



## A decoding method of an $n$ length binary BCH code through $(n + 1)n$ length binary cyclic code

TARIQ SHAH<sup>1</sup>, MUBASHAR KHAN<sup>1</sup> and ANTONIO A. DE ANDRADE<sup>2</sup>

<sup>1</sup>Department of Mathematics, Quaid-i-Azam University, 45320, Islamabad, Pakistan

<sup>2</sup>Departamento de Matemática, IBILCE, Universidade Estadual Paulista “Júlio de Mesquita Filho”, Rua Cristóvão Colombo, 2265, Bairro Jardim Nazareth, 15054-000 São José do Rio Preto, SP, Brasil

*Manuscript received on April 30, 2012; accepted for publication on April 29, 2013*

### ABSTRACT

For a given binary BCH code  $C_n$  of length  $n = 2^s - 1$  generated by a polynomial  $g(x) \in \mathbb{F}_2[x]$  of degree  $r$  there is no binary BCH code of length  $(n + 1)n$  generated by a generalized polynomial  $g(x^{\frac{1}{2}}) \in \mathbb{F}_2[x^{\frac{1}{2}} \mid \mathbb{Z} \geq 0]$  of degree  $2r$ . However, it does exist a binary cyclic code  $C_{(n+1)n}$  of length  $(n + 1)n$  such that the binary BCH code  $C_n$  is embedded in  $C_{(n+1)n}$ . Accordingly a high code rate is attained through a binary cyclic code  $C_{(n+1)n}$  for a binary BCH code  $C_n$ . Furthermore, an algorithm proposed facilitates in a decoding of a binary BCH code  $C_n$  through the decoding of a binary cyclic code  $C_{(n+1)n}$ , while the codes  $C_n$  and  $C_{(n+1)n}$  have the same minimum hamming distance.

**Key words:** BCH code, binary cyclic code, binary Hamming code, decoding algorithm.

### INTRODUCTION

The applications of finite commutative rings, particularly finite local rings, have great importance due to their principal ideals. In the design of communication systems and high rate digital computers, encoding and decoding have an importance for error control. The main component of the conventional error-correcting codes are ideals in a finite commutative principal ideal ring.

In Cazaran and Kelarev 1997 authors introduce the necessary and sufficient conditions for the ideal to be a principal ideal and describe all finite principal ideal rings  $\mathbb{Z}_m[x_1, x_2, \dots, x_n]/I$ , where  $I$  is generated by univariate polynomials. Moreover, in Cazaran and Kelarev 1999, they obtained conditions for certain rings to be finite commutative principal ideal rings. However, the extension of a BCH code embedded in a semigroup ring  $\mathbb{F}[S]$ , where  $S$  is a finite semigroup, is introduced by Cazaran et al. 2006, where an algorithm was given for computing the weights of extensions for codes embedded in  $\mathbb{F}[S]$  as ideals. A numerous information related with several ring constructions and concerning polynomial codes was given by Kelarev 2002. Whereas, in Kelarev 2007, 2008, Kelarev discusses the concerning extensions of BCH codes in several ring constructions, where the results can also be considered as particular cases of semigroup rings of particular nature. Andrade and Palazzo 2005 elaborated the cyclic, BCH, alternant,

---

Correspondence to: Antonio Aparecido de Andrade  
E-mail: andrade@ibilce.unesp.br

Goppa and Srivastava codes over finite rings, which are in real meanings constructed through a polynomial ring in one indeterminate with a finite coefficient ring. Shah in Shah et al. 2011a, b, instead of a polynomial ring, the construction methodology of cyclic, BCH, alternant, Goppa, and Srivastava codes over a finite ring is used through a semigroup ring, where the results of Andrade and Palazzo 2005 are improved in such a way that in the place of cancellative torsion free additive monoid  $\mathbb{Z}_{\geq 0}$  of non negative integers, the cancellative torsion free additive monoids  $\frac{1}{2}\mathbb{Z}_{\geq 0}$  and  $\frac{1}{2^s}\mathbb{Z}_{\geq 0}$  are taken, respectively. Consequently, this new structure gives a construction of a finite quotient ring of a polynomial ring into a finite quotient ring of monoid rings of particular nature. In Shah et al. 2011a, b,  $R$  is considered as a finite unitary commutative ring for the quotient rings  $R[x; \frac{1}{2^s}\mathbb{Z}_{\geq 0}]/((x^{\frac{1}{2^s}})^{2^n} - 1)$  and  $R[x; \frac{1}{2^s}\mathbb{Z}_{\geq 0}]/((x^{\frac{1}{2^s}})^{2^{2n}} - 1)$ , respectively. However, in (Andrade et al. 2010) authors describe the decoding principle based on modified Berlekamp-Massey algorithm for BCH, alternant and Goppa codes constructed through monoid rings  $R[x; \frac{1}{2^s}\mathbb{Z}_{\geq 0}]$ .

The existence of a binary cyclic  $((n+1)^{3^k} - 1, (n+1)^{3^k} - 1 - 3^k r)$  code, where  $k$  is a positive integer, corresponding to a binary cyclic  $(n, n-r)$  code is established in Shah et al. 2012 by monoid ring  $\mathbb{F}_2[x; \frac{1}{3^k}\mathbb{Z}_{\geq 0}]$ . Furthermore, in Shah et al. 2012 a decoding procedure for binary cyclic  $(n, n-r)$  code by the binary cyclic  $((n+1)^{3^k} - 1, (n+1)^{3^k} - 1 - 3^k r)$  code is also given, which improve the code rate and error corrections capabilities.

We were provoked by Shah et al. 2012 and initiated the inquiry in support to binary BCH codes alike binary cyclic codes. However, we observed that for an  $n$  length binary BCH code with  $n = 2^s - 1$  generated by the polynomial  $g(x) \in \mathbb{F}_2[x]$  of degree  $r$  it is not possible to construct a binary BCH code of length  $(n+1)n$  generated by the generalized polynomial  $g(x^{\frac{1}{2}}) \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$  of degree  $2r$ . However, in this study, we established that corresponding to a binary BCH code  $C_n(n, n-r)$  there is a binary cyclic code  $C_{(n+1)n}((n+1)n, (n+1)n-2r)$  such that  $C_n$  is embedded in  $C_{(n+1)n}$ . Furthermore, we propose an algorithm that enables decoding a binary BCH code of length  $n$  through the decoding of  $(n+1)n$  length binary cyclic code.

This paper is formulated as follows. In Section 2, first we investigate that, for a positive integer  $n = 2^s - 1$ , where  $s$  is a positive integer, such that if a polynomial  $g(x) \in \mathbb{F}_2[x; \mathbb{Z}_{\geq 0}]$  of degree  $r$  divides  $x^n - 1$ , then a generalized polynomial  $g(x^{\frac{1}{2}}) \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$  of degree  $2r$  divides  $x^{\frac{1}{2}(n+1)n} - 1$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ . Second, we discuss cyclic codes of length  $(n+1)n$  generated by  $g(x^{\frac{1}{2}})$ . In Section 3, we discuss the non existence and existence of a binary BCH code of length  $(n+1)n$  and a cyclic code of length  $(n+1)n$  against a binary BCH code of length  $n$ , respectively. Consequently, a link of a BCH code  $(n, n-r)$  and a cyclic code  $((n+1)n, (n+1)n-2r)$  is developed. However, in Section 4, we present the decoding procedure for a binary cyclic code  $((n+1)n, (n+1)n-2r)$  by which we can obtain the decoding of a binary BCH code  $(n, n-r)$ . Concluding remarks are given in Section 5.

#### CYCLIC CODE OF LENGTH $(n+1)n$ CONSTRUCTED THROUGH $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$

A semigroup ring  $R[x; S]$  is the set of all finitely nonzero functions from a semigroup  $(S, *)$  into an associative ring  $(R, +, \cdot)$  in which binary operations addition and multiplication are given by  $(f+g)(s) = f(s) + g(s)$  and  $(fg)(s) = \sum_{t*u=s} f(t)g(u)$ , where the  $\sum_{t*u=s}$  shows that the sum is taken over all pairs  $(t, u)$  of elements of  $S$  such that  $t * u = s$ , otherwise  $(fg)(s) = 0$ . If  $S$  is a monoid, then  $R[x; S]$  is called monoid ring. A nonzero element  $f$  of  $R[x; S]$  has unique representation  $\sum_{i=1}^n f_i x^{s_i}$ , where  $f_i \neq 0$  and  $s_i \neq s_j$  for  $i \neq j$ . If  $S$  is  $\mathbb{Z}_0$  and  $R$  is an associative ring, particularly the binary field  $\mathbb{F}_2$ , then the semigroup ring  $R[x; S]$  is simply the polynomial ring  $R[x]$ . Clearly, it follows that  $R[x] = R[x; \mathbb{Z}_{\geq 0}] \subset R[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ . Since  $\frac{1}{2}\mathbb{Z}_{\geq 0}$  is an ordered monoid, it follows that we can define the degree of an element in  $R[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ .

We initiate this study by an observation that the indeterminate of generalized polynomials in a semigroup ring  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$  is given by  $x^{\frac{1}{2}}$  and it behaves like an indeterminate  $x$  in  $\mathbb{F}_2[x]$ . For instance, for a torsion free cancellative monoid  $S$ , it follows that the monoid ring  $\mathbb{F}_2[x; S]$  is a Euclidean domain if  $\mathbb{F}_2$  is a field and  $S \cong \mathbb{Z}$  or  $S \cong \mathbb{Z}_{\geq 0}$  (Gilmer and Parker 1974). Of course, here  $\frac{1}{2}\mathbb{Z}_{\geq 0}$  is a torsion free cancellative and isomorphic to  $\mathbb{Z}_{\geq 0}$ .

Given any generalized polynomial  $f(x^{\frac{1}{2}}) \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ , we can construct the factor ring  $\frac{\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]}{(f(x^{\frac{1}{2}}))}$ , where  $(f(x^{\frac{1}{2}}))$  is a principal ideal in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$  generated by  $f(x^{\frac{1}{2}})$ . The elements of the factor ring are the cosets of the ideal  $(f(x^{\frac{1}{2}}))$ . The factor ring is a field if, and only if,  $f(x^{\frac{1}{2}})$  is irreducible over  $\mathbb{F}_2$ .

**Proposition 1** *Let  $g(x) \in \mathbb{F}_2[x, \mathbb{Z}_{\geq 0}]$  be a polynomial of degree  $r$ . If  $n = 2^s - 1$ , where  $s$  is a positive integer, then the generalized polynomial  $g(x^{\frac{1}{2}}) \in \mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_{\geq 0}]$  of degree  $2r$  divides  $x^{\frac{1}{2}(n+1)n} - 1$  in  $\mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_{\geq 0}]$ .*

**Proof.** Clearly  $g(x^{\frac{1}{2}}) \in \mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_{\geq 0}]$  divides  $x^{\frac{1}{2}2n} - 1$ . If  $x^{\frac{1}{2}(n+1)n} - 1 = x^{\frac{1}{2}(2^s - 1)2^s} - 1 = x^{\frac{1}{2}(2^s - 1)} - 1)^{2^s} = x^{\frac{1}{2}n} - 1)^{2^s}$ , then  $g(x^{\frac{1}{2}})$  divides  $x^{\frac{1}{2}(n+1)n} - 1$ .

Now onward, if  $f(x^{\frac{1}{2}}) = (x^{\frac{1}{2}})^{(n+1)n} - 1$ , then  $\frac{\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]}{((x^{\frac{1}{2}})^{(n+1)n} - 1)}$  is given by

$$\{a_0 + a_{\frac{1}{2}}\zeta + a_1\zeta^2 + \dots + a_{\frac{n(n+1)-1}{2}}\zeta^{n(n+1)-1} : a_0, a_{\frac{1}{2}}, a_1, \dots, a_{\frac{n(n+1)-1}{2}} \in \mathbb{F}_2\},$$

where  $\zeta$  denotes the coset  $x^{\frac{1}{2}} + (f(x^{\frac{1}{2}}))$ . Thus,  $f(\zeta) = 0$ , where  $\zeta$  satisfies the relation  $\zeta^{n(n+1)} - 1 = 0$ . Let us now make a change in notation and write  $x^{\frac{1}{2}}$  in place of  $\zeta$ . Thus, the ring  $\frac{\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]}{(x^{\frac{1}{2}n(n+1)} - 1)}$  becomes  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  in which the relation  $x^{\frac{1}{2}n(n+1)} - 1 = 0$  holds, that is  $(x^{\frac{1}{2}})^{n(n+1)} = 1$ .

The multiplication  $*$  in the ring  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  is modulo  $(x^{\frac{1}{2}n(n+1)} - 1)$ . So, given  $c(x^{\frac{1}{2}}), d(x^{\frac{1}{2}}) \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ , we write  $c(x^{\frac{1}{2}}) * d(x^{\frac{1}{2}})$  to denote their product in the ring  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  and  $c(x^{\frac{1}{2}})d(x^{\frac{1}{2}})$  to denote their product in the ring  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ . If  $\deg a(x^{\frac{1}{2}}) + \deg b(x^{\frac{1}{2}}) < \frac{1}{2}n(n+1)$ , then  $c(x^{\frac{1}{2}}) * d(x^{\frac{1}{2}}) = c(x^{\frac{1}{2}})d(x^{\frac{1}{2}})$ . Otherwise,  $c(x^{\frac{1}{2}}) * d(x^{\frac{1}{2}})$  is the remainder left on dividing  $c(x^{\frac{1}{2}})d(x^{\frac{1}{2}})$  by  $(x^{\frac{1}{2}})^{n(n+1)} - 1$ . In other words, if  $c(x^{\frac{1}{2}}) * d(x^{\frac{1}{2}}) = r(x^{\frac{1}{2}})$ , then  $c(x^{\frac{1}{2}})d(x^{\frac{1}{2}}) = r(x^{\frac{1}{2}})$ , then  $c(x^{\frac{1}{2}})d(x^{\frac{1}{2}}) = r(x^{\frac{1}{2}}) + ((x^{\frac{1}{2}})^{n(n+1)} - 1)q(x^{\frac{1}{2}})$  for some generalized polynomial  $q(x^{\frac{1}{2}})$ . Practically, to obtain  $c(x^{\frac{1}{2}}) * d(x^{\frac{1}{2}})$ , we simply compute the ordinary product  $c(x^{\frac{1}{2}})d(x^{\frac{1}{2}})$  and then put  $x^{\frac{1}{2}n(n+1)} = 1, x^{\frac{1}{2}n(n+1) + \frac{1}{2}} = x^{\frac{1}{2}}$  and so on. Now, consider  $x^{\frac{1}{2}} * c(x^{\frac{1}{2}})$  and it would be

$$x^{\frac{1}{2}} * (c_0 + c_{\frac{1}{2}}x^{\frac{1}{2}} + \dots + c_{\frac{n(n+1)-2}{2}}(x^{\frac{1}{2}})^{n(n+1)-2} + c_{\frac{n(n+1)-1}{2}}(x^{\frac{1}{2}})^{n(n+1)-1}).$$

That is

$$x^{\frac{1}{2}} * c(x^{\frac{1}{2}}) = c_{\frac{n(n+1)-1}{2}} + c_0x^{\frac{1}{2}} + c_{\frac{1}{2}}x^1 + \dots + c_{\frac{n(n+1)-2}{2}}(x^{\frac{1}{2}})^{n(n+1)-1}.$$

Particularly, we can take the product  $x^{\frac{1}{2}} * c(x^{\frac{1}{2}})$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  by following lemma.

**Lemma 2** *The  $\mathbb{F}_2$ -space  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  is isomorphic to  $\mathbb{F}_2$ -space  $\mathbb{F}_2^{n(n+1)}$ .*

**Proof.** It follows that  $(x^{\frac{1}{2}})^{n(n+1)n} - 1 = y^{n(n+1)} - 1$ , where  $x^{\frac{1}{2}} = y$ . In fact, we deal the coefficients of generalized polynomials  $c(x^{\frac{1}{2}}) = c_0 + c_{\frac{1}{2}}x^{\frac{1}{2}} + \dots + c_{\frac{n(n+1)-2}{2}}(x^{\frac{1}{2}})^{n(n+1)-2} + c_{\frac{n(n+1)-1}{2}}(x^{\frac{1}{2}})^{n(n+1)-1}$  of  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ . So  $c(x^{\frac{1}{2}})$  has  $n(n+1)$  terms and hence the coefficients in  $\mathbb{F}_2$ . Corresponding to  $c(x^{\frac{1}{2}}) \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ , there is a  $n(n+1)$ -tuppled vector  $(c_0, c_{\frac{1}{2}}, \dots, c_{\frac{n(n+1)-1}{2}})$  in  $\mathbb{F}_2^{n(n+1)}$ . Thus, there is an isomorphism between the vector space  $\mathbb{F}_2^{n(n+1)}$  and  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  defined by  $c \mapsto c(x^{\frac{1}{2}})$ .

We observed that, multiplication by  $x^{\frac{1}{2}}$  in the ring  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  corresponds to cyclic shift  $\sigma$  in  $\mathbb{F}_2^{n(n+1)}$ , that is  $x^{\frac{1}{2}} * c(x^{\frac{1}{2}}) = \sigma(c)(x^{\frac{1}{2}})$ . A subspace  $C$  of  $\mathbb{F}_2$ -space  $\mathbb{F}_2^{n(n+1)}$  is a linear code. From Lemma 2, identifying every vector  $\mathbf{c}$  in  $\mathbb{F}_2^{n(n+1)}$  with the polynomial  $c(x^{\frac{1}{2}})$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ , it follows that  $C \subset \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ . The elements of the code  $C$  are now referred as codewords or code generalized polynomials.

By use of the techniques of (Shah et al. 2012), the following results can easily be established for a positive integer  $n(n+1)$  instead of  $(n+1)^{3^k} - 1$ .

**Theorem 3** (Shah et al. 2012) *Let  $C$  be a linear code over  $\mathbb{F}_2$ . Then  $C$  is cyclic if, and only if,  $x^{\frac{1}{2}} * c(x^{\frac{1}{2}}) \in C$  for every  $c(x^{\frac{1}{2}}) \in C$ .*

**Theorem 4** (Shah et al. 2012) *A subset  $C$  of  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  is a cyclic code if, and only if,  $C$  is an ideal of the ring  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ .*

It is noticed that  $(p(x^{\frac{1}{2}})) = \{b(x^{\frac{1}{2}}) * p(x^{\frac{1}{2}}) : b(x^{\frac{1}{2}}) \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}\}$ , where  $p(x^{\frac{1}{2}}) \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  represents the principal ideal generated by  $p(x^{\frac{1}{2}})$  in the ring  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ .

**Theorem 5** (Shah et al. 2012) *If  $C$  is a nonzero ideal in the ring,  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  then,*

1. *there exists a unique monic polynomial  $g(x^{\frac{1}{2}})$  of least degree in  $C$ ;*
2.  *$g(x^{\frac{1}{2}})$  divides  $(x^{\frac{1}{2}})^{n(n+1)} - 1$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ ;*
3. *for all  $a(x^{\frac{1}{2}}) \in C$ ,  $g(x^{\frac{1}{2}})$  divides  $a(x^{\frac{1}{2}})$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ ; and*
4.  *$C = (g(x^{\frac{1}{2}}))$ .*

*Conversely, if  $C$  is an ideal generated by  $p(x^{\frac{1}{2}}) \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ , then  $p(x^{\frac{1}{2}})$  is a generalized polynomial of least degree in  $C$  if, and only if,  $p(x^{\frac{1}{2}})$  divides  $(x^{\frac{1}{2}})^{n(n+1)} - 1$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ .*

From Theorem 5, it follows that the only ideals in the ring  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  are linear codes which are generated by the factors of  $x^{\frac{1}{2}n(n+1)} - 1$ . Thus, we can obtain all cyclic codes of length  $n(n+1)$  over  $\mathbb{F}_2$  if we find all factors of  $x^{\frac{1}{2}n(n+1)} - 1$ . In the case of trivial factors, we get trivial codes. If  $g(x^{\frac{1}{2}}) = x^{\frac{1}{2}n(n+1)} - 1$ , then  $(g(x^{\frac{1}{2}})) = (0)$ . Whereas  $g(x^{\frac{1}{2}}) = 1$  implies  $(g(x^{\frac{1}{2}})) = \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ .

**Remark 6** *If  $p(x^{\frac{1}{2}})$  does not divide  $x^{\frac{1}{2}n(n+1)} - 1$ , then  $p(x^{\frac{1}{2}})$  cannot be of least degree in the ideal  $(p(x^{\frac{1}{2}}))$ .*

**Definition 7** *Let  $C$  be a nonzero ideal in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ . If  $g(x^{\frac{1}{2}})$  is a unique monic generalized polynomial of least degree in  $C$ , then  $g(x^{\frac{1}{2}})$  is called the generator generalized polynomial of the cyclic code  $C$ .*

Note that if  $C = (p(x^{\frac{1}{2}}))$  is the ideal generated by  $p(x^{\frac{1}{2}})$ , then  $p(x^{\frac{1}{2}})$  is the generator generalized polynomial of  $C$  if, and only if,  $p(x^{\frac{1}{2}})$  is monic and divides  $x^{\frac{1}{2}n(n+1)} - 1$ .

#### A LINK OF A BCH CODE $(n, n-r)$ AND A CYCLIC CODE $((n+1)n, (n+1)n-2r)$

In this section, we develop a link between a binary BCH code  $(n, n-r)$  and a binary cyclic code  $((n+1)n, (n+1)n - 2r)$ . For this, let  $C_n$  be a binary BCH code based on the positive integers  $c, \delta_1, q = 2$  and  $n$  such that  $2 \leq \delta_1 \leq n$  with  $\gcd(n, 2) = 1$  and  $n = 2^s - 1$ , where  $s \in \mathbb{Z}^+$ . Consequently, the binary BCH code  $C_n$  has generator polynomial of degree  $r$  given by  $g(x) = \text{lcm}\{m_i(x) : i = c, c+1, \dots, c+\delta_1-2\}$ , where  $m_i(x)$  are minimal polynomials of  $\zeta^i$  for  $i = c, c+1, \dots, c+\delta_1-2$ . Whereas  $\zeta$  is the primitive  $n^{\text{th}}$  root of unity in  $\mathbb{F}_{2^m}$ . Since  $m_i(x)$  divides  $x^n - 1$  for each  $i$ , it follows that  $g(x)$  divides  $x^n - 1$ . This implies  $C_n = (g(x))$  is a principal ideal in the

factor ring  $\mathbb{F}_2[x]_n$ . From Proposition 1, it follows that the generalized polynomial  $(g(x^{\frac{1}{2}})) \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$  of degree  $2r$  divides  $x^{\frac{1}{2}n(n+1)} - 1$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ . So, there is a cyclic code  $C_{(n+1)n}$  generated by  $g(x^{\frac{1}{2}})$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$ . Since  $x^{\frac{1}{2}2n} - 1$  divides  $x^{\frac{1}{2}n(n+1)} - 1$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ , it follows that  $(x^{\frac{1}{2}n(n+1)} - 1) \subset (x^{\frac{1}{2}2n} - 1)$ .

Now, by third isomorphism theorem for rings, it follows that  $\frac{\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]/(x^{\frac{1}{2}n(n+1)} - 1)}{(x^{\frac{1}{2}2n} - 1)/(x^{\frac{1}{2}n(n+1)} - 1)} \simeq \frac{\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]}{(x^{\frac{1}{2}2n} - 1)} \simeq \frac{\mathbb{F}_2[x]}{(x^n - 1)}$ .

Thus,  $C_n$  is embedded in  $C_{(n+1)n}$  and the monomorphism  $\phi : C_n \rightarrow C_{(n+1)n}$  is defined as  $\phi(a(x)) = \phi(a_0 + a_1x + \dots + a_{n-1}x^{n-1}) = a_0 + a_1(x^{\frac{1}{2}})^2 + \dots + a_{2(n-1)-1}(x^{\frac{1}{2}})^{2(n-1)} = a(x^{\frac{1}{2}})$ , where  $a(x) \in C_n$ . The above discussion shape the following theorem.

**Theorem 8** *Let  $s$  be a positive integer. If  $C_n$  is a binary BCH code of length  $n = 2^s - 1$  generated a polynomial of degree  $r$  given by  $g(x) = g_0 + g_1x + \dots + g_r x^r \in \mathbb{F}_2[x]$ , then*

1. *there exist a binary cyclic code  $C_{(n+1)n}$  of length  $(n+1)n$  generated by a generalized polynomial of degree  $2r$  given by  $g(x^{\frac{1}{2}}) = g_0 + g_1x^{\frac{1}{2}2} + \dots + g_r x^{\frac{1}{2}2r} \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ ; and*
2. *the binary BCH code  $C_n$  is embedded in the binary cyclic code  $C_{(n+1)n}$ .*

For a binary BCH code  $C_n$  with generator polynomial  $g(x)$  it is not possible to construct a binary BCH code  $C_{(n+1)n}$  with generator polynomial  $g(x^{\frac{1}{2}})$ . Indeed, as we know that generator polynomial of a binary BCH code is the least common multiple of irreducible polynomials over  $\mathbb{F}_2$ . For instance, if  $g(x) = \sum_{i=0}^r g_i x^i$  is the generator polynomial of the binary BCH code  $C_n$ , then  $g(x^{\frac{1}{2}}) = g_0 + g_1x^{\frac{1}{2}2} + \dots + g_r x^{\frac{1}{2}2r} = (g_0 + g_1x^{\frac{1}{2}2} + \dots + g_r x^{\frac{1}{2}2r})^2$  is not the least common multiple of irreducible polynomials in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ . Hence,  $g(x^{\frac{1}{2}})$  is not qualify for a generator of a binary BCH code.

**Example 9** *Let  $s = 2, n = 2^s - 1 = 2^2 - 1 = 3, \delta = 3, c = 1$  and  $p(x) = x^2 + x + 1$  a primitive polynomial of degree 2. Thus,  $\mathbb{F}_{2^2} = \frac{\mathbb{F}_2[x]}{(p(x))} = \{a_0 + a_1\zeta : a_0, a_1 \in \mathbb{F}_2\}$ , where  $\zeta$  satisfies the relation  $\zeta^2 + \zeta + 1 = 0$ . Using this relation, it follows that  $\{0, \zeta^1 = \zeta, \zeta^2 = 1 + \zeta, \zeta^3 = 1\}$ . Let  $m_i(x)$  be the minimal polynomial of  $\zeta^i$ , where  $i = c, c + 1, \dots, c, c + 1, \dots, c + \delta - 2$ . Thus,  $m_1(x) = x^2 + x + 1$ , and hence,  $g(x) = \text{lcm}\{m_i(x) : i = c, c + 1, \dots, c + \delta - 2\} = x^2 + x + 1$ . Also,  $C_3 = (g(x)) \subset \mathbb{F}_2[x]_3$  is a binary BCH code based on the positive integers  $c = 1, \delta = 3, q = 2$  and  $n = 3$  such that  $2 \leq \delta \leq n$  with  $\text{gcd}(n, 2) = 1$ . Since  $g(x^{\frac{1}{2}}) = (x^{\frac{1}{2}})^4 + (x^{\frac{1}{2}})^2 + 1$  divides  $(x^{\frac{1}{2}})^{3(3+1)} - 1$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$ , it follows that the corresponding cyclic code  $C_{12}(12, 8)$  is generated by  $g(x^{\frac{1}{2}})$ .*

**GENERAL DECODING PRINCIPLE**

Berlekamp et al. 1978 demonstrated that the maximum-likelihood decoding is a NP-hard problem for general linear codes. Whereas by the principle of maximum-likelihood decoding we obtain a code after decoding which is closest to the received vector when the errors are corrected. We use the decoding procedure which follows the same principle.

In the following we interpret the decoding terminology for a binary cyclic code  $C_{(n+1)n}$  with length  $(n+1)n$  and having parity-check matrix  $H$ . If the vector  $b$  is received, then we obtain the syndrome vector of  $b$  given by  $S(b) = bH^T$ . In this way, we calculate a table of syndromes which is useful in determining the error vector  $e$  such that  $S(b) = S(e)$ . So the decoding of received vector  $b$  has done as the transmitted vector  $a = b - e$ .

The general principle of decoding is to pick the codeword nearest to the received vector. For this purpose, we prepare a look-up table that gives the nearest codeword for every possible received vector.

The algebraic structure of a linear code as a subspace provides a convenient method for preparing such a table. If  $C_{(n+1)n}$  is a subspace of  $\mathbb{F}_2^{(n+1)n}$ , then  $C_{(n+1)n}$  is a subgroup of the additive group  $\mathbb{F}_2^{(n+1)n}$ . Recall that for every  $a \in \mathbb{F}_2^{(n+1)n}$ , the set  $a+C_{(n+1)n} = \{a + c : c \in C_{(n+1)n}\}$  is called a coset of  $C_{(n+1)n}$  and the set of these cosets form a partition of the set  $\mathbb{F}_2^{(n+1)n}$ . Hence,  $\mathbb{F}_2^{(n+1)n}$  is the disjoint union of distinct cosets of  $C_{(n+1)n}$ .

Let  $y$  be any vector in  $\mathbb{F}_2^{(n+1)n}$ , and suppose  $x \in C_{(n+1)n}$  is the codeword nearest to  $y$ . Now,  $x$  lies in the coset  $y + C_{(n+1)n} = \{y - c : c \in C_{(n+1)n}\}$ . For all  $c \in C_{(n+1)n}$ , it follows that  $d(y,x) \leq d(y,c)$ , i.e.  $w(y - x) \leq w(y - c)$ . Hence,  $y - x$  is the vector of least weight in the coset containing  $y$ . Writing  $e = y - x$ , it follows that  $x = y - e$ . Thus, the following theorem is obtained.

**Theorem 10** *Let  $C_{(n+1)n} \subset \mathbb{F}_2^{(n+1)n}$  be a linear code. Given a vector  $y \in \mathbb{F}_2^{(n+1)n}$ , the codeword  $x$  nearest to  $y$  is given by  $x = y - e$ , where  $e$  is the vector of least weight in the coset containing  $y$ . If the coset containing  $y$  has more than one vector of least weight, then there are more than one codewords nearest to  $y$ .*

**Definition 11** *Let  $C_{(n+1)n}$  be a linear code in  $\mathbb{F}_2^{(n+1)n}$ . The coset leader of a given coset of  $C_{(n+1)n}$  is defined to be the vector with the least weight in the coset.*

**Theorem 12** *Let  $C_{(n+1)n}$  be an  $((n+1)n, (n+1)n-2r)$  code over  $\mathbb{F}_2$ . If  $H$  is a parity-check matrix of  $C_{(n+1)n}$ , then  $C_{(n+1)n} = \{x \in \mathbb{F}_2^{(n+1)n} : xH^T = 0 = Hx^T\}$ .*

From Theorem 12, it follows that  $S(y) = 0$  if, and only if,  $y \in C_{(n+1)n}$ . Let  $y$  such that  $y' \in \mathbb{F}_2^{(n+1)n}$ . Thus,  $S(y) = S(y')$  holds if, and only if,  $(y - y')H^T = 0$ , that is,  $y - y' \in C_{(n+1)n}$ . Hence, two vectors have the same syndrome if, and only if, they lie in the same coset of  $C_{(n+1)n}$ . Thus, there is a one-to-one correspondence between the cosets of  $C_{(n+1)n}$  and the syndromes. A table with two columns showing the coset leader  $e_i$  and the corresponding syndromes  $S(e_i)$  is called the syndrome table. To decode a received vector  $y$ , we compute its syndrome  $S(y)$  and then look at the table to find the coset leader  $e$  for which  $S(e) = S(y)$ . Then  $y$  is decoded as  $x = y - e$ . The syndrome table is given by

coset leader	syndrome
$e_1$	$S(e_1)$
$e_2$	$S(e_2)$
$\vdots$	$\vdots$
$e_i$	$S(e_i)$
$\vdots$	$\vdots$
$e_N$	$S(e_N)$

where  $N = q^{n-k}$ ,  $\mathbb{F} = \mathbb{F}_{2q}$  and  $S(e_i) = e_i H^T$  for  $1 \leq i \leq N$ .

Now, consider a binary BCH code  $C_n$  based on the positive integers  $c, \delta, q = 2$  and  $n$  such that  $2 \leq \delta \leq n$  with  $n = 2^s - 1$ , where  $s$  is a positive integer. Let  $\zeta$  be a primitive  $n^{th}$  root of unity in  $\mathbb{F}_{2^m}$ . Let  $m_i(x) \in \mathbb{F}_2[x]$  denote the minimal polynomial of  $\zeta^i$ . Let  $g(x)$  be the product of distinct polynomials among  $m_i(x)$ , for  $i = c, c + 1, \dots, c + \delta - 2$ , that is,  $g(x) = lcm\{m_i(x) : i = c, c + 1, \dots, c + \delta - 2\}$ .

Assume that  $C_{(n+1)n}$  is the corresponding binary cyclic code of length  $(n + 1)n$  with minimum distance  $d$  and with generator generalized polynomial  $g(x^{\frac{1}{2}})$  which has the check generalized polynomial

$$h(x^{\frac{1}{2}}) = h_{n(n+1)-2r}(x^{\frac{1}{2}})^{n(n+1)-2r} + h_{n(n+1)-2r-1}(x^{\frac{1}{2}})^{n(n+1)-2r-1} + \dots + h_1(x^{\frac{1}{2}}) + h_0.$$

Of course,  $x^{\frac{1}{2}(n+1)n} - 1 = g(x^{\frac{1}{2}}) * h(x^{\frac{1}{2}})$ . Thus, the matrix  $H$  is given by

$$\begin{bmatrix} h_{n(n+1)-2r} & h_{n(n+1)-2r-1} & \dots & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_{n(n+1)-2r} & \dots & \dots & h_1 & h_0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & h_{n(n+1)-2r} & h_{n(n+1)-2r-1} & \dots & \dots & h_1 & h_0 \end{bmatrix}$$

is the parity-check matrix de order  $(2r \times (n + 1)n$  for binary cyclic code  $C_{(n+1)n}$  of dimension  $k = (n + 1)n - 2r$ . Syndrome of the vector  $a \in \mathbb{F}_2^{(n+1)n}$  is denoted as  $S(a) = aH^T$ . For the vector  $a$  given by  $a = (a_0, a_{\frac{1}{2}}, a_{\frac{1}{2}^2}, \dots, a_{\frac{n-1}{2}}, \dots, a_{\frac{(n-1)n-1}{2}}) \in \mathbb{F}_2^{(n+1)n}$ , it follows that the generalized polynomial is given by  $a(x^{\frac{1}{2}}) = a_0 + a_{\frac{1}{2}}x^{\frac{1}{2}} + \dots + a_{\frac{(n-1)}{2}}x^{\frac{1}{2}(n-1)} + \dots + a_{\frac{(n-1)n-1}{2}}x^{\frac{(n+1)n-1}{2}}$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{(n+1)n}$ . So,  $S(a) = aH^T$ , where

$$a = \left[ a_0 \quad a_{\frac{1}{2}} \quad \dots \quad a_{\frac{n-1}{2}} \quad a_{\frac{(n-1)n-1}{2}} \right].$$

Now, assume that the codeword  $v \in C$  is transmitted and the received vector is given by  $a = v + e$ , where  $e = (e_0, e_{\frac{1}{2}}, e_1, \dots, e_{\frac{(n-1)}{2}}, \dots, e_{\frac{(n-1)n-1}{2}})$  is the error vector which has the polynomial form

$$e(x^{\frac{1}{2}}) = e_0 + e_{\frac{1}{2}}x^{\frac{1}{2}} + \dots + e_{\frac{(n-1)}{2}}x^{\frac{1}{2}(n-1)} + \dots + e_{\frac{(n-1)n-1}{2}}x^{\frac{1}{2}(n+1)n - \frac{1}{2}}.$$

Therefore,  $S(e) = S(a)$ . Now, the syndrome table for the binary cyclic code  $C_{(n+1)n}$  is

coset leader	syndrome
$e_1$	$S(e_1)$
$e_2$	$S(e_2)$
$\vdots$	$\vdots$
$e_i$	$S(e_i)$
$\vdots$	$\vdots$
$e_N$	$S(e_N)$

where  $N = 2^{(n+1)n-k}$ ,  $k = (n+1)n - 2r$  and  $S(e_i) = e_iH^T$  for  $1 \leq i \leq N$ .

**DECODING ALGORITHM**

We establish a decoding method of a binary BCH code of length  $n$  through binary cyclic code of length  $(n+1)n$ . Though, here in the following we sum up the procedure which indicates the steps in decoding a received word of the cyclic code of length  $(n + 1)n$  and explain the technique obtaining the wrapped codeword of the BCH code of length  $n$ .

**Step 1:** Evaluate the check generalized polynomial  $h(x^{\frac{1}{2}})$  of binary cyclic code  $C_{(n+1)n}$ .

**Step 2:** Construct the syndrome table for the binary cyclic code  $C_{(n+1)n}$ .

**Step 3:** Calculate the received generalized polynomial  $b'(x^{\frac{1}{2}}) \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{n(n+1)}$  corresponding to received polynomial  $b(x) \in \mathbb{F}_2[x]_n$ .

**Step 4:** Calculate the syndrome vector for the vector

$$b' = b_0, b_{\frac{1}{2}}, b_{\frac{1}{2}^2}, \dots, b_{\frac{(n-1)}{2}}, \dots, a_{\frac{(n+1)n-1}{2}} \in \mathbb{F}_2^{(n+1)n},$$

corresponding to the received generalized polynomial

$$b'(x^{\frac{1}{2}}) = b_0 + b_{\frac{1}{2}}x^{\frac{1}{2}} + \dots + b_{\frac{(n-1)}{2}}x^{\frac{1}{2}(n-1)} + \dots + b_{\frac{(n+1)n-1}{2}}x^{\frac{(2((n+1)n)-1)}{2}} \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{(n+1)n}.$$

**Step 5:** By looking at syndrome table (step 2), find the coset leader  $e$  for which  $S(b') = S(e)$ .

**Step 6:** Decode  $b'$  as  $b' - e = a'$ .

**Step 7:** The corresponding corrected codeword polynomial  $a(x)$  in binary BCH code  $C_n$  is obtained.

**Example 13** Let  $s = 2$ ,  $n = 2^2 - 1 = 3$  and  $C_3$  be the BCH code with positive integers  $c, \delta$ ,  $\gcd(n, 2) = 1$  and generated by  $g(x) = x^2 + x + 1 \in \mathbb{F}_2[x]_3$ . In this case,  $g(x^{\frac{1}{2}}) = (x^{\frac{1}{2}})^4 + (x^{\frac{1}{2}})^2 + 1 \in \mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{12}$  is the generator polynomial of the corresponding binary cyclic code  $C_{(3+1)3} = C_{12}(12, 8, d)$ . The generator matrix of  $C_{12}$  is given by

$$G' = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

and parity-check matrix with check polynomial  $h(x^{\frac{1}{2}}) = 1 + (x^{\frac{1}{2}})^2 + (x^{\frac{1}{2}})^6 + (x^{\frac{1}{2}})^8$  is given by

$$H' = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Syndrome table is given by

coset leader	syndrome
$e_0 = 000000000000$	0000
$e_1 = 100000000000$	1000
$e_2 = 010000000000$	0100
$e_3 = 001000000000$	1010
$e_4 = 000100000000$	0101
$e_5 = 000010000000$	0010
$e_6 = 000001000000$	0001
$e_7 = 110000000000$	1100
$e_8 = 100100000000$	1101
$e_9 = 100001000000$	1001
$e_{10} = 011000000000$	1110
$e_{11} = 010010000000$	0110
$e_{12} = 001100000000$	1111
$e_{13} = 001001000000$	1011
$e_{14} = 000110000000$	0111
$e_{15} = 000011000000$	0011



Let  $b = 110 \in \mathbb{F}_2^3$  be the received vector of binary BCH code  $C_3$ . Then, its polynomial representation is given by  $b(x) = 1 + x$  in  $\mathbb{F}_2[x]_3$  and the corresponding received polynomial in the cyclic code  $C_{12}$  is given by  $b'(x^{\frac{1}{2}}) = 1 + (x^{\frac{1}{2}})^2$  in  $\mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_{\geq 0}]_{12}$ , and its vector representation is  $b' = 101000000000 \in \mathbb{F}_2^{12}$ . Also,  $S(b') = b' * (H')^T = 0010 = S(e_5)$ , hence the corrected codeword in  $C_{12}$  is  $a' = b' + e_5 = 101010000000$  and its polynomial representation is  $a'(x) = 1 + x^2 + x^4$  in  $\mathbb{F}_2[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]_{12}$ . Hence, the corresponding corrected codeword in binary BCH code  $C_3$  is  $a(x) = 1 + x + x^2$  in  $\mathbb{F}_2[x]_3$ , that is  $a = 111$ .

### AN APPLICATION TO COGNITIVE RADIO

Cognitive radio is a most recent technology in wireless communication by which the spectrum is vigorously used when the primary user, the approved possessor of the spectrum, is not consumed. The scheme of cognitive radio is initiated in Mitola 2000. Rendering this notion, the cognitive radio has the competence to judge the radio environs and step up the decision according to the transmission parameters such as code rate, modulation scheme, power, carrier frequency and bandwidth.

The fundamental map in Zhao and Sadler 2007 is to issue license spectrum to secondary users and hurdle the interference observed by primary users. To guard the primary user from the interference activated by the secondary user during transmission, (Srinivasa and Jafar 2006) offered an organization of transmission models as interweave, underlay and overlay.

By (Mitola 2000), in the interweave model the secondary user has opportunistic accesses to the spectrum slum while the primary user is not in and pull out when the primary user wants to in once more. For cognitive radio transformation under the interweave model we may get spectrum corresponding to the binary cyclic code  $C_{(n+1)n}$  for data transfer of the primary user. Now, the setup only allow the secondary user having binary BCH code  $C_n$  for its data transfer. Accordingly the secondary user obtain high speed data transfer as compare to its own scheme of the BCH code  $C_n$ .

### CONCLUSION

This paper addresses the following aspects:

1. There does not exist a binary BCH code of length  $(n+1)n$  generated by a generalized polynomial  $g(x^{\frac{1}{2}}) \in \mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_{\geq 0}]$  of degree  $2r$  corresponding to a binary BCH code of length  $n$  with  $n = 2^s - 1$  generated by a polynomial  $g(x) \in \mathbb{F}_2[x]$  of degree  $r$  such that  $C_n$  is embedded in  $C_{(n+1)n}$ .
2. There does exist a binary cyclic code of length  $(n+1)n$  generated by a generalized polynomial  $g(x^{\frac{1}{2}}) \in \mathbb{F}_2[x, \frac{1}{2}\mathbb{Z}_{\geq 0}]$  of degree  $2r$  corresponding to a binary BCH code of length  $n$  with  $n = 2^s - 1$  generated by a polynomial  $g(x) \in \mathbb{F}_2[x]$  of degree  $r$  such that  $C_n$  is embedded in  $C_{(n+1)n}$ .
3. An algorithm is given which enables in decoding of a given binary BCH code  $C_n$  of length  $n$  through the decoding of a binary cyclic code  $C_{(n+1)n}$  of length  $(n+1)n$ . Consequently, we have the advantage that, if  $n-r$  message transmitted under the cover of binary cyclic code  $C_{(n+1)n}$ , then we obtain high speed data transfer as compare to the BCH code  $C_n$ . Whereas the codes  $C_n$  and  $C_{(n+1)n}$  have same minimum hamming distance.
4. By the interweave model for cognitive radio, the secondary user transfers its data through the binary BCH code  $C_n$  and has opportunistic accesses to the spectrum of primary user which uses binary cyclic code  $C_{(n+1)n}$  for its data transfer. As a result the secondary user achieve high data transfer rate as compare to its own scheme based on the BCH code  $C_n$ .

## ACKNOWLEDGMENTS

The authors are very grateful to Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) by financial support, 2007/56052-8 and 2011/03441-2.

## RESUMO

Para um determinado código binário BCH  $C_n$  de comprimento  $n = 2^s - 1$  gerado por um polinômio  $g(x) \in \mathbb{F}_2[x]$  de grau  $r$  não existe um código BCH binário de comprimento  $(n + 1)n$  gerado por um polinômio generalizado  $g(x^{\frac{1}{2}}) \in \mathbb{F}_2[x, \frac{1}{2}\mathbb{Z} \geq 0]$  de grau  $2r$ . No entanto, não existe um código cíclico binário  $C_{(n+1)n}$  de comprimento  $(n + 1)n$  de tal modo que o código BCH binário  $C_n$  é imerso em  $C_{(n+1)n}$ . Assim, um código de taxa elevada é alcançado através de um código cíclico binário  $C_{(n+1)n}$  para um código BCH binário  $C_n$ . Além disso, propomos um algoritmo que facilita na decodificação de um código BCH binário  $C_n$  através da decodificação de um código cíclico binário  $C_{(n+1)n}$ , ao passo que os códigos  $C_n$  e  $C_{(n+1)n}$  possuem a mesma distância de Hamming mínima.

**Palavras-chave:** Código BCH, código cíclico binário, código de Hamming binário, algoritmo de decodificação.

## REFERENCES

- ANDRADE AA AND PALAZZO JR R. 2005. Linear codes over finite rings. *TEMA - Tend Mat Apl Comput* 6(2): 207-217.
- ANDRADE AA, SHAH T AND KHAN A. 2010. Goppa codes through generalized polynomials and its decoding principle. *Int J Appl Math* 23(3): 517-526.
- BERLEKAMP ER, MCELIECE RJ AND VAN TILBORG HCA. 1978. On the inherent intractability of certain coding problem. *IEEE Trans Inf Theory* 24(3): 384-386.
- CAZARAN J AND KELAREV AV. 1997. Generators and weights of polynomial codes. *Archiv Math* 69: 479-486.
- CAZARAN J AND KELAREV AV. 1999. On finite principal ideal rings. *Acta Math Univ Comenianae* 68(1): 77-84.
- CAZARAN J, KELAREV AV, QUINN SJ AND VERTIGAN D. 2006. An algorithm for computing the minimum distances of extensions of BCH-codes embedded in semigroup rings. *Semigroup Forum* 73: 317-329.
- GILMER R AND PARKER T. 1974. Divisibility properties in semigroup rings. *Michigan Math J* 21(1): 65-86.
- KELAREV AV. 2002. Ring constructions and applications. World Scientific, River Edge, New York, 300 p.
- KELAREV AV. 2007. Algorithms for computing parameters of graph-based extensions of BCH-codes. *J Discrete Algorithms* 5: 553-563.
- KELAREV AV. 2008. An algorithm for BCH-codes extended with finite state automata. *Fundam Inform* 84(1): 51-60.
- MITOLA J. 2000. Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. Ph.D. Dissertation, KTH, Stockholm, Sweden, 304 p. (Unpublished).
- SHAH T, KHAN A AND ANDRADE AA. 2011a. Encoding through generalized polynomial codes. *Comput Appl Math* 30(2): 349-366.
- SHAH T, KHAN A AND ANDRADE AA. 2011b. Constructions of codes through semigroup ring  $B[x; \frac{1}{2}\mathbb{Z}_0]$  and encoding. *Comput Math App* 62: 1645-1654.
- SHAH T, AMANULLAH AND ANDRADE AA. 2012. A decoding procedure which improves code rate and error corrections. *J Adv Res App Math* 4(4): 37-50.
- SRINIVASA S AND JAFAR SA. 2006. The throughput potential of cognitive radio: a theoretical perspective. *IEEE Commun Mag* 45(5): 73-79.
- ZHAO Q AND SADLER BM. 2007. A Survey of Dynamic Spectrum Access. *IEEE Sig Proc Magazine* 24: 79-89.