On Cyclic Lowest Density MDS Array Codes Constructed Using Starters

Mingqiang Li and Jiwu Shu
Tsinghua National Laboratory for Information Science and Technology (TNList)
Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
Email: lmq06@mails.tsinghua.edu.cn, shujw@tsinghua.edu.cn

***Abstract*—In this paper, we present a systematic study on cyclic lowest density MDS array codes constructed using starters. We first show that all cyclic lowest density MDS array codes of distance 3 and length $2n$ can be constructed using normalized cyclic bipyramidal starters in the additive group of congruence classes modulo $2n$. We then discuss when and how to transform non-cyclic lowest density MDS array codes constructed using other starters (including even starters and patterned starters) to cyclic codes. Finally, we also discuss how to construct quasi-cyclic lowest density MDS array codes using multi-starters for an even length when no cyclic lowest density MDS array code exists for this even length.**

I. Introduction

Array codes [1] are a class of linear codes whose information and parity bits are placed in a two-dimensional (or multidimensional) array rather than a one-dimensional vector. A common property of array codes is that they are implemented based on only simple XOR (Exclusive OR) operations. This is an attractive advantage in contrast to the family of Reed-Solomon codes [2], [3], whose encoding and decoding processes use complex finite-field operations. Thus, array codes are ubiquitous in data storage applications.

Among all kinds of array codes, cyclic lowest density MDS (Maximum-Distance Separable) array codes [4] are regarded as the optimal ones for data storage applications because they have all the following properties:

1) they are MDS codes, which attain the Singleton bound [5] and thus has optimal *storage efficiency* (i.e. the ratio of user data to the total of user data plus redundancy data);
2) their *update complexity* (defined as the average number of parity bits affected by a change of a single information bit) achieves the minimum update complexity that MDS codes can have; and
3) their regularity in the form of cyclic symmetry makes their implementation simpler and potentially less costly.

Fault tolerance is an important concern in the design of storage systems [6]. As today's storage systems grow in size and complexity, they are increasingly confronted with disk failures [7] together with latent sector errors [8]. Then, RAID (Redundant Array of Inexpensive Disks) Level 5 [9], which is widely used in modern storage systems to recover one disk failure, cannot provide sufficient reliability guarantee. This results in the demand of RAID Level 6 [9], which can tolerate two disk failures. RAID Level 6 is designed based on a linear code of distance 3, and a cyclic lowest density MDS array code of distance 3 is regarded as the best choice for RAID Level 6.

This work was supported by the National Science Foundation for Distinguished Young Scholars of China (Grant No. 60925006) and the National High Technology Research and Development Program of China (Grant No. 2009AA01A403).

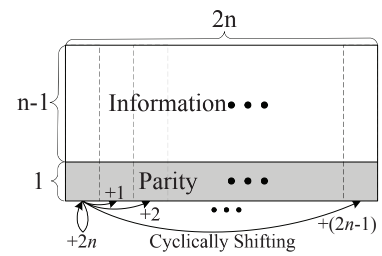

Fig. 1. The structure of a cyclic lowest density MDS array code of distance 3 and length $2n$.

Under this background, we will consider cyclic lowest density MDS array codes of distance 3 in this paper. The structure of a such array code of length $2n$ evolves from that of the B-Code in [10] and is illustrated in Figure 1. This kind of array code has dimensions $n\times 2n$, i.e. n rows and $2n$ columns, where n is an integer not smaller than 2. The first $n-1$ rows are information rows, and the last row is a parity row. In other words, the bits in the first $n-1$ rows are information bits, while those in the last row are parity bits. Because of the optimal update complexity, each information bit contributes to the calculation of (or is protected by) exactly 2 parity bits contained in other columns. Moreover, any two information bits do not contribute to the calculation of the same pair of parity bits. In addition, because of the cyclic symmetry, all the last $2n-1$ columns are constructed by cyclically shifting the first column. It was proved in [11] that this kind of array code achieves the maximum even length for a given column size, which MDS codes with optimal update complexity can have.

Definition 1 ([12]): A *one-factorization* of a graph is a partitioning of the set of its edges into subsets such that each subset is a graph of degree one. Here, each subset is called as a *one-factor*. A *perfect one-factorization* (*P1F*) is a particular one-factorization in which the union of any pair of one-factors is a Hamiltonian cycle.

(*Remark:* A Hamiltonian cycle is a cycle in an undirected graph, which visits each vertex exactly once and also returns to the starting vertex.)

Cyclic lowest density MDS array codes of distance 3 can be described using a graph approach proposed in [10]. It can be easily deduced from the result in [13] that the construction problem of a cyclic lowest density MDS array code of distance 3 can be completely converted into the well-known P1F problem [14] in graph theory. In the literature of graph theory, we noticed that most of known P1Fs are constructed using starters in group theory. Then, a natural question is whether all these starters can be used to construct cyclic lowest density MDS array codes. Unfortunately, it will be shown in this paper that the answer to this question is negative. Then, another question is immediately raised: *Which kinds of starters can be used to construct cyclic lowest density MDS array codes?*

In this paper, we will first show in Subsection III-A that all cyclic lowest density MDS array codes of distance 3 and length $2n$ can be constructed using normalized cyclic bipyramidal starters in the additive group of congruence classes modulo $2n$. Then, we will discuss in Subsection III-B when and how to transform non-cyclic lowest density MDS array codes constructed using other starters (including even starters and patterned starters) to cyclic codes. Besides, we found using an exhaustive search that there is no cyclic lowest density MDS array code for some even lengths, such as 8. Thus, we will also discuss in Section IV how to construct quasi-cyclic lowest density MDS array codes [4] (which partially hold cyclic symmetry) using multi-starters for these even lengths.

We begin this paper with a brief introduction of the graph description of cyclic lowest density MDS array codes of distance 3 in the next section.

II. A Brief Introduction of the Graph Description

In a cyclic lowest density MDS array code of distance 3, each information bit contributes to the calculation of (or is protected by) exactly 2 parity bits contained in other columns. Moreover, any two information bits do not contribute to the same pair of parity bits. Thus, a graph approach [10] can be used to describe a such array code.

In the graph description of a cyclic lowest density MDS array code of distance 3, each parity bit is represented by a vertex, and each information bit that contributes to the calculation of 2 parity bits is represented by the edge that connects the two corresponding vertices. Then, a cyclic lowest density MDS array code of distance 3 and length $2n$ (see Figure 1) can be described by a $(2n-2)$-regular graph G on $2n$ vertices. We label the $2n$ vertices with integers from 0 to $2n-1$ such that the i-th vertex ($i = 0, 1, \cdots, 2n-1$) represents the parity bit contained in the i-th column of the code. Then, for $i = 0, 1, \cdots, 2n-1$, the i-th column of the code can be represented by a set of $n-1$ edges, i.e.

$$C_i = \{\{x_{i,1}, y_{i,1}\}, \{x_{i,2}, y_{i,2}\}, \cdots, \{x_{i,n-1}, y_{i,n-1}\}\}, \quad (1)$$

where $\{x_{i,j}, y_{i,j}\}$ ($j = 1, 2, \cdots, n-1$) is an edge corresponding to an information bit contained in the i-th column. According to the cyclic symmetry of the code, for an arbitrary integer k, we have

$$C_{i+k \bmod 2n} = \{\{x + k \bmod 2n, y + k \bmod 2n\} : \{x, y\} \in C_i\}. \quad (2)$$

Now, add two infinity vertices ∞_1 and ∞_2 to the foregoing graph G. At the same time, for $i = 0, 1, \cdots, 2n-1$, add two edges $\{i, \infty_1\}$ and $\{r_i, \infty_2\}$ to C_i, where r_i is an integer from 0 to $2n-1$ such that the expanded set $\widetilde{C}_i$ is a one-factor of the expanded graph $\widetilde{G}$ of vertices $0, 1, \cdots, 2n-1, \infty_1, \infty_2$. Then, $\widetilde{C}_i$ ($i = 0, 1, \cdots, 2n-1$) has the following form:

$$\widetilde{C}_i = C_i \cup \{\{i, \infty_1\}, \{r_i, \infty_2\}\}. \quad (3)$$

For $i = 0, 1, \cdots, 2n-1$, define $\infty_1 + i = \infty_1$ and $\infty_2 + i = \infty_2$. Then, for an arbitrary integer k, we have

$$\widetilde{C}_{i+k \bmod 2n} = \left\{\{x + k \bmod 2n, y + k \bmod 2n\} : \{x, y\} \in \widetilde{C}_i\right\}. \quad (4)$$

It is clear that the new graph $\widetilde{G}$ is a $2n$-regular graph on $2n+2$ vertices. It can be easily deduced from the result in [13] that if a cyclic lowest density MDS array code of distance 3 exists for length $2n$, $F = \left\{\widetilde{C}_0, \widetilde{C}_1, \cdots, \widetilde{C}_{2n-1}\right\}$ is a P1F of $\widetilde{G}$.

III. Cyclic Lowest Density MDS Array Codes Constructed Using Starters

A. Code Construction Using Normalized Cyclic Bipyramidal Starters

In the literature of graph theory, it is well-known that a $2n$-regular graph on $2n+2$ vertices is one-factorizable [15]. For a $2n$-regular graph on $2n+2$ vertices, we define a cyclic bipyramidal one-factorization as follows:

Definition 2: For a $2n$-regular graph on a set of $2n+2$ vertices $\{a_0, a_1, \cdots, a_{2n-1}, \infty_1, \infty_2\}$ (where the two vertices ∞_1 and ∞_2 are not adjacent to each other), a *cyclic bipyramidal one-factorization* is a one-factorization consisting of $2n$ factors $F_0, F_1, \cdots, F_{2n-1}$, which meet $F_i = \left\{\{\sigma^i(x), \sigma^i(y)\} : \{x, y\} \in F_0\right\}$ for $i = 1, 2, \cdots, 2n-1$, where σ is a permutation represented by a product of disjoint cycles $(a_0\ a_1\ \cdots\ a_{2n-1})(\infty_1)(\infty_2)$.

In the above definition, if we relabel vertex a_i with i for $i = 0, 1, \cdots, 2n-1$, we then obtain a normalized $2n$-regular graph G on a set of $2n+2$ vertices $\{0, 1, \cdots, 2n-1, \infty_1, \infty_2\}$. The corresponding cyclic bipyramidal one-factorization thus becomes a one-factorization consisting of $2n$ factors $\bar{F}_0, \bar{F}_1, \cdots, \bar{F}_{2n-1}$, which meet $\bar{F}_i = \left\{\{\bar{\sigma}^i(x), \bar{\sigma}^i(y)\} : \{x, y\} \in \bar{F}_0\right\}$ for $i = 1, 2, \cdots, 2n-1$, where $\bar{\sigma} = (0\ 1\ \cdots\ 2n-1)(\infty_1)(\infty_2)$. Such a one-factorization is then called as a *normalized cyclic bipyramidal one-factorization*.

From the discussion in Section II, we can see that for a cyclic lowest density MDS array code of distance 3 and length $2n$, the corresponding P1F is a normalized cyclic bipyramidal one-factorization of a $2n$-regular graph on a set of $2n+2$

vertices $\{0, 1, \cdots, 2n-1, \infty_1, \infty_2\}$. For a normalized cyclic bipyramidal one-factorization, we define the corresponding normalized cyclic bipyramidal starter as follows.

Definition 3: For a $2n$-regular graph G on a set of $2n+2$ vertices $\{0, 1, \cdots, 2n-1, \infty_1, \infty_2\}$ (where the two vertices ∞_1 and ∞_2 are not adjacent to each other), suppose a one-factorization F is a normalized cyclic bipyramidal one-factorization in which F_0 is the one-factor that contains the edge $\{0, \infty_1\}$. Let $S = F_0 \setminus \{\{0, \infty_1\}, \{r, \infty_2\}\}$, where r is the vertex that is adjacent to the vertex ∞_2 in F_0. Then, S is called as a *normalized cyclic bipyramidal starter* for F.

From the above definition, we can see that a normalized cyclic bipyramidal one-factorization can be induced directly by a normalized cyclic bipyramidal starter.

Let Z_{2n} be the set of congruence classes modulo $2n$, i.e. $Z_{2n} = \{0, 1, \cdots, 2n-1\}$. Then, $(Z_{2n}, +)$ is the additive group of congruence classes modulo $2n$. The following theorem will tell us how to find a normalized cyclic bipyramidal starter in $(Z_{2n}, +)$.

Theorem 1: In $(Z_{2n}, +)$, choose $2n-2$ non-zero elements to form a set of $n-1$ pairs, i.e. $S = \{\{x_1, y_1\}, \{x_2, y_2\}, \cdots, \{x_{n-1}, y_{n-1}\}\}$, such that every integer from 1 to $n-1$ occurs as a difference of exactly one pair of S. Then, S is a normalized cyclic bipyramidal starter for a $2n$-regular graph G on a set of $2n+2$ vertices $\{0, 1, \cdots, 2n-1, \infty_1, \infty_2\}$, where there is no edge between the following pairs of vertices: $\{\infty_1, \infty_2\}$ and all $\{i, i+n\}$ for $i = 0, 1, \cdots, n-1$.

Proof: Let $\widetilde{S} = S \cup \{\{0, \infty_1\}, \{r, \infty_2\}\}$, where r is the non-zero element of Z_{2n} that does not appear in S. For $i = 0, 1, \cdots, 2n-1$, define $F_i = \left\{\{x+i, y+i\} : \{x, y\} \in \widetilde{S}\right\}$, where $\infty_1 + i = \infty_1$ and $\infty_2 + i = \infty_2$. It is clear that each F_i $(i = 0, 1, \cdots, 2n-1)$ is a one-factor of G. For each edge in G, it appears in exactly one of one-factors $F_0, F_1, \cdots, F_{2n-1}$. Thus, $F = \{F_0, F_1, \cdots, F_{2n-1}\}$ is a one-factorization of G. Then, a normalized cyclic bipyramidal one-factorization F is induced by S. This proves that S is a normalized cyclic bipyramidal starter. ■

For example, $S = \{\{1, 3\}, \{4, 5\}\}$ is a normalized cyclic bipyramidal starter in $(Z_6, +)$.

Then, we discuss how to construct cyclic lowest density MDS array codes using normalized cyclic bipyramidal starters. The steps to construct a cyclic lowest density MDS array code of distance 3 and length $2n$ are to first find a normalized cyclic bipyramidal starter S in $(Z_{2n}, +)$ and then check whether the normalized cyclic bipyramidal one-factorization F induced by S is a P1F of a $2n$-regular graph on a set of $2n+2$ vertices $\{0, 1, \cdots, 2n-1, \infty_1, \infty_2\}$. Here, let $F = \{F_0, F_1, \cdots, F_{2n-1}\}$. According to the cyclic symmetry of F, it is clear that if $F_0 \cup F_i$ is a Hamiltonian cycle for all i from 1 to n, F is then a P1F of G. Thus, only n rather than $\binom{2n}{2}$ subgraphs need to be checked in determining whether F is a P1F. From the discussion in Section II, if F is a P1F, a cyclic lowest density MDS array code of distance 3 and length $2n$, in which the i-th column $(i = 0, 1, \cdots, 2n-1)$ is $C_i = \{\{x + i \bmod 2n, y + i \bmod 2n\} : \{x, y\} \in S\}$, can be constructed using S; otherwise we try other normalized cyclic bipyramidal starters in $(Z_{2n}, +)$ until a cyclic lowest density MDS array code is constructed, or all the normalized cyclic bipyramidal starters in $(Z_{2n}, +)$ are checked.

For example, the foregoing normalized cyclic bipyramidal starter $S = \{\{1, 3\}, \{4, 5\}\}$ in $(Z_6, +)$ induces a P1F of a 6-regular graph on 8 vertices. Thus, a cyclic lowest density MDS array code of distance 3 and length 6 can be constructed using S. This code is the same as the instance of $\kappa_{1\circ}(7)$ in [4].

It should be noted that an exhaustive search showed that a cyclic lowest density MDS array code of distance 3 exists for most but not all of even lengths. For example, a cyclic lowest density MDS array code of distance 3 exists for every even length from 4 to 36 except 8.

B. Transformation from Non-Cyclic Codes Constructed Using Other Starters to Cyclic Codes

From the discussion in the previous subsection, we can see that every cyclic lowest density MDS array code of distance 3 and length $2n$ can be constructed using a normalized cyclic bipyramidal starter in $(Z_{2n}, +)$. Then, the question is: *Can non-cyclic lowest density MDS array codes constructed using other starters in group theory be transformed to cyclic codes?*

The answer to the above question is positive. We found that non-cyclic lowest density MDS array codes constructed using two well-known starters, i.e. even starters and patterned starters, can be transformed to cyclic codes if some conditions are satisfied.

1) Even Starters: Before discussing when and how to transform a non-cyclic lowest density MDS array code constructed using an even starter to a cyclic code, we first define even starters as follows.

Definition 4 ([16]): Let $(A_{2n}, \circ)$ be an abelian group of order $2n$ with identity e and unique element a^* of order 2 (i.e. $a^* \circ a^* = e$). An *even starter* S_E in $(A_{2n}, \circ)$ is a set of $n-1$ pairs of non-identity elements of A_{2n}, i.e. $S_E = \{\{x_1, y_1\}, \{x_2, y_2\}, \cdots, \{x_{n-1}, y_{n-1}\}\}$, such that every non-identity element of A_{2n} except a^* occurs in $\left\{x^{-1} \circ y, x \circ y^{-1} : \{x, y\} \in S_E\right\}$.

An even starter S_E in $(A_{2n}, \circ)$ induces a one-factorization of a $2n$-regular graph G on $2n+2$ vertices as follows. Label the vertices of G with the elements of A_{2n} and two infinity elements ∞_1 and ∞_2 such that there is no edge between the following pairs of vertices: $\{\infty_1, \infty_2\}$ and all $\{a, a \circ a^*\}$ for $a \in A_{2n}$. Let $\widetilde{S}_E = S_E \cup \{\{e, \infty_1\}, \{r, \infty_2\}\}$, where r is the non-identity element that does not appear in S_E. For all $a \in A_{2n}$, define $a \circ \infty_1 = \infty_1$ and $a \circ \infty_2 = \infty_2$. The corresponding one-factorization F_E is then given by $F_E = \left\{a \circ \widetilde{S}_E : a \in A_{2n}\right\}$, where $a \circ \widetilde{S}_E = \left\{\{a \circ x, a \circ y\} : \{x, y\} \in \widetilde{S}_E\right\}$. Such a one-factorization is called as a *bipyramidal one-factorization* [17].

For a bipyramidal one-factorization induced by an even starter, we have the following conclusion:

Theorem 2: A bipyramidal one-factorization F_E of a $2n$-regular graph G on $2n+2$ vertices, which is induced by an even starter S_E, is a cyclic bipyramidal one-factorization if and only if the corresponding starter group $(A_{2n}, \circ)$ is a cyclic group.

Proof: For a cyclic bipyramidal one-factorization induced by an even starter, it is clear that the corresponding starter group $(A_{2n}, \circ)$ is a cyclic group. We then prove that if $(A_{2n}, \circ)$ is a cyclic group, a bipyramidal one-factorization F_E of a $2n$-regular graph G on $2n+2$ vertices, which is induced by an even starter S_E in $(A_{2n}, \circ)$, is a cyclic bipyramidal one-factorization. Suppose $(A_{2n}, \circ)$ is a cyclic group of which a_g is a generator, i.e. $A_{2n} = \{{a_g}^0, {a_g}^1, \cdots, {a_g}^{2n-1}\}$. Let $\widetilde{S}_E = S_E \cup \{\{e, \infty_1\}, \{r, \infty_2\}\}$, where r is the non-identity element that does not appear in S_E. For $i = 0, 1, \cdots, 2n-1$, let $F_i = {a_g}^i \circ \widetilde{S}_E$. Then, $F_E = \{F_0, F_1, \cdots, F_{2n-1}\}$ is a bipyramidal one-factorization of G. For $i = 1, 2, \cdots, 2n-1$, it is clear that $F_i = \{\{\sigma^i(x), \sigma^i(y)\} : \{x, y\} \in F_0\}$, where $\sigma = (a_g^0 \ a_g^1 \ \cdots \ a_g^{2n-1})(\infty_1)(\infty_2)$. Thus, according to Definition 2 in Subsection III-A, F_E is a cyclic bipyramidal one-factorization. ∎

As shown in Subsection III-A, cyclic bipyramidal one-factorizations can be transformed to normalized cyclic bipyramidal one-factorizations that can be used to construct cyclic lowest density MDS array codes. Thus, from the above theorem, we can further make the following conclusion:

Theorem 3: A non-cyclic lowest density MDS array code constructed using an even starter in a cyclic group can always be transformed to a cyclic code.

Take even starters in a multiplicative group of congruence classes modulo p (denoted by $(Z_p^*, \times)$) for example, where p is an odd prime, and $Z_p^* = \{1, 2, \cdots, p-1\}$. Since $(Z_p^*, \times)$ is a cyclic group, a non-cyclic lowest density MDS array code constructed using an even starter in $(Z_p^*, \times)$ can always be transformed to a cyclic code. For example, $S_E = \{\{2, 6\}, \{3, 5\}\}$ is an even starter in $(Z_7^*, \times)$. Since S_E induces a P1F of a 6-regular graph on 8 vertices, a non-cyclic lowest density MDS array code of distance 3 and length 6 can be constructed using S_E. This code is the same as the P-Code of length 6 in [18]. Thus, the P-Code of length 6 can be transformed to a cyclic lowest density MDS array code.

Then, we discuss how to transform a non-cyclic lowest density MDS array code constructed using an even starter in a cyclic group to a cyclic code. Suppose an even starter S_E in a cyclic group $(A_{2n}, \circ)$ induces a P1F F_E of a $2n$-regular graph G on $2n+2$ vertices. Then, a non-cyclic lowest density MDS array code of distance 3 and length $2n$, in which the a-th column ($a \in A_{2n}$) is $C_a = a \circ S_E$, can be constructed using S_E. Suppose a_g is a generator of $(A_{2n}, \circ)$. For $i = 0, 1, \cdots, 2n-1$, replace each $\{{a_g}^j, {a_g}^k\} \in C_{{a_g}^i}$ with $\{j, k\}$ and then relabel the $({a_g}^i)$-th column with i. Reorder all the $2n$ columns in order according to their new labels. Then, a cyclic lowest density MDS array code is obtained.

2) Patterned Starters: We now discuss the case of patterned starters. A patterned starter is defined as follows.

Definition 5 ([12]): Let $(A_{2n+1}, \circ)$ be an abelian group of order $2n+1$ with identity e. The one and only *patterned starter* S_P in $(A_{2n+1}, \circ)$ is a set of n pairs of non-identity elements of A_{2n+1}, i.e. $S_P = \{\{x_1, y_1\}, \{x_2, y_2\}, \cdots, \{x_n, y_n\}\}$, such that $x \circ y = e$ for any $\{x, y\} \in S_P$.

The patterned starter S_P in $(A_{2n+1}, \circ)$ induces a one-factorization of a $2n$-regular graph G on $2n+2$ vertices as follows. Label the vertices of G with the elements of A_{2n+1} and an infinity element ∞ such that there is no edge between the following pairs of vertices: $\{e, \infty\}$ and all $\{x, y\} \in S_P$. For all $a \in A_{2n+1}$, define $a \circ \infty = \infty$. Let $\widetilde{S}_P = S_P \cup \{\{e, \infty\}\}$. The corresponding one-factorization F_P is then given by $F_P = \left\{a \circ \widetilde{S}_P : a \in (A_{2n+1} \setminus \{e\})\right\}$, where $a \circ \widetilde{S}_P = \left\{\{a \circ x, a \circ y\} : \{x, y\} \in \widetilde{S}_P\right\}$. Such a one-factorization is called as a *patterned one-factorization* [12].

Similarly to the case of even starters, a non-cyclic lowest density MDS array code constructed using S_P can be transformed to a cyclic code if and only if the patterned one-factorization F_P induced by S_P can be transformed to a cyclic bipyramidal one-factorization with a permutation $(a_0 \ a_1 \ \cdots \ a_{2n-1})(e)(\infty)$, where $\{a_0, a_1, \cdots, a_{2n-1}\} = A_{2n+1} \setminus \{e\}$. Thus, the necessary condition to transform a non-cyclic lowest density MDS array code constructed using S_P to a cyclic code is that $A_{2n+1} \setminus \{e\}$ can be used to construct a cyclic group $(A_{2n+1} \setminus \{e\}, \star)$ in which $x \star y^{-1}$ (or $x^{-1} \star y$) for any $\{x, y\} \in S_P$ is equal to the same element of order 2.

Take the patterned starter S_P in $(Z_p, +)$ for example, where p is an odd prime. It is well-known that the patterned one-factorization F_P induced by S_P is a P1F (see [12]), and a non-cyclic lowest density MDS array code of distance 3 and length $p-1$ thus can be constructed using S_P. Let $Z_p^* = Z_p \setminus \{0\}$. Then, $(Z_p^*, \times)$ is a multiplicative group of congruence classes modulo p, which is a cyclic group. For any $\{x, y\} \in S_P$, since $x + y = 0$, $x \times y^{-1}$ is then equal to $p-1$, which is an element of order 2 in $(Z_p^*, \times)$. Thus, the non-cyclic lowest density MDS array code of distance 3 and length $p-1$ constructed using the patterned starter S_P in $(Z_p, +)$ can always be transformed to a cyclic code. For example, the P-Code in [18] is a such non-cyclic code.

Here, the transformation process is similar to that in the case of even starters. We do not repeat it here.

IV. Quasi-Cyclic Lowest Density MDS Array Codes Constructed Using Multi-Starters

In the previous section, we have discussed cyclic lowest density MDS array codes constructed using starters. Our exhaustive search showed that there is no cyclic lowest density MDS array code for some even lengths, such as 8. Then, someone may ask: *Can we construct quasi-cyclic lowest density MDS array codes [4] (which partially hold cyclic symmetry) for these even lengths?*

In this section, we will introduce a concept of multi-starters and then discuss how to construct quasi-cyclic lowest density MDS array codes using multi-starters.

A κ-starter in $(Z_{2n}, +)$ (where $\kappa|2n$) is defined as follows.

Definition 6: A *κ-starter* in $(Z_{2n}, +)$ (where $\kappa|2n$) is a set $S^\kappa = \{S_0, S_1, \cdots, S_{\kappa-1}\}$, where S_i $(i = 0, 1, \cdots, \kappa-1)$ is a set of $n-1$ pairs of non-i elements of Z_{2n}, such that every integer from 1 to $n-1$ occurs κ times as a difference of a pair of S^κ.

For example, $S^2 = \{S_0, S_1\}$, where $S_0 = \{\{1,2\},\{3,6\},\{4,7\}\}$ and $S_1 = \{\{2,4\},\{3,5\},\{6,7\}\}$, is a 2-starter in $(Z_8, +)$.

A κ-starter $S^\kappa = \{S_0, S_1, \cdots, S_{\kappa-1}\}$ in $(Z_{2n}, +)$ (where $\kappa|2n$) induces a one-factorization of a $2n$-regular graph G on $2n+2$ vertices as follows. Label the vertices of G with the elements of Z_{2n} and two infinity elements ∞_1 and ∞_2 such that there is no edge between the following pairs of vertices: $\{\infty_1, \infty_2\}$ and all $\{j, j+n\}$ for $j = 0, 1, \cdots, n-1$. For all $a \in Z_{2n}$, define $a + \infty_1 = \infty_1$ and $a + \infty_2 = \infty_2$. For $i = 0, 1, \cdots, \kappa-1$, let $\widetilde{S}_i = S_i \cup \{\{i, \infty_1\}, \{r_i, \infty_2\}\}$, where r_i is the non-i element that does not appear in S_i. The corresponding one-factorization F^κ of G is then given by $F^\kappa = \left\{\kappa\tau + \widetilde{S}_0, \kappa\tau + \widetilde{S}_1, \cdots, \kappa\tau + \widetilde{S}_{\kappa-1} : \tau = 0, 1, \cdots, \frac{2n}{\kappa} - 1\right\}$, where $\kappa\tau + \widetilde{S}_i = \left\{\{\kappa\tau + x, \kappa\tau + y\} : \{x, y\} \in \widetilde{S}_i\right\}$ for $i = 0, 1, \cdots, \kappa-1$. Such a one-factorization is called as a *κ-quasi-cyclic pyramidal one-factorization*.

For a κ-starter $S^\kappa = \{S_0, S_1, \cdots, S_{\kappa-1}\}$ in $(Z_{2n}, +)$ (where $\kappa|2n$), if the κ-quasi-cyclic pyramidal one-factorization F^κ induced by S^κ is a P1F of a $2n$-regular graph on $2n+2$ vertices, a κ-quasi-cyclic lowest density MDS array code of distance 3 and length $2n$, in which the ι-th column $(\iota = 0, 1, \cdots, 2n-1)$ is $C_\iota = \{\{x + \kappa\varepsilon \bmod 2n, y + \kappa\varepsilon \bmod 2n\} : \{x, y\} \in S_\gamma\}$ (where $\varepsilon = \lfloor \frac{\iota}{\kappa} \rfloor$ and $\gamma = \iota - \kappa\varepsilon$), can be constructed using S^κ.

For example, the foregoing 2-starter $S^2 = \{S_0, S_1\}$ (where $S_0 = \{\{1,2\},\{3,6\},\{4,7\}\}$ and $S_1 = \{\{2,4\},\{3,5\},\{6,7\}\}$) in $(Z_8, +)$ induces a P1F of a 8-regular graph on 10 vertices. Thus, a 2-quasi-cyclic lowest density MDS array code of distance 3 can be constructed using S^2 for length 8. This code is the same as the instance of $\kappa_{3\circ}(5)$ in [4].

V. Conclusions

In this paper, we presented a systematic study on cyclic lowest density MDS array codes constructed using starters. We first showed that all cyclic lowest density MDS array codes of distance 3 and length $2n$ can be constructed using normalized cyclic bipyramidal starters in the additive group of congruence classes modulo $2n$. We then discussed when and how to transform non-cyclic lowest density MDS array codes constructed using other starters (including even starters and patterned starters) to cyclic codes. Finally, we also discussed how to construct quasi-cyclic lowest density MDS array codes using multi-starters for an even length when no cyclic lowest density MDS array code exists for this even length.

The results in this paper have revealed the underlying connection between cyclic (or quasi-cyclic) lowest density MDS array codes and starters in group theory and thus may enable the construction of new cyclic (or quasi-cyclic) lowest density MDS array codes of distance 3 besides those proposed in [4]. This optimistic view is supported by an exhaustive search that revealed new cyclic (or quasi-cyclic) lowest density MDS array codes of distance 3 with lengths that are not covered by the codes of length $p-1$ or $2(p-1)$ proposed in [4], where p is an odd prime. Due to space limitation, we do not list these new codes here.

References

[1] M. Blaum, P. Farrell, and H. van Tilborg, "Array codes," in *Handbook of Coding Theory*, V. Pless and W. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science B.V., 1998.

[2] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, Jun. 1960.

[3] R. M. Roth and A. Lempel, "On MDS codes via Cauchy matrices," *IEEE Trans. Inf. Theory*, vol. 35, no. 6, pp. 1314–1319, Nov. 1989.

[4] Y. Cassuto and J. Bruck, "Cyclic lowest density MDS array codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1721–1729, Apr. 2009.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: North-Holland, 1977.

[6] M. Li, J. Shu, and W. Zheng, "GRID codes: Strip-based erasure codes with high fault tolerance for storage systems," *ACM Transactions on Storage*, vol. 4, no. 4, pp. 1–22, Jan. 2009.

[7] B. Schroeder and G. A. Gibson, "Disk failures in the real world: What does an MTTF of 1,000,000 hours mean to you?" in *Proceedings of the 5th USENIX conference on File and Storage Technologies (FAST'07)*, San Jose, CA, Feb. 2007, pp. 1–16.

[8] L. N. Bairavasundaram, G. R. Goodson, S. Pasupathy, and J. Schindler, "An analysis of latent sector errors in disk drives," in *Proceedings of the 2007 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS'07)*, San Diego, CA, Jun. 2007, pp. 289–300.

[9] P. M. Chen, E. K. Lee, G. A. Gibson, R. H. Katz, and D. A. Patterson, "RAID: High-performance, reliable secondary storage," *ACM Computing Surveys*, vol. 26, no. 2, pp. 145–185, Jun. 1994.

[10] L. Xu, V. Bohossian, J. Bruck, and D. G. Wagner, "Low-density MDS codes and factors of complete graphs," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1817–1826, Sep. 1999.

[11] G. V. Zaitsev, V. A. Zinov'ev, and N. V. Semakov, "Minimum-check-density codes for correcting bytes of errors, erasures, or defects," *Problems of Information Transmission*, vol. 19, no. 3, pp. 197–204, 1983.

[12] W. D. Wallis, *One-Factorizations*. Norwell, MA: Kluwer, 1997.

[13] M. Li and J. Shu, "On the equivalence between the B-Code constructions and perfect one-factorizations," in *Proceedings of the 2010 IEEE International Symposium on Information Theory (ISIT 2010)*, Austin, TX, Jun. 2010.

[14] D. G. Wagner, "On the perfect one-factorization conjecture," *Discrete Mathematics*, vol. 104, no. 2, pp. 211–215, Jun. 1992.

[15] A. G. Chetwynd and A. J. W. Hilton, "Regular graphs of high degree are 1-factorizable," in *Proceedings of the London Mathematical Society (3), 50*, 1985, pp. 193–206.

[16] B. A. Anderson, "Sequencings and starters," *Pacific Journal of Mathematics*, vol. 64, no. 1, pp. 17–24, 1976.

[17] E. Mendelsohn and A. Rosa, "One-factorizations of the complete graph — a survey," *Journal of Graph Theory*, vol. 9, no. 4, pp. 43–65, 1985.

[18] C. Jin, H. Jiang, D. Feng, and L. Tian, "P-code: A new RAID-6 code with optimal properties," in *Proceedings of the 23rd International Conference on Supercomputing (ICS'09)*, Yorktown Heights, NY, Jun. 2009, pp. 360–369.