On some important classes of row-cyclic array codes*

Sapna Jain
Department of Mathematics
University of Delhi
Delhi 110 007
India
E-mail: sapna@vsnl.com

Abstract. Row-cyclic array codes have already been introduced by the author [9]. In this paper, we give some special classes of row-cyclic array codes as an extension of classical BCH and Reed-Solomon codes.

AMS Subject Classification (2000): 94B05

Keywords: Array codes, Linear codes, Row-Cyclic Codes

1. Introduction

In [6], the author introduced the notion of row-cyclic array codes equipped with m-metric [10] and gave decoding algorithm of row-cyclic array codes. The row-cyclic array codes are completely determined by the generator m-tuple of polynomials $(g_1(x), \cdots, g_m(x))$. However, in general, it is difficult to obtain information on the minimum m-distance of a row-cyclic array code from its generator m-tuple even though the former is completely determined by the later. On the other hand, if we choose some special generator m-tuple of polynomials properly, then information on the minimum m-distance can be gained and also simpler decoding algorithms could apply. In this paper, by carefully choosing the genrator m-tuple of polynomials, we obtain two important classes of row-cyclic array codes as an extension of classical BCH and Reed-Solomon codes [2] and we call them as the BCH array codes (or BCHA codes) and the Reed-Solomon array codes (or RSA codes). We also introduce the Generalized BCHA codes (or GBCHA codes) and the Generalized RSA codes (or GRSA codes).

*This research is supported by National Board for Higher Mathematics (NBHM), Department of Atomic Energy, Government of India, under a Research Project vide ref. no. NBHM/RP.3/2007.

2. Definitions and Notations

Let F_q be a finite field of q elements. Let $\mathrm{Mat}_{m\times s}(F_q)$ denote the linear space of all $m \times s$ matrices with entries from F_q. An m-metric array code is a subset of $\mathrm{Mat}_{m\times s}(F_q)$ and a linear m-metric array code is an F_q-linear subspace of $\mathrm{Mat}_{m\times s}(F_q)$. Note that the space $\mathrm{Mat}_{m\times s}(F_q)$ is identifiable with the space F_q^{ms}. Every matrix in $\mathrm{Mat}_{m\times s}(F_q)$ can be represented as a $1 \times ms$ vector by writing the first row of matrix followed by second row and so on. Similarly, every vector in F_q^{ms} can be represented as an $m \times s$ matrix in $\mathrm{Mat}_{m\times s}(F_q)$ by separating the co-ordinates of the vector into m groups of s-coordinates. The m-metric on $\mathrm{Mat}_{m\times s}(F_q)$ is defined as follows [10]:

Definition 2.1. Let $Y \in \mathrm{Mat}_{1\times s}(F_q)$ with $Y = (y_1, y_2, \cdots, y_s)$. Define row weight (or ρ-weight) of Y as

$$wt_\rho(Y) = \begin{cases} \max\,\{\, i \mid y_i \neq 0\} & \text{if } Y \neq 0 \\ 0 & \text{if } Y = 0. \end{cases}$$

Extending the definitions of wt_ρ to the class of $m \times s$ matrices as

$$wt_\rho(A) = \sum_{i=1}^{m} wt_\rho(R_i)$$

where $A = \begin{bmatrix} R_1 \\ R_2 \\ \cdots \\ R_m \end{bmatrix} \in \mathrm{Mat}_{m\times s}(F_q)$ and R_i denotes the i^{th} row of A. Then wt_ρ satisfies $0 \leq wt_\rho(A) \leq n(= ms)\ \forall\ A \in \mathrm{Mat}_{m\times s}(F_q)$ and determines a metric on $\mathrm{Mat}_{m\times s}(F_q)$ known as m-metric (or ρ-metric).

Now, we define the row-cyclic array codes [6]:

Definition 2.2. An $[m \times s, k]$ linear array codes $V \subseteq \mathrm{Mat}_{m\times s}(F_q)$ is said to be row-cyclic if

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{ms} \end{pmatrix} \in \mathrm{V}$$

$$\Longrightarrow \begin{pmatrix} a_{1s} & a_{11} & a_{12} & \cdots a_{1,s-1} \\ a_{2s} & a_{21} & a_{22} & \cdots a_{2,s-1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{ms} & a_{m1} & a_{m2} & \cdots a_{m,s-1} \end{pmatrix} \in \mathrm{V}$$

i.e. the array obtained by shifting the columns of a code array cyclically by one position to the right and the last column occupying the first place is also a code array. In fact, a row-cyclic array code V of order $m \times s$ turns out to be of the form $V = \bigoplus_{i=1}^{m} V_i$ where each V_i is a classical cyclic code of length s. Also, every matrix/array in $\mathrm{Mat}_{m\times s}(F_q)$ can be identified with an m-tuple in $A_s^{(m)}$ where $A_s^{(m)}$ is the direct product of algebra A_s taken m times and A_s is the algebra of all polynomials over F_q modulo the polynomial $x^s - 1$ and this identification is given by

$$\theta : \mathrm{Mat}_{m\times s}(F_q) \to A_s^{(m)}$$

$$\theta(A) = \theta \begin{pmatrix} R_1 \\ \vdots \\ R_m \end{pmatrix} = \begin{pmatrix} \theta' R_1 \\ \theta' R_2 \\ \vdots \\ \theta' R_m \end{pmatrix} = (\theta' R_1, \theta' R_2, \cdots, \theta' R_m) \qquad (1)$$

where $R_i (i = 1 \text{ to } m)$ denotes the i^{th} row of A and $\theta' : F_q^s \longrightarrow A_s$ is given by

$$\theta'(a_0, a_1, \cdots, a_{s-1}) = a_0 + a_1 x + \cdots + a_{s-1} x^{s-1}.$$

An equivalent definition of row-cyclic array code is given by [6]:

Definition 2.3. An $m \times s$ linear array codes $V \subseteq \mathrm{Mat}_{m\times s}(F_q)$ is said to be row-cyclic if

$$V = \bigoplus_{i=1}^{m} V_i$$

where each V_i is an $[s, k_i, d_i]$ classical cyclic code equipped with m-metric. The parameters of row-cyclic array code V are given by $[m\times s, \sum_{i=1}^{m} k_i, \min_{i=1}^{m} d_i]$. If $g_1(x)$ is the generator polynomial of classical cyclic code V_i, then the m-tuple $(g_1(x) \cdots, g_m(x))$ is called the generator m-tuple of row cyclic code V.

3. The BCH Array Codes(or BCHA Codes)

Definition 3.1. Let $(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be an m-tuple of primitive elements of $F_{q^r}(r \geq 1)$ and denote by $M_i^{(j)}(x)$, the minimal polynomials of $\alpha_i^j (i = 1, 2, \cdots, m, j = 1, 2, \cdots)$ over F_q. A (primitive) BCHA code of order $m \times (q^r - 1)$ with the designed m-distances δ is a q-ary row-cyclic array code generated by m-tuple $((g_1(x), g_2(x), \cdots, g_m(x))$, where for every $i = 1$ to m,

$$g_i(x) = \text{lcm } (M_i^{(a_i)}(x), M_i^{(a_i+1)}(x), \cdots, M_i^{(a_i+\delta-2)}(x)),$$

and a_i's are nonegative integers depending upon i. Furthermore, the code is called narrow-sense if $a_i = 1$ for all $i = 1$ to m.

Note. For $m = 1$, the definition of BCHA codes reduces to the classical definition of BCH codes [2].

Example 3.2. Let α_1 be a root of x^3+x+1 and α_2 be a root of x^3+x^2+1 over F_2. Then (α_1, α_2) is a 2-tuple of primitive elements of F_{2^3}. A narrow-sense binary BCHA code V of order 2×7 equipped with the m-metric and with designed m-distance $\delta = 3$ is generated by the 2-tuple $((g_1(x), g_2(x))$ where

$$\begin{aligned} g_1(x) &= \text{lcm } (M_1^{(1)}(x), M_1^{(2)}(x)) \\ &= M^{(1)}(x) \\ &= x^3 + x + 1. \end{aligned}$$

Similarly, we have $g_2(x) = x^3 + x^2 + 1$.

Let $V = \bigoplus_{i=1}^{2} V_i$ where each V_i is a [7,4,4] classical cyclic code equipped with the m-metric and generated by the generator polynomial $g_i(x) (i = 1, 2)$. Therefore, V is a $[2 \times 7, 4 + 4, 4]$ row-cyclic array code and is an example of BCHA code. A generator matrix for code V is given by

$$G = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

where

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

and

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Now we obtain a lower bound on the dimension of a BCHA code.

Theroem 3.3. A q-ary BCHA code of order of $m \times (q^r - 1)$ with designed m-distnace δ has dimension at least

$$m((q^r - 1) - r(\delta - 1)). \tag{2}$$

Proof. Let $V = \bigoplus_{i=1}^{m} V_i$ be a BCHA code with generator m-tuple $(g_1(x), \cdots, \cdots, g_m(x))$ and with designed m-distance δ. Let C_{l_i} denote the cyclotomic coset of q modulo $(q^r - 1)$ containing $l_i (l_i \geq 0)$. Put

$$C^{(i)} = \bigcup_{l_i = a_i}^{a_i + \delta - 2} C_{l_i}.$$

Now

$$\begin{aligned} g_i(x) &= \operatorname{lcm}\left(\prod_{j \in C_{a_i}} (x - \alpha_i^j), \prod_{j \in C_{a_i}+1} (x - \alpha_i^j), \cdots, \prod_{j \in (C_{a_i}+\delta-2)} (x - \alpha_i^j) \right) \\ &= \prod_{j \in C^{(i)}} (x - \alpha_i^j). \end{aligned}$$

Thus the dimension of V_i is equal to $q^r - 1 - \deg\,(g_i(x))$ i.e.

$$\begin{aligned} k_i &= q^r - 1 - |C^{(i)}| \\ &= q^r - 1 - |\bigcup_{l_i=a_i}^{a_i+\delta-2} C_{l_i}| \\ &\geq q^r - 1 - \sum_{l_i=a_i}^{a_i+\delta-2} |C_{l_i}| \\ &\geq q^r - 1 - \sum_{l_i=a_i}^{a_i+\delta-2} r \end{aligned} \tag{3}$$

(as $q^r \equiv 1 (\text{mod } q^r - 1)$, therefore, each cyclotomic coset contains atmost r elements i.e. $|C_{l_i}| \leq r \forall\, l_i$)

$$\begin{aligned} &= q^r - 1 - r(a_i + \delta - 2 - a_i + 1) \\ &= q^r - 1 - r(\delta - 1). \end{aligned}$$

Therefore

$$\begin{aligned} \sum_{i=1}^{m} k_i &\geq \sum_{i=1}^{m} (q^r - 1 - r(\delta - 1)) \\ &= m((q^r - 1) - r(\delta - 1)). \end{aligned}$$

Example 3.4. Consider the binary BCHA code V of Example 3.2. Here $V = \bigoplus_{i=1}^{2} V_i$ where for each $i = 1, 2$ V_i is a [7,4,4] m-metric classical cyclic code of length 7 with generator polynomials $g_i(x)$ where $g_1(x) = x^3 + x + 1$ and $g_2(x) = x^3 + x^2 + 1$. Also, $k_1 = k_2 = 4$ and dim $V = k_1 + k_2 = 8$. Moreover, R.H.S. of (2) is equal to

$$2((2^3 - 1) - 3(3 - 1)) = 2.$$

We note that for this example, the dimension of code V is strictly bigger than the lower bound obtained in Theorem 3.3.

Example 3.5. Consider the binary BCHA code V with designed m-distance $\delta = 3$ and having $(g_1(x), g_2(x))$ as generator 2-tuple where

$$g_1(x) = g_2(x) = \text{lcm } (M^{(2)}(x), M^{(3)}(x))$$

where $M^{(i)}(x)$ is the minimal polynomial of α^i for $i = 2, 3$ and α is the primitive element of F_{2^4} (Here $r = 4$).

Since $o(\alpha) = 15$, therefore V is a binary BCHA code of order 2 × 15.

We can write

$$V = \bigoplus_{i=1}^{2} V_i$$

where for each $i = 1, 2$, V_i is a $[15, k_i]$ classical cyclic code equipped with the m-metric and having generator polynomial $g_i(x)$.

Consider the cyclotomic cosets of 2 modulo 15, we have

$$C_0 = \{0\},$$

$$\begin{aligned}
C_1 &= C_2 = C_4 = C_8 = \{1,2,4,8\}, \\
C_3 &= C_6 = C_9 = C_{12} = \{3,6,9,12\}, \\
C_5 &= C_{10} = \{5,10\}, \\
C_7 &= C_{11} = C_{13} = C_{14} = \{7,11,13,14\}.
\end{aligned}$$

Now, from (3)

$$k_1 = 15 - |C_2 + C_3| = 15 - 8 = 7.$$

Similarly, $k_2 = 7$.

Therefore,

$$\dim\ (V) = k_1 + k_2 = 14.$$

Also,

$$\begin{aligned}
\text{R.H.S. of (2)} &= 2((2^4 - 1) - 4(3 - 1)) \\
&= 14.
\end{aligned}$$

Thus, the lower bound in Theorem 3.3. is attained in this example.

The following result gives a sufficient condition under which the lower bound in Theorem 3.3 can be achieved.

Theorem 3.6. *A narrow-sense q-ary BCHA code of order $m \times (q^r - 1)$ with designed m-distance δ has dimension exactly equal to $m((q^r - 1) - r(\delta - 1))$ provided*

$$\gcd\ (q^r - 1, e) = 1 \quad \text{for } 1 \leq e \leq \delta - 1.$$

Proof. For all $i = 1$ to m, we have

$$\begin{aligned}
k_i &= q^r - 1 - |\bigcup_{l_i=1}^{\delta-1} C_{l_i}| \quad \text{(on taking } a_i = 1 \text{ in (3))} \\
&= q^r - 1 - |\bigcup_{l=1}^{\delta-1} C_l| \qquad (4)
\end{aligned}$$

where C_l stands for cyclotomic coset of q modulo $q^r - 1$ containing l.

We claim that

$$|C_l| = r \ \forall\ 1 \ \leq l \leq \delta - 1, \qquad (5)$$

and

$$C_l \cap C_p = \phi \; \forall \; 1 \leq l < p \leq \delta - 1. \tag{6}$$

Proof of Claim in (5). For any integer $1 \leq t \leq r-1$, we claim that

$$l \not\equiv q^t l (\text{mod } q^r - 1) \text{ for } 1 \leq l \leq \delta - 1.$$

Let, if possible

$$\begin{aligned} & l \equiv q^t l (\text{mod } q^r - 1) \text{ for } 1 \leq l \leq \delta - 1, \\ \Rightarrow \quad & (q^t - 1) l \equiv 0 (\text{mod } q^r - 1) \text{ for } 1 \leq l \leq \delta - 1. \end{aligned} \tag{7}$$

Since gcd $(q^r - 1, l) = 1$ for $1 \leq l \leq \delta - 1$, therefore (7) gives

$$(q^t - 1) \equiv 0 (\text{mod } q^r - 1),$$

which is contradiction as $1 \leq t \leq r - 1$.

Thus, for $1 \leq t \leq r - 1$, we have

$$\begin{aligned} & l \equiv q^t l (\text{mod } q^r - 1) \text{ for } 1 \leq l \leq \delta - 1, \\ \Rightarrow \quad & |C_l| = r \text{ for } 1 \leq l \leq \delta - 1. \end{aligned}$$

Proof. of Claim in (6). For any integers $1 \leq l < p \leq \delta - 1$, we claim that

$$p \not\equiv q^s l (\text{mod } q^r - 1) \text{ for any integer } s \geq 0.$$

Let, if possible

$$p \equiv q^s l (\text{mod } q^r - 1) \text{ for some integer } s \geq 0$$

Also,

$$\begin{aligned} l & \equiv l (\text{mod } q^r - 1) \\ & \Rightarrow p - l \equiv (q^s - 1) l (\text{mod } q^r - 1), \end{aligned}$$

This forces

$$p - l \equiv 0 (\text{mod } q^r - 1).$$

A contradiction to the fact that

$$\gcd\,(p-l, q^r-1) = 1 \text{ as } 1 \le p-l \le \delta - 1.$$

Thus

$$p \not\equiv q^s l (\text{mod } q^r - 1) \quad \text{for any integer } s \ge 0.$$

Hence

$$C_l \cap C_p = \phi \quad \text{for every } 1 \le l < p \le \delta - 1.$$

Now, from (4), (5) and (6) we get

$$\begin{aligned} k_i &= (q^r-1) - r(\delta-1) \\ \Rightarrow \sum_{i=1}^{m} k_i &= m((q^r-1) - r(\delta-1)). \end{aligned}$$

□

Now, the following theorem relates the designed m-distance δ with the actual minimum m-distance of a BCHA code.

Theorem 3.7. *A BCHA code with designed m-distance δ has minimum m-distance δ has actual minimum m-distance at least δ.*

Proof. Let $(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be an m-tuple of primitve elements of F_{q^r} and let V be a BCHA code generated by $(g_1(x), \cdots, g_m(x))$ where for every $i = 1$ to m,

$$g_i(x) = \text{lcm}\,(M_i^{(a_i)}(x), M_i^{(a_i+1)}(x), \cdots, M_i^{(a_i+\delta-2)}(x)).$$

It is clear that the elements $\alpha_i^{a_i}, \alpha_i^{a_i+1}, \cdots, \alpha_i^{a_i+\delta-2}(x)$ are the roots of $g_i(x)$ for every $i = 1$ to m.

Let if possible, the minimum m-distance of code V is less than δ. Then there exists a nonzero code array $(w_1(x), w_2(x), \cdots, w_m(x))$ in V with m-weight $(w_i(x)) = d_i$ and

$$d_1 + d_2 + \cdots + d_m < \delta.$$

This implies that $d_i < \delta \; \forall i = 1$ to m.

Choose $i (1 \le i \le m)$ such that $d_i \ne 0$ and fix it.

Let $0 \neq \; w_i(x) = w_0^{(i)} + w_1^{(i)}x + \cdots + w_{s-1}^{(i)}x^{s-1}$.

Now,

$$m\text{-weight } (w_i(x)) = d_i(< \delta) \Rightarrow w_{d_i-1}^{(i)} \neq 0$$

and

$$w_{d_i}^{(i)} = w_{d_i-1}^{(i)} = w_{d_i+2}^{(i)} = \cdots = w_{s-1}^{(i)} = 0. \tag{8}$$

Now, $w_i(x)$ is an element of the ideal generated by $g_i(x)$ in the algebra A_s, the algebra of polynomials modulo the polynomial $x^s - 1$, therefore we have

$$w_i(\alpha_i^j) = 0 \quad \forall j = a_i, a_i + 1, \cdots, a_i + \delta - 2,$$

i.e.

$$\begin{pmatrix} 1 & \alpha_i^{a_i} & (\alpha_i^{a_i})^2 & \cdots & (\alpha_i^{a_i})^{s-1} \\ 1 & \alpha_i^{a_i+1} & (\alpha_i^{a_i+1})^2 & \cdots & (\alpha_i^{a_i+1})^{s-1} \\ 1 & \alpha_i^{a_i+2} & (\alpha_i^{a_i+2})^2 & \cdots & (\alpha_i^{a_i+2})^{s-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_i^{a_i+\delta-2} & (\alpha_i^{a_i+\delta-2})^2 & \cdots & (\alpha_i^{a_i+\delta-2})^{s-1} \end{pmatrix} \begin{pmatrix} w_0^{(i)} \\ w_1^{(i)} \\ w_2^{(i)} \\ \vdots \\ w_{s-1}^{(i)} \end{pmatrix} = 0 \tag{9}$$

In view of (8), the system of equations in (9) reduces to

$$\begin{pmatrix} 1 & \alpha_i^{a_i} & (\alpha_i^{a_i})^2 & \cdots & (\alpha_i^{a_i})^{d_i-1} \\ 1 & \alpha_i^{a_i+1} & (\alpha_i^{a_i+1})^2 & \cdots & (\alpha_i^{a_i+1})^{d_i-1} \\ 1 & \alpha_i^{a_i+2} & (\alpha_i^{a_i+2})^2 & \cdots & (\alpha_i^{a_i+2})^{d_i-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_i^{a_i+\delta-2} & (\alpha_i^{a_i+\delta-2})^2 & \cdots & (\alpha_i^{a_i+\delta-2})^{d_i-1} \end{pmatrix} \begin{pmatrix} w_0^{(i)} \\ w_1^{(i)} \\ w_2^{(i)} \\ \vdots \\ w_{d_i-1}^{(i)} \end{pmatrix} = 0 \tag{10}$$

Since $d_i \leq \delta - 1 \Rightarrow d_i - 1 \leq \delta - 2$, choosing first d_i equations from the system of equations in (10) gives

$$\begin{pmatrix} 1 & \alpha_i^{a_i} & (\alpha_i^{a_i})^2 & \cdots & (\alpha_i^{a_i})^{d_i-1} \\ 1 & \alpha_i^{a_i+1} & (\alpha_i^{a_i+1})^2 & \cdots & (\alpha_i^{a_i+1})^{d_i-1} \\ 1 & \alpha_i^{a_i+2} & (\alpha_i^{a_i+2})^2 & \cdots & (\alpha_i^{a_i+2})^{d_i-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_i^{a_i+d_i-1} & (\alpha_i^{a_i+d_i-1})^2 & \cdots & (\alpha_i^{a_i+d_i-2})^{d_i-1} \end{pmatrix} \begin{pmatrix} w_0^{(i)} \\ w_1^{(i)} \\ w_2^{(i)} \\ \vdots \\ w_{d_i-1}^{(i)} \end{pmatrix} = 0 \tag{11}$$

The determinant D of the coefficient matrix of system of equations in (11) is equal to

$$\begin{aligned}
D &= \prod_{j=0}^{d_i-1} (\alpha_i^{a_i})^j \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha_i & \alpha_i{}^2 & \cdots & \alpha_i^{d_i-1} \\ 1 & \alpha_i^2 & (\alpha_i^2)^2 & \cdots & (\alpha_i^2)^{d_i-1} \\ \vdots & \vdots & \vdots & \vdots & \\ 1 & \alpha_i^{d_i-1} & (\alpha_i^{d_i-1})^2 & \cdots & (\alpha_i^{d_i-1})^{d_i-1} \end{pmatrix} \\
&= \prod_{j=0}^{d_i-1} (\alpha_i^{a_i})^j \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ (\alpha_i)^0 & (\alpha_i)^1 & (\alpha_i)^2 & \cdots & (\alpha_i)^{d_i-1} \\ (\alpha_i^2)^0 & (\alpha_i^2)^1 & (\alpha_i^2)^2 & \cdots & (\alpha_i^2)^{d_i-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ (\alpha_i^{d_i-1})^0 & (\alpha_i^{d_i-1})^1 & (\alpha_i^{d_i-1})^2 & \cdots & (\alpha_i^{d_i-1})^{d_i-1} \end{pmatrix} \\
&= \prod_{j=0}^{d_i-1} (\alpha_i^{a_i})^j \times \prod_{\substack{l,m=0: \\ l>m}}^{d_i-1} (\alpha_i^l - \alpha_i^m) \neq 0.
\end{aligned}$$

Therefore, the coefficient matrix in (11) is a nonsingular matrix and since (11) is a homogeneous system of equation, we must have

$$\begin{pmatrix} w_0^{(i)} \\ w_1^{(i)} \\ w_2^{(i)} \\ \vdots \\ w_{d_i-1}^{(i)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad (12)$$

$\Rightarrow w_i(x) = w_0^{(i)} + w_1^{(i)}x + \cdots + w_{s-1}^{(i)}x^{s-1} = 0$. A contradiction. Thus there does not exist a nonzero code array in V having m-weight less than δ. Hence minimum m-distance of code V is at least δ. □

4. The Reed-Solomon Array Codes

RS codes in classical coding were introduced by I.S. Reed and G. Solomon in the year 1960. we extend the notion of RS codes to array codes equipped with m-metric and introduce RSA codes as a subclass of BCHA codes.

Cosnider a q-ary BCHA code of order $m \times (q^r - 1)$ with designed m-distance δ and generated by $(g_1(x), \cdots, g_m(x))$ where for every $i = 1$ to m,

$$g_i(x) = \text{lcm } (M_i^{(a_i)}(x), M_i^{(a_i+1)}(x), \cdots, M_i^{(a_i+\delta-2)}(x)).$$

and $M_i^{(a_i)}(x)$ is the minimal polynomial of $\alpha_i^{a_i}$ over F_q and $(\alpha_1, \alpha_2, \cdots, \alpha_m)$ is an m-tuple of primitve elements of F_{q^r}. If $r = 1$, then we obtain a q-ary BCHA code of order $m \times (q-1)$. In this case, the m-tuple $(\alpha_1, \alpha_2, \cdots, \alpha_m)$ is an m-tuple of primitive elements of F_q and moreover, the minimal polynomial of $\alpha_i^{a_i}$ over F_q is $x - \alpha_i^{a_i}$. Thus for $\delta \leq q-1, g_i(x)$ for $i = 1, 2, \cdots, m$ is given by

$$\begin{aligned} g_i(x) &= \text{lcm } ((x - \alpha_i^{a_i}), (x - \alpha_i^{a_i+1}), \cdots, (x - \alpha_i^{a_i+\delta-2})) \\ &= (x - \alpha_i^{a_i})(x - \alpha_i^{a_i+1}) \cdots (x - \alpha_i^{a_i+\delta-2}) \end{aligned}$$

since $\alpha_i^{a_i}, \alpha_i^{a_i+1}, \cdots, \alpha_i^{a_i+\delta-2}$ are pairwise distinct.

Defintion 4.1. A q-ary RSA code quipped with m-metric is a q-ary BCHA code of order $m \times (q-1)$ generated by m-tuple of polynomials $(g_1(x), g_2(x), \cdots, \cdots g_m(x))$ where for every $i = 1$ to m, $g_i(x)$ is given by

$$g_i(x) = (x - \alpha_i^{a_i})(x - \alpha_i^{a_i+1}) \cdots (x - \alpha_i^{a_i+\delta-2})$$

with $a_i \geq 0, 2 \leq \delta \leq q-1$ and α_i is a primitive element of F_q.

Theorem 4.2. *For RSA codes, actual minimum m-distance is equal to the designed m-distance.*

Proof. Let $\bigoplus_{i=1}^{m} V_i$ be an RSA code generated by $(g_1(x), g_2(x), \cdots, g_m(x))$ and having designed distance δ. Here each V_i is a $[q-1, k_i, d_i]$ m-metric array code. Since $\deg g_i(x) = \delta - 1 \Rightarrow k_i = q-1-(\delta-1) = q - \delta \Rightarrow \delta = q - k_i$. By Singelton's bound for component codes, we have

$$\begin{aligned} d_i &\leq (q-1) - k_i + 1 = q - k_i = \delta \\ \Rightarrow \min d_i &\leq \delta \\ \Rightarrow d &\leq \delta \end{aligned} \tag{13}$$

where $d = \min_{i=1}^{m} d_i$ is the actual minimum m-distance of RSA code V.

Also, by Theorem 3.7, we have

$$d \geq \delta \tag{14}$$

From (13) and (14), we get

$$d = \delta.$$

Thus for an RSA code, actual minimum m-distance is equal to the designed m-distance. □

Example 4.3. Let $(\alpha_1, \alpha_2) = (3, 5)$ be a 2-tuple of primtive elements of F_7. Consider the 7-ary RSA code $V = \bigoplus_{i=1}^{2} V_i$ of order 2×6 with designed m-distance $\delta = 4$ and generated by 2-tuple of polynomials $(g_1(x), g_2(x))$ where

$$g_1(x) = (x-3)(x-3^2)(x-3^3)$$

and

$$g_2(x) = (x-5)(x-5^2)(x-5^3).$$

The generator matrix of code V_1 is given by

$$\begin{pmatrix} 6 & 1 & 3 & 1 & 0 & 0 \\ 0 & 6 & 1 & 3 & 1 & 0 \\ 0 & 0 & 6 & 1 & 3 & 1 \end{pmatrix}.$$

Since no nonzero linear combination of elements of fourth column of G_1 over F_7 is zero, therefore, the minimum m-distance of code V_1 is 4.

Similarly, the minimum m-distance of code $V_2 = 4$.

Thus the minimum m-distance of RSA code V is $\min(4, 4) = 4$. Hence Theorem 4.1 is verified.

Theorem 4.4. *The dual of RSA code is again RSA code.*

Proof. The proof follows from the fact that if $V = \bigoplus_{i=1}^{n} V_i$ is a row-cyclic array code, then $V^{\perp} = \bigoplus_{i=1}^{n} V_i^{\perp}$ and the dual of a classical RS code is again an RS code. □

Reamrk 4.5. RSA codes are not MDS.

Proof. From Example 4.3 we have

$$\bigoplus_{i=1}^{2} V_i$$

is a RSA code where each V_i is [6,3,4] code.

Therefore, V is $[2 \times 6, 3+3, 4]$ i.e. [12,6,4] code.

Here parameters of V do not meet the Singelton's bound since for code V, we have

$$n - k + 1 = 12 - 6 + 1 = 7 \geq 4 = d.$$

5. The Generalized BCHA and RSA codes

We begin with the definition of generalized BCHA and generalized RSA codes:

Definition 5.1. Let $(\alpha_1, \alpha_2 \cdots, \alpha_m)$ be an m-tuple of primtive elements of $F_{q_r} (r \geq 1)$ and denote by $M_i^j(x)$, the minimal polynomial of $\alpha_i^j = (i = 1, 2, \cdots, m, j = 1, 2, \cdots)$ over F_q. The generalized BCHA code (or GBCHA code) of order $m \times (q^r - 1)$ with designed m-distance tuple $(\delta_1, \delta_2, \cdots \delta_m)(2 \leq \delta_i \leq q^r - 1)$ is a q-ary row-cyclic array code generated by m-tuple $(g_1(x), g_2(x), \cdots, g_m(x))$ where for each $i = 1$ to m

$$g_i(x) = \text{lcm } (M_i^{(a_i)}(x), M_i^{(a_i+1)}(x), \cdots, M_i^{(a_i+\delta_i-2)}(x)),$$

and a_i's are nonnegative integers depending upon i.

Furthermore, the code is called narrow-sense if $a_i = 1$ for all $i = 1$ to m.

Defintion 5.2. A q-ary GRSA code equipped with m-metric is a q-ary GBCHA code of order $m \times (q-1)$ generated by m-tuple of polynomials $(g_1(x), g_2(x), \cdots, g_m(x))$ where for every $i = 1$ to m, $g_i(x)$ is given by

$$g_i(x) = (x - \alpha_i^{a_i})(x - \alpha_i^{a_i+1}) \cdots (x - \alpha_i^{a_i+\delta_i-2})$$

with $a_i \geq 0, 2 \leq \delta_i \leq q - 1$ and α_i is a primitive element of F_q.

Remark. If we take designed m-distance tuple $(\delta_1, \delta_2, \cdots, \delta_m)$ to be $(\delta, \delta, \cdots, \delta)$ for some $2 \leq \delta \leq q^r - 1$, then the GBCHA and GRSA codes reduce to the BCHA codes and RSA codes respectively.

The following theorems on GBCHA and GRSA codes can easily be proved parallel to the theorems in Section 3 and 4.

Theroem 5.3. *A q-ary GBCHA code of order $m \times (q^r - 1)$ with designed m-distance tuple $(\delta_1, \delta_2, \cdots, \delta_m)$ has dimension at least*

$$m(q^r - 1) - r(\sum_{i=1}^{m} \delta_i - m).$$

Theorem 5.4. *A narrow-sense q-ary GBCHA code of order $m \times (q^r - 1)$ has dimension exactly euqal to $m(q^r - 1) - r(\sum_{i=1}^{m} \delta_i - m)$ provided $gcd(q^r - 1, e_i) = 1 \ \forall \ 1 \leq e_i \leq \delta_i - 1, i = 1, 2, \cdots, m$.*

Theorem 5.5. *A GBCHA code with designed m-distance tuple $(\delta_1, \delta_2, \cdots, \cdots \delta_m)$ has minimum m-distance at least $\min_{i=1}^{m} \delta_i$.*

Theorem 5.6. *For a GRSA code with desigend m-distance tuple $(\delta_1, \delta_2, \cdots, \cdots \delta_m)$, the actual minimum m-is equal to $\min_{i=1}^{m} \delta_i$.*

Theroem 5.7. *The dual of a GRSA code is again a GRSA code.*

Acknowledgment. The author would like to thank her husband Dr. Arihant Jain for his constant support and encouragement for pursuing this research work.

References

[1] M. Blum, P.G. Farrell and H.C.A. van Tilborg, *Array Codes*, in Handbook of Coding Theory, (Ed.: V. Pless and Huffman), Vol. II, Elsevier, North-Holland, 1998, pp.1855-1909.

[2] W. Cary Huffman and Vera Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, 2003.

[3] S. Jain, *Bursts in m-Metric Array Codes*, Linear Algebra and Its Applications, 418 (2006), 130-141.

[4] S. Jain, *Campopiano-Type Bounds in Non-Hamming Array Coding,* Linear Algebra and Its Applications, 420 (2007), 135-159.

[5] S. Jain, *An Algorithmic Approach to Achieve Minimum ρ-Distance at least d in Linear Array Codes*, Kyushu J. Math., 62 (2008), 189-200.

[6] S. Jain, *Row-Cyclic Codes in Array Coding*, Algebras, Groups, Geometries, 25 (2008), 287-310.

[7] S. Jain, *Decoding of Blockwise-Burst Errors in Row-Cyclic Array Codes*, to appear in Ars Combinatoria.

[8] S. Jain, *Decoding of Cluster Array Errors in Row-Cyclic Array Codes*, communicated.

[9] W. W. Peterson and E.J. Weldon, Jr., Error Correcting Codes, 2nd Edition, MIT Press, Cambridge, Massachusetts, 1972.

[10] M. Yu. Rosenbloom and M.A. Tsfasman, *Codes for m-metric*, Problems of Information Transmission, 33 (1997), 45-52.