Quasicyclic MDS Codes for Distributed Storage with Efficient Exact Repair

Andrew Thangaraj and Chinnadhurai Sankar
Department of Electrical Engineering
Indian Institute of Technology Madras
Chennai 600036, India
Email: andrew@ee.iitm.ac.in

***Abstract*—In a distributed storage system, codes for efficient repair of failed nodes has attracted significant recent research attention. Ideas from network coding and interference alignment have been used successfully to show bounds and construct coding schemes for efficient repair. In this article, we use ideas from classical algebraic codes to interpret the requirements of efficient repair as existence of certain specific types of codewords in the dual code. Since the construction is quasicyclic and works over small fields, it appears to be a promising method for reducing the computational complexity of efficient repair codes.**

I. Introduction and Notation

We consider a distributed storage system, where a K-bit message is encoded into a N-bit codeword and stored in $n = N/b$ nodes with each node storing b bits. The code is constructed such that a *data collector*, interested in accessing the message, will be able to recover the message by connecting to any $k = K/b$ out of the n nodes, downloading $kb = K$ bits and running a decoding algorithm. Therefore, from a data collector's point of view, maximum distance separable (MDS) codes provide a natural construction for distributed storage. Frequently, a node in the distributed storage system will fail requiring replacement by another node. The process of replicating the information of a failed node in a new node is called *exact repair*. Seminal study of efficient repair in distributed storage systems was reported in [1]. Several code constructions for different types of repair and limits have been later reported, and these results have been summarized in [2]. As a result of these studies, it has become apparent that standard MDS codes are not sufficient by themselves for efficient and exact repair. In this article, we report constructions of quasicyclic MDS codes that allow for efficient exact repair. We will use the following notation to describe our construction.

We will let $b = \alpha m$ (for some positive integers α and m), and view the bits stored in each node as a length-α vector over GF(2^m). The vector stored in node i is denoted $\bar{c}_i = [c_{i,1}\ c_{i,2}\ \cdots\ c_{i,\alpha}]$, $1 \leq i \leq n$ with coordinates $c_{i,j} \in$ GF(2^m). A codeword distributed over n nodes is denoted $\mathbf{c} = [\bar{c}_1\ \bar{c}_2\ \cdots\ \bar{c}_n]$. The set of all such codewords is denoted as the code C. We see that the code C is over the alphabet $\mathcal{A} =$ GF$(2^m)^\alpha$, which denotes the set of all α-tuples over GF(2^m). So, $|\mathcal{A}| = 2^{\alpha m}$, and the blocklength of C is n over $\mathcal{A}$. The message length of C over $\mathcal{A}$ is $k = K/b$.

In the "distributed storage with efficient repair" problem , the following properties of C are important considerations:

1) Data collection: The K-bit message can be recovered from $[\bar{c}_i : i \in S]$ for any subset $S \subseteq \{1, 2, \cdots, n\}$ with $|S| = k$.
2) Efficient, exact repair for node n: In case node n fails, the bits $\bar{c}_n$ in node n can be computed exactly with $\beta_i < \alpha$ symbols over GF(2^m) sent from node i for $1 \leq i \leq n-1$. The number of symbols sent for repair $\sum_{i=1}^{n-1} \beta_i$ should be strictly lesser than $k\alpha = K$, the number required for data collection.

For the data collection property to be satisfied, it is clear that the code C will have to be MDS over the alphabet $\mathcal{A}$ with a minimum distance (over $\mathcal{A}$) of $n - k + 1$.

The code C is said to be *quasicyclic*, if $[\bar{c}_1\ \bar{c}_2\ \cdots\ \bar{c}_n] \in C$ implies $[\bar{c}_2\ \bar{c}_3\ \cdots\ \bar{c}_n\ \bar{c}_1] \in C$. If C is quasicyclic, ensuring efficient exact repair for node n guarantees that the same repair property is applicable for all nodes.

Another useful view of a codeword of C is the following. A codeword $\mathbf{c} = [\bar{c}_1\ \bar{c}_2\ \cdots\ \bar{c}_n]$ can be thought of as a concatenation of α length-n vectors $\mathbf{c}_i = [c_{1,i}\ c_{2,i}\ \cdots\ c_{n,i}]$ for $i = 1, 2, \cdots, \alpha$. We will use the notation $\mathbf{c} = [\mathbf{c}_1|\mathbf{c}_2|\cdots|\mathbf{c}_\alpha]$ to denote this concatenation. Note that each vector $\mathbf{c}_j$ is stored over n nodes with one symbol $c_{i,j}$ stored in node i.

Since we consider cyclic codes over the field GF(2^m), we will assume that n is odd. This ensures that there exists a positive integer s such that n divides $2^{sm} - 1$. Extensions for general n are possible using standard methods.

In the terminology of [2] [3], we have let $d = n - 1$ be the number of nodes that will participate in the regeneration. The code C is said to be MSR (minimum storage regenerating) with no symbol extension if $\beta_i = 1$ (for all i) and $\alpha = n - k$. The efficiency of regeneration using a non-MSR code C can be measured by comparison with a MSR code. Since a MSR code needs $n-1$ symbols for repair, the difference $\sum_{i=1}^{n-1} \beta_i - (n-1)$ is a measure of efficiency in repair.

In prior work, product matrix and interference alignment ideas were used in [3] [4] for constructing codes and developing bounds on parameters for which exact repair is possible. In [5] and [6], algebraic ideas have been used in code construction. While [5] presents codes of rate 1/2, projective geometry ideas are used in [6]. In contrast, we use ideas from standard cyclic coding theory in our construction and the method can be used for rates greater than 1/2 as well.

II. Construction for $\alpha = 2$

For $\alpha = 2$, the code C is defined as follows:

$$C = \{[\mathbf{c}_1|\mathbf{c}_2] : \begin{bmatrix} H_{11} \\ H_{12} \end{bmatrix} \mathbf{c}_1^T + \begin{bmatrix} \mathbf{0} \\ H_{22} \end{bmatrix} \mathbf{c}_2^T = 0\}, \quad (1)$$

where H_{11}, H_{12} and H_{22} are $(n-k)\times n$ matrices with entries from GF(2^m), and $\mathbf{0}$ represents a $(n-k)\times n$ all-zero matrix. We will choose the matrices H_{ii} $(i = 1, 2)$ to be parity-check matrices of (n, k) cyclic codes (denoted C_{ii}) over GF(2^m). The first row of H_{ii}, denoted $[h_{ii,0}\ h_{ii,1}\ \cdots\ h_{ii,n-1}]$, specified in polynomial notation as $h_{ii}(x) = \sum_{l=0}^{n-1} h_{ii,l}x^l$, is the check polynomial of C_{ii}. The second row of H_{ii} is a cyclic right shift of the first row, and so on for other rows. As per standard cyclic codes theory [7], $h_{ii}(x)$ is a degree-k polynomial that divides $x^n + 1$.

The first row of H_{12}, denoted $[h_{12,0}\ h_{12,1}\ \cdots\ h_{12,n-1}]$, is written as $h_{12}(x) = \sum_{l=0}^{n-1} h_{12,l}x^l$ in polynomial notation. The second row of H_{12} will be a cyclic right shift of the first row, and so on, as before. However, unlike the $h_{ii}(x)$, we will not impose any degree or divisor constraint on $h_{12}(x)$, as of now.

A. Dimension of C

The definition in (1) implies that for a codeword $\mathbf{c}$, we need (a) $H_{11}\mathbf{c}_1^T = 0$ and (b) $H_{12}\mathbf{c}_1 = H_{22}\mathbf{c}_2$. There are $(2^m)^k$ vectors $\mathbf{c}_1$ that satisfy (a). For each such choice, there are $(2^m)^k$ vectors $\mathbf{c}_2$ that satisfy (b). Hence, the total number of codewords in C is $(2^m)^{2k} = (2^{2m})^k$, and the dimension of C over $\mathcal{A} = \text{GF}(2^m)^2$ is k.

We proceed to determine conditions on $h_{ij}(x)$ that make the overall code C MDS over $\mathcal{A}$ and quasicyclic.

B. MDS condition

Let the minimum distance of C_{ii} be d_i for $i = 1, 2$.

For a nonzero $\mathbf{c} \in C$, either (a) $\mathbf{c}_1 \neq 0$, which implies $\text{wt}(\mathbf{c}_1) \geq d_1$, since $H_{11}\mathbf{c}_i^T = 0$ according to the definition of (1); or (b) if $\mathbf{c}_1 = 0$, then $\mathbf{c}_2 \neq 0$ and $H_{22}\mathbf{c}_2^T = 0$ according to the definition of (1). Hence, $\text{wt}(\mathbf{c}_2) \geq d_2$.

Therefore, for a nonzero codeword $\mathbf{c} \in C$, $\text{wt}(\mathbf{c}) \geq \min(d_1, d_2)$ over the alphabet $\mathcal{A}$. Now, for C to be MDS, we need $\min(d_1, d_2) = n - k + 1$ with $d_1 \leq n - k + 1$ and $d_2 \leq n-k+1$. This condition is satisfied if $d_1 = d_2 = n-k+1$ i.e. C_{ii} are MDS over GF(2^m).

C. Quasicyclic condition

For the code C as defined in (1) to be quasicyclic, we need

$$h_{12}(x)\hat{h}_{22}(x) = 0 \mod h_{11}(x), \quad (2)$$

where $\hat{h}_{22}(x) = (x^n + 1)/h_{22}(x)$. The proof is given in the appendix.

D. Efficient and Exact Repair

We use the dual of C to determine and describe conditions for efficient exact repair. A vector $\mathbf{b} = [\bar{b}_1\ \bar{b}_2\ \cdots\ \bar{b}_n]$, where $\bar{b}_i = [b_{i,1}\ b_{i,2}]$ and $b_{i,j} \in \text{GF}(2^m)$, is said to be in the dual of C as defined in (1), if

$$[b_{1,1}\ b_{2,1} \cdots b_{n,1}]\mathbf{c}_1^T + [b_{1,2}\ b_{2,2} \cdots b_{n,2}]\mathbf{c}_2^T = 0 \quad (3)$$

for all $\mathbf{c} \in C$. In concatenation notation, we will denote a dual vector as $\mathbf{b} = [\mathbf{b}_1|\mathbf{b}_2]$, where $\mathbf{b}_i = [b_{1,i}\ b_{2,i} \cdots b_{n,i}]$ for $i = 1, 2$.

From (1), we see that $[\mathbf{u}H_{11} + \mathbf{v}H_{12}|\mathbf{v}H_{22}]$ is a dual vector for C for all length-$(n - k)$ vectors $\mathbf{u}$ and $\mathbf{v}$ over GF(2^m). Let us denote the set of such dual vectors as

$$C^\perp = \{[\mathbf{u}H_{11} + \mathbf{v}H_{12}|\mathbf{v}H_{22}] : \mathbf{u}, \mathbf{v} \in \text{GF}(2^m)^{n-k_2}\}. \quad (4)$$

Suppose node n fails, and a new node can access the nodes 1 to $n - 1$. In that case, $c_{i,j}$ for $1 \leq i \leq n - 1$ and $j = 1, 2$ are available for download to the new node, while $c_{n,1}$ and $c_{n,2}$ are unknowns. Note that a dual vector $\mathbf{b}$ provides one equation, such as (3), involving the two unknowns. So, given two dual vectors, say $[\mathbf{a}_1|\mathbf{a}_2]$ and $[\mathbf{b}_1|\mathbf{b}_2]$ in $C^\perp$, the new node can attempt to solve for the two unknowns and replicate the information in the failed node n. The equation to be solved can be written as follows:

$$\begin{bmatrix} \mathbf{a}_1|\mathbf{a}_2 \\ \mathbf{b}_1|\mathbf{b}_2 \end{bmatrix} [\mathbf{c}_1|\mathbf{c}_2]^T = \begin{bmatrix} \mathbf{a}_1 \\ \mathbf{b}_1 \end{bmatrix} \mathbf{c}_1^T + \begin{bmatrix} \mathbf{a}_2 \\ \mathbf{b}_2 \end{bmatrix} \mathbf{c}_2^T = 0,$$

which can be rewritten as

$$M_1 \begin{bmatrix} c_{1,1} \\ c_{1,2} \end{bmatrix} + M_2 \begin{bmatrix} c_{2,1} \\ c_{2,2} \end{bmatrix} + \cdots + M_{n-1} \begin{bmatrix} c_{n-1,1} \\ c_{n-1,2} \end{bmatrix} = M_n \begin{bmatrix} c_{n,1} \\ c_{n,2} \end{bmatrix}, \quad (5)$$

where

$$M_i = \begin{bmatrix} a_{i,1} & a_{i,2} \\ b_{i,1} & b_{i,2} \end{bmatrix} \quad (6)$$

for $i = 1, 2, \cdots, n$.

For (5) to be solvable for the two unknowns $c_{n,1}$ and $c_{n,2}$, we need that $\text{rank}(M_n) = 2$. Also, we see that the number of symbols to be downloaded from node i is given as $\beta_i = \text{rank}(M_i)$ for $i = 1, 2, \cdots, n-1$. For the code C to be MSR, we require that $\beta_i = 1$ and $\alpha = n - k = 2$. So, for C to be MSR, we require $n - k = 2$ and $[\mathbf{a}_1|\mathbf{a}_2]$, $[\mathbf{b}_1|\mathbf{b}_2]$ in $C^\perp$ such that

$$\begin{aligned} a_{n,1}b_{n,2} + a_{n,2}b_{n,1} &\neq 0, \\ a_{i,1}b_{i,2} + a_{i,2}b_{i,1} &= 0, 1 \leq i \leq n-1. \end{aligned}$$

In vector notation the above MSR condition can be written as

$$\mathbf{a}_1 * \mathbf{b_2} + \mathbf{a}_2 * \mathbf{b}_1 = [0 \cdots 0\ \delta], \quad (7)$$

where $*$ denotes the element-wise product of two vectors ($\mathbf{x} * \mathbf{y} = [x_1y_1\ x_2y_2 \cdots x_ny_n]$) and $\delta \in \text{GF}(2^m)$ is nonzero.

III. Fourier Domain Construction for $\alpha = 2$

Since n divides $2^{sm}-1$, there exists a primitive n-th root of unity in GF(2^{sm}), which we denote γ. Also, GF(2^m) is a subfield of GF(2^{sm}). For a length-n vector $\mathbf{a} = [a_0\ a_1 \cdots a_{n-1}]$ (in polynomial notation, $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}$) with $a_i \in$GF(2^m), the finite Fourier transform or the Mattson-Solomon (MS) polynomial [7] is defined as $A(z) = \sum_{j=0}^{n-1} A_{-j} z^j$, where $A_j = a(\gamma^j) = \sum_{i=0}^{n-1} a_i \gamma^{ij}$ for $j = 0, \pm 1, \pm 2, \cdots$. We will use the following notation: for a vector $\mathbf{a}$, the polynomial notation is $a(x)$ and the Fourier transform is written $A(z)$. See [7] for properties of the Fourier transform. Two crucial properties are listed below for future reference.

1) The Fourier transform of $\mathbf{a} * \mathbf{b}$ is the circular convolution $A(z)B(z) \mod z^n + 1$.
2) If $a(\gamma^{-j}) = 0$, then $A_{-j} = 0$ i.e. the coefficient of z^j is zero in the Fourier transform $A(z)$.

We will now interpret the construction of (1) and its various requirements in the Fourier domain. As noted above, the Fourier transforms of the polynomials $h_{11}(x)$, $h_{22}(x)$ and $h_{12}(x)$ will be denoted $H_{11}(z)$, $H_{22}(z)$ and $H_{12}(z)$, respectively.

A. Dimension and Distance

Since the dimension of C_{ii} $(i = 1, 2)$ is equal to k, $h_{ii}(x)$ has exactly k zeros in the set $\{1, \gamma, \gamma^2, \cdots, \gamma^{n-1}\}$. Hence, by property 2 of Fourier transforms, $H_{ii}(z)$ has exactly $n-k$ nonzero terms i.e. $H_{ii}(z)$ is of the form

$$H_{ii}(z) = \sum_{l=1}^{n-k} H_{ii,l} z^{e_{ii,l}}. \tag{8}$$

We will refer to $\{H_{ii,l} : 1 \le l \le n-k\}$ and $E_{ii} = \{e_{ii,l} : 1 \le l \le n-k\}$ as the nonzero coefficients and nonzero powers of $H_{ii}(z)$, respectively. Note that the powers of γ that are nonzeros of $h_{ii}(x)$ are given as $-E_{ii} \mod n$.

We now consider the minimum distance requirements on C_{ii}. From Section II-B, we require C_{ii} to be MDS over GF(2^m). From the theory of cyclic codes [7], we know that C_{ii} is MDS whenever the nonzero powers of $H_{ii}(z)$ are in an arithmetic progression (AP) (modulo n) with common difference relatively prime to n.

To summarize, if $H_{ii}(z)$ is of the form of (8) with the powers $\{e_{ii,l} : 1 \le l \le n-k\}$ in an AP modulo n with common difference relatively prime to n, the dimension and distance requirements are satisfied.

B. Quasicyclic condition

We will now characterize E_{12}, the nonzero powers of $H_{12}(z)$. Note that E_{12} is determined by the possible nonzeros of $h_{12}(x)$.

Suppose $h_{11}(x)$ and $h_{22}(x)$ have been fixed. From (2), we see that all powers of γ that are nonzeros of $h_{11}(x)$ can also be nonzeros of $h_{12}(x)$. Similarly, all nonzeros of $h_{22}(x)$ can also be nonzeros of $h_{12}(x)$. Therefore, the powers of γ that are possible nonzeros of $h_{12}(x)$ are $-E_{11} \cup -E_{22} \mod n$. So, the nonzero powers of $H_{12}(z)$ form the set $E_{12} = E_{11} \cup E_{22}$. We will denote the elements of E_{12} as $E_{12} = \{e_{12,1}, e_{12,2}, \cdots, e_{12,L}\}$, where $L = |E_{11} \cup E_{22}|$.

Thus, $H_{12}(z)$ has the form

$$H_{12}(z) = \sum_{l=1}^{|E_{11} \cup E_{22}|} H_{12,l} z^{e_{12,l}}. \tag{9}$$

C. Repair

Using the properties, we take the Fourier transform of (7) to obtain

$$[A_1(z)B_2(z) + B_1(z)A_2(z)]_n = \delta \sum_{i=0}^{n-1} \gamma^i z^i, \tag{10}$$

where $[(\cdot)]_n$ stands for mod z^7+1 and $\delta \in$ GF(2^m) is nonzero.

Since $[\mathbf{a}_1|\mathbf{a}_2]$ and $[\mathbf{b}_1|\mathbf{b}_2]$ are in $C^\perp$ and obey the structure $[\mathbf{u}H_{11} + \mathbf{v}H_{12}|\mathbf{v}H_{22}]$, there are some constraints between the coefficients of the polynomials $A_1(z)$, $A_2(z)$, $B_1(z)$ and $B_2(z)$. Suppose

$$[\mathbf{a}_1|\mathbf{a}_2] = [\mathbf{u}_a H_{11} + \mathbf{v}_a H_{12}|\mathbf{v}_a H_{22}], \tag{11}$$

$$[\mathbf{b}_1|\mathbf{b}_2] = [\mathbf{u}_b H_{11} + \mathbf{v}_b H_{12}|\mathbf{v}_b H_{22}], \tag{12}$$

where $\mathbf{u}_a$, $\mathbf{u}_b$, $\mathbf{v}_a$ and $\mathbf{v}_b$ are arbitrary length-$(n-k)$ vectors over GF(2^m). Taking Fourier transforms of the above equations, we get

$$A_1(z) = \sum_{l=0}^{n-k-1} u_{a,l} H_{11}(\gamma^{-l} z) + \sum_{l=0}^{n-k-1} v_{a,l} H_{12}(\gamma^{-l} z), \tag{13}$$

$$A_2(z) = \sum_{l=0}^{n-k-1} v_{a,l} H_{22}(\gamma^{-l} z), \tag{14}$$

$$B_1(z) = \sum_{l=0}^{n-k-1} u_{b,l} H_{11}(\gamma^{-l} z) + \sum_{l=0}^{n-k-1} v_{b,l} H_{12}(\gamma^{-l} z), \tag{15}$$

$$B_2(z) = \sum_{l=0}^{n-k-1} v_{b,l} H_{22}(\gamma^{-l} z), \tag{16}$$

where the coordinates of $\mathbf{u}_a$, $\mathbf{u}_b$, $\mathbf{v}_a$ and $\mathbf{v}_b$ have been indexed from 0 to $n-k-1$ using a natural notation. Since $\mathbf{u}_a$ and $\mathbf{u}_b$ are arbitrary, the first summation terms in (13) and (15) simply provide the Fourier transform of an arbitrary codeword of C_{11}. Therefore, they can be replaced by $\sum_{l=1}^{n-k} w_{i,l} z^{e_{ii,l}}$ for arbitrary $w_{i,l}$, $i = 1, 2$, $l = 1, 2, \cdots, n-k$. Simplifying the second summation term of (13) and (15) using (9), we have the following forms for $A_1(z)$ and $B_1(z)$:

$$A_1(z) = \sum_{l=1}^{n-k} w_{1,l} z^{e_{11,l}} + \sum_{l=1}^{|E_{12}|} v_a(\gamma^{-e_{12,l}}) H_{12,l} z^{e_{12,l}}, \tag{17}$$

$$B_1(z) = \sum_{l=1}^{n-k} w_{2,l} z^{e_{22,l}} + \sum_{l=1}^{|E_{12}|} v_b(\gamma^{-e_{12,l}}) H_{12,l} z^{e_{12,l}}, \tag{18}$$

where $v_a(x) = \sum_{l=0}^{n-k-1} v_{a,l} x^l$ and $v_b(x) = \sum_{l=0}^{n-k-1} v_{b,l} x^l$.

D. Search for codes

The polynomials $A_1(z)$, $A_2(z)$, $B_1(z)$ and $B_2(z)$ in the form given by (17), (14), (18), (16) are substituted in (10) to obtain the main equation that needs to be satisfied for the construction of a quasicyclic MDS code with efficient exact repair. The unknowns to be solved are E_{11}, E_{22}, $\{w_{i,j}\}$, the coefficients of $H_{11}(z)$, $H_{12}(z)$ and $H_{22}(z)$, and the vectors $\mathbf{v}_a$ and $\mathbf{v}_b$.

To facilitate computational search, we first fix n, k and m, and then choose at random the AP E_{11}, the AP E_{22}, the coefficients of $H_{22}(z)$, the vector $\mathbf{v}_a$ and the vector $\mathbf{v}_b$. With these choices made, the condition (10) provides linear equations in the remaining unknowns, namely $\{w_{i,j}\}$ and the coefficients of $H_{12}(z)$. The existence of solutions to this set of linear equations can be readily checked. If a solution exists, we are done. Else, the process is repeated with another set of random choices.

Whenever the above computational search succeeds, we have a quasicyclic MDS code with efficient exact repair.

E. Choice of n, k and an example

According to bounds reported in [4], MSR codes for exact repair are not possible if $d = n-1 < 2k-3$. Since we suppose that $\alpha = n - k$, we require $k > \alpha + 2$ or $n > 2\alpha + 2$.

For $\alpha = 2$, the only interesting odd-n case is $n = 5$ and $k = 3$. We show one construction for $n = 5$ over GF(4) (i.e. $m = 2$). Let $\kappa \in$GF(16) be a primitive element. Then, $\gamma = \kappa^3$ is a primitive 5-th root of unity, and $\omega = \kappa^5$ is a primitive element of GF(4) i.e. GF$(4) = \{0, 1, \omega, \omega^2\}$.

A computer search yields the following choices for the polynomials and vectors required in the construction:

$$\begin{aligned} H_{11}(z) &= \kappa z^2 + \kappa^4 z^3,\ H_{22}(z) = \kappa^8 z + \kappa^2 z^4, \\ H_{12}(z) &= \kappa^{11} z + \kappa^7 z^2 + \kappa^{13} z^3 + \kappa^{14} z^4, \\ h_{11}(x) &= 1 + \omega x + \omega x^2 + x^3,\ h_{12}(x) = 1 + x, \\ h_{22}(x) &= 1 + \omega^2 x + \omega^2 x^2 + x^3, \end{aligned}$$

$$\begin{bmatrix} \mathbf{a}_1 | \mathbf{a}_2 \\ \mathbf{b}_1 | \mathbf{b}_2 \end{bmatrix} = \left[\begin{array}{ccccc|ccccc} \omega^2 & \omega^2 & 1 & 0 & 1 & 1 & \omega^2 & \omega^2 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & \omega^2 & \omega^2 & 1 \end{array}\right].$$

We notice that $\beta_i = 1$ for $1 \le i \le 4$ and rank$(M_5) = 2$ for the above reconstruction vectors, and the code is MSR.

Beyond the MSR condition, construction of efficient exact repair codes is interesting whenever n and k are such that $k/n > 1/2$ [2]. Following the same computer search procedure, we are able to construct efficient exact repair codes for $n = 7$, $k = 4$ with $d = 6$ over GF(8). However, since $\alpha = 2 < n - k = 3$, this code is not MSR. We see that 6 symbols are needed for repair, while the message is of length 8 symbols. For $n = 7$, $k = 4$, $d = 6$ MSR codes with $\alpha = 3$ have been reported in the literature [4]. For these $(7, 4)$ MSR codes 6 symbols are needed for repair, when the message is of length 12 symbols.

IV. Construction for $\alpha = 3$

In this section, we will describe extensions of our quasicyclic approach for $\alpha = 3$. While we have not yet been able to construct MSR codes with $\alpha = 3$, we report some close-to-MSR codes in terms of symbols needed for repair.

For $\alpha = 3$, one possible extension to the construction of (1) is as follows.

$$C = \{[\mathbf{c}_1|\mathbf{c}_2|\mathbf{c}_3] : \begin{bmatrix} H_{11} \\ \mathbf{0} \\ H_{13} \end{bmatrix} \mathbf{c}_1^T + \begin{bmatrix} \mathbf{0} \\ H_{22} \\ H_{23} \end{bmatrix} \mathbf{c}_2^T + \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \\ H_{33} \end{bmatrix} \mathbf{c}_3^T = 0\}, \tag{19}$$

where the matrices H_{ij} (applicable i and j) are $n-k \times n$ with entries from GF(2^m) and $\mathbf{0}$ is the $n - k \times n$ all-zero matrix.

A. Distance, quasicyclic nature and repair

We will let H_{ii} $(i = 1, 2, 3)$ be parity check matrices of (n, k) cyclic MDS codes C_{ii}. The check polynomials and their Fourier transforms are denoted $h_{ii}(x)$ and $H_{ii}(z)$, respectively. The nonzero powers of $H_{ii}(z)$ will need to be in an AP modulo n with common difference coprime to n. The rows of the matrices H_{ij} will be cyclic shifts of the first row, as before. With the same proof as before, we can show that the code in (19) is quasicyclic, whenever the set of nonzero powers of $H_{23}(z)$ is the union of the nonzero powers of $H_{22}(z)$ and $H_{33}(z)$, and the set of nonzero powers of $H_{13}(z)$ is the union of the nonzero powers of $H_{11}(z)$ and $H_{33}(z)$.

Dual vectors for $\alpha = 3$ have the form $[\mathbf{u}_1 H_{11} + \mathbf{u}_3 H_{13} | \mathbf{u}_2 H_{22} + \mathbf{u}_3 H_{23} | \mathbf{u}_3 H_{33}]$. When node n fails and can connect to nodes 1 to $n-1$, three dual vectors $[\mathbf{p}_1|\mathbf{p}_2|\mathbf{p}_3]$, $[\mathbf{q}_1|\mathbf{q}_2|\mathbf{q}_3]$ and $[\mathbf{r}_1|\mathbf{r}_2|\mathbf{r}_3]$ are needed for solving for the three unknowns. The equation can be written as

$$M_1 \begin{bmatrix} c_{1,1} \\ c_{1,2} \\ c_{1,3} \end{bmatrix} + M_2 \begin{bmatrix} c_{2,1} \\ c_{2,2} \\ c_{2,3} \end{bmatrix} + \cdots + M_{n-1} \begin{bmatrix} c_{n-1,1} \\ c_{n-1,2} \\ c_{n-1,3} \end{bmatrix} = M_n \begin{bmatrix} c_{n,1} \\ c_{n,2} \\ c_{n,3} \end{bmatrix}, \tag{20}$$

$$M_i = \begin{bmatrix} p_{i,1} & p_{i,2} & p_{i,3} \\ q_{i,1} & q_{i,2} & q_{i,3} \\ r_{i,1} & r_{i,2} & r_{i,3} \end{bmatrix},\ 1 \le i \le n-1. \tag{21}$$

We will need rank$(M_n) = 3$, and we have that the number of symbols to be downloaded from node i is $\beta_i =$ rank(M_i).

B. Fourier domain search

The linear dependency condition for efficient repair given by (10) in the Fourier domain is now applied repeatedly for the components of the three dual vectors needed in the reconstruction. One set of possibilities is the following:

$$[P_1(z)R_2(z) + P_2(z)R_1(z)]_n = \delta_1 \sum_{i=0}^{n-1} \gamma^i z^i, \tag{22}$$

$$[P_1(z)R_3(z) + P_3(z)R_1(z)]_n = \delta_2 \sum_{i=0}^{n-1} \gamma^i z^i, \tag{23}$$

$$[Q_1(z)R_2(z) + Q_2(z)R_1(z)]_n = \delta_3 \sum_{i=0}^{n-1} \gamma^i z^i, \qquad (24)$$

$$[Q_1(z)R_3(z) + Q_3(z)R_1(z)]_n = \delta_4 \sum_{i=0}^{n-1} \gamma^i z^i, \qquad (25)$$

where $\delta_i \neq 0$, $i = 1, 2, 3, 4$. Using simplifications similar to the case when $\alpha = 2$, we fix the nonzeros powers of $H_{ii}(z)$ ($i = 1, 2, 3$), the nonzero coefficients of $H_{33}(z)$ and $R_i(z)$ ($i = 1, 2, 3$). This results in linear equations for the coefficients of $P_i(z)$, $Q_i(z)$ ($i = 1, 2, 3$) and the coefficients of $H_{13}(z)$ and $H_{23}(z)$. However, because of the non-exhaustive nature of the conditions (22), (23), (24) and (25), simply finding a solution is not sufficient. We have to further check that the solution satisfies the condition that the rank of M_n is three. Also, we need to compute the values of $\beta_i = \text{rank}(M_i)$, $i = 1, 2, \cdots, n-1$ to check the efficiency of the repair process.

C. Results

For $\alpha = 3$, we attempted computer search for $n = 7$ and $k = 4$ over GF(8). We can report that there are several codes with suitable reconstruction dual vectors that result in exactly two of the β_i ($i = 1, 2, 3, 4, 5, 6$) equal to 2 and the rest being 1. This implies that a new node will need to download one symbol each from 4 nodes and 2 symbols each from the remaining 2 nodes to exactly compute the symbols in the failed node. Therefore, 8 symbols are needed for a code with 12 message symbols. As discussed before [4], the best MSR code for these parameters can perform exact repair by downloading only 6 symbols. One such (7,4) code is the following: $H_{11}(z) = \gamma^6 z^4 + \gamma^3 z^5 + \gamma^2 z^6$, $H_{22}(z) = \gamma + \gamma^3 z + z^2$, $H_{33}(z) = \gamma z + \gamma^4 z^3 + z^5$, $H_{13}(z) = \gamma^6 z + \gamma z^3 + \gamma^5 z^4 + z^5 + \gamma^3 z^6$, $H_{23}(z) = \gamma^4 + \gamma^2 z + \gamma^2 z^2 + \gamma z^3 + \gamma^3 z^5$. The reconstruction dual vectors, listed one below the other, are

$$\left[\begin{array}{ccccccc|ccccccc|ccccccc} 1 & \gamma^4 & 0 & 0 & \gamma^3 & \gamma & \gamma^4 & 0 & 0 & 0 & 0 & \gamma^4 & \gamma^4 & \gamma & \gamma^2 & \gamma^5 & 0 & 0 & \gamma^3 & \gamma & \gamma \\ 1 & \gamma^3 & \gamma^4 & 1 & \gamma^6 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \gamma & \gamma^2 & \gamma^4 & 0 & \gamma^2 & \gamma^6 & 0 & \gamma^3 \\ \gamma^2 & \gamma^6 & 0 & \gamma^3 & \gamma^4 & 1 & \gamma^6 & 0 & 0 & 0 & \gamma^4 & \gamma^5 & \gamma^3 & \gamma^4 & \gamma^4 & 1 & \gamma^2 & 1 & \gamma^4 & 1 & \gamma^6 \end{array}\right],$$

with $\gamma \in \text{GF}(8)$ being a primitive element.

V. Concluding Remarks

We presented quasicyclic MDS codes with efficient exact repair properties for 2 and 3 symbols per node. We have used a parity check matrix method for construction with a suitable structure to ensure that the code is quasicyclic. Dual vectors are used in the reconstruction process with a Fourier domain search that simplifies the problem considerably.

Several aspects of the construction and search method are new in the area of codes for distributed storage with efficient exact repair. Also, the codes reported here have the advantage of simplicity both in terms of cyclic reconstruction and small field sizes.

While the construction appears to be fairly complete for two symbols per node, there are several interesting possibilities that have been unexplored in the three symbols per node case. However, for the two symbols per node case, the search for a $(7, 4)$ code with $d = 5$ remains an interesting problem.

References

[1] A. Dimakis, P. Godfrey, Y. Wu, M. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *Information Theory, IEEE Transactions on*, vol. 56, no. 9, pp. 4539 –4551, sept. 2010.

[2] A. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476 –489, march 2011.

[3] K. V. Rashmi, N. B. Shah, and P. Vijay Kumar, "Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction," *ArXiv e-prints 1005.4178*, May 2010, to appear in IEEE Transactions on Information Theory.

[4] N. B. Shah, K. V. Rashmi, P. Vijay Kumar, and K. Ramchandran, "Interference Alignment in Regenerating Codes for Distributed Storage: Necessity and Code Constructions," *ArXiv e-prints 1005.1634*, May 2010.

[5] B. Gastón, J. Pujol, and M. Villanueva, "Quasi-cyclic minimum storage regenerating codes for distributed data compression," in *Data Compression Conference (DCC), 2011*, march 2011, pp. 33 –42.

[6] F. Oggier and A. Datta, "Self-Repairing Codes for Distributed Storage - A Projective Geometric Construction," *ArXiv e-prints*, May 2011.

[7] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. Amsterdam, The Netherlands: North-Holland, 1977.

Appendix

Suppose $\mathbf{c} = [\mathbf{c}_1|\mathbf{c}_2] \in C$. Then, $H_{11}\mathbf{c}_1^T = 0$ and $H_{12}\mathbf{c}_1^T = H_{22}\mathbf{c}_2^T = [s_1\ s_2 \cdots s_{n-k_2}]^T$. Let a cyclic right shift of $\mathbf{c}$ be denoted $[\mathbf{c}_1'|\mathbf{c}_2']$, where $\mathbf{c}_1' = [c_{n,1}\ c_{1,1}\ c_{2,1} \cdots c_{n-1,1}]$ and $\mathbf{c}_2' = [c_{n,2}\ c_{1,2}\ c_{2,2} \cdots c_{n-1,2}]$.

Since H_{11} is a parity check matrix for a cyclic code, we have $H_{11}\mathbf{c}_1'^T = 0$. Since $\mathbf{c}_i'$ is a cyclic right shift of $\mathbf{c}_i$, we see that $H_{12}\mathbf{c}_1'^T = [s'\ s_1\ s_2 \cdots s_{n-k_2-1}]$ and $H_{22}\mathbf{c}_2'^T = [s\ s_1\ s_2 \cdots s_{n-k_2-1}]$, since rows of H_{ij} are cyclic right shifts of the first row. So, for C to be quasicyclic, we only need $s' = s$ or

$$[h_{12,1} \cdots h_{12,n-1}\ h_{12,0}][c_{1,1}\ c_{2,1} \cdots c_{n,1}]^T + [h_{22,1} \cdots h_{22,n-1}\ h_{22,0}][c_{1,2}\ c_{2,2} \cdots c_{n,2}]^T = 0,$$

for all $\mathbf{c} = [\mathbf{c}_1|\mathbf{c}_2] \in C$. Hence, we need $[\mathbf{h}_1|\mathbf{h}_2] = [h_{12,1} \cdots h_{12,n-1}\ h_{12,0}|h_{22,1} \cdots h_{22,n-1}\ h_{22,0}]$ to belong to the dual $C^\perp$ i.e. there should be $\mathbf{u}, \mathbf{v}$ such that $[\mathbf{h}_1|\mathbf{h}_2] = [\mathbf{u}H_{11} + \mathbf{v}H_{12}|\mathbf{v}H_{22}]$. In polynomial notation, we need $u(x)$ and $v(x)$ with degree $< n - k$ such that

$$x^{-1}h_{12}(x) = u(x)h_{11}(x) + v(x)h_{12}(x) \mod x^n + 1, \qquad (26)$$

$$x^{-1}h_{22}(x) = v(x)h_{22}(x) \mod x^n + 1. \qquad (27)$$

Since $h_{22}(x)\hat{h}_{22}(x) = x^n + 1$,

$$x^{-1}h_{22}(x) = [(1 + \hat{h}_{22}(x))x^{-1}]h_{22}(x) \mod x^n + 1,$$

where we have used the fact that $\hat{h}_{22,0} = 1$. From the above, we let $v(x) = [(1+\hat{h}_{22}(x))x^{-1}]$, which is a degree-$(n-k-1)$ polynomial that satisfies (27). Using $v(x) = [(1+\hat{h}_{22}(x))x^{-1}]$ in (26), we require $u(x)$ such that

$$h_{12}(x)\hat{h}_{22}(x) = u(x)h_{11}(x) \mod x^n + 1,$$

which is possible whenever $h_{12}(x)\hat{h}_{22}(x) = 0 \mod h_{11}(x)$.

Acknowledgment

The authors would like to thank Siddarth Jaggi, Nihar Shah, K. V. Rashmi and P. Vijay Kumar for several helpful discussions.