u,t-1} \end{pmatrix},$$

where $V_{i,j} \in \mathbb{F}_q^{(\delta-1)\times(r/2)}$, $W_{i,j} \in \mathbb{F}_q^{r\times(r/2)}$ for $i \in [u+1]$ and $j \in [t-1]$, and $(V_{i,0}\ V_{i,1}, \cdots, V_{i,t-1})$ is parity-check matrix of an $[r+\delta-1, r, \delta]_q$ MDS code for $i \in [u+1]$. This implies that the matrices $V_{i,t-1}$ and $W_{i,t-1}$, $i \in [u+1]$, have $\frac{r}{2}$ columns each when $r|(2r+2\delta-2)$, and $(2r+2\delta-2) \bmod \frac{r}{2}$ otherwise.

Let us consider the following square $(r+2\delta-2)\times(r+2\delta-2)$ matrices,

$E_{a,b,i,j} \triangleq$

$$\begin{pmatrix} V_{a,0} & \cdots & V_{a,i-1} & V_{a,i+1} & \cdots & V_{a,t-1} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & V_{b,0} & \cdots & V_{b,j-1} & V_{b,j+1} & \cdots & V_{b,t-1} \\ W_{a,0} & \cdots & W_{a,i-1} & W_{a,i+1} & \cdots & W_{a,t-1} & W_{b,0} & \cdots & W_{b,j-1} & W_{b,j+1} & \cdots & W_{b,t-1} \end{pmatrix},$$

where $a, b \in [u+1]$, $a \neq b$, and $i, j \in [t']$. Since the minimum Hamming distance of $\mathcal{C}$ is $r + 2\delta - 1$, any $r + 2(\delta - 1)$ columns

from P are linearly independent. This implies that the matrices $E_{a,b,i,j}$ defined above have full rank.

Recall that $(V_{a,0}, V_{a,1}, \cdots, V_{a,t-1})$ is a parity-check matrix of an $[r + \delta - 1, r, \delta]_q$ MDS code. Thus, $(V_{a,1}, \cdots, V_{a,i-1}, V_{a,i+1}, \cdots, V_{a,t-1})$ is an invertible $(\delta - 1) \times (\delta - 1)$ matrix. A similar claim follows for $(V_{b,1}, \cdots, V_{b,j-1}, V_{b,j+1}, \cdots, V_{b,t-1})$. Hence, after simple column and row operations, the full rank of $E_{a,b,i,j}$ implies that

$$\begin{pmatrix} 0 & V_{a,1} \cdots V_{a,i-1} V_{a,i+1} \cdots V_{a,t-1} & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & V_{b,1} \cdots V_{b,j-1} V_{b,j+1} \cdots V_{b,t-1} \\ W_{a,i}^* & 0 & \cdots & 0 & 0 & \cdots & 0 & W_{b,j}^* & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

has full rank, implying also that

$$\operatorname{rank}(W_{a,i}^*, W_{b,j}^*) = r, \tag{2}$$

for $a, b \in [u+1]$, $a \neq b$, and $i, j \in [t']$. We also mention that if either $i = 0$ or $j = 0$, natural adjustments need to be made, that is, zeroing $V_{a,1}$ instead of $V_{a,0}$, and $V_{b,1}$ instead of $V_{b,0}$.

Next, assume $a \in [u+1]$, and $i, j \in [t']$, $i \neq j$. We pick only $r + \delta - 1$ columns from P, which must therefore be linearly independent, giving us,

$r + \delta - 1$

$$= \operatorname{rank} \begin{pmatrix} V_{a,0} & V_{a,1} & \cdots & V_{a,t-1} \\ W_{a,0} & W_{a,1} & \cdots & W_{a,t-1} \end{pmatrix}$$

$$= \operatorname{rank} \begin{pmatrix} V_{a,0} & V_{a,0} & V_{a,1} & \cdots & V_{a,t-1} \\ W_{a,0} & W_{a,0} & W_{a,1} & \cdots & W_{a,t-1} \end{pmatrix}$$

$$= \operatorname{rank} \begin{pmatrix} V_{a,0} & 0 & V_{a,1} & \cdots & V_{a,t-1} \\ W_{a,0} & W_{a,j}^* & W_{a,1} & \cdots & W_{a,t-1} \end{pmatrix}$$

$$= \operatorname{rank} \begin{pmatrix} V_{a,0} & 0 & V_{a,1} & \cdots & V_{a,i-1} & V_{a,i+1} & \cdots & V_{a,t-1} \\ W_{a,0} & W_{a,j}^* & W_{a,1} & \cdots & W_{a,i-1} & W_{a,i+1} & \cdots & W_{a,t-1} \end{pmatrix}$$

$$= \operatorname{rank} \begin{pmatrix} 0 & 0 & V_{a,1} & \cdots & V_{a,i-1} & V_{a,i+1} & \cdots & V_{a,t-1} \\ W_{a,i}^* & W_{a,j}^* & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{3}$$

We explain why the fourth equality holds in more detail. The column operations performed in order to obtain $W_{a,j}^*$ may be written as

$$\begin{pmatrix} 0 \\ W_{a,j}^* \end{pmatrix} = \sum_{\tau \in [t] \setminus \{j\}} \begin{pmatrix} V_{a,\tau} \\ W_{a,\tau} \end{pmatrix} E_\tau,$$

where $E_0 = I$ is the identity matrix. It then follows that

$$(V_{a,0}, \ldots, V_{a,j-1}, V_{a,j+1}, \ldots, V_{a,t-1}) \cdot \begin{pmatrix} E_0 \\ \vdots \\ E_{j-1} \\ E_{j+1} \\ \vdots \\ E_{t-1} \end{pmatrix} = 0.$$

Since $(V_{a,0}, \ldots, V_{a,j-1}, V_{a,j+1}, \ldots, V_{a,t-1})$ is a parity-check matrix for an $[\frac{r}{2} + \delta - 1, \frac{r}{2}, \delta]_q$ MDS code, we have that the matrix $(E_0^\mathsf{T}, \ldots, E_{j-1}^\mathsf{T}, E_j^\mathsf{T}, \ldots, E_{t-1}^\mathsf{T})$ is a generator matrix for that code. Hence, any $\frac{r}{2}$ columns of it are linearly independent. In particular, that means E_i is invertible. We can therefore write,

$$\begin{pmatrix} V_{a,i} \\ W_{a,i} \end{pmatrix} = - \sum_{\tau \in [t] \setminus \{i,j\}} \begin{pmatrix} V_{a,\tau} \\ W_{a,\tau} \end{pmatrix} E_\tau E_i^{-1} + \begin{pmatrix} 0 \\ W_{a,j}^* \end{pmatrix} E_i^{-1}.$$

This completes the detailed explanation for the fourth equality in (3). The main observation is that (3) gives

$$\text{rank}(W_{a,i}^*, W_{a,j}^*) = r, \tag{4}$$

for $a \in [u+1]$, and $i, j \in [t']$, $i \neq j$. Again, if $i = 0$ or $j = 0$, a natural adjustment needs to be made.

Let us define the following set of subspaces

$$\mathcal{W} \triangleq \left\{ \text{colspan}(W_{a,i}^*) \ : \ a \in [u+1], i \in [t'] \right\},$$

where $\text{colspan}(\cdot)$ of a matrix denotes its column space. By (2) and (4) we learn that $\mathcal{W}$ contains only $\frac{r}{2}$-dimensional spaces, which are all distinct, hence

$$|\mathcal{W}| = (u+1)t' = (u+1) \left\lfloor \frac{2r + 2\delta - 2}{r} \right\rfloor.$$

Additionally, any two subspaces from $\mathcal{W}$ intersect only trivially, hence

$$(u+1) \left\lfloor \frac{2r + 2\delta - 2}{r} \right\rfloor = |\mathcal{W}| \leqslant \frac{q^r - 1}{q^{r/2} - 1} = q^{r/2} + 1.$$

Rearranging this gives the desired claim. ■

For the case $2 \nmid r$, we also have a similar lemma.

Lemma 3: Let $\mathcal{C}$ be an optimal $[n = (u+2)(r+\delta-1), ur, 2r+3\delta-2]_q$ LRC with all-symbol (r, δ)-locality. If $2 \nmid r$, then

$$u \leqslant q^{(r+1)/2}.$$

Proof: By Theorem 2, and after simple row operations, the code $\mathcal{C}$ has a parity-check matrix of the following form,

$$P =$$
$$\begin{pmatrix} I_{\delta-1} & V_{0,0} & V_{0,1} & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{\delta-1} & V_{1,0} & V_{1,1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & I_{\delta-1} & V_{u+1,0} & V_{u+1,1} \\ 0 & W_{0,0} & W_{0,1} & 0 & W_{1,0} & W_{1,1} & \cdots & 0 & W_{u+1,0} & W_{u+1,1} \end{pmatrix},$$

where $I_{\delta-1}$ is the $(\delta - 1) \times (\delta - 1)$ identity matrix, $V_{i,1} \in \mathbb{F}_q^{(\delta-1) \times ((r-1)/2)}$, $V_{i,2} \in \mathbb{F}_q^{(\delta-1) \times ((r+1)/2)}$, $W_{i,1} \in \mathbb{F}_q^{2r \times ((r-1)/2)}$, $W_{i,2} \in \mathbb{F}_q^{2r \times ((r+1)/2)}$, and $(I_{\delta-1}, V_{i,1}, V_{i,2})$ is a parity-check matrix of an $[r + \delta - 1, r, \delta]_q$ MDS code, for all $i \in [u+2]$.

Consider the following square $(2r+3\delta-3) \times (2r+3\delta-3)$ matrices,

$$E_{a,b} \triangleq \begin{pmatrix} I_{\delta-1} & V_{0,0} & V_{0,1}' & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{\delta-1} & V_{a,1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I_{\delta-1} & V_{b,1} \\ 0 & W_{0,0} & W_{0,1}' & 0 & W_{a,1} & 0 & W_{b,1} \end{pmatrix},$$

where $a, b \in [u+2] \setminus \{0\}$, $a \neq b$, and where $V_{0,1}'$ and $W_{0,1}'$ are the first $\frac{r-1}{2}$ columns of $V_{0,1}$ and $W_{0,1}$, respectively. Since the minimum Hamming distance of $\mathcal{C}$ is $2r + 3\delta - 2$, any $2r + 3\delta - 3$ columns from P are linearly independent, and in particular,

$$\text{rank}(E_{a,b}) = 2r + 3\delta - 3.$$

This implies that

$$\text{rank}(W_{0,0}, W_{0,1}', W_{a,1}, W_{b,1}) = 2r.$$

By the size of the matrices, we also must have

$$\text{rank}(W_{a,1}, W_{b,1}) = r + 1,$$

and also

$$\text{rank}(W_{a,1}) = \text{rank}(W_{b,1}) = \frac{r+1}{2}.$$

We now denote $U' = \text{colspan}(W_{0,0}, W_{0,1}') \subseteq \mathbb{F}_q^{2r}$. Obviously, $\dim(U') = r - 1$. Let us arbitrarily choose an $(r+1)$-dimensional subspace $\widetilde{U} \subseteq \mathbb{F}_q^{2r}$ such that $\mathbb{F}_q^{2r} = U' + \widetilde{U}$, namely, $\dim(\widetilde{U}) = r + 1$ and $U' \cap \widetilde{U} = \{0\}$. For any vector $x \in \mathbb{F}_q^{2r}$, let $\widetilde{x} \in \mathbb{F}_q^{2r}$ denotes its projection onto $\widetilde{U}$, that is, $\widetilde{x} \in \widetilde{U}$ is the unique vector such that $x = x' + \widetilde{x}$, with $x' \in U'$. For any $a \in [u+2] \setminus \{0\}$, we then construct $\widetilde{W}_{a,1}$ from $W_{a,1}$ by replacing each column vector with its projection onto $\widetilde{U}$. It then follows, that for all $a, b \in [u+2] \setminus \{0\}$, $a \neq b$,

$$\text{rank}(W_{0,0}, W_{0,1}', \widetilde{W}_{a,1}, \widetilde{W}_{b,1}) = 2r,$$

and also

$$\text{rank}(\widetilde{W}_{a,1}) = \text{rank}(\widetilde{W}_{b,1}) = \frac{r+1}{2}.$$

Let us construct the set of subspaces

$$\mathcal{W} \triangleq \left\{ \text{colspan}(\widetilde{W}_{a,1}) \ : \ a \in [u+2] \setminus \{0\} \right\}.$$

By the previous discussion, $\mathcal{W}$ contains $u + 1$ subspaces of $\widetilde{U}$, each of dimension $\frac{r+1}{2}$, any two of which intersect only trivially. Additionally, the sum of any two subspaces from $\mathcal{W}$, summed together with the fixed $(r-1)$-dimensional subspace $\text{colspan}(W_{0,0}) + \text{colspan}(W_{0,1}')$, gives $\mathbb{F}_q^{2r}$. Thus,

$$u + 1 = |\mathcal{W}| \leqslant \frac{q^{r+1} - 1}{q^{(r+1)/2} - 1} = q^{(r+1)/2} + 1,$$

completing the proof. ■

The final component in our main bounding theorem is a parameter-reduction lemma. This lemma was proved in [9].

Lemma 4 ([9] Corollary 2): Let $n = m(r + \delta - 1)$, $\delta \geqslant 2$, $k = ur + v > r$, and additionally, $r | k$ or $u \geqslant 2(r+1-v)$, where all parameters are integers. If there exists an optimal $[n, k, d]_q$ linear code $\mathcal{C}$ with $d > r + \delta$ and all-symbol (r, δ)-locality, then there exists an optimal linear code $\mathcal{C}'$ with all-symbol (r, δ)-locality and parameters $[n - \epsilon(r + \delta - 1), k, d' = d - \epsilon(r + \delta - 1)]_q$, where $\epsilon \leqslant \lceil (d-1)/(r + \delta - 1) \rceil - 1$.

Let us now state and prove our main bound. The next theorem gives a lower bound on the size of the field required for LRCs with all-symbol (r, δ)-locality.

Theorem 5: Let $\mathcal{C}$ be an optimal $[n, k, d]_q$ linear code with all-symbol (r, δ)-locality. Assume $n = m(r + \delta - 1)$, $k = ur$, $u \geqslant 2$. If $2 | r$ and $m \geqslant u + 1$ then,

$$q \geqslant \psi \left(\left(\left(\frac{k}{r} + 1 \right) \left\lfloor \frac{2r + 2\delta - 2}{r} \right\rfloor - 1 \right)^{\frac{2}{r}} \right),$$

where $\psi(x)$ is the smallest prime power greater or equal to x. If $2 \nmid r$ and $m \geqslant u + 2$ then

$$q \geqslant \psi \left(\left(\frac{k}{r} \right)^{\frac{2}{r+1}} \right).$$

Proof: The proof is straightforward. Apply Lemma 4 until reaching the required conditions of either Lemma 2 or Lemma 3, and then use them. ∎

Remark: Assume that there exists an optimal $[n, k, d]_q$ LRC with all-symbol (r, δ)-locality, and define $t = \lfloor (d-1)/\delta \rfloor \geqslant 2$. Rewriting the bound of Theorem 4 (which we cite from [9]) in a slightly looser yet more convenient way,

$$q = \Omega\left(\left(\frac{nr}{t(r+\delta)}\right)^{\frac{\lfloor (d-1)/\delta \rfloor}{2\lfloor \frac{d-1+v}{r+\delta-1} \rfloor r - 2v}} \right).$$

Thus, when only k and n tend to infinity, and the other parameters are constant, if

$$\frac{\lfloor (d-1)/\delta \rfloor}{2 \lfloor \frac{d-1+v}{r+\delta-1} \rfloor r - 2v} < \frac{2}{r+1},$$

then the exponent in the bound of Theorem 5 is higher, and it may outperform the known bound of Theorem 4 (where we denote $k = ur + v$ and $0 \leqslant v \leqslant r - 1$). For example, assume the following are positive integers, $\delta = 3(r-1)$, $d = 3\tau(r+\delta-1) + \delta$, $t = \lfloor \frac{d-1}{\delta} \rfloor = 4\tau$, as well as τ being a positive integer. Further assume that $k = ur$. In this case, the known bound of Theorem 4 gives us $q = \Omega(n^{\frac{2}{3r}})$. However, the new bound of Theorem 5 gives us $q = \Omega(n^{\frac{2}{r+1}})$ if $2|r$, and $q = \Omega(n^{\frac{2}{r}})$, otherwise. LRCs with such parameters can be constructed by the construction in [38].

Having seen that the new bound of Theorem 5 may provide an improvement, we focus on a single case. More specifically, the case of $r = 2$ is of particular interest, since we can then use Theorem 5 to prove that some known LRCs have optimal field size.

We first consider some Tamo-Barg codes [38].

Lemma 5 [38]: Let q be a prime power, $q = r + \delta - 1$, then there exists an optimal LRC with all-symbol (r, δ)-locality and parameters $[q^b, ur, (q^{b-1} - u)q + \delta]_{q^b}$, where $b \geqslant 2$ and $0 < u < q^{b-1}$.

Corollary 1: Let $\mathcal{C}$ be a code from Lemma 5 with $r = 2$ and $u = q^{b-1} - 1$. If $q^b - 1$ is not a prime power then $\mathcal{C}$ has optimal field size.

Example 1: Let $n = 2^4$, $r = 2$, $\delta = 3$, then by Lemma 5 there exists an optimal LRC with all-symbol $(2, 3)$-locality and parameters $[16, 6, 7]_{2^4}$, which has optimal field size since 15 is not a prime power.

We now examine a construction of cyclic optimal LRCs from [39].

Lemma 6 [39]: Let $r = 2$, $n = m(r + \delta - 1) = q^b - 1$, and $k = ur + v$ with $0 \leqslant v < r$, where q^b is prime power. Then there exists a cyclic optimal LRC with all-symbol $(2, \delta)$-locality and parameters $[q^b - 1, k, d]_{q^b}$.

Corollary 2: Let $\mathcal{C}$ be a code from Lemma 6 with $m = u+1$ and $v = 0$. If neither $q^b - 2$, nor $q^b - 1$, are prime powers, then $\mathcal{C}$ has optimal field size.

Example 2: Let $n = 2^6 - 1$, $r = 2$, and $\delta = 2$. Then by Lemma 6, there exists a cyclic optimal LRC with all-symbol $(2, 2)$-locality, and parameters $[63, 40, 5]_{2^6}$, which has optimal field size since both 62 and 63 are not prime powers.

Yet another construction of cyclic optimal LRCs comes from [13].

Lemma 7 [13]: Let $r = 2$, $\delta = 2$, $n = m(r + \delta - 1) = 3m = q^b + 1$, and $k = 2u$, with u an even integer, and where q^b is prime power. Then there exists a cyclic optimal LRC with all-symbol $(2, 2)$-locality and parameters $[q^b + 1 = 3m, 2u, d]_{q^m}$.

Corollary 3: Let $\mathcal{C}$ be a code from Lemma 7 with $m = u + 1$. Then $\mathcal{C}$ has optimal field size.

Example 3 [13]: Let $n = 9 = 2^3 + 1$, $r = 2$, $\delta = 2$, $k = 4$, then there exists a cyclic optimal $[9, 4, 5]_8$-LRC, which has optimal field size.

Note that an $(n, r = 2, h = 2, \delta, q)$-MR code is also an $[n = (u+1)(\delta+1), 2u, 2\delta + 1]_q$ optimal LRC. The following corollary can be derived directly from Lemma 2.

Corollary 4: Let $\mathcal{C}$ be an $(n, r = 2, h = 2, \delta, q)$-MR code. Then $q \geqslant n - 1$.

IV. CYCLIC MAXIMALLY RECOVERABLE (MR) CODES

We divide this section into two parts. In the first part we construct cyclic MR codes, and show that for certain parameters they have the exact optimal field size. The main idea behind our construction is to carefully choose the roots for the cyclic code we construct, in a way that produces an MR code. In the second part we study a known class of MR codes which are non-cyclic, but have the same parameters as the cyclic codes we construct. We then show that these non-cyclic codes can sometimes be permuted to obtain cyclic MR codes. For this part, as tools to prove the main results, we characterize the algebraic structure of the repair sets of *cyclic* optimal LRCs (Theorem 7) and the structure of punctured codes and shortened codes over repair sets (Corollary 7). On the one hand, we prove that for some parameters the known construction can be permuted to obtain cyclic MR codes by finding suitable permutations (Theorem 8). On the other hand, we show that such a permutation is not always possible (Theorem 9). By combining the two parts, we obtain our main result.

A. A New Construction

We immediately present our construction for cyclic MR codes. It is inspired by the construction of [39].

Construction 1: Let $b, r, \delta \geqslant 2$ be integers, q a prime power, $n = q^b - 1$, $\alpha \in \mathbb{F}_{q^b}$ a primitive element, $a = (r+\delta-1)|(q-1)$, and $m = n/a$ such that $\gcd(\delta, m) = 1$. Define

$$R \triangleq \left\{ \alpha^{ja+t} \ : \ 1 \leqslant j \leqslant m, 1 \leqslant t \leqslant \delta - 1 \right\} \cup \left\{1, \alpha^\delta \right\}.$$

The constructed code, $\mathcal{C}$, is the cyclic code of length n over $\mathbb{F}_{q^b}$ with root set R.

Our goal is now to show that the code from Construction 1 is indeed a cyclic MR code. However, in order to do so we require a technical lemma.

Lemma 8: Assume the setting and notation of Construction 1. Denote $\beta = \alpha^m$, and $\gamma = \alpha^\delta$. Assume $T_i = \{t_{i,1}, \ldots, t_{i,\delta}\} \subseteq [a]$ for $i = 1, 2$. Then for any $i_1, i_2 \in [m]$, $i_1 \neq i_2$, the matrix, shown in the equation at the bottom of the next page, has full rank.

Proof: Assume to the contrary that there exists $0 \neq E = (e_{1,1}, e_{1,2}, \cdots, e_{1,\delta-1}, e_{2,1}, e_{2,2}, \cdots, e_{2,\delta-1}, e_0, e_\delta) \in \mathbb{F}_{q^b}^{2\delta}$ satisfying $EM = 0$. Hence, the polynomials $f_1(x) = e_0 + \gamma^{i_1} e_\delta x^\delta + \sum_{i=1}^{\delta-1} e_{1,i} x^i$ and $f_2(x) = e_0 + e_\delta \gamma^{i_2} x^\delta + \sum_{i=1}^{\delta-1} e_{2,i} x^i$ have roots $\{\beta^{t_{1,i}} : 1 \leqslant i \leqslant \delta\}$ and $\{\beta^{t_{2,i}} : 1 \leqslant i \leqslant \delta\}$, respectively. Note that $E \neq 0$ implies that $e_\delta \neq 0$, for otherwise, $\deg(f_1(x)) < \delta$ and $\deg(f_2(x)) < \delta$, but they each have δ distinct roots, a contradiction. By Vieta's formula, we have

$$\frac{\prod_{1 \leqslant i \leqslant \delta} \beta^{t_{1,i}}}{\prod_{1 \leqslant i \leqslant \delta} \beta^{t_{2,i}}} = \gamma^{i_2 - i_1}.$$

Hence, there exists an integer t such that $\beta^t = \gamma^{i_2 - i_1}$, i.e., $\alpha^{mt} = \alpha^{\delta(i_2 - i_1)}$. It follows that

$$mt \equiv \delta(i_2 - i_1) \pmod{ma},$$

and then

$$0 \equiv \delta(i_2 - i_1) \pmod{m}.$$

This contradicts the facts that $i_1 \neq i_2$ and $\gcd(\delta, m) = 1$, and completes the proof. ∎

We can now prove that the constructed code is indeed a cyclic MR code.

Theorem 6: Assume the setting and notation of Construction 1. Then the code $\mathcal{C}$ of Construction 1 is a cyclic $(n = q^b - 1, r, h = 2, \delta, q^b)$-MR code, equivalently, a cyclic MR code with parameters $[n = q^b - 1, k = mr - 2, d]_{q^b}$ with repair sets of size $r + \delta - 1$, and

$$d = \begin{cases} \delta + 2 & r > 2, \\ 2\delta + 1 & r = 2. \end{cases}$$

Proof: Denote $\beta = \alpha^m$, and $\gamma = \alpha^\delta$. In the first step of our proof we contend that the following matrix is a parity-check matrix of $\mathcal{C}$, shown in the equation at the bottom of the next page. Define the following polynomial,

$$f(x) \triangleq \prod_{i=1}^{m-1} (x - \alpha^{ai}) = \sum_{j=0}^{m-1} e_j x^j.$$

Clearly, $f(1) \neq 0$. We then have

$$(e_0, e_1, \cdots, e_{m-1}) \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha^a & \alpha^{2a} & \cdots & \alpha^{a(n-1)} \\ 1 & \alpha^{2a} & \alpha^{4a} & \cdots & \alpha^{2a(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{a(m-1)} & \alpha^{2a(m-1)} & \cdots & \alpha^{a(m-1)(n-1)} \end{pmatrix}$$

$$= (f(1), 0, \ldots, 0, f(\alpha^{am}), 0, \ldots, 0, f(\alpha^{2am}), \ldots, 0, f(\alpha^{(a-1)am}), 0, \ldots, 0)$$

$$= (f(1), 0, \ldots, 0, f(1), 0, \ldots, 0, f(1), 0, \ldots, 0, f(1), 0, \ldots, 0).$$

The preceding equation also means that for all $1 \leqslant i \leqslant \delta - 1$,

$$(e_0, e_1, \cdots, e_{m-1}) \begin{pmatrix} 1 & \alpha^i & \alpha^{2i} & \cdots & \alpha^{i(n-1)} \\ 1 & \alpha^{a+i} & \alpha^{2a+2i} & \cdots & \alpha^{a(n-1)+i(n-1)} \\ 1 & \alpha^{2a+i} & \alpha^{4a+2i} & \cdots & \alpha^{2a(n-1)+i(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{a(m-1)+i} & \alpha^{2a(m-1)+2i} & \cdots & \alpha^{a(m-1)(n-1)+i(n-1)} \end{pmatrix}$$

$$= (f(1), 0, \ldots, 0, \alpha^{mi} f(1), 0, \ldots, 0, \alpha^{2mi} f(1), 0, \ldots, 0, \alpha^{(a-1)mi} f(1), 0, \ldots, 0). \tag{5}$$

Assume G is a generator matrix for $\mathcal{C}$. Recall that the roots of $\mathcal{C}$ are $R = \{\alpha^{ja+t} : 1 \leqslant j \leqslant m, 1 \leqslant t \leqslant \delta - 1\} \cup \{1, \alpha^\delta\}$. Hence, for all $1 \leqslant j \leqslant m$ and $1 \leqslant t \leqslant \delta - 1$,

$$G \cdot \left(1, \alpha^{ja+t}, \alpha^{2(ja+t)}, \ldots, \alpha^{(n-1)(ja+t)}\right)^{\mathsf{T}} = 0.$$

Define, for all $1 \leqslant i \leqslant \delta - 1$,

$$c_i = (1, 0, \cdots, 0, \beta^i, 0, \cdots, 0, \beta^{2i}, \cdots, 0, \beta^{(a-1)i}, 0, \cdots, 0).$$

Note that c_i is a linear combination of the rows of matrix in (5). Thus, the facts $\beta = \alpha^m$, and $f(1) \neq 0$ hint

$$G \cdot c_i^{\mathsf{T}} = 0,$$

and so, $c_i \in \mathcal{C}^\perp$. Combining this with the fact that $\mathcal{C}$ is cyclic (and therefore, also $\mathcal{C}^\perp$), $\sigma^j(c_i) \in \mathcal{C}^\perp$ for all j, where we recall that σ is the cyclic left-shift operator. Thus, the first $m(\delta - 1)$ rows of H contain codewords of $\mathcal{C}^\perp$. The remaining last two rows of H correspond to parity checks for the roots 1 and $\gamma = \alpha^\delta$, both of which are roots of $\mathcal{C}$. If we now denote by $\mathcal{C}'$ the $[n, k', d']_{q^b}$ code whose parity-check matrix is H, we can say $\mathcal{C} \subseteq \mathcal{C}'$. It remains to show that $\mathcal{C} = \mathcal{C}'$ to complete the proof.

We first observe that since H has $m(\delta - 1) + 2$ rows,

$$\dim(\mathcal{C}') = k' \geqslant n - m(\delta - 1) - 2 = mr - 2. \tag{6}$$

$$M = \left(\begin{array}{cccc|cccc} \beta^{t_{1,1}} & \beta^{t_{1,2}} & \cdots & \beta^{t_{1,\delta}} & 0 & 0 & \cdots & 0 \\ \beta^{2t_{1,1}} & \beta^{2t_{1,2}} & \cdots & \beta^{2t_{1,\delta}} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \beta^{(\delta-1)t_{1,1}} & \beta^{(\delta-1)t_{1,2}} & \cdots & \beta^{(\delta-1)t_{1,\delta}} & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & \cdots & 0 & \beta^{t_{2,1}} & \beta^{t_{2,2}} & \cdots & \beta^{t_{2,\delta}} \\ 0 & 0 & \cdots & 0 & \beta^{2t_{2,1}} & \beta^{2t_{2,2}} & \cdots & \beta^{2t_{2,\delta}} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \beta^{(\delta-1)t_{2,1}} & \beta^{(\delta-1)t_{2,2}} & \cdots & \beta^{(\delta-1)t_{2,\delta}} \\ \hline 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ \gamma^{t_{1,1}m+i_1} & \gamma^{t_{1,2}m+i_1} & \cdots & \gamma^{t_{1,\delta}m+i_1} & \gamma^{t_{2,1}m+i_2} & \gamma^{t_{2,1}m+i_2} & \cdots & \gamma^{t_{2,\delta}m+i_2} \end{array} \right)$$

An inspection of H reveals that $\mathcal{C}'$ has all-symbol (r, δ)-locality and the repair sets are given by $G_i \triangleq \langle m \rangle + i$ for $i \in [m]$. Plugging (6) into Theorem 1 we obtain that the minimum distance of $\mathcal{C}'$ satisfies

$$d' \leqslant \begin{cases} \delta + 2 & r > 2, \\ 2\delta + 1 & r = 2. \end{cases} \tag{7}$$

Let us first handle the case of $r > 2$. We contend that in that case, the minimum distance of $\mathcal{C}'$ is at least $d' \geqslant \delta + 2$. Even if we ignore the two bottom rows of H, the $(\delta - 1) \times (r + \delta - 1)$ Vandermonde matrices in the columns corresponding to a repair set show that any $\delta - 1$ columns of H are linearly independent. Thus, a linearly dependent set of columns from H requires at least δ columns from each repair set it intersects. If we try to pick linearly dependent columns from a single repair set, then taking into account also the bottom two rows of H, the columns of a repair set also form a $(\delta + 1) \times (r + \delta - 1)$ Vandermonde matrix (recall that $\gamma^m = \beta^\delta$), and so $\delta + 1$ columns of H from the same repair set are still linearly independent. If instead we pick columns from more than one repair set, at least 2δ columns are required. Combined together, since $\delta \geqslant 2$, the smallest set of linearly dependent columns of H contains at least $\delta + 2$ columns, i.e., $d' \geqslant \delta + 2$ as claimed. Together with (7),

$$d' = \delta + 2.$$

Again by Theorem 1, necessarily

$$k' = n - m(\delta - 1) - 2 = mr - 2.$$

Finally, we note that

$$\dim(\mathcal{C}) = k = n - |R| = n - m(\delta - 1) - 2 = k' = \dim(\mathcal{C}').$$

Since $\mathcal{C} \subseteq \mathcal{C}'$, and they are of equal dimension, we have $\mathcal{C} = \mathcal{C}'$, and H is a parity-check matrix for $\mathcal{C}$.

We turn to the case of $r = 2$. As in the previous case, a linearly dependent set of columns from H requires at least δ columns from each repair set it intersects. However, this time, since $r = 2$, we cannot choose $\delta + 2$ columns from the same repair set, since each repair set contains exactly $\delta + 1$ columns. Thus, a set of linearly dependent columns of H contains at least δ columns each from two repair sets. However, by Lemma 8, exactly δ columns each from two repair sets, still forms a set of linearly independent vectors. Thus, at least $2\delta + 1$ columns are required for a dependent set, namely, $d' \geqslant 2\delta + 1$. As in the previous case, by (7) we have

$$d' = 2\delta + 1,$$

and then

$$k' = n - m(\delta - 1) - 2 = k,$$

and $\mathcal{C} = \mathcal{C}'$, as desired.

In summary, we just proved the code $\mathcal{C}$ is an optimal LRC which is cyclic. The fact that it is a $(q^b - 1, r, 2, \delta, q^b)$-MR code follows directly from Lemma 8, since any erasure pattern hitting two repair sets with δ erasures each, corresponds to a full-rank set of columns from H, and is therefore correctable. ∎

The cyclic MR codes by Construction 1 have optimal Hamming distance, and order-optimal field size with respect to the bound in Lemma 1-(1), where we consider $\delta \geqslant 2$ as a constant. However, we can do better than that when $r = 2$, according to Corollary 4.

Corollary 5: When $r = 2$, the cyclic MR codes generated by Construction 1 have optimal field size by Corollary 4, provided that neither $q^b - 1$, nor $q^b - 2$, are prime powers. When $r > 2$, the cyclic MR codes by Construction 1 have optimal Hamming distance, and order-optimal field size with respect to the bound in Lemma 1-(1), where we consider $\delta \geqslant 2$ as a constant.

$$H = \begin{pmatrix} 1 & 0 & \cdots & 0 & \beta & 0 & \cdots & 0 & \cdots & \beta^{a-1} & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 & \beta^2 & 0 & \cdots & 0 & \cdots & \beta^{2(a-1)} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 1 & 0 & \cdots & 0 & \beta^{\delta-1} & 0 & \cdots & 0 & \cdots & \beta^{(\delta-1)(a-1)} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \beta & \cdots & 0 & \cdots & 0 & \beta^{a-1} & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \beta^2 & \cdots & 0 & \cdots & 0 & \beta^{2(a-1)} & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 1 & \cdots & 0 & 0 & \beta^{\delta-1} & \cdots & 0 & \cdots & 0 & \beta^{(\delta-1)(a-1)} & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & \beta & \cdots & 0 & 0 & \cdots & \beta^{a-1} \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & \beta^2 & \cdots & 0 & 0 & \cdots & \beta^{2(a-1)} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & \beta^{\delta-1} & \cdots & 0 & 0 & \cdots & \beta^{(\delta-1)(a-1)} \\ 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & \cdots & 1 & 1 & \cdots & 1 \\ 1 & \gamma & \cdots & \gamma^{m-1} & \gamma^m & \gamma^{m+1} & \cdots & \gamma^{2m-1} & \cdots & \gamma^{(a-1)m} & \gamma^{(a-1)m+1} & \cdots & \gamma^{n-1} \end{pmatrix}.$$

B. Turning Non-Cyclic Codes Into Cyclic Codes

Previous works that constructed *non-cyclic* (n, r, h, δ, q)-MR codes, for $h = 2$, did so with $q = \Theta(n(\delta - 1))$ in [4], and later, with $q = \Theta(n)$ [19] (see also [23], that obtained $q = \Theta(n)$ for the special case of $n = 2(r + \delta - 1)$). Of particular interest to us are the $(n, r, 2, \delta, q^b)$-MR codes from [19, Theorem IV.2]. These MR codes have the same parameters as Construction 1. However, they are not cyclic MR codes directly. In what follows, we shall attempt to determine whether the MR codes generated in [19, Theorem IV.2] can be rearranged to become cyclic codes. Along the way, we shall prove some interesting facts concerning cyclic optimal LRCs.

As a first step, we show the repair sets of cyclic optimal LRCs are severely restricted.

Theorem 7: Let $\mathcal{C}$ be a cyclic optimal LRC with parameters $[n, k, d]_q$ and all-symbol (r, δ)-locality. Write $k = ur + v$ with $0 < v \leqslant r$. If $u \geqslant 2(r - v + 1)$, then for any repair set $S \subseteq \mathbb{Z}_n$, and any $j \in \mathbb{Z}_n$, either $S + j = S$ or $(S + j) \cap S = \emptyset$.

The technical proof of Theorem 7 is deferred to the appendix. As an immediate consequence, we now show that the repair sets of cyclic optimal LRCs must be cosets of $\mathbb{Z}_n$.

Corollary 6: Let $\mathcal{C}$ be a cyclic optimal LRC with parameters $[n, k, d]_q$ and all-symbol (r, δ)-locality (where, to avoid trivial cases, we assume that $\mathcal{C}$ does not have all-symbol $(r - 1, \delta)$-locality). Let $k = ur + v$, $0 < v \leqslant r$. If $u \geqslant 2(r - v + 1)$, then $n = m(r + \delta - 1)$, $m \in \mathbb{N}$, and the repair sets of $\mathcal{C}$ are

$$G_i \triangleq \langle m \rangle + i = \{jm + i \ : \ j \in \mathbb{Z}\} \subseteq \mathbb{Z}_n,$$

for all $i \in \mathbb{Z}$.

Proof: Let $S_0 \subseteq \mathbb{Z}_n$ be a repair set such that $0 \in S_0$. By Theorem 7 we have $S_0 + i = S_0 \subseteq \mathbb{Z}_n$ for any $i \in S_0$. Thus, S_0 is a subgroup of the cyclic group $(\mathbb{Z}_n, +)$. Note that $|S_0| \leqslant r + \delta - 1$. If $|S_0| < r + \delta - 1$, then the fact $S_0 + i$, for $i \in \mathbb{Z}_n$, are also repair sets for $\mathcal{C}$, implies that $\mathcal{C}$ has all-symbol $(r - 1, \delta)$-locality, which contradicts our assumption. Thus, $|S_0| = r + \delta - 1$, $S_0 = \langle m \rangle$, and $(r + \delta - 1)|n$.

Let S be any repair set of $\mathcal{C}$. the same analysis shows that $|S| = r + \delta - 1$. Note that $S - i$ for any $i \in S$ is still a repair set of $\mathcal{C}$. Now it is easy to check that $S - i$ is a $r + \delta - 1$-subgroup of $(\mathbb{Z}_n, +)$, i.e., $S - i = S_0$, which completes the proof.   ∎

Remark: Corollary 6 shows that the condition $(r + \delta - 1)|n$ is not a restriction when $u \geqslant 2(r - v + 1)$, but rather a consequence.

Remark: For the case $u = 1$ (i.e., $k = r + v$), and $(r + \delta - 1) \nmid n$, explicit constructions were proposed in [33, Corollaries 27, 37, 43] for cyclic optimal LRCs. Corollary 6 implies that constructions with such parameters are possible only if $1 = u < 2(r - v + 1)$, i.e., $r \geqslant v$.

Further building on Corollary 6, we can now show that cyclic optimal LRCs have a parity-check matrix with a nice form.

Corollary 7: Let $\mathcal{C}$ be a cyclic optimal LRC with parameters $[n, k, d]_q$, and all-symbol (r, δ)-locality (where, to avoid trivial cases, we assume that $\mathcal{C}$ does not have all-symbol $(r - 1, \delta)$-locality). If $u \geqslant 2(r - v + 1)$, then a parity-check matrix of $\mathcal{C}$ can be given in the following form, shown in

the equation at the bottom of the next page, where s_i, h_j are column vectors, $(s_0, s_2, \cdots, s_{a-1})$ is a parity-check matrix of a cyclic code with minimum Hamming distance of at least δ, $a = r + \delta - 1$, $m = n/a$, and $(h_0, h_1, \cdots, h_{am-1})$ corresponds to the global parity checks. Moreover, the punctured codes satisfy $\mathcal{C}|_{G_i} = \mathcal{C}|_{G_0}$ for all $i \in [m]$, where $G_i \triangleq \langle m \rangle + i$. Similarly, the shortened codes satisfy $\mathcal{C}|^{G_i} = \mathcal{C}|^{G_0}$ for all $i \in [m]$, where $\mathcal{C}|^{G_i}$ is the code whose parity check matrix contains only the columns corresponding to G_i from H.

Proof: The parity-check matrix follows directly from Corollary 6 and the fact that $\mathcal{C}|_{\langle m \rangle} = \mathcal{C}|_{\langle m \rangle + i}$ for $i \in \mathbb{Z}$ is also a cyclic code. Additionally, since $\mathcal{C}$ is cyclic, trivially we have $\mathcal{C}|_{G_i} = \mathcal{C}|_{G_0}$ and $\mathcal{C}|^{G_i} = \mathcal{C}|^{G_0}$.   ∎

Now we recall a construction, which was first introduced in [19].

Construction 2 [19]: Let q be a prime power, $b \in \mathbb{N}$, $n = q^b - 1$, $a = r + \delta - 1$, $a|(q - 1)$, and $m = n/a$. Let α be a primitive element of $\mathbb{F}_{q^b}$, $\beta = \alpha^m$, and $\lambda = \alpha^s$, $\gcd(s, m) = 1$. The following parity-check matrix defines an $(n, r, 2, \delta, q^b)$-MR code, shown in the equation at the bottom of the next page.

To simply our notation, we define,

$$\boldsymbol{x} \triangleq \begin{pmatrix} x \\ x^2 \\ \vdots \\ x^{\delta - 1} \end{pmatrix}.$$

In this notation, the matrix H from Construction 2 becomes, shown in the equation at the bottom of the next page. One cannot avoid seeing a similarity between the parity-check matrix of Construction 2, and the parity-check matrix found in Theorem 6 for the code from Construction 1. However, the code from Construction 2 is not cyclic, but rather quasi-cyclic. In what follows we study whether permuting it produces a cyclic code.

Let $\mathbb{S}_n$ denote the set of permutations over $\mathbb{Z}_n$, for any $n \in \mathbb{N}$. Each permutation in $\mathbb{S}_n$ may be thought of as a bijection in $\mathbb{Z}_n^{\mathbb{Z}_n}$, namely, a bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_n$. Let $\mathcal{C}$ be a code of length n, whose coordinates are indexed by $\mathbb{Z}_n$. If $\ell \in \mathbb{S}_n$ is a permutation, we define the permutation of $\mathcal{C}$ by ℓ as

$$\mathcal{C}_\ell \triangleq \left\{ (c_{\ell(0)}, c_{\ell(1)}, \ldots, c_{\ell(n-1)}) \ : \ (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \right\}.$$

If $\mathcal{C}$ is a cyclic code, it is natural to ask for what permutations $\ell \in \mathbb{S}_n$, $\mathcal{C}_\ell$ is also cyclic. Apart from the trivial cyclic shifts of $\mathcal{C}$, a natural subset of candidate permutations are *multipliers*, namely,

$$\mu_t(x) \triangleq xt \bmod n,$$
$$\mathbb{Z}_n^\times \triangleq \{1 \leqslant t \leqslant n \ : \ \gcd(t, n) = 1\},$$
$$\Upsilon(n) \triangleq \{\mu_t \ : \ t \in \mathbb{Z}_n^\times\}.$$

Pálfy [29] proved that, in many cases, multipliers are the essential permutations keeping a code cyclic:

Lemma 9 [29]: Consider codes of length n whose coordinates are indexed by $\mathbb{Z}_n$.
1) When $\gcd(n, \varphi(n)) = 1$ or $n = 4$, for all cyclic codes $\mathcal{C}$, if $\mathcal{C}_{\ell'}$, $\ell' \in \mathbb{S}_n$, is also a cyclic code, then there is a multiplier $\ell \in \Upsilon(n)$ such that $\mathcal{C}_{\ell'} = \mathcal{C}_\ell$.

2) When $\gcd(n, \varphi(n)) \neq 1$ and $n \neq 4$, there exists a cyclic code $\mathcal{C}$, and $\ell' \in \mathbb{S}_n$ such that $\mathcal{C}_{\ell'}$ is cyclic, but $\mathcal{C}_{\ell'} \neq \mathcal{C}_\ell$ for all multipliers $\ell \in \Upsilon(n)$.

Here $\varphi(\cdot)$ denotes Euler's totient function.

Drawing inspiration from Lemma 9, we address the (different) question of finding permutations from $\mathbb{S}_n$ that turn the non-cyclic code of Construction 2 into a cyclic code. Recall that in the setting of Construction 2, $a, m, n \in \mathbb{N}$, and $n = ma$. We now define a set of functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ as follows:

$$\mu_{t,z}(xm + i) \triangleq (xmt_i + z_i) \bmod n,$$

where we assume $x \in [a]$, $i \in [m]$, $t = (t_0, \ldots, t_{m-1}) \in \mathbb{Z}^m$, and $z = (z_0, \ldots, z_{m-1}) \in \mathbb{Z}^m$. We then define the set,

$$\Psi(n, a) \triangleq \left\{ \mu_{t,z} \ : \ t \in (\mathbb{Z}_a^\times)^m, z \in \mathbb{Z}^m, (z \bmod m) \in \mathbb{S}_m \right\},$$

and where by abuse of notation, $z \bmod m$ denotes the $\mathbb{Z}_m \to \mathbb{Z}_m$ mapping that maps $i \mapsto (z_i \bmod m)$.

We would like to make some easy observations concerning the elements of $\Psi(n, a)$. Denote $G_0 \triangleq \langle m \rangle \subseteq \mathbb{Z}_n$. Then G_0 is an additive subgroup of $\mathbb{Z}_n$, and $G_0 \cong \mathbb{Z}_a$. Let us denote the cosets of G_0 by $G_i \triangleq G_0 + i$, for all $i \in \mathbb{Z}$. We now note that $j \mapsto jt \bmod n$ is a bijection from G_0 to G_0 if and only if $\gcd(t, a) = 1$. Thus, $\ell_{t,z}|_{G_i}$ (i.e., the restriction of $\ell_{t,z}$ to G_i) is a bijection from G_i to $G_{z_i \bmod m}$. With the extra requirement that $(z \bmod m) \in \mathbb{S}_m$, we have that distinct cosets G_i are mapped to distinct cosets $G_{z_i \bmod m}$, and hence, $\Psi(n, a) \subseteq \mathbb{S}_n$, namely, Ψ comprises of permutations over $\mathbb{Z}_n$.

Theorem 8: Assume the notation and setting of Construction 2, and let $\mathcal{C}$ be the resulting code when $r \geqslant 3$. Then there exists a permutation $\ell \in \Psi(n, a)$ such that $\mathcal{C}_\ell$ is a cyclic code if and only if $\gcd(m, \frac{a}{\gcd(a,\delta)}) = 1$.

Proof: We first observe that $\gcd(m, \frac{a}{\gcd(a,\delta)}) = 1$ if and only if the equation $\delta m \tau \equiv \delta \pmod{a}$ has at least one solution $\tau \in \mathbb{Z}_a$. We now prove both directions of the claim.

In the first direction, assume $\delta m \tau \equiv \delta \pmod{a}$ has a solution $\tau \in \mathbb{Z}_a$. Consider the permutation $\ell = \ell_{t,z} \in \Psi(n, a)$ for which $t = (1, \ldots, 1)$, and $z = (z_0, \ldots, z_{m-1})$, where

$$H = \begin{pmatrix}
s_0 & 0 & \cdots & 0 & s_1 & 0 & \cdots & 0 & \cdots & s_{a-1} & 0 & \cdots & 0 \\
0 & s_0 & \cdots & 0 & 0 & s_1 & \cdots & 0 & \cdots & 0 & s_{a-1} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & s_0 & 0 & 0 & \cdots & s_1 & \cdots & 0 & 0 & \cdots & s_{a-1} \\
h_0 & h_1 & \cdots & h_{m-1} & h_m & h_{m+1} & \cdots & h_{2m-1} & \cdots & h_{(a-1)m} & h_{(a-1)m+1} & \cdots & h_{am-1}
\end{pmatrix},$$

$$H = \begin{pmatrix}
1 & 0 & \cdots & 0 & \beta & 0 & \cdots & 0 & \cdots & \beta^{a-1} & 0 & \cdots & 0 \\
1 & 0 & \cdots & 0 & \beta^2 & 0 & \cdots & 0 & \cdots & \beta^{2(a-1)} & 0 & \cdots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\
1 & 0 & \cdots & 0 & \beta^{\delta-1} & 0 & \cdots & 0 & \cdots & \beta^{(\delta-1)(a-1)} & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 & 0 & \beta & \cdots & 0 & \cdots & 0 & \beta^{a-1} & \cdots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\
0 & 1 & \cdots & 0 & 0 & \beta^{\delta-1} & \cdots & 0 & \cdots & 0 & \beta^{(\delta-1)(a-1)} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1 & 0 & 0 & \cdots & \beta & \cdots & 0 & 0 & \cdots & \beta^{a-1} \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\
0 & \cdots & \cdots & 1 & 0 & 0 & \cdots & \beta^{\delta-1} & \cdots & 0 & 0 & \cdots & \beta^{(\delta-1)(a-1)} \\
\lambda^0 & \lambda^1 & \cdots & \lambda^{m-1} & \lambda^0 & \lambda^1 & \cdots & \lambda^{m-1} & \cdots & \lambda^0 & \lambda^1 & \cdots & \lambda^{m-1} \\
1 & 1 & \cdots & 1 & \beta^\delta & \beta^\delta & \cdots & \beta^\delta & \cdots & \beta^{\delta(a-1)} & \beta^{\delta(a-1)} & \cdots & \beta^{\delta(a-1)}
\end{pmatrix}.$$

$$H = \begin{pmatrix}
1 & 0 & \cdots & 0 & \beta & 0 & \cdots & 0 & \cdots & \beta^{a-1} & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 & 0 & \beta & \cdots & 0 & \cdots & 0 & \beta^{a-1} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1 & 0 & 0 & \cdots & \beta & \cdots & 0 & 0 & \cdots & \beta^{a-1} \\
\lambda^0 & \lambda^1 & \cdots & \lambda^{m-1} & \lambda^0 & \lambda^1 & \cdots & \lambda^{m-1} & \cdots & \lambda^0 & \lambda^1 & \cdots & \lambda^{m-1} \\
1 & 1 & \cdots & 1 & \beta^\delta & \beta^\delta & \cdots & \beta^\delta & \cdots & \beta^{\delta(a-1)} & \beta^{\delta(a-1)} & \cdots & \beta^{\delta(a-1)}
\end{pmatrix}.$$

$z_i = i + m\tau i$. Applying ℓ to the coordinates of $\mathcal{C}$, the parity-check matrix H from Construction 2 becomes, shown in the equation at the bottom of the page, which is a parity-check matrix for $\mathcal{C}_\ell$. Here we used $\delta m\tau \equiv \delta \pmod{a}$ to get that $\beta^{\delta m\tau} = \beta^\delta$. Now, by dividing some of the rows with appropriate scalars, another parity-check matrix for $\mathcal{C}_\ell$ is the following, shown in the equation at the bottom of the next page. It is now clear that $\mathcal{C}_\ell$ is cyclic, since $H'_\ell c^\intercal = 0$ implies $H'_\ell(\sigma(c))^\intercal = 0$, i.e., $c \in \mathcal{C}_\ell$ implies $\sigma(c) \in \mathcal{C}_\ell$.

In the second direction, assume that there exists $\ell \in \Psi(n, a)$ such that $\mathcal{C}_\ell$ is cyclic. Assume to the contrary that $\delta m\tau \not\equiv \delta \pmod{a}$ for all $\tau \in \mathbb{Z}_a$. Let us write $\ell = \ell_{t,z} \in \Psi(n, a)$, with $t = (t_0, \ldots, t_{m-1}) \in (\mathbb{Z}_a^\times)^m$, and $z = (z_0, \ldots, z_{m-1}) \in \mathbb{Z}^m$. We can now write,

$$\ell(xm + i) = (xmt_i + z_i) \bmod n = ((x + \tau_i)mt_i + \zeta_i) \bmod n$$

with $x, \tau_i \in [a]$, and $i, \zeta_i \in [m]$. Let us further define $\beta_i \triangleq \beta^{t_i}$. We can now apply ℓ to the order of the columns of H from Construction 2 to obtain a parity-check matrix H_ℓ for the code $\mathcal{C}_\ell$. By rearranging the order of the rows of the matrix, we may write, shown in the equation at the bottom of the next page.

Recall that, by construction, the multiplicative order of β is $o(\beta) = a$. Since $\gcd(t_j, a) = 1$, we also have that $o(\beta_j) = a$, for all $j \in \mathbb{Z}_m$. Taking into account that $r \geqslant 3$, namely, $a = r + \delta - 1 \geqslant \delta + 2$, we have that $1, \beta_j, \beta_j^2, \ldots, \beta_j^\delta$ are all distinct. Let us look at the columns of H_ℓ that correspond to G_j for some $j \in \mathbb{Z}_m$. These columns, after removing all-zero rows, form a (transposed) $(\delta + 1) \times a$ Vandermonde matrix.

$$\begin{pmatrix} \beta_j^{\tau_j} & \beta_j^{\tau_j+1} & \cdots & \beta_j^{\tau_j+a-1} \\ \lambda^{\zeta_j} & \lambda^{\zeta_j} & \cdots & \lambda^{\zeta_j} \\ \beta_j^{\tau_j\delta} & \beta_j^{(\tau_j+1)\delta} & \cdots & \beta_j^{(\tau_j+a-1)\delta} \end{pmatrix}$$

$$= \Pi \cdot \operatorname{diag}(\beta_j^{\tau_j}, \ldots, \beta_j^{\tau_j(\delta-1)}, \lambda^{\zeta_j}, \beta_j^{\tau_j\delta}) \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \beta_j & \cdots & \beta_j^{a-1} \\ 1 & \beta_j^2 & \cdots & \beta_j^{2(a-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \beta_j^\delta & \cdots & \beta_j^{\delta(a-1)} \end{pmatrix}, \quad (8)$$

where Π is a permutation matrix that moves the second row from the bottom to the top. Since $1, \beta_j, \beta_j^2, \ldots, \beta_j^\delta$ are all distinct, the rows of (8) are linearly independent. Thus, a linear combination of the rows of H_ℓ that results in zeros in all the positions of G_j must be a trivial combination.

We now use the fact that H_ℓ is a parity-check matrix for a cyclic code. By adding cyclic rotations of existing rows in H_ℓ, we obtain H'_ℓ which is also a parity-check matrix for the same code, shown in the equation at the bottom of the next page, where $i \in \mathbb{Z}_m$. However, these added rows must be linear combinations of the rows of H_ℓ. Since they contain zeros in

all the entries of G_j, $j \neq 0$, these linear combinations cannot use the last two rows of H_ℓ. It now follows that

$$\operatorname{rank}\begin{pmatrix} \beta_i^{\tau_i} & \beta_i^{\tau_i+1} & \cdots & \beta_i^{\tau_i+a-1} \\ \beta_0^{\tau_0} & \beta_0^{\tau_0+1} & \cdots & \beta_0^{\tau_0+a-1} \end{pmatrix}$$
$$= \operatorname{rank}\begin{pmatrix} \beta_0^{\tau_0} & \beta_0^{\tau_0+1} & \cdots & \beta_0^{\tau_0+a-1} \end{pmatrix}.$$

After the same treatment as (8), this gives

$$\operatorname{rank}\begin{pmatrix} 1 & \beta_i & \cdots & \beta_i^{a-1} \\ 1 & \beta_i^2 & \cdots & \beta_i^{2(a-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \beta_i^{\delta-1} & \cdots & \beta_i^{(\delta-1)(a-1)} \\ 1 & \beta_0 & \cdots & \beta_0^{a-1} \\ 1 & \beta_0^2 & \cdots & \beta_0^{2(a-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \beta_0^{\delta-1} & \cdots & \beta_0^{(\delta-1)(a-1)} \end{pmatrix}$$
$$= \operatorname{rank}\begin{pmatrix} 1 & \beta_0 & \cdots & \beta_0^{a-1} \\ 1 & \beta_0^2 & \cdots & \beta_0^{2(a-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \beta_0^{\delta-1} & \cdots & \beta_0^{(\delta-1)(a-1)} \end{pmatrix}.$$

If $\{\beta_0, \beta_0^2, \ldots, \beta_0^{\delta-1}\} \neq \{\beta_i, \beta_i^2, \ldots, \beta_i^{\delta-1}\}$, then by the fact that $r \geqslant 3$, we would have a contradiction to the rank equality above. It follows that

$$\{\beta_0, \beta_0^2, \ldots, \beta_0^{\delta-1}\} = \{\beta_i, \beta_i^2, \ldots, \beta_i^{\delta-1}\}, \quad (9)$$

for all $i \in \mathbb{Z}_m$.

We now repeat the argument, with an extra step. Take H'_ℓ and add to it a cyclic rotation of its last row to obtain the following parity-check matrix for the same code, shown in the equation at the bottom of the next page, where $i \in \mathbb{Z}_m$. Again, this added row is linearly dependent on the others, and so, looking at the columns of G_0 we obtain the rank equality

$$\operatorname{rank}\begin{pmatrix} \beta_i^{\tau_i} & \beta_i^{\tau_i+1} & \cdots & \beta_i^{\tau_i+a-1} \\ \beta_0^{\tau_0} & \beta_0^{\tau_0+1} & \cdots & \beta_0^{\tau_0+a-1} \\ \lambda^{\zeta_0} & \lambda^{\zeta_0} & \cdots & \lambda^{\zeta_0} \\ \beta_0^{\tau_0\delta} & \beta_0^{(\tau_0+1)\delta} & \cdots & \beta_0^{(\tau_0+a-1)\delta} \\ \beta_i^{\tau_i\delta} & \beta_i^{(\tau_i+1)\delta} & \cdots & \beta_i^{(\tau_i+a-1)\delta} \end{pmatrix}$$
$$= \operatorname{rank}\begin{pmatrix} \beta_0^{\tau_0} & \beta_0^{\tau_0+1} & \cdots & \beta_0^{\tau_0+a-1} \\ \lambda^{\zeta_0} & \lambda^{\zeta_0} & \cdots & \lambda^{\zeta_0} \\ \beta_0^{\tau_0\delta} & \beta_0^{(\tau_0+1)\delta} & \cdots & \beta_0^{(\tau_0+a-1)\delta} \end{pmatrix}.$$

$$H_\ell = \begin{pmatrix} 1 & 0 & \cdots & 0 & \beta & 0 & \cdots & 0 & \cdots & \beta^{a-1} & \cdots & 0 \\ 0 & \beta^\tau & \cdots & 0 & 0 & \beta^{\tau+1} & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \beta^{\tau(m-1)} & 0 & 0 & \cdots & \beta^{\tau(m-1)+1} & \cdots & 0 & \cdots & \beta^{\tau(m-1)+a-1} \\ \lambda^0 & \lambda^1 & \cdots & \lambda^{m-1} & \lambda^0 & \lambda^1 & \cdots & \lambda^{m-1} & \cdots & \lambda^0 & \cdots & \lambda^{m-1} \\ 1 & \beta^{\tau\delta} & \cdots & \beta^{\tau(m-1)\delta} & \beta^{\tau m\delta} & \beta^{\tau(m+1)\delta} & \cdots & \beta^{\tau(2m-1)\delta} & \cdots & \beta^{\tau m(a-1)\delta} & \cdots & \beta^{\tau(am-1)\delta} \end{pmatrix},$$

Again, using the same steps as in (8), we get

$$
\operatorname{rank}
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & \beta_i & \cdots & \beta_i^{a-1} \\
1 & \beta_i^2 & \cdots & \beta_i^{2(a-1)} \\
\vdots & \vdots & & \vdots \\
1 & \beta_i^\delta & \cdots & \beta_i^{\delta(a-1)} \\
1 & \beta_0 & \cdots & \beta_0^{a-1} \\
1 & \beta_0^2 & \cdots & \beta_0^{2(a-1)} \\
\vdots & \vdots & & \vdots \\
1 & \beta_0^\delta & \cdots & \beta_0^{\delta(a-1)}
\end{pmatrix}
$$

$$
= \operatorname{rank}
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & \beta_0 & \cdots & \beta_0^{a-1} \\
1 & \beta_0^2 & \cdots & \beta_0^{2(a-1)} \\
\vdots & \vdots & & \vdots \\
1 & \beta_0^\delta & \cdots & \beta_0^{\delta(a-1)}
\end{pmatrix}.
$$

As before, if $\left\{1, \beta_0, \beta_0^2, \ldots, \beta_0^\delta\right\} \neq \left\{1, \beta_i, \beta_i^2, \ldots, \beta_i^\delta\right\}$, then by the fact that $r \geqslant 3$, we would have a contradiction to the rank equality above. If follows that

$$
\left\{1, \beta_0, \beta_0^2, \ldots, \beta_0^\delta\right\} = \left\{1, \beta_i, \beta_i^2, \ldots, \beta_i^\delta\right\}, \tag{10}
$$

for all $i \in \mathbb{Z}_m$.

$$
H'_\ell =
\left(
\begin{array}{cccc|cccc|c|ccc}
1 & 0 & \cdots & 0 & \beta & 0 & \cdots & 0 & \cdots & \beta^{a-1} & \cdots & 0 \\
0 & 1 & \cdots & 0 & 0 & \beta & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1 & 0 & 0 & \cdots & \beta & \cdots & 0 & \cdots & \beta^{a-1} \\
\lambda^0 & \lambda^1 & \cdots & \lambda^{m-1} & \lambda^0 & \lambda^1 & \cdots & \lambda^{m-1} & \cdots & \lambda^0 & \cdots & \lambda^{m-1} \\
1 & \beta^{\tau\delta} & \cdots & \beta^{\tau(m-1)\delta} & \beta^{\tau m\delta} & \beta^{\tau(m+1)\delta} & \cdots & \beta^{\tau(2m-1)\delta} & \cdots & \beta^{\tau m(a-1)\delta} & \cdots & \beta^{\tau(am-1)\delta}
\end{array}
\right).
$$

$$
H_\ell =
\left(
\begin{array}{cccc|cccc|c|ccc}
\beta_0^{\tau_0} & 0 & \cdots & 0 & \beta_0^{\tau_0+1} & 0 & \cdots & 0 & \cdots & \beta_0^{\tau_0+a-1} & \cdots & 0 \\
0 & \beta_1^{\tau_1} & \cdots & 0 & 0 & \beta_1^{\tau_1+1} & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \beta_{m-1}^{\tau_{m-1}} & 0 & 0 & \cdots & \beta_{m-1}^{\tau_{m-1}+1} & \cdots & 0 & \cdots & \beta_{m-1}^{\tau_{m-1}+a-1} \\
\lambda^{\zeta_0} & \lambda^{\zeta_1} & \cdots & \lambda^{\zeta_{m-1}} & \lambda^{\zeta_0} & \lambda^{\zeta_1} & \cdots & \lambda^{\zeta_{m-1}} & \cdots & \lambda^{\zeta_0} & \cdots & \lambda^{\zeta_{m-1}} \\
\beta_0^{\tau_0\delta} & \beta_1^{\tau_1\delta} & \cdots & \beta_{m-1}^{\tau_{m-1}\delta} & \beta_0^{(\tau_0+1)\delta} & \beta_1^{(\tau_1+1)\delta} & \cdots & \beta_{m-1}^{(\tau_{m-1}+1)\delta} & \cdots & \beta_0^{\delta(\tau_0+a-1)} & \cdots & \beta_{m-1}^{\delta(\tau_{m-1}+a-1)}
\end{array}
\right).
$$

$$
H'_\ell =
\left(
\begin{array}{cccc|cccc|c|ccc}
\beta_i^{\tau_i} & 0 & \cdots & 0 & \beta_i^{\tau_i+1} & 0 & \cdots & 0 & \cdots & \beta_i^{\tau_i+a-1} & \cdots & 0 \\
\hline
\beta_0^{\tau_0} & 0 & \cdots & 0 & \beta_0^{\tau_0+1} & 0 & \cdots & 0 & \cdots & \beta_0^{\tau_0+a-1} & \cdots & 0 \\
0 & \beta_1^{\tau_1} & \cdots & 0 & 0 & \beta_1^{\tau_1+1} & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \beta_{m-1}^{\tau_{m-1}} & 0 & 0 & \cdots & \beta_{m-1}^{\tau_{m-1}+1} & \cdots & 0 & \cdots & \beta_{m-1}^{\tau_{m-1}+a-1} \\
\lambda^{\zeta_0} & \lambda^{\zeta_1} & \cdots & \lambda^{\zeta_{m-1}} & \lambda^{\zeta_0} & \lambda^{\zeta_1} & \cdots & \lambda^{\zeta_{m-1}} & \cdots & \lambda^{\zeta_0} & \cdots & \lambda^{\zeta_{m-1}} \\
\beta_0^{\tau_0\delta} & \beta_1^{\tau_1\delta} & \cdots & \beta_{m-1}^{\tau_{m-1}\delta} & \beta_0^{(\tau_0+1)\delta} & \beta_1^{(\tau_1+1)\delta} & \cdots & \beta_{m-1}^{(\tau_{m-1}+1)\delta} & \cdots & \beta_0^{\delta(\tau_0+a-1)} & \cdots & \beta_{m-1}^{\delta(\tau_{m-1}+a-1)}
\end{array}
\right),
$$

$$
H''_\ell =
\left(
\begin{array}{cccc|ccc|c|ccc}
\beta_i^{\tau_i} & 0 & \cdots & 0 & \beta_i^{\tau_i+1} & \cdots & 0 & \cdots & \beta_i^{\tau_i+a-1} & \cdots & 0 \\
\hline
\beta_0^{\tau_0} & 0 & \cdots & 0 & \beta_0^{\tau_0+1} & \cdots & 0 & \cdots & \beta_0^{\tau_0+a-1} & \cdots & 0 \\
0 & \beta_1^{\tau_1} & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \beta_{m-1}^{\tau_{m-1}} & 0 & \cdots & \beta_{m-1}^{\tau_{m-1}+1} & \cdots & 0 & \cdots & \beta_{m-1}^{\tau_{m-1}+a-1} \\
\lambda^{\zeta_0} & \lambda^{\zeta_1} & \cdots & \lambda^{\zeta_{m-1}} & \lambda^{\zeta_0} & \cdots & \lambda^{\zeta_{m-1}} & \cdots & \lambda^{\zeta_0} & \cdots & \lambda^{\zeta_{m-1}} \\
\beta_0^{\tau_0\delta} & \beta_1^{\tau_1\delta} & \cdots & \beta_{m-1}^{\tau_{m-1}\delta} & \beta_0^{(\tau_0+1)\delta} & \cdots & \beta_{m-1}^{(\tau_{m-1}+1)\delta} & \cdots & \beta_0^{\delta(\tau_0+a-1)} & \cdots & \beta_{m-1}^{\delta(\tau_{m-1}+a-1)} \\
\hline
\beta_i^{\tau_i\delta} & \beta_{i+1}^{\tau_{i+1}\delta} & \cdots & \beta_{i-1}^{(\tau_{i-1}+1)\delta} & \beta_i^{(\tau_i+1)\delta} & \cdots & \beta_{i-1}^{(\tau_{i-1}+2)\delta} & \cdots & \beta_i^{\delta(\tau_i+a-1)} & \cdots & \beta_{i-1}^{\tau_{i-1}\delta}
\end{array}
\right),
$$

The combination of (9) and (10) implies that $\beta_0^\delta = \beta_i^\delta$ for all $i \in \mathbb{Z}_m$. We observe that

$$\beta_0^\delta - 1 = (1 + \beta_0 + \cdots + \beta_0^{\delta-1})(\beta_0 - 1),$$
$$\beta_i^\delta - 1 = (1 + \beta_i + \cdots + \beta_i^{\delta-1})(\beta_i - 1).$$

By (9),

$$\frac{\beta_0^\delta - 1}{\beta_i^\delta - 1} = \frac{\beta_0 - 1}{\beta_i - 1}.$$

But now, since $\beta_0^\delta = \beta_i^\delta$, we conclude that

$$\beta_i = \beta_0,$$

for all $i \in \mathbb{Z}_m$.

Now that we know that $\beta_0 = \beta_1 = \cdots = \beta_{m-1}$, we can write H_ℓ as, shown in the equation at the bottom of the next page. Looking at the columns of H_ℓ that correspond to G_j, $j \in \mathbb{Z}_m$, once again we observe that the non-zero rows are equivalent to a (transposed) Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \beta_0 & \cdots & \beta_0^{a-1} \\ 1 & \beta_0^2 & \cdots & \beta_0^{2(a-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \beta_0^\delta & \cdots & \beta_0^{\delta(a-1)} \end{pmatrix}.$$

Hence, these rows are linearly independent. Let us now add a cyclically shifted version of the last row of H_ℓ, to obtain yet another parity-check matrix for the code, shown in the equation at the bottom of the next page. The added row is a linear combination of the original rows of H_ℓ. Assume $j \in \mathbb{Z}_m$, $j \neq m - 1$. If we look at the columns of G_j in H_ℓ^* we see that

$$\left(\beta_0^{\tau_{j+1}\delta}, \beta_0^{(\tau_{j+1}+1)\delta}, \ldots, \beta_0^{(\tau_{j+1}+a-1)\delta} \right)$$
$$= \beta^{(\tau_{j+1}-\tau_j)\delta} \left(\beta_0^{\tau_j\delta}, \beta_0^{(\tau_j+1)\delta}, \ldots, \beta_0^{(\tau_j+a-1)\delta} \right).$$

Since the non-zero rows in the columns of G_j are linearly independent, this linear combination is unique. Similarly, for $j = m - 1$ we get

$$\left(\beta_0^{(\tau_0+1)\delta}, \beta_0^{(\tau_0+2)\delta}, \ldots, \beta_0^{\tau_0\delta} \right)$$
$$= \beta^{(\tau_0 - \tau_{m-1})\delta + \delta} \left(\beta_0^{\tau_{m-1}\delta}, \beta_0^{(\tau_{m-1}+1)\delta}, \ldots, \beta_0^{(\tau_{m-1}+a-1)\delta} \right),$$

which is again unique. However, all these linear combinations must coincide simultaneously when viewing the entire H_ℓ^*, and so

$$\beta_0^{(\tau_1-\tau_0)\delta} = \beta_0^{(\tau_2-\tau_1)\delta} = \cdots = \beta_0^{(\tau_{m-1}-\tau_{m-2})\delta} = \beta_0^{(\tau_0-\tau_{m-1})\delta+\delta}.$$

Multiplying all of them together we get

$$\left(\beta_0^{(\tau_1-\tau_0)\delta} \right)^m = \beta_0^{(\tau_1-\tau_0)\delta} \cdot \ldots \cdot \beta_0^{(\tau_{m-1}-\tau_{m-2})\delta} \cdot \beta_0^{(\tau_0-\tau_{m-1})\delta+\delta}$$
$$= \beta_0^\delta.$$

However, this means that

$$\delta m(\tau_1 - \tau_0) \equiv \delta \pmod{a},$$

which completes the proof. ∎

While the last theorem shows us a sufficient condition under which the known code of Construction 2 may be permuted to a cyclic code, the next theorem shows us that for almost all cases, this condition is in fact necessary. First, we bring a technical proposition.

Proposition 1: Let a, r, δ be positive integers with $a = r + \delta - 1$, and $\tau, \tau' \in \mathbb{Z}_a^\times$. If

$$\{i\tau \bmod a \ : \ 1 \leqslant i \leqslant \delta - 1\} \subseteq \{i\tau' \bmod a \ : \ 1 \leqslant i \leqslant \delta\}, \tag{11}$$

and one of the following conditions holds,
  1) $\delta \geqslant 4$ and $r \geqslant 5$
  2) $\delta = 3$ and $r \geqslant 4$
  3) $\delta = 2$ and $r \geqslant 3$ is odd

then we have $\tau = \tau'$.

Proof: For Case 1, since $\tau, \tau' \in \mathbb{Z}_a^\times$ there exists an $\ell \in \mathbb{Z}_a^\times$ such that $\tau \equiv \ell\tau' \pmod{a}$. By (11), we have

$$\{(i+1)\tau \bmod a \ : \ 1 \leqslant i \leqslant \delta - 1\}$$
$$\subseteq \{(i\tau' + \tau) \bmod a \ : \ 1 \leqslant i \leqslant \delta\}$$
$$= \{(i+\ell)\tau' \bmod a \ : \ 1 \leqslant i \leqslant \delta\}.$$

Obviously,

$$|\{(i+1)\tau \bmod a \ : \ 1 \leqslant i \leqslant \delta - 1\}$$
$$\cap \{i\tau \bmod a \ : \ 1 \leqslant i \leqslant \delta - 1\}|$$
$$\geqslant \delta - 2,$$

and so,

$$|\{i\tau' \bmod a \ : \ 1 \leqslant i \leqslant \delta\}$$
$$\cap \{(i+\ell)\tau' \bmod a \ : \ 1 \leqslant i \leqslant \delta\}|$$
$$\geqslant \delta - 2,$$

and since $\tau' \in \mathbb{Z}_a^\times$,

$$|\{i \bmod a \ : \ 1 \leqslant i \leqslant \delta\} \cap \{(i+\ell) \bmod a \ : \ 1 \leqslant i \leqslant \delta\}|$$
$$\geqslant \delta - 2.$$

Since $\delta - 1 \geqslant 3$ and $a \geqslant \delta + 4$, we must have $\ell \in \{1, 2\}$. It remains to show that $\ell \neq 2$. Assume to the contrary that $\ell = 2$. Similarly, by (11), we have

$$\{(i+2)\tau \bmod a \ : \ 1 \leqslant i \leqslant \delta - 1\}$$
$$\subseteq \{(i\tau' + 2\tau) \bmod a \ : \ 1 \leqslant i \leqslant \delta\}$$
$$= \{(i+4)\tau' \bmod a \ : \ 1 \leqslant i \leqslant \delta\}.$$

Again,

$$|\{(i+2)\tau \bmod a \ : \ 1 \leqslant i \leqslant \delta - 1\}$$
$$\cap \{i\tau \bmod a \ : \ 1 \leqslant i \leqslant \delta - 1\}|$$
$$\geqslant \delta - 3,$$

which implies that,

$$|\{(i+4)\tau' \bmod a \ : \ 1 \leqslant i \leqslant \delta\}$$
$$\cap \{i\tau' \bmod a \ : \ 1 \leqslant i \leqslant \delta\}|$$
$$\geqslant \delta - 3,$$

and since $\tau' \in \mathbb{Z}_a^\times$,

$$|\{(i+4) \bmod a \ : \ 1 \leqslant i \leqslant \delta\} \cap \{i \bmod a \ : \ 1 \leqslant i \leqslant \delta\}|$$
$$\geqslant \delta - 3.$$

However, $a \geqslant \delta + 4$ implies that

$$|\{(i+4) \bmod a \ : \ 1 \leqslant i \leqslant \delta\} \cap \{i \bmod a \ : \ 1 \leqslant i \leqslant \delta\}|$$
$$\leqslant \delta - 4,$$

which is a contradiction. Thus, we have $\ell = 1$ and $\tau = \tau'$.

For Case 2, by (11), we have

$$\{\tau, 2\tau \bmod a\} \subseteq \{\tau', 2\tau' \bmod a, 3\tau' \bmod a\}.$$

If $\tau \equiv 2\tau' \pmod a$ then we have $2\tau \equiv 4\tau' \pmod a$, hence $4\tau' \bmod a \in \{\tau', 2\tau' \bmod a, 3\tau' \bmod a\}$. However, this is impossible since $\tau' \in \mathbb{Z}_a^\times$ and $a \geqslant 6$. Similarly, if $\tau \equiv 3\tau' \pmod a$ then we have $2\tau \equiv 6\tau' \pmod a$, hence $6\tau' \bmod a \in \{\tau', 2\tau' \bmod a, 3\tau' \bmod a\}$. Again, this is also impossible since $\tau' \in \mathbb{Z}_a^\times$ and $a \geqslant 6$. Thus, we have $\tau = \tau'$.

Finally, for Case 3, by (11) we have $\{\tau\} \subseteq \{\tau', 2\tau' \bmod a\}$. Obviously $\tau \equiv 2\tau' \pmod a$ is impossible since $2 \mid a$ and $a \geqslant 3$. Thus, $\tau = \tau'$. ∎

Theorem 9: Assume the notation and setting of Construction 2. Let $\mathcal{C}$ be the resulting code. Denote $k = \dim(\mathcal{C}) = ur + v$ with $0 < v \leqslant r$ and $u \geqslant 2(r - v + 1)$. Additionally, let $a = 4$ or $\gcd(a, \varphi(a)) = 1$. Furthermore, assume that $a = q^{b'} - 1 \mid q^b - 1 = n$, and that one of the following holds:

1) $\delta \geqslant 4$ and $r \geqslant 5$
2) $\delta = 3$ and $r \geqslant 4$
3) $\delta = 2$ and $r \geqslant 3$ is odd

Then there exists a permutation $\ell \in \mathbb{S}_n$ such that $\mathcal{C}_\ell$ is cyclic only if $\gcd(m, a) \mid \delta$.

Proof:

Assume $\ell \in \mathbb{S}_n$ is a permutation such that $\mathcal{C}_\ell$ is cyclic. By Construction 2, we have that $G_i \triangleq \langle m \rangle + i$, $i \in [m]$, are exactly the repair sets of $\mathcal{C}$. Thus, the image sets $\ell(G_i) \triangleq \{\ell(x) \ : \ x \in G_i\}$ are exactly the repair sets of $\mathcal{C}_\ell$. Note that $\mathcal{C}$ is an optimal LRC, which means that $\mathcal{C}_\ell$ is also optimal.

By Corollary 6, we have

$$\{\ell(G_i) \ : \ i \in [m]\} = \{G_i \ : \ i \in [m]\}.$$

Thus, there exists a sequence of permutations, ℓ_i over G_i, for all $i \in [m]$, and $z_i \in \mathbb{Z}$, such that for all $x \in G_i$,

$$\ell(x) = (\ell_i(x) + z_i) \bmod n, \tag{12}$$

which also implies that $\ell(G_i) = G_{i+z_i}$, and $(z_0, \ldots, z_{m-1})$ is a permutation of $[m]$. By assumption, $\mathcal{C}_\ell$ is cyclic. Hence, $\mathcal{C}_\ell|_{G_i}$ is also cyclic, for each $i \in [m]$.

By Construction 2, any punctured code, $\mathcal{C}|_{G_i}$, $i \in [m]$, is a subcode of the code with the $(\delta - 1) \times a$ parity-check matrix $(\mathbf{1}, \boldsymbol{\beta}, \ldots, \boldsymbol{\beta^{a-1}})$. Recall that $\mathcal{C}$ is an optimal LRC. Hence, by Theorem 2, we have that this punctured code, $\mathcal{C}|_{G_i}$, is an $[a = r + \delta - 1, r, \delta]_q$ MDS code. This implies that its parity-check matrix is *exactly* $(\mathbf{1}, \boldsymbol{\beta}, \ldots, \boldsymbol{\beta^{a-1}})$. Since this matrix clearly does not depend on i, we have $\mathcal{C}|_{G_i} = \mathcal{C}|_{G_j}$, for all $i, j \in [m]$. Additionally, since $\beta^a = 1$, all the punctured codes $\mathcal{C}|_{G_i}$ are cyclic.

By Corollary 7, we have that $\mathcal{C}_\ell|_{G_i} = \mathcal{C}_\ell|_{G_j}$ for all $i, j \in [m]$, and are all cyclic codes. Thus, a parity-check matrix of $\mathcal{C}_\ell|_{G_i}$ may be given by

$$H(\mathcal{C}_\ell|_{G_i}) = (\boldsymbol{\beta^{\tau_i,0}}, \boldsymbol{\beta^{\tau_i,1}}, \cdots, \boldsymbol{\beta^{\tau_i,a-1}}). \tag{13}$$

We now have that ℓ_0 maps the cyclic code $\mathcal{C}|_{G_0}$ into a cyclic code $\mathcal{C}_\ell|_{G_0}$, where we view these codes as indexed by $\mathbb{Z}_a$. Then, by Lemma 9, we can find a multiplier permutation from $\Upsilon(a)$ that also maps $\mathcal{C}|_{G_0}$ to $\mathcal{C}_\ell|_{G_0}$. More concretely, there exists $\tau' \in \mathbb{Z}_a^\times$, with which we define a permutation

$$\ell'(xm + i) = (xm\tau' + i) \pmod n,$$

for all $x \in [a]$ and $i \in [m]$. For this permutation we have $\mathcal{C}_\ell|_{G_i} = \mathcal{C}_{\ell'}|_{G_i}$ for all $i \in [m]$. Now, a parity-check matrix for

$$H_\ell = \begin{pmatrix} \beta_0^{\tau_0} & 0 & \cdots & 0 & \beta_0^{\tau_0+1} & 0 & \cdots & 0 & \cdots & \beta_0^{\tau_0+a-1} & \cdots & 0 \\ 0 & \beta_0^{\tau_1} & \cdots & 0 & 0 & \beta_0^{\tau_1+1} & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \beta_0^{\tau_{m-1}} & 0 & 0 & \cdots & \beta_0^{\tau_{m-1}+1} & \cdots & 0 & \cdots & \beta_0^{\tau_{m-1}+a-1} \\ \lambda^{\zeta_0} & \lambda^{\zeta_1} & \cdots & \lambda^{\zeta_{m-1}} & \lambda^{\zeta_0} & \lambda^{\zeta_1} & \cdots & \lambda^{\zeta_{m-1}} & \cdots & \lambda^{\zeta_0} & \cdots & \lambda^{\zeta_{m-1}} \\ \beta_0^{\tau_0\delta} & \beta_0^{\tau_1\delta} & \cdots & \beta_0^{\tau_{m-1}\delta} & \beta_0^{(\tau_0+1)\delta} & \beta_0^{(\tau_1+1)\delta} & \cdots & \beta_0^{(\tau_{m-1}+1)\delta} & \cdots & \beta_0^{\delta(\tau_0+a-1)} & \cdots & \beta_0^{\delta(\tau_{m-1}+a-1)} \end{pmatrix}.$$

$$H_\ell^* = \begin{pmatrix} \beta_0^{\tau_0} & 0 & \cdots & 0 & \beta_0^{\tau_0+1} & 0 & \cdots & 0 & \cdots & \beta_0^{\tau_0+a-1} & \cdots & 0 \\ 0 & \beta_0^{\tau_1} & \cdots & 0 & 0 & \beta_0^{\tau_1+1} & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \beta_0^{\tau_{m-1}} & 0 & 0 & \cdots & \beta_0^{\tau_{m-1}+1} & \cdots & 0 & \cdots & \beta_0^{\tau_{m-1}+a-1} \\ \lambda^{\zeta_0} & \lambda^{\zeta_1} & \cdots & \lambda^{\zeta_{m-1}} & \lambda^{\zeta_0} & \lambda^{\zeta_1} & \cdots & \lambda^{\zeta_{m-1}} & \cdots & \lambda^{\zeta_0} & \cdots & \lambda^{\zeta_{m-1}} \\ \beta_0^{\tau_0\delta} & \beta_0^{\tau_1\delta} & \cdots & \beta_0^{\tau_{m-1}\delta} & \beta_0^{(\tau_0+1)\delta} & \beta_0^{(\tau_1+1)\delta} & \cdots & \beta_0^{(\tau_{m-1}+1)\delta} & \cdots & \beta_0^{\delta(\tau_0+a-1)} & \cdots & \beta_0^{\delta(\tau_{m-1}+a-1)} \\ \beta_0^{\tau_1\delta} & \beta_0^{\tau_2\delta} & \cdots & \beta_0^{(\tau_0+1)\delta} & \beta_0^{(\tau_1+1)\delta} & \beta_0^{(\tau_2+1)\delta} & \cdots & \beta_0^{(\tau_0+2)\delta} & \cdots & \beta_0^{\delta(\tau_1+a-1)} & \cdots & \beta_0^{\tau_0\delta} \end{pmatrix}.$$

$\mathcal{C}_{\ell'}|_{G_i}$ may be given by

$$H(\mathcal{C}_{\ell'}|_{G_i}) = (\mathbf{1}, \boldsymbol{\beta}^{\boldsymbol{\tau}'}, \cdots, \boldsymbol{\beta}^{\boldsymbol{\tau}'(\boldsymbol{a-1})}),$$

and it must be row-equivalent to $H(\mathcal{C}_\ell|_{G_i})$ from (13).

We switch our view from the punctured codes to the shortened codes of $\mathcal{C}$. As above, the following shortened codes are all equal, $\mathcal{C}|^{G_i} = \mathcal{C}|^{G_0}$, for all $i \in [m]$. A parity-check matrix for them may be written as

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \mathbf{1} & \boldsymbol{\beta} & \cdots & \boldsymbol{\beta}^{\boldsymbol{a-1}} \\ 1 & \beta^\delta & \cdots & \beta^{\delta(a-1)} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \beta & \cdots & \beta^{a-1} \\ 1 & \beta^2 & \cdots & \beta^{2(a-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{\delta-1} & \cdots & \beta^{(\delta-1)(a-1)} \\ 1 & \beta^\delta & \cdots & \beta^{(\delta)(a-1)} \end{pmatrix}.$$

By the multiplicative order of β, the codes $\mathcal{C}|^{G_i}$ are all cyclic. By Corollary 7, $\mathcal{C}_\ell|^{G_i} = \mathcal{C}_\ell|^{G_0}$, for all $i \in [m]$, and a parity-check matrix for them may be given by

$$H(\mathcal{C}_\ell|^{G_i}) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,0}} & \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,1}} & \cdots & \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,a-1}} \\ \beta^{\delta\tau_{i,0}} & \beta^{\delta\tau_{i,1}} & \cdots & \beta^{\delta\tau_{i,a-1}} \end{pmatrix}, \qquad (14)$$

where $\tau_{i,j}$, $i \in [m]$, $j \in [a]$, are the same as those in (13). Once again, $\mathcal{C}_\ell|^{G_i}$ are all cyclic. Hence, by Lemma 9 we can find a multiplier permutation from $\Upsilon(a)$ that also maps $\mathcal{C}|^{G_0}$ to $\mathcal{C}_\ell|^{G_0}$. Namely, there exists $\tau'' \in \mathbb{Z}_a^\times$, with which we define

$$\ell''(xm + i) = (xm\tau'' + i) \pmod{n},$$

for all $x \in [a]$ and $i \in [m]$, such that $\mathcal{C}_\ell|^{G_i} = \mathcal{C}_{\ell''}|^{G_i}$, for all $i \in [m]$. A parity-check matrix for $\mathcal{C}_{\ell''}|^{G_i}$ may be given by

$$H(\mathcal{C}_{\ell''}|^{G_i}) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \mathbf{1} & \boldsymbol{\beta}^{\boldsymbol{\tau}''} & \cdots & \boldsymbol{\beta}^{\boldsymbol{\tau}''(\boldsymbol{a-1})} \\ 1 & \beta^{\delta\tau''} & \cdots & \beta^{\delta\tau''(a-1)} \end{pmatrix},$$

and it must be row-equivalent to $H(\mathcal{C}_\ell|^{G_i})$ from (14).

By the properties of Vandermonde matrices we have for all $i \in [m]$,

$$\delta + 1 = \mathrm{rank} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,0}} & \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,1}} & \cdots & \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,a-1}} \\ \beta^{\delta\tau_{i,0}} & \beta^{\delta\tau_{i,1}} & \cdots & \beta^{\delta\tau_{i,a-1}} \end{pmatrix}$$

$$= \mathrm{rank} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,0}} & \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,1}} & \cdots & \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,a-1}} \\ \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,0}} & \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,1}} & \cdots & \boldsymbol{\beta}^{\boldsymbol{\tau}_{i,a-1}} \\ \beta^{\delta\tau_{i,0}} & \beta^{\delta\tau_{i,1}} & \cdots & \beta^{\delta\tau_{i,a-1}} \end{pmatrix}$$

$$= \mathrm{rank} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \mathbf{1} & \boldsymbol{\beta}^{\boldsymbol{\tau}'} & \cdots & \boldsymbol{\beta}^{\boldsymbol{\tau}'(\boldsymbol{a-1})} \\ \mathbf{1} & \boldsymbol{\beta}^{\boldsymbol{\tau}''} & \cdots & \boldsymbol{\beta}^{\boldsymbol{\tau}''(\boldsymbol{a-1})} \\ 1 & \beta^{\delta\tau''} & \cdots & \beta^{\delta\tau''(a-1)} \end{pmatrix},$$

where the last equality holds by the row equivalence of $H(\mathcal{C}_\ell|_{G_i})$ and $H(\mathcal{C}_{\ell'}|_{G_i})$, as well as the row equivalence of $H(\mathcal{C}_\ell|^{G_i})$ and $H(\mathcal{C}_{\ell''}|^{G_i})$. Since $r \geqslant 3$, the above equality implies

$$\left\{ \beta^{j\tau'} \ : \ 1 \leqslant j \leqslant \delta - 1 \right\} \subseteq \left\{ \beta^{j\tau''} \ : \ 0 \leqslant j \leqslant \delta \right\}.$$

By construction, the multiplicative order of β is $o(\beta) = a$, and so

$$o(\beta^{\tau'}) = \frac{o(\beta)}{\gcd(\tau', o(\beta))} = \frac{a}{\gcd(\tau', a)} = a,$$

where the last equality follows from the fact that $\tau' \in \mathbb{Z}_a^\times$. Since $a = r + \delta - 1$,

$$1 \notin \left\{ \beta^{j\tau'} \ : \ 1 \leqslant j \leqslant \delta - 1 \right\}.$$

Thus,

$$\left\{ \beta^{j\tau'} \ : \ 1 \leqslant j \leqslant \delta - 1 \right\} \subseteq \left\{ \beta^{j\tau''} \ : \ 1 \leqslant j \leqslant \delta \right\}.$$

Since $o(\beta) = a$, we have

$$\{j\tau' \bmod a \ : \ 1 \leqslant j \leqslant \delta - 1\} \subseteq \{j\tau'' \bmod a \ : \ 1 \leqslant j \leqslant \delta\}.$$

Then, by Proposition 1, we have $\tau' = \tau''$.

Denote $\gamma \triangleq \beta^{\tau'} = \beta^{\tau''}$. Thus, $(\mathbf{1}, \boldsymbol{\gamma}, \cdots, \boldsymbol{\gamma}^{\boldsymbol{a-1}}) = (\mathbf{1}, \boldsymbol{\beta}^{\boldsymbol{\tau}'}, \cdots, \boldsymbol{\beta}^{\boldsymbol{\tau}'(\boldsymbol{a-1})})$. We now know that the following two matrices are row equivalent

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \mathbf{1} & \boldsymbol{\gamma} & \cdots & \boldsymbol{\gamma}^{\boldsymbol{a-1}} \\ 1 & \gamma^\delta & \cdots & \gamma^{\delta(a-1)} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \mathbf{1} & \boldsymbol{\gamma} & \cdots & \boldsymbol{\gamma}^{\boldsymbol{a-1}} \\ \beta^{\delta\tau_{i,0}} & \beta^{\delta\tau_{i,1}} & \cdots & \beta^{\delta\tau_{i,a-1}} \end{pmatrix},$$

$$(15)$$

for all $i \in [m]$. Recall that β and γ have the same order, $o(\beta) = o(\gamma)a = q^{b'} - 1$, i.e., the entries of the matrices in (15) belong to the field $\mathbb{F}_{q^{b'}}$. Hence, $(\beta^{\delta\tau_{i,0}}, \beta^{\delta\tau_{i,1}}, \cdots, \beta^{\delta\tau_{i,a-1}})$ can be represented as a linear combination

$$(\beta^{\delta\tau_{i,0}}, \beta^{\delta\tau_{i,1}}, \cdots, \beta^{\delta\tau_{i,a-1}})$$

$$= \sum_{s=0}^{\delta} \eta_{i,s}(1, \gamma^s, \cdots, \gamma^{s(a-1)}) \qquad (16)$$

where $\eta_{i,s} \in \mathbb{F}_{q^{b'}} \subseteq \mathbb{F}_{q^b}$ for all $i \in [m]$, $s \in [\delta + 1]$. We also highlight the fact that $\eta_{i,\delta} \neq 0$ for all $i \in [m]$, for otherwise we would have that the matrix on the right has rank δ whereas the one on the left has rank $\delta + 1$. For convenience, let us define $\xi_{i,j} \triangleq \eta_{i,\delta}\gamma^{\delta j} + \eta_{i,0}$, where $i \in [m]$, $j \in [a]$.

After focusing on shortened and punctured codes, let us look again at the entire code. If we permute the columns of the parity-check matrix of $\mathcal{C}$ using ℓ, we arrive at the following parity-check matrix for $\mathcal{C}_\ell$, to (14), shown in the equation at the bottom of the next page, where z_i, $i \in [m]$ are the same as in (12), and $\tau_{i,j}$, $i \in [m]$, $j \in [a]$, are the same as in (13). By (16) and the equivalence of $H(\mathcal{C}_\ell|_{G_i})$ and $H(\mathcal{C}_{\ell'}|_{G_i})$, the matrix H_ℓ is row equivalent with, shown in the equation at the bottom of the next page. Since H' is also a parity-check matrix for $\mathcal{C}_\ell$, which is a cyclic code, adding a dependent row to H' which is a cyclic shift of another row, does not change the code. Hence, we look at the following parity-check matrix for $\mathcal{C}_\ell$, shown in the equation at the bottom of the next page.

Let us now denote by h the bottom row of H'', and by h_{-2}, h_{-1} the bottom two rows of H'. We recall that $\xi_{i,j} \triangleq \eta_{i,\delta}\gamma^{\delta j} + \eta_{i,0}$, and hence,

$$h|_{G_i} = (\eta_{i+1,\delta}\gamma^0 + \eta_{i+1,0}, \eta_{i+1,\delta}\gamma^\delta + \eta_{i+1,0},$$
$$\ldots, \eta_{i+1,\delta}\gamma^{\delta(a-1)} + \eta_{i+1,0}), \qquad i \in [m-1]$$

$$h|_{G_{m-1}} = (\eta_{0,\delta}\gamma^\delta + \eta_{0,0}, \eta_{0,\delta}\gamma^{2\delta} + \eta_{0,0}, \ldots, \eta_{0,\delta}\gamma^0 + \eta_{0,0}),$$
$$h_{-1}|_{G_i} = (\eta_{i,\delta}\gamma^0 + \eta_{i,0}, \eta_{i,\delta}\gamma^\delta + \eta_{i,0},$$
$$\ldots, \eta_{i,\delta}\gamma^{\delta(a-1)} + \eta_{i,0}), \qquad i \in [m]$$
$$h_{-2}|_{G_i} = \lambda^{z_i}(1,1,\ldots,1) \qquad i \in [m].$$

We now observe that the last row of $H''|_{G_i}$ may be shown as a linear combination of the preceding two rows. More precisely, for all $i \in [m]$,

$$h|_{G_i} = \theta_{i,1}h_{-1}|_{G_i} + \theta_{i,2}h_{-2}|_{G_i},$$

where

$$\theta_{i,1} = \begin{cases} \frac{\eta_{i+1,\delta}}{\eta_{i,\delta}} & i \in [m-1], \\ \frac{\eta_{0,\delta}}{\eta_{m-1,\delta}}\gamma^\delta & i = m-1, \end{cases}$$

$$\theta_{i,2} = \begin{cases} \frac{\eta_{i+1,0} - \theta_{1,i}\eta_{i,0}}{\lambda^{z_i}} & i \in [m-1], \\ \frac{\eta_{0,0} - \theta_{m-1,1}\eta_{m-1,0}}{\lambda^{z_{m-1}}} & i = m-1. \end{cases} \qquad (17)$$

Since H'' is row equivalent with H', and $\operatorname{rank}(H'|_{G_i}) = \delta + 1$ (i.e., full rank), the linear combination above is the *unique* linear combination of the rows of $H'|_{G_i}$ that gives $h|_{G_i}$. This linear combination does not use the first $\delta - 1$ rows of $H'|_{G_i}$.

Looking at the entire matrix (instead of focusing on the projections onto G_i), once again, since H'' is row equivalent with H', h must be linear combination of the rows of H'. Since in each projection onto G_i there is a unique linear combination, all these must simultaneously agree. In particular, this means

$$\theta_{0,1} = \theta_{1,1} = \theta_{2,1} = \cdots = \theta_{m-1,1}.$$

We recall that $0 \neq \eta_{i,\delta} \in \mathbb{F}_{q^{b'}}$ for all $i \in [m]$, and $\gamma \in \mathbb{F}_{q^{b'}}$ is primitive. Thus, we may write

$$\theta_{0,1} = \theta_{1,1} = \theta_{2,1} = \cdots = \theta_{m-1,1} = \gamma^j, \qquad (18)$$

for some integer j. Also, by (17),

$$\frac{\eta_{1,\delta}}{\eta_{0,\delta}} = \frac{\eta_{2,\delta}}{\eta_{1,\delta}} = \frac{\eta_{3,\delta}}{\eta_{2,\delta}} = \cdots = \frac{\eta_{m-1,\delta}}{\eta_{m-2,\delta}} = \gamma^\delta \frac{\eta_{0,\delta}}{\eta_{m-1,\delta}}. \qquad (19)$$

Now, combining (18) and (19) we get

$$\gamma^{jm} = \prod_{i\in[m]} \theta_{i,1} = \gamma^\delta.$$

Thus,

$$jm \equiv \delta \pmod{a}.$$

This, in turn, implies that $\gcd(m,a) \mid \delta$, as we wanted to prove. ∎

To conclude this section, we make use of Theorem 9 in order to show that Construction 1 may produce cyclic MR codes with new parameters. Namely, in certain case, the construction of [19], which produces codes with the same parameters as our Construction 1, results in codes that are neither cyclic, nor can be permuted to become cyclic.

$$H_\ell = \begin{pmatrix} \beta^{\tau_{0,0}} & 0 & \cdots & 0 & \beta^{\tau_{0,1}} & 0 & \cdots & 0 & \cdots & \beta^{\tau_{0,a-1}} & 0 & \cdots & 0 \\ 0 & \beta^{\tau_{1,0}} & \cdots & 0 & 0 & \beta^{\tau_{1,1}} & \cdots & 0 & \cdots & 0 & \beta^{\tau_{1,a-1}} & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \beta^{\tau_{m-1,0}} & 0 & 0 & \cdots & \beta^{\tau_{m-1,1}} & \cdots & 0 & 0 & \cdots & \beta^{\tau_{m-1,a-1}} \\ \lambda^{z_0} & \lambda^{z_1} & \cdots & \lambda^{z_{m-1}} & \lambda^{z_0} & \lambda^{z_1} & \cdots & \lambda^{z_{m-1}} & \cdots & \lambda^{z_0} & \lambda^{z_1} & \cdots & \lambda^{z_{m-1}} \\ \beta^{\delta\tau_{0,0}} & \beta^{\delta\tau_{1,0}} & \cdots & \beta^{\delta\tau_{m-1,0}} & \beta^{\delta\tau_{0,1}} & \beta^{\delta\tau_{1,1}} & \cdots & \beta^{\delta\tau_{m-1,1}} & \cdots & \beta^{\delta\tau_{0,a-1}} & \beta^{\delta\tau_{1,a-1}} & \cdots & \beta^{\delta\tau_{m-1,a-1}} \end{pmatrix},$$

$$H' = \begin{pmatrix} 1 & 0 & \cdots & 0 & \gamma & 0 & \cdots & 0 & \cdots & \gamma^{a-1} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \gamma & \cdots & 0 & \cdots & 0 & \gamma^{a-1} & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & \gamma & \cdots & 0 & 0 & \cdots & \gamma^{a-1} \\ \lambda^{z_0} & \lambda^{z_1} & \cdots & \lambda^{z_{m-1}} & \lambda^{z_0} & \lambda^{z_1} & \cdots & \lambda^{z_{m-1}} & \cdots & \lambda^{z_0} & \lambda^{z_1} & \cdots & \lambda^{z_{m-1}} \\ \xi_{0,0} & \xi_{1,0} & \cdots & \xi_{m-1,0} & \xi_{0,1} & \xi_{1,1} & \cdots & \xi_{m-1,1} & \cdots & \xi_{0,a-1} & \xi_{1,a-1} & \cdots & \xi_{m-1,a-1} \end{pmatrix}.$$

$$H'' = \begin{pmatrix} 1 & 0 & \cdots & 0 & \gamma & 0 & \cdots & 0 & \cdots & \gamma^{a-1} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \gamma & \cdots & 0 & \cdots & 0 & \gamma^{a-1} & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & \gamma & \cdots & 0 & 0 & \cdots & \gamma^{a-1} \\ \lambda^{z_0} & \lambda^{z_1} & \cdots & \lambda^{z_{m-1}} & \lambda^{z_0} & \lambda^{z_1} & \cdots & \lambda^{z_{m-1}} & \cdots & \lambda^{z_0} & \lambda^{z_1} & \cdots & \lambda^{z_{m-1}} \\ \xi_{0,0} & \xi_{1,0} & \cdots & \xi_{m-1,0} & \xi_{0,1} & \xi_{1,1} & \cdots & \xi_{m-1,1} & \cdots & \xi_{0,a-1} & \xi_{1,a-1} & \cdots & \xi_{m-1,a-1} \\ \xi_{1,0} & \xi_{2,0} & \cdots & \xi_{0,1} & \xi_{1,1} & \xi_{2,1} & \cdots & \xi_{0,2} & \cdots & \xi_{1,a-1} & \xi_{2,a-1} & \cdots & \xi_{0,0} \end{pmatrix}.$$

Example 4: Set $q = 3$, $b_1 = 2$, $b = 4$, $r = 6$, $\delta = 3$, $a = 8$, $n = 80$, and $m = 10$. By using Construction 1, we may generate a cyclic $(n = 80, r = 6, h = 2, \delta = 3, q^b = 3^4)$-MR code, where we note that $\gcd(3, 10) = 1$. A *non-cyclic* MR code with the same parameters may be constructed using [19]. However, since $\gcd(m, a) = \gcd(10, 8) = 2 \nmid 3 = \delta$, by Theorem 9 this code cannot be permuted to become a cyclic code.

V. CONCLUSION

In this paper, we proved a new lower bound on the field size of optimal LRCs. As a byproduct, when $r = 2$ we were able to prove that some known code constructions actually have optimal field size (where we further had to assume that the field size minus 1 or 2 is not a prime power). We then constructed cyclic MR codes. When $r = 2$, these codes also attain the new bound with equality, and therefore have optimal field size (again, assuming the same number-theoretic condition). We concluded by showing a known quasi-cyclic MR code, with the same parameters as our cyclic construction, may sometimes be permuted to become cyclic, and in other cases it may not.

Many open questions remain. First and foremost, the construction for a cyclic MR code in this paper only works for the case of two global parity checks, i.e., $h = 2$. However, in the non-cyclic case, there are a few known constructions of MR codes with $h \geqslant 3$. Finding cyclic MR codes with $h \geqslant 3$ is still an open question.

As a second open question we mention our lower bound on the field size of optimal LRCs. We were able to show it is tight only when $r = 2$. Thus, finding out whether it is tight for cases in which $r \geqslant 3$, or improving it, remains widely open. We leave these questions and others for future work.

APPENDIX

In this appendix, we shall prove Theorem 7. To this end, we first recall some definitions and lemmas from [9].

Throughout the appendix we shall assume the coordinate of code of length n are indexed by $\mathbb{Z}_n$, and where operations on coordinates are required, they shall be made modulo n. Let $k = ru + v$ with $0 < v \leqslant r$. Denote the set of all the possible repair sets for an LRC $\mathcal{C}$ with all-symbol (r, δ)-locality as

$$\Gamma \triangleq \{ S \ : \ S \subseteq \mathbb{Z}_n, |S| \leqslant r + \delta - 1, d(\mathcal{C}|_S) \geqslant \delta \}.$$

Lemma 10 ([8], Lemma 7): Let $\mathcal{C}$ be an $[n, k]_q$ linear code with all-symbol (r, δ)-locality. If for a subset $\mathcal{V} \subseteq \Gamma$, and for all $S' \in \mathcal{V}$,

$$\left| S' \cap \left(\bigcup_{S \in \mathcal{V} \setminus \{S'\}} S \right) \right| \leqslant |S'| - \delta + 1,$$

then we have

$$\operatorname{rank} \left(\bigcup_{S \in \mathcal{V}} S \right) \leqslant \left| \bigcup_{S \in \mathcal{V}} S \right| - |\mathcal{V}| (\delta - 1).$$

For cyclic LRCs we have the following simple fact.

Lemma 11: Let $\mathcal{C}$ be a cyclic LRC. If $S \in \Gamma$ is a repair set of $\mathcal{C}$, then $S + i$ is also a repair set of $\mathcal{C}$, for all $i \in \mathbb{Z}$.

Proof: Since $\mathcal{C}$ is cyclic, $\mathcal{C}|_S = \mathcal{C}|_{S+i}$ for any $i \in \mathbb{Z}$. The claim follows immediately by definition. ∎

We are now ready for the main proof.

Proof of Theorem 7: Assume to the contrary that there exists a repair set $\widehat{S} \in \Gamma$ and $\widehat{t} \in \mathbb{Z}$ such that

$$0 < \left| \widehat{S} \cap (\widehat{S} + \widehat{t}) \right| < \left| \widehat{S} \right|. \tag{20}$$

As an auxiliary claim, we contend that for any $\tau \leqslant u/2$ there exists a 2τ-subset of $\mathcal{S} \subseteq \Gamma$ that satisfies one of the following properties:

P1. There exists a subset $\mathcal{S}' \subseteq \mathcal{S}$ and $S' \in \mathcal{S}'$ such that

$$|S'| - \delta + 1 \leqslant \left| S' \cap \left(\bigcup_{S \in \mathcal{S}' \setminus \{S'\}} S \right) \right| < |S'|. \tag{21}$$

P2. The following inequalities hold:

$$|\mathcal{S}| (r + \delta - 1) - \left| \bigcup_{S \in \mathcal{S}} S \right| \geqslant \tau, \tag{22}$$

$$\left| \bigcup_{S \in \mathcal{S}} S \right| \geqslant \operatorname{rank} \left(\bigcup_{S \in \mathcal{S}} S \right) + |\mathcal{S}| (\delta - 1). \tag{23}$$

We proceed to prove this auxiliary claim by induction on τ.

For the induction base, consider $\tau = 1 \leqslant u/2$. In that case, choose $\mathcal{S} = \mathcal{S}' = \left\{ \widehat{S}, \widehat{S} + \widehat{t} \right\}$. By (20), if additionally, $|\widehat{S}| - \delta + 1 \leqslant |\widehat{S} \cap (\widehat{S} + \widehat{t})|$, then P1 holds. Otherwise, by Lemma 10, P2 holds. Thus, the induction base is proved. Now arbitrarily choose $i_1 \in \widehat{S} \cap (\widehat{S} + \widehat{t})$.

For the induction hypothesis, assume the claim holds for τ, and let $\mathcal{S}_\tau$ be a set that satisfies the claim in that case, i.e., $|\mathcal{S}_\tau| = 2\tau$. For the induction step, we prove it also holds for $\tau + 1$, as long as $\tau + 1 \leqslant u/2$, namely, that there exists a repair set of repair sets, $\mathcal{S}_{\tau+1}$, containing $2(\tau+1)$ repair sets, that satisfies P1 or P2. We shall make an educated guess as to what $\mathcal{S}_{\tau+1}$ might be, which will work in most cases. When it does not, we shall offer a correction to our initial choice of $\mathcal{S}_{\tau+1}$.

Since $2\tau \leqslant u - 2$ we have

$$\operatorname{rank} \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \leqslant 2\tau r \leqslant (u - 2)r < k.$$

Hence, there exists an $i_{\tau+1} \in \mathbb{Z}_n$ with $\operatorname{span}(\{i_{\tau+1}\}) \not\subseteq \operatorname{span}(\bigcup_{S \in \mathcal{S}_\tau} S)$. As our initial guess, we now define the following:

$$S_{\tau+1,1} = \widehat{S} + i_{\tau+1} - i_1,$$
$$S_{\tau+1,2} = \widehat{S} + \widehat{t} + i_{\tau+1} - i_1,$$
$$\mathcal{S}_{\tau+1} = \mathcal{S}_\tau \cup \{ S_{\tau+1,1}, S_{\tau+1,2} \}.$$

We observe that $S_{\tau+1,1} \neq S_{\tau+1,2}$ since they are cyclic rotations by the same amount of $\widehat{S}$ and $\widehat{S} + \widehat{t}$, respectively, which by (20), are two distinct sets. Additionally, $i_{\tau+1} \in S_{\tau+1,1} \cap S_{\tau+1,2}$, and since $\operatorname{span}(\{i_{\tau+1}\}) \not\subseteq \operatorname{span}(\bigcup_{S \in \mathcal{S}_\tau} S)$, it follows that $S_{\tau+1,1}, S_{\tau+1,2} \notin \mathcal{S}_\tau$. Hence, $|\mathcal{S}_{\tau+1}| = 2(\tau+1)$.

If $\mathcal{S}_\tau$ satisfies P1 then trivially so does $\mathcal{S}_{\tau+1}$ and the claim follows. Assume then that S_τ only satisfies P2. In particular, by (23),

$$\left| \bigcup_{S \in \mathcal{S}_\tau} S \right| \geqslant \operatorname{rank}\left(\bigcup_{S \in \mathcal{S}_\tau} S \right) + |\mathcal{S}_\tau|\, (\delta - 1). \qquad (24)$$

Again, if $\mathcal{S}_{\tau+1}$ satisfies P1 then we are done. Otherwise, assume that $\mathcal{S}_{\tau+1}$ does not satisfy P1, which means

$$\left| S_{\tau+1,j} \cap \left(\bigcup_{S \in \mathcal{S}_{\tau+1} \setminus \{S_{\tau+1,j}\}} S \right) \right| = |S_{\tau+1,j}|, \qquad (25)$$

or

$$\left| S_{\tau+1,j} \cap \left(\bigcup_{S \in \mathcal{S}_{\tau+1} \setminus \{S_{\tau+1,j}\}} S \right) \right| < |S_{\tau+1,j}| - \delta + 1 \qquad (26)$$

for $j = 1, 2$.

If (25) holds for $S_{\tau+1,1}$, then the fact that

$$0 < |S_{\tau+1,1} \cap S_{\tau+1,2}| = \left| \widehat{S} \cap (\widehat{S} + \widehat{t}) \right| < \left| \widehat{S} \right|,$$

means that

$$\left| S_{\tau+1,1} \cap \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right| \geqslant 1. \qquad (27)$$

Recall that $\operatorname{span}(\{i_{\tau+1}\}) \not\subseteq \operatorname{span}(\cup_{S \in \mathcal{S}_\tau} S)$, but note that $i_{\tau+1} \in S_{\tau+1,1}$, which implies that

$$\left| S_{\tau+1,1} \cap \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right| < |S_{\tau+1,1}| - \delta + 1.$$

Thus, we can find a $(\delta - 1)$-subset $S_{\tau+1,1}^* \subseteq S_{\tau+1,1}$ such that $\operatorname{rank}(S_{\tau+1,1} \setminus S_{\tau+1,1}^*) = \operatorname{rank}(S_{\tau+1,1})$ and

$$S_{\tau+1,1}^* \cap \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) = \emptyset.$$

We therefore have,

$$\operatorname{rank}\left(S_{\tau+1,1} \cup \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right)$$

$$= \operatorname{rank}\left((S_{\tau+1,1} \setminus S_{\tau+1,1}^*) \cup \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right)$$

$$\leqslant \left| S_{\tau+1,1} \setminus \left(S_{\tau+1,1}^* \cup \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right) \right| + \operatorname{rank}\left(\bigcup_{S \in \mathcal{S}_\tau} S \right)$$

$$\leqslant \left| S_{\tau+1,1} \setminus \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right| - \delta + 1 + \left| \bigcup_{S \in \mathcal{S}_\tau} S \right| - 2\tau(\delta - 1)$$

$$= \left| S_{\tau+1,1} \cup \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right| - (2\tau + 1)(\delta - 1), \qquad (28)$$

where the second inequality holds by (24). Note that since $\mathcal{S}_\tau$ satisfies P2, by (22),

$$(2\tau + 1)(r + \delta - 1) \geqslant \left| \bigcup_{S \in \mathcal{S}_\tau} S \right| + \tau + r + \delta - 1$$

$$\geqslant \left| \bigcup_{S \in \mathcal{S}_\tau} S \right| + \tau + |S_{\tau+1,1}|$$

$$\geqslant \left| S_{\tau+1,1} \cup \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right| + \tau + 1, \qquad (29)$$

where the last inequality follows from (27). Recall that $\tau + 1 \leqslant u/2$, hence

$$\operatorname{rank}\left(S_{\tau+1,1} \cup \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right) \leqslant (2\tau + 1)r \leqslant (u - 1)r$$

$$\leqslant k - 1 - r.$$

It then follows that there exists a repair set $\widetilde{S}_{\tau+1,2} \in \Gamma$ such that

$$\operatorname{span}(\widetilde{S}_{\tau+1,2}) \not\subseteq \operatorname{span}\left(\bigcup_{S \in \mathcal{S}_\tau \cup \{S_{\tau+1,1}\}} S \right).$$

We now correct our initial guess, and for this case only, set $\mathcal{S}_{\tau+1} = \mathcal{S}_\tau \cup \left\{ S_{\tau+1,1}, \widetilde{S}_{\tau+1,2} \right\}$. We therefore have,

$$\operatorname{rank}\left(\bigcup_{S \in \mathcal{S}_{\tau+1}} S \right) > \operatorname{rank}\left(\bigcup_{S \in \mathcal{S}_\tau \cup \{S_{\tau+1,1}\}} S \right).$$

By the last inequality, there exists a $(\delta - 1)$-subset $\widetilde{S}_{\tau+1,2}^* \subseteq \widetilde{S}_{\tau+1,2} \setminus (\bigcup_{S \in \mathcal{S}_\tau \cup \{S_{\tau+1,1}\}} S)$, and then

$$\operatorname{rank}\left(\bigcup_{S \in \mathcal{S}_{\tau+1}} S \right)$$

$$= \operatorname{rank}\left((\widetilde{S}_{\tau+1,2} \setminus \widetilde{S}_{\tau+1,2}^*) \cup \left(\bigcup_{S \in \mathcal{S}_\tau \cup \{S_{\tau+1,1}\}} S \right) \right)$$

$$\leqslant \left| \widetilde{S}_{\tau+1,2} \setminus \left(\widetilde{S}_{\tau+1,2}^* \cup \left(\bigcup_{S \in \mathcal{S}_\tau \cup \{S_{\tau+1,1}\}} S \right) \right) \right|$$

$$+ \operatorname{rank}\left(\bigcup_{S \in \mathcal{S}_\tau \cup \{S_{\tau+1,1}\}} S \right)$$

$$\leqslant \left| \widetilde{S}_{\tau+1,2} \setminus \left(\bigcup_{S \in \mathcal{S}_\tau \cup \{S_{\tau+1,1}\}} S \right) \right| - \delta + 1$$

$$+ \left| S_{\tau+1,1} \cup \bigcup_{S \in \mathcal{S}_\tau} S \right| - (2\tau + 1)(\delta - 1)$$

$$= \left| \bigcup_{S \in \mathcal{S}_{\tau+1}} S \right| - (2\tau + 2)(\delta - 1), \qquad (30)$$

where the second inequality holds by (28). By (29) we have,

$$|\mathcal{S}_{\tau+1}|\,(r + \delta - 1) - \left| \bigcup_{S \in \mathcal{S}_{\tau+1}} S \right|$$

$$\geqslant (2\tau + 1)(r + \delta - 1) - \left| S_{\tau+1,1} \cup \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right|$$

$$\geqslant \tau + 1. \qquad (31)$$

In total, the combination of (30) and (31) shows that the modified $\mathcal{S}_{\tau+1}$ satisfies P2.

We now return to the original $\mathcal{S}_{\tau+1} = \mathcal{S}_\tau \cup \{S_{\tau+1,1}, S_{\tau+1,2}\}$. If $S_{\tau+1,2}$ satisfies (25), then a similar argument shows we can build a modified $\mathcal{S}_{\tau+1}$ for which P2 holds.

As a final case, we consider the situation where both $S_{\tau+1,1}$ and $S_{\tau+1,2}$ satisfy (26). In that case, there exist $(\delta-1)$-subsets $S^*_{\tau+1,j} \subseteq S_{\tau+1,j}$ with $S^*_{\tau+1,j} \cap (\bigcup_{S \in \mathcal{S}_{\tau+1} \setminus \{S^*_{\tau+1,j}\}} S) = \emptyset$ and $\mathrm{rank}(S_{\tau+1,j}) = \mathrm{rank}(S_{\tau+1,j} \setminus S^*_{\tau+1,j})$, for $j = 1, 2$. Thus, we have

$$
\mathrm{rank}\left(\bigcup_{S \in \mathcal{S}_{\tau+1}} S \right)
$$

$$
= \mathrm{rank}\left((S_{\tau+1,1} \setminus S^*_{\tau+1,1}) \cup (S_{\tau+1,2} \setminus S^*_{\tau+1,2}) \right.
$$

$$
\left. \cup \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right)
$$

$$
\leqslant \left| ((S_{\tau+1,1} \setminus S^*_{\tau+1,1}) \cup (S_{\tau+1,2} \setminus S^*_{\tau+1,2})) \right.
$$

$$
\left. \setminus \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right| + \mathrm{rank}\left(\bigcup_{S \in \mathcal{S}_\tau} S \right)
$$

$$
\leqslant \left| (S_{\tau+1,1} \cup S_{\tau+1,2}) \setminus \left(\bigcup_{S \in \mathcal{S}_\tau} S \right) \right| - 2(\delta-1)
$$

$$
+ \mathrm{rank}\left(\bigcup_{S \in \mathcal{S}_\tau} S \right)
$$

$$
\leqslant \left| \bigcup_{S \in \mathcal{S}_{\tau+1}} S \right| - (2\tau+2)(\delta-1), \tag{32}
$$

where the last inequality holds by (23). Additionally, by (22), and since $i_{\tau+1} \in S_{\tau+1,1} \cap S_{\tau+1,2}$,

$$
2(\tau+1)(r+\delta-1) - \left| \bigcup_{S \in \mathcal{S}_{\tau+1}} S \right|
$$

$$
\geqslant 2\tau(r+\delta-1) - \left| \bigcup_{S \in \mathcal{S}_\tau} S \right| + 2(r+\delta-1)
$$

$$
- |S_{\tau+1,1} \cup S_{\tau+1,2}|
$$

$$
\geqslant \tau+1. \tag{33}
$$

By combining (32) and (33) we learn that $\mathcal{S}_{\tau+1}$ satisfies P2, and the auxiliary claim follows.

We turn to prove the main claim. The proof is divided into two cases depending on properties P1 and P2:

Case 1: P1 holds for some $\tau \leqslant \frac{u}{2}$. Let $\mathcal{S} \subseteq \Gamma$ be a 2τ-subset, $\mathcal{S}' \subseteq \mathcal{S}$, and $S' \in \mathcal{S}'$, such that (21) holds. By that equation, we can choose a subset $\mathcal{V} \subseteq \mathcal{S}' \setminus \{S'\}$ such that $\mathrm{rank}(\bigcup_{S \in \mathcal{V}} S) = \mathrm{rank}(\bigcup_{S \in \mathcal{S}'} S)$. Of all such subsets, let us choose $\mathcal{V}$ to be minimal, namely, $\mathrm{rank}(\bigcup_{S \in \mathcal{V}} S) > \mathrm{rank}(\bigcup_{S \in \mathcal{V} \setminus \{A\}} S)$ for any $A \in \mathcal{V}$. Thus, by Lemma 10 we

have

$$
\mathrm{rank}\left(\bigcup_{S \in \mathcal{V}} S \right) \leqslant \left| \bigcup_{S \in \mathcal{V}} S \right| - |\mathcal{V}|(\delta-1). \tag{34}
$$

Assume $\mathcal{V}$ contains ν repairs sets, $\mathcal{V} = \{S_1, S_2, \ldots, S_\nu\}$. Since each repair set in Γ has rank at most r, and the union of u repair sets has rank at most $ur \leqslant k-1$, we can extend $\mathcal{V}$ to a u-set $\mathcal{V}' \subseteq \Gamma$ such that $\mathcal{V}' = \mathcal{V} \cup \{S_{\nu+1}, S_{\nu+2}, \ldots, S_u\}$, such that each added repair set increases the overall rank, i.e.,

$$
\mathrm{rank}\left(\mathcal{V} \cup \{S_{\nu+1}, S_{\nu+2}, \ldots, S_{\nu+i}\} \right)
$$

$$
< \mathrm{rank}\left(\mathcal{V} \cup \{S_{\nu+1}, S_{\nu+2}, \ldots, S_{\nu+i+1}\} \right) \tag{35}
$$

for all $1 \leqslant i \leqslant u - \nu - 1$.

Let $S^*_{\nu+1}$ be a $(\delta-1)$-subset of $S_{\nu+1} \setminus (\bigcup_{S \in \mathcal{V}} S)$ and $\overline{S'} \triangleq S' \setminus (\bigcup_{S \in \mathcal{V}} S)$. In a similar fashion to the analysis above, we have

$$
\mathrm{rank}\left(\bigcup_{S \in \mathcal{V} \cup \{S_{\nu+1}\}} S \right)
$$

$$
= \mathrm{rank}\left((S_{\nu+1} \setminus S^*_{\nu+1}) \cup \left(\bigcup_{S \in \mathcal{V}} S \right) \right)
$$

$$
\leqslant \begin{cases} |(S_{\nu+1} \setminus S^*_{\nu+1}) \setminus (\bigcup_{S \in \mathcal{V}} S)| - 1 + \mathrm{rank}(\bigcup_{S \in \mathcal{V}} S), \\ \quad \text{if } \overline{S'} \cap S_{\nu+1} \neq \emptyset \\ |(S_{\nu+1} \setminus S^*_{\nu+1}) \setminus (\bigcup_{S \in \mathcal{V}} S)| + \mathrm{rank}(\bigcup_{S \in \mathcal{V}} S), \\ \quad \text{otherwise} \end{cases}
$$

$$
\leqslant \begin{cases} |S_{\nu+1} \setminus (\bigcup_{S \in \mathcal{V}} S)| - \delta + \mathrm{rank}(\bigcup_{S \in \mathcal{V}} S), \\ \quad \text{if } \overline{S'} \cap S_{\nu+1} \neq \emptyset \\ |S_{\nu+1} \setminus (\bigcup_{S \in \mathcal{V}} S)| - \delta + 1 + \mathrm{rank}(\bigcup_{S \in \mathcal{V}} S), \\ \quad \text{otherwise} \end{cases}
$$

$$
\leqslant \begin{cases} |S_{\nu+1} \setminus (\bigcup_{S \in \mathcal{V}} S)| - \delta + |\bigcup_{S \in \mathcal{V}} S| - |\mathcal{V}|(\delta-1), \\ \quad \text{if } \overline{S'} \cap S_{\nu+1} \neq \emptyset \\ |S_{\nu+1} \setminus (\bigcup_{S \in \mathcal{V}} S)| - \delta + 1 + |\bigcup_{S \in \mathcal{V}} S| - |\mathcal{V}|(\delta-1), \\ \quad \text{otherwise} \end{cases}
$$

$$
\leqslant \begin{cases} |\bigcup_{S \in \mathcal{V} \cup \{S_{\nu+1}\}} S| - (|\mathcal{V}|+1)(\delta-1) - 1, \\ \quad \text{if } \overline{S'} \cap S_{\nu+1} \neq \emptyset \\ |\bigcup_{S \in \mathcal{V} \cup \{S_{\nu+1}\}} S| - (|\mathcal{V}|+1)(\delta-1), \\ \quad \text{otherwise} \end{cases}
$$

where to prove the first inequality we use the fact that $S' \subseteq \mathrm{span}(\bigcup_{S \in \mathcal{V}} S)$. Repeating the processing, at each iteration adding $S_{\nu+2}, \ldots, S_u$, we can conclude that

$$
\mathrm{rank}\left(\bigcup_{S \in \mathcal{V}'} S \right)
$$

$$
\leqslant \begin{cases} |\bigcup_{S \in \mathcal{V}'} S| - u(\delta-1) - 1, \\ \quad \text{if } \overline{S'} \cap (\bigcup_{i=1}^{u-\nu-1} S_{\nu+i}) \neq \emptyset \\ |\bigcup_{S \in \mathcal{V}'} S| - u(\delta-1), \\ \quad \text{otherwise}, \end{cases} \tag{36}
$$

by (34) and (35).

Recall that the rank of the union of u repair sets, and in particular, $\mathcal{V}'$, satisfies $\mathrm{rank}(\bigcup_{S \in \mathcal{V}'} S) \leqslant ur \leqslant k-1$. Thus,

we have a set of coordinates $B \subseteq \mathbb{Z}_n$, with $\bigcup_{S \in \mathcal{V}'} S \subseteq B$ and $\operatorname{rank}(B) = k - 1$. Consider the set $\widetilde{B} \triangleq B \cup \overline{S'}$. By (36),

$$\left| \widetilde{B} \right| - \operatorname{rank}\left(\widetilde{B} \right)$$

$$= \left| \widetilde{B} \right| - \operatorname{rank}(B)$$

$$\geqslant \begin{cases} |B| - \operatorname{rank}(B), & \text{if } \overline{S'} \cap \left(\bigcup_{i=1}^{u-\nu-1} S_{\nu+i} \right) \neq \emptyset \\ |B| - \operatorname{rank}(B) + 1, & \text{otherwise} \end{cases}$$

$$\geqslant \begin{cases} |\bigcup_{S \in \mathcal{V}'} S| - \operatorname{rank}(\bigcup_{S \in \mathcal{V}'} S), \\ \qquad \text{if } \overline{S'} \cap \left(\bigcup_{i=1}^{u-\nu-1} S_{\nu+i} \right) \neq \emptyset \\ |\bigcup_{S \in \mathcal{V}'} S| - \operatorname{rank}(\bigcup_{S \in \mathcal{V}'} S) + 1, \\ \qquad \text{otherwise} \end{cases}$$

$$\geqslant u(\delta - 1) + 1,$$

i.e.,

$$\left| \widetilde{B} \right| \geqslant k + u(\delta - 1). \tag{37}$$

Recall now that for an $[n, k, d]_q$ code $\mathcal{C}$,

$$d = n - \max \left\{ |I| \ : \ I \subseteq \mathbb{Z}_n, \operatorname{rank}(\mathcal{C}_I) = k - 1 \right\}.$$

Thus, by (37), for our code

$$d \leqslant n - k - u(\delta - 1).$$

However, since our code is an optimal LRC,

$$d = n - k + 1 - u(\delta - 1),$$

and thus, a have reached a contradiction.

Case 2: P2 holds for all 2τ-subsets $\mathcal{S} \subseteq \Gamma$, where $\tau \leqslant u/2$. Assume first that u is odd. Denote $\tau = \frac{u-1}{2}$, and arbitrarily pick $\mathcal{S} \subseteq \Gamma$, with $|\mathcal{S}| = 2\tau = u - 1$. By (22) and (23),

$$k - 1 - \operatorname{rank}\left(\bigcup_{S \in \mathcal{S}} S \right) = ur + v - 1 - \operatorname{rank}\left(\bigcup_{S \in \mathcal{S}} S \right)$$

$$\geqslant r + v - 1 + \frac{u-1}{2}$$

$$\geqslant 2r,$$

where the last inequality holds by the condition $u \geqslant 2(r - v + 1)$, and the fact that u is odd. Thus, we can extend $\mathcal{S}$ to $\mathcal{V}' = \mathcal{S} \cup \{S_u, S_{u+1}\} \subseteq \Gamma$ with $|\mathcal{V}'| = u + 1$, such that

$$\operatorname{rank}\left(\bigcup_{S \in \mathcal{S}} S \right) < \operatorname{rank}\left(S_u \cup \left(\bigcup_{S \in \mathcal{S}} S \right) \right)$$

$$< \operatorname{rank}\left(\bigcup_{S \in \mathcal{V}'} S \right)$$

$$\leqslant k - 1,$$

and

$$\left| \bigcup_{S \in \mathcal{V}'} S \right| \geqslant \operatorname{rank}\left(\bigcup_{S \in \mathcal{V}'} S \right) + (u + 1)(\delta - 1).$$

The fact that $\operatorname{rank}(\bigcup_{S \in \mathcal{V}'} S) \leqslant k - 1$ means that we can find a set $B \subseteq \mathbb{Z}_n$ with $\bigcup_{S \in \mathcal{V}'} S \subseteq B$ and $\operatorname{rank}(B) = k - 1$. Then,

$$|B| - k + 1 = |B| - \operatorname{rank}(B)$$

$$\geqslant \left| \bigcup_{S \in \mathcal{V}'} S \right| - \operatorname{rank}\left(\bigcup_{S \in \mathcal{V}'} S \right)$$

$$\geqslant (u + 1)(\delta - 1).$$

As in Case 1, we obtain

$$d \leqslant n - k + 1 - (u + 1)(\delta - 1),$$

which contradicts the minimum distance of an optimal LRC being

$$d = n - k + 1 - u(\delta - 1).$$

Assume now that u is even. Denote $\tau = \frac{u}{2}$, and arbitrarily pick $\mathcal{S} \subseteq \Gamma$, with $|\mathcal{S}| = 2\tau = u$. By (22) and (23),

$$k - 1 - \operatorname{rank}\left(\bigcup_{S \in \mathcal{S}} S \right) = ur + v - 1 - \operatorname{rank}\left(\bigcup_{S \in \mathcal{S}} S \right)$$

$$\geqslant v - 1 + \frac{u}{2}$$

$$\geqslant r,$$

where the last inequality holds by the condition $u \geqslant 2(r - v + 1)$. Thus, we can extend $\mathcal{S}$ to $\mathcal{V}' = \mathcal{S} \cup \{S_{u+1}\} \subseteq \Gamma$ with $|\mathcal{V}'| = u + 1$, such that

$$\operatorname{rank}\left(\bigcup_{S \in \mathcal{S}} S \right) < \operatorname{rank}\left(\bigcup_{S \in \mathcal{V}'} S \right) \leqslant k - 1,$$

and

$$\left| \bigcup_{S \in \mathcal{V}'} S \right| \geqslant \operatorname{rank}\left(\bigcup_{S \in \mathcal{V}'} S \right) + (u + 1)(\delta - 1).$$

We now continue exactly as in the case of odd u to obtain a contradiction.

In all of the above cases, we have reached a contradiction. Hence, our assumption that there exist $\widehat{S} \in \Gamma$ and $\widehat{t} \in \mathbb{Z}$ such that $0 < |\widehat{S} \cap (\widehat{S} + \widehat{t})| < |\widehat{S}|$ is incorrect, and the main claim of the theorem follows. ∎

REFERENCES

[1] A. Agarwal, A. Barg, S. Hu, A. Mazumdar, and I. Tamo, "Combinatorial alphabet-dependent bounds for locally recoverable codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3481–3492, May 2018.

[2] A. Beemer, R. Coatney, V. Guruswami, H. H. López, and F. Piñero, "Explicit optimal-length locally repairable codes of distance 5," in *Proc. 56th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2018, pp. 800–804.

[3] M. Blaum, J. L. Hafner, and S. Hetzler, "Partial-MDS codes and their application to RAID type of architectures," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4510–4519, Jul. 2012.

[4] M. Blaum, J. S. Plank, M. Schwartz, and E. Yaakobi, "Construction of partial MDS and sector-disk codes with two global parity symbols," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2673–2681, May 2016.

[5] V. R. Cadambe and A. Mazumdar, "Bounds on the size of locally recoverable codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 5787–5794, Nov. 2015.

[6] H. Cai, M. Cheng, C. Fan, and X. Tang, "Optimal locally repairable systematic codes based on packings," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 39–49, Jan. 2019.

[7] H. Cai, C. Fan, Y. Miao, M. Schwartz, and X. Tang, "Optimal locally repairable codes: An improved bound and constructions," *IEEE Trans. Inf. Theory*, vol. 68, no. 8, pp. 5060–5074, Aug. 2022.

[8] H. Cai, Y. Miao, M. Schwartz, and X. Tang, "On optimal locally repairable codes with multiple disjoint repair sets," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 2402–2416, Apr. 2020.

[9] H. Cai, Y. Miao, M. Schwartz, and X. Tang, "On optimal locally repairable codes with super-linear length," *IEEE Trans. Inf. Theory*, vol. 66, no. 8, pp. 4853–4868, Aug. 2020.

[10] H. Cai, Y. Miao, M. Schwartz, and X. Tang, "A construction of maximally recoverable codes with order-optimal field size," *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 204–212, Jan. 2022.

[11] H. Cai and M. Schwartz, "On optimal locally repairable codes and generalized sector-disk codes," *IEEE Trans. Inf. Theory*, vol. 67, no. 2, pp. 686–704, Feb. 2021.

[12] B. Chen, W. Fang, S. Xia, and J. Hao, "Improved bounds and Singleton-optimal constructions of locally repairable codes with minimum distance 5 and 6," *IEEE Trans. Inf. Theory*, vol. 67, no. 1, pp. 217–231, Apr. 2021.

[13] B. Chen, S.-T. Xia, J. Hao, and F.-W. Fu, "Constructions of optimal cyclic (r, δ) locally repairable codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2499–2511, Oct. 2018.

[14] Z. Chen and A. Barg, "Cyclic LRC codes with hierarchy and availability," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 616–621.

[15] R. Gabrys, E. Yaakobi, M. Blaum, and P. H. Siegel, "Constructions of partial MDS codes over small fields," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3692–3701, Jun. 2019.

[16] P. Gopalan, C. Huang, B. Jenkins, and S. Yekhanin, "Explicit maximally recoverable codes with locality," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5245–5256, Sep. 2014.

[17] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, "On the locality of codeword symbols," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6925–6934, Nov. 2011.

[18] S. Gopi and V. Guruswami, "Improved maximally recoverable LRCs using skew polynomials," 2020, *arXiv:2012.07804*.

[19] S. Gopi, V. Guruswami, and S. Yekhanin, "Maximally recoverable LRCs: A field size lower bound and constructions for few heavy parities," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6066–6083, Oct. 2020.

[20] V. Guruswami, L. Jin, and C. Xing, "Constructions of maximally recoverable local reconstruction codes via function fields," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6133–6143, Oct. 2020.

[21] V. Guruswami, C. Xing, and C. Yuan, "How long can optimal locally repairable codes be?" *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3662–3670, Jun. 2019.

[22] J. Hao and S.-T. Xia, "Constructions of optimal binary locally repairable codes with multiple repair groups," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1060–1063, Jun. 2016.

[23] G. Hu and S. Yekhanin, "New constructions of SD and MR codes over small finite fields," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 1591–1595.

[24] C. Huang, M. Chen, and J. Li, "Pyramid codes: Flexible schemes to trade space for access efficiency in reliable data storage systems," *ACM Trans. Storage*, vol. 9, no. 1, pp. 1–28, 2013.

[25] L. Jin, "Explicit construction of optimal locally recoverable codes of distance 5 and 6 via binary constant weight codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 4658–4663, Aug. 2019.

[26] G. Kim and J. Lee, "Locally repairable codes with unequal local erasure correction," *IEEE Trans. Inf. Theory*, vol. 64, no. 11, pp. 7137–7152, Nov. 2018.

[27] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: Elsevier, 1977.

[28] U. Martínez-Peñas and F. R. Kschischang, "Universal and dynamic locally repairable codes with maximal recoverability via sum-rank codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 7790–7805, Dec. 2019.

[29] P. P. Pálfy, "Isomorphism problem for relational structures with a cyclic automorphism," *Eur. J. Combinatorics*, vol. 8, no. 1, pp. 35–43, Jan. 1987.

[30] J. S. Plank and M. Blaum, "Sector-disk (SD) erasure codes for mixed failure modes in RAID systems," *ACM Trans. Storage*, vol. 10, no. 1, pp. 1–17, Jan. 2014.

[31] N. Prakash, G. M. Kamath, V. Lalitha, and P. V. Kumar, "Optimal linear codes with a local-error-correction property," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 2776–2780.

[32] J. Qian and L. Zhang, "New optimal cyclic locally recoverable codes of length $n = 2(q + 1)$," *IEEE Trans. Inf. Theory*, vol. 66, no. 1, pp. 233–239, Jan. 2019.

[33] J. Qiu, D. Zheng, and F.-W. Fu, "New constructions of optimal cyclic (r, δ) locally repairable codes from their zeros," *IEEE Trans. Inf. Theory*, vol. 67, no. 3, pp. 1596–1608, Mar. 2021.

[34] A. S. Rawat, O. O. Koyluoglu, N. Silberstein, and S. Vishwanath, "Optimal locally repairable and secure codes for distributed storage systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 212–236, Nov. 2013.

[35] A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, "Locality and availability in distributed storage," *IEEE Trans. Inf. Theory*, vol. 62, no. 8, pp. 4481–4493, Aug. 2016.

[36] B. Sasidharan, G. K. Agarwal, and P. V. Kumar, "Codes with hierarchical locality," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 1257–1261.

[37] W. Song, S. H. Dau, C. Yuen, and T. J. Li, "Optimal locally repairable linear codes," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 5, pp. 1019–1036, May 2014.

[38] 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.

[39] I. Tamo, A. Barg, S. Goparaju, and R. Calderbank, "Cyclic LRC codes, binary LRC codes, and upper bounds on the distance of cyclic codes," *Int. J. Inf. Coding Theory*, vol. 3, no. 4, pp. 345–364, 2016.

[40] A. Wang and Z. Zhang, "Repair locality with multiple erasure tolerance," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6979–6987, Nov. 2014.

[41] A. Wang and Z. Zhang, "An integer programming-based bound for locally repairable codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5280–5294, Oct. 2015.

[42] T. Westerbäck, R. Freij-Hollanti, T. Ernvall, and C. Hollanti, "On the combinatorics of locally repairable codes via matroid theory," *IEEE Trans. Inf. Theory*, vol. 62, no. 10, pp. 5296–5315, Oct. 2016.

[43] C. Xing and C. Yuan, "Construction of optimal locally recoverable codes and connection with hypergraph," in *Proc. 46th Int. Colloq. Automata, Lang., Program. (ICALP)*. Wadern, Germany: Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019, pp. 1–14.

[44] A. Zeh and E. Yaakobi, "Bounds and constructions of codes with multiple localities," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 640–644.

Han Cai (Member, IEEE) received the B.S. and M.S. degrees in mathematics from Hubei University, Wuhan, China, in 2009 and 2013, respectively, and the Ph.D. degree from the Department of Communication Engineering, Southwest Jiaotong University, Chengdu, China, in 2017. From October 2015 to October 2017, he was a Visiting Ph.D. student at the Faculty of Engineering, Information and Systems, University of Tsukuba, Japan. From 2018 to 2021, he was a Post-Doctoral Fellow at the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Israel. In 2021, he joined Southwest Jiaotong University, where he currently hold a tenure-track position. His research interests include coding theory and sequence design.

Moshe Schwartz (Senior Member, IEEE) received the B.A. (summa cum laude), M.Sc., and Ph.D. degrees from the Computer Science Department, Technion—Israel Institute of Technology, Haifa, Israel, in 1997, 1998, and 2004, respectively.

He was a Fulbright Post-Doctoral Researcher at the Department of Electrical and Computer Engineering, University of California San Diego, and a Post-Doctoral Researcher at the Department of Electrical Engineering, California Institute of Technology. While on sabbatical 2012–2014, he was a Visiting Scientist at the Massachusetts Institute of Technology (MIT). He is currently a Professor with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev. His research interests include algebraic coding, combinatorial structures, and digital sequences.

Prof. Schwartz has been an Editorial Board Member for the *Journal of Combinatorial Theory, Series A*, since 2021. He received the 2009 IEEE Communications Society Best Paper Award in Signal Processing and Coding for Data Storage and the 2020 NVMW Persistent Impact Prize. He served as an Associate Editor for Coding Techniques and Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 2014 to 2021. Since 2021, he has been serving as an Area Editor for Coding and Decoding for the IEEE TRANSACTIONS ON INFORMATION THEORY.