ISIT'2013 1569711823

Array BP-XOR Codes for Reliable Cloud Storage Systems

Yongge Wang

Dept. SIS, UNC Charlotte, NC 28223, USA
Email: yongge.wang@uncc.edu

***Abstract*—Low Density Parity Check (LDPC) codes such as LT codes have received significant attention from both academics and industry in the past few years. By employing the underlying ideas of efficient Belief Propagation (BP) decoding process in LT codes, this paper introduces array BP-XOR codes and shows the equivalence between the edge-colored graph model and degree-one-and-two encoding symbol based array BP-XOR codes. Using this equivalence result, novel $[n, n-2]$ and $[n, 2]$ MDS array BP-XOR codes are designed in this paper.**

I. Introduction

In order to achieve better fault tolerance with minimal redundancy in data storage systems, there has been active research in XOR based codes. For example, Blaum, Brady, Bruck, and Menon [1] proposed the array code EVENODD for tolerating two disk faults and correcting one disk errors. Blaum, Bruck, and Vardy [2] and Huang [8] have extended the construction of EVENODD code to general codes for tolerating three disk faults. Other XOR based codes include (but are not limited to) $[2k, k, d]$ chain code, Simple Product Code (SPC [5]), Row-Diagonal Parity (RDP [4]), and others.

By employing the underlying ideas of efficient Belief Propagation (BP) decoding process in LT codes [10], we introduce array BP-XOR codes. Edge-colored graph models were introduced by Wang and Desmedt in [15] to model homogeneous faults in networks. We will show the equivalence between the edge-colored graph model and degree-one-and-two encoding symbol based array BP-XOR codes. Using this equivalence result, we are able to design general array BP-XOR codes using graph based results. In the same time, we are able to get new results for edge-colored graph models using results from array BP-XOR codes.

The structure of this paper is as follows. Section II introduces array BP-XOR codes and establishes the equivalence between edge-colored graph models and array BP-XOR codes with degree one and two encoding symbols. Section III presents constructions of array BP-XOR codes from graph based results (e.g., perfect one factorization of complete graphs). Section IV presents several results on flat BP-XOR codes. In Section V, we briefly show how to obtain efficient secret sharing schemes from array BP-XOR codes.

II. Array BP-XOR codes

Array codes have been studied extensively for burst error correction in communication systems and in storage systems (see, e.g., [1], [2], [3], [17]). Array codes are linear codes where information and parity data are placed in a two dimensional matrix array. Appropriately designed array codes such as EVENODD [1], RDP [4], and STAR [8] are very useful for high speed storage application systems since they enjoy low-complexity decoding and low update complexity.

As mentioned in [10], LT codes or digital fountain techniques could be a better choice for distributed storage systems. One of the major advantages that contribute to the efficiency of LT codes is the Belief Propagation (BP) decoding process. In this paper, we propose array codes that could be efficiently decoded using the BP-decoding process. We call such kind of codes array BP-XOR codes. Appropriately designed array BP-XOR codes could achieve the MDS property from both communication and storage aspects: for k blocks of the original data, only k blocks of encoding symbols are needed for correct decoding. Note that in LT codes, in order to decode k blocks of data with probability $1-\delta$, $k + O(\sqrt{k}\ln^2(k/\delta))$ blocks of encoding symbols are needed.

Throughout the paper, we will use the message alphabet set $M = \{0, 1\}$. For fixed numbers n, k, t, and b where $n \geq \max\{k, t\}$, let $v_1, \cdots, v_{bk}$ be variables taking values from M, which are called information symbols. A t-erasure tolerating $[n, k]$ array code is a $b \times n$ matrix $\mathbf{C} = [\alpha_{i,j}]_{1\leq i\leq b, 1\leq j\leq n}$ such that each encoding symbol $\alpha_{i,j} \in \{0, 1\}$ is the exclusive-or (XOR) of one or more information symbols from $v_1, \cdots, v_{bk}$ and $v_1, \cdots, v_{bk}$ could be recovered from any $n-t$ columns of the matrix. For an encoding symbol $\alpha_{i,j} = v_{i_1} \oplus \cdots \oplus v_{i_\sigma}$, we call v_{i_j} $(1 \leq j \leq \sigma)$ a neighbor of $\alpha_{i,j}$ and call σ the degree of $\alpha_{i,j}$. A t-erasure tolerating $[n, k]$ $b \times n$ array code $\mathbf{C}$ is said to be maximum distance separable (MDS) if $k = n - t$.

The $[n, k]$ array code $\mathbf{C}$ over the alphabet M can be considered as a linear code over the extension alphabet M^b of length n or a linear code over the alphabet M of length bn. A $bt \times bn$ (respectively, $bk \times bn$) binary matrix is said to be a parity-check (respectively, generator) matrix of a $b \times n$ array code $\mathbf{C}$ if it is a parity-check (respectively, generator) matrix of $\mathbf{C}$ when $\mathbf{C}$ is considered as a length bn linear code over the alphabet M. For example, the matrix H (respectively G) is a parity-check (respectively, generator) matrix of the array code $\mathbf{C}$ if we have $H\mathbf{y}^T = 0$ (respectively, $\mathbf{y} = \mathbf{x}G$) where $\mathbf{y} = (\alpha_{1,1}, \cdots, \alpha_{b,1}, \cdots, \alpha_{1,n}, \cdots \alpha_{b,n})$, $\mathbf{x} = (v_1, \cdots, v_{bk})$, and the addition is defined as the XOR on bits. An array code $\mathbf{C}$ is called low density parity-check (LDPC) if its

parity-check (or equivalently, the generator) matrix contains small number of nonzero entries. For an MDS array code, it is straightforward to show that each row of the parity-check (respectively, the generator) matrix must contain at least $n-t+1$ (respectively, $t+1$) nonzero entries (see [3] for a proof).

The Belief Propagation decoding process (also called message passing iterative decoding) for binary symmetric channels (BSC) is present in Gallager [7]. The BP decoding process for binary erasure channels (BEC) is described as follows:

> (Cf. [10], [11]) If there is at least one encoding symbol that has exactly one neighbor then the neighbor can be recovered immediately. The value of the recovered information symbol is XORed into any remaining encoding symbols that have this information symbol as a neighbor. The recovered information symbol is removed as a neighbor of these encoding symbols and the degree of each such encoding symbol is decreased by one to reflect this removal.

A t-erasure tolerating $[n,k]$ array code $\mathbf{C} = [\alpha_{i,j}]_{1\le i\le b, 1\le j\le n}$ is called an $[n,k]$ array BP-XOR code if all information symbols $v_1,\cdots,v_{bk}$ can be recovered from any $n-t$ columns of encoding symbols using the BP-decoding process on the BEC.

If each encoding symbol in $\mathbf{C} = [\alpha_{i,j}]_{1\le i\le b, 1\le j\le n}$ has degree at most 2, then the restricted array BP-XOR codes are equivalent to edge-colored graphs introduced by Wang and Desmedt in [15] for tolerating network homogeneous faults.

A. Edge-colored graphs

In this section, we first describe the edge-colored graph model by Wang and Desmedt [15]. The reader should be reminded that the edge-colored graph model in [15] is slightly different from edge-colored graphs in other literatures. In other literatures, the coloring of the edges is required to meet the condition that no two adjacent edges have the same color. This condition is not required in the definition of [15].

Definition 2.1: (Wang and Desmedt [15]) An edge-colored graph is a tuple $G=(V,E,C,f)$, with V the node set, E the edge set, C the color set, and f a map from E onto C. The structure

$$\mathcal{Z}_{C,t} = \{Z : Z \subseteq E \text{ and } |f(Z)| \le t\}.$$

is called a *t-color* adversary structure. Let $A, B \in V$ be distinct nodes of G. A and B are called *$(t+1)$-color connected* for $t \ge 1$ if for any color set $C_t \subseteq C$ of size t, there is a path p from A to B in G such that the edges on p do not contain any color in C_t. An edge-colored graph G is *$(t+1)$-color connected* if and only if for any two nodes A and B in G, they are $(t+1)$-color connected.

As an example, Figure 1 shows a 3-color connected graph $G_{4,2}$ with 7 nodes, 12 edges, and 4 colors. In other words, the removal of any two colors in the graph will not disconnect the graph. The edge-colored graphs $G_{4,2}$ can also be represented

Fig. 1. 3-color connected edge-colored graph $G_{4,2}$

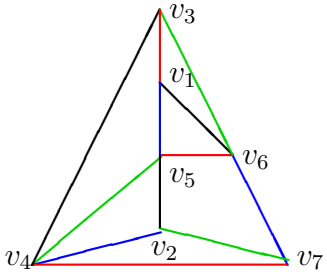

TABLE I
TABLE REPRESENTATION OF EDGE-COLORED GRAPH $G_{4,2}$

$\langle v_1, v_6\rangle$	$\langle v_2, v_7\rangle$	$\langle v_3, v_1\rangle$	$\langle v_4, v_2\rangle$
$\langle v_2, v_5\rangle$	$\langle v_3, v_6\rangle$	$\langle v_4, v_7\rangle$	$\langle v_5, v_1\rangle$
$\langle v_3, v_4\rangle$	$\langle v_4, v_5\rangle$	$\langle v_5, v_6\rangle$	$\langle v_6, v_7\rangle$

by the Table I where the edges with the same color are put in the same column.

Though Wang and Desmedt [15] presented a few simple constructions of edge-colored graphs with certain color connectivity, their results are not sufficient for our study of general array BP-XOR code design. In the following, we present a general construction of $(t+1)$-color connected edge-colored graphs using perfect one-factorizations of complete graphs. We use $K_n = (V,E)$ to denote the complete graph with n nodes. For an even n, a one-factor of K_n is a spanning 1-regular subgraph (or a perfect matching) of K_n. A one-factorization of K_n (n is even) is a set of one-factors that partition the set of edges E. A one-factorization is called perfect (or P1F) if the union of every two distinct one-factors is a Hamiltonian circuit. It is known (see, e.g., [12]) that perfect one-factorizations for K_{p+1}, K_{2p}, and certain K_{2n} do exist, where p is a prime number. It is conjectured that P1F exist for all K_{2n}.

Example 2.2:

- **P1F for K_{p+1}:** For an integer a, let $\langle a\rangle_p$ denote the integer $b \in \{0,\cdots,p-1\}$ such that $b \equiv a \bmod p$. Let $V=\{v_0,v_1,\cdots,v_p\}$ and

  $$F_i = \{\langle v_i, v_p\rangle\} \cup \{\langle v_{\langle j_1+i\rangle_p}, v_{\langle j_2+i\rangle_p}\rangle : \langle j_1+j_2\rangle_p = 0 \text{ and } 0 \le j_1 \ne j_2 < p\}$$

  for $i=0,\cdots,p-1$. Then $F_0,F_1,\cdots,F_{p-1}$ is a perfect one factorization of K_{p+1}.
- **P1F for K_{2p}:** Let $V=\{v_0,\cdots,v_{2p-1}\}$. For even i, let

  $$F_i = \{\langle v_{j_1}, v_{j_2}\rangle : j_1+j_2 = i \bmod 2p\} \cup \{\langle v_{\frac{i}{2}}, v_{\frac{i}{2}+p}\rangle\},$$

  and for odd $i \ne p$, let

  $$F_i = \{\langle v_{j_1}, v_{j_2}\rangle : j_1 \text{ is odd}, j_1 - j_2 = i \bmod 2p\}.$$

  Then $F_0,F_1,\cdots,F_{p-1},F_{p+1},\cdots,F_{2p-2}$ is a perfect one factorization of K_{2p}.

Theorem 2.3: Let n be an odd number such that there is

a perfect one-factorization $F_1, \cdots, F_n$ for K_{n+1}. For each $t \leq n-2$, there exists a $(t+1)$-color connected edge-colored graph G with n nodes, $(t+2)(n-1)/2$ edges, and $t+2$ colors.

Proof. Let $v_1, \ldots, v_{n+1}$ be a list of nodes for K_{n+1} and $V = \{v_1, \cdots, v_n\}$. Let $F_i' = F_i \setminus \{\langle v_{n+1}, v_j\rangle : j = 1, \cdots, n\}$, $E = F_1' \cup \cdots \cup F_{t+2}'$, and color all edges in F_i' with the color c_i for $i \leq t+2$. Then it is straightforward to check that the edge-colored graph (V, E) is $(t+1)$-color connected, $|V| = n$, and $|E| = (t+2)(n-1)/2$. □

Remarks on Theorem 2.3: Since only node connectivity instead of Hamiltonian circuit is required for $(t+1)$-color connected graphs, we could use F_i' instead of F_i to construct edge-colored graphs. By using F_i' instead of F_i, we eliminate $t+2$ edges and one node in the resulting edge-colored graph. This helps us to keep the minimum cost for connectivity.

B. MDS array BP-XOR codes from edge-colored graphs

As an example, we first describe the array BP-XOR code corresponding to graph $G_{4,2}$ in Table I. Each edge in Table I is mapped to the XOR of the two adjacent nodes. Then choose a fixed node (e.g., v_7) and remove all occurrences of this node (e.g., v_7) to get the $[4, 2]$ 3×4 array BP-XOR code in Table II.

TABLE II
BP-XOR CODE CORRESPONDING TO $G_{4,2}$

$v_1 \oplus v_6$	v_2	$v_3 \oplus v_1$	$v_4 \oplus v_2$
$v_2 \oplus v_5$	$v_3 \oplus v_6$	v_4	$v_5 \oplus v_1$
$v_3 \oplus v_4$	$v_4 \oplus v_5$	$v_5 \oplus v_6$	v_6

In the following, we give a general construction of array BP-XOR codes from edge-colored graphs. Let $v_1, v_2, \cdots, v_{bk}, v_{bk+1}$ be variables that take values from $M = \{0, 1\}$. Let $G = (V, E, C, f)$ be a $(t+1)$-color connected edge-colored graph with $V = \{v_1, \cdots, v_{bk}, v_{bk+1}\}$, $|E| = m$, and $C = \{c_1, c_2, \cdots, c_n\}$. If we consider the nodes in $G = (V, E, C, f)$ as data block variables, edges as their parity check blocks of the adjacent nodes, and colors on the edges as labels for placing the parity checks into different columns of the array codes, then the following steps construct a $b \times n$ array BP-XOR codes, where $b = \max_{c \in C}\{|Z| : Z \subseteq E, f(Z) = c\}$.

1) For $1 \leq i \leq n$, let β_i be defined as
$$\begin{aligned}\beta_i = \quad & \{v_{j_1} \oplus v_{j_2} : \langle v_{j_1}, v_{j_2}\rangle \in E, f(\langle v_{j_1}, v_{j_2}\rangle) = c_i, \\ & \text{and } j_1, j_2 \neq bk+1\} \cup \\ & \{v_j : \langle v_j, v_{bk+1}\rangle \in E, f(\langle v_j, v_{bk+1}\rangle) = c_i\}\end{aligned}$$
2) If $|\beta_i|$ is smaller than b, duplicate elements in β_i to make it a b-element set.
3) The array BP-XOR code is specified by the $b \times n$ matrix $\mathbf{C}_G = (\beta_1^T, \cdots, \beta_n^T)$.

Next we show that the above array BP-XOR code $\mathbf{C}_G$ can tolerate t-erasure columns. Assume that the missing t columns of the code $\mathbf{C}_G$ correspond to the t-color set $C_t \subset C$ of the graph G. Since the graph G is $(t+1)$-color connected, for any node $v_{i_0} \in V$, we have a path $p = \langle v_{bk+1}, v_{i_1}, v_{i_2}, \cdots, v_{i_j}, v_{i_0}\rangle$ without using any colors in C_t. Thus v_{i_0} could be recovered by the following equation

$$v_{i_0} = v_{i_1} \oplus (v_{i_1} \oplus v_{i_2}) \oplus \cdots \oplus (v_{i_j} \oplus v_{i_0})$$

where $v_{i_1}, v_{i_1} \oplus v_{i_2}, \cdots, v_{i_j} \oplus v_{i_0}$ are all available in the non-missing columns. In other words, the Belief Propagation decoding process could be used to recover the entire data blocks $v_1, \cdots, v_{bk}$ from the non-missing columns.

Theorem 2.4: Let n be an odd number such that there is a perfect one-factorization $F_1, \cdots, F_n$ for K_{n+1}. Then for $b = \frac{n-1}{2}$, there exists an $(n-2)$-erasure tolerating MDS $b \times n$ array BP-XOR code $\mathbf{C}_{b,n,2}$.

Proof. Follows from Theorem 2.3 and above discussions. □

Corollary 2.5: For a given b, let $n \leq 2b+1$. If $2b+1$ or $b+1$ is a prime number, then there exists an $(n-2)$-erasure tolerating MDS $b \times n$ array BP-XOR code $\mathbf{C}_{b,n,2}$.

C. Edge-colored graphs from array BP-XOR codes

In this section, we show that each array BP-XOR code could be converted to a corresponding edge-colored graph.

Theorem 2.6: Let $\mathbf{C}$ be an $b \times n$ array BP-XOR code with the following properties:

1) $\mathbf{C}$ is t-erasure tolerating;
2) $\mathbf{C}$ contains bk information symbols; and
3) $\mathbf{C}$ contains only degree one and two encoding symbols.

Then there exists a $(t+1)$-color connected edge-colored graph $G = (V, E, C, f)$ with $|V| = bk+1$, $|E| = bn$, and $|C| = n$.

Proof. Let $v_1, \cdots, v_{bk}$ be the information symbols of $\mathbf{C} = [\alpha_{i,j}]_{(i,j) \in [1,b] \times [1,n]}$ and $v_{i_1}, \cdots, v_{i_u}$ be a list of degree one encoding symbols in $\mathbf{C}$. Then the $(t+1)$-color connected edge-colored graph $G = (V, E, C, f)$ is defined by the following steps:

1) $V = \{v_1, \cdots, v_{bk}, v_{bk+1}\}$;
2) $E = \cup_{j \in [1,u]}\{\langle v_{bk+1}, v_{i_j}\rangle\} \cup \{\langle v_i, v_j\rangle : v_i \oplus v_j \in \mathbf{C}\}$;
3) $C = \{c_1, \cdots, c_n\}$;
4) Let $\alpha_{i,j} \in \mathbf{C}$. If $\alpha_{i,j} = v_{i'} \oplus v_{j'}$ then let $f(\langle v_{i'}, v_{j'}\rangle) = c_j$. Otherwise if $\alpha_{i,j} = v_{i'}$, let $f(\langle v_{bk+1}, v_{i'}\rangle) = c_j$.

Let C_t be a color set of size t and v_i and v_j be two nodes. Since the code $\mathbf{C}$ is t-erasure tolerating, both v_i and v_j could be recovered from encoding symbols not contained in the columns corresponding to the colors in C_t. Thus there exists a path p (respectively, q) connecting v_{bk+1} to v_i (respectively, to v_j) without using C_t-colored edges. It follows that $G = (V, E, C, f)$ is $(t+1)$-color connected. □

III. EXAMPLES OF MDS $[n, 2]$ ARRAY BP-XOR CODES

In this section, we use edge-colored graphs costructed in Theorem 2.3 to design array BP-XOR codes. In order to design $(n-2)$-erasure tolerating MDS $[n, 2]$ $b \times n$ array BP-XOR codes, we first design $(n-2+1)$-color connected edge-colored graphs with n colors. The edge-colored graphs are then converted to array BP-XOR codes using the process described in Section II-B. Specifically, we first find the smallest p (or $2p$) such that $n \leq p$ (or $n \leq 2p-1$), where p is an odd prime. By Example 2.2 for K_{p+1}, we get the perfect one-factorization of

K_{p+1} with node set $V = \{v_0, \cdots, v_p\}$ and the ith factor F_i as

$$\left\{\langle v_i, v_p\rangle; \langle v_{\langle 1+i\rangle_p}, v_{\langle p-1+i\rangle_p}\rangle; \cdots; \langle v_{\langle \frac{p-1}{2}+i\rangle_p}, v_{\langle \frac{p+1}{2}+i\rangle_p}\rangle\right\}$$

for $0 \le i \le p-1$. First we remove the edge $\langle v_i, v_p\rangle$ from F_i and the remaining edges in F_i are mapped to the XOR of the adjacent node variables. Then remove all occurrences of v_0 and we get the MDS $[n, 2]$ $b \times p$ array BP-XOR code in Table III where $b = (p-1)/2$. It should be noted that the dual code

TABLE III
$(p-1)/2 \times p$ BP-XOR CODE

$v_1 \oplus v_{p-1}$	$\cdots$	$v_{p-1} \oplus v_{p-3}$	v_{p-2}
$v_2 \oplus v_{p-2}$	$\cdots$	v_{p-4}	$v_1 \oplus v_{p-3}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$v_b \oplus v_{b+1}$	$\cdots$	$v_{b-2} \oplus v_{b-1}$	$v_{b-1} \oplus v_b$

of the MDS $[n, 2]$ array BP-XOR code in Table III is an MDS $[n, n-2]$ array BP-XOR code. It should also be noted that the $(p-1)/2 \times p$ array BP-XOR code in Table III is equivalent to the code designed by Zaitsev, Zinov'ev, and Semakov [6] which was reformulated later as the dual of B-code in [17] using perfect one-factorization of complete graphs.

IV. FLAT NON-MDS BP-XOR CODES

A $b \times n$ array BP-XOR code is called a flat BP-XOR code if $b = 1$. Furthermore, a $1 \times n$ BP-XOR code with k information symbols and distance d is called an $[n, k, d]$ BP-XOR code. In this section, we present several results on flat BP-XOR codes. We first present a fact based on a folklore regarding flat XOR codes.

Fact 4.1: Let $n \ge k+2$, $k \ge 2$, and $d = n-k+1$. Then there is no flat $[n, k, d]$ BP-XOR code.

Fact 4.1 could be proved by the following observation: Let $H = [\beta_1^T, \cdots, \beta_k^T | I_{n-k}]$ be an $(n-k) \times n$ parity check matrix. If every $n-k$ columns in the matrix $[\beta_i^T | I_{n-k}]$ are linearly independent, then $wt(\beta_i) = n-k$, where $wt(\cdot)$ is the Hamming weight. Thus for $n \ge k+2$, there is neither binary linear $[n, k, d]$ code nor flat $[n, k, d]$ BP-XOR code.

For an MDS $[n, k, d]$ code with $d = n-k+1$, we can tolerate $d-1$ erasure faults. The question that we are interested in is: for given $n \ge k+2$, what is the best distance d that we could achieve for a flat $[n, k, d]$ BP-XOR code? Fact 4.1 shows that d must be strictly less than $n-k+1$.

Tolerating one erasure fault: Let $\alpha \in \{1\}^k$. Then the generator matrix $\left[I_k | \alpha^T\right]$ corresponds to an MDS flat $[k+1, k, 2]$ BP-XOR code that could tolerate one erasure fault.

Tolerating two erasure faults: Fact 4.1 shows that two parity check symbols are not sufficient for tolerating two erasure faults for flat BP-XOR codes. In order to tolerate two erasure, we have to consider codes with $n \ge k+3$.

Theorem 4.2: For $n \ge k+3$ and $k \ge 3$, there exists a flat $[n, k, 3]$ BP-XOR code if and only if $k \le 2^{n-k} - (n-k) - 1$.

Proof. The truncated version (or non-truncated version if $k = 2^{n-k} - (n-k) - 1$) of the Hamming code could be used to prove the theorem. □

Tolerating three erasure faults: For this case, we have the following results.

Theorem 4.3: For $n \ge k+4$, there exists a systematic flat XOR $[n, k, 4]$ code if and only if

$$k \le \begin{cases} 2^{n-k-1} - n + k & \text{if } n-k \text{ is even} \\ 2^{n-k-1} - n + k - 1 & \text{if } n-k \text{ is odd} \end{cases}$$

Proof. Let

$$X = \{\beta : \beta \in \{0,1\}^{n-k}, wt(\beta) = 3, 5, 7, \cdots\}.$$

Then

$$\begin{aligned} |X| &= \sum_{i \ge 3, i \text{ is odd}} \binom{n-k}{i} \\ &= \sum_{i \ge 3, i \text{ is odd}} \left(\binom{n-k-1}{i-1} + \binom{n-k-1}{i}\right) \\ &= \begin{cases} 2^{n-k-1} - n + k & \text{if } n-k \text{ is even} \\ 2^{n-k-1} - n + k - 1 & \text{if } n-k \text{ is odd} \end{cases} \end{aligned}$$

Define an $(n-k) \times k$ matrix $A = (\beta_1^T, \cdots, \beta_k^T)$ where β_i are distinct elements from X. It is straightforward to show that every three columns in the parity check matrix $[A | I_{n-k}]$ are linearly independent. Thus the binary linear code corresponding to the parity check matrix $[A | I_{n-k}]$ (or the generator matrix $[I_k | A^T]$) is a flat XOR $[n, k, 4]$ code.

The other direction is proved by the fact that each vector $\beta \in \{0,1\}^{n-k}$ with even Hamming weight equals to $\beta_1 + \beta_2$ for some $\beta_1, \beta_2 \in X$. This completes the proof of the theorem. □

Theorem 4.3 establishes a necessary and sufficient condition for designing systematic flat XOR codes tolerating three erasure faults. However, the codes constructed in Theorem 4.3 are not necessarily flat BP-XOR codes. For example, let $n = 7, k = 3$, $d = 4$, and $\beta_1 = (1,1,1,0)$, $\beta_2 = (0,1,1,1)$, and $\beta_3 = (1,0,1,1)$. Then the corresponding code has the following generator matrix:

$$\left[\begin{array}{c|cccc} & 1 & 1 & 1 & 0 \\ I_3 & 0 & 1 & 1 & 1 \\ & 1 & 0 & 1 & 1 \end{array}\right]$$

If we remove the first three columns from the above generator matrix, then no column in the remaining generator matrix has Hamming weight 1. Indeed, for $n = 7, k = 3$, and $d = 4$, there is no flat $[7, 3, 4]$ BP-XOR code. The reason is that in order for a $[7, 3, 4]$ linear code to be a flat BP-XOR code, we need four columns with Hamming weight 1 in the generator matrix. Furthermore, we need to have Hamming weight 4 for each row. Without loss of generality, we may assume that the column $(1,0,0)^T$ occurs twice in the generator matrix. Then we have three columns in the generator matrix with the format $(b,1,1)^T$ where $b = 0, 1$. Thus there exist two columns in the generator matrix, each of which occurs twice. In other words,

the code distance is at most 3.

Tolerating four or more erasure faults: In the following, we present some sufficient (but not necessary) conditions for tolerating four erasure faults.

Theorem 4.4: For $n \geq k+5$, there exists a systematic flat XOR $[n,k,5]$ code if k is less than

$$\left\lfloor \frac{n-k-2}{2} \right\rfloor + 2\left\lfloor \left(\left\lceil \frac{n-k}{2} \right\rceil - 2 \right)/2 \right\rfloor + 2\left\lfloor \left(\left\lceil \frac{n-k}{4} \right\rceil - 2 \right)/2 \right\rfloor.$$

Proof. Let $U = \{a_1, \cdots, a_{n-k}\}$. In the following, we construct four-element subsets of U so that the characteristic sequences of these subsets could be used as the columns of the parity check matrix. It helps readers to understand the following definitions if elements of U are interpreted as leaf nodes on a binary tree of depth $\lfloor \log_2(n-k) \rfloor$.

$$V_i^1 = \{a_1, a_2, a_{2i+1}, a_{2i+2}\} \text{ for } 1 \leq i \leq \left\lfloor \tfrac{n-k-2}{2} \right\rfloor,$$
$$V_i^{2,0} = \{a_1, a_3, a_{4i+1}, a_{4i+3}\} \text{ for } 1 \leq i \leq \left\lfloor \left(\left\lceil \tfrac{n-k}{2} \right\rceil - 2 \right)/2 \right\rfloor,$$
$$V_i^{2,1} = \{a_2, a_4, a_{4i+2}, a_{4i+3}\} \text{ for } 1 \leq i \leq \left\lfloor \left(\left\lceil \tfrac{n-k}{2} \right\rceil - 2 \right)/2 \right\rfloor,$$
$$V_i^{3,0} = \{a_1, a_5, a_{8i+1}, a_{8i+5}\} \text{ for } 1 \leq i \leq \left\lfloor \left(\left\lceil \tfrac{n-k}{4} \right\rceil - 2 \right)/2 \right\rfloor,$$
$$V_i^{3,1} = \{a_4, a_8, a_{4i+2}, a_{8i+5}\} \text{ for } 1 \leq i \leq \left\lfloor \left(\left\lceil \tfrac{n-k}{4} \right\rceil - 2 \right)/2 \right\rfloor,$$
$\cdots\cdots$

Let $\beta_1, \cdots, \beta_w$ be the characteristic sequences of the above sets. Then the parity check matrix $H = [\beta_1^T, \cdots, \beta_w^T | I_{n-k}]$ corresponds to a systematic flat XOR code of distance 5. The code has distance 5 since every 4 columns in H are linearly independent by the facts that (1) for any β_1, β_2, we have $wt(\beta_1 + \beta_2) > 2$; and (2) any three or four β are linearly independent. The two facts follow from the construction. This completes the Proof of the Theorem. □

V. Efficient XOR-based secret sharing schemes

In a perfect (n,k) threshold secret sharing scheme, a secret s is encoded into n shares and each participant receives one share. Any $k \leq n$ participants can come together and reconstruct the secret s though no $k-1$ participants could learn any information of the secret. By an ideal threshold scheme, we mean a secret sharing scheme for which the size of the shares is the same as the size of the secret.

It is well known that each MDS code could be converted to a perfect and ideal secret sharing scheme (see, e.g., Karnin, Greene, and Hellman [9]). In this section, we use array BP-XOR codes to design perfect and ideal $(n-1,2)$ threshold BP-XOR secret sharing schemes that only use XOR operations both for secret distribution and reconstruction phases.

By Corollary 2.5, there exist MDS $b \times n$ array BP-XOR codes $\mathbf{C}_{b,n,2} = [\sigma_{i,j}]$ if $2b+1$ or $b+1$ is a prime number and $n \leq 2b+1$. Specifically, the first column of $\mathbf{C}_{b,n,2}$ corresponds to a one-factor of an edge-colored graph. Without loss of generality, we may assume that the first column of $\mathbf{C}_{b,n,2}$ consist of $v_{i_1} \oplus v_{i'_1}$, $v_{i_2} \oplus v_{i'_2}$, $\cdots$, $v_{i_b} \oplus v_{i'_b}$. For a given secret $s = (s_1, \cdots, s_b)$ where $s_i \in \{0,1\}$, the dealer chooses random values for $v_{i'_1}, \cdots, v_{i'_b} \in \{0,1\}$ and lets $v_{i_1} = v_{i'_1} \oplus s_1$, $v_{i_2} = v_{i'_2} \oplus s_2$, $\cdots$, $v_{i_b} = v_{i'_b} \oplus s_b$. The dealer computes the code $\mathbf{C}_{b,n,2}$ using the P1F of the complete graph K_{2b+2} and securely distributes the $(i+1)$th column of $\mathbf{C}_{b,n,2}$ to the ith participant.

By the MDS property of $\mathbf{C}_{b,n,2}$, any two participants could use their shares to reconstruct the secret. By the MDS property of $\mathbf{C}_{b,n,2}$, the above constructed secret sharing scheme is a perfect and ideal 2-out-of-$(n-1)$ threshold secret sharing scheme.

VI. Conclusion

In this paper, we used edge-colored graphs to design degree-one-and-two encoding symbol based array BP-XOR codes. Paterson, Stinson, and Wang [13] showed the limitation of lower degree encoding symbols and obtained several bounds on what one can achieve using degree one and degree two encoding symbols only. In particular, degree one and two encoding symbols could be used to design MDS array BP-XOR codes with $t = 2$ or $k = 2$, and higher degree encoding symbols are needed for general MDS array BP-XOR code design. It is clear that edge-colored graphs could not be used to model higher degree encoding symbols and it is an open question whether one can use edge-colored hyper-graphs to model higher degree encoding symbols and obtain non-trivial results for general array BP-XOR code design.

References

[1] M. Blaum, J. Brady, J. Bruck, and J. Menon. EVENODD: An efficient scheme for tolerating double disk failures in raid architectures. *IEEE Trans. Computers*, 44(2):192–202, 1995.

[2] M. Blaum, J. Bruck, and E. Vardy. MDS array codes with independent parity symbols. *IEEE Trans. on Information Theory*, 42:529–542, 1996.

[3] M. Blaum and R. M. Roth. On lowest-density MDS codes. *IEEE Trans. on Information Theory*, 45:46–59, 1999.

[4] P. Corbett, R. English, A. Goel, T. Grcanac, S. Kleiman, J. Leong, and S. Sankar. Row-diagonal parity for double disk failure correction. In *FAST*, pages 1–14, 2004.

[5] P. Elias. Error–free coding. Technical Report 285, MIT (Boston), 1954.

[6] N. V. Semakov G. V. Zaitsev, V. A. Zinov'ev. Minimum-check-density codes for correcting bytes of errors, erasures, or defects. *Problems Inform. Transmission*, 19(3):197–204, 1983.

[7] R. G. Gallager. *Low density Parity Check Codes*. MIT Press, 1963.

[8] C. Huang and L. Xu. STAR: an efficient coding scheme for correcting triple storage node failures. In *FAST*, pages 197–210, 2005.

[9] E. Karnin, J. Greene, and M. Hellman. On secret sharing systems. *IEEE Trans. Information Theory*, 29(1):35 – 41, jan 1983.

[10] M. Luby. LT codes. In *Proc. FOCS*, pages 271–280, 2002.

[11] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman. Efficient erasure correcting codes. *IEEE Trans. Inf. Theor.*, 47:569–584, 2001.

[12] R. Mendelsohn and A. Rosa. One-factorizations of the complete graph – a survey. *Journal of Graph Teory*, 9(1):43–65, 1985.

[13] M. Paterson, D. Stinson, and Yongge Wang. On encoding symbol degrees of array bp-xor codes. *Submitted for publication*, 2013.

[14] Yongge Wang. Efficient ldpc code based secret sharing schemes and private data storage in cloud without encryption. *Submitted for publication*, 2013.

[15] Yongge Wang and Yvo Desmedt. Edge-colored graphs with applications to homogeneous faults. *Inf. Process. Lett.*, 111(13):634–641, 2011.

[16] Yongge Wang and Yvo Desmedt. Efficient secret sharing schemes achieving optimal information rate. *Submitted for publication*, 2013.

[17] L. Xu, V. Bohossian, J. Bruck, and D. Wagner. Low density mds codes and factors of complete graphs. *IEEE Trans. Inf. Theor.*, 45:1817–1826, 1998.