Partial MDS Codes with Local Regeneration

Lukas Holzbaur*, Sven Puchinger†, Eitan Yaakobi‡, and Antonia Wachter-Zeh*
*Technical University of Munich, {lukas.holzbaur, antonia.wachter-zeh}@tum.de
†Technical University of Denmark, svepu@dtu.dk
‡Technion — Israel Institute of Technology, yaakobi@cs.technion.ac.il

***Abstract*—Partial MDS (PMDS) and sector-disk (SD) codes are classes of erasure codes that combine locality with strong erasure correction capabilities. We construct PMDS and SD codes where each local code is a bandwidth-optimal regenerating MDS code. The constructions require significantly smaller field size than the only other construction known in literature.**

I. Introduction

Distributed data storage is ever increasing its importance with the amount of data stored by cloud service providers and data centers in general reaching staggering heights. The data is commonly spread over a number of nodes (servers or hard drives) in a *distributed storage system* (DSS), with some additional redundancy to protect the system from data loss in the case of node failures (erasures). The resilience of a DSS against such events can be measured either by the minimal *number of nodes* that needs to fail for data loss to occur, i.e., the *distance* of the storage code, or by the expected time the system can be operated before a failure occurs that causes data loss, referred to as the *mean time to data loss*. For both measures the use of maximum distance separable (MDS) codes provides the optimal trade-off between storage overhead and resilience to data loss (note that replication is a trivial MDS code). The downside of using MDS codes is the cost of recovering (replacing) a failed node. Consider a storage system with k information nodes and s nodes for redundancy. If an MDS code is used for the recovery of a node by means of erasure decoding, it necessarily involves at least k nodes (helpers) and, if done by straight-forward methods, a large amount of network traffic, namely the download of the entire content from k nodes. To address these issues, the concepts of *locally repairable codes* (LRCs) [1]–[7] and *regenerating codes* [8]–[10] have been introduced.

To lower the amount of network traffic in recovery, regenerating codes allow for repairing nodes by accessing $d > k$ nodes, but only retrieve a function of the data stored on each node. This significantly decreases the repair traffic. Lower bounds on the required traffic for repair have been derived in [8], [9] which lead to two extremal code classes, namely *minimum bandwidth regenerating* (MBR) and *minimum storage regenerating* (MSR) *codes*. MBR codes offer the lowest possible repair traffic, but at the cost of increased storage overhead compared to MDS codes. In this work we consider d-MSR codes, which require more network traffic for repair than MBR codes, but are optimal in terms of storage overhead, i.e., they are MDS.

To address the other downside of node recovery in MDS codes, namely the large number of required helper nodes, LRCs introduce additional redundancy to the system, such that in the (more likely) case of a few node failures the recovery only involves less than k helper nodes, i.e., can be performed *locally*. This subset of helper nodes is referred to as a *local code*. Recently several constructions of LRCs which maximize the distance have been proposed. However, when considering the mean time to data loss as the performance metric, distance-optimal LRCs are not necessarily optimal, as it is possible to tolerate many failure patterns involving a larger number of nodes than the number that can be guaranteed, while still fulfilling the locality constraints [11], [12]. *Partial MDS* (PMDS) *codes* [13]–[15], also referred to as *maximally recoverable codes* [16], [17], are a subclass of LRCs which guarantee to tolerate *all* failure patterns possible under these constraints and thereby maximize the mean time to data loss. Specifically, an (r, s)-PMDS code of length μn can be partitioned into μ local groups of size n, such that any erasure pattern with r erasures in each local group plus any s erasures in arbitrary positions can be recovered.

However, the local recovery of nodes still induces a large amount of network traffic, as the entire content of the helper nodes needs to be downloaded when considering straightforward use recovery algorithms. To circumvent this bottleneck, several regenerating local codes [8] have been proposed [2]–[7]. In [18] it was shown that the LRC construction of [3] is in fact a PMDS code, implicitly giving the first construction of PMDS codes with local regeneration[1]. However, these PMDS codes require a field size exponential in the length of the code.

In this work, we propose the first constructions of locally regenerating PMDS codes with field size that is not exponential in the length. Our first construction gives $(r, s = 2)$-PMDS codes where each local code is a d-MSR code by a non-trivial combination of the $(r, s = 2)$-PMDS codes of [14] and the MSR codes of [10], over a field of size $O(rn)$. The second construction of (r, s)-PMDS codes with local d-MSR codes, which is valid for any value of s, combines the (r, s)-PMDS construction of [15] with the MSR codes of [10] and requires a field size of $O((\mu n)^{s(r+1)})$, when $r = O(1)$ and $s = O(1)$. The number of field elements stored at each node (*subpacketization*) is $\ell = O(r^n)$, and thus equal to the subpacketization in the MSR code construction of [10].

II. Preliminaries

A. Notation

We write $[a, b]$ for the set of integers $\{a, a + 1, ..., b\}$ and $[b]$ if $a = 1$. For a set of integers $R \subseteq [n]$ and a code $\mathcal{C}$ of length n we write $\mathcal{C}|_R$ for the code obtained by restricting $\mathcal{C}$ to the positions indexed by R, i.e., puncturing in the positions $[n] \setminus R$. For an element $\alpha \in \mathbb{F}$ we denote its order by $\mathcal{O}(\alpha)$.

The work of L. Holzbaur was supported by the Technical University of Munich – Institute for Advanced Study, funded by the German Excellence Initiative and European Union 7th Framework Programme under Grant Agreement No. 291763 and the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) under Grant No. WA3907/1-1. S. Puchinger has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement no. 713683 (COFUNDfellowsDTU). The work of E. Yaakobi was partially supported by the ISF grant 1817/18 and by the Technion Hiroshi Fujiwara cyber security research center and the Israel cyber directorate.

[1]The construction in [3] consists of two encoding stages, where in the second stage an arbitrary linear MDS code can be used to obtain the local codes. In [18] it was shown that the construction in fact gives a PMDS code, independent of the explicit choice of the MDS code in the second encoding stage. It follows that using a regenerating MDS code in the second encoding stage results in a PMDS code with local regeneration.

We denote a code of length n, dimension k, and distance $d_{\min}$ by $[n, k, d_{\min}]$. For a code over $\mathbb{F}_{q^\ell}$ that is linear over $\mathbb{F}_q$ we write $[n, k, d_{\min}; \ell]$. The parameter ℓ is referred to as the subpacketization of the code and as each codeword of this code can be viewed as an array over $\mathbb{F}_q$ with n columns and ℓ rows, we also refer to such codes as *array codes*. If the distance $d_{\min}$ is clear from context or not of interest, we omit it from the notation.

This work is largely based on the constructions of PMDS codes in [14], [15] and the construction of MSR codes in [10]. Since the notations in these works are conflicting, i.e., the same symbols are used for different parameters of the codes, Table I provides an overview of the notation used in this work compared to these works.

TABLE I
OVERVIEW OF THE NOTATION USED IN THIS WORK COMPARED TO THE NOTATION USED IN [10], [14], [15]. AS WE ARE CONSTRUCTING PMDS CODES WITH LOCAL MSR CODES IN THE FOLLOWING, THE LENGTH AND NUMBER OF PARITIES IN THE MSR CODE CONSTRUCTION OF [10] ARE MATCHED WITH THE PARAMETERS OF THE LOCAL CODES IN OUR WORK.

Description	[14]	[15]	[10]	This work
Number of local groups	r	m	-	μ
Length of local MSR code	n	n	n	n
Number of local parity symbols	m	r	r	r
Number of global parity symbols	s	s	-	s
Code length	rn	mn	-	μn
Subpacketization	-	-	l	ℓ
Number of nodes needed for repair	-	-	d	d

B. Definitions

We begin by formally defining PMDS codes in our notation.

Definition 1 (Partial MDS array codes)**.** *Let $\mu n, \mu, n, r, s, \ell \in \mathbb{Z}_{>0}$ such that $r \leq n$ and $s \leq (n-r)\mu$.*

Let $\mathcal{C} \subset \mathbb{F}_q^{\ell \times \mu n}$ be a linear $[\mu n, (n-r)\mu - s; \ell]$ code. The code $\mathcal{C}$ is a $\mathsf{PMDS}(\mu n, \mu, n, r, s; \ell)$ partial MDS array code *if there exists a partition $\mathcal{W} = \{W_1, W_2, ..., W_\mu\}$ of $[\mu n]$ with $|W_i| = n$ for all $i \in [\mu]$ such that*

- *the code $\mathcal{C}|_{W_i}$ is an $[n, n-r, r+1; \ell]$ MDS code for all $i \in [\mu]$ and*
- *the code $\mathcal{C}|_{[\mu n] \setminus \cup_{i=1}^{\mu} E_i}$ is an $[n - r\mu, n - r\mu - s, s+1; \ell]$ MDS code, where $E_i \subset W_i$ with $|E_i| = r$ for all $i \in [\mu]$.*

We refer to the code $\mathcal{C}|_{W_i}$ as the i-th *local code*.

Remark 1. *In [14], [15] each codeword of the PMDS and SD codes is regarded as an $\mu \times n$ array, where for PMDS codes each row can correct r erasures and for SD codes r erased columns can be corrected. As we will construct PMDS and SD codes with local MSR codes, we will require subpacketization, i.e., each node will not store a symbol, but a vector of multiple symbols. To avoid having different types of rows, we adopt the terminology commonly used in the LRC literature and view the codewords of a PMDS or SD code as vectors, and what we refer to as* local codes *is equivalent to the* rows *of [14], [15].*

In the following we will construct both PMDS and SD codes with local regeneration, but since the concepts and proofs are mostly the same, we provide them in less detail for SD codes.

Remark 2. *Sector-Disk codes are defined similar to PMDS codes as in Definition 1, except that $E_1 = E_2 = \ldots = E_\mu$ holds.*

Definition 2 (Regenerating code [8], [9])**.** *Let $\mathcal{F}, \mathcal{R} \subset [n]$ be two disjoint subsets with $\mathcal{F} \leq r$ and $\mathcal{R} \geq n - r$. Let $\mathcal{C}$ be an $[n, n-r; \ell]$ MDS array code $\mathcal{C}$ over $\mathbb{F}_q$. Define $M(\mathcal{C}, \mathcal{F}, \mathcal{R})$ as the smallest number of symbols of $\mathbb{F}$ one needs to download from the surviving nodes indexed by $\mathcal{R}$ to recover the erased nodes indexed by $\mathcal{F}$. Then*

$$M(\mathcal{C}, \mathcal{F}, \mathcal{R}) \geq \frac{|\mathcal{F}||\mathcal{R}|\ell}{|\mathcal{F}| + |\mathcal{R}| - n + r} \ . \tag{1}$$

*We say that the code $\mathcal{C}$ is an (h, d)-*MSR *code if*

$$\max_{\substack{|\mathcal{F}|=h, |\mathcal{R}|=d \\ \mathcal{F} \cap \mathcal{R} = \emptyset}} M(\mathcal{C}, \mathcal{F}, \mathcal{R}) = \frac{|\mathcal{F}||\mathcal{R}|\ell}{|\mathcal{F}| + |\mathcal{R}| - n + r} \ .$$

If $h = 1$ we say the code is a d-MSR code.

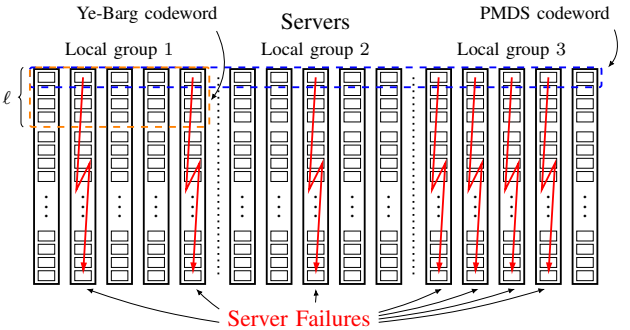

Fig. 1. Illustration of locally regenerating PMDS array codes as constructed in this work, with $n = 5$, $\mu = 3$ and each symbol of the code alphabet represented by a small rectangle. The shown erasure pattern can be corrected by an $(r = 2, s = 2)$-PMDS code.

Definition 3 (Locally (h, d)-MSR PMDS array codes)**.** *Let $\mathcal{C}$ be a $\mathsf{PMDS}(\mu n, \mu, n, r, s; \ell)$ code with partition $\mathcal{W}$. We say that the code $\mathcal{C}$ is locally (h, d)-MSR if $\mathcal{C}|_{W_i}$ is an (h, d)-MSR code for all $i \in [\mu]$. If $h = 1$ we say the code is a locally d-MSR PMDS code.*

Figure 1 shows an illustration of a locally regenerating PMDS array code. Assuming it to be an $(r = 2, s = 2)$-PMDS code, the erasures in the first local code can be corrected locally, but without taking advantage of the regenerating property, as the number of available helper nodes is only $n-r$. The erasure in the second local code can be corrected from the remaining $n-r+1$ nodes in the local group using the locally regenerating property, and the erasures in the third local code can be recovered by accessing nodes of the other local groups. Note that the example was chosen specifically to illustrate these different cases, the case of a single erasure in a local code, for which the locally regenerating property decreases the repair bandwidth, is far more likely than the other cases.

C. Ye-Barg Regenerating Codes

We repeat [10, Construction 2] in the slightly different notation which will be used in this work.

Definition 4 (Ye-Barg d-MSR codes [10, Construction 2])**.** *Let $\mathcal{C} \subset \mathbb{F}_q$ be an $[n, n-r; \ell]$ array code over $\mathbb{F}_q$, where $q \geq bn$ and $b = d + 1 - n + r$. Let $\{\beta_{i,j}\}_{i \in [n], j \in [b]}$ be a set of bn distinct elements of $\mathbb{F}_q$. Then each codeword is an array with $\ell = b^n$ rows and n columns, where the i-th row fulfills the parity check equations*

$$\mathbf{H}^{(a)} = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \beta_{1,a_1} & \beta_{2,a_2} & \ldots & \beta_{n,a_n} \\ \vdots & \vdots & & \vdots \\ \beta_{1,a_1}^{r-1} & \beta_{2,a_2}^{r-1} & \ldots & \beta_{n,a_n}^{r-1} \end{bmatrix} ,$$

for $a \in [0, \ell - 1]$ and $a = \sum_{i=1}^{n} a_i b^{i-1}$.

Remark 3. *The constructions presented in Section III and IV can also be applied to obtain locally (h, d)-MSR PMDS codes, where each local code is an (h, d)-MSR code as in [10, Construction 3], which is very similar in structure to [10,*

Construction 2] given in Definition 4. However, as the required subpacketization is larger for the former, we focus on d-MSR codes in this work.

Remark 4. *In Definition 4 we define each row of the array code by a set of parity check equations independent of the other $\ell - 1$ rows of the array. Note that this is not possible for array codes in general. However, for the existence of such a description it is sufficient that the matrices A_i, as defined in [10], are diagonal matrices. This simplifies the notation for the cases considered in this work, as this notation makes it obvious that each row is an $[n, n-r]$ RS code, and thereby MDS.*

III. Regenerating PMDS and Sector-Disk codes with Two Global Parities

We construct array codes from the PMDS and SD codes of [14] using the ideas of [10] to obtain locally d-MSR PMDS codes.

A. Generalization of known PMDS construction

To apply the ideas of [10] when constructing locally d-MSR PMDS and SD codes we need the local codes to be RS codes with specific code locators. The construction of PMDS codes given in [14] has the property that the local codes are RS codes, but the code locators are fixed to be the first n powers of some element β of sufficient order. We generalize this construction to allow for different choices of code locators for the local codes.

Let $\beta \in \mathbb{F}_{2^w}$ be an element of order $\mathcal{O}(\beta) \geq \mu N$. The $[\mu n, \mu(n-r)-2]$ code $\mathcal{C}(\mu, n, r, 2, \mathcal{L}, N)$ is given by the $(r\mu+2) \times \mu n$ parity-check matrix

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_0 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \dots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0 \\ \mathbf{H}_1 & \mathbf{H}_2 & \dots & \mathbf{H}_\mu \end{bmatrix}$$

where

$$\mathbf{H}_0 = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \beta^{i_1} & \beta^{i_2} & \dots & \beta^{i_n} \\ \beta^{2i_1} & \beta^{2i_2} & \dots & \beta^{2i_n} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{(r-1)i_1} & \beta^{(r-1)i_2} & \dots & \beta^{(r-1)i_n} \end{bmatrix}$$

for $\mathcal{L} = \{i_1, i_2, ..., i_n\}$ and, for $0 \leq j \leq \mu - 1$,

$$\mathbf{H}_{j+1} = \begin{bmatrix} \beta^{ri_1} & \beta^{ri_2} & \dots & \beta^{rn} \\ \beta^{-jN-i_1} & \beta^{-jN-i_2} & \dots & \beta^{-jN-i_n} \end{bmatrix} .$$

Note that this generalization includes both [14, Construction A] and [14, Construction B] as special cases

$$\mathcal{C}_A(\mu, n, r, 2, \{0, 1, ..., n-1\}, n)$$

and

$$\mathcal{C}_B(\mu, n, r, 2, \{0, 1, ..., n-1\}, N_B)$$

for $N_B = (r+1)(n-1-r)+1$, respectively.

We now derive a general, sufficient condition on N, based on the set $\mathcal{L}$, such that the code is a PMDS code.

Lemma 1. *Let $\mathcal{L}$ be any set of non-negative integers with $|\mathcal{L}| = n$, then the code $\mathcal{C}(\mu, n, r, 2, \mathcal{L}, N)$ is a PMDS code for any $N \geq (r+1)(\max_{i \in \mathcal{L}} i - r) + 1$*

Proof. We follow the proof of [14, Theorem 5]. Assume r positions in each local group (row of the PMDS code) have been erased and in addition there are 2 random erasures. If the two erasures occur in the same local group z, all local groups except for this one will be corrected by the local codes. Since all points in $\mathcal{L}$ are distinct, by the same argument as in [14], the matrix corresponding to the erased positions is a Vandermonde matrix and the erasures can be corrected.

Now consider the case of two local groups (horizontal codes) with $r+1$ erasures each, where the erased positions are given by $\{j_1, ..., j_{r+1}\} \subset \mathcal{L}$ and $\{j'_1, ..., j'_{r+1}\} \subset \mathcal{L}$, respectively. By the same arguments as in [14, Theorem 7] we obtain, that such an erasure pattern is correctable if

$$Nz + \sum_{u=1}^{r+1} j'_u - \sum_{u=1}^{r+1} j'_u \neq 0 \mod \mathcal{O}(\beta) .$$

Since all j_u are distinct, we have

$$\frac{r(r+1)}{2} = \sum_{u=0}^{r} u \leq \sum_{u=1}^{r+1} j_u$$

and

$$\sum_{u=1}^{r+1} j_u \leq \sum_{u=0}^{r} (\max_{j \in \mathcal{L}} j - r) + u$$
$$= (r+1)(\max_{j \in \mathcal{L}} j - r) + \sum_{u=0}^{r} u = N - 1 + \frac{r(r+1)}{2} .$$

The remaining steps are exactly the same as in [14, Theorem 7] and we obtain

$$1 \leq Nz + \sum_{u=1}^{r+1} j'_u - \sum_{u=1}^{r+1} j_u \leq N\mu - 1 < \mathcal{O}(\beta)$$

and the lemma statement follows. □

By similar arguments we also give a general, sufficient condition on N for the code to be an SD code.

Lemma 2. *Let $\mathcal{L}$ be any set of non-negative integers with $|\mathcal{L}| = n$, then the code $\mathcal{C}(\mu, n, r, 2, \mathcal{L}, N)$ is an SD code for any $N \geq \max_{j \in \mathcal{L}} j + 1$*

Proof. The case of $r+2$ erasures in the same local group (horizontal code) is the same as in Lemma 1 and [14, Theorem 5/7]. Now consider the case of r column erasures in positions $j_1, ..., j_r \in \mathcal{L}$ and two random erasures in distinct rows z and z' in positions $j, j' \in \mathcal{L} \setminus \{j_1, ..., j_r\}$. We assume without loss of generality that $z < z'$. By the same argument as in [14] we need to show that $\beta^{-j} + \beta^{-N(z-z')-j'}$ is invertible. With $1 \leq z, z' \leq \mu$ and $0 \leq j, j' \leq N-1$ we get

$$N(z'-z) + j' - j \geq N + j' - j \geq N - (N-1) > 0$$

and

$$N(z'-z) + j' - j \leq N(\mu-1) + N - 1 = N\mu - 1 < \mathcal{O}(\beta) .$$

Combining these we get $1 \leq N(z'-z) + j' - j \leq N\mu - 1$, so

$$N(z'-z) + j' - j \neq 0 \mod \mathcal{O}(\beta)$$

and it follows that $\beta^{-j} \oplus \beta^{-N(z-z')-j'}$ is invertible. □

With these generalizations of [14, Construction A/B] we are now ready to construct PMDS and SD codes, where each local code is a d-MSR code.

Construction 1 (Locally d-MSR PMDS/SD array codes)**.** *Let $s = 2$ and $q, \mu, n, r, d, N \in \mathbb{Z}_{>0}$ be positive integers with*

- $r \leq n$
- *q a power of* 2
- $q \geq \max\{\mu N, bn\}$, *where* $b = d + 1 - (n - r)$
- $\ell = b^n$

For an element $\beta \in \mathbb{F}_q$ with $\mathcal{O}(\beta) \geq \max\{\mu N, nb\}$ denote $\beta_{i,j} = \beta^{i-1+(j-1)n}, 1 \leq i \leq n, 1 \leq j \leq b$.

We define the following $[\mu n, \mu(n-r)-2; \ell]_{q^M}$ array code $\mathcal{C}(\mu, n, r, 2, N, d; \ell)_q$ as

$$\left\{ \mathbf{C} = \begin{bmatrix} \mathbf{c}^{(0)} \\ \mathbf{c}^{(1)} \\ \vdots \\ \mathbf{c}^{(\ell-1)} \end{bmatrix} \in \mathbb{F}_q^{\ell \times \mu n} \, : \, \mathbf{H}^{(a)} \mathbf{c}^{(a)} = \mathbf{0} \, \forall \, a = 0, \dots, \ell - 1 \right\},$$

The matrix $\mathbf{H}^{(a)}$ *is defined as*

$$\mathbf{H}^{(a)} = \begin{bmatrix} \mathbf{H}_0^{(a)} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0^{(a)} & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \dots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0^{(a)} \\ \mathbf{H}_1^{(a)} & \mathbf{H}_2^{(a)} & \dots & \mathbf{H}_\mu^{(a)} \end{bmatrix} \in \mathbb{F}_q^{r\mu+2\times\mu n} ,$$

where

$$\mathbf{H}_0^{(a)} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \beta_{1,a_1} & \beta_{2,a_2} & \dots & \beta_{n,a_n} \\ \vdots & \vdots & & \vdots \\ \beta_{1,a_1}^{r-1} & \beta_{2,a_2}^{r-1} & \dots & \beta_{n,a_n}^{r-1} \end{bmatrix} \in \mathbb{F}_q^{r\times n} , \tag{2}$$

with $a \in [0, \ell-1]$ *and* $a = \sum_{i=1}^{n} a_i b^{i-1}$. *For* $0 \le j \le \mu-1$ *let*

$$\mathbf{H}_{j+1}^{(a)} = \begin{bmatrix} \beta_{1,a_1}^{r} & \beta_{2,a_2}^{r} & \dots & \beta_{n,a_n}^{r} \\ \beta^{-jN}\beta_{1,a_1}^{-1} & \beta^{-jN}\beta_{2,a_2}^{-1} & \dots & \beta^{-jN}\beta_{n,a_n}^{-1} \end{bmatrix} \in \mathbb{F}_q^{2\times n} .$$

It remains to show that the local codes are MSR codes and the conditions under which the code is a PMDS or SD code.

Theorem 1. *Let* μ, n, r, d *be fixed and* $q \ge \max\{\mu N, bn\}$ *with*

$$N = (r+1)(rn-1-r)+1 .$$

Then the code $\mathcal{C}(\mu, n, r, 2, N, d; \ell)_q$ *as in Construction 1 is a locally* d*-MSR* $\mathsf{PMDS}(\mu n, \mu, n, r, 2; b^n)$ *code over* $\mathbb{F}_q$*, as in Definition 3.*

Proof. First, note that the $\beta_{i,j}$ in Construction 1 are the (distinct) elements $\beta^0, \beta^1, ..., \beta^{rn-1}$. Now consider the j-th local group. The a-th row fulfills the parity check equations given in (2) and since all elements $\beta_{i,j}$ are distinct, it is immediate that the local group is an $[n, n-r; b^n]$ Ye-Barg code as in Definition 4.

For the PMDS property, observe that the a-th row, i.e., the row fulfilling the parity-check equations $\mathbf{H}^{(a)}$, is a code $\mathcal{C}(\mu, n, r, 2, \mathcal{L}^{(a)}, N)$ as in Section III-A, where $\mathcal{L}^{(a)} = \{i - 1 + (a_i - 1)n \mid i \in [n]\}$ by definition of the $\beta_{i,j}$. For any a it holds that

$$\max_{i\in\mathcal{L}^{(a)}} i \le \max_{\substack{i\in\mathcal{L}^{(a)} \\ a\in[0,\ell-1]}} i = rn-1 .$$

By Lemma 1 a code as in Section III-A is PMDS if $N \ge (r+1)(\max_{i\in\mathcal{L}} i - r) + 1$ and the lemma statement follows. □

Theorem 2. *Let* μ, n, r, d *be fixed and* $q \ge \max\{rn\mu, bn\}$. *Then the code* $\mathcal{C}(\mu, n, r, 2, rn, d; \ell)_q$ *as in Construction 1 is a locally* d*-MSR* $\mathsf{SD}(\mu n, \mu, n, r, s; b^n)$ *code over* $\mathbb{F}_q$.

Proof. The proof follows immediately from the proof of Theorem 1 and Lemma 2. □

IV. PMDS CODES WITH LOCAL REGENERATION AND ANY NUMBER OF GLOBAL PARITIES

We now consider the more general problem of constructing locally d-MSR PMDS and SD codes for any number of local and global parities, based on the construction of PMDS and SD codes in [15] and the construction of d-MSR codes in [10].

A. Recapitulation and Generalization of the PMDS Construction in [15, Section III]

We first rephrase the construction of the PMDS codes of [15, Section III] in our notation and slightly generalize it.

Let q be a prime power and M be a positive integer. Furthermore, let $\mathbf{H}_0 \in \mathbb{F}_q^{r\times n}$ be a parity-check matrix of an $[n, n-r]_q$ MDS code and $\alpha_{i,j}$ be elements of the extension field $\mathbb{F}_{q^M}$ for $i = 1, \dots, \mu$ and $j = 1, \dots, n$. We write $\Gamma := (\alpha_{1,1}, \alpha_{1,2}, ..., \alpha_{\mu,n})$. The $[\mu n, \mu(n-r)-s]$ code $\mathcal{C}(\mu, n, r, s, \mathbf{H}_0, \Gamma)$ is given by the $(r\mu+s)\times\mu n$ parity-check matrix

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_0 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \dots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0 \\ \mathbf{H}_1 & \mathbf{H}_2 & \dots & \mathbf{H}_\mu \end{bmatrix}$$

where for $1 \le j \le \mu$,

$$\mathbf{H}_j = \begin{bmatrix} \alpha_{j,1} & \alpha_{j,2} & \dots & \alpha_{j,n} \\ \alpha_{j,1}^{q} & \alpha_{j,2}^{q} & \dots & \alpha_{j,n}^{q} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{j,1}^{q^{s-1}} & \alpha_{j,2}^{q^{s-1}} & \dots & \alpha_{j,n}^{q^{s-1}} \end{bmatrix} .$$

Whether this code is PMDS/SD depends on the choice of Γ. In [15] the authors present multiple methods of finding such a sequence and in this work we will focus on their main result given in [15, Section IV-A].

The original construction in [15] used for $\mathbf{H}_0$ a parity-check matrix of a specific Reed–Solomon code. It can be seen from the proof of [15, Lemma 2] that this restriction is not necessary in general and that an arbitrary MDS parity-check matrix gives a PMDS code as well. This slight generalization is necessary for the construction in the next subsection.

B. New Construction of d-MSR PMDS Array Codes

In the following, we construct PMDS array codes, in which each row constitutes a, possibly different, PMDS code as in [15] (cf. Subsection IV-A) and the local array codes are Ye–Barg codes [10].

Construction 2. *Let* q, M, μ, n, r, s, d *be positive integers where*

- $r \le n$
- $s \le (n-r)\mu$
- q *a prime power*
- $q \ge bn$, *where* $b = d+1-(n-r)$
- $\ell = b^n$.

Let $\mathbb{F}_q$ *be a finite field and let* $\alpha_{i,j} \in \mathbb{F}_{q^M}$ *for* $i = 1, \dots, \mu$ *and* $j = 1, \dots, n$, *and write* $\Gamma := (\alpha_{1,1}, \alpha_{1,2}, \dots, \alpha_{\mu,n})$. *Furthermore, let* $\beta_{i,j}$ *for* $i = 1, \dots, n$ *and* $j = 1, \dots, b$ *be distinct elements of* $\mathbb{F}_q$ *and write* $\mathcal{B} := (\beta_{1,1}, \beta_{1,2}, \dots, \beta_{n,b})$.

We define the following $[\mu n, \mu(n-r)-s; \ell]_{q^M}$ *array code* $\mathcal{C}(\mu, n, r, s, d, \mathcal{B}, \Gamma; \ell)_{q^M}$ *as*

$$\left\{ \mathbf{C} = \begin{bmatrix} \mathbf{c}^{(0)} \\ \mathbf{c}^{(1)} \\ \vdots \\ \mathbf{c}^{(\ell-1)} \end{bmatrix} \in \mathbb{F}_{q^M}^{\ell\times\mu n} \,:\, \mathbf{H}^{(a)}\mathbf{c}^{(a)} = \mathbf{0} \,\forall\, a = 0, \dots, \ell-1 \right\},$$

where the matrix $\mathbf{H}^{(a)}$ *is defined as*

$$\mathbf{H}^{(a)} := \begin{bmatrix} \mathbf{H}_0^{(a)} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0^{(a)} & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \dots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0^{(a)} \\ \mathbf{H}_1 & \mathbf{H}_2 & \dots & \mathbf{H}_\mu \end{bmatrix} \in \mathbb{F}_{q^M}^{r\mu+s\times\mu n} ,$$

and for each $a \in [0, \ell-1]$ *with* $a = \sum_{i=1}^{n} a_i b^{i-1}$, *we have*

$$\mathbf{H}_0^{(a)} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \beta_{1,a_1} & \beta_{2,a_2} & \dots & \beta_{n,a_n} \\ \vdots & \vdots & & \vdots \\ \beta_{1,a_1}^{r-1} & \beta_{2,a_2}^{r-1} & \dots & \beta_{n,a_n}^{r-1} \end{bmatrix} \in \mathbb{F}_q^{r\times n} , \tag{3}$$

Further, for $1 \le j \le \mu$, *define*

$$\mathbf{H}_j := \begin{bmatrix} \alpha_{j,1} & \alpha_{j,2} & \dots & \alpha_{j,n} \\ \alpha_{j,1}^{q} & \alpha_{j,2}^{q} & \dots & \alpha_{j,n}^{q} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{j,1}^{q^{s-1}} & \alpha_{j,2}^{q^{s-1}} & \dots & \alpha_{j,n}^{q^{s-1}} \end{bmatrix} \in \mathbb{F}_{q^M}^{s\times n}.$$

By the choice of the $\beta_{i,j}$, the local codes of the codes given by Construction 2 are Ye–Barg codes. As in [15], we need to choose the vector Γ in a suitable way to obtain PMDS array codes.

Lemma 3. *Let $\alpha_{1,1},\dots,\alpha_{\mu,n}$ be chosen such that any subset of $(r+1)s$ elements of the $\alpha_{i,j}$ is linearly independent over $\mathbb{F}_q$. Then, $\mathcal{C}(\mu,n,r,s,d,\mathcal{B},\Gamma;\ell)_{q^M}$ from Construction 2 is a d-MSR PMDS array code.*

Proof. The proof combines the ideas of [15, Lemma 2], [15, Corollary 5], and [15, Lemma 7]. Let

$$\mathbf{C}=\begin{bmatrix} \mathbf{c}_1^{(0)} & \mathbf{c}_2^{(0)} & \dots & \mathbf{c}_\mu^{(0)} \\ \mathbf{c}_1^{(1)} & \mathbf{c}_2^{(1)} & \dots & \mathbf{c}_\mu^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{c}_1^{(\ell-1)} & \mathbf{c}_2^{(\ell-1)} & \dots & \mathbf{c}_\mu^{(\ell-1)} \end{bmatrix} \in \mathbb{F}_{q^M}^{\ell\times\mu n}$$

be a codeword of $\mathcal{C}(\mu,n,r,s,\mathcal{L},\delta,\Gamma)$ (here, we group the rows of the codeword in blocks of length n, i.e., $\mathbf{c}_i^{(a)}\in\mathbb{F}_{q^M}^n$). By definition, for all $i=1,\dots,\mu$ and $a=0,\dots,\ell-1$, we have

$$\mathbf{H}^{(a)}{\mathbf{c}_i^{(a)}}^\top=\mathbf{0}, \tag{4}$$

where $\mathbf{H}^{(a)}$ is the parity-check matrix of an $[n,n-r]$ MDS code. Furthermore, with $\boldsymbol{\alpha}_i:=[\alpha_{i,1},\alpha_{i,2},\dots,\alpha_{i,n}]$, we have

$$\sum_{i=1}^{\mu}\boldsymbol{\alpha}_i^{q^j}{\mathbf{c}_i^{(a)}}^\top=0, \tag{5}$$

for all $j=0,\dots,s-1$ and $a=0,\dots,\ell-1$.

Let $S:=[\mathbf{s}_1,\dots,\mathbf{s}_\mu]$ be of the form

$$\mathbf{s}_i=[s_{i,1},\dots,s_{i,r}]\in[n]^r,\quad s_{i,1}<s_{i,2}<\dots<s_{i,r}.$$

Denote by $\bar{\mathbf{s}}_i$ the vector in $[n]^{n-r}$ that contains, again in increasing order, the entries of $[n]$ that are not contained in $\mathbf{s}_i$. The positions $\mathbf{s}_i$ correspond to the puncturing patterns E_i in the definition of PMDS array codes (cf. Definition 1). We need to show that for each such vector S, the array code punctured at these positions in each local group, gives an $[n-r\mu,n-r\mu-s;\ell]$ MDS array code.

For a vector $\mathbf{x}$ of length n, let $\mathbf{x}_{\mathbf{s}_i}$ and $\mathbf{x}_{\bar{\mathbf{s}}_i}$ be the vectors of length r and $n-r$ containing the entries of $\mathbf{x}$ indexed by the entries of $\mathbf{s}_i$ and $\bar{\mathbf{s}}_i$, respectively. Furthermore, for a vector $\mathbf{y}=[\mathbf{y}_1,\dots,\mathbf{y}_\mu]$ of length $n\mu$, let $\mathbf{y}^S$ denote the puncturing of $\mathbf{y}$ at all entries of S, i.e.,

$$\mathbf{y}^S=\big[(\mathbf{y}_1)_{\bar{\mathbf{s}}_1},\dots,(\mathbf{y}_\mu)_{\bar{\mathbf{s}}_\mu}\big].$$

Let $\mathbf{H}$ be a parity-check matrix of an MDS code of length n and dimension $n-r$. Then, the columns of $\mathbf{H}$ indexed by $\mathbf{s}_i$, denoted by $\mathbf{H}_{\mathbf{s}_i}$, are invertible and we have for any codeword $\mathbf{x}$ of the code

$$\mathbf{0}=\mathbf{H}\mathbf{x}^\top=\mathbf{H}_{\mathbf{s}_i}\mathbf{x}_{\mathbf{s}_i}^\top+\mathbf{H}_{\bar{\mathbf{s}}_i}\mathbf{x}_{\bar{\mathbf{s}}_i}^\top\quad\Rightarrow\quad\mathbf{x}_{\mathbf{s}_i}^\top=\mathbf{H}_{\mathbf{s}_i}^{-1}\mathbf{H}_{\bar{\mathbf{s}}_i}\mathbf{x}_{\bar{\mathbf{s}}_i}^\top$$

Hence, it directly follows from (4) that

$${(\mathbf{c}_i)_{\mathbf{s}_i}^{(a)}}^\top={\mathbf{H}_{\mathbf{s}_i}^{(a)}}^{-1}\mathbf{H}_{\bar{\mathbf{s}}_i}^{(a)}(\mathbf{c}_i)_{\bar{\mathbf{s}}_i}^\top,$$

and by (5) that (note that $\mathbf{H}^{(a)}$ has entries in $\mathbb{F}_q$, so $\mathbf{H}^{(a)}=\mathbf{H}^{(a)^{q^j}}$ for any j)

$$\begin{aligned}0&=\sum_{i=1}^{\mu}\boldsymbol{\alpha}_i^{q^j}{\mathbf{c}_i^{(a)}}^\top=\sum_{i=1}^{\mu}(\boldsymbol{\alpha}_i)_{\mathbf{s}_i}^{q^j}{(\mathbf{c}_i)_{\mathbf{s}_i}^{(a)}}^\top+(\boldsymbol{\alpha}_i)_{\bar{\mathbf{s}}_i}^{q^j}{(\mathbf{c}_i)_{\bar{\mathbf{s}}_i}^{(a)}}^\top\\&=\sum_{i=1}^{\mu}\Big[\underbrace{(\alpha_i)_{\mathbf{s}_i}\mathbf{H}_{\mathbf{s}_i}^{(a)}{}^{-1}\mathbf{H}_{\bar{\mathbf{s}}_i}^{(a)}+(\alpha_i)_{\bar{\mathbf{s}}_i}}_{=:\boldsymbol{\gamma}_{\mathbf{s}_i}^{(a)}}\Big]^{q^j}{(\mathbf{c}_i)_{\bar{\mathbf{s}}_i}^{(a)}}^\top.\end{aligned}$$

Thus, the vector $\mathbf{c}^S=\big[(\mathbf{c}_1)_{\bar{\mathbf{s}}_1}^{(a)},(\mathbf{c}_2)_{\bar{\mathbf{s}}_2}^{(a)},\dots,(\mathbf{c}_\mu)_{\bar{\mathbf{s}}_\mu}^{(a)}\big]$, which is the a-th row of a codeword punctured at the positions in S, is contained in a code with parity-check matrix

$$\mathbf{H}_\gamma^{(a)}:=\begin{bmatrix}\boldsymbol{\gamma}_S^{(a)^{q^0}}\\ \boldsymbol{\gamma}_S^{(a)^{q^1}}\\ \vdots\\ \boldsymbol{\gamma}_S^{(a)^{q^{s-1}}}\end{bmatrix},$$

where

$$\boldsymbol{\gamma}_S^{(a)}:=\Big[\boldsymbol{\gamma}_{\mathbf{s}_1}^{(a)},\boldsymbol{\gamma}_{\mathbf{s}_2}^{(a)},\dots,\boldsymbol{\gamma}_{\mathbf{s}_\mu}^{(a)}\Big]\in\mathbb{F}_{q^M}^{\mu(n-r)}.$$

By definition, we have

$$\boldsymbol{\gamma}_{\mathbf{s}_i}^{(a)}=(\alpha_i)_{\mathbf{s}_i}{\mathbf{H}_{\mathbf{s}_i}^{(a)}}^{-1}\mathbf{H}_{\bar{\mathbf{s}}_i}^{(a)}+(\alpha_i)_{\bar{\mathbf{s}}_i}.$$

Since ${\mathbf{H}_{\mathbf{s}_i}^{(a)}}^{-1}\mathbf{H}_{\bar{\mathbf{s}}_i}^{(a)}$ is an $r\times(n-r)$ matrix, each entry of $\boldsymbol{\gamma}_{\mathbf{s}_i}^{(a)}$, and thus each entry of $\boldsymbol{\gamma}_S^{(a)}$, is linear combination of at most $r+1$ of the $\alpha_{i,j}$. Furthermore, each such linear combination contains, non-trivially, one element from $\alpha_{i,j}$ (namely the corresponding entry in $(\alpha_i)_{\bar{\mathbf{s}}_i}$) that appears only in this linear combination. Any set of s entries from $\boldsymbol{\gamma}_S^{(a)}$ depend on at most $s(r+1)$ of the $\alpha_{i,j}$, which are linearly independent by the independence assumption. Hence, the s entries from $\boldsymbol{\gamma}_S^{(a)}$ are also linearly independent over $\mathbb{F}_q$. This means that any s columns of the parity-check matrix $\mathbf{H}_\gamma^{(a)}$ are linearly independent and $\mathbf{H}_\gamma^{(a)}$ is a parity-check matrix of an $[n\mu-r\mu,n\mu-r\mu-s]_{q^M}$ MDS code. Thus, the overall code is a PMDS array code.

It remains to show that the local codes are d-MSR codes. The proof is equivalent to the proof of the locally d-MSR property of Theorem 1. First, note that the $\beta_{i,j}$ in Construction 2 are the (distinct) elements $\beta^0,\beta^1,...,\beta^{rn-1}$. Now consider the j-th local array code. The a-th row fulfills the parity check equations given in (3) and since all elements $\beta_{i,j}$ are distinct, it is immediate that the local group is an $[n,n-r;b^n]$ Ye-Barg d-MSR code as in Definition 4. □

Similar to Construction 1 in the previous section, we give the following upper bound on the minimal field size for which d-MSR PMDS codes of the form as in Construction 2 exist.

Theorem 3. *Let μ,n,r,s be fixed. There is a d-MSR PMDS array code as in Construction 2 of field size*

$$q^M\le 2n(d+1-(n-r))(2n\mu)^{s(r+1)-1}$$

and subpacketization

$$\ell=\big[d+1-(n-r)\big]^n.$$

Proof. We choose q and M large enough such that we can ensure that suitable sequences $\alpha_{i,j}$ and $\beta_{i,j}$ exist. A sufficient condition for the existence of the $\beta_{i,j}$ is $q\ge n(d+1-(n-r))$. Thus, we can choose q to be the smallest prime power greater or equal to $n(d+1-(n-r))$, which is at most $q\le 2n(d+1-(n-r))$ by Bertrand's postulate.

For the $\alpha_{i,j}$, it is a bit more involved. By Lemma 3, it suffices to find $n\mu$ elements from $\mathbb{F}_{q^M}$ of which any subset of $s(r+1)$ elements is linearly independent. We use the same idea as in [15, Lemma 7]: take the columns of a parity-check matrix of a $\mathcal{C}[n\mu,n\mu-M,s(r+1)+1]_q$ code and interpret each column $\mathbb{F}_q^M$ as an element of $\mathbb{F}_{q^M}$. The independence condition is then fulfilled due to the choice of minimum distance.

The remaining question is for which M and q a code with parameters $[n\mu,n\mu-M,s(r+1)+1]_q$ exists. We use the result in [19, Problem 8.9], which we can reformulate in our terms as: For any $n'=q^a-1$, there exists a code with parameters $[n',n'-M,s(r+1)+1]_q$, where

$$M\le 1+\big[s(r+1)-1\big]a.$$

Choose a to be the smallest integer with $n'=q^a-1\ge n\mu$. Note that there is such an a with $q^a-1\le 2n\mu-1$, i.e., $a\le\log_q(2n\mu)$. Hence, there is an $[n',n'-M,s(r+1)+1]_q$ code with $M\le 1+\big[s(r+1)-1\big]\log_q(2n\mu)$. Shortening the codes gives an $[n\mu,n\mu-M,s(r+1)+1]_q$ code with $M\le 1+\big[s(r+1)-1\big]\log_q(2n\mu)$. □

REFERENCES

[1] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, "On the locality of codeword symbols," *IEEE Transactions on Information theory*, vol. 58, no. 11, pp. 6925–6934, 2012.

[2] G. M. Kamath, N. Prakash, V. Lalitha, and P. V. Kumar, "Codes with local regeneration and erasure correction," *IEEE Transactions on information theory*, vol. 60, no. 8, pp. 4637–4660, 2014.

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

[4] M. N. Krishnan, A. Narayanan R, and P. V. Kumar, "Codes with Combined Locality and Regeneration Having Optimal Rate, $d_{\min}$ and Linear Field Size," in *2018 IEEE International Symposium on Information Theory (ISIT)*. IEEE, jun 2018, pp. 1196–1200. [Online]. Available: https://ieeexplore.ieee.org/document/8437455/

[5] D. Gligoroski, K. Kralevska, R. E. Jensen, and P. Simonsen, "Locally repairable and locally regenerating codes obtained by parity-splitting of Hashtag codes," *CoRR, vol. abs/1701.06664*, 2017.

[6] H. D. Hollmann, "On the minimum storage overhead of distributed storage codes with a given repair locality," in *2014 IEEE International Symposium on Information Theory*. IEEE, 2014, pp. 1041–1045.

[7] M. Li, R. Li, and P. P. Lee, "Relieving both storage and recovery burdens in big data clusters with R-STAIR codes," *IEEE Internet Computing*, 2016.

[8] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE transactions on information theory*, vol. 56, no. 9, pp. 4539–4551, 2010.

[9] V. R. Cadambe, S. A. Jafar, H. Maleki, K. Ramchandran, and C. Suh, "Asymptotic interference alignment for optimal repair of MDS codes in distributed storage," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2974–2987, 2013.

[10] M. Ye and A. Barg, "Explicit constructions of high-rate MDS array codes with optimal repair bandwidth," *IEEE Transactions on Information Theory*, vol. 63, no. 4, pp. 2001–2014, 2017.

[11] I. Tamo, D. S. Papailiopoulos, and A. G. Dimakis, "Optimal locally repairable codes and connections to matroid theory," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 6661–6671, 2016.

[12] L. Holzbaur, S. Puchinger, and A. Wachter-Zeh, "Error decoding of locally repairable and partial MDS codes," 2019.

[13] M. Blaum, J. L. Hafner, and S. Hetzler, "Partial-MDS codes and their application to raid type of architectures," *IEEE Transactions on Information Theory*, vol. 59, no. 7, pp. 4510–4519, 2013.

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

[15] R. Gabrys, E. Yaakobi, M. Blaum, and P. H. Siegel, "Constructions of partial MDS codes over small fields," *IEEE Transactions on Information Theory*, vol. 65, no. 6, pp. 3692–3701, 2018.

[16] M. Chen, C. Huang, and J. Li, "On the maximally recoverable property for multi-protection group codes," in *2007 IEEE International Symposium on Information Theory*. IEEE, 2007, pp. 486–490.

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

[18] G. Calis and O. O. Koyluoglu, "A general construction for PMDS codes," *IEEE Communications Letters*, vol. 21, no. 3, pp. 452–455, 2016.

[19] R. Roth, *Introduction to coding theory*. Cambridge University Press, 2006.