Partial MDS Codes with Regeneration

Lukas Holzbaur, *Student Member, IEEE*, Sven Puchinger, *Member, IEEE*,
Eitan Yaakobi, *Senior Member, IEEE*, and Antonia Wachter-Zeh, *Senior Member, IEEE*

Abstract—**Partial MDS (PMDS) and sector-disk (SD) codes are classes of erasure correcting codes that combine locality with strong erasure correction capabilities. We construct PMDS and SD codes with local regeneration where each local code is a bandwidth-optimal regenerating MDS code. In the event of a node failure, these codes reduce both, the number of servers that have to be contacted as well as the amount of network traffic required for the repair process. The constructions require significantly smaller field size than the only other construction known in literature. Further, we present a construction of PMDS codes with global regeneration which allow to efficiently repair patterns of node failures that exceed the local erasure correction capability of the code and thereby invoke repair across different local groups.**

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) [2], [3], [4], [5], [6], [7], [8] and *regenerating codes* [9], [10], [11] have been introduced.

To lower the amount of network traffic in recovery, and thereby the required bandwidth, 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 bandwidth, i.e., the amount of data that needs to be transmitted for the recovery of a number of failed nodes. Lower bounds on the required bandwidth for repair have been derived in [9], [10] 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 bandwidth, but at the cost of increased storage overhead compared to MDS codes. In this work we consider d-MSR codes, which require a higher bandwidth 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 [12], [13]. *Partial MDS* (PMDS) *codes* [14], [15], [16], also referred to as *maximally recoverable codes* [17], [18], 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 requires substantial network bandwidth, as the entire content of the helper nodes needs to be downloaded when considering straight-forward use recovery algorithms. To circumvent this bottleneck, several locally regenerating codes [9] have been proposed [3], [4], [5], [6], [7], [8]. In [19] it was shown that the LRC construction of [4] 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 and the subpacketization of the local regenerating code (which may itself be exponential in the length of the local code). In the first part of this paper, we propose several constructions of locally MSR PMDS codes with significantly smaller field size than the construction in [4].

In the second part of this work, we consider PMDS codes with global regeneration properties that offer non-trivial repair schemes for the case where local recovery is not possible. Specifically, we give a PMDS code construction that, when punctured in any r positions in each local group, becomes an MSR code. The reduction in global repair bandwidth is of particular interest, as the bandwidth of connections between nodes of different local groups is often assumed to be smaller than of nodes within the same local groups. Accordingly, though being less likely to occur, the non-local repair of a larger number of erasures can take a substantial amount of time. Repair problems where the communication cost within a local group differs from the cost of communication between local groups have been studied in [20], [21], [22], [23] and, in particular, the notion of *rack-aware regenerating codes* (RRCs) [24], [25] has been introduced. In this setting, the nodes are partitioned into a smaller number of racks, similar to the partitioning of nodes for codes with locality. Under this model, when a (number of) node(s) fails within a rack, it is regenerated by transmitting from each rack a function of the content of its nodes. The distinction to regenerating codes is that the repair bandwidth is given measured in terms of the amount of data transmitted *between* the racks, while communication within each rack is ignored. Aside from this definition of the repair bandwidth, there are two important differences to the model we consider: 1) RRCs require a node that collects the data from the nodes within the rack and computes a function of it that is to be transmitted and 2) RRCs generally *do not have locality*, i.e., no repair is possible within each rack. *Double regenerating codes* [26] refine this model by considering two levels of regeneration, a local one, i.e., within the racks, and a global one, i.e., across the racks. A sightly different model has been considered in [27], in which repair is conducted by downloading a number of symbols from helper racks (also called clusters) and additionally a number of symbols is downloaded from a set of nodes of the same rack, where, unlike for RRCs, both contribute to the overall repair bandwidth. Similar to RCCs, the codes under this model do not have locality.

A rack-aware setting that also considers local recovery from node failures are codes for *multi-rack distributed storage* [28], [29]. There, a small number of nodes can be repaired/regenerated locally and failure patterns for which this is not possible are repaired by contacting other racks in addition to the surviving local nodes. Similar to RRCs, it

is assumed that the contacted helper racks can process the data of the nodes within the rack and that the communication between racks is more costly than within a rack. Along with an information-theoretic bound, [29] presents a construction for the case of an efficient local repair of a single node failure. The minimization of the cross-rack repair bandwidth is stated as an open problem. In [28] the authors consider a more general setting which improves both, the repair bandwidth within a rack in case of a small number of failure and across racks for failure patterns that cannot be repaired locally. Similar to RRCs, this model differs from the one in this work in that racks are able to process the data from their nodes prior to sending it to other racks. Additionally, we consider a stronger notion of locality in requiring the storage code to be PMDS.

The work with closest relation to the model of global regeneration in codes with locality that we consider is [6], which introduces local redundancy by splitting parity-check equations of HashTag codes [30], [31], [32]. While it is shown that the codes are distance-optimal LRCs, they are generally not PMDS codes and possess only information locality, i.e., the recovery from a small subset of positions is only guaranteed for a set of systematic positions. Further, as the construction of HashTag codes [30], [31] is not explicit, but partially relies on computer search, the construction of these parity-split HashTag codes with locality [6] also partially relies on computer search.

A. Contributions and Outline

In Section III, we construct a new PMDS code with two global parities ($s = 2$), where each local code is a d-MSR code. The construction is a non-trivial combination of the PMDS codes in [15] with the MSR codes in [11]. This PMDS code construction is based on Reed-Solomon codes and only defined for a specific set of code locators. We generalize this construction to accept arbitrary code locators, which enables us to combine it with the MSR codes of [11]. This construction has field size in the order of

$$O(\mu r^2 n).$$

In Section IV, we present a new general construction of locally MSR PMDS codes for any number of global parities. The construction is based on the observation that any universal PMDS code (that is, the local codes can be chosen almost arbitrarily) can be combined with a specific subclass of MSR codes, namely, MSR codes for which each row is an MDS code, to obtain locally MSR PMDS codes. The main contribution in this part of the work is the recognition of the interplay of these properties, both of which received little attention in the literature so far. This immediately leads to several new explicit locally MSR PMDS codes using known universal PMDS code families and the MSR codes in [11]: the PMDS codes in [4] result in a field size in the order of

$$O\big((rn)^{\mu(n-r)}\big)$$

and the ones in [33] give a field size in

$$O\big(\max\{rn, \mu + 1\}\big)^{n-r}\big).$$

We also slightly generalize the PMDS code family in [16] and prove that this generalization in fact gives a universal PMDS

---

[1]The construction in [4] consists of two encoding stages, where in the second stage an arbitrary linear MDS code can be used to obtain the local codes. In [19] 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.

code. The resulting field size of the corresponding locally MSR PMDS code is in

$$O(nr(2n\mu)^{s(r+1)-1}).$$

All new locally MSR PMDS codes have the same subpacketization as the underlying MSR code from [11].

In Section V, we analyze the field size of the new constructions of locally MSR PMDS codes. For the two-global-parities construction and the universal construction with the PMDS codes in [33] and [16], there is a reasonable parameter range in which the respective construction has lowest field size among all known constructions. Moreover, for all parameters, there is a new construction that has a smaller field size than the known construction in [4].

In Section VI, we propose the first known construction of globally MSR PMDS codes (that is, the MDS code obtained from puncturing r positions in each local group is an MSR code), which allows for a significant reduction in the repair bandwidth in case a global repair event is triggered. To achieve this, we introduce a new MSR code construction based on [11] which utilizes Gabidulin instead of Reed-Solomon codes and prove that it is in fact an MSR code. This allows for building PMDS codes with regenerating properties in a similar fashion as the Gabidulin-code-based PMDS code construction (without regeneration) in [4]. The involved part for retaining the MSR property for any puncturing of r positions in each local group is the choice of evaluation points of these Gabidulin codes. We present an explicit choice based on pairwise trivially intersecting subspaces and prove that it fulfills the required property for any such puncturing pattern. The resulting code has a field size in $O(n^{\mu(n+s)})$ and subpacketization in $O((8n)^{\mu n(n+s)})$.

II. Preliminaries

A. Notation

We write $[a, b]$ for the set of integers $\{a, a + 1, \ldots, b\}$ 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 $\mathcal{O}(\alpha)$. For an $a \times b$ matrix $\mathbf{B}$ we denote by $\mathbf{B}_{i,j}$ the entry in the i-th row and j-th column. For the i-th row/column we write $\mathbf{B}_{i,:}$ and $\mathbf{B}_{:,i}$, respectively. For a set $\mathcal{S} \subset [b]$, we denote by $\mathbf{B}_{\mathcal{S}}$ the restriction of the matrix $\mathbf{B}$ to the columns indexed by $\mathcal{S}$. We denote the Gaussian binomial coefficient, i.e., the number of k-dimensional subspaces of $\mathbb{F}_q^n$, by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{cases} \frac{(1-q^n)(1-q^{n-1})\ldots(1-q^{n-k+1})}{(1-q)(1-q^2)\ldots(1-q^k)}, & k \leq n, \\ 0, & k > n. \end{cases}$$

We denote a linear code of length n, dimension k, and distance $d_{\min}$ over a field $\mathbb{F}_q$ by $[n, k, d_{\min}]_q$. If the field size or minimum distance is not relevant, we sometimes omit the respective parameters and write $[n, k]$, $[n, k]_q$, or $[n, k, d_{\min}]$. Similarly, an $[n, k]$ RS code denotes a Reed–Solomon code of length n, dimension k and minimum distance $n - k + 1$ over a sufficiently large field. For a code over $\mathbb{F}_{q^\ell}$ that is linear over $\mathbb{F}_q$ we write $[n, k, d_{\min}; \ell]_q$, $[n, k, d_{\min}; \ell]$, or $[n, k; \ell]$, respectively. 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*.

This work is largely based on the constructions of PMDS codes by Rawat *et al.* [4], Blaum *et al.* [15] and Gabrys *et al.* [16], Martínez-Peñas–Kschischang [33], and the construction of MSR codes by Ye and Barg in [11]. 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.

B. Definitions

All code construction presented in the following are vector codes, where each row is an arbitrary codeword of a specific code. To keep the presentation compact, we define a notation for the special case of the code being the same in each row.

Definition 1. *For a linear $[n, k, d_{\min}]$ code $\mathcal{C}$ over $\mathbb{F}_q$ we denote by*

$$\mathcal{C}^{\times \ell} = \underbrace{\mathcal{C} \times \cdots \times \mathcal{C}}_{\ell \ times}$$

the ℓ-fold Cartesian product of the code $\mathcal{C}$ with itself arranged as an $\ell \times n$ matrix, i.e., the set

$$\mathcal{C}^{\times \ell} = \left\{ \mathbf{C} \in \mathbb{F}_q^{\ell \times n} \mid \mathbf{C}_{i,:} \in \mathcal{C} \ \forall \ i \in [\ell] \right\}.$$

It is generally desirable to keep the size of the field in which operations are conducted small. While we have to rely on larger fields to achieve some of the code properties in the following, it can be useful to regard codes over larger fields as array codes over a subfield.

Corollary 1. *Let $\{\gamma_1, \ldots, \gamma_\ell\}$ be a basis of $\mathbb{F}_{q^\ell}$ over $\mathbb{F}_q$ and $\mathcal{C}$ be an $[n, k, d_{\min}]$ code over $\mathbb{F}_q$. Then the code*

$$\left\{ (\gamma_1, \ldots, \gamma_\ell) \cdot \mathbf{C} \mid \mathbf{C} \in \mathcal{C}^{\times \ell} \right\} \simeq \langle \mathcal{C} \rangle_{\mathbb{F}_{q^\ell}}$$

is an $[n, k, d_{\min}]$ code over $\mathbb{F}_{q^\ell}$.

With these basic notions established, we now define the code classes and concepts used in this work, starting with a formal definition of PMDS codes. This special class of LRCs is able to correct all patterns of erasures that are theoretically correctable and thereby provides the strongest possible protection against data loss, given the locality constraints.

Definition 2 (Partial MDS array codes). *Let $n, \mu, r, s, \ell \in \mathbb{Z}_{>0}$ be such that $\mu \geq 2$, $r < n$, and $s \leq (n - r)(\mu - 1)$. Let $\mathcal{W} = \{W_1, W_2, \ldots, W_\mu\}$ be a partition of $[\mu n]$ with $|W_i| = n \ \forall \ i \in [\mu]$.*

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 $\mathsf{PMDS}(\mu, n, r, s, \mathcal{W}; \ell)$ partial MDS array code if

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

TABLE I
AN OVERVIEW OF THE NOTATION USED IN THIS WORK COMPARED TO THE NOTATION USED IN [15], [16], [33], [4], [11]. THE LARGEST BENEFIT FROM THIS COMPARISON IS IN SECTIONS III TO V, WHERE WE CONSTRUCT AND DISCUSS PMDS CODES WITH LOCAL MSR CODES. THEREFORE, THE LENGTH AND NUMBER OF PARITIES IN THE MSR CODE CONSTRUCTION OF [11] ARE MATCHED WITH THE PARAMETERS OF THE LOCAL CODES IN OUR WORK. NOTE THAT, IN OUR NOTATION, THE LENGTH OF THE MSR CODE IN SECTION VI, WHERE WE CONSIDER PMDS CODES WITH GLOBAL REPAIR PROPERTIES, IS $\mu(n-r)$ AND THE NUMBER OF PARITIES IS s.

Description	[15]	[16]	[33]	[4]	[11]	This work
Number of local groups	r	m	g	g	-	μ
Length of local MSR code	n	n	$r+\delta-1$	$r+\delta-1$	n	n
Number of local parity symbols	m	r	$\delta-1$	$\delta-1$	r	r
Number of global parity symbols	s	s	h	$D-1$	-	s
Code length	rn	mn	n	n	-	μn
Subpacketization	-	-	-	α	l	ℓ
Number of nodes needed for repair	-	-	-	d	d	d

We refer to the code $\mathcal{C}|_{W_i}$ as the i-th *local code*. Furthermore, we refer to parameters n, μ, r, s satisfying the constraints of Definition 2 as *valid PMDS parameters*. Note that we exclude trivial parameters for which the definition results simply in an MDS code or a concatenation of MDS codes[2]. The requirement $s \leq (n-r)(\mu-1)$ is necessary for the PMDS code definition since otherwise the dimension of the local code exceeds the one of the global code — a contradiction.

Remark 1. *In [15], [16] each codeword of the PMDS and SD codes is regarded as a $\mu \times n$ 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 [15], [16].*

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. *A Sector-Disk $\mathsf{SD}(\mu, n, r, s, \mathcal{W}; \ell)$ code is defined similar to a PMDS codes as in Definition 2, except that $E_1 = E_2 = \cdots = E_\mu$ holds.*

Definition 3 (Regenerating code [9], [10]). *Let $\mathcal{F}, \mathcal{R} \subset [n]$ be two disjoint subsets. 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 $\mathbb{F}_q$ one needs to download from the surviving nodes indexed by $\mathcal{R}$ to recover the erased nodes indexed by $\mathcal{F}$. Then*

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

For two integers h, d, with $1 \leq h \leq r$ and $n - r \leq d \leq n - h$, we say that the code $\mathcal{C}$ is an (h, d)-MSR code if

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

---

[2]There are several parameter combinations for which such a trivial case occurs. One trivial case is given by $r = 0$ (and arbitrary μ, s) where the code obtained from "puncturing $r = 0$ positions" in each local group, i.e., the unpunctured code, is MDS by the second property of Definition 2. On the other hand, if $s = 0$ (and arbitrary μ, r) the code is just a concatenation of (independent) local MDS codes.
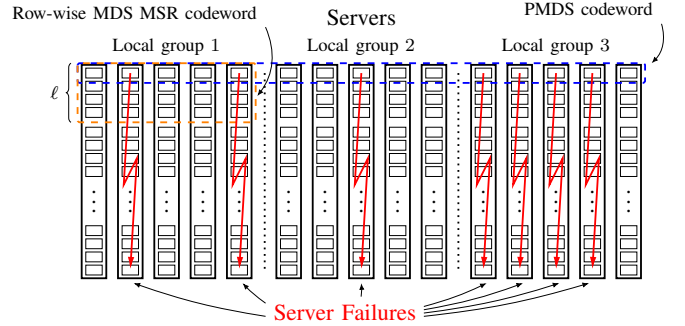

Fig. 1. Illustration of locally MSR PMDS array codes as constructed in this work, with $n = 5$, $\mu = 3$ and each symbol of the code alphabet represented by a small rectangle. The shown erasure pattern can be corrected by an $(r = 2, s = 2)$-PMDS code.

If $h = 1$ we say that the code is a d-MSR code. If in addition, $d = n - 1$, we simply say that the code is an MSR code.

Informally, in a regenerating array code, as in Definition 3, we require that every codeword can be recovered from an arbitrary subset of $n-r$ columns. We now define a slightly stronger property, which contains additionally a similar requirement on every row of a codeword.

Definition 4. *Let $\mathcal{C}$ be an $[n, n-r; \ell]$ regenerating code as in Definition 3. We say that the code $\mathcal{C}$ is a **row-wise MDS regenerating code** if for any $i \in [\ell]$ the set $\{\boldsymbol{C}_{i,:} \mid \boldsymbol{C} \in \mathcal{C}\}$ is an MDS code.*

With these notions established, we combine Definitions 2 and 3 to formally define the class of codes we construct and analyse in Sections III to V.

Definition 5 (Locally (h, d)-MSR PMDS array codes). *Let $\mathcal{C}$ be a $\mathsf{PMDS}(\mu, n, r, s, \mathcal{W}; \ell)$ code and d, h be chosen such that $1 \leq h$ and $n - r \leq d \leq n - h$. 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. If in addition, $d = n - 1$, we simply say that the code is an MSR PMDS code.*

Fig. 1 shows an illustration of a locally MSR 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, while 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.

A globally-MSR PMDS code is formally defined as follows.

Definition 6 (Globally (h,d)-MSR PMDS Code). *Let $\mathcal{C}$ be a $\mathsf{PMDS}(\mu, n, r, s, \mathcal{W}; \ell)$ code and d, h be chosen such that $1 \leq h \leq s$ and $\mu(n-r) - s \leq d \leq \mu(n-r) - h$. We say that the code $\mathcal{C}$ is globally (h,d)-MSR if the restriction $\mathcal{C}|_{[\mu n] \setminus \cup_{i=1}^{\mu} E_i}$ is a $[\mu(n-r), \mu n - r\mu - s, s+1; \ell]$ (h,d)-MSR code for any $E_i \subset W_i$ with $|E_i| = r$ for all $i \in [\mu]$. Again, we say d-MSR if $h = 1$ and simply MSR if in addition $d = \mu(n-r) - 1$.*

Throughout the paper, we consider in all constructions $h = 1$. This is the most interesting case since in a storage system, it is more likely that one node needs to be regenerated than multiple nodes. In the globally-MSR case, we further fix d to be maximal, i.e., $d = \mu(n-r) - 1$. It can be seen from the bound in Definition 3 that the repair bandwidth decreases in d, i.e., it is minimal for this choice of d. See Section VII for a discussion on how the results can be generalized.

C. Ye-Barg Regenerating Codes

We repeat [11, Construction 2] in the slightly different notation which will be used in this work.

Definition 7 (Ye-Barg d-MSR codes [11, 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 $\{\beta_{i,j}\}_{i \in [b], j \in [n]}$ 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 a-th row fulfills the parity check equations*

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

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

It is easy to see that a Ye-Barg code as in Definition 7 is in fact *row-wise MDS d-MSR code*.

Remark 3. *The constructions presented in Sections 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 [11, Construction 3], which is very similar in structure to [11, Construction 2] given in Definition 7. However, as the required subpacketization is larger for the former, we focus on d-MSR codes in this work.*

Remark 4. *In Definition 7 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 [11], 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 thus MDS.

D. Gabidulin Codes

Gabidulin codes [34], [35], [36] are rank-metric codes that have been used repeatedly in the literature to construct LRCs and PMDS codes. They are defined as follows.

Definition 8 (Gabidulin codes). *Let $\mathbf{b} = (\beta_1, \ldots, \beta_n) \in \mathbb{F}_{q^M}^n$ be such that the β_i are linearly independent over $\mathbb{F}_q$. The $[n,k]_{q^M}$ Gabidulin code $\mathsf{Gab}(n,k,\mathbf{b})$ is defined as*

$$\mathsf{Gab}(n,k,\mathbf{b}) = \left\{ \mathbf{c} \in \mathbb{F}_{q^M}^n \mid \mathbf{c} \cdot \mathbf{H}^T = \mathbf{0} \right\}$$

with

$$\mathbf{H} = \begin{bmatrix} \beta_1 & \beta_2 & \cdots & \beta_n \\ \beta_1^{q^1} & \beta_2^{q^1} & \cdots & \beta_n^{q^1} \\ \vdots & \vdots & & \vdots \\ \beta_1^{q^{n-k-1}} & \beta_2^{q^{n-k-1}} & \cdots & \beta_n^{q^{n-k-1}} \end{bmatrix}.$$

Note that the existence of linearly independent β_i implies $n \leq M$. In the paper, we refer to the set $\{\beta_i\}, i \in [n]$ as the *code locators* of the Gabidulin code. Note that, unlike the code locators of GRS codes, the code locators of a Gabidulin code are generally not the same in the generator and the parity-check matrix. In the following, when we refer to the code locators of a Gabidulin code, we always refer to the β_i's used for the *parity-check matrix* as in Definition 8.

The codewords of an $[n,k]_{q^M}$ Gabidulin code can be seen as matrices in $\mathbb{F}_q^{M \times n}$ by expanding elements of $\mathbb{F}_{q^M}$ into vectors in $\mathbb{F}_q^M$ (using a fixed basis of $\mathbb{F}_{q^M}$ over $\mathbb{F}_q$). Thus, we can define the rank distance of two codewords as the rank of their matrix representations' difference. It is well-known that the minimum rank distance of a Gabidulin code is $n - k + 1$, i.e., it fulfills the Singleton-like bound in the rank metric with equality.

III. REGENERATING PMDS AND SECTOR-DISK CODES WITH TWO GLOBAL PARITIES

We construct array codes from the PMDS codes of [15] using the ideas of [11] to obtain locally d-MSR PMDS codes. Since the PMDS code construction in [15] can be easily turned into an SD code (which is a slightly weaker notion, but results in a smaller field size), we also include the respective construction of SD codes with local d-MSR codes in this section.

A. Generalization of known PMDS construction

To apply the ideas of [11] 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 [15] 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

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_0 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0 \\ \mathbf{H}_1 & \mathbf{H}_2 & \dots & \mathbf{H}_\mu \end{bmatrix}, \qquad (2)$$

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

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

Note that this generalization includes both [15, Construction A] and [15, Construction B] as special cases:

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

and

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

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

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 μ, n, r and $s = 2$ be valid PMDS parameters and $\mathcal{L}$ be a 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 proofs of [15, Theorem 5] and [15, Theorem 7]. The difference to the construction above is that in [15], the powers $i_1, \dots, i_n$ are consecutive, i.e., $i_j = j - 1$. This results in a slightly more technical proof.

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. Assume the erasures in local group z occurred in positions $\mathcal{E}_z \subset [n]$. Since all points in $\mathcal{L}$ are distinct, by the same argument as in [15], the erased positions can be recovered uniquely if the matrix

$$\hat{\mathbf{H}} = \begin{pmatrix} \mathbf{H}_0 \\ \mathbf{H}_z \end{pmatrix}$$

restricted to the erased positions $\mathcal{E}$ is of full rank. Say that the erased positions are $1 \leq j_1 < j_2 < \dots < j_{r+2} \leq n$. It is easy to see that this matrix $\hat{\mathbf{H}}_\mathcal{E}$ can be transformed into a Vandermonde matrix by multiplying the last row by β^{jN} and the ξ-th column by $\beta^{i_{j_\xi}}$ for all $\xi \in [r-2]$ (instead of $\beta^{j_\xi - 1}$ as in [15, Theorem 5]). Therefore, it is of full rank and the

erasures can be corrected.

Now consider the case of two local groups (horizontal codes) with $r+1$ erasures each. Assume, without loss of generality, that the erased positions are given by $\{j_1, \dots, j_{r+1}\} \subset \mathcal{L}$ in local group 1 and $\{j'_1, \dots, j'_{r+1}\} \subset \mathcal{L}$ in local group $z + 1$ with $1 \leq z \leq \mu - 1$. Define the matrix

$$\mathbf{F}(j_1, \dots, j_{r+1}; j_1, \dots, j_{r+1}; r; N; z) =$$
$$\begin{bmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ \alpha^{j_1} & \dots & \alpha^{j_{r+1}} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{(r-1)j_1} & \dots & \alpha^{(r-1)j_{r+1}} & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & \dots & 1 \\ 0 & \dots & 0 & \alpha^{j'_1} & \dots & \alpha^{j'_{r+1}} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \alpha^{(r-1)j'_1} & \dots & \alpha^{(r-1)j'_{r+1}} \\ \alpha^{rj_1} & \dots & \alpha^{rj_{r+1}} & \alpha^{rj'_1} & \dots & \alpha^{rj'_{r+1}} \\ \alpha^{-j_1} & \dots & \alpha^{-j_{r+1}} & \alpha^{-Nz-j'_1} & \dots & \alpha^{-Nz-j'_{r+1}} \end{bmatrix}.$$

To show that the erased positions can be recovered, we need to show that this matrix is invertible. By [15, Lemma 3] this is true if

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

Note that in [15, Lemma 3] shows this relation only for $0 \leq j_1 < j_2 < \dots < j_{r+1} \leq n - 1$ and $0 \leq j'_1 < j'_2 < \dots < j'_{r+1} \leq n - 1$. However, it is easy to check that the result is independent of the specific values and only depends on the sums $\sum_{u=1}^{r+1} j_u$ and $\sum_{u=1}^{r+1} j'_u$. Since all j_u are distinct, we have

$$\frac{r(r+1)}{2} = \sum_{u=0}^{r} u \leq \sum_{u=1}^{r+1} j_u \qquad (3)$$

and

$$\sum_{u=1}^{r+1} j_u \leq \sum_{u=0}^{r} \left((\max_{j \in \mathcal{L}} j - r) + u \right)$$
$$= (r+1)(\max_{j \in \mathcal{L}} j - r) + \sum_{u=0}^{r} u = N - 1 + \frac{r(r+1)}{2}. \qquad (4)$$

Combining (3) and (4) we get

$$-(N-1) \leq \sum_{u=1}^{r+1} j'_u - \sum_{u=1}^{r+1} j_u \leq N - 1.$$

Then,

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

and thus it follows that

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

$\blacksquare$

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

Lemma 2. *Let μ, n, r and $s = 2$ be valid PMDS parameters and $\mathcal{L}$ 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 [15, Theorem 5]. Now consider the case of r column erasures in positions $j_1, \ldots, j_r \in \mathcal{L}$ and two random erasures in local groups $z + 1$ and $z' + 1$, with $0 \leq z < z' \leq \mu - 1$ in positions $j, j' \in \mathcal{L} \setminus \{j_1, \ldots, j_r\}$. By the same argument as in [15, Theorem 5] 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

$$N(z' - z) + j' - j \not\equiv 0 \mod \mathcal{O}(\beta)$$

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

With these generalizations of [15, 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
- $q \geq \max\{\mu N, bn\} + 1$, 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 $\beta_{i,j} = \beta^{in+j-1}, 0 \leq i \leq b - 1, 1 \leq j \leq n$.

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

$$\left\{ \mathbf{C} \in \mathbb{F}_q^{\ell \times \mu n} : \mathbf{H}^{(a)} \mathbf{C}_{a,:} = \mathbf{0} \, \forall \, a = 0, \ldots, \ell - 1 \right\}.$$

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

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

where

$$\mathbf{H}_0^{(a)} = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \beta_{a_1,1} & \beta_{a_2,2} & \ldots & \beta_{a_n,n} \\ \vdots & \vdots & & \vdots \\ \beta_{a_1,1}^{r-1} & \beta_{a_2,2}^{r-1} & \ldots & \beta_{a_n,n}^{r-1} \end{bmatrix} \in \mathbb{F}_q^{r \times n} , \quad (5)$$

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

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

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 and $s = 2$ be valid PMDS parameters, d be an integer with $n - r \leq d \leq n - 1$, and $q > \max\{\mu N, bn\}$ 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 PMDS$(\mu, n, r, 2, \mathcal{W}; b^n)$ code over $\mathbb{F}_q$, as in Definition 5, for $\mathcal{W} = \{W_1, \ldots, W_\mu\}$ with $W_i = [(i - 1)n + 1, in]$.

Proof: First, note that the $\beta_{i,j}$ in Construction 1 are the (distinct) elements $\beta^0, \beta^1, \ldots, \beta^{bn-1}$. In order for the β^i to be distinct, we require $\mathcal{O}(\beta) \geq bn$, i.e., $q > bn$. Now consider the j-th local group. The a-th row fulfills the parity check equations given in Eq. (5) 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 7.

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

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

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

Corollary 2. *Let μ, n, r and $s = 2$ be valid PMDS parameters and d be an integer with $n - r \leq d \leq n - 1$. Then, there is a d-MSR PMDS code over $\mathbb{F}_q$ with these parameters of field size*

$$\mu r(rn - r + n - 2) + 1 \leq q \leq 2\mu r(rn - r + n - 2)$$

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

Proof: We use Theorem 1 and derive bounds on the smallest field size q satisfying the bound $q > \max\{\mu N, bn\}$ with $N = (r + 1)(rn - 1 - r) + 1 = r(rn - r + n - 2)$.

First note that $1 \leq b = d + 1 - (n - r) \leq r$ for the valid choices of d. Furthermore, note that $r \geq 1$ and $n \geq r + 1 \geq 2$. Thus, we have

$$\begin{aligned} \mu N &= \mu r(rn - r + n - 2) \\ &= \mu \Big[rn + \underbrace{r^2(n - 1) - 2r}_{\geq -1} \Big] \\ &\geq \mu(rn - 1) \geq rn \geq bn . \end{aligned}$$

Hence, we in fact only require $q > \mu N$. There is a prime power[3] between $\mu N + 1$ and $2\mu N$, which proves the claim. ∎

Theorem 2. *Let μ, n, r and $s = 2$ be valid PMDS parameters and $q > \max\{rn\mu, bn\}$. Then the code $\mathcal{C}(\mu, n, r, 2, rn, d; \ell)_q$ as in Construction 1 is a locally d-MSR SD$(\mu, n, r, s, \mathcal{W}; b^n)$*

---

[3] Trivially, there is a power of two in this range. Further, by Bertrand's postulate, there is even a prime number within this range.

code over $\mathbb{F}_q$, for $\mathcal{W} = \{W_1, \ldots, W_\mu\}$ with $W_i = [(i-1)n + 1, in]$.

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

Remark 5. *It is easy to check that by removing the last row of the parity-check matrix (2) of the PMDS codes in [15], we obtain a PMDS code with one global parity ($s = 1$). By the same operation on all the parity-check matrices for the rows of the d-MSR PMDS code in Construction 1, we similarly obtain d-MSR PMDS codes with one global parity. We do not discuss this case in detail since the resulting codes have the same field size as the ones with two global parities.*

IV. UNIVERSAL PMDS CODES WITH LOCAL ROW-WISE MDS MSR CODES

In this section, we present a general technique for constructing PMDS codes with MSR local codes, by combining an arbitrary row-wise MDS MSR code (cf. Definition 4) with a universal PMDS code family. The latter notion was first defined in [33], and we formalize its definition below in Definition 9. Roughly speaking, a universal PMDS code family arises from a PMDS construction in which the local code can be chosen arbitrarily as the $\mathbb{F}_{q^M}$-span of an $\mathbb{F}_q$-linear MDS code. Although the universality requirement seems to be strong, there are several PMDS constructions in the literature that fulfill this property, for instance [4], [33] (cf. the overview in [33]). For the construction of [16], we show its universality in Section IV-D. Hence, some of the PMDS constructions with the smallest field sizes in the literature have this property, which enables the new general construction to achieve rather small field sizes as well. Note that the PMDS construction with local regeneration in Section III is not of the type presented here, since the PMDS family in [15] is not universal (due to strong dependencies between the choice of the local and global parities).

A. A general code construction

The following definition formalizes the notion of universal PMDS code family, which was introduced in [33].

Definition 9 (Universal Partial MDS code family)**.** *Let μ, n, r, s be valid PMDS parameters. A family of codes is a universal PMDS code family $\mathcal{F}_{\mathsf{PMDS}}(\mu, n, r, s)$ over $\mathbb{F}_{q^M}$ if there is a partition $\mathcal{W} = \{W_1, W_2, \ldots, W_\mu\}$ (fixed for the entire family) such that*

- *every code $\mathcal{C} \in \mathcal{F}_{\mathsf{PMDS}}(\mu, n, r, s)$ is a $\mathsf{PMDS}(\mu, n, r, s, \mathcal{W}; 1)$ code over $\mathbb{F}_{q^M}$ and*
- *for any MDS code $\mathcal{C}_{\mathsf{local}}[n, n - r, r + 1]$ over $\mathbb{F}_q$, there is exactly one $\mathcal{C} \in \mathcal{F}_{\mathsf{PMDS}}(\mu, n, r, s)$ such that $\mathcal{C}|_{W_i} = \langle \mathcal{C}_{\mathsf{local}} \rangle_{\mathbb{F}_{q^M}} \simeq \mathcal{C}_{\mathsf{local}}^{\times M}$ for all $i = 1, \ldots, \mu$ (see Fig. 2 for an illustration of this property). We denote this unique code by $\mathcal{F}(\mathcal{C}_{\mathsf{local}}) := \mathcal{C}$ (i.e., $\mathcal{F}(\cdot)$ is an injective mapping between the set of MDS codes and the family $\mathcal{F}$).*

The following code construction combines a universal PMDS code family and a row-wise MSR code. Note that the code is well-defined since the MSR code is row-wise MDS (i.e., $\mathcal{F}(C_{\mathsf{MSR}}^{(a)})$ is well-defined for all rows a of the MSR code).

Construction 2. *Let μ, n, r, s be valid PMDS parameters and $\mathcal{F}_{\mathsf{PMDS}}(\mu, n, r, s)$ be a universal PMDS code family. Let $\mathcal{C}_{\mathsf{MSR}}[n, n - r; \ell]$ be a row-wise MDS (h, d)-MSR code and denote by $\mathcal{C}_{\mathsf{MSR}}^{(a)}$ the MDS code in its a-th row for $a = 0, \ldots, \ell$. We define the code*

$$\mathcal{F}_{\mathsf{PMDS}}(\mathcal{C}_{\mathsf{MSR}}) :=$$
$$\left\{ \mathbf{C} \in \mathbb{F}_{q^M}^{\ell \times \mu n} : \mathbf{C}_{a,:} \in \mathcal{F}(\mathcal{C}_{\mathsf{MSR}}^{(a)}) \, \forall a = 0, \ldots, \ell - 1 \right\}.$$

Theorem 3. *The code $\mathcal{F}_{\mathsf{PMDS}}(\mathcal{C}_{\mathsf{MSR}})$ in Construction 2 is a locally (h, d)-MSR PMDS$(\mu, n, r, s, \mathcal{W}; \ell)$ code over $\mathbb{F}_{q^M}$, for a partition $\mathcal{W} = \{W_1, W_2, \ldots, W_\mu\}$ of $[\mu n]$ with $|W_i| = n \, \forall \, i \in [\mu]$.*

Proof: By construction, the codewords of $\mathcal{F}_{\mathsf{PMDS}}(\mathcal{C}_{\mathsf{MSR}})$ are matrices whose rows are contained in a PMDS code of the family $\mathcal{F}_{\mathsf{PMDS}}$. In particular, the PMDS code in the a-th row has the MDS code $C_{\mathsf{MSR}}^{(a)}$ as its local code. If we puncture all rows in all positions but W_i (for some $i = 1, \ldots, \mu$), we obtain in the a-th row the code $C_{\mathsf{MSR}}^{(a)}$. Hence,

$$\mathcal{F}_{\mathsf{PMDS}}(\mathcal{C}_{\mathsf{MSR}})|_{W_i} =$$

$$\left\{ \begin{bmatrix} \mathbf{C}_{0,:}^{(0)} \\ \vdots \\ \mathbf{C}_{M-1,:}^{(0)} \\ \mathbf{C}_{0,:}^{(1)} \\ \vdots \\ \mathbf{C}_{M-1,:}^{(\ell-1)} \end{bmatrix} \in \mathbb{F}_q^{M\ell \times n} : \mathbf{C}_{j,:}^{(a)} \in C_{\mathsf{MSR}}^{(a)} \, \forall \, \substack{a=0,\ldots,\ell-1 \\ j=0,\ldots,M-1} \right\}$$

$$\simeq \underbrace{\mathcal{C}_{\mathsf{MSR}} \times \cdots \times \mathcal{C}_{\mathsf{MSR}}}_{M \text{ times}} \quad \forall i = 1, \ldots, \mu,$$

where the last step follows by re-arranging the rows of a codeword (see Fig. 3 for an illustration). Hence, the overall local code is a product of M d-MSR codes, and hence is d-MSR itself. The claim follows by the definition of d-MSR PMDS codes. ∎

The remaining difficulty in Construction 2 is to find suitable constructions of universal PMDS code families. In fact, some families in the literature already have this property: the Gabidulin-code-based construction of PMDS codes in [4] and the PMDS code family constructed from linearized Reed–Solomon (RS) codes in [33] are both universal. For another construction in the literature, [16], we first show that it can be turned into a universal PMDS code family. We then summarize the resulting parameters and field sizes for all three specific constructions.

B. Construction 2 using the Gabidulin-Code-Based PMDS Family

The PMDS code construction in [4] is based on Gabidulin codes (see Section II-D), where the fact that the codes have maximal minimum rank distance is used to show that the constructed codes are PMDS. The construction works as follows.
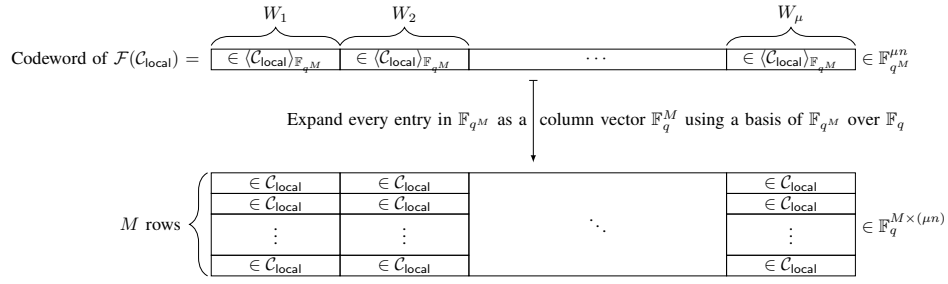
Fig. 2. Illustration of the codeword structure of the PMDS code $\mathcal{F}(\mathcal{C}_{\text{local}})$ in Definition 9.
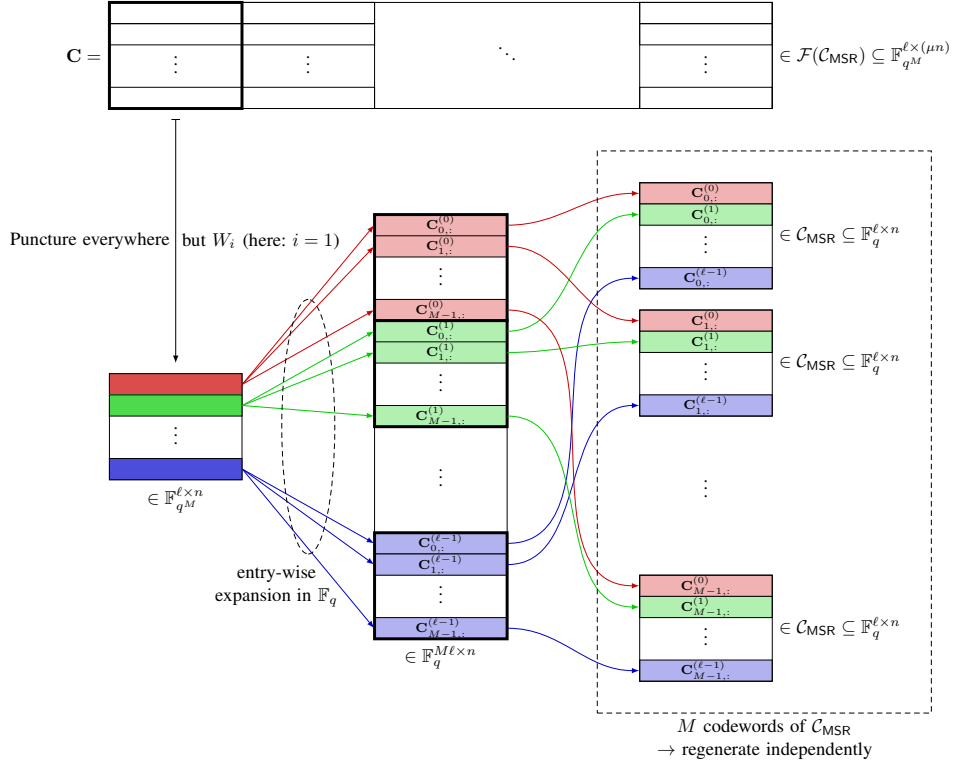

Fig. 3. Illustration of the local regeneration procedure implied by the proof of Theorem 3 (notation as in the proof).

- Choose an arbitrary MDS code $\mathcal{C}_{\text{local}}[n, n-r, r+1]$ over $\mathbb{F}_q$ and a generator matrix $\mathbf{G}_{\text{local}}$ thereof.
- Choose a Gabidulin code $\mathcal{C}_{\mathcal{G}}$ (cf. Section II-D) of parameters $[\mu(n-r), \mu(n-r)-s]$ over $\mathbb{F}_{q^M}$. This requires $M \geq \mu(n-r)$.
- Encode a message in $\mathbb{F}_{q^M}^{\mu(n-r)-s}$ with the Gabidulin code $\mathcal{C}_{\mathcal{G}}$, which gives a vector $\mathbf{x} \in \mathbb{F}_{q^M}^{\mu(n-r)}$.
- Split the vector $\mathbf{x}$ into μ sub-blocks $\mathbf{x}^{(i)}$ of size $(n-r)$, i.e., $\mathbf{x} = [\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\mu)}]$.
- Encode each subblock with the generator matrix $\mathbf{G}_{\text{local}}$ to obtain the final codeword $\boldsymbol{c}$, i.e.,

$$\boldsymbol{c} = \left[\mathbf{x}^{(1)}\mathbf{G}_{\text{local}}, \ldots, \mathbf{x}^{(\mu)}\mathbf{G}_{\text{local}}\right] \in \mathbb{F}_{q^M}^{\mu n}.$$

As $\mathcal{C}_{\text{local}}$ is an arbitrary MDS code, we obtain a universal PMDS code family by fixing a Gabidulin code $\mathcal{C}_{\mathcal{G}}$ and varying the local code. For fixed PMDS code parameters, the construction requires only $M \geq \mu(n-r)$ (due to the Gabidulin code)

and no further restriction on q (other than coinciding with the field size of the local code). Combining this family with the Ye–Barg MSR codes (which are row-wise MDS), Theorem 3 implies the following statement.

Corollary 3. *For all valid PMDS parameters μ, n, r, s, integer d with $n - r \leq d \leq n - 1$, and $\mathcal{W} = \{W_1, W_2, \ldots, W_\mu\}$ a partition of $[\mu n]$ with $|W_i| = n \; \forall \; i \in [\mu]$, there is a d-MSR $\mathrm{PMDS}(\mu, n, r, s, \mathcal{W}; \ell)$ code over $\mathbb{F}_{q^M}$ if the field size and subpacketization satisfies*

$$M \geq \mu(n-r), \quad q \geq bn, \quad \text{and} \quad \ell = b^n,$$

where $b = d + 1 - n + r$. In particular, such a code exists for a field of size $q^M = [(d + 1 - n + r)n]^{\mu(n-r)}$.

C. Construction 2 using the Linearized-RS-Codes-Based PMDS Family

The PMDS code construction in [33] is based on linearized Reed–Solomon codes, which are sum-rank-metric codes that were introduced in [37] and can be seen as a combination of Reed–Solomon and Gabidulin codes. We do not formally introduce the codes here, but briefly summarize some of their key properties. Let $\mu < q$, $n' \leq M$, and $k' \leq n'\mu$. Then, a linearized Reed–Solomon code of parameters $[\mu n', k']$ over $\mathbb{F}_{q^M}$ is a k'-dimensional subspace of $\mathbb{F}_{q^M}^{\mu n'}$. The codes are considered in the sum-rank metric w.r.t. the parameter μ, in which codewords are subdivided into μ blocks of size n' and the distance of two codewords is the sum of the rank distances of the μ blocks. The minimal sum-rank distance of a linearized Reed–Solomon code is $\mu n' - k' + 1$. This property is again essential for the codes in [33] to be PMDS. The construction works as follows.

- Choose an arbitrary MDS code $\mathcal{C}_{\text{local}}[n, n-r, r+1]$ over $\mathbb{F}_q$ and a generator matrix $\mathbf{G}_{\text{local}}$ thereof.
- Choose a linearized Reed–Solomon code $\mathcal{C}_{\mathcal{LRS}}$ (cf. [37], [33]) of parameters $[\mu(n-r), \mu(n-r)-s]$ over $\mathbb{F}_{q^M}$. This requires $M \geq n-r$ and $q > \mu$.
- Encode a message in $\mathbb{F}_{q^M}^{\mu(n-r)}$ with the linearized Reed–Solomon code $\mathcal{C}_{\mathcal{LRS}}$, which gives a vector $\mathbf{x} \in \mathbb{F}_{q^M}^{\mu(n-r)}$.
- Split the vector $\mathbf{x}$ into μ sub-blocks $\mathbf{x}^{(i)}$ of size $(n-r)$, i.e., $\mathbf{x} = [\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\mu)}]$.
- Encode each subblock with the generator matrix $\mathbf{G}_{\text{local}}$ to obtain the final codeword $\boldsymbol{c}$, i.e.,

$$\boldsymbol{c} = \left[\mathbf{x}^{(1)} \mathbf{G}_{\text{local}}, \ldots, \mathbf{x}^{(\mu)} \mathbf{G}_{\text{local}} \right] \in \mathbb{F}_{q^M}^{\mu n}.$$

As $\mathcal{C}_{\text{local}}$ is an arbitrary MDS code, we obtain a universal PMDS code family by fixing a linearized Reed–Solomon code $\mathcal{C}_{\mathcal{LRS}}$ and varying the local code. For fixed PMDS code parameters, the construction requires only $M \geq n-r$ and $q > \mu$ in addition to q being equal to the field size of the local code.[4] Combining this family with the Ye–Barg MSR codes (which are row-wise MDS), Theorem 3 implies the following statement.

Corollary 4. *For all valid PMDS parameters μ, n, r, s, integer d with $n-r \leq d \leq n-1$, and $\mathcal{W} = \{W_1, W_2, \ldots, W_\mu\}$ a partition of $[\mu n]$ with $|W_i| = n \ \forall \ i \in [\mu]$, there is a d-MSR $\mathrm{PMDS}(\mu, n, r, s, \mathcal{W}; \ell)$ code over $\mathbb{F}_{q^M}$ if the field size and subpacketization satisfies*

$$M \geq n-r, \quad q \geq \max\{bn, \mu+1\}, \quad \text{and} \quad \ell = b^n,$$

where $b = d+1-n+r$. In particular, such a code exists for a field of size $q^M = \max\{(d+1-n+r)n, \mu+1\}^{n-r}$.

D. Construction 2 using the PMDS Family in Gabrys et al.

The PMDS code construction in [16, Section IV.A] uses Reed–Solomon codes as its local codes. The following theorem generalizes the construction to arbitrary local codes,

showing that the code family is in fact universal. Note that we heavily rely on ideas from [16, Lemma 2], [16, Corollary 5], and [16, Lemma 7] in the proof.

Theorem 4 (Generalization of the PMDS Construction in [16])**.** *Let n, μ, r, s be valid PMDS parameters and $\mathbb{F}_{q^M}$ be a field. Suppose that there are distinct field elements $\alpha_{1,1}, \alpha_{1,2}, \ldots, \alpha_{\mu,n} \in \mathbb{F}_{q^M}$ such that any subset of $(r+1)s$ elements of the $\alpha_{i,j}$ is linearly independent over $\mathbb{F}_q$. Define*

$$\mathbf{H}^{(j)} = \begin{bmatrix} \alpha_{j,1} & \alpha_{j,2} & \cdots & \alpha_{j,n} \\ \alpha_{j,1}^q & \alpha_{j,2}^q & \cdots & \alpha_{j,n}^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{j,1}^{q^{s-1}} & \alpha_{j,2}^{q^{s-1}} & \cdots & \alpha_{j,n}^{q^{s-1}} \end{bmatrix} \quad \forall\, 1 \leq j \leq \mu.$$

Then, the $[\mu n, \mu(n-r)-s]_{\mathbb{F}_{q^M}}$ code with parity-check matrix

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}^{(0)} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}^{(0)} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \cdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{H}^{(0)} \\ \mathbf{H}^{(1)} & \mathbf{H}^{(2)} & \cdots & \mathbf{H}^{(\mu)} \end{bmatrix} \in \mathbb{F}_{q^M}^{(\mu r + s) \times \mu n}$$

is a PMDS code, where $\mathbf{H}^{(0)} \in \mathbb{F}_q^{r \times n}$ (note $\mathbb{F}_q \subseteq \mathbb{F}_{q^M}$) is a parity-check matrix of an arbitrary $[n, n-r]_q$ MDS code.

Proof: Let $\boldsymbol{c} = \left[\boldsymbol{c}^{(1)}, \ldots, \boldsymbol{c}^{(\mu)} \right]$ be a codeword of the code, which is divided into μ blocks $\boldsymbol{c}^{(i)} \in \mathbb{F}_{q^M}^n$. By definition, for all $i = 1, \ldots, \mu$, we have

$$\mathbf{H}^{(0)} \boldsymbol{c}^{(i)\top} = \mathbf{0}. \tag{6}$$

Furthermore, with $\boldsymbol{\alpha}_i := [\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,n}]$, we have

$$\sum_{i=1}^{\mu} \boldsymbol{\alpha}_i^{q^j} \boldsymbol{c}^{(i)\top} = 0, \tag{7}$$

for all $j = 0, \ldots, s-1$. Let $S := [\mathbf{s}_1, \ldots, \mathbf{s}_\mu]$ be of the form

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

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 2). We need to show that for each such vector S, the array code punctured at these positions in each local group, gives an $[\mu n - \mu r, \mu n - \mu r - s]$ MDS 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. 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 (6) that

$$\left(\boldsymbol{c}^{(i)} \right)_{\mathbf{s}_i}^\top = \mathbf{H}_{\mathbf{s}_i}^{(0)^{-1}} \mathbf{H}_{\bar{\mathbf{s}}_i}^{(0)} \left(\boldsymbol{c}^{(i)} \right)_{\bar{\mathbf{s}}_i}^\top,$$

---

[4]Note that, compared to the Gabidulin-based PMDS construction above, the restriction on M is much weaker, and we have an additional condition on q. This means that the logarithm of the field size (and thus the soft-O complexity of operations in the field) is not linear in μ anymore, but logarithmic in μ.

and by (7) that (note that $\mathbf{H}^{(0)}$ has entries in $\mathbb{F}_q$, so $\mathbf{H}^{(0)} = \mathbf{H}^{(0)q^j}$ for any j)

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

Thus, the vector $\boldsymbol{c}_S = \left[\left(\boldsymbol{c}^{(1)}\right)_{\bar{\mathbf{s}}_1}, \left(\boldsymbol{c}^{(2)}\right)_{\bar{\mathbf{s}}_2}, \ldots, \left(\boldsymbol{c}^{(\mu)}\right)_{\bar{\mathbf{s}}_\mu} \right]$, which is the codeword punctured at the positions in S, is contained in a code with parity-check matrix

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

where

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

By definition, we have

$$
\boldsymbol{\gamma}_{\mathbf{s}_i} = (\boldsymbol{\alpha}_i)_{\mathbf{s}_i} \left(\mathbf{H}^{(0)}\right)_{\mathbf{s}_i}^{-1} \left(\mathbf{H}^{(0)}\right)_{\bar{\mathbf{s}}_i} + (\boldsymbol{\alpha}_i)_{\bar{\mathbf{s}}_i}.
$$

Since $\left(\mathbf{H}^{(0)}\right)_{\mathbf{s}_i}^{-1} \left(\mathbf{H}^{(0)}\right)_{\bar{\mathbf{s}}_i}$ is an $r \times (n-r)$ matrix, each entry of $\boldsymbol{\gamma}_{\mathbf{s}_i}$, and thus each entry of $\boldsymbol{\gamma}_S$, is a 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 $(\boldsymbol{\alpha}_i)_{\bar{\mathbf{s}}_i}$) that appears only in this linear combination. Any set of s entries from $\boldsymbol{\gamma}_S$ depends on at most $s(r+1)$ of the $\alpha_{i,j}$, which are linearly independent by the independence assumption. Hence, the s entries from $\boldsymbol{\gamma}_S$ are also linearly independent over $\mathbb{F}_q$. This means that any s columns of the parity-check matrix $\mathbf{H}_{\gamma}$ are linearly independent and $\mathbf{H}_{\gamma}$ is a parity-check matrix of an $[n\mu - r\mu, n\mu - r\mu - s]_{q^M}$ MDS code.

It remains to show that the local codes equal the $\mathbb{F}_{q^M}$-span of the $[n, n-r]_q$ MDS code with parity-check matrix $\mathbf{H}^{(0)}$. It is clear by construction that the local codes are subcodes of this code. To see that the local codes are equal to this code, consider the code obtained from the PMDS code after puncturing arbitrary r positions in each local group. This is an $[\mu(n-r), \mu(n-r) - s]_{q^M}$ MDS code. Since valid PMDS parameters fulfill $\mu(n-r) - s \geq n-r$, any $n-r$ columns of a generator matrix of the punctured code are linearly independent. In particular, by further puncturing all positions, except for the remaining $n-r$ positions in one local group, we get an $[n-r, n-r]_{q^M}$ MDS code. This proves that all the local codes have dimension $n-r$, and thus the claim. Hence, the overall code is a PMDS code. ∎

As the MDS code over $\mathbb{F}_q$ can be chosen arbitrarily for fixed $\alpha_{1,1}, \alpha_{1,2}, \ldots, \alpha_{\mu,n} \in \mathbb{F}_{q^M}$, Theorem 4 immediately implies a universal PMDS code family as in Definition 9. By Theorem 3, we get the following result.

Corollary 5. *For all valid PMDS parameters μ, n, r, s, integer d with $n - r \leq d \leq n - 1$, and $\mathcal{W} = \{W_1, W_2, \ldots, W_\mu\}$ a partition of $[\mu n]$ with $|W_i| = n \ \forall \ i \in [\mu]$, there is a d-MSR PMDS array code as in Construction 2 of field size*

$$
n\big[d + 1 - (n-r)\big](n\mu)^{s(r+1)-1} \leq q^M
$$
$$
\leq 2n\big[d + 1 - (n-r)\big](2n\mu)^{s(r+1)-1}
$$

and subpacketization

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

Proof: We combine the universal PMDS code family in Theorem 4 with Ye–Barg codes (cf. Definition 7) using Construction 2. We choose q and M large enough such that we can ensure that suitable field elements $\alpha_{i,j}$ (of the PMDS code family) and $\beta_{i,j}$ (of the Ye–Barg codes) exist. A sufficient condition for the existence of the $\beta_{i,j}$ is $q \geq n(d+1-(n-r))$. Thus, we can choose q to be the smallest prime power greater or equal to $n(d + 1 - (n - r))$, which is at most $q \leq 2n(d + 1 - (n - r))$ by Bertrand's postulate.

For the $\alpha_{i,j}$, it is a bit more involved. By Theorem 4, 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 [16, 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 in $\mathbb{F}_q^M$ as an element of $\mathbb{F}_{q^M}$. The independence condition is then fulfilled due to the choice of the 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 [38, Problem 8.9], which we can reformulate in our terms as follows. For any $n' = q^a - 1$, there exists a code with parameters $[n', n' - M, s(r+1)+1]_q$, where

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

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

V. DISCUSSION AND COMPARISON OF PMDS CODE CONSTRUCTIONS WITH LOCAL REGENERATION

A. Field Size Comparison

Table II compares the field sizes of the d-MSR PMDS constructions in Section IV (universal PMDS code construction), for Ye–Barg MSR codes and three universal PMDS families, and Section III (two parities). We also compare our new constructions to the only existing construction of d-MSR PMDS codes, which was presented in [4]. For easier reference, we label the five constructions by the letters A–E.

The known Construction E (see [4, Construction 1, case "$(r + \delta - 1) \mid n$"]) first encodes an information word from $\mathbb{F}_{q^M}^{\ell \times (\mu(n-r)-s)}$ with an $[\ell\mu(n-r), \ell(\mu(n-r) - s)]_{q^M}$

Gabidulin code. The resulting codeword is then subdivided into μ groups, each of length $\ell(n-r)$. These subblocks are then independently encoded using a generator matrix of an $[n, n-r; \ell]_q$ d-MSR code. This gives a d-MSR PMDS array code with subpacketization ℓ and field size q^M, where the only requirements on ℓ and q are the constraints of the MSR code, and we require $M \geq \ell\mu(n-r)$ in order for the Gabidulin code to exist. An advantage of this construction over ours is that it does not require the MSR code to be row-wise MDS. However, the field size is exponential in the subpacketization (i.e., doubly exponential in n for Ye–Barg codes).

The following theorem states some relations between the minimal field sizes achievable by the five compared constructions. It can be interpreted as follows:

- Construction C has always smaller field size than Constructions B and E.
- For two global parities, Construction A has the smallest field size among all constructions (unless r or μ is very large).
- For a large number of global or local parities (and $s > 2$), Construction C has the smallest field size among all constructions.
- For a small number of global (but $s > 2$) and local parities, Construction D has the smallest field size among all constructions.

Theorem 5. *For all valid PMDS parameters μ, n, r, s and integers d with $n-r < d \leq n-1$ (we exclude the trivial case $d = n-r$), denote by Q_A, Q_B, Q_C, Q_D, Q_E the smallest field sizes obtained from the constructions in Table II.*

(i) For all parameters, we have $Q_C < Q_B < Q_E$.

(ii) For $s = 2$, we have $Q_A < Q_D$. If in addition, $r < n-3$, and $\mu \leq n^{n-r-3}$, then $Q_A < Q_C$.

(iii) For $s(r+1) + 2r - 1 \geq 2n$, we have $Q_C < Q_D$.

(iv) For $2s(r+1) + r \leq n$, we have $Q_D < Q_C$.

Proof: We use (a) $a \leq a + 1 < 3^a$ and (b) $a^b \geq ab$ for integers $a, b \geq 1$, which can both be proven easily by induction.

Ad (i): As $d > n-r$, we have $d+1-n-r > 1$, so obviously $Q_E > Q_B$. If $(d+1-n-r)n \geq \mu+1$, it is clear that $Q_B > Q_C$ (here we use $\mu \geq 2$). In the case $(d+1-n-r)n \geq \mu+1$, we have

$$Q_C = (\mu+1)^{n-r} \overset{(a)}{<} 4^{\mu(n-r)} \leq [(d+1-n+r)n]^{\mu(n-r)},$$

where $(d+1-n+r)n \geq 4$ holds by assumption.

Ad (ii): We have

$$Q_A \leq 2\mu r(rn - r + n - 2)$$
$$< 2\mu n^2[2(r+1) - 1]$$
$$\overset{(b)}{\leq} 2n(n\mu)^{2(r+1)-1}$$
$$\leq n[d+1-n+r](n\mu)^{s(r+1)-1} \leq Q_D,$$

where we use $d+1-n+r \geq 2$. Furthermore, if also $r < n-3$ and $\mu \leq n^{n-r-3}$, we have

$$Q_A \leq 2\mu r(rn - r + n - 2)$$
$$< 2\mu n^3 \leq 2n^{n-r}$$
$$\leq [(d+1-n+r)n]^{n-r} \leq Q_C.$$

Ad (iii): Denote $b := d+1-n+r$ and recall that $2 \leq b \leq r < n$. We must show $Q_D > (bn)^{n-r}$ and $Q_D > (\mu+1)^{n-r}$. We start with the first inequality:

$$Q_D \geq nb(n\mu)^{s(r+1)-1} \geq nbn^{s(r+1)-1}$$
$$\geq nb\underbrace{\left(n^2\right)}_{>nb}^{\frac{s(r+1)-1}{2}}$$
$$> (nb)^{\frac{s(r+1)+1}{2}} \geq (nb)^{n-r}.$$

The second inequality holds since

$$Q_D \geq nb(n\mu)^{s(r+1)-1} > (\mu+1)^{s(r+1)-1} \geq (\mu+1)^{n-r}.$$

Ad (iv): Define $\xi := \max\{nb, \mu\}$ (we use $b := d+1-n+r$ with $2 \leq b \leq r < n$ as above). It suffices to show $Q_D < \xi^{n-r}$ under the given conditions. We have

$$Q_D \leq 2nb(\underbrace{2n}_{\leq nb \leq \xi}\mu)^{s(r+1)-1} < \xi^{2s(r+1)} \leq \xi^{n-r} \leq Q_C.$$

This concludes the proof. ∎

Figures 4, 5, and 6 plot the field size bounds of Table II over the number of local parities r for different sets of PMDS code parameters and $d = n-1$. The plots also illustrate the change of field size for a varying number of global parities s: For Construction D, we include several curves for different s. Note that the field sizes of Constructions B and C are independent of s, and Construction A exists only for $s = 2$. Hence, we only need one curve for each of these three constructions. The field size of Construction E (known construction) is way out of the plot range, which is why it is not contained in the figures. The plots confirm the statements of Theorem 5 for these example parameters.
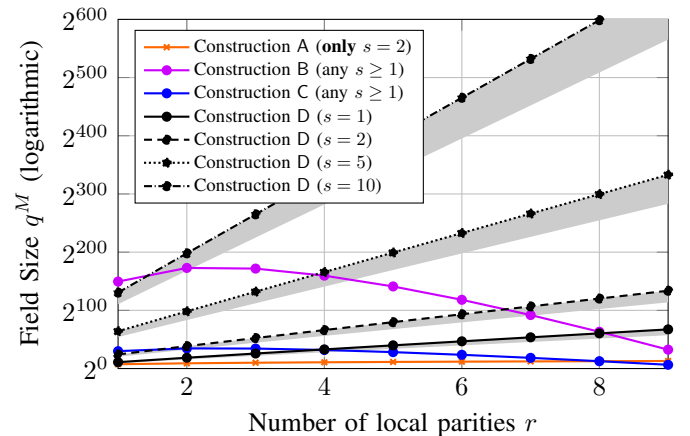

Fig. 4. Comparison of field sizes of Constructions A–D for $n = 10$, $\mu = 5$, and $d = 9$. Construction E is not shown as it is out of plot range. Lines are upper bounds, shadows indicate lower bounds. The field sizes of Constructions B and C are independent of s.

TABLE II
COMPARISON OF FIELD SIZES OF d-MSR PMDS ARRAY CODE CONSTRUCTIONS (PARAMETERS: d, n, μ, r, s SUCH THAT $r \leq n$, $s \leq (n-r)\mu$, AND $n - r \leq d \leq n - 1$).

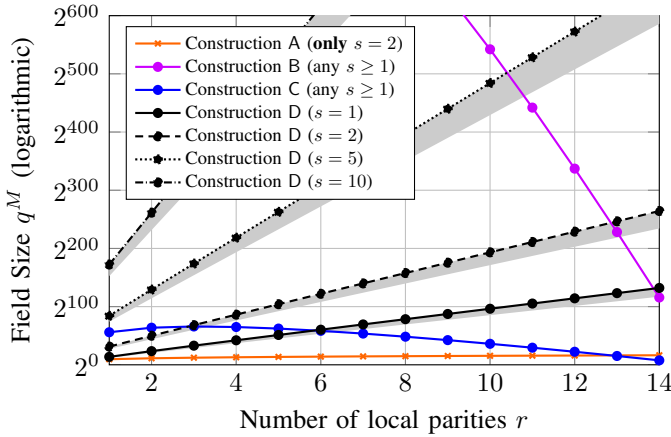| $\star$	Construction	Restr.	Smallest field size $Q_\star = q^M$ obtained from the construction
A	Constr. 1 (Corollary 2)	$s=2$	$\mu r(rn - r + n - 2) + 1 \leq Q_{\mathsf{A}} \leq 2\mu r(rn - r + n - 2)$
B	Constr. 2 + Gabidulin-based PMDS + Ye–Barg (Cor. 3)	–	$Q_{\mathsf{B}} = [(d + 1 - n + r)n]^{\mu(n-r)}$
C	Constr. 2 + Lin. RS-based PMDS + Ye–Barg (Cor. 4)	–	$Q_{\mathsf{C}} = \max\left\{(d + 1 - n + r)n, \mu + 1\right\}^{n-r}$
D	Constr. 2 + "small fields" PMDS + Ye–Barg (Cor. 5)	–	$n\left[d + 1 - n + r\right](n\mu)^{s(r+1)-1} \leq Q_{\mathsf{D}}$ $\leq 2n\left[d + 1 - n + r\right](2n\mu)^{s(r+1)-1}$
E	Known construction: [4, Construction 1] + Ye–Barg	–	$Q_{\mathsf{E}} = [(d + 1 - n + r)n]^{(d+1-n+r)^n \mu(n-r)}$

Fig. 5. Comparison of field sizes of Constructions A–D for $n = 15$, $\mu = 15$, and $d = 14$. Construction E is not shown as it is out of plot range. Lines are upper bounds, shadows indicate lower bounds. The field sizes of Constructions B and C are independent of s.

Fig. 6. Comparison of field sizes of Constructions A–D for $n = 30$, $\mu = 10$, and $d = 29$. Construction E is not shown as it is out of plot range. Lines are upper bounds, shadows indicate lower bounds. The field sizes of Constructions B and C are independent of s.
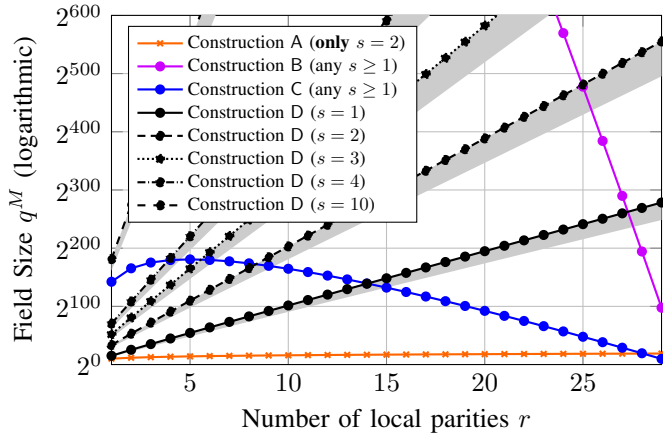
VI. PMDS CODES WITH NON-TRIVIAL GLOBAL REGENERATION

By definition, a PMDS code punctured in arbitrary r positions per group is an MDS code of distance $s + 1$. In the following we construct PMDS codes where each of these MDS codes is an MSR code. For the sake of simplicity, we focus

on the case of highest practical interest: MSR codes with that repair one position ($h = 1$) from all remaining positions ($d = \mu(n-r) - 1$) of the MDS code.

The construction is based on two main observations: first, the principle used in the MSR codes of [11] can also be applied using Gabidulin codes (recall Definition 8 in Section II) instead of RS codes; second, performing linearly independent linear combinations of the symbols of a Gabidulin code yields another Gabidulin code with different code locators. Using these observations and carefully choosing the code locators for each row in an array of Gabidulin codewords, we assure the code obtained from puncturing r positions in each local group is MSR. The construction that we study works as follows.

Construction 3 (Globally MSR PMDS array codes)**.** *Let μ, n, r, s be valid PMDS parameters and $\boldsymbol{B} \in \mathbb{F}_{q^M}^{\ell \times \mu(n-r)}$ be a matrix with entries $\beta_{i,j}, i \in [\ell], j \in [\mu(n-r)]$. We define the following $[\mu n, \mu(n-r) - s; \ell]_{q^M}$ array code $\mathcal{C}(\mu, n, r, s, \boldsymbol{B}; \ell)_q$ as*

$$\left\{ \mathbf{C} \in \mathbb{F}_q^{\ell \times \mu n} : \mathbf{C}_{a,:} = \boldsymbol{u}^{(a)} \cdot \mathbf{G}_{\boldsymbol{B}}^{(a)} \cdot \mathrm{diag}(\mathbf{G}_{\mathsf{MDS}}, \mathbf{G}_{\mathsf{MDS}}, \ldots) \right.$$
$$\left. \forall \boldsymbol{u}^{(a)} \in \mathbb{F}_{q^m}^{\mu(n-r)-s}, a = 0, \ldots, \ell - 1 \right\},$$

where $\mathbf{G}_{\boldsymbol{B}}^{(a)}$ is the generator matrix of the code $\mathsf{Gab}(\mu(n - r), \mu(n-r) - s, \boldsymbol{B}_{a,:})$ code as in Definition 8 and $\mathbf{G}_{\mathsf{MDS}}$ is a generator matrix of an $[n, n-r]_q$ MDS code.

It is easy to see that if the rows of the matrix $\boldsymbol{B}$ in Construction 3 contain linearly independent elements, then each row of the code is a PMDS code of the code family constructed in [4]. In the remainder of this section, we prove that if the matrix $\boldsymbol{B}$ is chosen in a suitable way, then the MDS array codes obtained from erasing r positions in each local group are MSR codes of the following type, which can be seen as a Gabidulin-analog of Ye–Barg codes.

Definition 10 (Skew Ye–Barg d-MSR codes)**.** *Let μ, n, r, s be valid PMDS parameters, $\ell \in \mathbb{Z}_{>0}$, and $\boldsymbol{B} \in \mathbb{F}_{q^m}^{\ell \times \mu(n-r)}$ be a matrix with entries $\boldsymbol{B}_{i,j} = \beta_{i,j}$. Define $\mathcal{C}(\mu, n, r, s, \boldsymbol{B}) \subset \mathbb{F}_q^{\ell \times \mu(n-r)}$ to be an $[\mu(n-r), \mu(n-r) - s; \ell]$ array code over $\mathbb{F}_{q^m}$, where each codeword is a matrix with ℓ rows and $\mu(n-r)$ columns, where the a-th row is a codeword of a code*

with parity-check matrix

$$\mathbf{H}_{B}^{(a)} = \begin{bmatrix} \beta_{a,1} & \beta_{a,2} & \cdots & \beta_{a,\mu(n-r)} \\ \beta_{a,1}^{q^1} & \beta_{a,2}^{q^1} & \cdots & \beta_{a,\mu(n-r)}^{q^1} \\ \vdots & \vdots & & \vdots \\ \beta_{a,1}^{q^{s-1}} & \beta_{a,2}^{q^{s-1}} & \cdots & \beta_{a,\mu(n-r)}^{q^{s-1}} \end{bmatrix},$$

for $a \in [0, \ell - 1]$. Denote by $\mathbf{G}_{B}^{(a)}$ a generator matrix corresponding to $\mathbf{H}_{B}^{(a)}$.

Remark 6. *Definition 10 is essentially the same as Definition 7, except that it relies on Gabidulin codes. Note that there is also a difference in presentation: the locators are not given as a set of elements, but instead given explicitly as an input for each row. For Definition 7 the corresponding matrix B is easily obtained from a set $\mathcal{B} = \{\beta_{i,j}\}_{i \in [b], j \in [n]}$ of distinct elements of $\mathbb{F}_{q^M}$ by assigning $B_{a,j} = \beta_{a_j,j}$ for $a \in [0, \ell - 1]$ and $a = \sum_{i=1}^{n} a_i b^{i-1}$ with $a_i \in [0, b-1]$, i.e., assigning the code locators of $\mathbf{H}^{(a)}$ to the a-th row of B.*

For the node repair algorithm of Ye–Barg codes [11], it is essential that the rows of a codeword can be partitioned into subsets for which there exist parity checks that differ exactly in position i, i.e., for which all entries are the same except for those at position i, which are all distinct (this is due to the close relation of Ye–Barg to Reed–Solomon codes). In Lemma 3 below, we analogously prove that Skew Ye–Barg codes are MSR codes if they have the following property (which is due to their relation to Gabidulin codes).

Definition 11 (YB-Grouping Property). *Let μ, n, r, s be valid PMDS parameters and $B \in \mathbb{F}_{q^m}^{\ell \times \mu(n-r)}$. We say that the matrix B has the **YB-grouping property w.r.t.** s if for each position i the rows of the matrix can be partitioned into $\frac{\ell}{s}$ subsets of s rows for which the elements in the i-th position are linearly independent and the elements in all other positions are the same for all s rows.*

Lemma 3. *Let μ, n, r, s be valid PMDS parameters and $B \in \mathbb{F}_{q^M}^{\ell \times \mu(n-r)}$ be a matrix such that for any $a \in [\ell]$ the elements of its a-th row $B^{(a)}$ are linearly independent over $\mathbb{F}_q$. Further, let B have the Ye-Barg grouping property w.r.t. s as in Definition 11. Then the code $\mathcal{C}(\mu, n, r, s, B)$ as in Definition 10 is an MSR code.*

Proof: The MDS property follows directly as each row is a codeword of a Gabidulin code, which are well-known to be MDS. It is easy to check that the recovery algorithm of [11, Theorem 1] also applies to the code of Definition 10. For completeness we include a short proof here. Assume node i failed, i.e., we need to recover the set $\{\mathbf{C}_{a,i} \, \forall \, a \in [\ell]\}$ from the helper nodes with indices $[\mu(n-r)] \setminus \{i\}$. Denote by $\mathbb{A}_i = \{\mathcal{A}_{i,1}, \mathcal{A}_{i,2}, \ldots, \mathcal{A}_{i,\frac{\ell}{s}}\}$ the partition of $[\ell]$ into the subsets $\mathcal{A}_{i,z}$ of s row indices for which the parity check equations differ exactly in position i and the entries in position i are linearly independent. Note that such a partition exists for every $i \in [\mu(n-r)]$ by definition of the Ye-Barg grouping property. The a-th row of a codeword $\mathbf{C} \in \mathcal{C}$ is determined by the s

parity checks

$$0 = \sum_{j=1}^{\mu(n-r)} \beta_{a,j}^{q^t} \mathbf{C}_{a,j} = \beta_{a,i}^{q^t} \mathbf{C}_{a,i} + \sum_{\substack{j=1 \\ j \neq i}}^{\mu(n-r)} \beta_{a,j}^{q^t} \mathbf{C}_{a,j}$$

for $t \in [0, s-1]$. Observe that $\beta_{\mathcal{A}_{i,z},j} := \beta_{a,j} = \beta_{a',j} \, \forall \, a, a' \in \mathcal{A}_{i,z}, j \neq i$. Summing over $a \in \mathcal{A}_{i,z}$ gives

$$\sum_{a \in \mathcal{A}_{i,z}} \beta_{a,i}^{q^t} \mathbf{C}_{a,i} = \sum_{a \in \mathcal{A}_{i,z}} \sum_{\substack{j=1 \\ j \neq i}}^{\mu n} \left(\beta_{a,j}^{q^t} \mathbf{C}_{a,j} \right)$$

$$= \sum_{\substack{j=1 \\ j \neq i}}^{\mu n} \left(\beta_{\mathcal{A}_{i,z},j}^{q^t} \sum_{a \in \mathcal{A}_{i,z}} \mathbf{C}_{a,j} \right). \quad (8)$$

This is a linear system of equations with s unknowns $\mathbf{C}_{a,i}, a \in \mathcal{A}_{i,z}$ and s equations, one for each $t \in [0, s-1]$. As the elements $\{\beta_{a,i} \mid a \in \mathcal{A}_{i,z}\}$ are linearly independent by definition (recall that B has the Ye-Barg grouping property), the equations are linearly independent. Hence, the unknowns can be uniquely determined if the right hand side of Eq. (8) is known. Therefore, for repair of node i, node j transmits the set of symbols

$$\left\{ \sum_{a \in \mathcal{A}_{i,z}} \mathbf{C}_{a,j} \mid z \in [\ell/s] \right\}.$$

As the cardinality of this set is $\frac{\ell}{s}$, the repair bandwidth is $(\mu(n-r)-1)\frac{\ell}{s}$ and thereby fulfills the bound on the minimal repair bandwidth of Definition 3 with equality. ∎

The code in Construction 3 can be obtained from a skew Ye–Barg code by multiplying it from the right by the $\mu(n-r) \times \mu n$ matrix $\mathrm{diag}(\mathbf{G}_{\mathsf{MDS}}, \mathbf{G}_{\mathsf{MDS}}, \ldots)$. When puncturing arbitrary r positions in each local group, we do not obtain the original skew Ye–Barg code. However, we do get the original code multiplied by an invertible matrix over $\mathbb{F}_q$ from the right. The rows of such a code are again Gabidulin codes by the following well-known result. For completeness, we include a short proof of the property.

Lemma 4 ([39, Lemma 3]). *Let $\mathbf{G} \in \mathbb{F}_{q^M}^{k \times n}$ be a generator matrix of an $[n, k, d_{\min}]$ Gabidulin code $\mathsf{Gab}(n, k, \mathbf{b})$. Then, for any full-rank matrix $\mathbf{A} \in \mathbb{F}_q^{n \times n}$, the code*

$$\mathcal{C}' = \langle \mathbf{G} \cdot \mathbf{A} \rangle$$

is an $[n, k, d_{\min}]$ Gabidulin code $\mathsf{Gab}(n, k, \mathbf{b}')$ with

$$\mathbf{b}' = \mathbf{b} \cdot \mathbf{A}^{-1}.$$

Proof: Let $\mathbf{H}, \mathbf{H}' \in \mathbb{F}_{q^M}^{n-k \times n}$ be the parity-check matrix of the code $\mathsf{Gab}(n, k, \mathbf{b})$, $\mathsf{Gab}(n, k, \mathbf{b}')$, respectively, as in Definition 8. By definition we have

$$\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$$
$$\mathbf{G} \cdot \mathbf{A} \cdot \underbrace{\mathbf{A}^{-1} \mathbf{H}^T}_{\overset{(a)}{=} \mathbf{H}'^T} = \mathbf{0},$$

where (a) follows from the fact that $\lambda_i \beta_i^{q^l} + \lambda_j \beta_j^{q^l} = (\lambda_i \beta_i + \lambda_j \beta_j)^{q^l} \, \forall \, \lambda_i, \lambda_j \in \mathbb{F}_q$. As $\mathbf{A}$ is of full rank over $\mathbb{F}_q$, we have

$\mathrm{rank}_q(\mathbf{b}') = \mathrm{rank}_q(\mathbf{b})$ and, in particular, if the elements of $\mathbf{b}$ are linearly independent, so are the elements of $\mathbf{b}'$, thereby fulfilling the requirements of Definition 8 on the code locators. ∎

Using the intermediate statements above, the following theorem gives a sufficient condition on the matrix $\boldsymbol{B}$ for Construction 3 to give a globally-MSR PMDS code.

Theorem 6. *Let μ, n, r, s be valid PMDS parameters, $\mathcal{W} = \{W_1, W_2, \ldots, W_\mu\}$ be a partition of $[\mu n]$ with $|W_i| = n \,\forall\, i \in [\mu]$. Then, the code $\mathcal{C}(\mu, n, r, s, \boldsymbol{B}; \ell)_{q^M}$ as in Construction 3 is a globally-MSR PMDS code if the matrix*

$$\boldsymbol{B} \cdot (\mathrm{diag}(\mathbf{G}_{\mathsf{RS}}, \mathbf{G}_{\mathsf{RS}}, \ldots)|_{[\mu n] \setminus \cup_{i=1}^{\mu} E_i})^{-1}$$

has the YB grouping property *(as in Definition 11) for any $E_i \subset W_i$ with $|E_i| = r$.*

Proof: Without loss of generality assume that $W_i = [(i-1)n+1, in]$. Denote $\mathcal{I} = [\mu n] \setminus \cup_{i=1}^{\mu} E_i$, where $E_i \subset W_i$ with $|E_i| = r$ for all $i \in [\mu]$, and $\bar{E}_i = [n] \setminus E_i$. The restriction of the code $\mathcal{C}$ to the positions indexed by $\mathcal{I}$ is the code generated by

$$\mathcal{C}_{\mathcal{I}} = \left\langle \left(\mathbf{G}^{(a)} \cdot \mathrm{diag}(\mathbf{G}_{\mathsf{RS}}, \mathbf{G}_{\mathsf{RS}}, \ldots) \right)\big|_{\mathcal{I}} \right\rangle$$
$$= \left\langle \mathbf{G}^{(a)} \cdot (\mathrm{diag}(\mathbf{G}_{\mathsf{RS}}, \mathbf{G}_{\mathsf{RS}}, \ldots))\big|_{\mathcal{I}} \right\rangle .$$

As $\mathbf{G}_{\mathsf{RS}}$ is the generator matrix of an MDS code, the matrix $\mathrm{diag}(\mathbf{G}_{\mathsf{RS}}|_{\bar{E}_0}, \mathbf{G}_{\mathsf{RS}}|_{\bar{E}_1}, \ldots)$ is a full-rank $\mathbb{F}_q^{\mu(n-r) \times \mu(n-r)}$ matrix. By Lemma 4 it follows that code $\mathcal{C}_{\mathcal{I}}^{(a)}$, consisting of the a-th row of every codeword of $\mathcal{C}_{\mathcal{I}}$, is a $\mathsf{Gab}(\mu(n-r), \mu(n-r) - s, \mathbf{b})$ code with

$$\mathbf{b} = \boldsymbol{B}_{a,:} \cdot (\mathrm{diag}(\mathbf{G}_{\mathsf{RS}}, \mathbf{G}_{\mathsf{RS}}, \ldots)|_{\mathcal{I}})^{-1} .$$

As $\boldsymbol{B} \cdot (\mathrm{diag}(\mathbf{G}_{\mathsf{RS}}, \mathbf{G}_{\mathsf{RS}}, \ldots)|_{\mathcal{I}})^{-1}$ has the Ye-Barg grouping property by definition, it follows from Lemma 3 that the code is MSR. ∎

It remains to construct a matrix $\boldsymbol{B}$ that fulfills the property of Theorem 6. We use the following slightly stronger property to simplify the analysis.

Definition 12. $\boldsymbol{B} \in \mathbb{F}_{q^M}^{\ell \times (\mu(n-r))}$ *has the* **scrambled YB grouping property** *if $\boldsymbol{B} \cdot \mathrm{diag}(\mathbf{G}_1, \ldots, \mathbf{G}_\mu)$ has the YB grouping property for all invertible matrices $\mathbf{G}_i \in \mathbb{F}_q^{(n-r) \times (n-r)}$.*

The following theorem gives a construction of a matrix $\boldsymbol{B}$ having the scrambled YB grouping property.

Theorem 7. *Let $M = \mu(n-r+s-1)$ and choose μ subspaces*

$$\mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(\mu)} \in \mathrm{Gr}(\mathbb{F}_q^M, n-r+s-1).$$

i.e., $n-r+s-1$-dimensional subspaces of $\mathbb{F}_q^M$, that span the space $\mathbb{F}_q^M$.

For $i = 1, \ldots, \mu$, consider the sets

$$\mathcal{S}^{(i)} := \{[\beta_1, \ldots, \beta_{n-r}] : \langle \beta_1, \ldots, \beta_{n-r} \rangle_{\mathbb{F}_q}$$
$$\text{is an } (n-r)\text{-dimensional subspace of } \mathcal{B}^{(i)}\}$$

and

$$\mathcal{S} := \left\{ [\mathbf{b}^{(1)} \mid \cdots \mid \mathbf{b}^{(\mu)}] : \mathbf{b}^{(i)} \in \mathcal{S}^{(i)} \right\} .$$

Then, the cardinality of $\mathcal{S}$ is

$$\ell := |\mathcal{S}| = \left(\begin{bmatrix} n-r+s-1 \\ n-r \end{bmatrix}_q \prod_{i=0}^{n-r-1} \left(q^{n-r} - q^i \right) \right)^\mu$$
$$\leq 4^\mu q^{\mu(n-r)(n-r+s-1)}.$$

Let $\boldsymbol{B} \in \mathbb{F}_{q^M}^{\ell \times (n-r)\mu}$ be a matrix whose rows are exactly the entries of $\mathcal{S}$. Then, $\boldsymbol{B}$ has the scrambled YB grouping property as in Definition 12.

Proof: The cardinality of $\mathcal{S}^{(i)}$ is the number of $(n-r)$-dimensional subspaces of an $n-r+s-1$-dimensional vector space over $\mathbb{F}_q$, times the number of bases of such a subspace. The latter equals the number of invertible $(n-r) \times (n-r)$ matrices over $\mathbb{F}_q$. Hence, we have

$$|\mathcal{S}_i| = \begin{bmatrix} n-r+s-1 \\ n-r \end{bmatrix}_q \prod_{i=0}^{n-r-1} \left(q^{n-r} - q^i \right)$$
$$\leq 4 q^{(s-1)(n-r)} q^{(n-r)^2} = 4 q^{(n-r)(n-r+s-1)}.$$

Overall, we get

$$\ell = |\mathcal{S}| = \prod_{i=1}^{\mu} |\mathcal{S}^{(i)}|$$
$$= \left(\begin{bmatrix} n-r+s-1 \\ n-r \end{bmatrix}_q \prod_{i=0}^{n-r-1} \left(q^{n-r} - q^i \right) \right)^\mu$$
$$\leq 4^\mu q^{\mu(n-r)(n-r+s-1)}.$$

If we write the elements of $\mathcal{S}$ as a matrix, then this matrix has the YB group property, i.e.,

- every element of $\mathcal{S}$ is a vector consisting of linearly independent entries (this is obvious since for any choice of the bases $\mathbf{b}^{(i)}$ their entries are linearly independent by construction of the subspaces $\mathcal{B}^{(i)}$).
- for a position $j \in \{1, \ldots, n-r\}$ in the i-th block ($i = 1, \ldots, \mu$) and an element $\mathbf{b} \in \mathcal{S}$, there are the following s elements in $\mathcal{S}$: Choose $s-1$ elements $a_2, \ldots, a_s$ that expand the basis $b_1^{(i)}, \ldots, b_{n-r}^{(i)}$ (which spans an $(n-r)$-dimensional subspace) to the $(n-r+s-1)$-dimensional subspace $\mathcal{B}^{(i)}$. Then, the s vectors

$$\mathbf{b}^{(i)} =: \mathbf{b}_{(1)}^{(i)} = \begin{bmatrix} b_1^{(i)} & \cdots & b_{j-1}^{(i)} & b_j^{(i)} & b_{j+1}^{(i)} & b_{n-r}^{(i)} \end{bmatrix}$$
$$\mathbf{b}_{(2)}^{(i)} = \begin{bmatrix} b_1^{(i)} & \cdots & b_{j-1}^{(i)} & a_2 & b_{j+1}^{(i)} & b_{n-r}^{(i)} \end{bmatrix}$$
$$\vdots$$
$$\mathbf{b}_{(s)}^{(i)} = \begin{bmatrix} b_1^{(i)} & \cdots & b_{j-1}^{(i)} & a_s & b_{j+1}^{(i)} & b_{n-r}^{(i)} \end{bmatrix}$$

are all in $\mathcal{S}^{(i)}$. Hence, the vectors

$$\begin{bmatrix} \mathbf{b}^{(1)} \mid \cdots \mid \mathbf{b}^{(i-1)} \mid \mathbf{b}_{(1)}^{(i)} \mid \mathbf{b}^{(i+1)} \mid \cdots \mid \mathbf{b}^{(\mu)} \end{bmatrix}$$
$$\begin{bmatrix} \mathbf{b}^{(1)} \mid \cdots \mid \mathbf{b}^{(i-1)} \mid \mathbf{b}_{(2)}^{(i)} \mid \mathbf{b}^{(i+1)} \mid \cdots \mid \mathbf{b}^{(\mu)} \end{bmatrix}$$
$$\vdots$$
$$\begin{bmatrix} \mathbf{b}^{(1)} \mid \cdots \mid \mathbf{b}^{(i-1)} \mid \mathbf{b}_{(s)}^{(i)} \mid \mathbf{b}^{(i+1)} \mid \cdots \mid \mathbf{b}^{(\mu)} \end{bmatrix}$$

are all in $\mathcal{S}$ and differ only in position j in the i-th block. Furthermore, the entries $b_j^{(i)}, a_2, \ldots, a_s$ in the j-th position in the i-th block are linearly independent over $\mathbb{F}_q$ by construction.

Furthermore, we have $\mathcal{S} = \mathcal{S} \cdot \mathrm{diag}(\mathbf{G}_1, \ldots, \mathbf{G}_\mu) := [\mathbf{b} \cdot \mathrm{diag}(\mathbf{G}_1, \ldots, \mathbf{G}_\mu) : \mathbf{b} \in \mathcal{S}]$ for all invertible matrices $\mathbf{G}_i \in \mathbb{F}_q^{(n-r) \times (n-r)}$. To see this, consider the following: multiplying a subblock $\mathbf{b}^{(i)}$ with an invertible matrix $\mathbf{G}_i$ from the right gives another basis of the same subspace— hence $\mathbf{b}^{(i)} \mathbf{G}_i \in \mathcal{S}^{(i)}$ and $\mathbf{b} \cdot \mathrm{diag}(\mathbf{G}_1, \ldots, \mathbf{G}_\mu) \in \mathcal{S}$ for all $\mathbf{b} \in \mathcal{S}$. Since the $\mathbf{G}_i$ are invertible, the mapping $\mathbf{b} \mapsto \mathbf{b} \cdot \mathrm{diag}(\mathbf{G}_1, \ldots, \mathbf{G}_\mu)$ is bijective.

These two observations imply that a matrix with the elements of $\mathcal{S}$ as rows has the scrambled YB grouping property as in Definition 12. ∎

By combining Theorems 6 and 7, we get the following existence result for a globally-MSR PMDS code.

Corollary 6. *Let μ, n, r, s be valid PMDS parameters. There is a globally-MSR PMDS code with field size*

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

and subpacketization

$$\ell = \left(\begin{bmatrix} n-r+s-1 \\ n-r \end{bmatrix}_q \prod_{i=0}^{n-r-1} \left(q^{n-r} - q^i \right) \right)^\mu$$
$$\le 4^\mu q^{\mu(n-r)(n-r+s-1)}.$$

Proof: The corollary follows directly using the matrix B constructed in Theorem 7 in Construction 3 (see 6). Choosing q as the smallest prime power $\ge n-1$ ensures that there is an $[n, n-r]_q$ MDS code as required in Construction 3. Trivially, there is a power of two with $n-1 \le q < 2(n-1)$, which proves the claim. ∎

Remark 7. *There are no globally-MSR codes in the literature that we can compare the new construction with. Therefore, we only compare the field size and subpacketization to a PMDS code without the globally-MSR property, as well as the subpacketization of an MSR code with the same parameters after puncturing r positions in each local group. I.e., we determine how much we "pay" in terms of field size and subpacketization if we go from a purely PMDS or MSR code to a globally-MSR PMDS code.*

Construction 3 is an adaption of the Gabidulin-based PMDS code construction in [4] (without local or global regeneration), which has field size $q^M < [2(n-1)]^{\mu(n-r)}$. Compared to such a PMDS code, the exponent in the field size in Corollary 6 is larger by a factor $1 + \frac{s-1}{n-r}$. This difference is significant if the number of global parities is large (recall that $1 \le s \le \mu(n-r)$). Hence, we pay more in field size for the globally MSR property if there are many global parities. It appears possible to adapt other PMDS constructions, such as [33] or [16], to have the globally MSR property as well. Such a construction may reduce the field size significantly.

Compared to a Ye–Barg MSR code with parameters $[\mu(n-r), \mu(n-r)-s; \ell]$ (which are the code parameters after puncturing r positions in each group of a PMDS code) with

subpacketization $[(d+1-n+r)\mu(n-r)]^{\mu(n-r)}$, the subpacketization of the globally-MSR PMDS code in Corollary 6 is larger by roughly a factor $(n-r+s-1)$ in the exponent. Roughly spoken, the exponent of the subpacketization is in $O(\mu n)$ without the PMDS property and in $O(\mu n(n+s))$ for a globally-MSR PMDS code.

VII. CONCLUSION

In this paper, we have presented constructions for PMDS array codes with local or global regeneration. We have presented a construction for local regeneration for two global parities, whose field size is polynomial for a fixed number of local parities. Furthermore, we have proposed a general construction that combines an arbitrary family of universal PMDS codes with a local row-wise MDS MSR code. We have explicitly stated the resulting field sizes and subpacketizations for three families of universal PMDS codes, where we first proved the universality property for one existing PMDS construction in the literature. The presented constructions are based on the PMDS code constructions in [15], [4], [33], [16] and Ye–Barg MSR codes [11]. All constructions have a significantly smaller field size than the—to the best of our knowledge—only existing construction of PMDS codes with local regeneration: [4]. We have also compared the new constructions and identified parameter ranges in which they are best in terms of field size.

Moreover, we have presented a construction of a globally MSR PMDS code by introducing a new MSR code, which can be seen as the skew-analog of Ye–Barg codes (similar to the analogy between Gabidulin and Reed–Solomon codes), and combining it with the Gabidulin-code-based PMDS construction in [4]. Compared to the underlying PMDS code, the additional globally-regenerating restriction increases the field size by a factor in the exponent. Similarly, the PMDS property increases the subpacketization compared to a (global) Ye–Barg MSR code, also by a factor in the exponent.

Several open problems related to the presented results offer interesting opportunities for further research. Applying the ideas of the presented constructions to the recently proposed PMDS code constructions of [40], [41], [42] could reduce the required field size. Further, the presented constructions of locally and globally MSR PMDS codes require large levels of subpacketization. The former rely on Ye-Barg regenerating codes, which are known to be suboptimal in terms of subpacketization. However, aside from being optimal in terms of repair bandwidth, they are also row-wise MDS, a property that is essential to the presented constructions. A construction that can afford to relax this requirement could improve the required subpacketization by employing different classes of MSR codes as the local MDS codes. Additionally, the construction of globally MSR PMDS codes is based on Gabidulin codes and thereby inherently suffers from a large required field size. This field size could be lowered by instead employing linearized RS codes to achieve similar gains as shown for locally MSR PMDS codes in Section V. Aside from the improvements of the constructions, lower bounds on the required subpacketization and field size would help evaluate the performance of the presented constructions. Finally, for

the globally MSR PMDS codes, it remains an open problem to utilize surviving local redundancy nodes, in particular in the extreme case where $r + 1$ nodes in a single local group fail while all other nodes survive.

REFERENCES

[1] L. Holzbaur, S. Puchinger, E. Yaakobi, and A. Wachter-Zeh, "Partial MDS codes with local regeneration," in *2020 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2020, pp. 628–633.

[2] 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.

[3] 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.

[4] 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, 2014.

[5] 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, 2018, pp. 1196–1200.

[6] D. Gligoroski, K. Kralevska, R. E. Jensen, and P. Simonsen, "Repair duality with locally repairable and locally regenerating codes," in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*. IEEE, 2017, pp. 979–984.

[7] 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.

[8] 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*, vol. 22, no. 4, pp. 15–26, 2018.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] L. Holzbaur, S. Puchinger, and A. Wachter-Zeh, "On error decoding of locally repairable and partial MDS codes," in *2019 IEEE Information Theory Workshop (ITW)*, 2019, pp. 1–5.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

[20] B. Gastón, J. Pujol, and M. Villanueva, "A realistic distributed storage system that minimizes data storage and repair bandwidth," in *2013 Data Compression Conference*, 2013, pp. 491–491.

[21] J. Pernas, C. Yuen, B. Gastón, and J. Pujol, "Non-homogeneous two-rack model for distributed storage systems," in *2013 IEEE International Symposium on Information Theory*. IEEE, 2013, pp. 1237–1241.

[22] J.-Y. Sohn, B. Choi, and J. Moon, "A class of MSR codes for clustered distributed storage," in *2018 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2018, pp. 2366–2370.

[23] J.-Y. Sohn, B. Choi, S. W. Yoon, and J. Moon, "Capacity of clustered distributed storage," *IEEE Transactions on Information Theory*, vol. 65, no. 1, pp. 81–107, 2018.

[24] H. Hou, P. P. Lee, K. W. Shum, and Y. Hu, "Rack-aware regenerating codes for data centers," *IEEE Transactions on Information Theory*, vol. 65, no. 8, pp. 4730–4745, 2019.

[25] H. Hou, P. P. Lee, and Y. S. Han, "Minimum storage rack-aware regenerating codes with exact repair and small sub-packetization," in *2020 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2020, pp. 554–559.

[26] Y. Hu, P. P. Lee, and X. Zhang, "Double regenerating codes for hierarchical data centers," in *2016 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2016, pp. 245–249.

[27] N. Prakash, V. Abdrashitov, and M. Médard, "The storage versus repair-bandwidth trade-off for clustered storage systems," *IEEE Transactions on Information Theory*, vol. 64, no. 8, pp. 5783–5805, 2018.

[28] M. A. Tebbi, T. H. Chan, and C. W. Sung, "A code design framework for multi-rack distributed storage," in *2014 IEEE Information Theory Workshop (ITW 2014)*. IEEE, 2014, pp. 55–59.

[29] S. Qu, Y. Liu, J. Zhang, H. Cao, and X. Wang, "Multi-rack regenerating codes for hierarchical distributed storage systems," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[30] K. Kralevska, D. Gligoroski, and H. Øverby, "General sub-packetized access-optimal regenerating codes," *IEEE Communications Letters*, vol. 20, no. 7, pp. 1281–1284, 2016.

[31] K. Kralevska, D. Gligoroski, R. E. Jensen, and H. Øverby, "Hashtag erasure codes: From theory to practice," *IEEE Transactions on Big Data*, vol. 4, no. 4, pp. 516–529, 2017.

[32] J. Li, X. Tang, and C. Tian, "A generic transformation to enable optimal repair in MDS codes for distributed storage systems," *IEEE Transactions on Information Theory*, vol. 64, no. 9, pp. 6257–6267, 2018.

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

[34] P. Delsarte, "Bilinear forms over a finite field with applications to coding theory," *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978.

[35] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems of Information Transmission*, vol. 21, no. 1, pp. 3–16, 1985.

[36] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 328–336, 1991.

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

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

[39] T. P. Berger, "Isometries for rank distance and permutation group of Gabidulin codes," *IEEE Transactions on Information Theory*, vol. 49, no. 11, pp. 3016–3019, 2003.

[40] H. Cai, Y. Miao, M. Schwartz, and X. Tang, "A construction of maximally recoverable codes with order-optimal field size," *arXiv preprint arXiv:2011.13606*, 2020.

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

[42] U. Martínez-Peñas, "A general family of MSRD codes and PMDS codes with smaller field sizes from extended Moore matrices," *arXiv preprint arXiv:2011.14109*, 2020.