U.P.B. Sci. Bull., Series A, Vol. 78, Iss. 3, 2016 ISSN 1223-7027

CYCLIC CODES AS IDEALS IN $\mathbb{F}_2[x;a\mathbb{N}_0]_n$, $\mathbb{F}_2[x]_{an}$, AND $\mathbb{F}_2[x;\frac{1}{b}\mathbb{N}_0]_{abn}$: A LINKAGE

Tariq SHAH,[1], Asma SHAHEEN [2]

Random error correcting codes are not efficient for correcting burst errors; therefore, it is required to design specialized codes which can correct burst errors. In this study, construction technique of cyclic codes is improved by using monoid rings instead of polynomial ring. The new scheme is formulated in such a way, that, for a given n length binary cyclic code C_n, three different binary cyclic codes C_{an}, C_{bn} and C_{abn} of length an, bn and abn are constructed. It is proved that these binary cyclic codes are interleaved codes of depths a,b, and ab respectively. Therefore, if the initial code C_n corrects t errors, then the interleaved codes C_{an}, C_{bn} and C_{abn} correct t bursts of length a,b and ab or less.

Keywords: Monoid rings, binary cyclic codes, generating and parity check matrices, interleaved codes.

1. Introduction

Algebraic coding theory is one of the most effective and widely applied branch of abstract algebra. It forms the basis of modern communication systems and is used in essentially all hardware level implementations of smart and intelligent machines, such as scanners, optical devices, and telecom equipment. It is due to the algebraic codes that we are able to communicate over long distances and are able to achieve megabit, bandwidth over a wireless communication channel.

One of the important class of algebraic codes is cyclic codes. Cyclic codes were initially studied by Prange in the year 1957 ([19], [20]). He noticed that the class of cyclic codes has a rich algebraic structure, the first indication that algebra would be a valuable tool in code design. Since then, advancement in the theory of cyclic codes for correcting random as well as burst errors has been encouraged by many coding theorists (see [4], [18], [8], and [5]). Cyclic codes were first studied over the binary field $\mathbb{F}_2$, then were extended to to its Galois field extension $\mathbb{F}_q$, where $q = p^m$, p is a prime number and $m \geq 1$. The correspondence of cyclic codes with ideals was observed independently by Peterson [17] and Kasami [7]. A cyclic code C of length n over a Galois field $\mathbb{F}_q$ can be viewed as an ideal of the factor ring $\frac{\mathbb{F}_q[x]}{(x^n-1)}$. Many authors have considered properties of cyclic codes defined as ideals in ring constructions (see [9], [12], [13], [14] and [15]).

[1] Dept.of mathematics, Quaid-i-AzamUniversity, Islamabad, e-mail: stariqshah@gmail.com
[2] Dept.of mathematics, Quaid-i-AzamUniversity, Islamabad, e-mail: asia_ansari@hotmail.com

Cyclic codes are effectively applied for correcting random as well as burst errors. *A burst of length* $l>1$ *is a binary vector whose nonzero components are confined to* l *cyclically consecutive positions, with the first and last positions being nonzero*. The binary vector 0011010000 has a burst of length 4. *A code is called an* l *burst error correcting code if it can correct all burst errors of length* l *or less*. Cyclic codes for single burst error correction were first studied by Abramson ([1], [2]). The most efficient cyclic codes for the correction of random as well as burst errors are *interleaved codes*. By interleaving a t random error correcting (n,k) cyclic code to degree β, we obtain a $(\beta n, \beta k)$ cyclic code which is capable of correcting any combination of t bursts of length β or less [11, Section 9.4].

In a sequence of papers [3], [21], [22], [23], [24], [25] and [26], cyclic codes using different monoid rings, over a local finite commutative ring were constructed. However, in this study our focus is on binary field $\mathbb{F}_2$, since in present digital computers and digital data communication systems, information is coded in binary bits, therefore it is more applicable than local finite commutative rings. To construct cyclic codes using the monoid ring $\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]$, where a and b are integers satisfying $a,b\geq 1$ with $b=a+1$, we will first construct cyclic codes using the monoid ring $\mathbb{F}_2[x;a\mathbb{N}_0]$. This is certain because $\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]$ does not contain the polynomial ring $\mathbb{F}_2[x]$ for $a,b>1$, whereas the ring $\mathbb{F}_2[x;a\mathbb{N}_0]$ is properly contained in both the rings $\mathbb{F}_2[x]$ and $\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]$.

The factor rings $\frac{\mathbb{F}_2[x;a\mathbb{N}_0]}{((x^a)^n-1)}$, $\frac{\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]}{((x^{\frac{a}{b}})^{bn}-1)}$ and $\frac{\mathbb{F}_2[x;\frac{1}{b}\mathbb{N}_0]}{((x^{\frac{1}{b}})^{abn}-1)}$ are denoted by $\mathbb{F}_2[x;a\mathbb{N}_0]_n$, $\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$ and $\mathbb{F}_2[x;\frac{1}{b}\mathbb{N}_0]_{abn}$, where $((x^a)^n-1)$, $((x^{\frac{a}{b}})^{bn}-1)$ and $((x^{\frac{1}{b}})^{abn}-1)$ are the principal ideals in the monoid rings $\mathbb{F}_2[x;a\mathbb{N}_0]$, $\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]$ and $\mathbb{F}_2[x;\frac{1}{b}\mathbb{N}_0]$ respectively. Consequently, a method is devised such that; for a given (n,k) binary cyclic code C_n generated by r degree (generalized) polynomial $g(x^a)\in\mathbb{F}_2[x;a\mathbb{N}_0]$, we get (an,ak), (bn,bk) and (abn,abk) binary cyclic codes C_{an}, C_{bn} and C_{abn} generated by ar, br and abr degree (generalized) polynomials $g(x)\in\mathbb{F}_2[x]$, $g(x^{\frac{a}{b}})\in\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]$ and $g(x^{\frac{1}{b}})\in\mathbb{F}_2[x;\frac{1}{b}\mathbb{N}_0]$. By [18, Theorem 11.1], the binary cyclic codes C_{an}, C_{bn} and C_{abn} are interleaved codes of degree a, b and ab, respectively. Therefore, if the initial code C_n corrects up to t errors, then the interleaved codes C_{an}, C_{bn} and C_{abn} correct t bursts of length a,b and ab or less. Whereas this t bits error in each row will be corrected by the base code C_n. The interleaved codes C_{an}, C_{bn} and C_{abn} are capable of correcting all bursts of length al, bl and abl or less, whenever the base code C_n corrects all bursts of length l or less.

This paper is organized as follows: Section 1 describes a brief introduction to the semigroup rings. In section 2, the construction of binary cyclic codes C_{an}, C_{bn} and C_{abn}, as ideals in the rings $F_2[x]_n$, $F_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$ and $F_2[x;\frac{1}{b}\mathbb{N}_0]_{abn}$, is explained. In section 3, the relationship among all of these binary cyclic codes is obtained through interleaving technique and by their generator and parity check matrices. Their error correction capability and decoding is discussed in section 4. The last section 5 concludes the findings.

2. Semigroup Rings

Throughout, Z denotes the ring of integers, $\mathbb{N}_0$ the additive monoid of all non-negative integers, and F_q is a Galois field of q elements, where q is a prime or a power of a prime.

Let F_2 be a binary field, and let x be a variable. For an additive semigroup S, $F_2[x;S]$ denotes the set of all finite sums of the form $\sum_{i=1}^{n} f_i x^{s_i}$, where $n\in\mathbb{N}_0$, $0\neq f_i\in F_2$ and $s_i\in S$. The set $F_2[x;S]$ is a ring with respect to binary operation addition defined as; $\sum_{i=0}^{n} f_i x^{s_i}+\sum_{i=0}^{n} g_i x^{s_i}=\sum_{i=0}^{n}(f_i+g_i)x^{s_i}$, (1)

where $n\in\mathbb{N}_0$, $f_i,g_i\in F_2$ and $s_i\in S$. Whereas multiplication is defined by the distributive law and the rule $f_1x^{s_1}.f_2x^{s_2}=(f_1.f_2)x^{s_1+s_2}$. (2)

In particular we have $\sum_{i=0}^{n} f_i x^{s_i}.\sum_{j=0}^{m} g_j x^{s_j}=\sum_{i,j}(f_i g_j)x^{s_i+s_j}$, (3)

where $n,m\in\mathbb{N}_0$, $f_i,g_j\in F_2$ and $s_i,s_j\in S$. The set $F_2[x;S]$ is called a *semigroup ring* of S over F_2. If S is a monoid, then $F_2[x;S]$ is called a *monoid ring*. The monoid ring $F_2[x;S]$ is a *polynomial ring* in one indeterminate if the monoid S is $\mathbb{N}_0$. Let us refer to [10, Section 3.2], for an alternative equivalent definition of a semigroup ring.

In semigroup rings, the concepts of degree and order are not defined generally. However, if S is a totally ordered semigroup then, the degree and order of an element of the semigroup ring $F_2[x;S]$ is defined as: Let $f=\sum_{i=1}^{n} f_i x^{s_i}$ be the arbitrary nonzero element in $F_2[x;S]$, where $s_1<s_2<\cdots<s_n$, then s_n is the *degree of* f and the order of f is s_1.

In this study, the monoid S is taken to be totally ordered monoids $a\mathbb{N}_0=\{0,a,2a,...\}$ and $\frac{a}{b}\mathbb{N}_0=\{0,\frac{a}{b},\frac{2a}{b},...\}$, where a and b are integers satisfying $a,\ b\ \geq 1$ with $b=a+1$.

3. Cyclic codes as ideals in $F_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$

Definition 1: *A subspace of the vector space of all* $n-$*tuples over the binary field* F_2 *is called a linear code* C *of length* n.

Definition 2: *A linear code* C *over* F_2 *is a cyclic code, if* $v=(v_0,v_1,\cdots,v_{n-1})\in C$ *, then every cyclic shift* $v^{(1)}=(v_{n-1},v_0,\cdots,v_{n-2})\in C$ *, where* $v_i\in F_2$ *and* $0\le i\le n-1$.

Due to the fact that $F_2[x]\subset F_2[x;\frac{1}{b}N_0]$, the generator polynomials of cyclic codes in $\frac{F_2[x]}{(x^n-1)}$ and $\frac{F_2[x;\frac{1}{b}N_0]}{((x^{\frac{1}{b}})^{bn}-1)}$ have a relationship. But since $F_2[x]\not\subseteq F_2[x;\frac{a}{b}N_0]$, this posed a hurdle to construct the cyclic codes in the factor ring $\frac{F_2[x;\frac{a}{b}N_0]}{((x^{\frac{a}{b}})^{bn}-1)}$. However, the fact $F_2[x;aN_0]\subset F_2[x;\frac{a}{b}N_0]$ provides a justification for constructing the binary cyclic codes in $F_2[x;\frac{a}{b}N_0]_{bn}$ by using an n length cyclic code C_n obtained from $F_2[x;aN_0]_n$. Let

$$f(x^a)=f_0+f_a(x^a)+f_{2a}(x^a)^2+\cdots+f_{an}(x^a)^n\in F_2[x;aN_0] \tag{4}$$

be a generalized polynomial of degree n, then $f(x^a)$ has degree bn in the monoid ring $F_2[x;\frac{a}{b}N_0]$ and is represented by

$$f(x^{\frac{a}{b}})=f_0+f_{\frac{a}{b}}(x^{\frac{a}{b}})^b+f_{2\frac{a}{b}}(x^{\frac{a}{b}})^{2b}+\cdots+f_{n\frac{a}{b}}(x^{\frac{a}{b}})^{bn}. \tag{5}$$

If $f(x^{\frac{a}{b}})$ is monic, then the factor ring $\frac{F_2[x;\frac{a}{b}N_0]}{(f(x^{\frac{a}{b}}))}$ is the ring of residue classes of generalized polynomials in $F_2[x;\frac{a}{b}N_0]$ modulo ideal $(f(x^{\frac{a}{b}}))$. Thus, if we take $f(x^{\frac{a}{b}})$ to be $(x^{\frac{a}{b}})^{bn}-1$, then the factor ring is

$$\frac{F_2[x;\frac{a}{b}N_0]}{((x^{\frac{a}{b}})^{bn}-1)}=\{c_0+c_{\frac{a}{b}}\beta+\ldots+c_{\frac{a}{b}(n-1)}\beta^{bn-1}\ :\ c_0,c_{\frac{a}{b}},\ldots,c_{\frac{a}{b}(n-1)}\in F_2\}, \tag{6}$$

Where β denotes the coset $x^{\frac{a}{b}}+((x^{\frac{a}{b}})^{bn}-1)$. Also, $f(\beta)=0$, when β satisfies the relation $\beta^{bn}-1=0$. By writing $x^{\frac{a}{b}}$ in place of β,the ring $\frac{F_2[x;\frac{a}{b}N_0]}{((x^{\frac{a}{b}})^{bn}-1)}$ becomes $F_2[x;\frac{a}{b}N_0]_{bn}$ in which the relation $(x^{\frac{a}{b}})^{bn}=1$ holds. The factor ring $F_2[x;\frac{a}{b}N_0]_{bn}$ is algebra over the field F_2. The multiplication $*$ in the ring $F_2[x;\frac{a}{b}N_0]_{bn}$ is defined as: for $c(x^{\frac{a}{b}})$ in $F_2[x;\frac{a}{b}N_0]_{bn}$ the product $(x^{\frac{a}{b}})*c(x^{\frac{a}{b}})$ is given by:

$$\begin{aligned}(x^{\frac{a}{b}})*c(x^{\frac{a}{b}})&=(x^{\frac{a}{b}})*(c_0+c_{\frac{a}{b}}(x^{\frac{a}{b}})+c_{2\frac{a}{b}}(x^{\frac{a}{b}})^2+\ldots+c_{\frac{a}{b}(n-1)}(x^{\frac{a}{b}})^{n-1})\\&=c_{\frac{a}{b}(n-1)}+c_0(x^{\frac{a}{b}})+c_{\frac{a}{b}}(x^{\frac{a}{b}})^2+\ldots+c_{\frac{a}{b}(n-2)}(x^{\frac{a}{b}})^{n-1}\end{aligned} \tag{7}$$

Following results give a method of obtaining the generator generalized polynomial, which generates a principal ideal of the factor ring $F_2[x;\frac{a}{b}N_0]_{bn}$.

Theorem 1: *A subset* C_{bn} *in* $F_2[x;\frac{a}{b}N_0]_{bn}$ *is a binary cyclic code if and only if* C_{bn} *is an ideal in the ring* $F_2[x;\frac{a}{b}N_0]_{bn}$.

The following Theorem extends [16, Theorem 4.3.6] for the monoid ring $F_2[x;\frac{a}{b}N_0]$.

Theorem 2: *Let* C_{bn} *be a nonzero ideal in the ring* $F_2[x;\frac{a}{b}N_0]_{bn}$. *Then the following* *hold.*

1) *There exists a unique monic generalized polynomial* $g(x^{\frac{a}{b}})$ *of least degree in* C_{bn},

2) $g(x^{\frac{a}{b}})$ *divides* $(x^{\frac{a}{b}})^{bn}-1$ *in* $F_2[x;\frac{a}{b}\mathbb{N}_0]$,

3) *For all* $c(x^{\frac{a}{b}})\in C_{bn}$, *it follows that* $g(x^{\frac{a}{b}})$ *divides* $c(x^{\frac{a}{b}})$ *in* $F_2[x;\frac{a}{b}\mathbb{N}_0]$, *and*

4) $C_{bn}=(g(x^{\frac{a}{b}}))$.

Conversely, if C_{bn} *is the ideal generated by* $p(x^{\frac{a}{b}})\in F_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$, *then* $p(x^{\frac{a}{b}})$ *is a generalized polynomial of least degree in* C_{bn} *if and only if* $p(x^{\frac{a}{b}})$ *divides* $(x^{\frac{a}{b}})^{bn}-1$ *in* $F_2[x;\frac{a}{b}\mathbb{N}_0]$.

Similar to [N], the following Theorem gives the generator matrix of the binary cyclic code C_{bn}.

Theorem 3: *Let* $C_{bn}\subset F_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$ *be a binary cyclic code with generator polynomial*

$$g(x^{\frac{a}{b}})=g_0+g_{\frac{a}{b}}(x^{\frac{a}{b}})^b+g_{2\frac{a}{b}}(x^{\frac{a}{b}})^{2b}+\cdots+g_{r\frac{a}{b}}(x^{\frac{a}{b}})^{br},\ g_{r\frac{a}{b}}=1. \quad (8)$$

Then C_{bn} *is of dimension* $bk=b(n-r)$, *which has a generator matrix of order* $bk\times bn$ *given by:*

$$G_{br}=\begin{bmatrix} g_0 & 0 & \cdots & 0 & g_{\frac{a}{b}} & 0 & \cdots & 0 & \cdots & g_{r\frac{a}{b}} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & 0 & \cdots & 0 & g_{\frac{a}{b}} & 0 & \cdots & 0 & \cdots & g_{r\frac{a}{b}} & 0 & \cdots & 0 \\ \vdots & \vdots & & & & & & & \vdots & & & & & \vdots \\ 0 & \cdots & 0 & g_0 & 0 & \cdots & 0 & g_{\frac{a}{b}} & 0 & \cdots & 0 & \cdots & 0 & g_{r\frac{a}{b}} \end{bmatrix} \quad (9)$$

The sequence $0\cdots0$ *between* g_i*'s in* G_{br} *has length* $b-1$.

Definition 3: *The generalized polynomial* $h(x^{\frac{a}{b}})$, *such that* $(x^{\frac{a}{b}})^n-1=g(x^{\frac{a}{b}})h(x^{\frac{a}{b}})$, *is called the check generalized polynomial of binary cyclic code* $C_{bn}\subset F_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$, *where* $g(x^{\frac{a}{b}})$ *is the generator generalized polynomial of* C_{bn}.

Theorem 4: *Let* C_{bn} *be a* bn *length binary cyclic code in* $F_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$ *with check generalized polynomial* $h(x^{\frac{a}{b}})$. *Then* $a(x^{\frac{a}{b}})\in C_{bn}$, *where* $a(x^{\frac{a}{b}})\in F_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$, *if and only if* $a(x^{\frac{a}{b}})*h(x^{\frac{a}{b}})=0$.

The following Theorem gives a parity check matrix for a binary cyclic code C_{bn} in $F_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$.

Theorem 5: *Let* C_{bn} *be a binary cyclic* (bn,bk) *code with check generalized polynomial*

$$h(x^{\frac{a}{b}})=h_0+h_{\frac{a}{b}}(x^{\frac{a}{b}})^b+\cdots+h_{\frac{a}{b}k}(x^{\frac{a}{b}})^{bk},\ h_{\frac{a}{b}k}=1. \quad (10)$$

Then the $b(n-k)\times bn$ *matrix given by:*

$$H_{bk}=\begin{bmatrix} h_{\frac{a}{b}k} & 0 & \cdots & 0 & h_{\frac{a}{b}(k-1)} & \cdots & & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_{\frac{a}{b}k} & 0 & \cdots & 0 & h_{\frac{a}{b}(k-1)} & \cdots & & \cdots & h_0 & 0 & \cdots 0 \\ \vdots & \vdots & & & & & & \vdots & & & & \\ 0 & \cdots & 0 & h_{\frac{a}{b}k} & 0 & \cdots & 0 & h_{\frac{a}{b}(k-1)} & \cdots & & \cdots & h_0 \end{bmatrix} \tag{11}$$

is a parity check matrix for C_{bn} *and the sequence* $0\cdots0$ *in* H_{bk} *has length* $b-1$.

Remark 1: *All of the above results follow for* $F_2[x;aN_0]$, *by taking* $b=1$.

Now shift the generalized polynomial $f(x^{\frac{a}{b}})$ of arbitrary degree n in $F_2[x;\frac{a}{b}N_0]$ to a generalized polynomial $f(x^{\frac{1}{b}})$ in $F_2[x;\frac{1}{b}N_0]$ as

$$f(x^{\frac{1}{b}})= f_0 + f_{\frac{1}{b}}(x^{\frac{1}{b}})^a + f_{\frac{2}{b}}(x^{\frac{1}{b}})^{2a} +\cdots+ f_{\frac{n}{b}}(x^{\frac{1}{b}})^{an}. \tag{12}$$

The degree of an arbitrary generalized polynomial in $F_2[x;\frac{a}{b}N_0]$ has exceeded from n to an in $F_2[x;\frac{1}{b}N_0]$. Consequently, the degree of the generator generalized polynomial $g((x^{\frac{1}{b}}))$ also exceeds from $r'=br$ to $r''=abr$, where $g(x^{\frac{1}{b}})$ divides $(x^{\frac{1}{b}})^{abn}-1$ and generates a binary cyclic (abn,abk) code C_{abn} in $F_2[x;\frac{1}{b}N_0]_{abn}$.

Thus, from the generator and parity check matrices of the code C_{bn} we obtain the generator and parity check matrices of the code C_{abn}.

Theorem 6: *Let* $C_{abn}\subset F_2[x;\frac{1}{b}N_0]_{abn}$ *be a binary cyclic code with generator polynomial*

$$g((x^{\frac{1}{b}}))=g_0+g_{\frac{1}{b}}(x^{\frac{1}{b}})^{ab}+g_{\frac{2}{b}}(x^{\frac{1}{b}})^{2b}+\cdots+g_{\frac{r}{b}}(x^{\frac{a}{b}})^{br},\ g_{\frac{r}{b}}=1. \tag{13}$$

Then C_{abn} *is of dimension* $abk=ab(n-r)$, *which has a generator matrix of order* $abk\times abn$ *given by*

$$G_{abr}=\begin{bmatrix} g_0 & 0 & \cdots & 0 & g_{\frac{1}{b}} & 0 & \cdots & 0 & \cdots & g_{\frac{r}{b}} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & 0 & \cdots & 0 & g_{\frac{1}{b}} & 0 & \cdots & 0 & \cdots & g_{\frac{r}{b}} & 0 & \cdots & 0 \\ \vdots & \vdots & & & & & & & \vdots & & & & & \vdots \\ 0 & \cdots & 0 & g_0 & 0 & \cdots & 0 & g_{\frac{1}{b}} & 0 & \cdots & 0 & \cdots & 0 & g_{\frac{r}{b}} \end{bmatrix} \tag{14}$$

Where the sequence $0\cdots0$ *between* g_i*'s in* G_{abr} *has length* $ab-1$.

Theorem 7: *Let* C_{abn} *be a binary cyclic* (abn,abk) *code with check generalized polynomial*

$$h(x^{\frac{1}{b}})=h_0+h_{\frac{1}{b}}(x^{\frac{1}{b}})^{ab}+\cdots+h_{\frac{k}{b}}(x^{\frac{1}{b}})^{abk},\ h_{\frac{k}{b}}=1. \tag{15}$$

Then the $ab(n-k)\times abn$ *matrix given by*

$$H_{abk}=\begin{bmatrix} h_{\frac{k}{b}} & 0 & \cdots & 0 & h_{\frac{(k-1)}{b}} & \cdots & & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_{\frac{k}{b}} & 0 & \cdots & 0 & h_{\frac{(k-1)}{b}} & \cdots & & \cdots & h_0 & 0 & \cdots 0 \\ \vdots & \vdots & & & & & & \vdots & & & & \\ 0 & \cdots & 0 & h_{\frac{k}{b}} & 0 & \cdots & 0 & h_{\frac{(k-1)}{b}} & \cdots & & \cdots & h_0 \end{bmatrix} \tag{16}$$

is a parity check matrix for C_{abn} *and the sequence* $0\cdots0$ *between* h_i*'s in* H_{abk} *has length* $ab-1$.

Example 1: *Let* $g(x^2)=1+(x^2)+(x^2)^2\in F_2[x;2N_0]$ *be the generalized polynomial with degree* $r=2$ *and divides* $(x^2)^3-1$. *Clearly* $g(x^2)$ *generates a binary cyclic* $(3,1)$ *code in* $F_2[x;2N_0]_3$ *which has a generator matrix*

$$G_2 = [1 \quad 1 \quad 1]. \tag{17}$$

In $F_2[x]$, *the polynomial* $g(x^2) = g(x) = 1 + x^2 + x^4$ has degree $4 = 2r$ and divides $x^6 - 1$. *Therefore, generates a binary cyclic* $(6,2)$ *code in* $F_2[x]_6$ *which has a generator matrix*

$$G_4 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \tag{18}$$

Since $(x^2)^3 - 1 = (1 + x^2 + (x^2)^2)(1 + (x^2))$, *it follows that* $h(x^2) = 1 + (x^2)$ *is the parity check generalized polynomial of* $(3,1)$ *code in* $F_2[x;2\mathbb{N}_0]_3$. *This gives the parity check matrix*

$$H_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}. \tag{19}$$

In $F_2[x]$, $(x^2)^3 - 1$ *becomes* $x^6 - 1 = (1 + x^2 + x^4)(1 + x^2)$. *Hence* $h(x) = 1 + x^2$ *is the parity check polynomial of* $(6,2)$ *code and the corresponding parity check matrix is*

$$H_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}. \tag{20}$$

Let $g(x^{\frac{2}{3}}) = 1 + (x^{\frac{2}{3}})^3 + (x^{\frac{2}{3}})^6$ *be a generator generalized polynomial of degree* 6 *and it divides* $(x^{\frac{2}{3}})^9 - 1$, *then* $g(x^{\frac{2}{3}})$ *generates a binary cyclic* $(9,3)$ *code with generator matrix*

$$G_6 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}. \tag{21}$$

Whereas, in $F_2[x;\frac{1}{3}\mathbb{N}_0]$, $g(x^{\frac{2}{3}})$ *becomes* $g((x^{\frac{1}{3}})) = 1 + (x^{\frac{1}{3}})^6 + (x^{\frac{1}{3}})^{12}$ *and has degree* 12 *and divides* $(x^{\frac{1}{3}})^{18} - 1$. *Thus, it generates a cyclic* $(18,6)$ *code having generator matrix*

$$G_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{22}$$

The parity check generalized polynomials are

$$h(x^{\frac{2}{3}}) = 1 + (x^{\frac{2}{3}})^3 \text{ and } h((x^{\frac{1}{3}})) = 1 + (x^{\frac{1}{3}})^6. \tag{23}$$

Which give the following parity check matrices

$$H_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \text{ and} \tag{24}$$

(25)

$$H_4 = \begin{bmatrix} 1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0\\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1 \end{bmatrix}$$

4. Relationship among the cyclic codes C_n, C_{an}, C_{bn} and C_{abn}

In this section, we demonstrate the association between the binary cyclic codes C_n, C_{an}, C_{bn} and C_{abn} by two ways:

(i) Using the technique of interleaving,. (ii) Through the generator and parity check matrices of the binary cyclic codes C_n, C_{an},, C_{bn} and C_{abn}.

Relationship of C_n, C_{an}, C_{bn} and C_{abn} by interleaving

For a given (n,k) cyclic code, a $(\beta n, \beta k)$ cyclic code can be constructed by interleaving. This is done by simply arranging β code vectors in the original code into β rows of a rectangular array and then transmitting them column by column. In this way a codeword of βn digits is obtained whose two consecutive bits are now separated by $\beta - 1$ positions. The parameter β is called *interleaving degree*.

Proposition 1: *The codes C_{an}, C_{bn} and C_{abn} are interleaved codes of degree a, b and ab respectively, where the code C_n is the base code.*

Proof: Take a code vectors from the base code C_n and arrange them into a rows of an $a \times n$ array. Then by transmitting this code array column by column in serial manner we get the binary cyclic code C_{an}. Similarly, the binary cyclic code C_{bn} is obtained by taking b code vectors from the base code C_n, arranging them into b rows of an $b \times n$ array and then transmitting it column by column in serial manner. In this way codewords of an and bn digits are obtained whose two consecutive bits are now separated by $a-1$ and $b-1$ positions respectively. Now, by arranging ab code vectors from the code C_n and arranging them into ab rows of an $ab \times n$ array and then transmitting it column by column, the binary cyclic code C_{abn} is obtained. This gives codewords of abn digits whose two consecutive bits are separated by $ab-1$ positions.

Example 2: *In Example 1, the $(3,1)$ code C_3 acts as a base code. The code C_6 is obtained by arranging 2 codewords 111 and 000 in C_3 into 2 rows of an 2×3 array, that is:*

$$\begin{matrix} 1 & 1 & 1 \\ 0 & 0 & 0 \end{matrix}, \qquad (26)$$

and then by transmitting this code array column by column we get 101010, which is a codeword in C_6. Similarly, by arranging 3 and 6 codewords in C_3 into 3 and 6 rows of an 3×3 and 6×3 arrays, that is:

$$\begin{matrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{matrix} \quad \text{and} \quad \begin{matrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{matrix}, \tag{27}$$

we get the codewords by transmitting them column by column 101101101 and 0100010100 01010001 in C_9 and C_{18}.

Relationship of C_n, C_{an}, C_{bn} and C_{abn} by the generator and parity check matrices

Now, we explain the relationship between the codes C_n, C_{an}, C_{bn} and C_{abn} through their generator and parity check matrices, using the notion of direct sum of codes.

Definition 4: [6] *(a) Let C_i be an (n_i, k_i) code, where $i\in\{1,2\}$, both having symbols from the same Galois field $\mathbb{F}_q$. Then their direct sum*

$C_1 \oplus C_2 = \{(c_1, c_2) \mid c_1 \in C_1, c_2 \in C_2\}$ *is a* (n_1+n_2, k_1+k_2) *code.*

(b) For $i\in\{1,2\}$, if C_i has generator matrix G_i and parity check matrix H_i, then

$$G_1 \oplus G_2 = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix} \text{ and } H_1 \oplus H_2 = \begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix} \tag{28}$$

are the generator and parity check matrices for the code $C_1 \oplus C_2$.

The following result explains the relationship between the binary cyclic codes C_n, C_{an}, C_{bn} and C_{abn} through their generator matrices.

Theorem 8: *Let G_r, G_{ar}, G_{br}, and G_{abr}, be the generator matrices corresponding to the generator generalized polynomials*

$g(x^a)=1+(x^a)+\cdots+(x^a)^r$, $g(x)=1+x^a+\cdots+x^{ar}$, $g(x^{\frac{a}{b}})=1+(x^{\frac{a}{b}})^b+\cdots+(x^{\frac{a}{b}})^{br}$ and $g((x^{\frac{1}{b}})^a)=1+(x^{\frac{1}{b}})^{ab}+\cdots(x^{\frac{1}{b}})^{abr}$

of the binary cyclic codes C_n, C_{an}, C_{bn} and C_{abn} in $\mathbb{F}_2[x;a\mathbb{N}_0]_n$, $\mathbb{F}_2[x]_{an}$, $\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$ and $\mathbb{F}_2[x;\frac{1}{b}\mathbb{N}_0]_{abn}$. Then the following conditions hold.

1) $G_{ar} \sim \oplus_1^a G_r$,

2) $G_{br} \sim G_r \oplus G_{ar} \sim \oplus_1^b G_r$, *and*

3) $G_{abr} \sim \oplus_1^a G_{br} \sim \oplus_1^a G_r \oplus G_{ar} \sim \oplus_1^{ab} G_r$.

Proof: *As $g(x^a)=1+(x^a)+\cdots+(x^a)^r$ divides $(x^a)^n-1$ in $\mathbb{F}_2[x;a\mathbb{N}_0]$, therefore the generator matrix G_r has order $k\times n$, where $k=n-r$ In $\mathbb{F}_2[x]$, the generalized polynomial $g(x^a)=g(x)=1+x^a+\cdots+x^{ar}$ divides $x^{an}-1$. Consequently, a generator matrix G_{ar} of order $ak\times an$ is obtained which after some suitable column operations becomes*

$$G_{ar} \sim \begin{bmatrix} G_r & 0 & \cdots & 0 \\ 0 & G_r & 0\cdots & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & G_r \end{bmatrix}_{a(k\times n)} \quad (29)$$

This implies that G_{ar} *contains* a *blocks of* G_r *at its main diagonal and hence* $G_{ar} \sim \oplus_1^a G_r$ *Similarly,* $g(x^{\frac{a}{b}}) = 1 + (x^{\frac{a}{b}}) + \cdots + (x^{\frac{a}{b}})^{br}$ *divides* $x^{bn} - 1,$ *which have generator matrix* G_{br} *of order* $bk \times bn$*. On applying suitable column operations, blocks of* G_{ar} *and* G_r *are obtained at the main diagonal of* G_{br}

$$G_{br} \sim \begin{bmatrix} G_{ar} & 0 \\ 0 & G_r \end{bmatrix}_{(a+1)(k\times n)} \quad (30)$$

Putting the value of G_{ar} from (31) in (32) we get,

$$G_{br} \sim \begin{bmatrix} G_r & 0 & \cdots & 0 \\ 0 & G_r & 0\cdots & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & G_r \end{bmatrix}_{(a+1)(k\times n)}. \quad (31)$$

The generator polynomial $g((x^{\frac{1}{b}})^a) = 1 + (x^{\frac{1}{b}})^{ab} + \cdots + (x^{\frac{1}{b}})^{abr}$ divides $x^{abn} - 1$ and gives a generator matrix G_{abr} of order $abk \times abn$ which after suitable column operations gives

$$G_{abr} \sim \begin{bmatrix} G_{br} & 0 & \cdots & 0 \\ 0 & G_{br} & 0\cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & G_{br} \end{bmatrix}_{a(bk\times bn)}. \quad (32)$$

Putting the value of G_{br} from (33) we get

$$G_{abr} \sim \begin{bmatrix} G_r & 0 & \cdots & 0 \\ 0 & G_r & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & G_r \end{bmatrix}_{ab(k\times n)}, \quad (33)$$

which shows that G_{abr} *contains* ab *blocks of* G_r *, that is,* $G_{abr} \sim \oplus_1^{ab} G_r$.

The following example illustrates Theorem 8.

Example 3: *Let* $a = 2,\ b = 3$ *and* $r = 2$. *From Example 1 equation 24 we get the generator matrix* G_{12} *which after applying some suitable column operations becomes:*

$$G_{12} \sim \begin{bmatrix} 1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1 \end{bmatrix} \quad (34)$$

By Example 1 equation 14 *it is clear that* $G_{12} \sim G_6 \oplus G_6$.

Again on applying suitable column operations on G_6*, it gives*

$$G_6 \sim \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \sim G_4 \oplus G_2 \quad (35)$$

and similarly G_4 *becomes*

$$G_4 \sim \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \sim G_2 \oplus G_2. \quad (36)$$

So, $G_6 \sim G_2 \oplus G_2 \oplus G_2$ and $G_{12} \sim G_2 \oplus G_2 \oplus G_2 \oplus G_2 \oplus G_2 \oplus G_2$.

Encoding: In the matrix G_{abr}, the matrices G_{br}, G_{ar} and G_r exist as block matrices and the generator generalized polynomial of the cyclic (abn, abk) code C_{abn} can be used for encoding. So, a message word $u \in \mathbb{F}_2^{abk}$ is encoded as uG_{abr}. Hence the code $C_{abr} = \{uG_{abr} : u \in F_2^{abk}\}$. On partitioning u as $u = (u_{1\times b} : u_{1\times a} : u_{1\times k})$, where $u_{1\times b} \in \mathbb{F}_2^{bk}$, $u_{1\times a} \in \mathbb{F}_2^{ak}$ and $u_{1\times k} \in F_2^k$, we get $C_{abr} \sim \{u_{1\times b}G_{br} : u_{1\times a}G_{ar} : u_{1\times k}G_r\}$.

Example 4: *Let* $a = 2$, $b = 3$ *and* $r = 2$, *then* $u \in F_2^6$ *is given by* $u = [1 \ 1 \ 0 \ 0 \ 1 \ 1]$. *The row matrix* u *has order* 1×6. *By partitioning the matrix* u *we get* $u = [1 \ 1 \ 0]_{1\times 3} : [0 \ 1]_{1\times 2} : [1]_{1\times 1} = [u_1 : u_2 : u_3]$ *and*

$$\begin{aligned} uG_{12} &= [u_1 G_{6_{(3\times 9)}} : u_2 G_{4_{(2\times 6)}} : u_3 G_{2_{(1\times 3)}}] \\ &= 110110110010101111 \end{aligned} \quad (37)$$

Thus, the message word u *is encoded as the codeword* uG_{12}.

For parity check matrix, Theorem 8 doesn't hold, whereas it holds for the canonical parity check matrix. In general, for a linear code, a generator matrix G is transformed into the canonical form by applying elementary row operations. But, in the case of a cyclic code, the canonical form can be obtained by using the generator generalized polynomial and the division algorithm in the Euclidean domain $\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]$. For any generalized polynomial $f(x^{\frac{a}{b}}) \in \mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]$, let $r(f(x^{\frac{a}{b}}))$ denote the remainder on dividing $f(x^{\frac{a}{b}})$ by $g(x^{\frac{a}{b}})$.

Theorem 9: *Let* $g(x^{\frac{a}{b}})$ *be the generator generalized polynomial of a binary cyclic* (bn, bk) *code* C_{bn} *in* $\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$ *and* A_{br} *be a* $bk \times b(n-k)$ *matrix whose* i*-th row is* $r((x^{\frac{a}{b}})^{b(n-k)+i-1})$, *for* $i = 1, \cdots, k$. *Then the canonical generator and parity check matrices of* C_{bn} *respectively are*

$$G_{br} = [I_{bk} \ \vdots \ A_{br}] \text{ and } H_{bk} = [(A_{br})^T \ \vdots \ I_{b(n-k)}]. \quad (38)$$

Theorem 10: *Let* A_r, A_{ar}, A_{br} *and* A_{abr} *be the matrices as taken in Theorem 9 with respect to the corresponding generator (generalized) polynomials* $g(x^a)$, $g(x)$, $g(x^{\frac{a}{b}})$ *and* $g((x^{\frac{1}{b}}))$ *in* $\mathbb{F}_2[x;a\mathbb{N}_0]_n$, $\mathbb{F}_2[x]_{an}$, $\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$ *and* $\mathbb{F}_2[x;\frac{1}{b}\mathbb{N}_0]_{abn}$ *respectively. Then*

1) $A_{ar} \sim \oplus_1^a A_r$, 2) $A_{br} \sim A_r \oplus A_{ar} \sim \oplus_1^b A_r$, *and* 3) $A_{abr} \sim \oplus_1^a A_{br} \sim \oplus_1^a A_r \oplus A_{ar} \sim \oplus_1^{ab} A_r$.

Proof: For the generator generalized polynomial $g(x^a) = 1 + (x^a) + \cdots + (x^a)^r$, the remainders $r(x^a)^j$, where $n-k \le j \le n-1$ give the matrix A_r of order $k \times (n-k)$.

Similarly, for $g(x)=1+x^a+\cdots+x^{ar}$, the matrix A_{ar} of order $ak\times a(n-k)$ is obtained through the remainders $r(x^j)$, where $a(n-k)\le j\le an-1$. After applying suitable column operations on A_{ar}, it gives

$$A_{ar} \sim \begin{bmatrix} A_r & 0 & 0\cdots & 0 \\ 0 & A_r & 0\cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & A_r \end{bmatrix}_{a(k\times n-k)} \sim \oplus_1^a A_r. \tag{39}$$

For the generator generalized polynomial $g(x^{\frac{a}{b}})=1+(x^{\frac{a}{b}})^b+\cdots+(x^{\frac{a}{b}})^{br}$, the remainders $r((x^{\frac{a}{b}})^j)$ gives the matrix A_{br} of order $bk\times b(n-k)$, where $b(n-k)\le j\le b(n-1)$. On applying suitable column operations it gives submatrices of order $ak\times a(n-k)$ and $k\times n-k$, that is,

$$A_{br} \sim \begin{bmatrix} A_{ar} & O \\ O & A_r \end{bmatrix}_{(a+1)(k\times n-k)} \sim A_r\oplus A_{ar} \sim \oplus_1^{a+1=b} A_r. \tag{40}$$

Finally, for $g((x^{\frac{1}{b}})^a)=1+(x^{\frac{1}{b}})^{ab}+\cdots+(x^{\frac{1}{b}})^{abr}$, the remainders $r((x^{\frac{1}{b}})^j)$, where $ab(n-k)\le j\le ab(n-1)$ gives A_{abr} of order $abk\times ab(n-k)$. Which on applying suitable column operations gives submatrices of order $bk\times b(n-k)$, that is,

$$A_{abr} \sim \begin{bmatrix} A_{br} & 0\cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A_{br} \end{bmatrix}_{a(bk\times b(n-k))} \sim \oplus_1^a A_{br} \sim \oplus_1^a A_r\oplus A_{ar} \sim \oplus_1^{ab} A_r, \tag{41}$$

which proves the theorem.

The following example illustrates Theorem 10.

Example 5: *To find the parity check matrix for* $(18,6)$ *code obtained by the monoid ring* $F_2[x;\frac{1}{3}N_0]$, *we first divide* $(x^{\frac{1}{3}})^j$ *by* $g((x^{\frac{1}{3}}))=1+(x^{\frac{1}{3}})^6+(x^{\frac{1}{3}})^{12}$, *where* $j=12,13,\cdots,17$, *to get the remainders*

$$\begin{gathered} r(x^{\frac{1}{3}})^{12}=1+(x^{\frac{1}{3}})^6,\ r(x^{\frac{1}{3}})^{13}=(x^{\frac{1}{3}})+(x^{\frac{1}{3}})^7, \\ r(x^{\frac{1}{3}})^{14}=(x^{\frac{1}{3}})^2+(x^{\frac{1}{3}})^8,\ r(x^{\frac{1}{3}})^{15}=(x^{\frac{1}{3}})^3+(x^{\frac{1}{3}})^9, \\ r(x^{\frac{1}{3}})^{16}=(x^{\frac{1}{3}})^4+(x^{\frac{1}{3}})^{10},\ r(x^{\frac{1}{3}})^{17}=(x^{\frac{1}{3}})^5+(x^{\frac{1}{3}})^{11}. \end{gathered} \tag{42}$$

Therefore,

$$A_{12}=\begin{bmatrix} 1&0&0&0&0&0&1&0&0&0&0&0 \\ 0&1&0&0&0&0&0&1&0&0&0&0 \\ 0&0&1&0&0&0&0&0&1&0&0&0 \\ 0&0&0&1&0&0&0&0&0&1&0&0 \\ 0&0&0&0&1&0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0&0&0&0&0&1 \end{bmatrix}. \tag{43}$$

Accordingly,

$$H_{12}=\left[(A_{12})^T\ \vdots\ I_{12}\right]. \tag{44}$$

Similarly,

$$A_6=\begin{bmatrix} 1&0&0&1&0&0 \\ 0&1&0&0&1&0 \\ 0&0&1&0&0&1 \end{bmatrix},\ A_4=\begin{bmatrix} 1&0&1&0 \\ 0&1&0&1 \end{bmatrix} \text{ and } A_2=\begin{bmatrix}1 & 1\end{bmatrix} \text{ gives} \tag{45}$$

$$H_6 = [(A_6)^T \ \vdots \ I_6],\ H_4 = [(A_4)^T \ \vdots \ I_4] \text{ and } H_2 = [(A_2)^T \ \vdots \ I_2]. \quad (46)$$

Thus by Theorem 10,

$$H_{12} = [\oplus_1^2 (A_6)^T \ \vdots \ I_{12}],\ H_6 = [(A_2)^T \oplus (A_4)^T \ \vdots \ I_6] \text{ and } H_4 = [\oplus_1^2 A_2 \ \vdots \ I_4]. \quad (47)$$

5. Decoding procedure

The codes C_n, C_{an}, C_{bn} and C_{abn} have the same minimum distance and hence the same error correction capability along with the same code rate, but as it is shown in section sec4, the codes C_{an}, C_{bn} and C_{abn} are interleaved codes of degree a,b and ab, where the base code C_n is cyclic. Thus, if the initial code C_n is capable of correcting t errors, then the interleaved codes C_{an}, C_{bn} and C_{abn} are capable of correcting t bursts of length a,b and ab or less, no matter where it starts, will affect no more than t bits in each row. This t bits error in each row will be corrected by the base code C_n. If C_n is capable of correcting all bursts of length l or less, then the interleaved codes C_{an}, C_{bn} and C_{abn} are capable of correcting all bursts of length al, bl and abl or less.

We give decoding scheme only for the code C_{bn}, through which decoding of C_n and C_{an} can easily be obtained. Decoding of the code C_{abn} can be obtained by shifting $(x^{\frac{a}{b}})$ to $(x^{\frac{1}{b}})^a$.

The following theorem gives the syndrome for binary cyclic codes C_{bn} through its canonical parity check matrix H_{bk}.

Theorem 11: *Let C_{bn} be a binary cyclic (bn,bk) code in $\mathbb{F}_2[x;\frac{a}{b}\mathbb{N}_0]_{bn}$ with generator polynomial $g(x^{\frac{a}{b}})$ and the canonical parity check matrix H_{bk}. Then, for any vector $c \in \mathbb{F}_2^{bn}$, the syndrome $S(c) = r((x^{\frac{a}{b}})^{b(n-k)}c(x^{\frac{a}{b}}))$.*

In a similar way, we get the syndromes for the binary cyclic codes C_{abn} and C_{an} through their canonical parity check matrices H_{abk} and H_{ak}.

In a binary cyclic code C_{bn}, with generator generalized polynomial $g(x^{\frac{a}{b}})$, two vectors $c,d \in \mathbb{F}_2^{bn}$ lie in the same coset if and only if $g(x^{\frac{a}{b}})$ divides $c(x^{\frac{a}{b}}) - d(x^{\frac{a}{b}})$, that is, $r(c(x^{\frac{a}{b}})) = r(d(x^{\frac{a}{b}}))$. Let $v(x^{\frac{a}{b}}) \in C_{bn}$ be a generalized code polynomial, and $u(x^{\frac{a}{b}})$ be a generalized received polynomial. Then, $v(x^{\frac{a}{b}}) = u(x^{\frac{a}{b}}) - e(x^{\frac{a}{b}})$, where $e(x^{\frac{a}{b}})$ is a generalized error polynomial. Then their syndromes $S(v) = S(u) - S(e)$ implies $S(u) = S(e)$ as $S(v) = 0$. Based on the previous discussion, we deduce the following decoding steps.

Decoding Algorithm

1) For the received vector $u = (u_0, u_{\frac{a}{b}}, \cdots, u_{\frac{a}{b}(bn-1)}) \in \mathbb{F}_2^{bn}$ with generalized received

polynomial $u(x^{\frac{a}{b}}) = u_0 + u_{\frac{a}{b}}(x^{\frac{a}{b}}) + \cdots + u_{\frac{a}{b}(bn-1)}(x^{\frac{a}{b}})^{(bn-1)}$, find the syndrome $S(u) = r((x^{\frac{a}{b}})^{b(n-k)}u(x^{\frac{a}{b}}))$.

2) Construct a syndrome table for the generalized error polynomials.
3) Verify by the table that for which i, where $1 \le i \le n-1$, $S(u) = S(e_i)$. Then the generalized error polynomial $e_i(x^{\frac{a}{b}})$ for the generalized received polynomial $u(x^{\frac{a}{b}})$ is obtained.
4) Consequently, $v(x^{\frac{a}{b}}) = u(x^{\frac{a}{b}}) - e(x^{\frac{a}{b}})$ is the generalized decoded code polynomial of the binary cyclic code C_{bn}.
5) The received interleaved sequence in C_{bn} is de-interleaved and rearranged back to a rectangular array of b rows of the binary cyclic code C_n. Then each row is decoded based on binary cyclic code C_n.

Example 6: In Example 1, the $(3,1)$ code acts as a base code capable of correcting single error. Let $n=9$, $k=3$ and $g(x^{\frac{2}{3}}) = 1 + (x^{\frac{2}{3}})^3 + (x^{\frac{2}{3}})^6 \in F_2[x; \frac{2}{3}N_0]_{3n}$ be the generator generalized polynomial. Let $u(x^{\frac{2}{3}}) = 1 + (x^{\frac{2}{3}}) + (x^{\frac{2}{3}})^6 \in F_2[x; \frac{2}{3}N_0]_9$ be the generalized received polynomial, then following are the syndrome tables of error generalized polynomials $e_i(x^{\frac{2}{3}})$, for $0 \le i \le 8$ and $e_i(x^{\frac{1}{3}})$, for $0 \le i \le 17$:

Syndrome Table I

$e_i(x^{\frac{2}{3}})$	$e(x^{\frac{2}{3}})$	$S(e)$
$e_0(x^{\frac{2}{3}})$	1	$1+(x^{\frac{2}{3}})^3$
$e_1(x^{\frac{2}{3}})$	$x^{\frac{2}{3}}$	$(x^{\frac{2}{3}})+(x^{\frac{2}{3}})^4$
$e_2(x^{\frac{2}{3}})$	$(x^{\frac{2}{3}})^2$	$(x^{\frac{2}{3}})^2+(x^{\frac{2}{3}})^5$
$e_3(x^{\frac{2}{3}})$	$(x^{\frac{2}{3}})^3$	1
$e_4(x^{\frac{2}{3}})$	$(x^{\frac{2}{3}})^4$	$(x^{\frac{2}{3}})$
$e_5(x^{\frac{2}{3}})$	$(x^{\frac{2}{3}})^5$	$(x^{\frac{2}{3}})^2$
$e_6(x^{\frac{2}{3}})$	$(x^{\frac{2}{3}})^6$	$(x^{\frac{2}{3}})^3$
$e_7(x^{\frac{2}{3}})$	$(x^{\frac{2}{3}})^7$	$(x^{\frac{2}{3}})^4$
$e_8(x^{\frac{2}{3}})$	$(x^{\frac{2}{3}})^8$	$(x^{\frac{2}{3}})^5$

Syndrome Table II

$e_i(x^{\frac{1}{3}})$	$e(x^{\frac{1}{3}})$	$S(e)$
$e_{0,1}(x^{\frac{1}{3}})$	1	$1+(x^{\frac{1}{3}})^6$
$e_{2,3}(x^{\frac{1}{3}})$	$(x^{\frac{1}{3}})^2$	$(x^{\frac{1}{3}})^2+(x^{\frac{1}{3}})^8$
$e_{4,5}(x^{\frac{1}{3}})$	$(x^{\frac{1}{3}})^4$	$(x^{\frac{1}{3}})^4+(x^{\frac{1}{3}})^{10}$
$e_{6,7}(x^{\frac{1}{3}})$	$(x^{\frac{1}{3}})^6$	1
$e_{8,9}(x^{\frac{1}{3}})$	$(x^{\frac{1}{3}})^8$	$(x^{\frac{1}{3}})^2$
$e_{10,11}(x^{\frac{1}{3}})$	$(x^{\frac{1}{3}})^{10}$	$(x^{\frac{1}{3}})^4$
$e_{12,13}(x^{\frac{1}{3}})$	$(x^{\frac{1}{3}})^{12}$	$(x^{\frac{1}{3}})^6$
$e_{14,15}(x^{\frac{1}{3}})$	$(x^{\frac{1}{3}})^{14}$	$(x^{\frac{1}{3}})^8$
$e_{16,17}(x^{\frac{1}{3}})$	$(x^{\frac{1}{3}})^{16}$	$(x^{\frac{1}{3}})^{10}$

From the Syndrome Table I we find that $S(u) = S(e_1) + S(e_3)$. So the generalized error polynomial is $e(x^{\frac{2}{3}}) = (x^{\frac{2}{3}}) + (x^{\frac{2}{3}})^3$ which has error pattern $e = 010100000$, which is a burst of length 3. Therefore, $v(x^{\frac{2}{3}}) = u(x^{\frac{2}{3}}) - e(x^{\frac{2}{3}}) = 1 + (x^{\frac{2}{3}})^3 + (x^{\frac{2}{3}})^6$, which is the generator generalized polynomial of the code C_9, its vector form is 100100100. Now, on shifting the generalized received polynomial $u(x^{\frac{2}{3}}) = 1 + (x^{\frac{2}{3}}) + (x^{\frac{2}{3}})^6$ to $u(x^{\frac{1}{3}}) = 1 + (x^{\frac{1}{3}})^2 + (x^{\frac{1}{3}})^{12} \in F_2[x; \frac{1}{3}N_0]_{18}$,

we get the received word $u = 101000000000100000$ in C_{18}. The syndrome of $u(x^{\frac{1}{3}})$ is $S(u) = (x^{\frac{1}{3}})^8 + (x^{\frac{1}{3}})^2 + 1$. From the Syndrome Table II we get $S(u) = S(e_{2,3}(x^{\frac{1}{3}})) + S(e_{6,7}(x^{\frac{1}{3}}))$. This gives the generalized error polynomial $e(x^{\frac{1}{3}}) = (x^{\frac{1}{3}}) + (x^{\frac{1}{3}})^6$ which has error pattern $e = 001000100000000000$, which is a burst of length 5.

Therefore, $v(x^{\frac{1}{3}})=u(x^{\frac{1}{3}})-e(x^{\frac{1}{3}})=1+(x^{\frac{1}{3}})^6+(x^{\frac{1}{3}})^{12}$, is the generator generalized polynomial of the binary cyclic code C_{18}, and its vector form is 1000001000 00100000 . The vector u in C_9 is formed by interleaving 3 rows $u_1=101$, $u_2=100$ and $u_3=000$ in C_3 which have respectively the error vectors $e_1=010$, $e_2=100$ and $e_3=000$. On interleaving the vectors $u_1=101$ and $u_2=100$ in C_3, we get a received vector $u=110010$ in C_6. Its decoding gives the error vector $e=011000$ which is a burst of length 2 . Hence, the interleaved codes $(18,6)$, $(9,3)$ and $(6,2)$ are capable of correcting single burst of length 6, 3 and 2 or less.

6. Conclusions

In this study, a new technique of constructing binary cyclic codes is introduced using the monoid rings $F_2[x;aN_0]$, $F_2[x;\frac{a}{b}N_0]$ and $F_2[x;\frac{1}{b}N_0]$ instead of the polynomial ring $F_2[x]$. So, a scheme is articulated in such a manner that; for an n length binary cyclic code C_n, an ideal in the factor ring $F_2[x;aN_0]_n$; there exists binary cyclic codes C_{an}, C_{bn} and C_{abn} of lengths an, bn and abn. The pronouncements of this study are as follows:

1) The generator and parity check matrix of the binary cyclic code C_{abn} contains blocks of the generator and parity check matrices of the binary cyclic codes C_n, C_{an} and C_{bn}. Hence, encoding and decoding of all the binary cyclic codes C_n, C_{an} and C_{bn} can be done simultaneously by the encoding and decoding of the binary cyclic code C_{abn}.
2) The constructed binary cyclic codes C_{an}, C_{bn} and C_{abn} are interleaved codes of degree a, b and ab, respectively, where the binary cyclic code C_n is the base code. Therefore, if the base code C_n corrects t errors, then the interleaved codes C_{an}, C_{bn} and C_{abn} are capable of correcting t bursts of length a, b and ab or less. If C_n is capable of correcting all bursts of length l or less, then the interleaved codes C_{an}, C_{bn} and C_{abn} are capable of correcting all bursts of length al, bl and abl or less.

This study can further be extended to $q-array$ cyclic codes instead of $2-array$. Also, using the same monoid rings, the BCH codes can be constructed for better error correction capability.

REFERENCES

[1]. *N. Abramson*, A class of systematic codes for non-independent errors, IRE Trans. Inf. Theory, IT-**4**(4) (1959), 150-157.

[2]. *N. Abramson and B. Elspas*, Double-error-correcting coders and decoders for non-independent binary errors, presented at the UNESCO Inf. Process. Conf. Paris, (1959).

[3]. *A.A. Andrade, T. Shah and A. Khan*, A note on linear codes over semigroup rings, TEMA - Tend. Mat. Apl. Comput. **12**(2) (2011), 79-89.
[4]. *E.R. Berlekamp*, Algebraic coding theory, McGraw-Hill, NewYork, (1968).
[5]. *I.F. Blake and R.C. Mullin*, The mathematical theory of coding, Academic Press, New York, (1975).
[6]. *W.C. Huffman and Vera Pless*, Fundamentals of error-correcting codes, Cambridge University Press, (2003).
[7]. *T. Kasami*, Systematic codes using binary shift register sequences, J. info. Processing Soc. Japan **1** (1960), 198-200.
[8]. *T. Kasami, N. Tokura, Y. Iwadare, and Y. Inagaki*, Coding theory, Corona, Tokyo, (1974).
[9]. *A.V. Kelarev and P. Solé*, Error-correcting codes as ideals in group rings, *Contemp. Math.* 273 (2001), 11-18.
[10]. *A.V. Kelarev*, Ring Constructions and Applications, World Scientific, River Edge, (2002).
[11]. S. Lin, D.J. Costello, Jr., Error control coding fundamentals and Applications, Prentice-Hall, Inc., Englewood Cliffs, N. J., (1983).
[12]. *S.R. López-Permouth, B.R. Parra-Avila and S. Szabo*, Dual generalizations of the concept of cyclicity of codes. *Adv. Math. Commun.* **3**(3) (2009), 227-234.
[13]. S.R. López-Permouth and S. Szabo, Convolutional codes with additional algebraic structure, *J. Pure Appl. Algebra*, **217**(5) (2013), 958-972.
[14]. *S.R. López-Permouth and S. Szabo*, On the Hamming weight of repeated root cyclic and negacyclic codes over Galois rings. *Adv. in Math. of Comm.* **3**(4) (2009), 409-420.
[15]. *S.R. López-Permouth, H. Üzadam and S. Ferruh*, Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes, Finite Fields Th. App. **19** (2013), 16-38.
[16]. *S.R. Nagpaul, S.K. Jain*, Topics in Applied Abstract Algebra, Thomson, Brooks/Cole, (2005).
[17]. *W.W. Peterson*, Encoding and error-correction procedures for the Bose-Chaudhuri codes, *IRE Trans.* IT-6 (1960), 459-470.
[18]. *W.W. Peterson and E.J. Weddon*, Jr., Error correcting codes, 2nd edittion, MIT Press Cambridge, Mass., (1972).
[19]. *E. Prange*, Cyclic Error-correcting Codes in two Symbols (AFCRC-TN-57-103, Air force Cambridge research center, Cambridge, Mass. 1957).
[20]. *E. Prange*, *The Use of Coset Equivalence in the Analysis and Decoding of Group Codes* (AFCRC-TR-59-164, Air force Cambridge research center, Cambridge, Mass. 1959).
[21]. *T. Shah, Amanullah and A.A. Andrade*, A method for improving the code rate and error correction capability of a cyclic code, Comput. Appl. Math. **32**(2) (2013), 261-274.
[22]. *T. Shah, Amanullah and A.A. Andrade*, A decoding procedure which improves code rate and error corrections, JARAM. **4**(4) (2012), 37-50.
[23]. *T. Shah and A.A. Andrade*, Cyclic codes through $B[X]$, $B[X;\frac{1}{kp}Z_0]$ and $B[X;\frac{1}{p^k}Z_0]$: A comparison, J. Algebra Appl. **11**(4)(2012),(19 pages).
[24]. *T. Shah and A.A. Andrade*, Cyclic codes through $B[X;\frac{a}{b}Z_0](\frac{a}{b}\in Q^+, b=a+1)$ and Encoding, DMAA. **4**(4)(2012), (8 pages).
[25]. *T. Shah, A. Khan and A.A. Andrade*, Encoding through generalized polynomial codes, Comput. Appl. Math. **30**(2) (2011), 349-366.
[26]. *T. Shah, A. Khan and A.A. Andrade*, Constructions of codes through semigroup ring $B[x;\frac{1}{2}Z_0]$ and encoding, Comput. Math. Appl.