A Construction of Maximally Recoverable Codes With Order-Optimal Field Size

Han Cai, *Member, IEEE*, Ying Miao, Moshe Schwartz, *Senior Member, IEEE*, and Xiaohu Tang, *Senior Member, IEEE*

***Abstract*— We construct maximally recoverable codes (corresponding to partial MDS codes) which are based on linearized Reed-Solomon codes. The new codes have a smaller field size requirement compared with known constructions. For certain asymptotic regimes, the constructed codes have order-optimal alphabet size, asymptotically matching the known lower bound.**

***Index Terms*— Distributed storage, linearized Reed-Solomon codes, locally repairable codes, maximally recoverable codes, partial MDS codes, sum-rank metric.**

I. Introduction

DISTRIBUTED storage systems use erasure codes to recover from node failures. Compared with the naive replication solution, erasure-correcting codes, such as the maximum distance separable (MDS) codes, can provide similar protection ability but with a far smaller redundancy. However, as the scale of system grows, new challenges arise for MDS codes, such as repair bandwidth [40] and repair complexity [29], due to the large number of nodes that need to be contacted during the recovery process - even for a single erased node.

One of the approaches that have been suggested to overcome those issues is locally repairable codes (LRCs) [15]. In such a code, k information symbols are encoded into n code symbols, which are arranged in repair sets (perhaps overlapping) of size $r+\delta-1$. Each repair set is capable of recovering from $\delta-1$ erasures by using the contents of the r non-erased code symbols. Those codes are called LRCs with (r,δ)-locality. Compared with MDS codes, even to recover just one erasure, LRCs may dramatically reduce the required repair bandwidth and repair complexity, since for MDS codes we always need to contact k code symbols, whereas in LRCs we only contact $r \ll k$ code symbols. For instances, in Microsoft Azure, an LRC with $n=16$, $k=12$, $r=6$, and $\delta=2$, is used to reduce the repair bandwidth [24].

The original definition of LRCs with $(r,\delta=2)$-locality was introduced in [15]. Several generalizations have followed later. The definition of LRCs was expanded to (r,δ)-locality with $\delta>2$ in [36], to allow repair sets to recover from more than one erasure. The concept of availability was studied in [6], [38], [44] to allow simultaneous recovery of a given code symbol from multiple repair sets. To allow different requirements for local recovery, hierarchical and unequal locality were introduced in [39] and [26], [47], respectively. Over the past decade, many bounds and constructions for LRCs have been introduced, e.g., [4], [7], [8], [10], [19], [23], [28], [33], [37], [42], [45], [46] for (r,δ)-locality [5], [6], [25], [38], [43] for multiple repair sets, [11], [30], [39], [48] for hierarchical locality, and [26], [47] for unequal locality.

As is usually the case, locality comes at a cost of reduced code rate and minimum Hamming distance. It was shown in [15] that, except for trivial cases, the minimum Hamming distance of LRCs cannot attain the well known Singleton bound [41]. To make the most out of this restriction, one natural problem is whether LRCs can recover from some predetermined erasure patterns beyond those guaranteed by their minimum Hamming distance. A subclass of LRCs named *maximally recoverable* (MR) codes [15] offer a positive answer to this question, by correcting the maximal possible set of erasure patterns beyond the minimum Hamming distance. *Partial MDS* (PMDS) codes [1], that form a subclass of MR codes, improve the storage efficiency of RAID systems, where h extra erasures may be recovered in addition to $\delta-1$ erasures in each repair set.

Motivated by their efficiency and applicability, $[n,k,d]_q$ MR codes with (r,δ)-locality, and h global parity-check symbols, have received much attention over the recent few years, where $[n,k,d]_q$ denotes a linear code with length n, dimension k, and minimum Hamming distance d, over a field of size q. For $[n,k,d]_q$ MR codes with (r,δ)-locality, of particular interest have been the asymptotic regime in which h and δ are constants, and the goal to construct codes with the smallest possible field size q. For the case of $h=1$, MR codes were constructed over a finite field of size $q=\Theta(r+\delta-1)$ [1] and a characterization was given in [21]. When $h=2$, MR codes

Manuscript received November 27, 2020; revised June 30, 2021; accepted September 23, 2021. Date of publication October 14, 2021; date of current version December 23, 2021. This work was supported in part by the German Israeli Project Cooperation (DIP) under Grant PE2398/1-1, in part by the Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (B) under Grant 18H01133, and in part by the National Natural Science Foundation of China under Grant 61871331. *(Corresponding author: Han Cai.)*

Han Cai and Xiaohu Tang are with the School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China (e-mail: hancai@aliyun.com; xhutang@swjtu.edu.cn).

Ying Miao is with the Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba 305-8573, Japan (e-mail: miao@sk.tsukuba.ac.jp).

Moshe Schwartz is with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer Sheva 8410501, Israel (e-mail: schwartz@ee.bgu.ac.il).

Communicated by C. Hollanti, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2021.3120016

TABLE I

KNOWN (n, r, h, δ, q)-MR CODES (PMDS CODES) IN THE ASYMPTOTIC REGIME WHERE h AND δ ARE CONSTANT, AND WHERE $m \triangleq \frac{n}{r+\delta-1}$

r	δ	h	Size of Alphabet (q)	Cases with order optimal field size	Restrictions	Ref.
any	any	1	$\Theta(r+\delta-1)$	all possible cases		[1, Thm. 5.4]
any	any	2	$\Theta(n\delta)$	all possible cases		[2, Thm. 7]
			$\Theta(n)$	all possible cases	q is odd	[17, Thm. IV.4]
			$n \cdot \exp(O(\sqrt{\log n}))$	None	q is even	[17, Thm. IV.4]
			$\Theta(n)$	all possible cases	q is even, $n = \Theta(m^2)$	Construction A
any	any	3	$\Theta(n^{3/2})$	None	r is a constant, q is even	[14, Cor. 23]
			$\Theta(n^3)$		q is odd	[17, Thm. V.4]
			$n^3 \cdot \exp(O(\sqrt{\log n}))$		q is even	[17, Thm. V.4]
			$\Theta(n^3)$			Construction A
2	any	any	$O(n^{h-1})$	$h = 2$	$m \geqslant h$	[3, Cor. 7.14]
any	2	any	$\Theta(k^{\lceil (h-1)(1-1/2^r) \rceil})$	$h = 3$, $m \geqslant 3$ is a constant		[14, Cor. 18]
any	any	any	$\Theta((r+\delta-1)^{nr/(r+\delta-1)})$	None		[9, Cor. 11]
any	any	any	$\Theta((r+\delta-1)n^{h\delta-1})$	None	$q_1 = r+\delta-1$, $2n = q_1^t$	[12, Lem. 7]
any	any	any	$\Theta(\max\{m, (r+\delta-1)^{h+\delta-1}\}^h)$	None	$q_1 = r+\delta-1$, $m+1 = q_1^t$	[12, Cor. 10]
any	any	any	$\Theta(\max\{m, (2(r+\delta-1))^{h+\delta-1}\}^{\min(m,h)})$	None		[18, Thm. 17]
any	any	any	$\Theta(\max\{m, (2(r+\delta-1))^{r+\delta-1}\}^{\min(m,h)})$	None		[18, Thm. 19]
any	any	any	$\Theta(\max\{r+\delta-1, m\}^r)$	None		[32, Cor. 8]
any	any	any	$\Theta(\max\{r+\delta-1, m\}^h)$	$h \leqslant \min\{m, \delta+1\}$, $n = \Theta(m^2)$		Construction A

were constructed in [2] with $q = \Theta(n(\delta-1))$, and later, with $q = \Theta(n)$ [17] (see [22] for $n = 2(r+\delta-1)$). For $h = 3$, MR codes were constructed with $q = \Theta(n^{3/2})$ for a constant $r+\delta-1$, and $q = \Theta(n^3)$ for an odd q [17]. For the case of $\delta = 2$, constructions for MR codes were provided for finite fields with size $q = \Theta(k^{h-1})$ [14]. For the case $r = 2$, the existence of MR codes was proved in [3] using a field of size $q = \Theta(n^{h-1})$. For general δ and h, a construction of MR codes with flexible parameters was introduced based on Gabidulin codes [9], which requires a field with size $q = \Theta((r+\delta-1)^{nr/(r+\delta-1)})$. Additionally, MR codes were constructed over finite fields with size $q = \Theta((r+\delta-1)n^{h\delta-1})$ and $q = \Theta(\max(\frac{n}{r+\delta-1}, (r+\delta-1)^{h+\delta-1})^h)$ [12]. In [18], MR codes were constructed with $q = \Theta(\max(\frac{n}{r+\delta-1}, (2r)^{h+\delta-1})^{\min(\frac{n}{r+\delta-1}, h)})$ and $q = \Theta(\max(\frac{n}{r+\delta-1}, (2r)^{r+\delta-1})^{\min(\frac{n}{r+\delta-1}, h)})$, respectively. Recently, based on linearized Reed-Solomon codes, MR codes were constructed with $q = \Theta(\max(r+\delta-1, \frac{n}{r+\delta-1})^r)$ [32], which is independent of the number of global parity-check symbols h, thus outperforming other known constructions when h is relatively large, namely, $h \geqslant r$. In [20], the authors construct MR codes with optimal repairing bandwidth inside repair sets. The parameters of MR codes from the known constructions, as well as a new one of this paper, are listed in Table I.

However, there is still an asymptotic gap between the known lower bounds on the minimum field size of MR codes [17] and the known constructions. The main contribution of this paper is a new construction of MR codes over small finite fields when h is relatively small, namely, $h < r$. Our construction is inspired by the construction in [32], and we also use linearized Reed-Solomon codes, yielding MR codes with field size $\Theta(\max\{r+\delta-1, \frac{n}{r+\delta-1}\}^h)$. Compared with the known constructions in [9], [12], [18], [32], our construction generates MR codes with a smaller field size. In particular, our MR codes have order-optimal field size, asymptotically matching the lower bound in [17] when $r+\delta-1 = \Theta(\sqrt{n})$ and $h \leqslant \min\{\frac{n}{r+\delta-1}, \delta+1\}$. Our construction also answers an open problem from [17], by providing MR codes over a field with even (or odd) characteristic. We would like to comment that shortly after we published our results, we learned that [16] have independently obtained a similar construction.

The remainder of this paper is organized as follows. Section II introduces basic notation and definitions of LRCs and MR codes, known bounds, as well as required facts on linearized Reed-Solomon codes. Section III presents our construction of MR codes. Section IV concludes this paper by summarizing and comparing our codes with the known codes, and discussing important cases.

II. PRELIMINARIES

Let us introduce the notation, definitions, and known results used throughout this paper. For a positive integer n, we denote $[n] \triangleq \{1, 2, \cdots, n\}$. If q is a prime power, let $\mathbb{F}_q$ denote the finite field with q elements.

An $[n, k]_q$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with a $k \times n$ generator matrix $G = (\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_n)$, where $\mathbf{g}_i$ is a column vector of length k for all $i \in [n]$. Specifically, $\mathcal{C}$ is called an $[n, k, d]_q$ linear code if the minimum Hamming distance of $\mathcal{C}$ is d. For an $m \times n$ matrix $A = (A_1, A_2, \ldots, A_n) \in \mathbb{F}_q^{m \times n}$ and $I \subseteq [n]$, let $A|_I$ denote the projection of A upon columns specified by I, i.e., $A|_I = (A_i)_{i \in I}$. For any codeword $C = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$, we say that c_i, $i \in [n]$, is the ith code symbol.

Definition 1 ([15], [36]): The ith code symbol of an $[n,k,d]_q$ linear code $\mathcal{C}$ is said to have (r,δ)-*locality* if there exists a subset $S_i \subseteq [n]$ (an (r,δ)-*repair set*) such that

- $i \in S_i$ and $|S_i| \leqslant r+\delta-1$; and
- The minimum Hamming distance of the punctured code $\mathcal{C}|_{S_i}$ obtained by deleting the code symbols c_j ($j \in [n] \setminus S_i$) is at least δ.

Furthermore, an $[n,k,d]_q$ linear code $\mathcal{C}$ is said to have information (r,δ)-locality (denoted as $(r,\delta)_i$-locality) if there exists a k-subset $I \subseteq [n]$ with $\mathrm{rank}(G|_I) = k$ such that for each $i \in I$, the ith code symbol has (r,δ)-locality, and all symbol (r,δ)-locality (denoted as $(r,\delta)_a$-locality) if all the n code symbols have (r,δ)-locality.

An upper bound on the minimum Hamming distance of linear codes with $(r,\delta)_i$-locality was derived as follows (for $\delta = 2$ in [15], and for general δ in [36]):

Lemma 1 ([15], [36]): For an $[n,k,d]_q$ code $\mathcal{C}$ with $(r,\delta)_i$-locality,

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

A linear code with information $(r,\delta)_i$-locality (or $(r,\delta)_a$-locality) is said to be optimal if its minimum Hamming distance achieves the bound in (1).

Definition 2: Let $\mathcal{C}$ be an $[n,k,d]_q$ code with $(r,\delta)_a$-locality, and define $\mathcal{S} \triangleq \{S_i \;:\; i \in [n]\}$, where S_i is an (r,δ)-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 $\mathcal{C}|_{\cup_{1\leqslant i\leqslant n} R_i}$ is an MDS code.

Of particular interest are MR codes for which $\mathcal{S}$ is a partition of $[n]$ with equal-size parts.

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 $|S_i| = r+\delta-1$, then $r+\delta-1|n$. 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 note that in general, MR codes need not have repair sets of equal size, nor do the repair sets have to form a partition of $[n]$. In this paper we choose to follow the more restrictive definition from [14], [15].

We also note that it is easy to verify that (n,r,h,δ,q)-MR codes are optimal $[n,k,d]_q$ LRCs with $(r,\delta)_a$-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 viewed in this way, (n,r,h,δ,q)-MR codes match the definition of partial MDS (PMDS) codes, as defined in [1], where in a codeword, each entry of the array corresponds to a sector, and each column of the array corresponds to a disk.

For the sake of completeness, we would like to mention that aside from PMDS codes, there are other codes with locality that can recover from predetermined erasure patterns beyond the minimum Hamming distances [8], [13], [27], [35]. As an example, sector-disk (SD) codes [35] with $(r,\delta)_a$-locality can correct $\delta-1$ disk erasures together with any additional h sector erasures, where h denotes the number of global parity-check symbols.

One interesting problem arising from the definition of MR codes is to determine the minimum alphabet size for fixed n, r, h, and δ. For the case $h = 1$, it is easy to check that an $(n,r,1,\delta,q)$-MR code is an optimal LRC with $(r,\delta)_a$-locality and $d = \delta+1$, where $(r+\delta-1)|n$ and $k = \frac{rn}{r+\delta-1} - 1$. For this case, the field size requirement may be as small as $q = \Theta(r+\delta-1)$, which is asymptotically optimal for the simple reason that the punctured code over any repair set together with the only global parity check is an $[r+\delta, r, \delta+1]_q$ MDS code when $(r+\delta-1)|n$. For the case $h \geqslant 2$, in [17], the following asymptotic lower bounds on the field size are derived. We emphasize that here, and throughout the paper, we assume h and δ are constants.

Lemma 2 ([17, Theorem I.1]): Let $h \geqslant 2$ and $\mathcal{C}$ be an (n,r,h,δ,q)-MR code. 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 h and δ are regarded as constants. The above lower bound may be simplified as

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 $\delta-1 > h - \frac{2h}{m}$:
$$q = \Omega\left(n^{m-1}\right).$$

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

A. The Sum-Rank Metric and Linearized Reed-Solomon Codes

We turn to introduce some necessary definitions for linearized Reed-Solomon codes, which form the main tool used in this paper. We first recall the definition of the sum-rank metric as defined in [34] and [31].

Definition 5 ([31]): Let $\mathbb{F}_q$ be a subfield of $\mathbb{F}_{q_1}$ and N, L_i for $1 \leqslant i \leqslant g$, be positive integers with $N = \sum_{i=1}^{g} L_i$. Let $\boldsymbol{C} = (\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_g) \in \mathbb{F}_{q_1}^N$, where $\boldsymbol{C}_i \in \mathbb{F}_{q_1}^{L_i}$ for $1 \leqslant i \leqslant g$. The *sum-rank weight* in $\mathbb{F}_{q_1}^N$, with length partition $(L_1, L_2, \ldots, L_g)$, is defined as

$$\mathrm{wt}_{\mathrm{SR}}(\boldsymbol{C}) = \sum_{i=1}^{g} \mathrm{rank}_q(\boldsymbol{C}_i),$$

where $\mathrm{rank}_q(\boldsymbol{C}_i)$ denotes the rank of $\boldsymbol{C}_i \in \mathbb{F}_{q_1}^{L_i}$ over $\mathbb{F}_q$. Furthermore, for $\boldsymbol{C}, \boldsymbol{C}' \in \mathbb{F}_{q_1}^N$, define the *sum-rank distance* as

$$d_{\mathrm{SR}}(\boldsymbol{C}, \boldsymbol{C}') = \mathrm{wt}_{\mathrm{SR}}(\boldsymbol{C} - \boldsymbol{C}').$$

For a code $\mathcal{C} \subseteq \mathbb{F}_{q_1}^N$, with length partition $(L_1, L_2, \ldots, L_g)$ as before, we define the minimum sum-rank distance by

$$d_{\mathrm{SR}}(\mathcal{C}) = \min\left\{d_{\mathrm{SR}}(\boldsymbol{C}, \boldsymbol{C}') \;:\; \boldsymbol{C}, \boldsymbol{C}' \in \mathcal{C}, \boldsymbol{C} \neq \boldsymbol{C}'\right\}.$$

In an analogy with the Hamming metric, there is also a Singleton bound for the sum-rank metric codes.

Lemma 3 ([31]): Let $q_1 = q^m$ and $\mathcal{C} \subseteq \mathbb{F}_{q_1}^N$. Then we have

$$|\mathcal{C}| \leqslant q^{m(N - d_{\mathrm{SR}}(\mathcal{C}) + 1)}.$$

Similar to MDS codes, codes that attain the above Singleton bound with equality are called *maximum sum-rank distance (MSRD) codes* [31].

This general definition of the sum-rank metric includes the Hamming metric as a special case when the length partition is $g = N$ and $L_1 = L_2 = \cdots = L_n = 1$. It also includes the rank metric as a special case when the length partition is $g = 1$ and $L_1 = N$. In what follows, we introduce one class of MSRD codes called *linearized Reed-Solomon codes* [31].

Let $\mathbb{F}_q \subseteq \mathbb{F}_{q_1}$ and define $\sigma : \mathbb{F}_{q_1} \to \mathbb{F}_{q_1}$ as

$$\sigma(\alpha) \triangleq \alpha^q.$$

For any $\alpha \in \mathbb{F}_{q_1}$ and $i \in \mathbb{N}$, define

$$\mathrm{Norm}_i(\alpha) \triangleq \sigma^{i-1}(\alpha) \cdots \sigma(\alpha)\alpha.$$

The $\mathbb{F}_q$-linear operator $\mathcal{D}_\alpha^i : \mathbb{F}_{q_1} \to \mathbb{F}_{q_1}$ is defined by

$$\mathcal{D}_\alpha^i(\beta) \triangleq \sigma^i(\beta)\,\mathrm{Norm}_i(\alpha).$$

Let $\alpha \in \mathbb{F}_{q_1}$, and let $\mathcal{B} = (\beta_1, \beta_2, \cdots, \beta_L) \in \mathbb{F}_{q_1}^L$. For $i \in \mathbb{N} \cup \{0\}$ and $k, \ell \in \mathbb{N}$, where $\ell \leqslant L$, define the matrices

$$D(\alpha^i, \mathcal{B}, k, \ell) \triangleq \begin{pmatrix} \beta_1 & \beta_2 & \cdots & \beta_\ell \\ \mathcal{D}_{\alpha^i}^1(\beta_1) & \mathcal{D}_{\alpha^i}^1(\beta_2) & \cdots & \mathcal{D}_{\alpha^i}^1(\beta_\ell) \\ \vdots & \vdots & & \vdots \\ \mathcal{D}_{\alpha^i}^{k-1}(\beta_1) & \mathcal{D}_{\alpha^i}^{k-1}(\beta_2) & \cdots & \mathcal{D}_{\alpha^i}^{k-1}(\beta_\ell) \end{pmatrix} \in \mathbb{F}_{q_1}^{k \times \ell}. \quad (2)$$

The matrix defined by (2) satisfies the following column linearity:

Proposition 1: With the setting as in (2), for any $A \in \mathbb{F}_q^{\ell \times \ell_1}$ we have

$$D(\alpha^i, \mathcal{B}, k, \ell)A = D(\alpha^i, \mathcal{B}|_{[\ell]}A, k, \ell_1).$$

Proof: Write $\mathcal{B}|_{[\ell]}A = (\beta_1', \beta_2', \ldots, \beta_{\ell_1}')$. Then, by (2),

$$\begin{aligned} &D(\alpha^i, \mathcal{B}, k, \ell)A \\ &= \begin{pmatrix} \beta_1 & \beta_2 & \cdots & \beta_\ell \\ \mathcal{D}_{\alpha^i}^1(\beta_1) & \mathcal{D}_{\alpha^i}^1(\beta_2) & \cdots & \mathcal{D}_{\alpha^i}^1(\beta_\ell) \\ \vdots & \vdots & & \vdots \\ \mathcal{D}_{\alpha^i}^{k-1}(\beta_1) & \mathcal{D}_{\alpha^i}^{k-1}(\beta_2) & \cdots & \mathcal{D}_{\alpha^i}^{k-1}(\beta_\ell) \end{pmatrix} A \\ &= \begin{pmatrix} \beta_1' & \beta_2' & \cdots & \beta_{\ell_1}' \\ \mathcal{D}_{\alpha^i}^1(\beta_1') & \mathcal{D}_{\alpha^i}^1(\beta_2') & \cdots & \mathcal{D}_{\alpha^i}^1(\beta_{\ell_1}') \\ \vdots & \vdots & & \vdots \\ \mathcal{D}_{\alpha^i}^{k-1}(\beta_1') & \mathcal{D}_{\alpha^i}^{k-1}(\beta_2') & \cdots & \mathcal{D}_{\alpha^i}^{k-1}(\beta_{\ell_1}') \end{pmatrix} \\ &= D(\alpha^i, \mathcal{B}|_{[\ell]}A, k, \ell_1). \end{aligned}$$

■

Definition 6 ([31]): For positive integers N, M, L, and g, let $N = L_1 + L_2 + \cdots + L_g$, $g \leqslant q-1$, and $1 \leqslant L_i \leqslant L \leqslant M$. Set $\mathbb{F}_{q_1} = \mathbb{F}_{q^M}$. Let $\mathcal{B}$ be a sequence of elements that are linearly independent over $\mathbb{F}_q$. Then the *linearized Reed-Solomon code* with dimension k, primitive element $\gamma \in \mathbb{F}_{q^M}$, and basis $\mathcal{B}$, is the linear code $\mathcal{C}_{L,k}^\sigma(\mathcal{B}, \gamma) \subseteq \mathbb{F}_{q^M}^N$ with generator matrix

$$\begin{aligned} D = \big(&D(\gamma^0, \mathcal{B}, k, L_1), D(\gamma^1, \mathcal{B}, k, L_2), \\ &\cdots, D(\gamma^{g-1}, \mathcal{B}, k, L_g)\big)_{k \times N}. \end{aligned}$$

We comment that Definition 6 is a *narrow-sense* linearized Reed-Solomon code, which suffices for this paper. For a more general definition of linearized Reed-Solomon code the reader is referred to [31]. We also point out that linearized Reed-Solomon codes are MSRD codes [31]. For more details on sum-rank metric codes and their applications to LRCs, the reader may refer to [32].

Let $\mathrm{diag}(W_1, W_2, \cdots, W_g)$ denote the block-diagonal matrix, whose main-diagonal blocks are $W_1, W_2, \cdots, W_g$, i.e.,

$$\mathrm{diag}(W_1, W_2, \cdots, W_g) = \begin{pmatrix} W_1 & 0 & \cdots & 0 \\ 0 & W_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & W_g \end{pmatrix}.$$

Since linearized Reed-Solomon codes are MSRD codes, the dimension k of the code $\mathcal{C}$ is $k = N - d_{\mathrm{SR}}(\mathcal{C}) + 1$. When it comes to correcting erasures, if the non-erased part has sum-rank weight at least k, the code can correctly recover the codeword. This is more formally described in the following lemma from [32].

Lemma 4 ([32]): Let $g \leqslant q - 1$, and let $\mathcal{C}_{L,k}^\sigma(\mathcal{B}, \gamma)$ be the $[N, k, N-k+1]_{q^M}$ linearized Reed-Solomon code from Definition 6, with $N = L_1 + L_2 + \cdots + L_g$, and $1 \leqslant L_i \leqslant L \leqslant M$. Then for all integers $n_i \geqslant 1$, and all matrices $W_i \in \mathbb{F}_q^{L_i \times n_i}$, $i \in [g]$, satisfying

$$\sum_{i=1}^{g} \mathrm{rank}(W_i) \geqslant k,$$

there exists a decoder

$$\mathrm{Dec} : \mathcal{C}_{L,k}^\sigma(\mathcal{B}, \gamma)\,\mathrm{diag}(W_1, W_2, \cdots, W_g) \to \mathcal{C}_{L,k}^\sigma(\mathcal{B}, \gamma)$$

such that

$$\mathrm{Dec}(C\,\mathrm{diag}(W_1, W_2, \cdots, W_g)) = C \quad \text{for any } C \in \mathcal{C}_{L,k}^\sigma(\mathcal{B}, \gamma),$$

where

$$\begin{aligned} &\mathcal{C}_{L,k}^\sigma(\mathcal{B}, \gamma)\,\mathrm{diag}(W_1, W_2, \cdots, W_g) \\ &\triangleq \{C\,\mathrm{diag}(W_1, W_2, \cdots, W_g) \;:\; C \in \mathcal{C}_{L,k}^\sigma(\mathcal{B}, \gamma)\}. \end{aligned}$$

Furthermore, when we analyze the case in which the non-erased part has sum rank less than k, we arrive at the following property of generator matrices for linearized Reed-Solomon codes, which is a direct application of the previous lemma.

Theorem 1: Let $g \leqslant q - 1$, and D be generator matrix of a linearized Reed-Solomon code from Definition 6 with $N = L_1 + L_2 + \cdots + L_g$, and $1 \leqslant L_i \leqslant L \leqslant M$. For all integers $n_i \geqslant 1$ and all matrices $W_i \in \mathbb{F}_q^{L_i \times n_i}$, for $i \in [g]$, satisfying

$$\sum_{i=1}^{g} \operatorname{rank}(W_i) \geqslant k,$$

we have

$$\begin{aligned}
&\operatorname{rank}(D \operatorname{diag}(W_1, W_2, \ldots, W_g)) \\
=&\operatorname{rank}((D(\gamma^0, \mathcal{B}, k, L_1)W_1, D(\gamma^1, \mathcal{B}, k, L_2)W_2, \\
&\quad \cdots, D(\gamma^{g-1}, \mathcal{B}, k, L_g)W_g)) \\
=&k.
\end{aligned}$$

For the case

$$\sum_{i=1}^{g} \operatorname{rank}(W_i) < k,$$

we have

$$\begin{aligned}
&\operatorname{rank}(D \operatorname{diag}(W_1, W_2, \ldots, W_g)) \\
=&\operatorname{rank}((D(\gamma^0, \mathcal{B}, k, L_1)W_1, D(\gamma^1, \mathcal{B}, k, L_2)W_2, \\
&\quad \cdots, D(\gamma^{g-1}, \mathcal{B}, k, L_g)W_g)) \\
=&\sum_{i=1}^{g} \operatorname{rank}(W_i).
\end{aligned}$$

Proof: The first claim is exactly Lemma 4. For the second one, we assume to the contrary that there exist $W_i \in \mathbb{F}_q^{L_i \times n_i}$, for all $i \in [g]$, with

$$\sum_{i=1}^{g} \operatorname{rank}(W_i) < k,$$

and

$$\operatorname{rank}(D \operatorname{diag}(W_1, W_2, \ldots, W_g)) < \sum_{i=1}^{g} \operatorname{rank}(W_i), \tag{3}$$

where we apply a fact that $\operatorname{rank}(D \operatorname{diag}(W_1, W_2, \ldots, W_g)) \leqslant \operatorname{rank}(\operatorname{diag}(W_1, W_2, \ldots, W_g)) = \sum_{i=1}^{g} \operatorname{rank}(W_i)$. Note that there exist $W_i' \in \mathbb{F}_q^{L_i \times n_i'}$ for all $i \in [g]$, such that $\operatorname{rank}(W_i') = n_i'$,

$$\sum_{i=1}^{g} \operatorname{rank}(W_i') = k - \sum_{i=1}^{g} \operatorname{rank}(W_i),$$

and

$$\sum_{i=1}^{g} \operatorname{rank}(W_i, W_i') = k.$$

By the first claim,

$$\operatorname{rank}(D \operatorname{diag}((W_1, W_1'), (W_2, W_2'), \ldots, (W_g, W_g'))) = k.$$

But now, combining this with (3), we get

$$\begin{aligned}
&\operatorname{rank}(D \operatorname{diag}(W_1', W_2', \ldots, W_g')) \\
>&\sum_{i=1}^{g} n_i' = \operatorname{rank}(\operatorname{diag}(W_1', W_2', \ldots, W_g')),
\end{aligned}$$

which is a contradiction. Thus, the desired result follows. ■

III. Code Construction

In this section, we describe a construction for (n, r, h, δ, q)-MR codes. The main idea of our construction is to use generator matrices of linearized Reed-Solomon codes for global parity-check symbols of MR codes.

Throughout this section, we use the $(\delta - 1) \times (r + \delta - 1)$ matrix

$$P_1 \triangleq \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{r+\delta-1} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{\delta-2} & \alpha_2^{\delta-2} & \cdots & \alpha_{r+\delta-1}^{\delta-2} \end{pmatrix} \in \mathbb{F}_q^{(\delta-1)\times(r+\delta-1)}, \tag{4}$$

and the $h \times (r + \delta - 1)$ matrix

$$P_2 \triangleq \begin{pmatrix} \alpha_1^{\delta-1} & \alpha_2^{\delta-1} & \cdots & \alpha_{r+\delta-1}^{\delta-1} \\ \alpha_1^{\delta} & \alpha_2^{\delta} & \cdots & \alpha_{r+\delta-1}^{\delta} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{\delta+h-2} & \alpha_2^{\delta+h-2} & \cdots & \alpha_{r+\delta-1}^{\delta+h-2} \end{pmatrix} \in \mathbb{F}_q^{h\times(r+\delta-1)}, \tag{5}$$

where $\alpha_i \in \mathbb{F}_q \setminus \{0\}$, and $\alpha_i \neq \alpha_j$ for $i \neq j$. Let $\gamma_1, \gamma_2, \ldots, \gamma_h \in \mathbb{F}_{q^h}$ form a basis of $\mathbb{F}_{q^h}$ over $\mathbb{F}_q$. Define $\Gamma \triangleq (\gamma_1, \gamma_2, \ldots, \gamma_h) \in \mathbb{F}_{q^h}^h$, and

$$\boldsymbol{\beta} \triangleq (\beta_1, \beta_2, \ldots, \beta_{r+\delta-1}) = \Gamma P_2 \in \mathbb{F}_{q^h}^{r+\delta-1}, \tag{6}$$

namely, each column of P_2 is translated to an element of $\mathbb{F}_{q^h}$.

Construction A: For $m \in \mathbb{N}$, let $\mathcal{C}$ be the linear code with length n over $\mathbb{F}_{q^h}$ given by the parity-check matrix

$$H \triangleq \begin{pmatrix} P_1 & 0 & \cdots & 0 \\ 0 & P_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & P_1 \\ D(\gamma^0, \boldsymbol{\beta}, h, a) & D(\gamma^1, \boldsymbol{\beta}, h, a) & \cdots & D(\gamma^{m-1}, \boldsymbol{\beta}, h, a) \end{pmatrix}, \tag{7}$$

where $\gamma \in \mathbb{F}_{q^h}$ is a primitive element and $a = r + \delta - 1$.

Theorem 2: Let $q \geqslant \max\{r + \delta, m + 1\}$. Then the code $\mathcal{C}$ from Construction A is an $(n = m(r + \delta - 1), r, h, \delta, q^h)$-MR code with the minimum Hamming distance $d = (\lfloor \frac{h}{r} \rfloor + 1)(\delta - 1) + h + 1$.

Proof: To simplify the notation, let us denote the $((i - 1)(r+\delta-1)+j)$th coordinate by the pair (i, j), where $i \in [m]$ and $j \in [r + \delta - 1]$. Using this notation, the ith repair set is given by $S_i = \{(i, j) \ : \ j \in [r + \delta - 1]\}$, for $i \in [m]$.

Recall from (4) that P_1 is a Vandermonde matrix. Therefore, by (7), $\mathcal{C}|_{S_i}$ is a subcode of an $[r + \delta - 1, r, \delta]_q$ MDS code, which implies that the code $\mathcal{C}$ has $(r, \delta)_a$-locality. We shall now prove the code can recover from all erasure patterns $\mathcal{E} = \{E_{i_1}, E_{i_2}, \ldots, E_{i_t}\}$ such that $E_{i_\ell} \subseteq S_{i_\ell}$, $|E_{i_\ell}| \geqslant \delta$, and

$$\sum_{\ell=1}^{t} |E_{i_\ell}| - t(\delta - 1) \leqslant h, \tag{8}$$

namely, $\mathcal{C}$ is an (n, r, h, δ, q^h)-MR code.

For $\ell \in [t]$, assume $E_{i_\ell} = \{(i_\ell, j_1), (i_\ell, j_2), \ldots, (i_\ell, j_{|E_{i_\ell}|})\}$, and the columns of P_1 are denoted by $P_1 = (P_{1,1}, P_{1,2}, \ldots, P_{1,r+\delta-1})$. Define the projections of P_1 and $D(\gamma^{i-1}, \boldsymbol{\beta}, h, r+\delta-1)$ onto the erased coordinates as

$$P_1|_{E_{i_\ell}} \triangleq (P_{1,j_1}, P_{1,j_2}, \cdots, P_{1,j_{|E_{i_\ell}|}}),$$

and

$$D(\gamma^{i-1}, \boldsymbol{\beta}, h, r+\delta-1)|_{E_{i_\ell}} \triangleq \begin{pmatrix} \beta_{j_1} & \beta_{j_2} & \cdots & \beta_{j_{|E_{i_\ell}|}} \\ \mathcal{D}^1_{\gamma^{i-1}}(\beta_{j_1}) & \mathcal{D}^1_{\gamma^{i-1}}(\beta_{j_2}) & \cdots & \mathcal{D}^1_{\gamma^{i-1}}(\beta_{j_{|E_{i_\ell}|}}) \\ \vdots & \vdots & & \vdots \\ \mathcal{D}^{h-1}_{\gamma^{i-1}}(\beta_{j_1}) & \mathcal{D}^{h-1}_{\gamma^{i-1}}(\beta_{j_2}) & \cdots & \mathcal{D}^{h-1}_{\gamma^{i-1}}(\beta_{j_{|E_{i_\ell}|}}) \end{pmatrix}. \quad (9)$$

Proving that $\mathcal{E}$ is recoverable is equivalent to showing that the matrix

$$H_{\mathcal{E}} \triangleq \begin{pmatrix} P_1|_{E_{i_1}} & 0 & \cdots & 0 \\ 0 & P_1|_{E_{i_2}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & P_1|_{E_{i_t}} \\ D_{i_1,E_{i_1}} & D_{i_2,E_{i_2}} & \cdots & D_{i_t,E_{i_t}} \end{pmatrix}$$

has full column rank, where $D_{i_\ell,E_{i_\ell}} = D(\gamma^{i_\ell-1}, \boldsymbol{\beta}, h, a)|_{E_{i_\ell}}$ for $\ell \in [t]$. Otherwise, we cannot distinguish between a codeword $C \in \mathcal{C}$ from $C + C'$, where the nonzero components of C' is a nonzero solution of $H_{\mathcal{E}}X = 0$.

Since P_1 is a Vandermonde matrix, for any $E^*_{i_\ell} \subseteq E_{i_\ell}$ with $|E^*_{i_\ell}| = \delta - 1$, $\ell \in [t]$, we have that $P_1|_{E^*_{i_\ell}}$ has full rank. Denote $\overline{E}_{i_\ell} = E_{i_\ell} \setminus E^*_{i_\ell}$. Thus, there exists a matrix $A_{i_\ell} \in \mathbb{F}_q^{|E^*_{i_\ell}| \times |\overline{E}_{i_\ell}|}$ such that

$$\begin{pmatrix} P_1|_{E^*_{i_\ell}} & P_1|_{\overline{E}_{i_\ell}} \\ P_2|_{E^*_{i_\ell}} & P_2|_{\overline{E}_{i_\ell}} \end{pmatrix} \begin{pmatrix} I_{E^*_{i_\ell}} & -A_{i_\ell} \\ 0 & I_{\overline{E}^*_{i_\ell}} \end{pmatrix} = \begin{pmatrix} P_1|_{E^*_{i_\ell}} & 0 \\ P_2|_{E^*_{i_\ell}} & W_{i_\ell} \end{pmatrix} \quad (10)$$

i.e.,

$$P_1|_{\overline{E}_{i_\ell}} = P_1|_{E^*_{i_\ell}} A_{i_\ell}, \quad (11)$$

and

$$W_{i_\ell} = P_2|_{\overline{E}_{i_\ell}} - (P_2|_{E^*_{i_\ell}}) A_{i_\ell}, \quad (12)$$

where W_{i_ℓ} is an $h \times |\overline{E}_{i_\ell}|$ matrix over $\mathbb{F}_q$. Denote

$$\boldsymbol{\beta}^*_{i_\ell} = \Gamma W_{i_\ell} \quad (13)$$

for $\ell \in [t]$. For $\tau \in \overline{E}_{i_\ell}$, write

$$P_{1,\tau} = \sum_{a \in E^*_{i_\ell}} e^{(i_\ell)}_{a,\tau} P_{1,a} \quad (14)$$

with $e^{(i_\ell)}_{a,\tau} \in \mathbb{F}_q$ determined by A_{i_ℓ}. Then, it follows from (6) and (11)-(14) that

$$\beta^*_{i_\ell,\tau} = \beta_\tau - \sum_{a \in E^*_{i_\ell}} e^{(i_\ell)}_{a,\tau} \beta_a.$$

Note that

$$\begin{aligned} & D(\gamma^{i_\ell-1}, \boldsymbol{\beta}, h, r+\delta-1)|_{E_{i_\ell}} \begin{pmatrix} I_{E^*_{i_\ell}} & -A_{i_\ell} \\ 0 & I_{\overline{E}^*_{i_\ell}} \end{pmatrix} \\ =& D(\gamma^{i_\ell-1}, \Gamma(P_2|_{E^*_{i_\ell}}, P_2|_{\overline{E}_{i_\ell}}), h, |E_{i_\ell}|) \begin{pmatrix} I_{E^*_{i_\ell}} & -A_{i_\ell} \\ 0 & I_{\overline{E}^*_{i_\ell}} \end{pmatrix} \\ =& D(\gamma^{i_\ell-1}, \Gamma(P_2|_{E^*_{i_\ell}}, W_{i_\ell}), h, |E_{i_\ell}|) \\ =& (D_{i_\ell}, D(\gamma^{i_\ell-1}, \boldsymbol{\beta}^*_{i_\ell}, h, |\overline{E}_{i_\ell}|)), \end{aligned}$$

where the second equality holds by the linearity of $\mathcal{D}^i_\alpha(\cdot)$ (Proposition 1) and (10), and the last equality holds by (13). This is to say that $H_{\mathcal{E}}$ is equivalent with

$$\begin{pmatrix} P_1|_{E^*_{i_1}} & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & P_1|_{E^*_{i_2}} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & P_1|_{E^*_{i_t}} & 0 \\ D_{i_1} & D^*_{i_1,\overline{E}_{i_1}} & D_{i_2} & D^*_{i_2,\overline{E}_{i_2}} & \cdots & D_{i_t} & D^*_{i_t,\overline{E}_{i_t}} \end{pmatrix},$$

where $D^*_{i_\ell,\overline{E}_{i_\ell}} = D(\gamma^{i_\ell-1}, \boldsymbol{\beta}^*_{i_\ell}, h, |\overline{E}_{i_\ell}|)$ for $\ell \in [t]$. Recall that $P_1|_{E^*_{i_j}}$ for $j \in [t]$ has full rank. Hence, $H_{\mathcal{E}}$ is equivalent with

$$H^*_{\mathcal{E}} \triangleq \begin{pmatrix} P_1|_{E^*_{i_1}} & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & P_1|_{E^*_{i_2}} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & P_1|_{E^*_{i_t}} & 0 \\ 0 & D^*_{i_1,\overline{E}_{i_1}} & 0 & D^*_{i_2,\overline{E}_{i_2}} & \cdots & 0 & D^*_{i_t,\overline{E}_{i_t}} \end{pmatrix},$$

where $D^*_{i_\ell,\overline{E}_{i_\ell}} = D(\gamma^{i_\ell-1}, \boldsymbol{\beta}^*_{i_\ell}, h, |\overline{E}_{i_\ell}|)$ for $\ell \in [t]$. Then, $H_{\mathcal{E}}$ has full column rank if and only if

$$\begin{aligned} & (D^*_{i_1,\overline{E}_{i_1}}, D^*_{i_1,\overline{E}_{i_1}}, \cdots, D^*_{i_1,\overline{E}_{i_1}}) \\ =& (D(\gamma^{i_1-1}, \boldsymbol{\beta}^*_{i_1}, h, |\overline{E}_{i_1}|), D(\gamma^{i_2-1}, \boldsymbol{\beta}^*_{i_2}, h, |\overline{E}_{i_2}|), \\ & \cdots, D(\gamma^{i_t-1}, \boldsymbol{\beta}^*_{i_t}, h, |\overline{E}_{i_t}|)) \end{aligned}$$

has full column rank. Note from (4) and (5), that $\binom{P_1}{P_2}$ forms an $(h+\delta-1) \times (r+\delta-1)$ Vandermonde matrix. Clearly, $|E_{i_\ell}| \leqslant \min\{h+\delta-1, r+\delta-1\}$ for $\ell \in [t]$, which means

$$\operatorname{rank} \begin{pmatrix} P_1|_{E^*_{i_\ell}} & P_1|_{\overline{E}_{i_\ell}} \\ P_2|_{E^*_{i_\ell}} & P_2|_{\overline{E}_{i_\ell}} \end{pmatrix} = |E^*_{i_\ell}| + |\overline{E}_{i_\ell}|,$$

and $\operatorname{rank}(P_1|_{E^*_{i_\ell}}) = |E^*_{i_\ell}|$. Thus, (10) implies $\operatorname{rank}(W_{i_\ell}) = |\overline{E}_{i_\ell}|$ for $\ell \in [t]$. Now, according to (2), (13) and the linearity of $\mathcal{D}^i_\alpha(\cdot)$, we have

$$\begin{aligned} & \operatorname{rank}((D(\gamma^{i_1-1}, \boldsymbol{\beta}^*_{i_1}, h, |\overline{E}_{i_1}|), D(\gamma^{i_2-1}, \boldsymbol{\beta}^*_{i_2}, h, |\overline{E}_{i_2}|), \\ & \quad \cdots, D(\gamma^{i_t-1}, \boldsymbol{\beta}^*_{i_t}, h, |\overline{E}_{i_t}|))) \\ =\ & \operatorname{rank}((D(\gamma^{i_1-1}, \Gamma, h, h)W_{i_1}, D(\gamma^{i_2-1}, \Gamma, h, h)W_{i_2}, \\ & \quad \cdots, D(\gamma^{i_t-1}, \Gamma, h, h)W_{i_t})) \\ =\ & \operatorname{rank}((D(\gamma^0, \Gamma, h, h)W'_1, D(\gamma^1, \Gamma, h, h)W'_2, \\ & \quad \cdots, D(\gamma^{m-1}, \Gamma, h, h)W'_m)), \end{aligned} \quad (15)$$

where

$$W_i' \triangleq \begin{cases} W_i, & \text{if } i \in \{i_\ell \ : \ \ell \in [t]\}, \\ 0, & \text{otherwise}. \end{cases} \tag{16}$$

We observe that

$$(D(\gamma^0, \Gamma, h, h), D(\gamma^1, \Gamma, h, h), \cdots, D(\gamma^{m-1}, \Gamma, h, h))$$

can be regarded as the generator matrix of a linearized Reed-Solomon code with parameters $[mh, h]_{q^h}$ according to Definition 6. Then, applying Theorem 1 to (15) and (16), we conclude that

$$\begin{aligned} &\operatorname{rank}((D(\gamma^{i_1-1}, \boldsymbol{\beta}^*_{i_1}, h, |\overline{E}_{i_1}|), D(\gamma^{i_2-1}, \boldsymbol{\beta}^*_{i_2}, h, |\overline{E}_{i_2}|), \\ &\quad \cdots, D(\gamma^{i_t-1}, \boldsymbol{\beta}^*_{i_t}, h, |\overline{E}_{i_t}|))) \\ &= \sum_{i=1}^{m} \operatorname{rank}(W_i') \\ &= \sum_{\ell=1}^{t} \operatorname{rank}(W_{i_\ell}) \\ &= \sum_{\ell=1}^{t} |\overline{E}_{i_\ell}|, \end{aligned}$$

which means $H^*_{\mathcal{E}}$ has full rank, i.e., $H_{\mathcal{E}}$ has full rank for all possible $\mathcal{E}$ that satisfy (8). Therefore, $\mathcal{C}$ can recover all the erasure patterns required by MR codes.

Having reached this point, the desired result follows from the fact that MR codes are optimal LRCs. Hereafter, for the sake of completeness, we derive the minimum Hamming distance for the reader's convenience. We know the code $\mathcal{C}$ can recover from any erasure pattern that affects at most $\delta - 1$ coordinates in each repair set, and any additional h erased positions. Let us consider the other erasure patterns, obviously where all the affected repair sets have at least δ erasures each. In particular, we consider the *minimal* erasure configurations, namely, configurations in which the removal of any one erasure makes it recoverable. Assume that a repair sets are affected. Then, the total number of erasures is $a(\delta-1)+h+1$, where the $h+1$ erasures are distributed among the a affected repair sets, i.e., it requires $a(\delta - 1) + h + 1 \leqslant a(r + \delta - 1)$ and thus

$$a \geqslant \left\lceil \frac{h+1}{r} \right\rceil = \left\lfloor \frac{h}{r} \right\rfloor + 1.$$

Therefore, a lower bound on the Hamming distance of $\mathcal{C}$ is

$$d \geqslant \left(\left\lfloor \frac{h}{r} \right\rfloor + 1 \right) (\delta - 1) + h + 1.$$

Note from (7) that $k \geqslant n - h - m(\delta - 1) = mr - h$ which implies $\lceil \frac{k}{r} \rceil + \lfloor \frac{h}{r} \rfloor \geqslant m$. Since $\mathcal{C}$ is a locally repairable code with $(r, \delta)_a$-locality, by Lemma 1 we have

$$\begin{aligned} d &\leqslant n - k - \left(\left\lceil \frac{k}{r} \right\rceil - 1 \right) (\delta - 1) + 1 \\ &\leqslant n - k - \left(m - \left\lfloor \frac{h}{r} \right\rfloor - 1 \right) (\delta - 1) + 1 \\ &\leqslant h + \left(\left\lfloor \frac{h}{r} \right\rfloor + 1 \right) (\delta - 1) + 1. \end{aligned}$$

Combining this with the lower bound on d, we obtain

$$d = \left(\left\lfloor \frac{h}{r} \right\rfloor + 1 \right) (\delta - 1) + h + 1.$$

Thus, $\mathcal{C}$ is an (n, r, h, δ, q^h)-MR code with $d = (\lfloor \frac{h}{r} \rfloor + 1)(\delta - 1) + h + 1$. ∎

Corollary 1: Let $q \geqslant \max\{r+\delta, m+1\}$ and $\delta \geqslant 2$. If $m = \Theta(q)$ and $r = \Theta(q)$ (implying $n = \Theta(q^2)$), then for fixed $h \leqslant \min\{m, \delta+1\}$ the code $\mathcal{C}$ generated by Construction A is an $(n = m(r+\delta-1), r, h, \delta, q^h)$-MR code with asymptotically order-optimal field size $q^h = \Theta(n^{h/2})$.

Proof: By our setting, the field size of the code generated by Construction A is $\Theta(q^h)$. According to Lemma 2, the field size must be at least

$$\Omega(nr^{\min\{\delta-1, h-2\}}) = \Omega(m(r + \delta - 1)r^{h-2}) = \Omega(q^h),$$

where the first equality holds by $h \leqslant \delta + 1$, and the second one follows from $m = \Theta(q)$, $r = \Theta(q)$, and the fact that h, δ are regarded as constants. Thus, the code $\mathcal{C}$ generated by Construction A has asymptotically order-optimal field size $\Theta(q^h)$. ∎

Example 1: Let $r = 2$, $\delta = 2$, $q = 4$, and $m = 3$. By Construction A and Theorem 2, an $(n = 9, r = 2, h = 2, \delta = 2, q^2 = 16)$-MR code can be given by the following parity-check matrix

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \alpha^6 & \alpha^9 & \alpha^{10} & \alpha^7 & \alpha^{10} & \alpha^{11} & \alpha^8 & \alpha^{11} & \alpha^{12} \\ \alpha^{10} & \alpha^7 & \alpha^{11} & \alpha^0 & \alpha^{12} & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^6 \end{pmatrix},$$

where α is a primitive element of $\mathbb{F}_{16}$.

IV. Concluding Remarks

In this paper, we introduced a construction of maximally recoverable codes with uniform-sized disjoint repair sets, also known as partial MDS (PMDS) codes. Our construction is based on linearized Reed-Solomon codes, and it yields maximally recoverable codes with field size $\Theta((\max\{r + \delta - 1, \frac{n}{r+\delta-1}\})^h)$, where h and δ are constants. Compared with known constructions, our construction can generate maximally recoverable codes with a smaller field size in certain cases. In some particular regimes, described in Corollary 1, the construction produces code families with order-optimal field size. For more details about parameters for MR codes, a summary of the results in comparison with known constructions is given in Table I, where q and q_1 are prime powers, and $m = \frac{n}{r+\delta-1}$.

We would like to highlight some interesting cases from Table I. In [17], a construction for $(n, r, 3, \delta, q)$-MR codes was provided, achieving $q = \Theta(n^3)$, but only for odd characteristic. Finding a comparable construction for even characteristic was left as an open question. Here, Construction A provides an answer to this question, since our construction does not impose a restriction on the parity of the field characteristic, and it achieves the same order $q = \Theta(n^3)$.

Another case we would like to point out involves the asymptotic regime where $r = \Theta(n)$. In this regime, our construction achieves a field size of $q = \Theta(n^h)$. For odd q or $\delta > 2$, this improves upon the best known construction from [12], which achieves $q = \Theta(n^{h\delta})$. When $\delta = 2$, q is even, and $r = \Theta(n)$, the best known result is still the one in [14] with $q = \Theta(k^{h-1}) = \Theta(n^{h-1})$.

In addition, [12] challenged researchers to find families of PMDS codes with smaller field sizes than $\max\{m, (r+\delta-1)^{h+\delta-1}\}^h$. The construction in [32] does so for the case $h < r$ and $(r+\delta-1)^{h+\delta-1} > m$. Similarly, the construction in [3] also improves upon [12] for the case $r = 2$. In this paper, the MR codes generated by Construction A provide an improvement over [12] for $(r+\delta-1)^{h+\delta-1} > m$, since in this case $\max\{r+\delta-1, \frac{n}{r+\delta-1}\}^h < \max\{m, (r+\delta-1)^{h+\delta-1}\}^h$.

The broad problem of closing the gap between the field-size requirements of known constructions and the theoretic bounds is still largely open. Further closing this gap, beyond the results of this paper, is left for future work.

ACKNOWLEDGMENT

The authors would like to thank the Associate Editor, Prof. Camilla Hollanti and the anonymous reviewers, whose comments and suggestions improved the presentation of this article.

REFERENCES

[1] 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. 2013.

[2] 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.

[3] T. Bogart, A.-L. Horlemann-Trautmann, D. Karpuk, A. Neri, and M. Velasco, "Constructing partial MDS codes from reducible curves," 2020, *arXiv:2007.14829*. [Online]. Available: http://arxiv.org/abs/2007.14829

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] G. Calis and O. O. Koyluoglu, "A general construction for PMDS codes," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 452–455, Mar. 2017.

[10] B. Chen, W. Fang, S.-T. Xia, J. Hao, and F.-W. Fu, "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, Jan. 2021.

[11] 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.

[12] 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.

[13] P. Gopalan, G. Hu, S. Kopparty, S. Saraf, C. Wang, and S. Yekhanin, "Maximally recoverable codes for grid-like topologies," in *Proc. 28th Annu. ACM-SIAM Symp. Discrete Algorithms*, Jan. 2017, pp. 2092–2108.

[14] 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.

[15] 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.

[16] S. Gopi and V. Guruswami, "Improved maximally recoverable LRCs using skew polynomials," 2020, *arXiv:2012.07804*. [Online]. Available: http://arxiv.org/abs/2012.07804

[17] 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.

[18] 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.

[19] J. Hao, S.-T. Xia, K. W. Shum, B. Chen, F.-W. Fu, and Y. Yang, "Bounds and constructions of locally repairable codes: Parity-check matrix approach," *IEEE Trans. Inf. Theory*, vol. 66, no. 12, pp. 7465–7474, Dec. 2020.

[20] L. Holzbaur, S. Puchinger, E. Yaakobi, and A. Wachter-Zeh, "Partial MDS codes with regeneration," *IEEE Trans. Inf. Theory*, vol. 67, no. 10, pp. 6425–6441, Oct. 2021.

[21] A.-L. Horlemann-Trautmann and A. Neri, "A complete classification of partial MDS (maximally recoverable) codes with one global parity," *Adv. Math. Commun.*, vol. 14, no. 1, pp. 69–88, 2020.

[22] 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.

[23] 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.

[24] C. Huang *et al.*, "Erasure coding in windows azure storage," in *Proc. USENIX Annu. Tech. Conf. (ATC)*, 2012, pp. 15–26.

[25] L. Jin, L. Ma, and C. Xing, "Construction of optimal locally repairable codes via automorphism groups of rational function fields," *IEEE Trans. Inf. Theory*, vol. 66, no. 1, pp. 210–221, Jan. 2020.

[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] M. Li and P. P. C. Lee, "STAIR codes: A general family of erasure codes for tolerating device and sector failures," *ACM Trans. Storage*, vol. 10, no. 4, pp. 1–30, Oct. 2014.

[28] X. Li, L. Ma, and C. Xing, "Construction of asymptotically good locally repairable codes via automorphism groups of function fields," *IEEE Trans. Inf. Theory*, vol. 65, no. 11, pp. 7087–7094, Nov. 2019.

[29] M. Luby, R. Padovani, T. J. Richardson, L. Minder, and P. Aggarwal, "Liquid cloud storage," *ACM Trans. Storage*, vol. 15, no. 1, pp. 1–49, Apr. 2019.

[30] G. Luo and X. Cao, "Optimal cyclic codes with hierarchical locality," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3302–3310, Jun. 2020.

[31] U. Martínez-Peñas, "Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring," *J. Algebra*, vol. 504, pp. 587–612, Jun. 2018.

[32] 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.

[33] A. Neri and A.-L. Horlemann-Trautmann, "Random construction of partial MDS codes," *Des., Codes Cryptogr.*, vol. 88, no. 4, pp. 711–725, Apr. 2020.

[34] R. W. Nobrega and B. F. Uchoa-Filho, "Multishot codes for network coding using rank-metric codes," in *Proc. 3rd IEEE Int. Workshop Wireless Netw. Coding*, Jun. 2010, pp. 1–6.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] M. Sathiamoorthy *et al.*, "XORing elephants: Novel erasure codes for big data," *Very Large Data Based Endowment*, vol. 6, no. 5, pp. 325–336, Mar. 2013.
[41] R. C. R. C. Singleton, "Maximum distance Q-nary codes," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 2, pp. 116–118, Apr. 1964.
[42] 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.
[43] I. Tamo, A. Barg, and A. Frolov, "Bounds on the parameters of locally recoverable codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3070–3083, Jun. 2016.
[44] A. Wang and Z. Zhang, "Repair locality with multiple erasure tolerance," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6979–6987, Nov. 2014.
[45] 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.
[46] C. Xing and C. Yuan, "Construction of optimal locally recoverable codes and connection with hypergraph," in *Proc. 46th Int. Colloq. Automata, Lang., Program. (ICALP)*, 2019, pp. 98:1–98:13.
[47] 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.
[48] G. Zhang and H. Liu, "Constructions of optimal codes with hierarchical locality," *IEEE Trans. Inf. Theory*, vol. 66, no. 12, pp. 7333–7340, Dec. 2020.

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 with the Faculty of Engineering, Information and Systems, University of Tsukuba, Japan. Since 2018, he has been a Post-Doctoral Fellow with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Israel. In 2021, he joined Southwest Jiaotong University, where he currently holds a tenure-track position. His research interests include coding theory and sequence design.

Ying Miao received the D.Sci. degree in mathematics from Hiroshima University, Hiroshima, Japan, in 1997.

From 1989 to 1993, he worked with the Suzhou Institute of Silk Textile Technology, Suzhou, Jiangsu, China. From 1995 to 1997, he was a Research Fellow with the Japan Society for the Promotion of Science. From 1997 to 1998, he was a Post-Doctoral Fellow with the Department of Computer Science, Concordia University, Montreal, QC, Canada. In 1998, he joined the University of Tsukuba, Tsukuba, Ibaraki, Japan, where he is currently a Full Professor with the Faculty of Engineering, Information and Systems. His current research interests include combinatorics, coding theory, and information security. He received the 2001 Kirkman Medal from the Institute of Combinatorics and its Applications. He is on the editorial boards of several journals, such as *Graphs and Combinatorics* and *Journal of Combinatorial Designs*.

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 with the Department of Electrical and Computer Engineering, University of California at San Diego, and a Post-Doctoral Researcher with the Department of Electrical Engineering, California Institute of Technology. While on sabbatical 2012–2014, he was a Visiting Scientist with 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, Israel. His research interests include algebraic coding, combinatorial structures, and digital sequences. 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 has served as an Associate Editor of 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 of coding and decoding for the IEEE TRANSACTIONS ON INFORMATION THEORY. He is also an Editorial Board Member of the *Journal of Combinatorial Theory, Series A* since 2021.

Xiaohu Tang (Senior Member, IEEE) received the B.S. degree in applied mathematics from Northwest Polytechnic University, Xi'an, China, in 1992, the M.S. degree in applied mathematics from Sichuan University, Chengdu, China, in 1995, and the Ph.D. degree in electronic engineering from Southwest Jiaotong University, Chengdu, in 2001.

From 2003 to 2004, he was a Research Associate with the Department of Electrical and Electronic Engineering, The Hong Kong University of Science and Technology. From 2007 to 2008, he was a Visiting Professor with the University of Ulm, Germany. Since 2001, he has been with the School of Information Science and Technology, Southwest Jiaotong University, where he is currently a Professor. His research interests include coding theory, network security, distributed storage and information processing for big data. He was a recipient of the National excellent Doctoral Dissertation Award, China, in 2003, the Humboldt Research Fellowship, Germany, in 2007, and the Outstanding Young Scientist Award by NSFC, China, in 2013. He has served as an Associate Editors for several journals, including IEEE TRANSACTIONS ON INFORMATION THEORY and *IEICE Transactions on Fundamentals*. He has served on a number of technical program committees of conferences.