International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 5(2013) pp.589-596
© MIR Labs, www.mirlabs.net/ijcisim/index.html

On the Class of $\mathcal{T}$-*Direct* Codes Over $GF(2^{\mathcal{N}})$

R. S. RAJA DURAI[1], **MEENAKSHI DEVI**[2]

[1]Jaypee University of Information Technology, Department of Mathematics,
Waknaghat, Solan - 173 234, India
rsraja.durai@juit.ac.in

[2]Bahra University, Department of Mathematics,
Shimla Hills, Waknaghat, Solan - 173 234, India
meenakshi_juit@yahoo.co.in

Abstract: **A $\mathcal{T}$-*Direct* code is defined as the set of $\mathcal{T}$ F-ary linear codes $\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}}$ such that $\Gamma_i \cap \Gamma_i^{\perp} = \{\mathbf{0}\}$, where $\Gamma_i^{\perp}$ = $\Gamma_1 \oplus \Gamma_2 \oplus \cdots \oplus \Gamma_{i-1} \oplus \Gamma_{i+1} \oplus \cdots \oplus \Gamma_{\mathcal{T}}$ is the dual of Γ_i with respect to the direct sum Λ = $\Gamma_1 \oplus \Gamma_2 \oplus \cdots \oplus \Gamma_{\mathcal{T}}$ for each i = 1, 2, ..., $\mathcal{T}$. In this paper, a construction to a class of $\mathcal{T}$-*Direct* codes with the *constituent* codes from the class of 2-Cyclic Maximum Rank Distance codes is given. These class of codes are defined with a Rank metric. An application of the constructed class of codes over the $\mathcal{T}$-user F-Adder Channel, namely a coding scheme for the *noisy* case, is given. In an attempt to show the usefulness of $\mathcal{T}$-*Direct* codes as multi-user codes, a *distance* construction method for the class of $\mathcal{T}$-*Direct* codes constituted by a set of $\mathcal{T}$ *maximum rank distance* codes is proposed. The proposed *distance* construction is shown to increase the minimum distance of the *constituent* codes of $\mathcal{T}$-*Direct* codes when employed. Further, a construction procedure that constructs $(n+m)$-*Direct* codes over $GF(2^n)$ is developed from the proposed *distance* construction, $0 < m \leq \frac{n(n+1)}{2}$. It is shown that the extended *distance* construction procedure increases the number of users (*constituent* codes) of a $\mathcal{T}$-*Direct* code; when employed on an n-*Direct* code, it constructs an $\left[\frac{n(n+1)}{2}\right]$-*Direct* code, thereby supporting more users in a multi-user environment.**

Keywords: LCD codes, $\mathcal{T}$-*Direct* codes, MRD codes, q-Cyclic MRD codes, $\mathcal{T}$-user F-Adder Channel, Kronecker product.

I. Introduction

The coding problem for a multi-user communication system is to assign codes to each user so that they can communicate simultaneously over a common channel with a single receiver. The study of multiple-access communication systems was first initiated by Shannon in 1961 - he studied the two-way communication channels and also bounds on the capacity region were established [1]. Several authors investigated the information-theoretic aspects of multiple-access channels [3]-[7]. In the literature, there has been extensive research work on the coding schemes and capacity calculations for a multiple access channel known as the *binary adder channel* [9], [10], [11], [14]. Various aspects of multiple access channels were also given in [2], [12].

In recent years, linear network coding has been a promising new approach to information dissemination over networks. Some of upcoming technologies which attracted research attention in the recent years are Wireless Sensor Networks (WSNs) [28] and Voice over Internet Protocol (VoIP) [29]. A study on the multi-user F-Adder Channel has been discussed in [16], [17], where a coding scheme is given using Reed-Solomon codes. The problem of error control in network coding had been discussed in [21]-[26], where an additive-multiplicative matrix channel was considered as a model for network coding. Recently, a coding problem of communicating messages between multiple sources and destinations over a general noisy network is considered [33]. In connection to the network coding problem, a coding scheme for the $\mathcal{T}$-user F-Adder Channel had been studied in [18], [19] where the class of $\mathcal{T}$-*Direct* codes are introduced and shown to be effective in coding for the *noiseless* scenario. This class of multi-user codes is an extension to the so called *linear codes with complementary duals* (LCD codes) [15]. For an arbitrary finite field F, an F-ary linear code Γ is called an LCD code if $\Gamma \cap \Gamma^{\perp} = \{\mathbf{0}\}$. An F-ary $\mathcal{T}$-*Direct* code or simply a $\mathcal{T}$-*Direct* code is defined as the set of $\mathcal{T}$ F-ary linear codes $\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}}$ such that $\Gamma_i \cap \Gamma_i^{\perp} = \{\mathbf{0}\}$, where $\Gamma_i^{\perp}$ = $\Gamma_1 \oplus \Gamma_2 \oplus \cdots \oplus \Gamma_{i-1} \oplus \Gamma_{i+1} \oplus \cdots \oplus \Gamma_{\mathcal{T}}$ is the dual of Γ_i with respect to the direct sum $\Lambda = \Gamma_1 \oplus \Gamma_2 \oplus \cdots \oplus \Gamma_{\mathcal{T}} \subseteq F^n$ for each i = 1, 2, ..., $\mathcal{T}$ denoted by $(\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}})$; each Γ_i is called the *constituent* code [18]. Unlike the *binary adder channels* which are real-number adder channels, arithmetic operations on the channel alphabets (elements of the field F) in F-Adder Channel are performed under the operations defined in the underlying field F.

Our main objective in this paper is to explore some of the interesting coding characteristics enjoyed by the class of $GF(2^n)$-ary $\mathcal{T}$-*Direct* codes and thus showing the usefulness of $\mathcal{T}$-*Direct* codes in a multi-user environment. To facilitate our objective, first we present a coding scheme for the $\mathcal{T}$-user F-Adder Channel (for *noisy* case) by incorporating the ideas of the class of $\mathcal{T}$-*Direct* codes. The coding scheme is accomplished by constructing a class of $\mathcal{T}$-*Direct* codes with *constituent* codes from the class of 2-cyclic MRD codes. Using the constructed class of $\mathcal{T}$-*Direct* codes ($\mathcal{T}$-*Direct* 2-cyclic MRD codes), the coding for the *noisy* $\mathcal{T}$-user F-Adder Channel is described. The class of Rank Distance codes is a newer branch of Algebraic coding theory and is introduced by E. M. Gabidulin in 1985 [13]. Some useful applications of Rank Distance codes are discussed in [30], [32], [34].

Further, a construction method is proposed for the class of $\mathcal{T}$*-Direct* codes to increase the minimum distance of the *constituent* codes. Since the proposed construction procedure increases the minimum distance of the *constituent* codes of a $\mathcal{T}$*-Direct* code when employed, it is termed as the *distance* construction. Further, the *distance* construction is extended to increase the number of *users* (*constituent* codes) of a $\mathcal{T}$-*Direct* code: the procedure when employed on an n*-Direct* code defined over $GF(2^n)$ constructs an $\left\lceil \frac{n(n+1)}{2} \right\rceil$*-Direct* code over the same field $GF(2^n)$. For both the constructions, the Kronecker product is used as a basic tool.

The remaining part of the paper is organized as follows. The following section presents the basic definitions and notations, in order to make this paper self-contained. In section III, we make an interesting observation that a certain class of Rank Distance codes qualify to be LCD codes. Further, a construction to a class of $\mathcal{T}$*-Direct* codes with *constituent* codes being Rank Distance codes is presented. Section IV describes an application of the constructed class of $\mathcal{T}$*-Direct* codes over the $noisy$ $\mathcal{T}$-user F-Adder Channel. The section V proposes a *distance* construction procedure for the class of $\mathcal{T}$*-Direct* codes, as outlined in [31]. Section VI gives a code construction for the class of $\mathcal{T}$*-Direct* codes defined over $GF(2^n)$ that is based on the *distance* construction procedure proposed. This extended *distance* construction procedure enables the class of 2^n-ary n*-Direct* codes to allow more users to participate in the channel under consideration; $n < \mathcal{T} \leq \frac{n(n+1)}{2}$ - precisely. Final section draws the conclusion based on the results.

II. Preliminary Ideas

This section describes some fundamentals of rank distance codes introduced by Gabidulin in 1985 and $\mathcal{T}$*-Direct* codes. Let V^n be an n-dimensional *vector space* over the field $GF(q^N)$, where q is a power of a *prime* and $n \leq N$. Assume that u_1, u_2, ..., u_N is some fixed basis of the field $GF(q^N)$, regarded as a *vector space* over $GF(q)$. Any element $x_i \in GF(q^N)$ can be uniquely represented in the form x_i = $a_{1i}u_1$ + $a_{2i}u_2$+ $\cdots$ + $a_{Ni}u_N$. Let x = $(x_1, x_2, \ldots, x_n)$ $\in V^n$ and A^n_N be the collection of all $N \times n$ matrices over $GF(q)$. Associated with each $x \in V^n$, the $N \times n$ matrix denoted by $A(x)$ is defined as

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{Nn} \end{pmatrix}$$

Definition 2.1 [13] The rank of a vector $x \in V^n$ over $GF(q^N)$ is defined as the rank of the matrix $A(x)$ and is denoted by $r(x; q)$. The norm $r(x; q)$ specifies a rank metric on V^n as $d(x, y)$ = $r(x - y; q)$ for all $x, y \in V^n$.

Definition 2.2 [13] A linear (n, k, d) code which is a k-dimensional subspace of V^n is said to be a Rank Distance (RD) code if its metric is induced by the rank norm. An (n, k, d) RD code is said to be Maximum Rank Distance (MRD) code if d = n - k + 1. Here d is the minimum distance of the code and is defined as the minimum rank any non-zero codeword can have.

Definition 2.3 [13] An (n, k, d) RD code Γ is called q-Cyclic if q-Cyclic shift of any code vector is also a code vector, i.e., if $(c_0, c_1, \ldots, c_{n-1})$ belongs to Γ, then $(c^{[1]}_{n-1}, c^{[1]}_0, \ldots, c^{[1]}_{n-2})$ also belongs to Γ, where and here after we use the notation: $[m]$ = q^m for some positive integer m.

Definition 2.4 [13] An (n, k, d) q-Cyclic code with d = $n - k + 1$, termed as q-Cyclic MRD code, is generated by the generator matrix G defined as follows:

$$G = \begin{pmatrix} \alpha^{[0]} & \alpha^{[1]} & \cdots & \alpha^{[n-1]} \\ \alpha^{[1]} & \alpha^{[2]} & \cdots & \alpha^{[n]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{[k-1]} & \alpha^{[k]} & \cdots & \alpha^{[k+n-2]} \end{pmatrix}$$

where $\{\alpha^{[0]}, \alpha^{[1]}, \ldots, \alpha^{[n-1]}\}$ forms a normal basis in $GF(q^n)$. The paper considers the case when $n = N$.

For an arbitrary finite field F, the class of F-ary $\mathcal{T}$*-Direct* codes are a natural extension to the class of *linear codes with complementary duals*. The following theorem gives the necessary and sufficient condition for a set of $\mathcal{T}$ F-ary linear codes to constitute a $\mathcal{T}$*-Direct* code.

Theorem 2.5 [18] Let Γ_i be an (n, k_i) F-ary linear code with the generator matrix G_i such that $G_iGj^{\mathbf{T}}$ = $(\mathbf{0})$ for each i = $1, 2, \ldots, \mathcal{T}$ with $i \neq j$. Then $(\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}})$ is a $\mathcal{T}$*-Direct* code if and only if the $k_i \times k_i$ matrix $G_iG_i^{\mathbf{T}}$ is non-singular for every i. Further, if $(\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}})$ is a $\mathcal{T}$*-Direct* code, then $\Pi_{\Gamma_i} = G_i^{\mathbf{T}}(G_iG_i^{\mathbf{T}})^{-1}G_i$ is the *orthogonal projector* from $\Lambda = \Gamma_1 \oplus \Gamma_2 \oplus \cdots \oplus \Gamma_{\mathcal{T}}$ onto Γ_i for each i.

$\mathcal{T}$-user F-Adder Channel 2.6 Given any finite field F, the F-Adder Channel is described as the channel whose inputs are elements of F and the output is the sum (over F) of the inputs. It is important to note that, unlike the *adder channel*, the addition performed is not the real addition but a modulo addition defined in the underlying field F. The reader is advised to refer [16] and [17] for more details on F-Adder Channel. In this communication system, the $\mathcal{T}$ users send the $\mathcal{T}$ n-tuples say $\gamma_1, \gamma_2, \ldots, \gamma_{\mathcal{T}}$ respectively from the F-ary linear codes $\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}}$. When the channel is *noiseless*, the received sequence **r** is the componentwise sum **r** = $\gamma_1 + \gamma_2 + \cdots + \gamma_{\mathcal{T}}$ over F. The problem for the receiver is

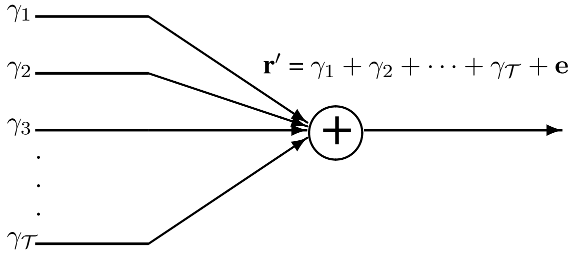
γ_1
γ_2
γ_3
$\gamma_{\mathcal{T}}$
$\mathbf{r}' = \gamma_1 + \gamma_2 + \cdots + \gamma_{\mathcal{T}} + \mathbf{e}$
+

Fig. 1: $Noisy$ $\mathcal{T}$-user F-Adder Channel

to decode the received sequence $\mathbf{r}$ into the actual codewords $\gamma_1, \gamma_2, \ldots, \gamma_{\mathcal{T}}$ originally transmitted. The class of $\mathcal{T}$*-Direct* codes provides a solution to this problem [18].

In the $noisy$ case, as depicted in figure 1, the received sequence $\mathbf{r}'$ is the componentwise sum $\mathbf{r}' = \gamma_1 + \gamma_2 + \cdots + \gamma_{\mathcal{T}} + \mathbf{e}$ where the n-tuple $\mathbf{e}$ is an error induced by the noisy channel. Here, the problem for the receiver is to employ an efficient error-correcting decoding technique to decode the received sequence $\mathbf{r}' = \gamma_1 + \gamma_2 + \cdots + \gamma_{\mathcal{T}} + \mathbf{e}$ into the actual codewords $\gamma_1, \gamma_2, \ldots, \gamma_{\mathcal{T}}$ originally transmitted. The class of $\mathcal{T}$*-Direct* 2-Cyclic MRD codes constructed in section 3 provides a solution to this problem, where it is explained how the constructed class of $\mathcal{T}$*-Direct* codes can be effectively employed over the $noisy$ $\mathcal{T}$-user F-Adder Channel.

Notation and abbreviation 2.7 We use the notation $(\{n_1, n_2, \ldots, n_{\mathcal{T}}\}, \{k_1, k_2, \ldots, k_{\mathcal{T}}\}, \{d_1, d_2, \ldots, d_{\mathcal{T}}\})$ to denote a $\mathcal{T}$*-Direct* code constituted by the *constituent* codes (n_1, k_1, d_1), (n_2, k_2, d_2), …, $(n_{\mathcal{T}}, k_{\mathcal{T}}, d_{\mathcal{T}})$ and is abbreviated as $(\{n_i\}, \{k_i\}, \{d_i\})$. In particular, a $\mathcal{T}$*-Direct* code with $k_1 = k_2 = \cdots = k_{\mathcal{T}} = k$ (say) is denoted by $(\{n_i\}, \{k\}, \{d_i\})$ rather than $(\{n_i\}, k, \{d_i\})$ - to distinguish a $\mathcal{T}$*-Direct* code from a conventional single user code, namely (n, k, d). Also, note that, when we consider q^n-ary (n, k, d) MRD codes in association with F-Adder Channel, the channel alphabets would be the elements from the underlying field $GF(q^n)$; i.e., $F = GF(q^n)$.

III. $\mathcal{T}$*-Direct* q-Cyclic MRD Codes

By a $\mathcal{T}$*-Direct* q-Cyclic MRD code, we mean a $\mathcal{T}$*-Direct* code with *constituent* codes from the class of q-Cyclic MRD codes. Our objective in this section is to give a construction to the class of $\mathcal{T}$*-Direct* 2-Cyclic MRD codes. Before that, we make an interesting observation of the class of 2-Cyclic MRD codes.

A. 2-Cyclic MRD Codes as Complementary Duals

This subsection identifies certain class of Rank Distance codes which are LCD codes. This observation allows us to choose these Rank Distance codes, having complementary duals as *constituent* codes, in the construction of $\mathcal{T}$*-Direct* 2-Cyclic MRD codes. The results of this subsection are drawn from [20].

Proposition 3.1.1 An (n, k, d) 2-Cyclic MRD code defined by the matrix

$$G = \begin{pmatrix} \alpha^{[0]} & \alpha^{[1]} & \cdots & \alpha^{[n-1]} \\ \alpha^{[1]} & \alpha^{[2]} & \cdots & \alpha^{[n]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{[k-1]} & \alpha^{[k]} & \cdots & \alpha^{[k+n-2]} \end{pmatrix}$$

with $\{\alpha^{[0]}, \alpha^{[1]}, \ldots, \alpha^{[n-1]}\}$ being a *trace-orthogonal basis* in $GF(2^n)$ is an LCD code.

Proof: In order to prove that the code, say Γ, generated by G is an LCD code, one has to prove that the $k \times k$ matrix $GG^{\mathbf{T}}$ is non-singular [15]. Since $\{\alpha^{[0]}, \alpha^{[1]}, \ldots, \alpha^{[n-1]}\}$ being a *trace-orthogonal basis* in $GF(2^n)$, the k row-vectors are orthonormal vectors. It follows that $GG^{\mathbf{T}} = \mathbf{I}$, where $\mathbf{I}$ denotes the identity matrix. Thus, $GG^{\mathbf{T}}$ is non-singular.

In the above proposition, it is proved that the class of (n, k, d) 2-Cyclic MRD codes defined by the generator matrices with a *trace-orthogonal basis* being the first row are LCD codes. For a positive integer r, a *trace-orthogonal basis* $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ is a basis of $GF(2^r)$ over $GF(2)$ with the property that $\mathbf{tr}(\alpha_\imath \alpha_j) = \delta_{\imath j}$, $1 \leq \alpha_{\imath j} \leq r$ for all $\imath$ and j, where $\mathbf{tr}$ is the absolute trace from $GF(2^r)$ to $GF(2)$ defined as $\mathbf{tr}(\alpha) = \sum_{\imath=0}^{r-1} \alpha^{2^\imath}$. The existence of a *trace-orthogonal basis* of $GF(2^r)$ over $GF(2)$ for arbitrary value of r has been established in [8].

The following theorem gives a sufficient condition for a set of $\mathcal{T}$ F-ary linear codes $\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}}$ to constitute a $\mathcal{T}$*-Direct* code $(\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}})$.

Theorem 3.1.2 Let Γ_i be an (n, k_i) F-ary linear code with generator matrix G_i for each $i = 1, 2, \ldots, \mathcal{T}$. Then $(\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}})$ is a $\mathcal{T}$*-Direct* code if the $k_1 + k_2 + \cdots + k_{\mathcal{T}}$ row-vectors of $G_1, G_2, \ldots, G_{\mathcal{T}}$ are orthonormal vectors in F^n.

Proof: Since the row-vectors of $G_1, G_2, \ldots, G_{\mathcal{T}}$ are orthonormal, $G_i G_j^{\mathbf{T}}$ = $(\mathbf{0})$ and $G_i G_i^{\mathbf{T}}$ = $\mathbf{I}$ for each i with $i \neq j$, where $\mathbf{I}$ is the $k_i \times k_i$ identity matrix. Thus, by Theorem 2.5, the $\mathcal{T}$ F-ary linear codes with the generator matrices having orthonormal row-vectors constitute a $\mathcal{T}$*-Direct* code.

B. Construction of $\mathcal{T}$*-Direct* 2*-Cyclic MRD Codes*

Let $\{\alpha^{[0]}, \alpha^{[1]}, \ldots, \alpha^{[n-1]}\}$ be a *trace-orthogonal basis* in $GF(2^n)$. Let $k_1, k_2, \ldots, k_{\mathcal{T}} \geq 0$ be a set of positive integers such that $k_1 + k_2 + \cdots + k_{\mathcal{T}} \leq n$. We choose (n, k_1, d_1), (n, k_2, d_2), …, $(n, k_{\mathcal{T}}, d_{\mathcal{T}})$ 2-Cyclic MRD codes Γ_1, Γ_2, …, $\Gamma_{\mathcal{T}}$ with the generator matrices G_{k_1}, G_{k_2}, …, $G_{k_{\mathcal{T}}}$ respectively defined as

$$G_{k_1} = \begin{pmatrix} \alpha^{[0]} & \alpha^{[1]} & \cdots & \alpha^{[n-1]} \\ \alpha^{[1]} & \alpha^{[2]} & \cdots & \alpha^{[n]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{[k_1-1]} & \alpha^{[k_1]} & \cdots & \alpha^{[k_1+n-2]} \end{pmatrix}$$

$$G_{k_2} = \begin{pmatrix} \alpha^{[\delta_1]} & \alpha^{[\delta_1+1]} & \cdots & \alpha^{[\delta_1+n-1]} \\ \alpha^{[\delta_1+1]} & \alpha^{[\delta_1+2]} & \cdots & \alpha^{[\delta_1+n]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{[\delta_1+k_2-1]} & \alpha^{[\delta_1+k_2]} & \cdots & \alpha^{[\delta_1+k_2+n-2]} \end{pmatrix}$$

$$\vdots$$

$$G_{k_{\mathcal{T}}} = \begin{pmatrix} \alpha^{[\delta_{\mathcal{T}-1}]} & \cdots & \alpha^{[\delta_{\mathcal{T}-1}+n-1]} \\ \alpha^{[\delta_{\mathcal{T}-1}+1]} & \cdots & \alpha^{[\delta_{\mathcal{T}-1}+n]} \\ \vdots & \ddots & \vdots \\ \alpha^{[\delta_{\mathcal{T}-1}+k_{\mathcal{T}}-1]} & \cdots & \alpha^{[\delta_{\mathcal{T}-1}+k_{\mathcal{T}}+n-2]} \end{pmatrix}$$

where δ_i = $k_1 + k_2 + \cdots + k_i$ for each i = 1, 2, …, $\mathcal{T}$.

Since $\{\alpha^{[0]}, \alpha^{[1]}, \ldots, \alpha^{[n-1]}\}$ being a normal basis in $GF(2^n)$, the set $\{\alpha^{[k_1+\cdots+k_{i-1}]}$, $\alpha^{[k_1+\cdots+k_{i-1}+1]}, \ldots, \alpha^{[k_1+\cdots+k_{i-1}+n-1]}\}$ also forms a normal basis in $GF(2^n)$ for each $i = 1, 2, \ldots, \mathcal{T}$. Thus G_{k_i}

indeed defines an (n, k_i, d_i) 2-Cyclic MRD code Γ_i for each $i = 1, 2, \ldots, \mathcal{T}$. Let $\Lambda = \Gamma_1 \oplus \Gamma_2 \oplus \cdots \oplus \Gamma_{\mathcal{T}}$. The $\mathcal{T}$ 2-Cyclic MRD codes generated by the generator matrices G_{k_1}, G_{k_2}, $\ldots$, $G_{k_{\mathcal{T}}}$ defined above in fact constitute a *$\mathcal{T}$-Direct* code as the following theorem states.

Theorem 3.2.1 Let Γ_i denote the (n, k_i, d_i) 2-Cyclic MRD code generated by the generator matrix G_{k_i} defined above for each i. Then $(\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}})$ is a *$\mathcal{T}$-Direct* code.

The proof is straightforward from theorem 3.1.2. It then follows that, $(\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}})$ being a *$\mathcal{T}$-Direct* code, the *orthogonal projector* Π_{Γ_i} from Λ onto Γ_i defined as $\mathbf{r}\Pi_{\Gamma_i} = \mathbf{r}G^{\mathbf{T}}_{k_i}(G_{k_i}G^{\mathbf{T}}_{k_i})^{-1}G_{k_i} = \mathbf{r}G^{\mathbf{T}}_{k_i}G_{k_i}$ for all $\mathbf{r} \in \Lambda$ exists for each $i = 1, 2, \ldots, \mathcal{T}$ [18]. When employing *$\mathcal{T}$-Direct* codes over the $\mathcal{T}$-user F-Adder Channel, the *orthogonal projector* plays a vital role in decoding the received sequence in both the *noiseless* and *noisy* cases, as can be seen in the next section.

IV. Coding for the noisy $\mathcal{T}$-User F-Adder Channel

Let F be a Galois field with characteristic 2, namely $F = GF(2^n)$ - unless otherwise specified. Consider the *noisy* $\mathcal{T}$-user F-Adder Channel. Let Γ_1, Γ_2, $\ldots$, $\Gamma_{\mathcal{T}}$ respectively denote (n, k_1, d_1), (n, k_2, d_2), $\ldots$, $(n, k_{\mathcal{T}}, d_{\mathcal{T}})$ 2-Cyclic MRD codes with their respective generator matrices $G_{k_1}, G_{k_2}, \ldots, G_{k_{\mathcal{T}}}$ (defined as in section III) such that $(\Gamma_1, \Gamma_2, \ldots, \Gamma_{\mathcal{T}})$ is a *$\mathcal{T}$-Direct* code. Let $K = k_1 + k_2 + \cdots + k_{\mathcal{T}}$ and $D = n - K + 1$.

$$\text{Let } G \quad = \quad \begin{bmatrix} G_{k_1} \\ G_{k_2} \\ \vdots \\ G_{k_{\mathcal{T}}} \end{bmatrix}$$

be the $K \times n$ matrix with the K row-vectors from the generator matrices G_{k_1}, G_{k_2}, $\ldots$, $G_{k_{\mathcal{T}}}$. Let H be such that $GH^{\mathbf{T}} = (\mathbf{0})$.

By the very construction of G, it defines an (n, K, D) 2-Cyclic MRD code with complementary duals. Let Γ denote the (n, K, D) 2-Cyclic MRD code defined by G. Being an LCD code, the *orthogonal projector* Π_Γ from $[GF(2^n)]^n$ onto Γ defined as $\mathbf{r}\Pi_\Gamma = \mathbf{r}G^{\mathbf{T}}(GG^{\mathbf{T}})^{-1}G$ for all $\mathbf{r} \in [GF(2^n)]^n$ exists [15]. Also note that if $\gamma_i \in \Gamma_i$ for each $i = 1, 2, \ldots, \mathcal{T}$, then $\gamma_1 + \gamma_2 + \cdots + \gamma_{\mathcal{T}} \in \Gamma$.

Suppose that the $\mathcal{T}$ users send the $\mathcal{T}$ codewords, say γ_1, γ_2, $\ldots$, $\gamma_{\mathcal{T}}$ respectively from the *constituent* codes Γ_{k_1}, Γ_{k_2}, $\ldots$, $\Gamma_{k_{\mathcal{T}}}$ of the *$\mathcal{T}$-Direct* 2-Cyclic MRD code $(\Gamma_{k_1}, \Gamma_{k_2}, \ldots, \Gamma_{k_{\mathcal{T}}})$. As described, in this *noisy* channel, the received vector $\mathbf{r}'$ is $\gamma_1 + \gamma_2 + \cdots + \gamma_{\mathcal{T}} + \mathbf{e}$ over $GF(2^n)$, where $\mathbf{e} = (e_1, e_2, \ldots, e_n) \in [GF(2^n)]^n$ is an error-vector. Assume that the rank of the error-vector e is $m \leq \lfloor (D-1)/2 \rfloor$. The receiver recovers the codewords $\gamma_1, \gamma_2, \ldots, \gamma_{\mathcal{T}}$ from $\mathbf{r}'$ as described below. The decoder first computes the syndrome of the received vector. The syndrome S of the received vector $\mathbf{r}'$ is,

$$\begin{aligned} S &= \mathbf{r}'H^{\mathbf{T}} \\ &= (\gamma_1 + \gamma_2 + \cdots + \gamma_{\mathcal{T}} + \mathbf{e})H^{\mathbf{T}} \\ &= (\mathbf{0}) + \mathbf{e}H^{\mathbf{T}} \quad [since\ \gamma_i H^{\mathbf{T}} = (\mathbf{0})\ \forall\ i] \\ &= \mathbf{e}H^{\mathbf{T}} \\ &= (s_0, s_1, \ldots, s_{D-2}). \end{aligned}$$

The receiver then determines the error-vector $\mathbf{e}$ by applying an error-correcting decoding technique of the underlying code Γ. Then $\mathbf{r} = \mathbf{r}' - \mathbf{e} = \gamma_1 + \gamma_2 + \cdots + \gamma_{\mathcal{T}}$ is the sum of the codewords $\gamma_1, \gamma_2, \ldots, \gamma_{\mathcal{T}}$ over $GF(2^n)$. The decoder's problem now reduces to finding the codewords $\gamma_1, \gamma_2, \ldots, \gamma_{\mathcal{T}}$ from $\mathbf{r} = \gamma_1 + \gamma_2 + \cdots + \gamma_{\mathcal{T}}$. To find the codewords γ_1, γ_2, $\ldots$, $\gamma_{\mathcal{T}}$, the receiver simply applies the *orthogonal projector* $\Pi_{\Gamma_i} = (G_{k_i}G^{\mathbf{T}}_{k_i})^{-1}G_{k_i}$ on $\mathbf{r}$ for each i,

$$\begin{aligned} \mathbf{r}\Pi_{\Gamma_i} &= (\mathbf{r}' - \mathbf{e})\Pi_{\Gamma_i} \\ &= (\gamma_1 + \cdots + \gamma_i + \cdots + \gamma_{\mathcal{T}})\Pi_{\Gamma_i} \\ &= \gamma_i G^{\mathbf{T}}_{k_i}(G_{k_i}G^{\mathbf{T}}_{k_i})^{-1}G_{k_i} \\ &= \gamma_i G^{\mathbf{T}}_{k_i}G_{k_i} \quad (since\ G_{k_i}G^{\mathbf{T}}_{k_i} = \mathbf{I}) \\ &= \gamma_i. \end{aligned}$$

In this way, the transmitted codewords γ_1, γ_2, $\ldots$, $\gamma_{\mathcal{T}}$ are retrieved from the received vector $\mathbf{r}'$ successfully.

V. The Distance Construction

Let k_1, k_2, $\ldots$, $k_n \geq 0$ be a set of positive integers such that $k_1 + k_2 + \cdots + k_n \leq n$. Let $(\Gamma_1, \Gamma_2, \ldots, \Gamma_n)$ be an $(\{n\}, \{k_\imath\}, \{d_\imath\})$ *n-Direct* code such that $\Gamma_\imath$ is an $(n, k_\imath, d_\imath)$ MRD code generated by the generator matrix $G_\imath$, $\imath = 1, 2, \ldots, n$:

$$G_1 \quad = \quad \begin{pmatrix} \alpha_1^{[1]} & \alpha_2^{[1]} & \cdots & \alpha_n^{[1]} \\ \alpha_1^{[2]} & \alpha_2^{[2]} & \cdots & \alpha_n^{[2]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{[k_1]} & \alpha_2^{[k_1]} & \cdots & \alpha_n^{[k_1]} \end{pmatrix}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a *trace-orthogonal basis* in $GF(2^n)$. In a similar way, the $k_\imath \times n$ matrix G_i with the first row being $\{\ \alpha_1^{[k_1+\cdots+k_{i-1}+1]}, \alpha_2^{[k_1+\cdots+k_{i-1}+1]}, \ldots, \alpha_n^{[k_1+\cdots+k_{i-1}+1]}\ \}$ is given by

$$G_\imath \quad = \quad \left[\ \alpha_s^{[k_1+\cdots+k_{i-1}+r]}\ \right]_{r,s=1}^{k_\imath, n} \qquad i = 2, 3, \ldots, n$$

It is known that a *trace-orthogonal basis* of $GF(2^r)$ over $GF(2)$ exists for any positive integer r [8]. Since $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a normal basis in $GF(2^n)$, $\{\alpha_1^{[\imath]}, \alpha_2^{[\imath]}, \ldots, \alpha_n^{[\imath]}\}$ is also some normal basis in $GF(2^n)$ for each $i = 1, 2, \ldots, n$. Let $\Lambda = \Gamma_1 \oplus \Gamma_2 \oplus \cdots \oplus \Gamma_n$.

Consider taking the Kronecker product of G_n with each of the generator matrices of the *constituent* codes as follows:

$$\begin{aligned} G'_1 &= G_n \otimes G_1 \\ G'_2 &= G_n \otimes G_2 \\ &\vdots \\ G'_n &= G_n \otimes G_n. \end{aligned}$$

For each $\imath = 1, 2, \ldots, n$, using the $k_n k_\imath \times n^2$ matrix $G'_\imath$, generate an $(n^2,\ k_n k_\imath)$ $GF(2^n)$-ary code $\Gamma'_\imath$ (say). The parity-check matrix for the $(n^2,\ k_n k_\imath)$ code having generator matrix $G'_\imath$ can be given as:

$$H'_\imath \;=\; \begin{bmatrix} G_i \\ H_i \\ G_n \end{bmatrix} \otimes H_i$$

Clearly, $G'_\imath H_i^{'\mathbf{T}} = (\mathbf{0})$. It remains to find the minimum distance of the newly defined codes $\Gamma'_1, \Gamma'_2, \ldots, \Gamma'_n$.

Note that the resultant codes $\Gamma'_1, \Gamma'_2, \ldots, \Gamma'_n$ are not MRD codes and consequently the minimum distance of these codes can be found in the following sense. Rank distance between two codewords is at most the Hamming distance between them: if d' denotes the Hamming distance, then for all $c_1, c_2 \in \Gamma$, the rank distance satisfies the inequality $d(c_1, c_2) \leq d'(c_1, c_2)$ [13]. Let $\gamma \in \Gamma'_\imath$ be a non-zero codeword, $\imath = 1, 2, \ldots, n$. By the very construction of $\Gamma'_\imath$, an arbitrary codeword $c \in \Gamma'_i$ can be written as the Kronecker product of $c_1 \in \Gamma_n$ and $c_2 \in \Gamma_\imath$. Consequently, the weight $w(\gamma)$ of a non-zero codeword $\gamma \in \Gamma'_i$ can be calculated as follows:

$$\begin{aligned} w(\gamma) &= w(\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n) \otimes (\beta_1,\ \beta_2,\ \ldots,\ \beta_n) \\ &= w(\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n) w(\beta_1,\ \beta_2,\ \ldots,\ \beta_n) \\ &= w(\alpha) w(\beta) \\ &\geq d_n d_\imath \end{aligned}$$

for some non-zero codewords $\alpha \in \Gamma_n$ and $\beta \in \Gamma_i$. It follows that, the minimum distance of the i^{th} *constituent* code Γ'_i is $d_n d_\imath$. Thus we have the following proposition.

Proposition 5.1 If $G_\imath$ is the generator matrix of an (n, k_i, d_i) MRD code as defined above, then $G'_\imath = G_n \otimes G_\imath$ defines an $(n^2,\ k_n k_\imath,\ d_n d_\imath)$ code, for each $\imath = 1, 2, \ldots, n$.

Having obtained a set of n $(n^2, k_n k_\imath, d_n d_\imath)$ $GF(2^n)$-ary codes from *n-Direct* code $(\{n\}, \{k_\imath\}, \{d_\imath\})$ $(\Gamma_1, \Gamma_2, \ldots, \Gamma_n)$, our next step is to check to see if they constitute an $(\{n^2\}, \{k_n k_\imath\}, \{d_n d_\imath\})$ *n-Direct* code $(\Gamma'_1, \Gamma'_2, \ldots, \Gamma'_n)$. The following theorem affirms it positively.

Theorem 5.2 The $GF(2^n)$-ary codes $\Gamma'_1,\ \Gamma'_2, \ldots, \Gamma'_n$ generated by the respective generated matrices $G'_1,\ G'_2, \ldots, G'_n$ constitute an $(\{n^2\}, \{k_n k_\imath\}, \{d_n d_\imath\})$ *n-Direct* code.

Proof: For any $\imath$ and j:

$$\begin{aligned} G'_\imath G_j'^{\mathbf{T}} &= (G_n \otimes G_\imath)(G_n \otimes G_j)^{\mathbf{T}} \\ &= (G_n \otimes G_\imath)(G_n^{\mathbf{T}} \otimes G_j^{\mathbf{T}}) \\ &= (G_n G_n^{\mathbf{T}}) \otimes (G_\imath G_j^{\mathbf{T}}) \\ &= \begin{cases} \mathbf{I} & ,\ i = j \\ (\mathbf{0}) & ,\ i \neq j \end{cases} \quad \text{(by Theorem 2.5)} \end{aligned}$$

where $\mathbf{I}$ is the $k_n k_\imath \times k_n k_j$ identity matrix and $(\mathbf{0})$ is the $k_n k_\imath \times k_n k_j$ zero-matrix.

Thus the $GF(2^n)$-ary codes $\Gamma'_1, \Gamma'_2, \ldots, \Gamma'_n$ obtained thus in fact constitute an $(\{n^2\}, \{k_n k_\imath\}, \{d_n d_\imath\})$ *n-Direct* code $(\Gamma'_1, \Gamma'_2, \ldots, \Gamma'_n)$. Observe that, the distance construction increases the minimum distance of the *constituent* codes of the resultant $\mathcal{T}$*-Direct* code. Because of the increase in the minimum distance, we call the construction outlined as the *distance construction* and the matrix used is called the *distance matrix*.

Additionally, the *orthogonal projector* for the *n-Direct* code $(\Gamma'_1, \Gamma'_2, \ldots, \Gamma'_n)$ is given by $\Pi_{\Gamma'_i} = (G_n^{\mathbf{T}} G_n) \otimes (G_i^{\mathbf{T}} G_i)$, which is a mapping from $\Lambda' = \Gamma'_1 \oplus \Gamma'_2 \oplus \cdots \oplus \Gamma'_n$ onto Γ'_i for each $i = 1, 2, \ldots, n$.

Observe that, in the *distance* construction outlined above, Kronecker product of generator matrices of the *constituent* codes are considered. And yet another Kronecker product construction of codes can also be found in [27], wherein the Kronecker product of parity-check matrices of conventional codes were considered. Though the usages of Kronecker product look similar, the construction procedures adopted are totally different.

Example 5.3 Consider the $(\{3\}, \{1, 2\}, \{3, 2\})$ 2*-Direct* code (Γ_1, Γ_2) along with the generator matrices of the *constituent* codes:

$$\begin{aligned} G_1 &= \begin{bmatrix} \alpha^3 & \alpha^6 & \alpha^5 \end{bmatrix} \\ G_2 &= \begin{bmatrix} \alpha^6 & \alpha^5 & \alpha^3 \\ \alpha^5 & \alpha^3 & \alpha^6 \end{bmatrix} \end{aligned}$$

Then the generator matrices G'_1, G'_2 can be obtained by taking Kronecker product of G_2 with each of G_1 and G_2.

$$\begin{aligned} & G'_1 \\ = \;& G_2 \otimes G_1 \\ = \;& \begin{bmatrix} \alpha^2 & \alpha^5 & \alpha^4 & \alpha & \alpha^4 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha \\ \alpha & \alpha^4 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha & \alpha^2 & \alpha^5 & \alpha^4 \end{bmatrix} \end{aligned}$$

$$\begin{aligned} & G'_2 \\ = \;& G_2 \otimes G_2 \\ = \;& \begin{bmatrix} \alpha^5 & \alpha^4 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha & \alpha^2 & \alpha & \alpha^6 \\ \alpha^4 & \alpha^2 & \alpha^5 & \alpha^3 & \alpha & \alpha^4 & \alpha & \alpha^6 & \alpha^2 \\ \alpha^4 & \alpha^3 & \alpha & \alpha^2 & \alpha & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^2 \\ \alpha^3 & \alpha & \alpha^4 & \alpha & \alpha^6 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha^5 \end{bmatrix} \end{aligned}$$

Clearly, G'_1 and G'_2 define $(9, 2, 6)$ and $(9, 4, 4)$ codes, respectively. It is easy to verify that the codes Γ'_1, Γ'_2 obtained indeed constitute a $(\{9\}, \{2, 4\}, \{6, 4\})$ 2*-Direct* code $(\Gamma'_1,\ \Gamma'_2)$.

Thus, the proposed *distance* construction allows *constituent* codes of a $\mathcal{T}$*-Direct* code to have higher minimum distance, but at the cost of increased code length for each *constituent* code. The next section attempts to extend a $\mathcal{T}$*-Direct* code to include more *constituent* codes, thereby increasing the number of users that can be supported by a conventional $\mathcal{T}$*-Direct* code.

VI. $\left[\frac{n(n+1)}{2}\right]$-*Direct* codes in $GF(2^n)$

The number of users that can be assigned a (*constituent*) code in case of a $\mathcal{T}$*-Direct* code, defined over $GF(2^n)$, is at most n; i.e., $\mathcal{T} \leq n$. In what follows, a coding procedure based on distance construction that constructs a $\mathcal{T}$*-Direct* code which can assign *constituent* codes to more than n users is presented.

Consider an $(\{n\},\{1\},\{n\})$ n-*Direct* code $(\Gamma_1,\Gamma_2,\ldots,\Gamma_n)$ along with the generator matrices of the *constituent* codes:

$$\begin{aligned} G_1 &= \left[\begin{array}{cccc} \alpha_1^{[1]} & \alpha_2^{[1]} & \cdots & \alpha_n^{[1]} \end{array}\right] \\ G_2 &= \left[\begin{array}{cccc} \alpha_1^{[2]} & \alpha_2^{[2]} & \cdots & \alpha_n^{[2]} \end{array}\right] \\ &\vdots \\ G_n &= \left[\begin{array}{cccc} \alpha_1^{[n]} & \alpha_2^{[n]} & \cdots & \alpha_n^{[n]} \end{array}\right] \end{aligned}$$

where $\alpha_1,\alpha_2,\ldots,\alpha_n$ is a *trace-orthogonal basis* in $GF(2^n)$. Clearly, $(\Gamma_1,\Gamma_2,\ldots,\Gamma_t)$ is a t-*Direct* code for each $t = 2,3,\ldots,n$. Using G_n as the distance matrix, employ the *distance* construction on $(\Gamma_1,\Gamma_2,\ldots,\Gamma_{n-1})$:

$$\begin{aligned} \mathcal{A}_1 &= G_n \otimes G_1 \\ \mathcal{A}_2 &= G_n \otimes G_2 \\ &\vdots \\ \mathcal{A}_{n-1} &= G_n \otimes G_{n-1} \end{aligned}$$

Clearly, $\mathcal{A}_i$ defines an $(n^2,1,n^2)$ $GF(2^n)$-ary code, say, $\Gamma'_\imath$ for each $\imath = 1,2,\ldots,n-1$. Further, the construction procedure attempts to define a set of n more $GF(2^n)$-ary codes of same length, as follows.

$$\begin{aligned} \text{Define}\quad \mathcal{B}_1 &= G_1 \otimes G_1 \\ \mathcal{B}_2 &= G_2 \otimes G_2 \\ &\vdots \\ \mathcal{B}_n &= G_n \otimes G_n \end{aligned}$$

Clearly, $\mathcal{B}_i$ $(i = 1,2,\ldots,n)$ defines an $(n^2,1,n^2)$ $GF(2^n)$-ary code. Let Γ'_n, Γ'_{n+1}, …, Γ'_{2n-1} denote the codes generated by $\mathcal{B}_1,\mathcal{B}_2,\ldots,\mathcal{B}_n$, respectively. It remains now to show that the codes Γ'_1, Γ'_2, …, Γ'_{n-1} together with Γ'_n, Γ'_{n+1}, …, Γ'_{2n-1} constitute an $(\{n^2\},\{1\},\{n^2\})$ $(2n-1)$-*Direct* code $(\Gamma'_1,\Gamma'_2,\ldots,\Gamma'_{2n-1})$.

Theorem 6.1 The *constituent* codes Γ'_1, $\Gamma'_2,\ldots,\Gamma'_{2n-1}$ defined by the respective generator matrices $\mathcal{A}_1,\mathcal{A}_2,\ldots,\mathcal{A}_{n-1},\mathcal{B}_1,\mathcal{B}_2,\ldots,\mathcal{B}_n$ constitute an $(\{n^2\},$ $\{1\},\{n^2\})$ $(2n-1)$-*Direct* code.

Proof: For each $\imath = 1,2,\ldots,n-1$:

$$\begin{aligned} \mathcal{A}_\imath\mathcal{A}_i{}^{\mathbf{T}} &= (G_n \otimes G_\imath)(G_n \otimes G_i)^{\mathbf{T}} \\ &= \mathbf{I} \end{aligned}$$

where $\mathbf{I}$ is the $k_nk_i \times k_nk_i$ identity matrix.

For each $j = 1,2,\ldots,n$:

$$\begin{aligned} \mathcal{B}_j\mathcal{B}_j{}^{\mathbf{T}} &= (G_j \otimes G_j)(G_j \otimes G_j)^{\mathbf{T}} \\ &= \mathbf{I} \end{aligned}$$

where $\mathbf{I}$ is the $k_jk_j \times k_jk_j$ identity matrix.

For each $\imath = 1,2,\ldots,n-1$ and $j = 1,2,\ldots,n$:

$$\begin{aligned} \mathcal{A}_\imath\mathcal{B}_j^{\mathbf{T}} &= (G_n \otimes G_\imath)(G_j \otimes G_j)^{\mathbf{T}} \\ &= (G_n \otimes G_\imath)(G_j^{\mathbf{T}} \otimes G_j^{\mathbf{T}}) \\ &= (G_nG_j^{\mathbf{T}}) \otimes (G_\imath G_j^{\mathbf{T}}) \\ &= (\mathbf{0}) \end{aligned}$$

where $(\mathbf{0})$ is the $k_nk_\imath \times k_jk_j$ zero-matrix.

An example is given below to facilitate the construction procedure described above.

Example 6.2 Consider an $(\{3\},\{1\},\{3\})$ 3-*Direct* code $(\Gamma_1,\Gamma_2,\Gamma_3)$ along with the generator matrices of the *constituent* codes:

$$\begin{aligned} G_1 &= \left[\begin{array}{ccc} \alpha^3 & \alpha^6 & \alpha^5 \end{array}\right] \\ G_2 &= \left[\begin{array}{ccc} \alpha^6 & \alpha^5 & \alpha^3 \end{array}\right] \\ G_3 &= \left[\begin{array}{ccc} \alpha^5 & \alpha^3 & \alpha^6 \end{array}\right] \end{aligned}$$

Using G_3 as the distance matrix, employ the *distance* construction on $(\Gamma_1,\ \Gamma_2)$:

$$\begin{aligned} \mathcal{A}_1 &= G_3 \otimes G_1 \\ &= \left[\begin{array}{ccccccccc} \alpha & \alpha^4 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha & \alpha^2 & \alpha^5 & \alpha^4 \end{array}\right] \\ \mathcal{A}_2 &= G_3 \otimes G_2 \\ &= \left[\begin{array}{ccccccccc} \alpha^4 & \alpha^3 & \alpha & \alpha^2 & \alpha & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^2 \end{array}\right] \end{aligned}$$

Clearly, $\mathcal{A}_i$ defines a $(9,1,9)$ $GF(2^3)$-ary code, say, $\Gamma'_\imath$ for each $\imath = 1,2$. Further, the construction procedure attempts to define a set of 3 more $GF(2^3)$-ary *constituent* codes of same length, as follows.

$$\begin{aligned} \mathcal{B}_1 &= G_1 \otimes G_1 \\ &= \left[\begin{array}{ccccccccc} \alpha^6 & \alpha^2 & \alpha & \alpha^2 & \alpha^5 & \alpha^4 & \alpha & \alpha^4 & \alpha^3 \end{array}\right] \\ \mathcal{B}_2 &= G_2 \otimes G_2 \\ &= \left[\begin{array}{ccccccccc} \alpha^5 & \alpha^4 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha & \alpha^2 & \alpha & \alpha^6 \end{array}\right] \\ \mathcal{B}_3 &= G_3 \otimes G_3 \\ &= \left[\begin{array}{ccccccccc} \alpha^3 & \alpha & \alpha^4 & \alpha & \alpha^6 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha^5 \end{array}\right] \end{aligned}$$

Let Γ'_3, Γ'_4, Γ'_5 denote the codes generated by $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$, respectively. It is straightforward to verify that the codes $\Gamma'_1,\Gamma'_2,\Gamma'_3,\Gamma'_4,\Gamma'_5$ thus obtained indeed constitute a $(\{9\},\{1\},\{9\})$ 5-*Direct* code $(\Gamma'_1,\Gamma'_2,\Gamma'_3,\Gamma'_4,\Gamma'_5)$. Note that, the proposed construction increased the number of users from 3 to 5.

We can further generalize the above result in the following way using the same set of generator matrices $G_1,G_2,\ldots,G_n$ as defined above. For each $j = 1,2,\ldots,n-1$, using G_j as the *distance* matrix, define $j-1$ generator matrices as follows:

$$\begin{aligned} \mathcal{G}_1^{(j)} &= G_{j+1} \otimes G_1 \\ \mathcal{G}_2^{(j)} &= G_{j+1} \otimes G_2 \\ &\vdots \\ \mathcal{G}_j^{(j)} &= G_{j+1} \otimes G_j \end{aligned}$$

For each $j = 1,2,\ldots,n-1$ and $\imath = 1,2,\ldots,j$, let $\Gamma_\imath^{(j)}$ denote the $(n^2,1,n^2)$ $GF(2^n)$-ary code defined by the generator matrix $\mathcal{G}_\imath^{(j)} = G_{j+1} \otimes G_\imath$. Further, consider the Kronecker product of $G_\imath$ with itself for each $\imath = 1,2,\ldots,n$:

$$\begin{aligned} \mathcal{G}_1^{(n)} &= G_1 \otimes G_1 \\ \mathcal{G}_2^{(n)} &= G_2 \otimes G_2 \\ &\vdots \\ \mathcal{G}_n^{(n)} &= G_n \otimes G_n \end{aligned}$$

Denote by $\Gamma_\imath^{(n)}$, the $(n^2, 1, n^2)$ code generated by $\mathcal{G}_\imath^{(n)} = G_\imath \otimes G_\imath, \imath = 1, 2 \ldots, n$. It is easy to verify that the $\left\lceil \frac{n(n+1)}{2} \right\rceil$ codes $\Gamma_1^{(j)}, \Gamma_2^{(j)}, \ldots, \Gamma_j^{(j)}$ $(j = 1, 2, \ldots, n)$ thus obtained constitute an $(\{n^2\}, \{1\}, \{n^2\})$ $\left\lceil \frac{n(n+1)}{2} \right\rceil$-*Direct* code.

Clearly, the extended *distance* construction method for the class of $\mathcal{T}$-*Direct* codes defined over $GF(2^n)$ in fact increases the number of *constituent* codes and thus offers the benefit of allowing more users to the channel under consideration, where $n < \mathcal{T} \leq \frac{n(n+1)}{2}$.

VII. Conclusion

In this paper, a coding scheme for the *noisy* $\mathcal{T}$-user F-Adder Channel is described via a class of $\mathcal{T}$ Rank Distance codes that constitute a $\mathcal{T}$-*Direct* code. The coding scheme is accomplished by constructing a class of $\mathcal{T}$-*Direct* codes with *constituent* codes from the class of 2-cyclic MRD codes. The constructed class of $\mathcal{T}$-*Direct* 2-cyclic MRD codes are shown to be effective in coding for the *noisy* $\mathcal{T}$-user F-Adder Channel, in that they uniquely determine the transmitted codewords from the received *noisy* sequence. Further, a *distance* construction method for the class of $\mathcal{T}$-*Direct* codes is proposed. When employed on a $\mathcal{T}$-*Direct* code that is defined on $GF(2^n)$, the proposed *distance* construction method not only increases the minimum distance of the *constituent* codes, it also enables the resultant $\mathcal{T}$-*Direct* code to have at most $\frac{n(n+1)}{2}$ *constituent* codes, thereby allowing a greater number of users to participate in the channel.

References

[1] C. E. Shannon. Two-way communication channels. In *proceedings of* 4^{th} *Berkley Symposium on Mathematical Statistics and Probability*, 1, pp. 611-644, 1961.

[2] R. G. Gallager. *Information theory and reliable communication*, John Wiley and Sons Inc., New York, 1968.

[3] R. Ahlswede. Multi-way communication channels. In *proceedings of* 2^{nd} *International Symposium on Information Theory*, pp. 23-52, Tsahkadsor, Armenian, U.S.S.R., 1971.

[4] E. C. Van der Meulen. The discrete memoryless channel with two senders and one receiver. In *proceedings of* 2^{nd} *International Symposium on Information Theory*, pp. 103-135, Tsahkadsor, Armenian, U.S.S.R., 1971.

[5] H. Liao. A coding theorem for multiple access communications. *presented at the International Symposium on Information Theory*, Asilomar, 1972.

[6] R. Ahlswede. The capacity region of a channel with two senders and two receivers, *Annals of Probability*, 2(5), pp. 805-814, 1974.

[7] E. C. Van der Meulen. A survey of multi-way channels in information theory: 1961-1976, *IEEE Transactions on Information Theory*, 23(1) , pp. 1-37, 1977.

[8] A. Lempel. Matrix factorization over F_2 and trace-orthogonal bases of F_{2^n}, *SIAM Journal on Computations*, 4, pp. 175-186, 1975.

[9] T. Kasami and S. Lin. Coding for a multiple-access channel, *IEEE Transactions on Information Theory*, 22(2), pp. 129-137, 1976.

[10] S. C. Chang and E. J. Weldon. Coding for $\mathcal{T}$-user multiple access channels, *IEEE Transactions on Information Theory*, 25(6), pp. 684-691,1979.

[11] T. Kasami, S. Lin, S. Yamamura, and V. K. Wei. Graph theoretic approaches to the code construction for the two-user multiple-access binary adder channel, *IEEE Transactions on Information Theory*, 29, pp. 114-130, 1983.

[12] R. G. Gallager. A perspective on multiple access channels, *IEEE Transactions on Information Theory*, 31(2), pp. 124-142, 1985.

[13] E. M. Gabidulin. Theory of codes with maximum rank distance, *Problems in Information Transmission*, 21, pp. 1-12, 1985.

[14] J. H. Wilson. Error correcting codes for a $\mathcal{T}$-user binary adder channel, *IEEE Transactions on Information Theory*, 34(4), pp. 888-890, 1988.

[15] J. L. Massey. Linear codes with complementary duals, *Discrete Mathematics*, 106 and 107, pp. 337-342, 1992.

[16] R. Urbanke and B. Rimoldi. Coding for the F-Adder Channel: Two applications for Reed-Solomon codes. In *proceedings of IEEE International Symposium on Information Theory*, p. 85, San Antonio, 1993.

[17] B. Rimoldi. Coding for the Gaussian multiple access channel: An algebraic approach. In *proceedings of IEEE International Symposium on Information Theory*, p. 81, Austin, TX, 1993.

[18] W. B. Vasantha and R. S. Raja Durai. $\mathcal{T}$-*Direct* codes: An application to $\mathcal{T}$-user BAC. In *proceedings of IEEE Information Theory Workshop*, p. 214, Bangalore, India, 2002.

[19] W. B. Vasantha and R. S. Raja Durai. Some results on $\mathcal{T}$-*Direct* Codes. In *proceedings of* 3^{rd} *Asia-Europe Workshop on Information Theory*, pp. 43-44, Kamogawa, Chiba, Japan, 2003.

[20] R. S. Raja Durai. Distributed source coding using $\mathcal{T}$-*Direct* codes. In *proceedings of SympoTIC'06*, pp. 24-27, Bratislava, Slovakia, 2006.

[21] D. Silva and F. R. Kshischang. Using rank-metric codes for error correction in random network coding. In *proceedings of IEEE International Symposium on Information Theory*, pp. 796-800, Nice, France, 2007.

[22] R. Kotter and F. R. Kshischang. Coding for errors and erasures in random network coding, *IEEE Transactions on Information Theory*, 54(8), pp. 3579-3591, 2008.

[23] D. Silva, F. R. Kshischang, and R. Kotter. A rank-metric approach to error control in random network coding, *IEEE Transactions on Information Theory*, 54(9), pp. 3951-3967, 2008.

[24] D. Silva and F. R. Kshischang. On metrics for error correction in network coding, *IEEE Transactions on Information Theory*, 55(12), pp. 5479-5490, 2009.

[25] D. Silva, F. R. Kshischang, and R. Kotter. Communication over finite-field matrix channels, *IEEE Transactions on Information Theory*, 56(3), pp. 1296-1305, 2010.

[26] M. Gadouleau and Z. Yan. Constant-rank codes and their connection to constant-dimension codes, *IEEE Transactions on Information Theory*, 56(7), pp. 3207-3216, 2010.

[27] Josep Rifà and Victor A. Zinoviev. New completely regular q-ary codes based on Kronecker products, *IEEE Transactions on Information Theory*, 56(1), pp. 266-272, 2010.

[28] Norman A. Benjamin and Suresh Sankaranarayanan. Performance of wireless body sensor based mesh network for health application, *International Journal of Computer Information Systems and Industrial Management Applications*, 2, pp. 20-28, 2010.

[29] K. Maheswari and M. Punithavalli. Performance evaluation of packet loss replacement using repetititon technique in VoIP streams, *International Journal of Computer Information Systems and Industrial Management Applications*, 2, pp. 289-296, 2010.

[30] Antonia Wachter, Vladimir Sidorenko, Martin Bossert, and Victor Zyablov. On (partial) unit memory codes based on Gabidulin codes, *Problems of Information Transmission*, 47(2), pp. 117-129, 2011.

[31] R. S. Raja Durai and Meenakshi Devi. Construction of $(\mathcal{N}+\mathcal{M})$-*Direct* codes in $GF(2^{\mathcal{N}})$. In *proceedings of World Congress on Information and Communication Technologies (WICT'11)*, pp. 770-775, Mumbai, India, 2011.

[32] D. Silva and F. R. Kschischang. Universal secure network coding via rank-metric codes, *IEEE Transactions on Information Theory*, 57(2), pp. 1124-1135, 2011.

[33] Sung Hoon Lim, Young-Han Kim, Abbas El Gamal, and Sae-Young Chung. Noisy Network Coding, *IEEE Transactions on Information Theory*, 57(5), pp. 3132-3152, 2011.

[34] Shengtian Yang and Thomas Honold. Good Random Matrices Over Finite Fields, *Advances in Mathematics of Communications*, 23(4), pp. 605-635, 2012.

Author Biographies

R. S. RAJA DURAI was born in Thirunelveli district in the south of India on 14^{th} May 1975. He received his bachelor's and master's (IIT Madras) degrees in Mathematics in 1997 and 1999 respectively. In 2004, he completed his doctoral research on *Error-Control Coding theory*; guided by Dr. W. B. Vasantha at the Department of Mathematics, Indian Institute of Technology Madras. He has then carried out his first post-doctoral research on *sequence design for mobile and wireless communications* under the supervision of Prof. Naoki Suehiro at the University of Tsukuba, Japan. His second post-doc project was a research-cum-implementation work on *distributed video coding* with IRISA/INRIA, France. He is currently a faculty member in the Department of Mathematics, Jaypee University of Information Technology, India. He is primarily interested in the implementation of his research work to real channels.

Meenakshi Devi was born in Himachal Pradesh, India on 27^{th} February 1981. She received M.Sc. (Mathematics) degree in 2006 and M.Ed. in 2007, both from Himachal Pradesh University, Shimla, India. She worked as a lecturer in Shimla College of Education, Shimla during 2007-2008. At present, she is a faculty member of the Department of Mathematics, Bahra University, Solan, Himachal Pradesh, India. She is also pursuing her doctoral research at the Department of Mathematics, Jaypee University of Information Technology, India. Her research interests include information theory and algebraic coding theory.