Applicable Algebra in Engineering, Communication and Computing (2022) 33:117–134
https://doi.org/10.1007/s00200-020-00435-x

ORIGINAL PAPER

Multiple-rate error-correcting coding scheme

R. S. Raja Durai[1] · Meenakshi Devi[2] · Ashwini Kumar[1]

Received: 5 February 2019 / Revised: 22 April 2020 / Accepted: 25 April 2020 /
Published online: 2 June 2020

Abstract

Error-correcting codes that can effectively encode and decode messages of distinct lengths while maintaining a constant blocklength are considered. It is known conventionally that a k-dimensional block code of length n defined over $\mathtt{GF}(q^n)$ is designed to encode a k-symbol user data in to an n-length codeword, resulting in a fixed-rate coding. In contrast, considering $q = p^{\lambda}$, this paper proposes two coding procedures (for the cases of $\lambda = k$ and $\lambda = n$) each deriving a multiple-rate code from existing channel codes defined over a composite field $\mathtt{GF}(q^n)$. Formally, the proposed coding schemes employ λ codes $\mathcal{C}_1(\lambda, 1), \mathcal{C}_2(\lambda, 2), \ldots, \mathcal{C}_{\lambda}(\lambda, \lambda)$ defined over $\mathtt{GF}(q)$ to encode user messages of distinct lengths and incorporate variable-rate feature. Unlike traditional block codes, the derived multiple-rate codes of fixed blocklength n can be used to encode and decode user messages $\mathbf{m}$ of distinct lengths $|\mathbf{m}| = 1, 2, \ldots, k, k+1, \ldots, kn$, thereby supporting a range of information rates—inclusive of the code rates $1/n^2, 2/n^2, \ldots, k/n^2$ and $1/n, 2/n, \ldots, k/n$! A simple decoding procedure to the derived multiple-rate code is also given; in that, *orthogonal projectors* are employed for the identification of encoded user messages of variable length.

Keywords Multiple-rate · Error-correcting codes · Rank distance codes

Mathematics Subject Classification 94B05 · 94B35

✉ Meenakshi Devi
meenakshi.devi@spu.ac.za

R. S. Raja Durai
rsraja.durai@juit.ac.in

Ashwini Kumar
ashwinipatiyal@gmail.com

[1] Department of Mathematics, Jaypee University of Information Technology, Waknaghat 173234, India

[2] Department of Mathematical Sciences, Sol Plaatje University, Private Bag X5008, Kimberley, South Africa

1 Introduction

Let $\mathbb{F}_q = \mathtt{GF}(q)$ be a finite field with q elements, where q is a power of a prime p [1]. An error-correcting code $\mathcal{C}(n, k, d)$ defined over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ consisting of q^k q-ary codewords with the minimum Hamming distance being d. The information rate $\mathcal{R}$ of the code $\mathcal{C}$ which describes the efficiency with which information is transferred by a given coding scheme is usually defined as the ratio of $\log_q |\mathcal{C}|$ information symbols to the coded n symbols. Consider the composite field $\mathtt{GF}(q^n)$ defined over $\mathtt{GF}(q)$. The base field $\mathtt{GF}(q)$ over which the composite field is defined is called the ground field. The composite field $\mathtt{GF}(q^n)$ is in fact an extension field defined over the ground field $\mathtt{GF}(q)$.

A linear block code $\mathcal{C}(n, k)$ is conventionally designed to consider user messages of fixed k-symbol at a time and encode them into n symbols for transmission, which is in fact a fixed-rate coding. Under this conventional block coding, the information rate of the resultant code is being fixed at k/n. However, in the design of many practical error-control coding systems, the use of codes that can accommodate variable rates is desired. The *adaptive modulation* technique is used in wireless systems, where fading is very common, to achieve reliable and efficient communication [2]. Besides the *adaptive modulation* technique, *automatic repeat-request* protocol is also an integral part of modern wireless communication systems. These techniques require channel codes which are flexible with regard to code rate and blocklength. In such scenarios, use of error-correcting codes with all possible interest rates is more appropriate [3, 4]. Recently, constructions of codes supporting wide range of rates received more attention [5–12].

The present paper, motivated by the above-mentioned problem, attempts to construct two q^n-ary error-correcting codes which collectively lead to the encoding and decoding of q-ary user messages of lengths 1, 2, ⋯, kn, simultaneously, with a common encoder and decoder, where and here after $q = p^\lambda$ for some positive number λ. To facilitate this objective, this paper considers a p^λ-ary message-block, of user symbols, of length $\ell = \ell_1 + \ell_2 + \cdots + \ell_s \leq s\lambda$ with ℓ_i denoting the length of the ith segment of the message-block such that $1 \leq \ell_i \leq \lambda$, where $\lambda = \begin{cases} k\ , & \text{for } s = 1 \\ n\ , & \text{for } s = k \end{cases}$. To make variable-rate feature simpler, a code $\mathcal{C}(n, k, d)$ defined over the composite field $\mathtt{GF}((p^\lambda)^n)$ termed as 'mother' code, and codes $\mathcal{C}_1(\lambda, 1), \mathcal{C}_2(\lambda, 2), \ldots, \mathcal{C}_\lambda(\lambda, \lambda)$ defined over the ground field $\mathtt{GF}(p^\lambda)$ termed as 'children' codes are considered. Each message-segment of length ℓ_i is encoded using the child code $\mathcal{C}_{\ell_i}$ over $\mathtt{GF}(p^\lambda)$ to obtain an λ-length vector, and the resulting s encoded-message segments are further channel encoded by the mother code $\mathcal{C}$ defined over $\mathtt{GF}((p^\lambda)^n)$.

In sequel, employing the proposed coding procedures, the longer data symbols at the output of source encoder can be broken up flexibly in to blocks of s, and/or $s + 1, \ldots$, and/or $s\lambda p^\lambda$-ary symbols and then each block is encoded independently for transmission, which is in contrast to conventionally encoding messages of fixed block-size. Consequently, together with mother and children codes, the proposed coding schemes determine multiple-rate codes that support the following variable code rates:

$$\mathcal{R}_s = \frac{\log_{q^n} |\mathcal{C}_{\ell_1} \times \mathcal{C}_{\ell_2} \times \cdots \times \mathcal{C}_{\ell_s}|}{n} = \frac{s}{n^2}, \frac{s+1}{n^2}, \ldots, \frac{s\lambda}{n^2}$$

retaining the constant code length n and distance d, where $1 \leq \ell_i \leq \lambda$. The procedure (correspond to the case $\lambda = n$) outlined as above is in fact an extension to the multiple-rate coding procedure (for the case of $\lambda = k$) introduced by the author in an earlier paper [12], which is presented in Sect. 3 along with an illustrative example. The mother and children codes, respectively called inner and outer codes, considered in this paper are chosen from the class of rank distance codes introduced by Gabidulin in [13].

The rest of the paper is structured as follows. The following section reviews the basic definitions and preliminary results needed. The multiple-rate code construction that correspond to the case of $\lambda = k$ handling multiple-rates $1/n^2, 2/n^2, \ldots, k/n^2$ simultaneously is presented in Sect. 3; the coding procedure is demonstrated with an example given in Sect. 4. While the coding procedure for the case of $\lambda = k$ results in low coding rates, Sect. 5 describes an enhanced multiple-rate coding procedure (the case of $\lambda = n$) that supports wide range of information rates including the rates $1/n, 2/n, \ldots, k/n$; it is also provided with an associated decoding technique. Section 6 provides an example of a multiple-rate code construction in support of the coding procedure described in Sect. 5 and finally, the paper concludes in Sect. 7.

2 Preliminaries

This preliminary section briefly summarizes some fundamentals of the class of rank distance codes [13] and basic definitions concerning the dual bases [14] of interest to this paper.

2.1 Rank distance codes

Let $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in [\mathtt{GF}(q^N)]^n$, $n \leq N$. The rank norm $||\mathbf{a}||$ of $\mathbf{a}$ is defined as the maximum number of linearly independent coordinates over $\mathtt{GF}(q^N)$. The rank distance between two vectors $\mathbf{x}$ and $\mathbf{y}$ of $[\mathtt{GF}(q^N)]^n$ is the norm of the difference of these vectors $||\mathbf{x} - \mathbf{y}||$. The rank norm induces a metric called rank metric (or rank distance) on $[\mathtt{GF}(q^N)]^n$. The rank distance of a code is then defined as the minimal rank distance between the codewords. As opposed to the so-called Hamming metric [15], the rank metric considered to be an ideal metric as it acknowledges the linear dependency of the code symbols of the alphabet, especially when the symbols are from higher dimensional Galois field [16].

Equipped with the rank metric, the class of *rank distance* (RD) codes are defined as subsets of an n-dimensional space $[\mathtt{GF}(q^N)]^n$ of n-vectors over an extension field $\mathtt{GF}(q^N)$. Rank distance codes over finite field extensions were introduced in different representations under various frameworks [13, 16–18]. The rank distance codes have been well studied in terms of properties, bounds and decoding [19–21]. This paper considers a subclass of rank metric codes

introduced by Gabidulin in 1985 [13]; of particular interest are the codes (n, k, d) attaining equality in the Singleton-like bound $d \leq n - k + 1$ in rank metric, called *maximum rank distance* (MRD) codes.

Definition 2.1 An (n, k, d) MRD code is generated by the $k \times n$ matrix:

$$\mathbf{G} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix}$$

where $g_1, g_2, \ldots, g_n \in \mathtt{GF}(q^N)$ are linearly independent over $\mathtt{GF}(q)$. The paper considers the case when $n = N$.

2.2 Self-complementary bases

Consider two bases $\boldsymbol{\alpha} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $\boldsymbol{\beta} = \{\beta_1, \beta_2, \ldots, \beta_n\}$ of $\mathtt{GF}(q^n)$ over $\mathtt{GF}(q)$. They are called dual (or complementary) bases if $\mathbf{tr}(\alpha_i \beta_j) = \delta_{ij}$, where $\mathbf{tr}$ is the *trace* from $\mathtt{GF}(q^n)$ to $\mathtt{GF}(q)$ defined as $\mathbf{tr}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$ and $\delta_{i,j}$ $(1 \leq i, j \leq n)$ is kroneker delta function. A basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of $\mathtt{GF}(q^n)$ over $\mathtt{GF}(q)$ is called *self-dual* or *self-complementary* if

$$\mathbf{tr}(\alpha_i \alpha_j) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

A *self-complementary* basis exists in every extension $\mathtt{GF}(q^n)$ of $\mathtt{GF}(q)$ where q is even or both q and n are odd [22]. In this paper, *self-complementary* bases are used in defining generator and parity-check matrices of codes. A criteria for the existence of *self-complementary bases* is obtained in [23], where it has been established that $\mathtt{GF}(q^n)$ has a *self-complementary normal* basis if and only if n is odd or $n \equiv 2 \pmod 4$ and q is even.

Symbols, notations and nomenclature

- While this paper refers a q-ary linear code $\mathcal{C}$ defined over the field $\mathbb{F}_q = \mathtt{GF}(q)$ with the parameters n, k and d as $\mathcal{C}(n, k, d)_q$ or simply by $\mathcal{C}(n, k, d)$ throughout the article, the same is sometimes denoted by $\mathcal{C}(n, k)_q$ or simply $\mathcal{C}(n, k)$ when the code is not required to perform error correction.
- For arbitrary vectors $\mathbf{a} = (\mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_{\ell_1}) \in \mathbb{F}_q^{\ell_1}$ and $\mathbf{b} = (\mathrm{b}_1, \mathrm{b}_2, \ldots, \mathrm{b}_{\ell_2}) \in \mathbb{F}_q^{\ell_2}$, the concatenation of $\mathbf{a}$ and $\mathbf{b}$ is $(\mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_{\ell_1}, \mathrm{b}_1, \mathrm{b}_2, \ldots, \mathrm{b}_{\ell_2})$ of length $\ell_1 + \ell_2$ and abbreviated as $(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_q^{\ell_1} \times \mathbb{F}_q^{\ell_2}$.
- Let $\mathbf{c} = (c_1, c_2, \ldots, c_{\ell_3}) \in \mathbb{F}_q^{\ell_3}$ be arbitrary. It is known that $\mathbb{F}_{q^{\ell_3}}$ is isomorphic (as a vector space over $\mathbb{F}_q$) to the vector space $\mathbb{F}_q^{\ell_3}$. Consequently, the vector $(c_1, c_2, \ldots, c_{\ell_3}) \in \mathbb{F}_q^{\ell_3}$ can be considered as an element of $\mathbb{F}_{q^{\ell_3}}$. By abuse of notation, this paper uses the vector notation $\mathbf{c}$ also to represent the (isomorphic) element of $\mathbb{F}_{q^{\ell_3}}$ as an isomorphism $\mathbf{c} \leftrightarrow (c_1, c_2, \ldots, c_{\ell_3})$ where applicable.

3 Multiple-rate codes: Construction-I

Consider the composite field $\mathtt{GF}((p^k)^n)$ defined over the subfield $\mathtt{GF}(p^k)$, where k and n are such that $n > k > 1$. Let β be a root of an irreducible polynomial of degree n over $\mathtt{GF}(p^k)$. Then $\mathtt{GF}(q^n) = \{0, \beta, \beta^2, \ldots, \beta^{q^n-1}\}$, where $q = p^k$. In order to be able to perform field operations in the ground field $\mathtt{GF}(p^k)$, consider a primitive element α in $\mathtt{GF}(p^k)$ so that $\mathtt{GF}(p^k) = \{0, \alpha, \alpha^2, \ldots, \alpha^{p^k-1}\}$. Define the mother code $\mathcal{C}(n,\ k,\ d)$ over the composite field $\mathtt{GF}(q^n)$ with the following generator matrix:

$$\mathbf{G} = \begin{pmatrix} \beta_1 & \beta_2 & \cdots & \beta_n \\ \beta_1^q & \beta_2^q & \cdots & \beta_n^q \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{q^{k-1}} & \beta_2^{q^{k-1}} & \cdots & \beta_n^{q^{k-1}} \end{pmatrix}$$

where $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is some basis in $\mathtt{GF}(q^n)$. Clearly, the $k \times n$ matrix $\mathbf{G}$ defines an $\mathcal{C}(n,\ k,\ d)$ MRD code. Further, define k children codes $\mathcal{C}_i(k,\ i)$ over the ground field $\mathtt{GF}(p^k)$ with the generator matrix $\mathbf{G}_i$ $(i = 1, 2, \ldots, k)$:

$$\mathbf{G}_i = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ \alpha_1^p & \alpha_2^p & \cdots & \alpha_k^p \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{p^{i-1}} & \alpha_2^{p^{i-1}} & \cdots & \alpha_k^{p^{i-1}} \end{pmatrix}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_k$ is a *self-complementary basis* in $\mathtt{GF}(p^k)$. Clearly, each child code $\mathcal{C}_i(k,\ i)_{p^k}$ is an i-dimensional MRD code of length k. Note that, $\mathcal{C}_i \subseteq [\mathtt{GF}(p^k)]^k$ and $\mathcal{C}_i = [\mathtt{GF}(p^k)]^k$ when $i = k$.

The concept of a linear code $\mathcal{C}$ together with its *dual* $\mathcal{C}^\perp$ having trivial intersection $\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}$, called as *linear code with a complementary dual* (in short, LCD), was first introduced by Massey in [24]. In 2004 [25], it was discovered that certain class of MRD codes defined over $\mathtt{GF}(2^n)$ are LCD codes [26, 27]; more recently, the result is obtained for the case of MRD codes over $\mathtt{GF}(q^n)$: MRD codes generated by *self-complementary* basis in $\mathtt{GF}(q^n)$ are LCD codes [28]. Consequently, each MRD code $\mathcal{C}_i$ (child code) defined by $\mathbf{G}_i$ as above is an LCD code. These children codes are then associated with the linear mapping $\Pi_{\mathcal{C}_i} : [\mathtt{GF}(q)]^k \to \mathcal{C}_i$ given by $\Pi_{\mathcal{C}_i} = \mathbf{G}_i^{\mathbf{T}}(\mathbf{G}_i\mathbf{G}_i^{\mathbf{T}})^{-1}\mathbf{G}_i$. By the very notion of LCD codes, $\mathcal{C}_i$ is an LCD code just when $[\mathtt{GF}(q)]^n$ is the direct sum of $\mathcal{C}_i$ and $\mathcal{C}_i^\perp$: $[\mathtt{GF}(q)]^n = \mathcal{C}_i \oplus \mathcal{C}_i^\perp$. Further, a necessary and sufficient condition for a code $\mathcal{C}_i$ defined by $\mathbf{G}_i$ to be LCD is that $\mathbf{G}_i\mathbf{G}_i^{\mathbf{T}}$ is non-singular [24].

The *orthogonal projectors* associated with the children codes play a crucial role in the decoding of user messages of different length. The family of mother and children codes defined as above can be used to encode and decode user messages of length $i = 1, 2, \ldots, k$ - the encoding procedure [12] is presented in the following subsection for completeness.

3.1 Encoding

For $1 \leq \ell \leq k$, let $\mathbf{m}_\ell = (m_1, m_2, \ldots, m_\ell) \in [\mathtt{GF}(p^k)]^\ell$ be a message of length ℓ that is to be transmitted over the noisy q^n-ary channel. First encode the ℓ-length message $\mathbf{m}_\ell$ using the ℓth child code $\mathcal{C}_\ell(k,\ \ell)_{p^k}$ to obtain a k-length codeword, say $\mathbf{m}'_{\ell k} = (m'_{\ell 1}, m'_{\ell 2}, \ldots, m'_{\ell k})$. The *orthogonal projectors* will be used to recover $\mathbf{m}_\ell$ from $\mathbf{m}'_{\ell k} = \mathbf{m}_\ell \mathbf{G}_\ell$ on reception of error-free $\mathbf{m}'_{\ell k}$, which will be discussed shortly.

Let $\beta'_1, \beta'_2, \ldots, \beta'_k \in \mathtt{GF}(q^n)$ be distinctly chosen such that $\beta'_1, \beta'_2, \ldots, \beta'_k \notin \mathtt{GF}(p^k)$. Consider adding a k-length vector $(\beta'_\ell, \beta'_\ell, \ldots, \beta'_\ell) \in [\mathtt{GF}(q^n)]^k$ to the child codeword $\mathbf{m}'_{\ell k} \in [\mathtt{GF}(p^k)]^k$ associated to the message $\mathbf{m}_\ell$ - resulting in a k-length vector $\mathbf{m}''_{\ell k} \in [\mathtt{GF}(q^n)]^k$:

$$\mathbf{m}''_{\ell k} = \mathbf{m}'_{\ell k} + \underbrace{(\beta'_\ell, \beta'_\ell, \ldots, \beta'_\ell)}_{k \text{ components}}$$

The padding is done so that the coder can handle multiple rates simultaneously. Assume that the fixed k-length vector $(\beta'_\ell, \beta'_\ell, \ldots, \beta'_\ell)$ is known both at the encoder and decoder. Note that $\mathbf{m}'_{\ell k} \in \mathcal{C}_\ell(k,\ \ell)$ and $\mathbf{m}''_{\ell k} \notin \mathcal{C}_\ell(k,\ \ell)$; that is, $\mathbf{m}''_{\ell k} \in [\mathtt{GF}(q^n)]^k$. Finally, the q^n-ary k-length vector $\mathbf{m}''_{\ell k}$ is further encoded by the mother code $\mathcal{C}(n,\ k,\ d)$ through $\mathbf{G}$ to obtain an n-length codeword $\mathbf{c}$ for transmission.

In summary, the information symbols of distinct lengths are subsequently channel encoded by the respective child code and the mother code. Consequently, the derived multiple-rate code, denoted by $\mathcal{C}^{(1)}_{MR}(n, \{1, 2, \ldots, k\}_q, d)_{q^n}$, supports the rates $\mathcal{R}_1 = \frac{\log_{q^n} |\mathcal{C}_\ell|}{n}$, $\ell = 1, 2, \ldots, k$; $(1/n^2 \leq \mathcal{R}_1 \leq k/n^2)$. In this way, the mother code is designed along with the children codes to support multiple rates.

4 Example—Coding for $\mathcal{C}^{(1)}_{MR}(5, \{1, 2, 3\}_8, 3)_{8^5}$

Take $n = 5$, $k = 3$, and $q = 2^3$. Let α be a primitive element in $\mathtt{GF}(2^3)$ satisfying $\alpha^3 + \alpha + 1 = 0$. Consider $\mathtt{GF}(8^5) = \{0, \beta, \beta^2, \ldots, \beta^{8^5-1}\}$, where $\beta \in \mathtt{GF}(8^5)$ is a root of the primitive polynomial $x^5 + x^2 + x + \alpha^3$ over $\mathtt{GF}(8)$.

$$\text{Define } \mathbf{G} = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 \\ 1 & \beta^8 & \beta^{16} & \beta^{24} & \beta^{32} \\ 1 & \beta^{16} & \beta^{32} & \beta^{48} & \beta^{64} \end{bmatrix}$$

where β is a primitive element in $\mathtt{GF}(8^5)$. The generator matrix $\mathbf{G}$ generates the 'mother' MRD code $\mathcal{C}(5, 3, 3)_{8^5}$. The 'children' MRD codes $\mathcal{C}_1(3,\ 1)_{2^3}$, $\mathcal{C}_2(3,\ 2)_{2^3}$ and $\mathcal{C}_3(3,\ 3)_{2^3}$ defined respectively by the generator matrices $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_3$ along with their associated *orthogonal projectors* are below:

$$\mathbf{G}_1 = \begin{bmatrix} \alpha^3 & \alpha^6 & \alpha^5 \end{bmatrix}; \quad \Pi_{\mathcal{C}_1} = \begin{bmatrix} \alpha^6 & \alpha^2 & \alpha \\ \alpha^2 & \alpha^5 & \alpha^4 \\ \alpha & \alpha^4 & \alpha^3 \end{bmatrix}$$

$$\mathbf{G}_2 = \begin{bmatrix} \alpha^3 & \alpha^6 & \alpha^5 \\ \alpha^6 & \alpha^5 & \alpha^3 \end{bmatrix}; \quad \Pi_{\mathcal{C}_2} = \begin{bmatrix} \alpha & \alpha & \alpha^4 \\ \alpha & \alpha^2 & \alpha^2 \\ \alpha^4 & \alpha^2 & \alpha^4 \end{bmatrix}$$

$$\text{and } \mathbf{G}_3 = \begin{bmatrix} \alpha^3 & \alpha^6 & \alpha^5 \\ \alpha^6 & \alpha^5 & \alpha^3 \\ \alpha^5 & \alpha^3 & \alpha^6 \end{bmatrix}; \quad \Pi_{\mathcal{C}_3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The parity-check matrix $\mathbf{H}_i$ associated with the generator matrix $\mathbf{G}_i$ and the *orthogonal projector* $\Pi_{\mathcal{C}_i^\perp}$ of the dual code $\mathcal{C}_i^\perp$ $(i = 1, 2, 3)$ are obtained as

$$\mathbf{H}_1 = \begin{bmatrix} \alpha^6 & \alpha^5 & \alpha^3 \\ \alpha^5 & \alpha^3 & \alpha^6 \end{bmatrix}; \quad \Pi_{\mathcal{C}_1^\perp} = \begin{bmatrix} \alpha^2 & \alpha^2 & \alpha \\ \alpha^2 & \alpha^4 & \alpha^4 \\ \alpha & \alpha^4 & \alpha \end{bmatrix}$$

$$\mathbf{H}_2 = \begin{bmatrix} \alpha^5 & \alpha^3 & \alpha^6 \end{bmatrix}; \quad \Pi_{\mathcal{C}_2^\perp} = \begin{bmatrix} \alpha^3 & \alpha & \alpha^4 \\ \alpha & \alpha^6 & \alpha^2 \\ \alpha^4 & \alpha^2 & \alpha^5 \end{bmatrix}$$

$$\text{and } \mathbf{H}_3 = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}; \quad \Pi_{\mathcal{C}_3^\perp} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Take $\beta_1' = \beta$, $\beta_2' = \beta^2$, and $\beta_3' = \beta^3$ for instance. Since $k = 3$, we have $1 \le \ell \le 3$ so that message $\mathbf{m} = (\mathbf{m}_{1\ell}) \in [\mathrm{GF}(q)]^\ell$ of length $\ell = 1$ or 2 or 3 can be encoded for transmission over the 8^5-ary channel.

(a) For $\ell = 1$: consider $\mathbf{m} = (\mathbf{m}_{11}) = (\alpha)$. The q-ary message $\mathbf{m}_{11}$ is encoded by the child code $\mathcal{C}_1(3,\ 1)_{2^3}$ and $\mathbf{m}'_{13}$ is obtained as follows:

$$\mathbf{m}\mathbf{G}_1 = (\alpha)\mathbf{G}_1 = \begin{pmatrix} \alpha^4, & 1, & \alpha^6 \end{pmatrix} \leftrightarrow \mathbf{m}'_{13}$$

By adding $\begin{pmatrix} \beta_1', & \beta_1', & \beta_1' \end{pmatrix}$, $\mathbf{m}''_{13} = \mathbf{m}'_{13} + \begin{pmatrix} \beta_1', & \beta_1', & \beta_1' \end{pmatrix} = \begin{pmatrix} \alpha^4, & 1, & \alpha^6 \end{pmatrix} + \begin{pmatrix} \beta, & \beta, & \beta \end{pmatrix} = (\beta^{31491}, \beta^{32373}, \beta^{1493})$. Then the 8^5-ary message $\mathbf{m}'' = (\mathbf{m}''_{13}) = (\beta^{31491}, \beta^{32373}, \beta^{1493})$ is finally channel encoded with the mother code $\mathcal{C}(5, 3, 3)_{8^3}$ to obtain $\mathbf{c}$ (say): $\mathbf{c} = \mathbf{m}''\mathbf{G} = (\mathbf{m}''_{13})\mathbf{G} = (\beta^{25415}, \beta^{19646}, \beta^{7654}, \beta^{4579}, \beta^{17386})$.

(b) For $\ell = 2$: consider $\mathbf{m} = (\mathbf{m}_{12}) = (\alpha,\ 0)$. This time the child code $\mathcal{C}_2(3,\ 2)_{2^3}$ is used to encode $\mathbf{m}_{12}$. Consequently, $\mathbf{m}'_{13}$ is obtained as follows:

$$\mathbf{m}\mathbf{G}_2 = (\alpha,\ 0)\mathbf{G}_2 = \begin{pmatrix} \alpha^4, & 1, & \alpha^6 \end{pmatrix} \leftrightarrow \mathbf{m}'_{13}.$$

$$\mathbf{m}''_{13} = \mathbf{m}'_{13} + \begin{pmatrix} \beta_2', & \beta_2', & \beta_2' \end{pmatrix} = \begin{pmatrix} \alpha^4, & 1, & \alpha^6 \end{pmatrix} + \begin{pmatrix} \beta_2', & \beta_2', & \beta_2' \\ \beta^2, & \beta^2, & \beta^2 \end{pmatrix}$$

By adding

$= \left(\beta^{108}, \quad \beta^{31979}, \quad \beta^{12734} \right)$ which is encoded with $\mathcal{C}(5,3,3)_{8^3}$ to obtain $\mathbf{c} = \mathbf{m}''\mathbf{G} = (\mathbf{m}''_{13})\mathbf{G} = \left(\beta^{30215}, \quad \beta^{24825}, \quad \beta^{25147}, \quad \beta^{17463}, \quad \beta^{8804} \right)$.

(c) For $\ell = 3$: consider $\mathbf{m} = (\mathbf{m}_{13}) = \left(\alpha, \alpha^2, \alpha^3\right)$. The code $\mathcal{C}_3(3,\ 3)_{2^3}$ is used to encode $\mathbf{m}_{13}$ to obtain $\mathbf{m}'_{13}$:

$$\mathbf{m}\mathbf{G}_3 = \left(\alpha, \alpha^2, \alpha^3\right)\mathbf{G}_3 = \left(\alpha^4, \alpha^6, \alpha^4\right) \leftrightarrow \mathbf{m}'_{13}.$$

By adding $\left(\beta'_3, \quad \beta'_3, \quad \beta'_3 \right)$, $\mathbf{m}''_{13} = \mathbf{m}'_{13} + \left(\beta'_3, \quad \beta'_3, \quad \beta'_3 \right) = \left(\alpha^4, \alpha^6, \alpha^4\right) + \left(\beta^3, \quad \beta^3, \quad \beta^3 \right) = \left(\beta^{10094}, \beta^{31339}, \beta^{10094}\right)$ so that $\mathbf{m}'' = (\mathbf{m}''_{13})$ is encoded by $\mathcal{C}(5,3,3)_{8^5}$ as $\mathbf{c} = \mathbf{m}''\mathbf{G} = (\mathbf{m}''_{13})\mathbf{G} = \left(\beta^{31399}, \beta^{13222}, \beta^{10733}, \beta^{24757}, \beta^{23790}\right)$.

Remark 1 Observe that, in the above coding procedure, the p^k-ary information symbols of arbitrary blocklength (up to k) is subsequently channel encoded by the respective child code and the mother code. In doing so, the derived multiple-rate code $\mathcal{C}^{(1)}_{MR}$ restricts the message alphabets for the user information symbols of length $\ell \leq k$ to be from the 'smaller' ground field $\mathtt{GF}(p^k)$ rather than from the 'bigger' composite field $\mathtt{GF}((p^k)^n)$ - that is, $\mathbf{m}_\ell \in [\mathtt{GF}(p^k)]^\ell$ but $\mathbf{c} \in [\mathtt{GF}(q^n)]^n$. Although this turns out to be the reason for the lower information rates $1/n^2, 2/n^2, \ldots, k/n^2$, the coding procedure can be extended to attain a wide range of rates including the code rates $1/n, 2/n, \ldots, k/n$ as detailed in the following section. In that, the composite field $\mathtt{GF}(q^n)$ is considered over $\mathtt{GF}(p^n)$ instead of $\mathtt{GF}(p^k)$. Also, n children codes are used instead of k.

5 Multiple-rate codes: Construction-II

Considering the composite field $\mathtt{GF}((p^k)^n)$, the constructed multiple-rate code $\mathcal{C}^{(1)}_{MR}(n, \{1, 2, \ldots, k\}_q, d)_{q^n}$ supports the encoding of variable-length messages; though the coding scheme introduced enabled multiple-rate feature, the efficiency of the derived multiple-rate code is severely affected by having lower code rates $\mathcal{R}_1 = 1/n^2, 2/n^2, \ldots, k/n^2$—rates much lower than that of the mother and children codes involved. In contrast to this lower multiple code-rate support, this section presents an improvement of the coding scheme, in that, by considering the composite field $\mathtt{GF}((p^n)^n)$, it derives a multiple-rate code that not only handles the encoding and decoding of user messages of arbitrary lengths, also provides the support of higher code rates $\mathcal{R}_k = k/n^2, (k+1)/n^2, \ldots, kn/n^2$ up to the fixed rates supported by the mother and children codes, where k is the dimension of the mother code in both the coding schemes.

Consider the code $\mathcal{C}(n,\ k,\ d)$ defined over the composite field $\mathtt{GF}(q^n)$ with $q = p^n$, where k and n are such that $n \geq k \geq 1$. Let β be a root of a primitive polynomial of degree n over $\mathtt{GF}(q)$. Clearly, $\mathtt{GF}(q^n) = \{0, \beta, \beta^2, \ldots, \beta^{q^n-1}\}$. Let α be a primitive element in $\mathtt{GF}(q)$ so that $\mathtt{GF}(q) = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$. Further, in order to manage variable-length encoding of user messages, consider defining n children codes $\mathcal{C}_i(n,\ i)$ for $i = 1, 2, \ldots, n$ over the ground field $\mathtt{GF}(p^n)$ with the generator matrix $\mathbf{G}_i$:

$$\mathbf{G}_i = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^p & \alpha_2^p & \cdots & \alpha_n^p \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{p^{i-1}} & \alpha_2^{p^{i-1}} & \cdots & \alpha_n^{p^{i-1}} \end{pmatrix}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a *self-complementary basis* in $\mathtt{GF}(p^n)$. In contrast to the previous construction, each child code $\mathcal{C}_i(n,\ i)_{p^n}$ is an i-dimensional MRD code of length n, rather than of length k. Further, $\mathcal{C}_i \subseteq [\mathtt{GF}(p^n)]^n$ and $\mathcal{C}_i = [\mathtt{GF}(p^n)]^n$ when $i = n$. Moreover, the child code $\mathcal{C}_i$ obtained by $\mathbf{G}_i$ is an LCD code [26, 27].

The nest of mother and children codes defined respectively over $\mathtt{GF}(q^n)$ and $\mathtt{GF}(p^n)$ as above can then be used to encode and decode p^n-ary user messages of lengths from k to kn simultaneously; the procedure is explained in the following subsections. The *orthogonal projectors* associated with the children (LCD) codes play a crucial role in the decoding of encoded user messages of variable lengths.

5.1 Encoding

For $1 \leq \ell_1, \ell_2, \ldots, \ell_k \leq n$, consider $\mathbf{m} = (\mathbf{m}_{1\ell_1}, \mathbf{m}_{2\ell_2}, \ldots, \mathbf{m}_{k\ell_k}) \in [\mathtt{GF}(q)]^{\ell_1} \times [\mathtt{GF}(q)]^{\ell_2} \times \cdots \times [\mathtt{GF}(q)]^{\ell_k}$ as the actual p^n-ary message-block of length $\ell = \ell_1 + \ell_2 + \cdots + \ell_k$, that is to be transmitted over the noisy q^n-ary channel, where $\mathbf{m}_{i\ell_i} = (m_{i1}, m_{i2}, \ldots, m_{i\ell_i}) \in [\mathtt{GF}(q)]^{\ell_i}$ and $\ell = k, k+1, \ldots, kn$.

For each $i = 1, 2, \ldots, k$, encode the ith message-segment $\mathbf{m}_{i\ell_i}$ (of the user message-block $\mathbf{m}$) of length ℓ_i using the child code $\mathcal{C}_{\ell_i}(n,\ \ell_i)$ to obtain an n-length vector $\mathbf{m}'_{in}$ (say). Then, by considering a vector $(m'_{i1}, m'_{i2}, \ldots, m'_{in})$ in $[\mathtt{GF}(q)]^n$ also as a symbol element $\mathbf{m}'_{in}$ in $\mathtt{GF}(q^n)$, one obtains the k-length children-encoded vector-block $\mathbf{m}' = (\mathbf{m}'_{1n}, \mathbf{m}'_{2n}, \ldots, \mathbf{m}'_{kn}) \in [\mathtt{GF}(q^n)]^k$. The complementary-dual property of the children codes considered plays an important role in the decoding of user messages of different lengths; in that, the *orthogonal projectors* will be used to recover $\mathbf{m}_{i\ell_i}$ from $\mathbf{m}'_{in}$.

Further, in order for the coder to handle multiple rates efficiently, an element $\beta'_{\ell_i} \in \mathtt{GF}(q^n)$ is added to (the ith children encoded-segment) $\mathbf{m}'_{in} \in \mathtt{GF}(q^n)$ - resulting in an element $\mathbf{m}''_{in}$ of $\mathtt{GF}(q^n)$:

$$\begin{aligned} \mathbf{m}''_{1n} &= \mathbf{m}'_{1n} + \beta'_{\ell_1} \\ \mathbf{m}''_{2n} &= \mathbf{m}'_{2n} + \beta'_{\ell_2} \\ &\vdots \\ \text{and} \quad \mathbf{m}''_{kn} &= \mathbf{m}'_{kn} + \beta'_{\ell_k} \end{aligned}$$

where $\beta'_{\ell_i} \leftrightarrow \left(\alpha'_{\ell_i}, \alpha'_{\ell_i}, \ldots, \alpha'_{\ell_i}\right) \in [\mathtt{GF}(p^n)]^n$ and $\alpha'_1, \alpha'_2, \ldots, \alpha'_n \in \mathtt{GF}(p^n)$ are distinctly chosen such that $\alpha'_1, \alpha'_2, \ldots, \alpha'_n \notin \mathtt{GF}(p)$. Note that $\mathbf{m}'_{in} \leftrightarrow \mathbf{m}_{i\ell_i}\mathbf{G}_{\ell_i}$ and $\beta'_{\ell_i} \in \mathtt{GF}(q^n)$ is purposefully added to the $\mathbf{m}'_{in} \in \mathtt{GF}(q^n)$ that was previously encoded by the child code $\mathcal{C}_{\ell_i}(n,\ \ell_i)$; this padding of β'_{ℓ_i} to $\mathbf{m}'_{in}$ helps the decoder to identify the correct child code $\mathcal{C}_{\ell_i}(n,\ \ell_i)$ that is used for encoding. Observe that $\mathbf{m}'_{in} \leftrightarrow (m'_{i1}, m'_{i2}, \ldots, m'_{in}) \in \mathcal{C}_{\ell_i}(n,\ \ell_i)$ and $\mathbf{m}''_{in} = \mathbf{m}'_{in} + \beta'_{\ell_i} \leftrightarrow (m''_{i1}, m''_{i2}, \ldots, m''_{in}) \notin \mathcal{C}_{\ell_i}(n,\ \ell_i)$ except for $\ell_i = n$.

Let $\mathbf{m}'' = (\mathbf{m}''_{1n}, \mathbf{m}''_{2n}, \ldots, \mathbf{m}''_{kn})$. Clearly, $\mathbf{m}'' \in [\mathtt{GF}(q^n)]^k$. Finally, the resultant k-length vector $\mathbf{m}''$ is channel encoded conventionally by the mother code $\mathcal{C}(n,\ k,\ d)$ through $\mathbf{G}$ to obtain an n-length q^n-ary codeword $\mathbf{c}$ for transmission. Assume that the fixed element β'_{ℓ_i} is known both at the encoder and decoder.

The improved multiple-rate encoding procedure presented above comprised of $n+1$ codes - a mother code over the 'bigger' composite field and n children codes over the 'smaller' ground field. The coding scheme is depicted via the block diagram as shown in Fig. 1. The diagram depicts the typical sequential components of the proposed coding scheme. The coding procedure actually consists of inner- and outer- encodings that can be described by three mappings as discussed below. Firstly, the outer-encoding is carried out by k (out of n children to operate on k blocks) children codes, which encode q-ary messages of length ℓ_i into codewords of length n; this results in k n-tuples over $\mathtt{GF}(q)$. This outer-encoding by the children codes is described by the mapping $\mathcal{E}_i : \left[\mathtt{GF}(q)\right]^{\ell_i} \rightarrow \mathcal{C}_{\ell_i}$ given by $\mathbf{m}_{i\ell_i} \mapsto \mathbf{m}'_{in}$. Noting that there is a one-to-one correspondence between the elements of the fields $[\mathtt{GF}(q)]^n$ and $\mathtt{GF}(q^n)$, n-tuples of $\mathcal{C}_{\ell_i} \subseteq [\mathtt{GF}(q)]^n$ are mapped as symbols of $\mathtt{GF}(q^n)$ through the bijection $\mathtt{g} : \left[\mathtt{GF}(q)\right]^{n^{\ell_i}} \rightarrow \mathtt{GF}(q^n)$. Finally, the inner encoder $\mathcal{C}$ channel encodes the respective coded-symbols of length k conventionally into a codeword of length n over $\mathtt{GF}(q^n)$ for transmission; this inner-encoding is specified by $\mathcal{E} : \mathcal{C}_{\ell_1} \times \mathcal{C}_{\ell_2} \times \cdots \times \mathcal{C}_{\ell_k} \rightarrow \mathcal{C}$ defined as $(\mathtt{g}(\mathbf{m}'_{1n}), \mathtt{g}(\mathbf{m}'_{2n}), \ldots, \mathtt{g}(\mathbf{m}'_{kn})) \mapsto \mathbf{c}$. Note that $\mathcal{C}_{\ell_i} \subseteq [\mathtt{GF}(q)]^n$ and $\mathcal{C} \subseteq [\mathtt{GF}(q^n)]^n$.

5.2 Decoding

Assume that an n-length vector $\mathbf{r} = \mathbf{c} + \mathbf{e}$ over $\mathtt{GF}(q^n)$ is received when $\mathbf{c} \in \mathcal{C}$ was transmitted. The receiver then employs the decoding technique of the mother code $\mathcal{C}(n,\ k,\ d)$ to $\mathbf{r}$ - decoding conventionally. As long as the rank of the error-vector $\mathbf{e}$ is less than or equal to $\lfloor \frac{d-1}{2} \rfloor$, the decoder outputs the k-length vector $\mathbf{m}''$ $= (\mathbf{m}''_{1n}, \mathbf{m}''_{2n}, \ldots, \mathbf{m}''_{kn})$. The problem now for the receiver is to recover the actual ℓ -length message $\mathbf{m}$ from the k-length vector $\mathbf{m}''$.

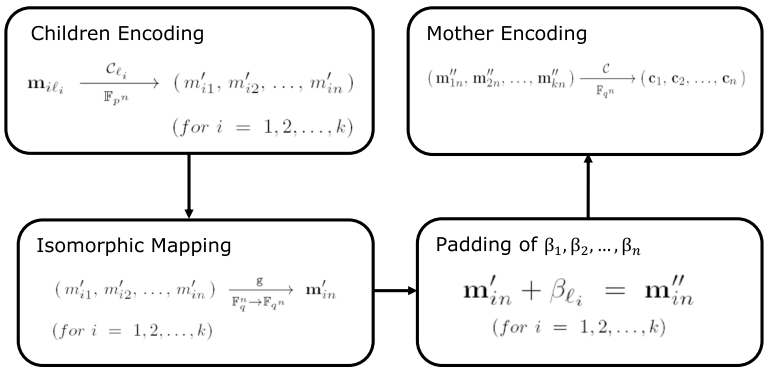

Fig. 1 Block diagram showing steps involved in the proposed multiple-rate coding scheme

Recall that $\mathbf{m}''_{in} = \mathbf{m}'_{in} + \beta'_{\ell_i}$ with $\mathbf{m}'_{in} \in \mathtt{GF}(q^n)$. The recovery of variable-length message-segments $\mathbf{m}_{1\ell_1}, \mathbf{m}_{2\ell_2}, \ldots, \mathbf{m}_{k\ell_k}$ is carried out in two stages: in the first stage, the fixed element β'_{ℓ_i} is identified (and hence the child code $\mathcal{C}_{\ell_i}$) to obtain $\mathbf{m}'_{in}$ from $\mathbf{m}''_{in}$; secondly, the receiver uses the *orthogonal projector* associated with the child code $\mathcal{C}_{\ell_i}$ to recover the ith message-segment $\mathbf{m}_{i\ell_i}$ from $\mathbf{m}'_{in}$ as detailed below.

For $\ell_i = 1, 2, \ldots, n-1$: (for fixed i)

$$\begin{aligned} (1) \quad \textbf{let} \quad & \mathbf{m}^{(0)}_{in} = \mathbf{m}''_{in} - \beta'_{\ell_i}. \\ (2) \quad \textbf{set} \quad & \mathbf{m}^{(1)}_{in} = \mathbf{m}^{(0)}_{in} \Pi_{\mathcal{C}_{\ell_i}}; \\ & \mathbf{m}^{(2)}_{in} = \mathbf{m}^{(0)}_{in} \Pi_{\mathcal{C}^{\perp}_{\ell_i}}, \end{aligned}$$

where $\mathbf{m}^{(0)}_{in} \leftrightarrow \mathbf{m}''_{in} - \beta'_{\ell_i}$. As long as $\mathbf{m}^{(1)}_{in} = \mathbf{m}^{(0)}_{in} \in \mathcal{C}_{\ell_i}$ and $\mathbf{m}^{(2)}_{in} = \mathbf{0}$ (an n-length zero-vector), upon decoding the n-length vector $\mathbf{m}^{(1)}_{in}$ by the child code $\mathcal{C}_{\ell_i}(n, \ell_i)$, the decoder outputs the actual message vector $\mathbf{m}_{i\ell_i}$ (this second decoding by the child code $\mathcal{C}_{\ell_i}$ can be avoided if $\mathbf{G}_{\ell_i}$ is in standard form). On the other hand, when the conditions are not met during the search till $\ell_i = n-1$, the length ℓ_i of the user message $\mathbf{m}_{i\ell_i}$ must be n in this case and $\mathbf{m}'_{in}$ should be $\mathbf{m}^{(0)}_{in} = \mathbf{m}''_{in} - \beta'_n$. The user message $\mathbf{m}_{i\ell_i}$ can then be retrieved from $\mathbf{m}'_{in}$ (this second decoding by the child code $\mathcal{C}_n$ can be avoided if $\mathbf{G}_n$ is in standard form). In this way, for each $i = 1, 2, \ldots, k$, the ith message-segment $\mathbf{m}_{i\ell_i}$ (of length ℓ_i) is recovered from the children-encoded message $\mathbf{m}'_{in}$ (of length n) to obtain the actual ℓ-length message-block $\mathbf{m} = (\mathbf{m}_{1\ell_1}, \mathbf{m}_{2\ell_2}, \ldots, \mathbf{m}_{k\ell_k}) \in [\mathtt{GF}(q)]^{\ell_1} \times [\mathtt{GF}(q)]^{\ell_2} \times \cdots \times [\mathtt{GF}(q)]^{\ell_k}$ transmitted.

In addition to the conventional decoding by the mother code, the associated decoding procedure presented employs *orthogonal projectors* in the recovery of k message-segments from the mother-decoded vector. Eventually, the mother code is designed along with the children codes to support multiple rates. Consequently, the derived code, termed as the multiple-rate MRD code and denoted by $\mathcal{C}^{(2)}_{MR}(n, \{k, k+1, \ldots, kn\}_q, d)_{q^n}$, facilitates transmission of user messages of arbitrary lengths ℓ over $\mathtt{GF}(q)$ at rates $\mathcal{R}_k = \frac{\log_{q^n} |\mathcal{C}^{(2)}_{MR}|}{n} = \frac{\log_{q^n}(q^\ell)}{n} = \frac{\log_q(q^\ell)}{n^2} = \frac{\ell}{n^2}$, where $\ell = \ell_1 + \ell_2 + \cdots + \ell_k$. Since $\ell = k, k+1, \ldots, n, n+1, \ldots, 2n, 2n+1, \ldots, kn$, we have $\mathcal{R}_k = \frac{k}{n^2}, \frac{k+1}{n^2}, \ldots, \frac{kn}{n^2}$.

By the very construction of the multiple-rate code $\mathcal{C}^{(2)}_{MR}$, its encoder can be described by the *systematic* encoding map: while a q^n-ary $\mathcal{C}(n, k, d)$-code is given by an injective map $\mathcal{E}' : \left[\mathtt{GF}(q^n)\right]^k \to \left[\mathtt{GF}(q^n)\right]^n$ from the q^n-ary symbols of length k to q^n-ary symbols of length n, the derived code $\mathcal{C}^{(2)}_{MR}$ has an associated encoding map $\mathcal{E}'' : \left[\mathtt{GF}(q)\right]^\ell \to \left[\mathtt{GF}(q^n)\right]^n$ from the q-ary strings of length ℓ to q^n-ary symbols of length n.

Unlike the traditional fixed-rate coding schemes, in the proposed coding scheme, the q-ary information symbols of arbitrary blocklength (from k to kn) is encoded twice in two stages—first by the respective child/outer code encoding in k segments and the subsequent encoding of the resultant k-length vector (over $\mathtt{GF}(q^n)$) followed by the mother/inner code—to allow room for multiple-rate transmission over the noisy channel. In that, as opposed to the fixed-rate codes, the proposed multiple-rate

code allows the message alphabets for the user information symbols of length ℓ to be from across the 'smaller' ground field $\mathtt{GF}(q)$ and the 'bigger' composite field $\mathtt{GF}(q^n)$. In a sense, the proposed coding procedure generalizes the conventional coding procedure of fixed k/n-rate coding and constructs codes operating at rates up to k/n. The mother code and n children (LCD) codes considered in this paper can be any linear error-correcting codes defined respectively over the composite field $\mathtt{GF}(q^n)$ and $\mathtt{GF}(q)$, not necessarily MRD codes—they are merely used to facilitate the presentation of the proposed multiple-rate coding procedure; however, the LCD-property for the children codes and the padding of distinct elements to the children-encoded vectors are essential for the proposed (multiple-rate) decoding strategy.

6 Example—Coding for $\mathcal{C}_{MR}^{(2)}(4, \{2, 3, 4, 5, 6, 7, 8\}_{16}, 3)_{16^4}$

Consider $q = 2^4$, $k = 2$, and $n = 4$. Let $\beta \in \mathtt{GF}(16^4)$ be a root of the primitive polynomial $x^4 + x^2 + \alpha x + \alpha^2$ over $\mathtt{GF}(16)$, where α is a primitive element in $\mathtt{GF}(2^4)$ satisfying $\alpha^4 + \alpha + 1 = 0$ [29]. Consider the 'mother' MRD code $\mathcal{C}(4, 2, 3)_{16^4}$ with the following generator matrix:

$$\mathbf{G} = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 \\ 1 & \beta^{16} & \beta^{32} & \beta^{48} \end{bmatrix}$$

where β is a primitive element in $\mathtt{GF}(16^4)$. Generator matrices for 'children' MRD codes $\mathcal{C}_1(4,\ 1)_{2^4}$, $\mathcal{C}_2(4,\ 2)_{2^4}$, $\mathcal{C}_3(4,\ 3)_{2^4}$ and $\mathcal{C}_4(4,\ 4)_{2^4}$ along with their associated *orthogonal projectors*:

$$\mathbf{G}_1 = \begin{bmatrix} \alpha^3 & \alpha^7 & \alpha^{12} & \alpha^{13} \end{bmatrix}; \quad \Pi_{\mathcal{C}_1} = \begin{bmatrix} \alpha^6 & \alpha^{10} & 1 & \alpha \\ \alpha^{10} & \alpha^{14} & \alpha^4 & \alpha^5 \\ 1 & \alpha^4 & \alpha^9 & \alpha^{10} \\ \alpha & \alpha^5 & \alpha^{10} & \alpha^{11} \end{bmatrix}$$

$$\mathbf{G}_2 = \begin{bmatrix} \alpha^3 & \alpha^7 & \alpha^{12} & \alpha^{13} \\ \alpha^6 & \alpha^{14} & \alpha^9 & \alpha^{11} \end{bmatrix}; \quad \Pi_{\mathcal{C}_2} = \begin{bmatrix} \alpha^4 & 1 & 0 & \alpha^5 \\ 1 & \alpha^2 & \alpha^5 & 1 \\ 0 & \alpha^5 & \alpha & 1 \\ \alpha^5 & 1 & 1 & \alpha^8 \end{bmatrix}$$

$$\mathbf{G}_3 = \begin{bmatrix} \alpha^3 & \alpha^7 & \alpha^{12} & \alpha^{13} \\ \alpha^6 & \alpha^{14} & \alpha^9 & \alpha^{11} \\ \alpha^{12} & \alpha^{13} & \alpha^3 & \alpha^7 \end{bmatrix}; \quad \Pi_{\mathcal{C}_3} = \begin{bmatrix} \alpha^{14} & \alpha^5 & 1 & \alpha^8 \\ \alpha^5 & \alpha^9 & \alpha^2 & \alpha^{10} \\ 1 & \alpha^2 & \alpha^{11} & \alpha^5 \\ \alpha^8 & \alpha^{10} & \alpha^5 & \alpha^6 \end{bmatrix}$$

and $$\mathbf{G}_4 = \begin{bmatrix} \alpha^3 & \alpha^7 & \alpha^{12} & \alpha^{13} \\ \alpha^6 & \alpha^{14} & \alpha^9 & \alpha^{11} \\ \alpha^{12} & \alpha^{13} & \alpha^3 & \alpha^7 \\ \alpha^9 & \alpha^{11} & \alpha^6 & \alpha^{14} \end{bmatrix}; \quad \Pi_{\mathcal{C}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Further, parity-check matrix $\mathbf{H}_i$ associated with the generator matrix $\mathbf{G}_i$ and *orthogonal projector* $\Pi_{\mathcal{C}_i^\perp}$ of the dual code $\mathcal{C}_i^\perp$ $(i = 1, 2, 3, 4)$ are given below:

$$\mathbf{H}_1 = \begin{bmatrix} \alpha^6 & \alpha^{14} & \alpha^9 & \alpha^{11} \\ \alpha^{12} & \alpha^{13} & \alpha^3 & \alpha^7 \\ \alpha^9 & \alpha^{11} & \alpha^6 & \alpha^{14} \end{bmatrix}; \quad \Pi_{\mathcal{C}_1^\perp} = \begin{bmatrix} \alpha^{13} & \alpha^{10} & 1 & \alpha \\ \alpha^{10} & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^4 & \alpha^7 & \alpha^{10} \\ \alpha & \alpha^5 & \alpha^{10} & \alpha^{12} \end{bmatrix}$$

$$\mathbf{H}_2 = \begin{bmatrix} \alpha^{12} & \alpha^{13} & \alpha^3 & \alpha^7 \\ \alpha^9 & \alpha^{11} & \alpha^6 & \alpha^{14} \end{bmatrix}; \quad \Pi_{\mathcal{C}_2^\perp} = \begin{bmatrix} \alpha & 1 & 0 & \alpha^5 \\ 1 & \alpha^8 & \alpha^5 & 1 \\ 0 & \alpha^5 & \alpha^4 & 1 \\ \alpha^5 & 1 & 1 & \alpha^2 \end{bmatrix}$$

$$\mathbf{H}_3 = \begin{bmatrix} \alpha^9 & \alpha^{11} & \alpha^6 & \alpha^{14} \end{bmatrix}; \quad \Pi_{\mathcal{C}_3^\perp} = \begin{bmatrix} \alpha^3 & \alpha^5 & 1 & \alpha^8 \\ \alpha^5 & \alpha^7 & \alpha^2 & \alpha^{10} \\ 1 & \alpha^2 & \alpha^{12} & \alpha^5 \\ \alpha^8 & \alpha^{10} & \alpha^5 & \alpha^{13} \end{bmatrix}$$

and $\mathbf{H}_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}; \quad \Pi_{\mathcal{C}_4^\perp} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$

Take $\beta_1' = \beta^{51362} \leftrightarrow (\alpha, \alpha, \alpha, \alpha)$, $\beta_2' = \beta^{25148} \leftrightarrow (\alpha^2, \alpha^2, \alpha^2, \alpha^2)$, $\beta_3' = \beta^{55731} \leftrightarrow (\alpha^3, \alpha^3, \alpha^3, \alpha^3)$, and $\beta_4' = \beta^{20779} \leftrightarrow (\alpha^4, \alpha^4, \alpha^4, \alpha^4)$ for instance. The proposed multi-rate coding procedure is demonstrated in the following subsections in several cases.

6.1 Encoding for $\mathcal{C}_{MR}^{(2)}(4, \{2, 3, 4, 5, 6, 7, 8\}_{16}, 3)_{16^4}$

Since $k = 2$, we have $1 \le \ell_1, \ell_2 \le 4$ so that message $\mathbf{m} = (\mathbf{m}_{1\ell_1}, \mathbf{m}_{2\ell_2}) \in [\mathrm{GF}(q)]^{\ell_1} \times [\mathrm{GF}(q)]^{\ell_2}$ of lengths ℓ_1 and $\ell_2 = 1$ or 2 or 3 or 4 can be encoded for transmission over the 16^4-ary channel.

(1) For $\ell_1 = \ell_2 = \ell$: consider $\mathbf{m} = (\mathbf{m}_{13}, \mathbf{m}_{23}) = ((\alpha, \alpha^2, \alpha^3), (1, \alpha, \alpha^2))$. The q-ary message $\mathbf{m}_{13}$ and $\mathbf{m}_{23}$ is encoded by the child code $\mathcal{C}_3(4, 3)_{2^4}$ and $\mathbf{m}_{14}', \mathbf{m}_{24}'$ is obtained as follows:

$$\mathbf{m}_{13}\mathbf{G}_3 = (\alpha, \alpha^2, \alpha^3)\mathbf{G}_3 = (\alpha^{10}, \alpha^8, \alpha^{12}, \alpha^4) \leftrightarrow \mathbf{m}_{14}'$$
$$\mathbf{m}_{23}\mathbf{G}_3 = (1, \alpha, \alpha^2)\mathbf{G}_3 = (\alpha^9, \alpha^7, \alpha^{11}, \alpha^3) \leftrightarrow \mathbf{m}_{24}'$$

which correspond to the elements β^{1853} and β^{32436} of $\mathrm{GF}(16^4)$. Thus $\mathbf{m}_{14}'' = \mathbf{m}_{14}' + \beta_3' = \beta^{1853} + \beta^{55731} = \beta^{61931}$ and $\mathbf{m}_{24}'' = \mathbf{m}_{24}' + \beta_3' = \beta^{32436} + \beta^{55731} = \beta^{26814}$. Then the q^n-ary message $\mathbf{m}'' = (\mathbf{m}_{14}'', \mathbf{m}_{24}'') = (\beta^{61931}, \beta^{26814})$ is finally channel encoded with mother code $\mathcal{C}(4, 2, 3)_{16^4}$ to obtain $\mathbf{c}_1$ (say):

$\mathbf{m}''\mathbf{G} = (\mathbf{m}''_{14},\ \mathbf{m}''_{24})\mathbf{G} = \left(\ \beta^{41174},\quad \beta^{34647},\quad \beta^{65220},\quad \beta^{7249}\ \right) = \mathbf{c}_1.$

(2) For $\ell_1 \neq \ell_2$: consider $\mathbf{m} = (\mathbf{m}_{13},\ \mathbf{m}_{22}) = \big((\alpha,\ \alpha^2,\ \alpha^3), (\ 1,\ \alpha^2)\big)$. This time the child code $\mathcal{C}_3(4,\ 3)_{2^4}$ and $\mathcal{C}_2(4,\ 2)_{2^4}$ are used to encode $\mathbf{m}_{13}$ and $\mathbf{m}_{22}$. Consequently, $\mathbf{m}'_{14}$ and $\mathbf{m}'_{24}$ are obtained as follows:

$$\mathbf{m}_{13}\mathbf{G}_3 = (\ \alpha,\ \alpha^2,\ \alpha^3)\mathbf{G}_3 = \left(\ \alpha^{10},\quad \alpha^8,\quad \alpha^{12},\quad \alpha^4\ \right) \leftrightarrow \mathbf{m}'_{14}$$
$$\mathbf{m}_{22}\mathbf{G}_2 = (\ 1,\ \alpha^2)\mathbf{G}_2 \qquad = \left(\ \alpha^4,\quad \alpha^9\quad \alpha^3\quad \alpha\ \right) \leftrightarrow \mathbf{m}'_{24}$$

Let $\mathbf{m}''_{14} = \mathbf{m}'_{14} + \beta'_3 = \beta^{1853} + \beta^{55731} = \beta^{61931}$ and $\mathbf{m}''_{24} = \mathbf{m}'_{24} + \beta'_2 = \beta^{28078} + \beta^{25148} = \beta^{41364}$. Thus

$$\mathbf{m}''\mathbf{G} = (\mathbf{m}''_{14},\ \mathbf{m}''_{24})\mathbf{G} = \left(\ \beta^{43269},\quad \beta^{31541},\quad \beta^{1865},\quad \beta^{61449}\ \right) = \mathbf{c}_2.$$

6.2 Decoding for $\mathcal{C}^{(2)}_{MR}(4, \{2, 3, 4, 5, 6, 7, 8\}_{16}, 3)_{16^4}$

By employing the mother code $\mathcal{C}(4, 2, 3)_{16^4}$, the transmitted codeword $\mathbf{c}_j$ (for fixed j) can be recovered from a received vector $\mathbf{r} = \mathbf{c}_j + \mathbf{e}$, as long as the error-vector $\mathbf{e}$ is of rank at most 1. After retrieving the transmitted codeword $\mathbf{c}_j$ and hence the message $\mathbf{m}''$, the receiver then employs the *orthogonal* projectors and recovers the actual user message $(\mathbf{m}_{1\ell_1}, \mathbf{m}_{2\ell_2})$ of length $\ell_1 + \ell_2$ from $\mathbf{m}''$ $(1 \leq \ell_1,\ \ell_2 \leq 4)$ as discussed below.

Case 1: Recovering $(\mathbf{m}_{13}, \mathbf{m}_{23})$ from $\mathbf{c}_1$:

(1) $\ell_1 = \ell_2 = 1$:

$$\mathbf{m}^{(0)}_{14} = \mathbf{m}''_{14} - \beta'_1 = \beta^{61931} - \beta^{51362} = \beta^{3857} \leftrightarrow \left(\ \alpha^{13},\quad \alpha^{12},\quad \alpha^8,\quad \alpha^{14}\ \right);$$
$$\mathbf{m}^{(1)}_{14} = \mathbf{m}^{(0)}_{14}\Pi_{\mathcal{C}_1} = \left(\ \alpha^6,\ \alpha^{10},\ 1,\ \alpha\right);$$
$$\mathbf{m}^{(2)}_{14} = \mathbf{m}^{(0)}_{14}\Pi_{\mathcal{C}_1^\perp} = \left(\ 1,\ \alpha^3,\ \alpha^2,\ \alpha^7\right), \text{ and}$$
$$\mathbf{m}^{(0)}_{24} = \mathbf{m}''_{24} - \beta'_1 = \beta^{26814} - \beta^{51362} = \beta^{49939} \leftrightarrow \left(\ 0,\quad 1,\quad \alpha^2,\quad \alpha\ \right);$$
$$\mathbf{m}^{(1)}_{24} = \mathbf{m}^{(0)}_{24}\Pi_{\mathcal{C}_1} = \left(\alpha^{10}, \alpha^{14}, \alpha^4, \alpha^5\right);$$
$$\mathbf{m}^{(2)}_{24} = \mathbf{m}^{(0)}_{24}\Pi_{\mathcal{C}_1^\perp} = \left(\alpha^{10}, \alpha^3, \alpha^{10}, \alpha^2\right).$$

As the conditions are not met for either $\ell_1 = 1$ or $\ell_2 = 1$, the decoder moves to the next step.

(2) $\ell_1 = \ell_2 = 2$:

$$\mathbf{m}_{14}^{(0)} = \mathbf{m}_{14}'' - \beta_2' = \beta^{61931} - \beta^{25148} = \beta^{21810} \leftrightarrow \left(\alpha^6, \alpha^{11}, \alpha^2, \alpha^3\right);$$
$$\mathbf{m}_{14}^{(1)} = \mathbf{m}_{14}^{(0)} \Pi_{\mathcal{C}_2} = \left(\alpha^6,\ \alpha,\ \alpha,\ \alpha^9\right);$$
$$\mathbf{m}_{14}^{(2)} = \mathbf{m}_{14}^{(0)} \Pi_{\mathcal{C}_2^\perp} = \left(0,\ \alpha^6,\ \alpha^5,\ \alpha\right), \text{ and}$$
$$\mathbf{m}_{24}^{(0)} = \mathbf{m}_{24}'' - \beta_2' = \beta^{26814} - \beta^{25148} = \beta^{8972} \leftrightarrow \left(1,\ 0,\ \alpha^8,\ \alpha^4\right);$$
$$\mathbf{m}_{24}^{(1)} = \mathbf{m}_{24}^{(0)} \Pi_{\mathcal{C}_2} = \left(\alpha^{14}, \alpha^{12},\ \alpha^{14}, \alpha^6\right);$$
$$\mathbf{m}_{24}^{(2)} = \mathbf{m}_{24}^{(0)} \Pi_{\mathcal{C}_2^\perp} = \left(\alpha^3,\ \alpha^{12},\ \alpha^6,\ \alpha^{12}\right).$$

Again, as the required conditions are not met for either $\ell_1 = 2$ or $\ell_2 = 2$, the decoder goes to the next step.

(3) $\ell_1 = \ell_2 = 3$:

$$\mathbf{m}_{14}^{(0)} = \mathbf{m}_{14}'' - \beta_3' = \beta^{61931} - \beta^{55731} = \beta^{1853} \leftrightarrow \left(\alpha^{10}, \alpha^8, \alpha^{12}, \alpha^4\right);$$
$$\mathbf{m}_{14}^{(1)} = \mathbf{m}_{14}^{(0)} \Pi_{\mathcal{C}_3} = \left(\alpha^{10},\ \alpha^8,\ \alpha^{12},\ \alpha^4\right);$$
$$\mathbf{m}_{14}^{(2)} = \mathbf{m}_{14}^{(0)} \Pi_{\mathcal{C}_3^\perp} = \left(0,\ 0,\ 0,\ 0\right), \text{ and}$$
$$\mathbf{m}_{24}^{(0)} = \mathbf{m}_{24}'' - \beta_3' = \beta^{26814} - \beta^{55731} = \beta^{32436} \leftrightarrow \left(\alpha^9, \alpha^7, \alpha^{11}, \alpha^3\right);$$
$$\mathbf{m}_{24}^{(1)} = \mathbf{m}_{24}^{(0)} \Pi_{\mathcal{C}_3} = \left(\alpha^9,\ \alpha^7,\ \alpha^{11},\ \alpha^3\right);$$
$$\mathbf{m}_{24}^{(2)} = \mathbf{m}_{24}^{(0)} \Pi_{\mathcal{C}_3^\perp} = \left(0,\ 0,\ 0,\ 0\right),$$

where $\beta^{1853} \leftrightarrow \left(\alpha^{10}, \alpha^8, \alpha^{12}, \alpha^4\right) = \mathbf{m}_{14}^{(0)}$ and $\beta^{32436} \leftrightarrow \left(\alpha^9, \alpha^7, \alpha^{11}, \alpha^3\right) = \mathbf{m}_{24}^{(0)}$. In this case, conditions are met at $\ell_1 = 3$ and $\ell_2 = 3$ so that the child code $\mathcal{C}_3(4,3)_{16}$ is used and $\mathbf{m} = \left((\alpha, \alpha^2, \alpha^3), (1, \alpha, \alpha^2)\right)$ is recovered from $(\mathbf{m}_{14}^{(1)}, \mathbf{m}_{24}^{(1)})$ and hence $\mathbf{m} = (\mathbf{m}_{13}, \mathbf{m}_{23}) = \left((\alpha, \alpha^2, \alpha^3), (1, \alpha, \alpha^2)\right)$.

Case 2: Recovering $(\mathbf{m}_{13}, \mathbf{m}_{22})$ from $\mathbf{c}_2$:

(1) $\ell_1 = \ell_2 = 1$:

$$\mathbf{m}_{14}^{(0)} = \mathbf{m}_{14}'' - \beta_1' = \beta^{61931} - \beta^{51362} = \beta^{3857} \leftrightarrow \left(\alpha^{13}, \alpha^{12}, \alpha^8, \alpha^{14}\right);$$
$$\mathbf{m}_{14}^{(1)} = \mathbf{m}_{14}^{(0)} \Pi_{\mathcal{C}_1} = \left(\alpha^6,\ \alpha^{10},\ 1,\ \alpha\right);$$
$$\mathbf{m}_{14}^{(2)} = \mathbf{m}_{14}^{(0)} \Pi_{\mathcal{C}_1^\perp} = \left(1,\ \alpha^3,\ \alpha^2,\ \alpha^7\right), \text{ and}$$
$$\mathbf{m}_{24}^{(0)} = \mathbf{m}_{24}'' - \beta_1' = \beta^{41364} - \beta^{51362} = \beta^{34121} \leftrightarrow \left(\alpha,\ \alpha^7,\ \alpha^{14},\ \alpha^4\right);$$
$$\mathbf{m}_{24}^{(1)} = \mathbf{m}_{24}^{(0)} \Pi_{\mathcal{C}_1} = \left(0,\ 0,\ 0,\ 0\right);$$
$$\mathbf{m}_{24}^{(2)} = \mathbf{m}_{24}^{(0)} \Pi_{\mathcal{C}_1^\perp} = \left(\alpha,\ \alpha^7,\ \alpha^{14},\ \alpha^4\right).$$

As the conditions are not satisfied for either $\ell_1 = 1$ or $\ell_2 = 1$, the decoder moves to the next step.

(2) $\ell_1 = \ell_2 = 2$:

$$\mathbf{m}_{14}^{(0)} = \mathbf{m}''_{14} - \beta'_2 = \beta^{61931} - \beta^{25148} = \beta^{21810} \leftrightarrow \left(\alpha^6, \quad \alpha^{11}, \quad \alpha^2, \quad \alpha^3\right);$$
$$\mathbf{m}_{14}^{(1)} = \mathbf{m}_{14}^{(0)} \Pi_{\mathcal{C}_2} = \left(\alpha^6, \quad \alpha, \quad \alpha, \quad \alpha^9\right);$$
$$\mathbf{m}_{14}^{(2)} = \mathbf{m}_{14}^{(0)} \Pi_{\mathcal{C}_2^{\perp}} = \left(0, \quad \alpha^6, \quad \alpha^5, \quad \alpha\right), \text{ and}$$
$$\mathbf{m}_{24}^{(0)} = \mathbf{m}''_{24} - \beta'_2 = \beta^{41364} - \beta^{25148} = \beta^{28078} \leftrightarrow \left(\alpha^4, \quad \alpha^9, \quad \alpha^3, \quad \alpha\right);$$
$$\mathbf{m}_{24}^{(1)} = \mathbf{m}_{24}^{(0)} \Pi_{\mathcal{C}_2} = \left(\alpha^4, \quad \alpha^9, \quad \alpha^3, \quad \alpha\right);$$
$$\mathbf{m}_{24}^{(2)} = \mathbf{m}_{24}^{(0)} \Pi_{\mathcal{C}_2^{\perp}} = \left(0, \quad 0, \quad 0, \quad 0\right),$$

where $\beta^{28078} \leftrightarrow \left(\alpha^4, \alpha^9, \alpha^3, \alpha\right) = \mathbf{m}_{24}^{(0)}$. Here, the conditions are satisfied for $\ell_2 = 2$ but not for $\ell_1 = 2$, the decoder moves to next step for ℓ_1.

(3) $\ell_1 = 3$:

$$\mathbf{m}_{14}^{(0)} = \mathbf{m}''_{14} - \beta'_3 = \beta^{61931} - \beta^{55731} = \beta^{1853} \leftrightarrow \left(\alpha^{10}, \quad \alpha^8, \quad \alpha^{12}, \quad \alpha^4\right);$$
$$\mathbf{m}_{14}^{(1)} = \mathbf{m}_{14}^{(0)} \Pi_{\mathcal{C}_3} = \left(\alpha^{10}, \quad \alpha^8, \quad \alpha^{12}, \quad \alpha^4\right);$$
$$\mathbf{m}_{14}^{(2)} = \mathbf{m}_{14}^{(0)} \Pi_{\mathcal{C}_3^{\perp}} = \left(0, \quad 0, \quad 0, \quad 0\right),$$

where $\beta^{1853} \leftrightarrow \left(\alpha^{10}, \alpha^8, \alpha^{12}, \alpha^4\right) = \mathbf{m}_{14}^{(0)}$.

The requirements are met at $\ell_1 = 3$ and $\ell_2 = 2$; consequently, the children codes $\mathcal{C}_3(4, 3)_{16}$ and $\mathcal{C}_2(4, 2)_{16}$ are used and $\mathbf{m} = \left((\alpha, \alpha^2, \alpha^3), (1, \alpha^2)\right)$ is recovered from $(\mathbf{m}_{14}^{(1)}, \mathbf{m}_{24}^{(1)})$ and finally, $\mathbf{m} = (\mathbf{m}_{13}, \ \mathbf{m}_{22}) = \left((\alpha, \alpha^2, \alpha^3), (1, \alpha^2)\right)$.

The above example demonstrates the proposed multi-rate encoding and decoding procedure for $\mathcal{C}_{MR}^{(2)}(4, \{2, 3, 4, 5, 6, 7, 8\}_{16}, 3)_{16^4}$. If in case, a 3-dimensional 'mother' code $\mathcal{C}(4, 3, 2)_{16^4}$ defined by

$$\mathbf{G} = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 \\ 1 & \beta^{16} & \beta^{32} & \beta^{48} \\ 1 & \beta^{32} & \beta^{48} & \beta^{64} \end{bmatrix}$$

is employed along with the 'children' codes $\mathcal{C}_1(4, 1)_{2^4}$, $\mathcal{C}_2(4, 2)_{2^4}$, $\mathcal{C}_3(4, 3)_{2^4}$ and $\mathcal{C}_4(4, 4)_{2^4}$, we will have $1 \leq \ell_1, \ell_2, \ell_3 \leq 4$, so that the multi-rate code $\mathcal{C}_{MR}^{(2)}(4, \{3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}_{16}, 2)_{16^4}$ can be used to encode and decode user messages $\mathbf{m} = (\mathbf{m}_{1\ell_1}, \mathbf{m}_{2\ell_2}, \mathbf{m}_{3\ell_3}) \in [\mathrm{GF}(q)]^{\ell_1} \times [\mathrm{GF}(q)]^{\ell_2} \times [\mathrm{GF}(q)]^{\ell_3}$ of length $\ell = 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ for transmission over a 16^4-ary noiseless channel.

7 Conclusions

Over the communication systems, data transmissions frequently demand codes with variable code rates. In order to address this issue, this paper proposes two multiple-rate coding schemes that employ existing error-correcting codes and enable variable-rate coding; in that, codes that can efficiently encode and decode variable-length message segments while retaining a constant code length are considered. In fact, it considers an existing fixed *k*/*n*-rate error-correcting code over a composite field

$\mathrm{GF}(q^n)$ and employs (1) k children codes of different rates $1/n, 2/n, \ldots, k/n$ defined over the ground field $\mathrm{GF}(q)$ [under construction-I: $q = p^k$]; (2) n children codes of different rates $1/n, 2/n, \ldots, n/n$ defined over the ground field $\mathrm{GF}(q)$ [under construction-II: $q = p^n$] to encode and decode variable block sized user messages. Employing the combination of mother and children codes, the proposed schemes derive two multiple-rate codes over $\mathrm{GF}(q^n)$ which simultaneously encode and decode information symbols over $\mathrm{GF}(q)$ of various lengths ranging (1) from 1 to k [under construction-I: $q = p^k$] (2) from k to kn [under construction-II: $q = p^n$], enabling multiple-rate feature. While the first construction facilitates transmission for information rates $1/n^2, 2/n^2, \ldots, k/n^2$, the second construction adds support for the transmission of more flexible rates $k/n^2, (k+1)/n^2, \ldots, kn/n^2$. Decoding of coded messages of different lengths is achieved using children's codes *orthogonal projectors*. The authors are considering further development of multiple-rate codes that can handle variable-length codeword sets, in addition to the support of variable message-length.

References

1. Birkhoff, G., Mac Lane, S.: A Survey of Modern Algebra, 5th edn. Macmillan Publishers Ltd., New York (1996)
2. Tse, D., Viswanath, P.: Fundamentals of Wireless Communication. Cambridge University Press, Cambridge (2005)
3. Goldsmith, A., Chua, S.-G.: Adaptive coded modulation for fading channels. IEEE Trans. Commn. **46**(5), 595–602 (1998)
4. Sun, Y., Karkooti, M., Cavallaro, J. R.: VLSI decoder architecture for high throughput, variable block-size and multi-rate LDPC codes. In: Proceedings of International Symposium on Circuits and Systems (ISCAS), pp. 2104–2107. New Orleans, LA (2007)
5. Hagenauer, J.: Rate-compatible punctured convolutional codes and their application. IEEE Trans. Commun. **36**, 389–400 (1988)
6. Acikel, O., Ryan, W.: Punctured turbo-codes for BPSK/QPSK channels. IEEE Trans. Commun. **47**, 1315–1323 (1999)
7. Yazdani, M.R., Banihashemi, A.H.: On construction of rate-compatible low-density parity-check codes. IEEE Commun. Lett. **8**(3), 159–161 (2004)
8. Ha, J., Kim, J., McLaughlin, S.: Rate-compatible puncturing of low-density parity-check codes. IEEE Trans. Inf. Theory **50**(11), 2824–2836 (2004)
9. Zhang, K., Ma, X., Zhao, S., Bai, B., Zhang X.: A new ensemble of rate-compatible LDPC codes. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), pp. 2536–2540. Cambridge, MA (2012)
10. Casado, A.I.V., Weng, W.-Y., Valle, S., Wesel, R.: Multiple-rate low-density parity-check codes with constant blocklength. IEEE Trans. Commun. **57**(1), 75–83 (2009)
11. Liu, L., Zhou, W., Zhou, S.: Nonbinary multiple rate QC-LDPC codes with fixed information or block bit length. J. Commun. Netw. **14**(4), 429–433 (2012)
12. Raja Durai, R. S.: Multiple-rate maximum rank distance codes. In: Proceedings of the 14th International Symposium on Information Theory and Its Applications (ISITA), pp. 696–699. Monterey, California (2016)
13. Gabidulin, E.M.: Theory of codes with maximum rank distance. Probl. Inf. Transm. **21**, 1–12 (1985)
14. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge (1986)
15. Hamming, R.W.: Error detecting and error correcting codes. Bell Syst. Techn. J. **29**, 147–160 (1950)
16. Roth, R.M.: Maximum-rank array codes and their application to crisscross error correction. IEEE Trans. Inf. Theory **37**, 328–336 (1991)

17. Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. J. Combin. Theory **25**(3), 226–241 (1978)
18. Cooperstein, B.N.: External flats to varieties in $M_{n,n}(\mathrm{GF}(q))$. Linear Alg. Appl. **267**, 175–186 (1997)
19. Loidreau, P.: Properties of codes in rank metric. In: Proceedings of the Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, pp. 192–198. Bulgaria (2008)
20. Gadouleau, M., Yan, Z.: On the decoder error probability of bounded rank-distance decoders for maximum rank distance codes. IEEE Trans. Inf. Theory **54**(7), 3202–3206 (2008)
21. Gadouleau, M., Yan, Z.: Packing and covering properties of rank metric codes. IEEE Trans. Inf. Theory **54**(9), 3873–3883 (2008)
22. Seroussi, G., Lempel, A.: Factorization of symmetric matrices and trace-orthogonal bases in finite fields. SIAM J. Comput. **9**(4), 758–767 (1980)
23. Lempel, A., Weinberger, M.: Self-complementary normal bases in finite fields. SIAM J. Discret. Math. **1**, 193–198 (1988)
24. Massey, J.L.: Linear codes with complementary duals. Discret. Math. **106 and 107**, 337–342 (1992)
25. Raja Durai, R. S.: On linear codes with rank metric: constructions, properties, and applications. Ph.D dissertation, Department of Mathematics, Indian Institute of Technology - Chennai, India (2004)
26. Vasantha Kandasamy, W.B., Smarandache, F., Sujatha, R., Raja Durai, R.S.: Erasure Techniques in MRD Codes. ZIP Publishing, Columbus (2012)
27. Raja Durai, R.S., Devi, M.: On the class of T-Direct codes over $\mathrm{GF}(2^N)$. Int. J. Comput. Inf. Syst. Ind. Manag. Appl. **5**, 589–596 (2013)
28. Liu, X., Liu, H.: Rank-metric complementary dual codes. J. Appl. Math. Comput. **61**, 281–295 (2019)
29. Green, D.H., Taylor, I.S.: Irreducible polynomials over composite Galois fields and their applications in coding techniques. Proc. Inst. Electr. Eng. **121**, 935–939 (1974)