Explicit MBR All-Symbol Locality Codes

Govinda M. Kamath*, Natalia Silberstein†, N. Prakash*, Ankit S. Rawat†,
V. Lalitha*, O. Ozan Koyluoglu†, P. Vijay Kumar* and Sriram Vishwanath†
* Department of ECE, Indian Institute of Science, Bangalore, India
Email: {govinda, prakashn, lalitha, vijay}@ece.iisc.ernet.in
† Department of ECE, The University of Texas at Austin, Austin, TX
Email: {natalys, ankitsr, ozan, sriram}@austin.utexas.edu

***Abstract*—Node failures are inevitable in distributed storage systems (DSS). To enable efficient repair when faced with such failures, two main techniques are known: Regenerating codes, i.e., codes that minimize the total repair bandwidth; and codes with locality, which minimize the number of nodes participating in the repair process. This paper focuses on regenerating codes with locality, using pre-coding based on Gabidulin codes, and presents constructions that utilize minimum bandwidth regenerating (MBR) local codes. The constructions achieve maximum resilience (i.e., optimal minimum distance) and have maximum capacity (i.e., maximum rate). Finally, the same pre-coding mechanism can be combined with a subclass of fractional-repetition codes to enable maximum resilience and repair-by-transfer simultaneously.**

I. Background

A. Vector Codes

An $[n, K, d_{\min}, \alpha]$ *vector code* over a field $\mathbb{F}_q$ is a code $\mathcal{C}$ of block length n, having a symbol alphabet $\mathbb{F}_q^{\alpha}$ for some $\alpha > 1$, satisfying the additional property that given $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ and $a, b \in \mathbb{F}_q$, $a\mathbf{c} + b\mathbf{c}'$ also belongs to $\mathcal{C}$. As a vector space over $\mathbb{F}_q$, $\mathcal{C}$ has dimension K, termed the scalar dimension (equivalently, the file size) of the code and as a code over the alphabet $\mathbb{F}_q^{\alpha}$, the code has minimum distance $d_{\min}$.

Associated with the vector code $\mathcal{C}$ is an $\mathbb{F}_q$-linear scalar code $\mathcal{C}^{(s)}$ of length $N = n\alpha$, where $\mathcal{C}^{(s)}$ is obtained by expanding each vector symbol within a codeword into α scalar symbols (in some prescribed order). Given a generator matrix G for the scalar code $\mathcal{C}^{(s)}$, the first code symbol in the vector code is naturally associated with the first α columns of G etc. We will refer to the collection of α columns of G associated with the i^{th} code symbol $\mathbf{c}_i$ as the i^{th} thick column and to avoid confusion, the columns of G themselves as thin columns.

B. Locality in Vector Codes

Let $\mathcal{C}$ be an $[n, K, d_{\min}, \alpha]$ vector code over a field $\mathbb{F}_q$, possessing a $(K \times n\alpha)$ generator matrix G. The i^{th} code symbol, $\mathbf{c}_i$, is said to have (r, δ) locality, $\delta \geq 2$, if there exists a punctured code $\mathcal{C}_i := \mathcal{C}|_{S_i}$ of $\mathcal{C}$ (called a *local code*) with support $S_i \subseteq \{1, 2, \cdots, n\}$ such that

- $i \in S_i$,
- $|S_i| \leq n_L := r + \delta - 1$, and
- $d_{\min}(\mathcal{C}|_{S_i}) \geq \delta$.

The code $\mathcal{C}$ is said to have (r, δ) *information locality* if there exists l code symbols with (r, δ) locality and respective support sets $\{S_i\}_{i=1}^{l}$ satisfying

- $\text{Rank}(G|_{\cup_{i=1}^{l} S_i}) = K$.

The code $\mathcal{C}$ is said to have (r, δ) *all-symbol locality* if all code symbols have (r, δ) locality. A code with (r, δ) information (respectively, all-symbol) locality is said to have *full* (r, δ) information (respectively, all-symbol) locality, if all local codes have parameters given by $|S_i| = r + \delta - 1$ and $d_{\min}(\mathcal{C}_i) = \delta$, for $i = 1, \cdots, l$.

The concept of locality for scalar codes, with $\delta = 2$, was introduced in [1] and extended in [2] and [3] to scalar codes with arbitrary δ, and vector codes with $\delta = 2$, respectively. This was further extended to vector codes with arbitrary δ in [4] and [5], where, in addition to constructions of vector codes with locality, authors derive minimum distance upper bounds and also consider settings in which the local codes have regeneration properties.

Consider now a vector code $\mathcal{C}$ with full (r, δ) locality whose associated local codes $\mathcal{C}_i$ have parameters $[n_L, K_L, \delta]$. In this paper, we are interested in local codes that have the uniform rank accumulation property, in particular, local MBR codes and local fractional-repetition codes.

Definition 1 (Uniform rank accumulation (URA) codes)**.** *Let G be a generator matrix for a code $\mathcal{C}$, and S_i be an arbitrary subset of i thick columns of G, for some $i = 1, \cdots, n$. Then, $\mathcal{C}$ is an URA code, if the restriction $G|_{S_i}$ of G to S_i, has rank ρ_i that is independent of the specific subset S_i of i indices chosen and given by $\rho_i = \sum_{j=1}^{i} a_j$ for some set of non-negative integers $\{a_j\}$.*

We will refer to the sequence $\{a_i, 1 \leq i \leq n\}$ as the *rank accumulation profile* of the code $\mathcal{C}$.

We now present the minimum distance upper bound given in [4] for the case when local codes are URA codes. Consider the finite length vector $(a_1, a_2, \cdots, a_{n_L})$, and its extension to a periodic semi-infinite sequence $\{a_i\}_{i=1}^{\infty}$ of period n_L by defining $a_{i+jn_L} = a_i, \ 1 \leq i \leq n_L, \ j \geq 1$. Let $P(\cdot)$ denote the sequence of partial sums,

$$P(s) \quad = \quad \sum_{i=1}^{s} a_i, \quad s \geq 1. \tag{1}$$

Then, given integers $u_1 \geq 0, \quad 1 \leq u_0 \leq n_L$, $P(u_1 n_L + u_0) = u_1 K_L + P(u_0)$. Next, let us define the function $P^{(\text{inv})}$ by setting $P^{(\text{inv})}(\nu)$, for $\nu \geq 1$, to be the smallest integer s such that $P(s) \geq \nu$. It can be verified that for $v_1 \geq 0$ and

$1 \leq v_0 \leq K_L$,

$$P^{(\text{inv})}(v_1 K_L + v_0) \quad = \quad v_1 n_L + P^{(\text{inv})}(v_0),$$

where $P^{(\text{inv})}(v_0) \leq r$ as $1 \leq v_0 \leq K_L$.

The minimum distance of a code $\mathcal{C}$ whose local codes $\mathcal{C}_i$ are URA codes can be bounded as follows.

Theorem I.1 (Theorem 5.1 of [4]). *The minimum distance of $\mathcal{C}$ is upper bounded by*

$$d_{\min} \quad \leq \quad n - P^{(\text{inv})}(K) + 1. \tag{2}$$

The codes achieving the bound in (2) are referred to as codes having optimal locality. For such locality optimal codes, one can then analyze whether the code allows for efficient data storage in DSS. Towards this end, file size bound for codes with locality are given in [5] using the min-cut techniques similar to that of [3]. As noted in [4], when URA codes are used as local codes, the file size bound for $d_{\min}$-optimal codes can be represented in the form

$$\begin{aligned} K &\leq P(n - d_{\min} + 1) \\ &= \left(\left\lceil \frac{n - d_{\min} + 1}{n_L} \right\rceil - 1 \right) K_L + P(l_0), \end{aligned} \tag{3}$$

where $l_0 \in \{1, \cdots, n_L\}$ is such that

$$n - d_{\min} + 1 = \left(\left\lceil \frac{n - d_{\min} + 1}{n_L} \right\rceil - 1 \right) n_L + l_0.$$

We note that $P(l_0) = P(r)$, for $r \leq l_0$.

C. MBR Codes

An $((n, k, d), (\alpha, \beta), K)$ *minimum-bandwidth regenerating* (MBR) code is an $[n, K, d_{\min} = n - k + 1, \alpha]$ vector code satisfying additional constraints described below. The code is intended to be used in a distributed storage network in which each code symbol is stored within a distinct node. The code is structured in such a way that the entire file can be recovered by processing the contents of any k, $1 \leq k \leq n$ nodes. Further, in case of a single node failure, the replacement node can reconstruct the data stored in the failed node by connecting to any d, $k \leq d \leq n-1$, nodes and downloading $\beta = \frac{\alpha}{d}$ symbols from each node. The scalar dimension (or file size) parameter K can be expressed in terms of the other parameters as:

$$K \quad = \quad \left(dk - \binom{k}{2} \right) \beta,$$

as proved in [6]. A cut-set bound derived from network coding shows us that the file size cannot be any larger, and thus, MBR codes are example of regenerating codes that are optimal with respect to file size. A regenerating code is said to be exact if the replacement of a failed node stores the same data as did the failed node, and functional otherwise. We are concerned here only with exact-repair codes. Constructions of MBR codes for all $k \leq d = \alpha < n$ and $\beta = 1$ are presented in [7]. MBR codes with repair by transfer and $d = n - 1$ are presented in [8].

It can be inferred from the results in [8] that MBR codes are URA codes. In particular, for an $((n, k, d), (\alpha, \beta), K)$ MBR code, the rank accumulation profile is given by

$$a_j = \begin{cases} \alpha - (j-1)\beta, & 1 \leq j \leq k \\ 0, & k+1 \leq j \leq n. \end{cases} \tag{4}$$

D. MBR-Local Codes

Let $\mathcal{C}$ be an $[n, K, d_{\min}, \alpha]$ vector code with

- full (r, δ)-information locality with $\delta \geq 2$, and
- all of whose associated local codes $\mathcal{C}_i, i \in \mathcal{L}$ are MBR codes with identical parameters $((n_L = r + \delta - 1, r, d), (\alpha, \beta), K_L)$.

Then, the dimension of each local code is given by

$$K_L \quad = \quad \sum_{i=1}^{n_L} a_i \quad = \quad \alpha r - \binom{r}{2} \beta, \tag{5}$$

where $\{a_i, 1 \leq i \leq n_L\}$ is the rank accumulation profile of the MBR code $\mathcal{C}$.

1) Minimum distance bound for MBR-Local Codes: As MBR codes are URA codes, from Theorem I.1, we have

$$d_{\min} \leq n - P^{(\text{inv})}(K) + 1, \tag{6}$$

where, for MBR codes we have

$$P^{(\text{inv})}(v_1 K_L + v_0) = v_1 n_L + \nu \tag{7}$$

for some $v_1 \geq 0$, $1 \leq v_0 \leq K_L$, and ν is uniquely determined from $\alpha(\nu - 1) - \binom{\nu - 1}{2}\beta < v_0 \leq \alpha\nu - \binom{\nu}{2}\beta$.

2) File size bound for MBR-Local Codes: From (3), the file size bound for an optimal locality code with MBR local codes is given by

$$K \leq \left(\left\lceil \frac{n - d_{\min} + 1}{n_L} \right\rceil - 1 \right) K_L + \alpha\mu - \binom{\mu}{2}\beta, \tag{8}$$

where $\mu = \min\{l_0, r\}$ with l_0 as defined in Subsection I-B. Note that (8) follows from the rank accumulation profile of MBR codes, i.e., from (4).

E. Linearized Polynomials

A polynomial $f(x)$ over the field $\mathbb{F}_{q^m}$, is said to be *linearized* of q-degree t, if

$$f(x) = \sum_{i=0}^{t} u_i x^{q^i} \ , \ u_i \in \mathbb{F}_{q^m}, \ u_t \neq 0. \tag{9}$$

A linearized polynomial $f(x)$ over $\mathbb{F}_{q^m}$ satisfies the following property [9]:

$$\begin{aligned} f(\lambda_1\theta_1 + \lambda_2\theta_2) &= \lambda_1 f(\theta_1) + \lambda_2 f(\theta_2) \\ &\quad \forall\ \theta_1, \theta_2 \in \mathbb{F}_{q^m},\ \lambda_1, \lambda_2 \in \mathbb{F}_q. \end{aligned} \tag{10}$$

A linearized polynomial $f(x)$ over $\mathbb{F}_{q^m}$ of q-degree t, $m > t$, is uniquely determined from its evaluation at a set of $(t+1)$ points $g_1, \cdots, g_{t+1} \in \mathbb{F}_{q^m}$, that are linearly independent over $\mathbb{F}_q$.

F. Gabidulin Maximum Rank Distance Codes

Now, we present a construction of maximum rank distance codes, provided by Gabidulin in [10]. This codes can be viewed as a rank-metric analog of Reed-Solomon codes.

The *rank* of a vector $\mathbf{v} \in \mathbb{F}_{q^m}^{\mathcal{N}}$, denoted by $\mathrm{rank}(\mathbf{v})$ is defined as the rank of the $m \times \mathcal{N}$ matrix $\mathbf{V}$ over $\mathbb{F}_q$, obtained by expansion of every entry of $\mathbf{v}$ to a column vector in $\mathbb{F}_q^m$, based on the isomorphism between $\mathbb{F}_{q^m}$ and $\mathbb{F}_q^m$. Similarly, for two vectors $\mathbf{v}, \mathbf{u} \in \mathbb{F}_{q^m}^{\mathcal{N}}$, the *rank distance* is defined by $d_R(\mathbf{v}, \mathbf{u}) = \mathrm{rank}(\mathbf{V} - \mathbf{U})$.

An $[\mathcal{N}, \mathcal{K}, \mathcal{D}]_{q^m}$ rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^{\mathcal{N}}$ is a linear block code over $\mathbb{F}_{q^m}$ of length $\mathcal{N}$, dimension $\mathcal{K}$ and minimum rank distance $\mathcal{D}$. A rank-metric code that attains the Singleton bound $\mathcal{D} \leq \mathcal{N} - \mathcal{K} + 1$ in rank-metric is called a *maximum rank distance* (MRD) code. For $m \geq \mathcal{N}$, a construction of MRD codes, called Gabidulin codes is given as follows [10].

A codeword in an $[\mathcal{N}, \mathcal{K}, \mathcal{D} = \mathcal{N} - \mathcal{K} + 1]_{q^m}$ Gabidulin code $\mathcal{C}^{\mathrm{Gab}}$, $m \geq \mathcal{N}$, is defined as $\mathbf{c} = (f(\theta_1), f(\theta_2), \ldots, f(\theta_{\mathcal{N}})) \in \mathbb{F}_{q^m}^{\mathcal{N}}$, where $f(x)$ is a linearized polynomial over $\mathbb{F}_{q^m}$ of q-degree at most $\mathcal{K} - 1$ with the coefficients given by the information message, and where the $\theta_1, \ldots, \theta_{\mathcal{N}} \in \mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$ [10].

II. Construction of Codes with MBR Locality

In this section, we will present two constructions of codes with local regeneration. In both cases, the local codes are MBR codes with identical parameters and both codes are optimal, i.e., they achieve the upper bound of Theorem I.1 on minimum distance. The first construction is an all-symbol locality construction, while the second has information locality.

The constructions presented in this paper, adopt the linearized polynomial approach made use of in [11], [12], [5]. In particular, similar to the constructions proposed in [12], [5], the constructions of this paper have a two-step encoding process with the first step utilizing Gabidulin codes, which in turn, are based on linearized polynomials. The first code construction given below also proves the tightness of the bound on minimum distance of codes with URA derived in [4] (Theorem 5.1) for the case when $K_L \nmid K$, where K_L is the scalar dimension of the local MBR code.

Consider a code $\mathcal{C}_{\text{BASIC}}$ that is simply the concatenation of t local MBR codes having identical parameters $((n_L, k, d), (\alpha, \beta), K_L)$. Thus a typical codeword $\mathbf{c} \in \mathcal{C}_{\text{BASIC}}$ looks like

$$\mathbf{c} \quad = \quad \left(\begin{array}{cccc} \mathbf{c}_1^{\mathrm{mbr}} & \mathbf{c}_2^{\mathrm{mbr}} & \cdots & \mathbf{c}_t^{\mathrm{mbr}} \end{array} \right),$$

where each vector $\mathbf{c}_i^{\mathrm{mbr}}$ is a codeword belonging to the MBR code. The generator matrix G_{BASIC} of the code will clearly have a block-diagonal structure. It is straightforward to show that the smallest number ρ, such that any ρ thick columns of G_{BASIC} have rank $\geq K$ is given by $P^{(\mathrm{inv})}(K)$, for any $1 \leq K \leq tK_L$.

Construction II.1. *We will describe the construction by showing how encoding of a message vector takes place. The encoding is illustrated in Fig. 1. Given the message vector* $\mathbf{u} \in \mathbb{F}_{q^m}^{K}$, *we first encode* $\mathbf{u}$ *to a* tK_L *long Gabidulin codeword using* tK_L *linearly independent points (over* $\mathbb{F}_q$*)* $\{\theta_1, \theta_2, \ldots, \theta_{tK_L}\} \subset \mathbb{F}_{q^m}$, *i.e., by applying an* $[tK_L, K, tK_L - K + 1]_{q^m}$ *Gabidulin code, assuming* $m \geq tK_L$. *We then partition* tK_L *symbols of the Gabidulin codeword,* $(f(\theta_1), f(\theta_2), \ldots, f(\theta_{tK_L}))$, *into* t *disjoint sets of* K_L *symbols each. Each of these sets is then fed in as a message vector to a bank of* t *identical MBR encoders whose outputs constitute* $((n_L, r, d), (\alpha, \beta), K_L)$ *MBR codes. If* $\{\mathbf{c}_i^{\mathrm{mbr}} \mid i = 1, 2, \ldots, t\}$ *is the resulting set of* t *codewords, these codewords are then concatenated to obtain the desired codeword* $\mathbf{c}$. *The code* $\mathcal{C}$ *thus constructed has:*

- *length* $n = tn_L$
- t *local* $((n_L, r, d), (\alpha, \beta), K_L)$ *MBR codes with disjoint supports*
- *full* (r, δ) *all-symbol locality where* δ *is defined from* $n_L = r + \delta - 1$.

Theorem II.2. *Given any set of parameters* n, r, δ, K, *such that* $n = tn_L$ *and* $K \leq tK_L$, *the construction II.1, yields an optimal MBR-local code with full* (r, δ) *all-symbol locality whose minimum distance is given by*

$$d_{\min} = n \ - \ P^{(inv)}(K) + 1.$$

We first present a useful lemma on codes that are obtained by concatenating a Gabidulin code (over $\mathbb{F}_{q^m}$) with a vector code (over $\mathbb{F}_q$).

Lemma II.3. *Let* G *be the generator matrix of an* $[n, J, d_{\min}, \alpha]$ *vector code over the field* $\mathbb{F}_q$. *Let* $\tilde{J}$ *be an integer such that* $\tilde{J} \leq J$. *Let* ρ *be the smallest integer, such that the submatrix of* G *obtained by selecting any* ρ *thick columns of* G *results in a matrix of rank* $\geq \tilde{J}$. *Let*

$$f(x) = \sum_{i=0}^{\tilde{J}-1} u_i x^{q^i}, u_i \in \mathbb{F}_{q^m}, \quad m > J,$$

be a linearized polynomial of q-degree at most $\tilde{J} - 1$ *over the extension field* $\mathbb{F}_{q^m}$, *for* $m \geq J$. *Let* $\{\theta_i\}_{i=1}^{J}$ *be any collection of* J *elements of* $\mathbb{F}_{q^m}$ *that are linearly independent over* $\mathbb{F}_q$. *The mapping*

$$(u_0, u_1, \cdots, u_{\tilde{J}-1}) \quad \rightarrow \quad (f(\theta_1), f(\theta_2), \cdots, f(\theta_J))G$$

defines a linear code $\mathcal{C}$ *over* $\mathbb{F}_{q^m}$ *having message vector* $(u_0, u_1, \cdots, u_{\tilde{J}-1})$. *Then* $\mathcal{C}$ *has minimum distance* $D_{\min}$ *given by*

$$D_{\min} \quad = \quad n - \rho + 1,$$

i.e., $\mathcal{C}$ *is an* $[n, \tilde{J}, D_{\min}]$ *code over* $\mathbb{F}_{q^m}$.

Proof: Since $f(\cdot)$ is linearized, we can interchange linear operations with the operation of evaluation:

$$(f(\theta_1) \ f(\theta_2) \ \cdots f(\theta_J))G \quad = \quad f\left((\theta_1 \ \theta_2 \cdots \theta_J)G\right).$$

We have extended here the definition of $f(\cdot)$ to vectors through termwise application. Consider next, the matrix product

$$\Gamma \quad := \quad [\theta_1 \ \theta_2 \cdots \theta_J]G.$$

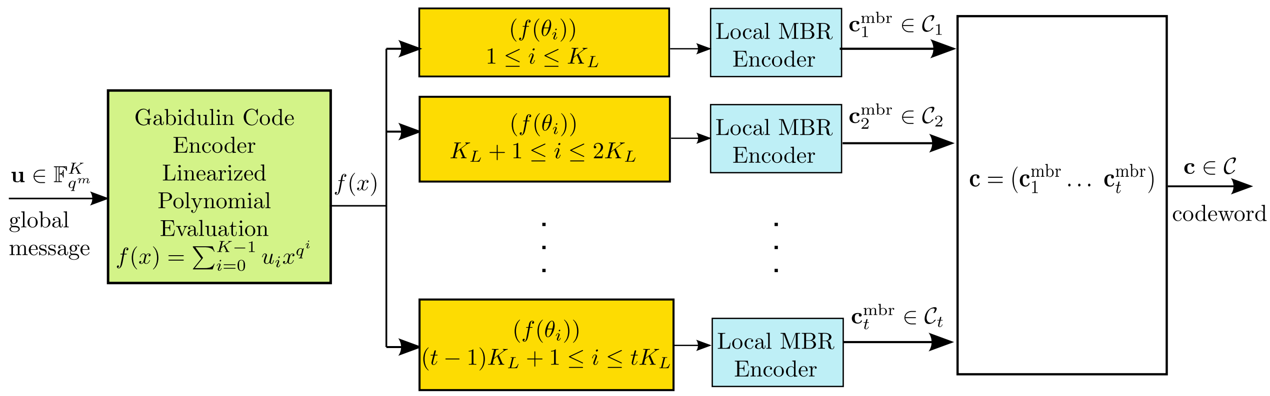

Fig. 1. Illustrating the two-step construction of the all-symbol MBR-local code.

In writing this, we have abused notation and identified elements in $\mathbb{F}_{q^m}$ with their representations as vectors over $\mathbb{F}_q$ lying in $\mathbb{F}_q^m$. The $m \times J$ matrix $[\theta_1\ \theta_2 \cdots \theta_J]$ on the left has the property that all of its columns are linearly independent. Hence linear dependence relations amongst columns of Γ are precisely those inherited from the matrix G. It follows that ρ is also the smallest number, such that any ρ thick columns of the product matrix Γ have rank $\geq \tilde{J}$. Since $f(\cdot)$ is uniquely determined by its evaluation at a collection of $\tilde{J}$ linearly independent vectors lying in $\mathbb{F}_q^m$, it follows that the maximum number of erasures that the code $\mathcal{C}$ can recover from is given by $n-\rho$. Then, we have

$$D_{\min} \quad = \quad n - \rho + 1.$$

■

Proof: (of Thm. II.2) Let G_{BASIC} be the generator matrix of the code that is simply the disjoint union of the t MBR codes. As it was explained previously, the smallest number ρ of thick columns of G_{BASIC} such that any ρ columns of G_{BASIC} have rank $\geq K$ is given by $P^{(\text{inv})}(K)$. It follows therefore from Lemma II.3 (by substituting $\tilde{J} = K$, $J = tK_L$ and also assuming that G_{BASIC} is over $\mathbb{F}_q$) that the code has minimum distance given by

$$d_{\min} \quad = \quad n \quad - \quad P^{(\text{inv})}(K) + 1,$$

hence the code attains the bound of Theorem I.1, and thus, optimal. ■

Remark 1. *We note that whenever $K = v_1 K_L + v_0$, $v_1 \geq 0$, $1 \leq v_0 \leq K_L$ is such that $v_0 = \nu\alpha - \binom{\nu}{2}\beta$ for some $1 \leq \nu \leq r$, then the code constructed by Construction II.1 has maximum possible scalar dimension given in (8). This observation holds for the code we will construct using Construction II.4 as well.*

Construction II.4. *We describe here a method by which we construct a code of length $n = tn_L + \Delta$, with (r,δ)* information *locality for scalar dimension $K \leq tK_L$. Given the message vector $\mathbf{u} \in \mathbb{F}_{q^m}^K$, we first encode $\mathbf{u}$ to a $tK_L + \Delta\alpha$ long Gabidulin codeword using a $[tK_L + \Delta\alpha, K, tK_L + \Delta\alpha - K + 1]_{q^m}$ Gabidulin code, for $m \geq tK_L + \Delta\alpha$. We then divide the first tK_L symbols of the Gabidulin codeword into t disjoint groups of equal size and encode each of these t groups using an $((n_L, r, d), (\alpha, \beta), K_L)$ MBR code (similar to the second step of encoding in Construction II.1). This gives us a code of length tn_L with MBR all-symbol locality, whose elements are $\{\mathbf{c}_i^{\text{mbr}} \mid i = 1, 2, \ldots, t\}$. We then partition the remaining $\Delta\alpha$ symbols of the Gabidulin codeword into Δ equal sets and denote the i^{th} set by $\mathbf{c}_{tn_L+i}$. The construction outputs $(\mathbf{c}_1^{\text{mbr}}, \ldots, \mathbf{c}_t^{\text{mbr}}, \mathbf{c}_{tn_L+1}, \ldots, \mathbf{c}_{tn_L+\Delta})$ as a final codeword. The resultant vector code $\mathcal{C}$ has:*

- *Length $n = tn_L + \Delta$*
- *t local $((n_L, r, d), (\alpha, \beta), K_L)$ MBR codes with disjoint support*
- *full (r, δ) information locality*

Theorem II.5. *Given any set of parameters n, r, δ, K, such that $n = tn_L + \Delta$ and $K \leq tK_L$, Construction II.1 results in an optimal MBR-local code with (r,δ) information locality whose minimum distance is given by*

$$d_{\min} = n \quad - \quad P^{(inv)}(K) + 1.$$

Proof: The proof follows along the same lines as the proof of Theorem II.2. ■

III. Fractional-Repetition Codes as Local Codes

In this section, we discuss the usage of fractional repetition (FR) codes as local codes in Constructions II.1 and II.4. FR codes can be viewed as a generalization of repair-by-transfer MBR codes, where a repair process is *uncoded* and *table-based*, i.e., FR codes have a "repair-by-transfer" property, while only specific sets of nodes of size d participate in a node repair process. For the sake of completeness, we provide an overview of the t-design-based construction for FR codes presented in [13][1].

Let t, n, w, λ be integers with $n > w \geq t$ and $\lambda > 0$. A t-(n, w, λ) design is a collection $\mathcal{B}$ of w-subsets (the *blocks*), of an n-set $\mathcal{X}$ (the *points*), such that every t-subset of $\mathcal{X}$ is

[1]The construction in [13] sets $t = 2$ and $\lambda = 1$; and the corresponding codes are called transposed codes.

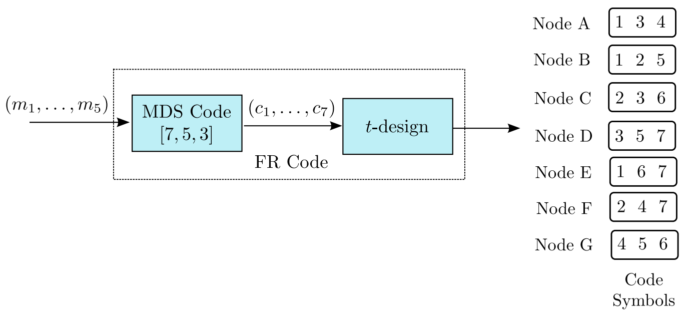

Fig. 2. Fractional Repetition Code based on $2-(7,3,1)$ design.

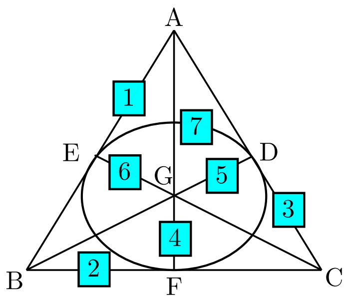

Fig. 3. Fano Plane, a $2-(7,3,1)$ design.

contained in exactly λ blocks. Let $x_1,\ldots,x_t \in \mathcal{X}$ be a set of t points. We denote by λ_s the number of blocks containing $x_1,\ldots,x_s$, $1 \le s \le t$. Then,

$$\lambda_s = \lambda \frac{\binom{n-s}{t-s}}{\binom{w-s}{t-s}};$$

the number of blocks in the t-design is $b = \lambda_0 = \lambda\binom{n}{t}/\binom{w}{t}$; and each point in $\mathcal{X}$ is contained in λ_1 blocks where $\lambda_1 = \lambda\binom{n-1}{t-1}/\binom{w-1}{t-1}$ [9].

Construction III.1. *Let $B_1,\ldots,B_b \in \mathcal{B}$ be the blocks and $x_1,\ldots,x_n \in \mathcal{X}$ the points of a t-(n,w,λ) design. Then the n nodes of a FR code C are given by the points of the design, i.e., a node N_i contains $\alpha \triangleq \lambda_1$ symbols given by $N_i = \{j : x_i \in B_j\}$. Note that the cardinality of an intersection of any $s \le t$ nodes are given by the numbers λ_s, and hence the cardinality of a union of any $s \le t$ nodes can be easily derived by the inclusion-exclusion formula. Let k, K be two integers such that $k \le t$ and*

$$|\bigcup_{i=1}^{k-1} N_i| < K \le |\bigcup_{i=1}^{k} N_i|. \tag{11}$$

Then we have an FR code over an alphabet of size b, with the property that there exists *a set of d nodes which can repair a failed node and from* any *set of k nodes one can reconstruct the original K symbols.*

Given a message vector $[m_1\ m_2\ \cdots m_K]$, we encode the message symbols first by using an $[b, K, b-K+1]$ MDS code to produce b coded symbols $(c_1,\ c_2 \cdots c_b)$ and then by employing the FR code based on the t-design to produce n nodes each containing λ_1 symbols.

This family of FR codes based on t-designs is also an example of codes with uniform rank accumulation, and thus the bound of Theorem I.1 can be used here as well. Thus, we have the following result.

Theorem III.2. *When FR codes based on a t-design obtained by Construction III.1 are used as the local codes in Constructions II.1 and II.4, then the resulting code with locality attains the bound of Theorem I.1 on minimum distance.*

An example of an encoding is shown in Fig. 2, where the encoding is done using 2-$(7,3,1)$ design, also known as the Fano plane (see Fig. 3). When we replace a local MBR code with the FR code based on Fano plane in Fig. 1, we obtain a code with locality which has the optimal minimum distance.

Acknowledgements

This research is supported in part by the National Science Foundation under Grant 0964507 and in part by the NetApp Faculty Fellowship program. The work of V. Lalitha is supported by a TCS Research Scholarship.

References

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

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

[3] D. S. Papailiopoulos and A. G. Dimakis, "Locally repairable codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Cambridge, MA, Jul. 2012, pp. 2771–2775.

[4] G. M. Kamath, N. Prakash, V. Lalitha, and P. V. Kumar, "Codes with local regeneration," Nov. 2012. [Online]. Available: arXiv:1211.1932

[5] A. S. Rawat, O. O. Koyluoglu, N. Silberstein, and S. Vishwanath, "Optimal locally repairable and secure codes for distributed storage systems," Oct. 2012. [Online]. Available: arXiv:1210.6954

[6] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4539–4551, Sep. 2010.

[7] K. V. Rashmi, N. B. Shah, and P. V. Kumar, "Optimal exact-regenerating codes for distributed storage at the MSR and MBR points via a product-matrix construction," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5227–5239, Aug. 2011.

[8] N. B. Shah, K. V. Rashmi, P. V. Kumar, and K. Ramchandran, "Distributed storage codes with repair-by-transfer and nonachievability of interior points on the storage-bandwidth tradeoff," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1837–1852, Mar. 2012.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1983.

[10] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems of Information Transmission*, vol. 21, pp. 1–12, July 1985.

[11] F. Oggier and A. Datta, "Self-repairing homomorphic codes for distributed storage systems," in *Proc. IEEE Int. Conf. Comput. Communications (INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1215–1223.

[12] N. Silberstein, A. S. Rawat, and S. Vishwanath, "Error resilience in distributed storage via rank-metric codes," in *Proc. 50th Annual Allerton Conf. on Communication, Control, and Computing (Allerton)*, Urbana-Champaign, IL, Oct. 2012, pp. 1150 –1157.

[13] S. El Rouayheb and K. Ramchandran, "Fractional repetition codes for repair in distributed storage systems," in *Proc. 48th Annual Allerton Conf. on Communication, Control, and Computing (Allerton)*, Urbana-Champaign, IL, Sep. 2010, pp. 1510 –1517.