Ansari and Shah *EURASIP Journal on Wireless Communications and Networking* (2016) 2016:38
DOI 10.1186/s13638-016-0526-3

EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

An association between primitive and non-primitive BCH codes using monoid rings

Asma Shaheen Ansari* and Tariq Shah

Abstract

BCH codes are one of the most important classes of cyclic codes for error correction. In this study, we generalize BCH codes using monoid rings instead of a polynomial ring over the binary field F_2. We show the existence of a non-primitive binary BCH code C_{bn} of length bn, corresponding to a given length n binary BCH code C_n. The value of b is investigated for which the existence of the non-primitive BCH code C_{bn} is assured. It is noticed that the code C_n is embedded in the code C_{bn}. Therefore, encoding and decoding of the codes C_n and C_{bn} can be done simultaneously. The data transmitted by C_n can also be transmitted by C_{bn}. The BCH code C_{bn} has better error correction capability whereas the BCH code C_n has better code rate, hence both gains can be achieved at the same time.

Keywords: BCH code, Non-primitive BCH code, Monoid ring, Error correction, Code rate

Mathematical subject classification: 11T71, 94B15, 94B20, 94B60

1 Introduction

The BCH codes form a large class of error-correcting cyclic codes that are constructed using finite fields. One of the key features of BCH codes is that during code design, there is a precise control over the number of symbol errors correctable by the code. In particular, it is possible to design binary BCH codes that can correct multiple bit errors. Another advantage of BCH codes is the ease with which they can be decoded, namely, via an algebraic method known as syndrome decoding. This simplifies the design of the decoder for these codes using small low-power electronic hardware.

Cyclic codes were initially considered by Prange (see [1, 2]). After him progress in the theory of cyclic codes for random as well as burst-error correction has been motivated by many coding theorists. The correspondence of cyclic codes with ideals was observed independently by Peterson [3], and Kasami [4]. Though most of the conventional error-correcting codes are principal ideals in the factor ring of a polynomial ring in one indeterminate. In [5], instead of one indeterminate, the authors have given the necessary and sufficient conditions for an ideal to have a single generator while, in [6], they have described all finite commutative principal ideal rings $\frac{\mathbb{Z}_m[x_1,\cdots,x_n]}{J}$, where J is an ideal generated by univariate polynomials.

The extension of a BCH code embedded in a semigroup ring is considered in [7]. A great amount of information regarding rings construction and its corresponding polynomial codes is given in [8]. In [8], Sections 9.1 and 9.2 are devoted to error correcting codes in ring construction closely related to semigroup rings. Particularly, Section 9.1 deals with error-correcting cyclic codes of length l which are in fact the ideals in the group ring $F[G]$, where F is a field and G is a finite torsion group of order l. However, in [9] and [10], the authors have mentioned about extensions of BCH codes in many ring constructions, where the outcomes can be considered as the special case of semigroup rings.

Through monoid rings, in a sequence of papers [11–17], several classes of cyclic codes over a finite unitary commutative ring are constructed. The purpose of these constructions is to address the error correction and the code rate trade off in a smart way. However, for a particular interest in [18], it is established that, there does not exist a binary BCH code of length $(n+1)n$ in the factor ring $F_2\left[x;\frac{1}{2}\mathbb{Z}_{\geq 0}\right] / \left(\left(x^{\frac{1}{2}}\right)^{(n+1)n} - 1\right)$ generated by generalized polynomial $g\left(x^{\frac{1}{2}}\right) \in F_2\left[x;\frac{1}{2}\mathbb{Z}_{\geq 0}\right]$ of degree $2r$ corresponding to the length n binary BCH code in

*Correspondence: asia_ansari@hotmail.com
Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan

$F_2[x]/(x^n-1)$ having generator polynomial $g(x) \in F_2[x]$ of degree r. But, there does exist a binary cyclic code of length $(n+1)n$ such that the length n binary BCH code is embedded in it. Besides this, the existence of a binary cyclic $\left((n+1)^{3^k}-1, (n+1)^{3^k}-1-3^k r\right)$ code, where k is a positive integer, corresponding to a binary cyclic $(n, n-r)$ code is established in [15] by the use of monoid ring $F_2\left[x; \frac{1}{3^k}\mathbb{Z}_{\geq 0}\right]$.

In both papers [18] and [15], the authors cannot show the existence of binary BCH codes corresponding to the length n binary BCH code in $F_2[x]/(x^n-1)$. In this study, we address this issue and construct a binary BCH code using monoid ring $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$, where a, b are integers such that $a, b > 1$. We show the existence of non-primitive binary BCH code C_{bn} of length bn using an irreducible polynomial $p\left(x^{\frac{a}{b}}\right) \in F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ of degree br, corresponding to a given length n binary BCH code C_n generated by r degree primitive polynomial $p(x^a)$ in $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$. It is noticed that the binary BCH code C_n is embedded in non-primitive BCH code C_{bn}. In this way a link between a primitive and non-primitive BCH code is attained. The length of the binary BCH C_{bn} is well controlled and has better error correction capability as compared to the length $(n+1)n$ binary cyclic code $C_{(n+1)n}$ initiated in [18].

This paper is organized in the following way: Section 2 contains a brief introduction to the monoid rings and a description of binary BCH codes as ideals in the factor ring $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]_n = F_2\left[x; a\mathbb{Z}_{\geq 0}\right]/((x^a)^n-1)$, a case parallel to Ham$(r, 2)$. Section 3 gives the construction technique of a non-primitive BCH code C_{bn} of length bn in the factor ring $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]_{bn} = F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]/\left(\left(x^{\frac{a}{b}}\right)^{bn}-1\right)$, corresponding to a given length n primitive BCH code C_n obtained in Section 2. Moreover, a link has been established between the binary BCH codes C_n and C_{bn}. In Section 4, decoding of the binary BCH code C_n through the decoding of binary BCH code C_{bn} is explained. Section 5 concludes the study.

2 BCH code C_n as ideal in $F_2[x; a\mathbb{Z}_{\geq 0}]/((x^a)^n-1)$

Let $(S, *)$ be a commutative monoid and F_2 be the binary field. The set of all finitely non-zero functions f from S into F_2 is denoted by $F_2[S]$. The set $F_2[S]$ is a ring with respect to binary operations addition and multiplication defined as: $(f+g)(s) = f(s) + g(s)$ and $(fg)(s) = \sum_{t*u=s} f(t)g(u)$, where the symbol $\sum_{t*u=s}$ indicates that the sum is taken over all pairs (t, u) of elements of S such that $t*u = s$, and it is understood that in the situation where s is not expressible in the form $t*u$ for any $t, u \in S$, then $(fg)(s) = 0$. $F_2[S]$ is known as the *monoid ring of S over* F_2. The representation of $F_2[S]$ will be $F_2[x; S]$ whenever S is an additive monoid. As there is an isomorphism between additive semigroup S and multiplicative semigroup $\{x^s : s \in S\}$, so a non-zero element f of $F_2[x; S]$ is uniquely represented in the canonical form $\sum_{i=1}^{n} f(s_i)x^{s_i} = \sum_{i=1}^{n} f_i x^{s_i}$, where $f_i \neq 0$ and $s_i \neq s_j$ for $i \neq j$. Of course, the monoid ring $F_2[x; S]$ is a polynomial ring in one indeterminate if $S = \mathbb{Z}_{\geq 0}$ (the set of non-negative integers).

The concept of degree and order are not generally defined in monoid rings. However, if we consider S to be a totally ordered monoid, we can define degree and order of an element of monoid ring $F_2[x; S]$ in the following manner: if $f = \sum_{i=1}^{n} f_i x^{s_i}$ is the canonical form of the non-zero element $f \in F_2[x; S]$, where $s_1 < s_2 < \ldots < s_n$, then s_n is called the degree of f written as $\deg(f) = s_n$ and s_1 is the order of f written as $ord(f) = s_1$.

A polynomial ring $F_2[x]$ is initially a monoid ring $F_2[x; S]$, where S is an additive monoid $\mathbb{Z}_{\geq 0}$. It can be observed that $F_2[x] \subset F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ only when $a = 1$. This forces us to first define cyclic codes using monoid ring $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$ and then define cyclic codes using monoid ring $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$. As $F_2\left[x; a\mathbb{Z}_{\geq 0}\right] \subset F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$, also $F_2\left[x; a\mathbb{Z}_{\geq 0}\right] \subset F_2[x]$ for all $a \geq 1$. Where both the monoids $a\mathbb{Z}_{\geq 0}$ and $\frac{a}{b}\mathbb{Z}_{\geq 0}$ are totally ordered, so degree and order of elements in $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$ and $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ are defined. The indeterminate of polynomials in monoid rings $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$ and $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ are respectively given by x^a and $x^{\frac{a}{b}}$, and they behave like an indeterminate x in $F_2[x]$. The arbitrary elements in $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$ and $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ are $f(x^a) = 1 + (x^a) + (x^a)^2 + \ldots (x^a)^n$ and $f\left(x^{\frac{a}{b}}\right) = 1 + \left(x^{\frac{a}{b}}\right) + \left(x^{\frac{a}{b}}\right)^2 + \ldots \left(x^{\frac{a}{b}}\right)^n$ and we call them generalized polynomials.

The construction of a BCH code in the factor ring $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]_n$ is similar to that of a BCH code in $F_2[x]_n$, as $F_2\left[x; a\mathbb{Z}_{\geq 0}\right] \subset F_2[x]$. For this, let C_n be a binary BCH code based on the positive integers $c, d, q = 2$ and n such that $2 \leq d \leq n$ with $gcd(n, 2) = 1$ and $n = 2^s - 1$, where s is the degree of a primitive polynomial in $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$. Consequently, the length n binary BCH code C_n has generator polynomial of degree r given by $g(x^a) = lcm\{m_i(x^a) : i = c, c+1, \ldots, c+d-2\}$, where $m_i(x^a)$ are minimal polynomials of ξ^i for $i = c, c+1, \ldots, c+d-2$. Where ξ is the primitive nth root of unity in F_{2^s}, an s degree Galois field extension of F_2. Since $m_i(x^a)$ divides $(x^a)^n - 1$ for each i, it follows that $g(x^a)$ divides $(x^a)^n - 1$. This implies $C_n = \left(g(x^a)\right)$ is a principal ideal in the factor ring $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]_n$.

In the following example, primitive BCH code of length 15 is discussed using monoid ring $F_2\left[x; 2\mathbb{Z}_{\geq 0}\right]$.

Example 1. *Let $p\left(x^2\right) = \left(x^2\right)^4 + \left(x^2\right) + 1$ be a primitive polynomial in $F_2\left[x; 2\mathbb{Z}_0\right]$, then we have a primitive BCH code of length $n = 2^4 - 1 = 15$. Let ξ be a primitive root in $GF\left(2^4\right)$, satisfying the relation $\xi^4 + \xi + 1 = 0$. Using this relation we have $\xi^{15} = 1$, that is ξ is the primitive 15th root of unity. Since $g\left(x^2\right) = lcm\{m_i\left(x^2\right), i = c, c+1, \ldots, c+d-2\}$; therefore, first we calculate $m_i\left(x^2\right)$. By ([19], Theorem 4.4.2), ξ, ξ^2, ξ^4, ξ^8 have same minimal polynomial $m_1\left(x^2\right) = p\left(x^2\right)$. Similarly we get $m_3\left(x^2\right) = \left(x^2\right)^4 + \left(x^2\right)^3 + \left(x^2\right)^2 + \left(x^2\right) + 1$, $m_5\left(x^2\right) = \left(x^2\right)^2 + \left(x^2\right) + 1$ and $m_7\left(x^2\right) = \left(x^2\right)^4 + \left(x^2\right)^3 + 1$.*

The BCH code with designed distance $d = 3$ has generator polynomial $g\left(x^2\right) = m_1\left(x^2\right) = \left(x^2\right)^4 + \left(x^2\right) + 1$. It has a minimum distance of at least 3 and corrects up to 1 error. Since the generator polynomial is of degree 4, it is therefore a $(15, 11)$ code having code rate $R = 0.733$. BCH codes of length 15 with different design distances are discussed in Table 1.

3 BCH codes as ideals in $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]_{bn}$

In this section, we investigate the values of b for which there exists a BCH code of length bn in $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]_{bn}$, corresponding to a length n binary BCH code C_n in $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]_n$. For this, let C_n be a binary BCH code in $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]_n$ constructed in previous section. Now using the following map $p\left(x^a\right) = p_0 + p_1 x^a + \ldots + p_{n-1}\left(x^a\right)^{n-1} \mapsto p_0 + p_1\left(x^{\frac{a}{b}}\right)^b + \ldots + p_{n-1}\left(x^{\frac{a}{b}}\right)^{b(n-1)} = p\left(x^{\frac{a}{b}}\right)$, we convert the s degree primitive polynomial $p(x^a)$ in $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$ to a bs degree polynomial $p\left(x^{\frac{a}{b}}\right)$ in $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$. This converted polynomial is never primitive; therefore, the corresponding BCH code will also be non-primitive. However, the non-primitive BCH code can be constructed only when $p\left(x^{\frac{a}{b}}\right)$ is irreducible. Hence, for the construction of a non-primitive BCH code in $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]_{bn}$, we choose only such a primitive irreducible polynomial $p\left(x^a\right)$ in $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$ for which there is an irreducible polynomial $p\left(x^{\frac{a}{b}}\right)$ in $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$.

Table 1 BCH codes of length 15

d	(n, k)	*t*	*R*
3	$(15, 11)$	1	0.733
5	$(15, 7)$	2	0.466
7	$(15, 5)$	3	0.333
15	$(15, 1)$	7	0.066

Table 2 Irreducible polynomials $p\left(x^{\frac{a}{b}}\right)$ against primitive polynomials $p(x^a)$

deg	$p\left(x^a\right)$	$p\left(x^{\frac{a}{b}}\right)$
2	$(x^a)^2 + (x^a) + 1$	$\left(x^{\frac{a}{3}}\right)^6 + \left(x^{\frac{a}{3}}\right)^3 + 1$
3	$(x^a)^3 + (x^a) + 1$	$\left(x^{\frac{a}{7}}\right)^{21} + \left(x^{\frac{a}{7}}\right)^7 + 1$
4	$(x^a)^4 + (x^a) + 1$	$\left(x^{\frac{a}{3}}\right)^{12} + \left(x^{\frac{a}{3}}\right)^3 + 1, \left(x^{\frac{a}{5}}\right)^{20} + \left(x^{\frac{a}{5}}\right)^5 + 1$
6	$(x^a)^6 + (x^a) + 1$	$\left(x^{\frac{a}{3}}\right)^{18} + \left(x^{\frac{a}{3}}\right)^3 + 1, \left(x^{\frac{a}{7}}\right)^{42} + \left(x^{\frac{a}{7}}\right)^7 + 1$
8	$(x^a)^8 + (x^a)^4 + (x^a)^3$ $+(x^a)^2 + 1$	$\left(x^{\frac{a}{3}}\right)^{24} + \left(x^{\frac{a}{3}}\right)^{12} + \left(x^{\frac{a}{3}}\right)^9 + \left(x^{\frac{a}{3}}\right)^6 + 1,$ $\left(x^{\frac{a}{5}}\right)^{40} + \left(x^{\frac{a}{5}}\right)^{20} + \left(x^{\frac{a}{5}}\right)^{15} + \left(x^{\frac{a}{5}}\right)^{10} + 1$
9	$(x^a)^9 + (x^a)^4 + 1$	$\left(x^{\frac{a}{7}}\right)^{63} + \left(x^{\frac{a}{7}}\right)^{28} + 1$
10	$(x^a)^{10} + (x^a)^3 + 1$	$\left(x^{\frac{a}{3}}\right)^{30} + \left(x^{\frac{a}{3}}\right)^9 + 1$
$\vdots$	$\vdots$	$\vdots$

Particularly for $b = 2$ or $2l$, there neither exists a primitive BCH code nor a non-primitive BCH code, since we know that $p\left(x^2\right) = (p(x))^2$ in $F_2[x]$, the same result holds in $F_2\left[x; \frac{a}{2}\mathbb{Z}_{\geq 0}\right]$. Similarly, for $s = 5, 7, 11, 13, 17, \ldots$ and there multiples we do not find any b for which we have an irreducible polynomial in $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$.

For instance, see Table 2 for the list of irreducible polynomials of degree bs in $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ corresponding to primitive irreducible polynomial of degree s in $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$.

Table 2 explains that for $s = 2$ and 3 we have $b = 3$ and 7 and for $s = 4$ and 6 we have $b = (3, 5)$ and $(3, 7)$, respectively, and similarly we have for their multiples. From this, we have the list of BCH codes of length n and bn, where bn divides $2^{bs} - 1$, mentioned in Table 3.

The above discussion can be summed up with the following result.

Proposition 2. *Let $p\left(x^a\right) \in F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$ be a primitive irreducible polynomial of degree $s \in \{2l, 3l, 4l, 6l\}$, where $l \in \mathbb{Z}^+$. Then the corresponding bs degree generalized*

Table 3 BCH codes of length n and bn w.r.t s

s	*n*	*bn*
2	3	9
3	7	49
4	15	4575
6	63	189,441
8	255	765,1275
9	511	3577
10	1023	1023
$\vdots$	$\vdots$	$\vdots$

polynomial $p\left(x^{\frac{a}{b}}\right)$ *in* $F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ *is non-primitive irreducible polynomial for* $b \in \{3,7,\{3,5\},\{3,7\}\}$, *respectively.*

Proof. Let $p(x^a) = 1 + x^a + \ldots + (x^a)^s$ be a primitive irreducible polynomial in $F_2\left[x;a\mathbb{Z}_{\geq 0}\right]$, where $s \in \{2l,3l,4l,6l\}$, where $l \in \mathbb{Z}^+$ such that α is its root and $\alpha^{2^s-1} = 1$. Then the corresponding generalized polynomial $p\left(x^{\frac{a}{b}}\right) = 1 + \left(x^{\frac{a}{b}}\right)^b + \ldots + \left(x^{\frac{a}{b}}\right)^{bs}$ in $F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ has root $\beta = (p_{si})^M \in F_2^{bs}$, where p_{si} is a primitive element in F_2^{bs} and M is a positive integer such that $M\left(b(2^s-1)\right) = 2^{bs}-1$. This implies $\beta^{b(2^s-1)} = 1$. Hence $p\left(x^{\frac{a}{b}}\right)$ is not primitive. But, $p\left(x^{\frac{a}{b}}\right)$ is irreducible over F_2 for $b \in \{3,7,\{3,5\},\{3,7\}\}$, respectively by ([20], Theorem 5.1 and Example 5.4) where the indeterminate $x^{\frac{a}{b}}$ behaves as indeterminate x. □

Theorem 3. *Let* $n = 2^s - 1$ *be the length of primitive BCH code* C_n, *where* $p(x^a) \in F_2\left[x;a\mathbb{Z}_{\geq 0}\right]$ *is a primitive irreducible polynomial of degree s such that* $p\left(x^{\frac{a}{b}}\right) \in F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ *is irreducible polynomial of degree bs.*

1) *Then, for positive integers* c', d', bn *such that* $2 \leq d' \leq bn$ *and bn is relatively prime to 2, there exists a non-primitive binary BCH code* C_{bn} *of length bn, where bn is order of an element* $\alpha \in F_{2^{bs}}$.
2) *The non-primitive BCH code* C_{bn} *of length bn is defined as*

$$C_{bn} = \{v\left(x^{\frac{a}{b}}\right) \in F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]_{bn} : v(\alpha^i) = 0 \text{ for all } i = c', c'+1, \ldots c'+d'-2.$$

Equivalently, C_{bn} *is the null space of the matrix*

$$H = \begin{bmatrix} 1 & \alpha^{c'} & \alpha^{2c'} & \cdots & \alpha^{(bn-1)c'} \\ 1 & \alpha^{c'+1} & \alpha^{2(c'+1)} & \cdots & \alpha^{(bn-1)(c'+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{c'+d'-2} & \alpha^{2(c'+d'-2)} & \cdots & \alpha^{(bn-1)(c'+d'-2)} \end{bmatrix}.$$

Proof. 1) Since it is given that the bs degree polynomial $p\left(x^{\frac{a}{b}}\right) \in F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ is not primitive, so the BCH code constructed through it is also not primitive. Hence the length of the code $n \neq 2^{bs}-1$. However, there is an element $\alpha \in F_{2^{bs}}$ of order bn vanishing $p\left(x^{\frac{a}{b}}\right)$. Let $m_i\left(x^{\frac{a}{b}}\right) \in F_2\left[x;\frac{a}{b}\mathbb{Z}_0\right]$ denotes the minimal polynomial of α^i and $g\left(x^{\frac{a}{b}}\right)$ be the *lcm* of distinct polynomials among $m_i\left(x^{\frac{a}{b}}\right)$, $i = c', c'+1, \ldots, c'+d'-2$; that is,

$$g\left(x^{\frac{a}{b}}\right) = \text{lcm}\{m_i\left(x^{\frac{a}{b}}\right) : i = c', c'+1, \ldots, c'+d'-2\}.$$

As $m_i\left(x^{\frac{a}{b}}\right)$ divides $\left(x^{\frac{a}{b}}\right)^{bn} - 1$ for each i, therefore $g\left(x^{\frac{a}{b}}\right)$ also divides $\left(x^{\frac{a}{b}}\right)^{bn} - 1$. This implies that C_{bn} is a principal ideal generated by $g\left(x^{\frac{a}{b}}\right)$ in the factor ring $F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]_{bn}$. Hence, C_{bn} is a non-primitive BCH code of length bn over $F_2$with designed distance d'.

2) Let $v\left(x^{\frac{a}{b}}\right) \in C_{bn}$, then $v\left(x^{\frac{a}{b}}\right) = g\left(x^{\frac{a}{b}}\right)q\left(x^{\frac{a}{b}}\right)$ for some $q\left(x^{\frac{a}{b}}\right) \in F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]$, where $g\left(x^{\frac{a}{b}}\right)$ is the generator polynomial of C_{bn}. Hence, $v(\alpha^i) = 0$ for all $i = c', c'+1, \ldots c'+d'-2$. Conversely, let $v\left(x^{\frac{a}{b}}\right) \in F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]_{bn}$ such that $v(\alpha^i) = 0$ for all $i = c', c'+1, \ldots c'+d'-2$. Then $m_i\left(x^{\frac{a}{b}}\right)$ divides $v\left(x^{\frac{a}{b}}\right)$ for all $i = c', c'+1, \ldots c'+d'-2$. Hence $g\left(x^{\frac{a}{b}}\right)$ divides $v\left(x^{\frac{a}{b}}\right)$, so $v\left(x^{\frac{a}{b}}\right) \in C_{bn}$.

For the second part, let $v\left(x^{\frac{a}{b}}\right) = v_0 + v_1\left(x^{\frac{a}{b}}\right) + \ldots v_{bn-1}\left(x^{\frac{a}{b}}\right)^{bn-1} \in F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]_{bn}$. Then, $v(\alpha^i) = 0$ for all $i = c', c'+1, \ldots c'+d'-2$ if and only if $Hv^T = 0$, where $v = (v_0, v_1, \ldots v_{bn-1}) \in F_2^{bn}$. This proves that C_{bn} is the null space of H. □

Remark 4. *Corresponding to the* (n,k) *BCH code* C_n *with generator polynomial* $g(x^a) = p(x^a)$ *in* $F_2\left[x;a\mathbb{Z}_{\geq 0}\right]$, *we have a* (bn,bk) *BCH code* C_{bn} *with generating polynomial* $g\left(x^{\frac{a}{b}}\right) = p\left(x^{\frac{a}{b}}\right)$ *in* $F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]$. *This* (bn,bk) *BCH code* C_{bn} *is an interleaved code of degree b, capable of correcting a single error burst of length b or less (see [21], Theorem 11.1).*

The following example illustrates the construction of a non-primitive BCH code of length bn through $F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]$.

Example 5. *For a primitive polynomial* $p(x^2) = 1 + (x^2) + (x^2)^4$ *in* $F_2[x;2\mathbb{Z}_{\geq 0}]$, *there is a non-primitive irreducible polynomial* $p\left(x^{\frac{2}{3}}\right) = 1 + \left(x^{\frac{2}{3}}\right)^3 + \left(x^{\frac{2}{3}}\right)^{12}$ *in* $F_2\left[x;\frac{2}{3}\mathbb{Z}_{\geq 0}\right]$. *Let* $\alpha \in F_{2^{12}}$, *satisfies the relation* $\alpha^{12} + \alpha^3 + 1 = 0$. *Using this relation, we can compute all the distinct powers of* α *in* $GF(2^{12})$, *see Table 4 (it is clear that* α *has order 45). Here, we have* $bn = n' = 3 \times 15 = 45$. *To calculate the generating polynomial* $g\left(x^{\frac{2}{3}}\right)$, *we first calculate the minimal polynomials which are :* $m_1'\left(x^{\frac{2}{3}}\right) = \left(x^{\frac{2}{3}}\right)^{12} + \left(x^{\frac{2}{3}}\right)^3 + 1$, $m_3'\left(x^{\frac{2}{3}}\right) = \left(x^{\frac{2}{3}}\right)^4 + \left(x^{\frac{2}{3}}\right) + 1$, $m_5'\left(x^{\frac{2}{3}}\right) = \left(x^{\frac{2}{3}}\right)^6 + \left(x^{\frac{2}{3}}\right)^3 + 1$, $m_7'\left(x^{\frac{2}{3}}\right) = \left(x^{\frac{2}{3}}\right)^{12} + \left(x^{\frac{2}{3}}\right)^9 + 1$, $m_9'\left(x^{\frac{2}{3}}\right) = \left(x^{\frac{2}{3}}\right)^4 + \left(x^{\frac{2}{3}}\right)^3 + \left(x^{\frac{2}{3}}\right)^2 + \left(x^{\frac{2}{3}}\right) + 1$, $m_{15}'\left(x^{\frac{2}{3}}\right) = \left(x^{\frac{2}{3}}\right)^2 + \left(x^{\frac{2}{3}}\right) + 1$, $m_{21}'\left(x^{\frac{2}{3}}\right) = \left(x^{\frac{2}{3}}\right)^4 + \left(x^{\frac{2}{3}}\right)^3 + 1$.

Table 4 Distinct powers of α GF$\left(2^{12}\right)$

$\alpha^{12}=\alpha^3+1$	$\alpha^{21}=1+\alpha^3+\alpha^9$	$\alpha^{30}=1+\alpha^3+\alpha^6$	$\alpha^{39}=1+\alpha^6+\alpha^9$
$\alpha^{13}=\alpha+\alpha^4$	$\alpha^{22}=\alpha+\alpha^4+\alpha^{10}$	$\alpha^{31}=\alpha+\alpha^4+\alpha^7$	$\alpha^{40}=\alpha+\alpha^7+\alpha^{10}$
$\alpha^{14}=\alpha^2+\alpha^5$	$\alpha^{23}=\alpha^2+\alpha^5+\alpha^{11}$	$\alpha^{32}=\alpha^2+\alpha^5+\alpha^8$	$\alpha^{41}=\alpha^2+\alpha^8+\alpha^{11}$
$\alpha^{15}=\alpha^3+\alpha^6$	$\alpha^{24}=1+\alpha^6$	$\alpha^{33}=\alpha^3+\alpha^6+\alpha^9$	$\alpha^{42}=1+\alpha^9$
$\alpha^{16}=\alpha^4+\alpha^7$	$\alpha^{25}=\alpha+\alpha^7$	$\alpha^{34}=\alpha^4+\alpha^7+\alpha^{10}$	$\alpha^{43}=\alpha+\alpha^{10}$
$\alpha^{17}=\alpha^5+\alpha^8$	$\alpha^{26}=\alpha^8+\alpha^2$	$\alpha^{35}=\alpha^5+\alpha^8+\alpha^{11}$	$\alpha^{44}=\alpha^2+\alpha^{11}$
$\alpha^{18}=\alpha^6+\alpha^9$	$\alpha^{27}=\alpha^3+\alpha^9$	$\alpha^{36}=1+\alpha^3+\alpha^6+\alpha^9$	$\alpha^{45}=1$
$\alpha^{19}=\alpha^7+\alpha^{10}$	$\alpha^{28}=\alpha^4+\alpha^{10}$	$\alpha^{37}=\alpha+\alpha^4+\alpha^7+\alpha^{10}$	
$\alpha^{20}=\alpha^8+\alpha^{11}$	$\alpha^{29}=\alpha^5+\alpha^{11}$	$\alpha^{38}=\alpha^2+\alpha^5+\alpha^8+\alpha^{11}$	

Which gives the following generating polynomials of BCH codes of length 45 with design distance $d'=3,5,7,9,15,21$ *and* 45.

$$\begin{aligned}
g\left(x^{\frac{2}{3}}\right) &= 1+\left(x^{\frac{2}{3}}\right)^{3}+\left(x^{\frac{2}{3}}\right)^{12}, g\left(x^{\frac{2}{3}}\right)=\left(x^{\frac{2}{3}}\right)^{16}+\left(x^{\frac{2}{3}}\right)^{13}\\
&\quad+\left(x^{\frac{2}{3}}\right)^{12}+\left(x^{\frac{2}{3}}\right)^{7}+\left(x^{\frac{2}{3}}\right)^{3}+\left(x^{\frac{2}{3}}\right)+1\\
g\left(x^{\frac{2}{3}}\right) &= \left(x^{\frac{2}{3}}\right)^{22}+\left(x^{\frac{2}{3}}\right)^{18}+\left(x^{\frac{2}{3}}\right)^{15}+\left(x^{\frac{2}{3}}\right)^{12}+\left(x^{\frac{2}{3}}\right)^{10}\\
&\quad+\left(x^{\frac{2}{3}}\right)^{9}+\left(x^{\frac{2}{3}}\right)^{4}+\left(x^{\frac{2}{3}}\right)+1\\
g\left(x^{\frac{2}{3}}\right) &= \left(x^{\frac{2}{3}}\right)^{34}+\left(x^{\frac{2}{3}}\right)^{31}+\left(x^{\frac{2}{3}}\right)^{30}+\left(x^{\frac{2}{3}}\right)^{19}+\left(x^{\frac{2}{3}}\right)^{16}\\
&\quad+\left(x^{\frac{2}{3}}\right)^{15}+\left(x^{\frac{2}{3}}\right)^{4}+\left(x^{\frac{2}{3}}\right)+1\\
g\left(x^{\frac{2}{3}}\right) &= \left(x^{\frac{2}{3}}\right)^{38}+\left(x^{\frac{2}{3}}\right)^{37}+\left(x^{\frac{2}{3}}\right)^{36}+\left(x^{\frac{2}{3}}\right)^{34}+\left(x^{\frac{2}{3}}\right)^{30}\\
&\quad+\left(x^{\frac{2}{3}}\right)^{23}+\left(x^{\frac{2}{3}}\right)^{22}+\left(x^{\frac{2}{3}}\right)^{21}+\left(x^{\frac{2}{3}}\right)^{19}+\left(x^{\frac{2}{3}}\right)^{15}\\
&\quad+\left(x^{\frac{2}{3}}\right)^{8}+\left(x^{\frac{2}{3}}\right)^{7}+\left(x^{\frac{2}{3}}\right)^{6}+\left(x^{\frac{2}{3}}\right)^{4}+1\\
g\left(x^{\frac{2}{3}}\right) &= \left(x^{\frac{2}{3}}\right)^{40}+\left(x^{\frac{2}{3}}\right)^{38}+\left(x^{\frac{2}{3}}\right)^{35}+\left(x^{\frac{2}{3}}\right)^{34}+\left(x^{\frac{2}{3}}\right)^{32}\\
&\quad+\left(x^{\frac{2}{3}}\right)^{31}+\left(x^{\frac{2}{3}}\right)^{30}+\left(x^{\frac{2}{3}}\right)^{25}+\left(x^{\frac{2}{3}}\right)^{23}+\left(x^{\frac{2}{3}}\right)^{20}\\
&\quad+\left(x^{\frac{2}{3}}\right)^{19}+\left(x^{\frac{2}{3}}\right)^{17}+\left(x^{\frac{2}{3}}\right)^{16}+\left(x^{\frac{2}{3}}\right)^{15}+\left(x^{\frac{2}{3}}\right)^{10}\\
&\quad+\left(x^{\frac{2}{3}}\right)^{8}+\left(x^{\frac{2}{3}}\right)^{5}+\left(x^{\frac{2}{3}}\right)^{4}+\left(x^{\frac{2}{3}}\right)^{2}+\left(x^{\frac{2}{3}}\right)+1\\
g\left(x^{\frac{2}{3}}\right) &= \left(x^{\frac{2}{3}}\right)^{44}+\left(x^{\frac{2}{3}}\right)^{43}+\left(x^{\frac{2}{3}}\right)^{42}+\ldots+\left(x^{\frac{2}{3}}\right)^{2}+\left(x^{\frac{2}{3}}\right)+1
\end{aligned}$$

Which generates $(45,33),(45,29),(45,23),(45,11),$ $(45,7),(45,5)$ *and* $(45,1)$ *codes and corrects up to 1, 2, 3, 4, 7, 10, and 22 errors having code rate* $0.733, 0.644, 0.511, 0.244, 0.155, 0.11, 0.022,$ *respectively. Where the code* $(45,33)$ *is also capable of correcting any single error burst of length 3 or less by Remark 4.*

Table 5 gives comparison between minimum distance, code rate and error correction capability of codes C_{15}, C_{45} in $F_2\left[x;2\mathbb{Z}_{\geq 0}\right]$, $F_2\left[x;\frac{2}{3}\mathbb{Z}_{\geq 0}\right]$, respectively.

Now, we are in position to develop a link between a primitive $(n,n-r)$ binary BCH code C_n and a non-primitive $(bn,bn-r')$ binary BCH code C_{bn}, where r and r' are, respectively, the degrees of their generating polynomials $g\left(x^a\right)$ and $g\left(x^{\frac{a}{b}}\right)$.

From Theorem 3(1), it follows that the generalized polynomial $g\left(x^{\frac{a}{b}}\right)\in F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ divides $\left(x^{\frac{a}{b}}\right)^{bn}-1$ in $F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]$. So, there is a non-primitive BCH code C_{bn} generated by $g\left(x^{\frac{a}{b}}\right)$ in $F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]_{bn}$. By the same argument, as bn divides $n'=2^{bs}-1$, so $\left(x^{\frac{a}{b}}\right)^{bn}-1$ divides $\left(x^{\frac{a}{b}}\right)^{n'}-1$ in $F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]$. It follows that $\left(\left(x^{\frac{a}{b}}\right)^{n'}-1\right)\subset\left(\left(x^{\frac{a}{b}}\right)^{bn}-1\right)$. Consequently, third isomorphism theorem for rings gives

$$\frac{F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]/\left(\left(x^{\frac{a}{b}}\right)^{n'}-1\right)}{\left(\left(x^{\frac{a}{b}}\right)^{bn}-1\right)/\left(\left(x^{\frac{a}{b}}\right)^{n'}-1\right)}\simeq\frac{F_2\left[x;\frac{a}{b}\mathbb{Z}_{\geq 0}\right]}{\left(\left(x^{\frac{a}{b}}\right)^{bn}-1\right)}\simeq\frac{F_2\left[x;a\mathbb{Z}_{\geq 0}\right]}{\left(\left(x^{a}\right)^{n}-1\right)}.$$

Thus, there is embedding $C_n\hookrightarrow C_{bn}\hookrightarrow C_{n'}$ of codes, whereas C_n, C_{bn}, and $C_{n'}$ are, respectively, primitive BCH, non-primitive BCH and primitive BCH codes. Whereas the embedding $C_n\hookrightarrow C_{bn}$ is defined as:

$$\begin{aligned}
a\left(x^{a}\right)=a_0+a_1\left(x^{a}\right)+\ldots+a_{n-1}\left(x^{a}\right)^{n-1}&\mapsto a_0+a_1\left(x^{\frac{a}{b}}\right)^{b}\\
+\ldots+a_{n-1}\left(x^{\frac{a}{b}}\right)^{b(n-1)}&=a\left(x^{\frac{a}{b}}\right).
\end{aligned}$$

Where $a\left(x^{a}\right)\in C_n$ and $a\left(x^{\frac{a}{b}}\right)\in C_{bn}$.

Table 5 Comparison of codes C15 and C45

(n,k)	d	t	R	(n,k)	d'	t_1	R_1
$(15,11)$	3	1	0.733	$(45,33)$	3	1	0.733
$(15,7)$	5	2	0.466	$(45,29)$	5	2	0.644
$(15,5)$	7	3	0.333	$(45,23)$	7	3	0.511
$(15,1)$	15	7	0.066	$(45,11)$	9	4	0.244
				$(45,7)$	15	7	0.155
				$(45,5)$	21	10	0.11
				$(45,1)$	45	22	0.022

The above discussion shapes the following.

Theorem 6. *Let C_n be a primitive binary BCH code of length $n = 2^s - 1$ generated by r degree polynomial $g(x^a)$ in $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]$, then:*

1) *There exists a bn length binary non-primitive BCH code C_{bn} generated by br degree polynomial $g\left(x^{\frac{a}{b}}\right)$ in $F_2\left[x; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$; and*
2) *The binary primitive BCH code C_n is embedded in the binary non-primitive BCH code C_{bn}.*

Also, we can deduce $g\left(x^a\right)$ from $g\left(x^{\frac{a}{b}}\right)$ by substituting x^a for y^b.

Example 7. *Following Examples 1 and 5:*

The BCH codes with designed distance $d = 3$ have generator polynomials $g(x^2) = m_1(x^2) = 1 + (x^2) + (x^2)^4$ and $g\left(x^{\frac{2}{3}}\right) = 1 + \left(x^{\frac{2}{3}}\right)^3 + \left(x^{\frac{2}{3}}\right)^{12}$ with the same error correction capability and code rate. The only difference is that the degree, data bits, code length, and check sum of the code C_{45} is three times that of code C_{15}.

Whereas, on letting $\left(x^{\frac{2}{3}}\right) = y$ in the generating polynomial of $(45, 29)$ code, that is $x^2 = y^3$, we get

$$\begin{aligned} g\left(x^{\frac{2}{3}}\right) &= \left(x^{\frac{2}{3}}\right)^{16} + \left(x^{\frac{2}{3}}\right)^{13} + \left(x^{\frac{2}{3}}\right)^{12} + \left(x^{\frac{2}{3}}\right)^{7} + \left(x^{\frac{2}{3}}\right)^{3} \\ &\quad + \left(x^{\frac{2}{3}}\right) + 1 \\ g(y) &= (y)^{16} + (y)^{13} + (y)^{12} + (y)^7 + (y)^3 + (y) + 1 \\ g\left(y^3\right) &= \left(y^3\right)^{16} + \left(y^3\right)^{13} + \left(y^3\right)^{12} + \left(y^3\right)^{7} + \left(y^3\right)^{3} + \left(y^3\right) + 1 \\ g\left(x^2\right) &= \left(x^2\right)^{16} + \left(x^2\right)^{13} + \left(x^2\right)^{12} + \left(x^2\right)^{7} + \left(x^2\right)^{3} + \left(x^2\right) + 1 \\ &= (x^2)^{13} + (x^2)^{12} + (x^2)^7 + (x^2)^3 + 1 \in F_2\left[x; 2\mathbb{Z}_{\geq 0}\right]_{15}. \end{aligned}$$

Where the generating polynomial $(x^2)^4 + (x^2) + 1$ divides $(x^2)^{13} + (x^2)^{12} + (x^2)^7 + (x^2)^3 + 1$. Hence, the corresponding vector is in $(15, 11)$. So $(15, 11)$ code is embedded in $(45, 29)$ code.

Similarly, in Table 6, we have shown that which code in $F_2\left[x; 2\mathbb{Z}_{\geq 0}\right]_{15}$ with designed distance d is embedded in a code in $F_2\left[x; \frac{2}{3}\mathbb{Z}_{\geq 0}\right]_{45}$ with designed distance d'.

Table 6 Embedding of codes C15 in C45

d'	(bn, k')	t'	R'	d	(n, k)	t	R
5	(45, 29)	2	0.644	3	(15, 11)	1	0.733
7	(45, 23)	3	0.511	4	(15, 11)	1	0.733
9	(45, 11)	4	0.244	6	(15, 11)	1	0.733
15	(45, 7)	7	0.155	7	(15, 7)	2	0.466
21	(45, 5)	10	0.11	10	(15, 5)	3	0.333
45	(45, 1)	22	0.022	15	(15, 1)	7	0.066

The corresponding code vectors of the generating polynomials

$$\begin{aligned} g(x^2) &= (x^2)^8 + (x^2)^7 + (x^2)^6 + (x^2)^4 + 1 \textit{ and} \\ g\left(x^{\frac{2}{3}}\right) &= \left(x^{\frac{2}{3}}\right)^{38} + \left(x^{\frac{2}{3}}\right)^{37} + \left(x^{\frac{2}{3}}\right)^{36} + \left(x^{\frac{2}{3}}\right)^{34} + \left(x^{\frac{2}{3}}\right)^{30} \\ &\quad + \left(x^{\frac{2}{3}}\right)^{23} + \left(x^{\frac{2}{3}}\right)^{22} + \left(x^{\frac{2}{3}}\right)^{21} + \left(x^{\frac{2}{3}}\right)^{19} + \left(x^{\frac{2}{3}}\right)^{15} \\ &\quad + \left(x^{\frac{2}{3}}\right)^{8} + \left(x^{\frac{2}{3}}\right)^{7} + \left(x^{\frac{2}{3}}\right)^{6} + \left(x^{\frac{2}{3}}\right)^{4} + 1 \textit{ are} \end{aligned}$$

$$\begin{aligned} v &= (100010111000000) \\ v' &= (100010111000000 \\ &\quad\; 100010111000000 \\ &\quad\; 100010111000000). \end{aligned}$$

Clearly v is properly contained in v'; in fact, it is repeated three times after a particular pattern. Hence, the generating matrix G' of $g\left(x^{\frac{2}{3}}\right)$ will contain the generating matrix G of $g(x^2)$ such that $G' = \oplus_1^3 G$.

The following lemma explains the relation between the minimal polynomials of the narrow sense BCH codes C_n and C_{bn}.

Lemma 8. *Let d, d' be the design distances of the narrow sense BCH codes C_n and C_{bn}, respectively. Then the exponents of the minimal polynomials $m_i\left(x^a\right), i = 1, 3, \ldots, d - 1$ of the code C_n are equal to the exponents of the following minimal polynomials $m_b\left(x^{\frac{a}{b}}\right)$, $m_{3b}\left(x^{\frac{a}{b}}\right), \ldots, m_{b(d-1)}\left(x^{\frac{a}{b}}\right)$ of the code C_{bn} with the same number of non-zero terms. The remaining minimal polynomials of the code C_{bn} have exponents three times the exponents of the minimal polynomials $m_i\left(x^a\right), i = 1, 3, \ldots, d-1$ of the code C_n with same number of non-zero terms.*

Proof is straightforward and easily follows from Examples 1 and 2.

4 General decoding principle

As the binary BCH code C_n is embedded in the binary non-primitive BCH code C_{bn}, we only describe the decoding principal for the code C_{bn}. We use the decoding procedure which follows the same principle as of the primitive binary BCH code.

Take $a' \in F_2^{bn}$ as a received vector. We obtain the syndrome matrix of a', $S(a') = a'H^T$. In this way, we calculate a table of syndromes which is useful in determining the error vector e such that $S\left(a'\right) = S(e)$. So, the decoding of received vector a' has done as the transmitted vector $v' = a' - e$. We adopt the algebraic method for finding e from the syndrome vector $S\left(a'\right)$.

Let C_{bn} be the binary non-primitive BCH code with length bn and designed distance d'. Let H be the $(d' - 1) \times bn$ matrix over $F_{2^{bs}}$. We use this matrix to define the syndrome of a vector $a' \in F_2^{bn}$ as $S(a') = a'H^T$. Writing $a' = \left(a'_0, a'_1, \ldots, a'_{bn-1}\right)$ in the polynomial form $a'(x^{\frac{a}{b}}) = a'_0 + a'_1\left(x^{\frac{a}{b}}\right) + a'_2\left(x^{\frac{a}{b}}\right)^2 + \ldots + a'_{bn-1}\left(x^{\frac{a}{b}}\right)^{bn-1}$. So, the syndrome of the vector a', $S(a')$ will be

$$\left[a'_0\ a'_1\ \ldots\ a'_{bn-1}\right]\begin{bmatrix} 1 & 1 & \ldots & 1\\ \alpha^{c'} & \alpha^{c'+1} & \ldots & \alpha^{c'+d'-2}\\ \alpha^{2c'} & \alpha^{2(c'+1)} & \ldots & \alpha^{2(c'+d'-2)}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha^{(bn-1)c'} & \alpha^{(bn-1)(c'+1)} & \ldots & \alpha^{(bn-1)(c'+d'-2)}\end{bmatrix},$$

and hence,

$$S\left(a'\right) = \left[S_{c'}\ S_{c'+1}\ \ldots\ S_{c'+d'-2}\right],$$

where $S_j = a'_0 + a'_1\alpha^j + \ldots a'_{bn-1}\alpha^{(bn-1)j} = a'(\alpha^j)$ for $j = c', c'+1, \ldots, c'+d'-2$. Now, let a codeword $v \in C_{bn}$ be transmitted and the vector received is $a' = v' + e$, where e is the error vector. Then $S(e) = S(a')$. Let $e\left(x^{\frac{a}{b}}\right) = e_0 + e_1\left(x^{\frac{a}{b}}\right) + e_2\left(x^{\frac{a}{b}}\right)^2 + \ldots + e_{bn-1}\left(x^{\frac{a}{b}}\right)^{bn-1}$ be the error polynomial. Suppose $i_1, \ldots, i_m$ be the positions where an error has occurred. Then, $e_i \neq 0$ if and only if $i \in I = \{i_1, \ldots, i_m\}$. Hence, $e\left(x^{\frac{a}{b}}\right) = \sum_{i\in I} e_i\left(x^{\frac{a}{b}}\right)^i$. Since the code corrects up to t errors, where $t = \left\lfloor \frac{d'-1}{2} \right\rfloor$. So we assume $m \leq t$, that is $2m < d'$. Since $S(e) = S(a')$, we have $e(\alpha^j) = S_j$ for $j = c', c'+1, \ldots, c'+d'-2$. Thus the $2m$ unknowns $i_1, \ldots, i_m$ and $e_{i_1}, \ldots, e_{i_m}$ satisfy the following system of $d'-1$ linear equations in $e_{i_1}, \ldots, e_{i_m}$:

$$\sum_{i=I} e_i\alpha^{ji} = S_j, j = c', c'+1, \ldots, c'+d'-2 \ldots..(1).$$

We first obtain a solution for the error positions $i_1, \ldots, i_m$. We define the error locator polynomial $f\left(x^{\frac{a}{b}}\right) = f_0 + f_1\left(x^{\frac{a}{b}}\right) + f_2\left(x^{\frac{a}{b}}\right)^2 + \ldots + f_{m-1}\left(x^{\frac{a}{b}}\right)^{m-1} + \left(x^{\frac{a}{b}}\right)^m$. Since $f\left(\alpha^i\right) = 0$ for each $i = I$, we have

$$f_0 + f_1\left(\alpha^i\right) + \ldots + f_{m-1}\left(\alpha^i\right)^{m-1} + \left(\alpha^i\right)^m = 0,$$

On multiplying this equation by $e_i\alpha^{ji}$, we get

$$f_0e_i\alpha^{ji} + f_1e_i\alpha^{(j+1)i} + \ldots f_{m-1}e_i\alpha^{(j+m-1)i} + e_i\alpha^{(j+m)i} = 0,$$

for each $i \in I$. Summing these m equations for $i = i_1, \ldots, i_r$ and using the relations (1), we have

$$f_0S_j + f_1S_{j+1} + \ldots f_{m-1}S_{j+m-1} + S_{j+m} = 0,$$

for each $j = c', c'+1, \ldots, c'+m-1$. Thus, the m unknowns $f_0, f_1, \ldots, f_{m-1}$ satisfy the following $m \times m$ system of linear equations:

$$\begin{bmatrix} S_c & S_{c+1} & \ldots & S_{c+m-1}\\ S_{c+1} & S_{c+2} & \ldots & S_{c+m}\\ \vdots & \vdots & \ddots & \vdots\\ S_{c+m-1} & S_{c+m} & \ldots & S_{c+2m-2}\end{bmatrix}\begin{bmatrix} f_0\\ f_1\\ \vdots\\ f_{m-1}\end{bmatrix} = \begin{bmatrix} S_{c+m}\\ S_{c+m+1}\\ \vdots\\ S_{c+2m-1}\end{bmatrix} \ldots..(2)$$

Let S denote the coefficient matrix in the above linear system. It can be verified by direct computation that $S = VDV^T$, where

$$V = \begin{bmatrix} 1 & 1 & \ldots & 1\\ \alpha^{i_1} & \alpha^{i_2} & \ldots & \alpha^{i_m}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha^{i_1(m-1)} & \alpha^{i_2(m-1)} & \ldots & \alpha^{i_m(m-1)}\end{bmatrix},$$

$$D = \begin{bmatrix} e_{i_1}\alpha^{i_{1c}} & 0 & \ldots & 0\\ 0 & e_{i_2}\alpha^{i_2c} & \ldots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \ldots & e_{i_m}\alpha^{i_mc}\end{bmatrix},$$

where V is a Vandermonde matrix. Since α is a non-primitive bnth root of unity in $F_{2^{bs}}$ and $i_1, \ldots i_m$ are distinct integers in $\{0, \ldots, bn-1\}$, we have $\alpha^{i_1}, \ldots, \alpha^{i_m}$ are all distinct. Hence, $\det V \neq 0$. Further, $e_{i_1}, \ldots, e_{i_m}$ are all non-zero and hence $\det D \neq 0$. Therefore, $\det S \neq 0$ and linear system (2) have a unique solution.

We have assumed that the number of positions where an error has occurred is $m \leq t$. If the actual number of error positions is less than m, then for any choice of distinct positions $i_1, \ldots i_m$, the coefficients $e_{i_1}, \ldots, e_{i_m}$ cannot be all zero. So, $\det D = 0$. Hence, m is the greatest positive integer $\leq t$ such that system (2) has a unique solution. Therefore, we find the value of m by taking successively $m = t, t-1, \ldots$ in system (2) until we have a value for which system (2) has a unique solution, which gives us the error locator polynomial $f\left(x^{\frac{a}{b}}\right) = f_0 + f_1\left(x^{\frac{a}{b}}\right) + f_2\left(x^{\frac{a}{b}}\right)^2 + \ldots + f_{m-1}\left(x^{\frac{a}{b}}\right)^{m-1} + \left(x^{\frac{a}{b}}\right)^m$. Now, to find the roots of $f\left(x^{\frac{a}{b}}\right)$, we put $x^{\frac{a}{b}} = \alpha^i$, $i = 0, 1, \ldots$. By the definition of $f\left(x^{\frac{a}{b}}\right)$, these roots are $\alpha^{i_1}, \ldots, \alpha^{i_m}$. Thus, we find the unique solution for the unknowns $i_1, \ldots i_m$. Having thus found the error vector e, we decode the received vector a as the codeword $v' = a' - e$.

To compute the syndrome of a binary BCH code, we have $S_2 = (S_1)^2, S_6 = (S_3)^2$ and so on. We can compute the syndrome more easily by using the division algorithm. If $m(x^{\frac{a}{b}})$ is the minimal polynomial of α, then $S_1 = a'(\alpha)$ can be obtained by finding the remainder on dividing $a'\left(x^{\frac{a}{b}}\right)$ by $m\left(x^{\frac{a}{b}}\right)$ and then putting $x^{\frac{a}{b}} = \alpha$ in it. In general, to find S_j, we divide $a'\left(x^{\frac{a}{b}}\right)$ by $m\left(x^{\frac{a}{b}}\right)$ and find the remainder.

The decoding of the code C_n from the decoding of the code C_{bn} can be obtained as; take $x^{\frac{a}{b}} = y$, which gives $x^a = y^b$. In this way, the code polynomial $v(x^{\frac{a}{b}})$ in $F_2[x; \frac{a}{b}\mathbb{Z}_{\geq 0}]_{bn}$ becomes $v'(y)$. Again on replacing y by y^b, we get $v'(y^b) = v'(x^a)$. The remainder after dividing $v(x^a)$ by $(x^a)^n - 1$, will be the decoded vector of $F_2\left[x; a\mathbb{Z}_{\geq 0}\right]_n$ and the generator polynomial $g(x^a)$ divides $v(x^a)$.

The above discussion can be sumed up in the following steps.

Step I: For binary non-primitive BCH code C_{bn} with designed distance d', let $a\left(x^{\frac{a}{b}}\right)$ be the received polynomial with m errors, where $m \leq t_2$.
Step II: Compute the syndromes and find the value of m, such that the system (2) has a unique solution.
Step III: Step II gives us the error locator polynomial $f\left(x^{\frac{a}{b}}\right)$. Now, find the roots of$f\left(x^{\frac{a}{b}}\right)$ through which we obtain the error polynomial $e\left(x^{\frac{a}{b}}\right)$.
Step IV: We decode the received polynomial $a'\left(x^{\frac{a}{b}}\right)$ as $v'\left(x^{\frac{a}{b}}\right) = a'\left(x^{\frac{a}{b}}\right) - e\left(x^{\frac{a}{b}}\right)$.
Step V: The code vector v in C_n can be dragged out from the decoded code vector v' in C_{bn} by putting $x^{\frac{a}{b}} = y$ in corresponding code polynomial $v'\left(x^{\frac{a}{b}}\right)$. This gives $v'\left(x^{\frac{a}{b}}\right) = v'(y)$. Again by replacing y by y^b, we get $v'(y) = v'(y^b) = v'(x^a)$.
Step VI: Divide $v'(x^a)$ by $(x^a)^n - 1$, the remainder $v(x^a)$ will be in $F_2[x; a\mathbb{Z}_{\geq 0}]_n$, and the generator polynomial $g(x^a)$ divides $v(x^a)$. Then, its corresponding vector $v \in C_n$.

Illustration

Let C_{45} be a $(45, 29)$ binary non-primitive BCH code with design distance $d' = 4$. Assume that $a'\left(x^{\frac{2}{3}}\right) = 1 + \left(x^{\frac{2}{3}}\right) + \left(x^{\frac{2}{3}}\right)^3 + \left(x^{\frac{2}{3}}\right)^7 + \left(x^{\frac{2}{3}}\right)^{11} + \left(x^{\frac{2}{3}}\right)^{12} + \left(x^{\frac{2}{3}}\right)^{13} + \left(x^{\frac{2}{3}}\right)^{16} + \left(x^{\frac{2}{3}}\right)^{44}$ is the received polynomial. The error position $m = 2$ and the syndromes are $S_1 = a'(\alpha) = \alpha^2$, $S_2 = (S_1)^2 = \alpha^4$, $S_3 = a'(\alpha^3) = \alpha^{30}$ and $S_4 = (S_2)^2 = \alpha^8$. The error locator polynomial is given by $f\left(x^{\frac{2}{3}}\right) = f_0 + f_1\left(x^{\frac{2}{3}}\right) + \left(x^{\frac{2}{3}}\right)^2$. Then, we have the following system of equations for f_0 and f_1.

$$\begin{bmatrix} \alpha^2 & \alpha^4 \\ \alpha^4 & \alpha^{30} \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \end{bmatrix} = \begin{bmatrix} \alpha^{30} \\ \alpha^8 \end{bmatrix},$$

$$\begin{bmatrix} f_0 \\ f_1 \end{bmatrix} = \begin{bmatrix} \frac{\alpha^{30}}{\alpha^{14}} & \frac{\alpha^4}{\alpha^{14}} \\ \frac{\alpha^4}{\alpha^{14}} & \frac{\alpha^2}{\alpha^{14}} \end{bmatrix} \begin{bmatrix} \alpha^{30} \\ \alpha^8 \end{bmatrix} = \begin{bmatrix} \alpha^{10} \\ \alpha^2 \end{bmatrix}.$$

Hence, the error locator polynomial is$f\left(x^{\frac{2}{3}}\right) = \alpha^{10} + \alpha^2\left(x^{\frac{2}{3}}\right) + \left(x^{\frac{2}{3}}\right)^2$. Trying successively $x = 1, \alpha, \alpha^2, \ldots,$ we find that α^{11} and α^{44} are the roots. Hence, the error polynomial is $e(x^{\frac{2}{3}}) = \left(x^{\frac{2}{3}}\right)^{11} + (x^{\frac{2}{3}})^{44}$. Thus, we decode $a'\left(x^{\frac{2}{3}}\right)$ as $v'\left(x^{\frac{2}{3}}\right) = a'\left(x^{\frac{2}{3}}\right) + e\left(x^{\frac{2}{3}}\right) = \left(x^{\frac{2}{3}}\right)^{16} + \left(x^{\frac{2}{3}}\right)^{13} + \left(x^{\frac{2}{3}}\right)^{12} + \left(x^{\frac{2}{3}}\right)^7 + \left(x^{\frac{2}{3}}\right)^3 + \left(x^{\frac{2}{3}}\right) + 1$. Now, letting $x^{\frac{2}{3}} = y$, this gives $y^3 = x^2$, we get

$$v'(y^3) = \left(y^3\right)^{16} + \left(y^3\right)^{13} + \left(y^3\right)^{12} + \left(y^3\right)^7 + \left(y^3\right)^3 + \left(y^3\right) + 1$$
$$v'\left(x^2\right) = \left(x^2\right)^{16} + \left(x^2\right)^{13} + \left(x^2\right)^{12} + \left(x^2\right)^7 + \left(x^2\right)^3 + \left(x^2\right) + 1.$$

After dividing $v'\left(x^2\right)$ by $\left(x^2\right)^{15} - 1$, we obtain the remainder $v'(x^2)$ as

$$v'(x^2) = (x^2)^{13} + (x^2)^{12} + (x^2)^7 + (x^2)^3 + (x^2) + 1 \in C_{15},$$

where C_{15} is primitive binary BCH code $(15, 11)$ and it is due to the reason that the generator polynomial $g(x^2) = (x^2)^4 + (x^2) + 1$ divides $v'(x^2)$.

5 Conclusions

These are the following pronouncements of the study.

1) The existence of a non-primitive BCH code in $F_2\left[x; \frac{a}{b}\mathbb{Z}_0\right]_{bn}$ of length bn based on a primitive BCH code of length n has been explained.
2) The construction technique of bn length non-primitive BCH code is given in such a manner that the binary BCH code C_n is embedded in the binary BCH code C_{bn} and thus the the transmitted data configurated through C_n can be received through binary BCH code C_{bn}.
3) The binary BCH code C_{bn} has higher code rate and error correction capability than binary BCH code C_n along with a burst error correction capability.

This work can further be extended over the Galois field F_{2^m} and has applications in cognitive radio. Further, these results can be generalized to data mining.

Competing interests

Non-financial academic competing interest. This manuscript would be part of the author's P.h.D thesis.

Acknowledgements

The authors would like to thank the anonymous referees for their valuable comments and suggestions which improved the presentation of the paper.

Received: 11 August 2015 Accepted: 13 January 2016
Published online: 04 February 2016

References

1. E Prange, *Cyclic error-correcting codes in two symbols*. (Air force Cambridge research center, Cambridge, 1957). AFCRC-TN-57-103
2. E Prange, *The use of coset equivalence in the analysis and decoding of group codes*. (Air force Cambridge research center, Cambridge, 1959). AFCRC-TR-59-164
3. WW Peterson, Encoding and error-correction procedures for the Bose-Chaudhuri codes. IRE Trans. IT-6, 459–470 (1960)
4. T Kasami, Systematic codes using binary shift register sequences. J. Info. Processing Soc. Japan. **1**, 198–200 (1960)
5. J Cazaran, AV Kelarev, Generators and weights of polynomial codes. Archiv. Math. **69**(6), 479–486 (1997)
6. J Cazaran, AV Kelarev, On finite principal ideal rings. Acta Math. Univ. Comenianae. **68**(1), 77–84 (1999)
7. J Cazaran, AV Kelarev, SJ Quinn, D Vertigan D, An algorithm for computing the minimum distances of extensions of BCH codes embedded in semigroup rings. Semigroup Forum. **73**(3), 317–329 (2006)
8. AV Kelarev, *Ring Constructions and Applications*. (World Scientific, River Edge, New York, 2002)

9. AV Kelarev, An algorithm for BCH codes extended with finite state automata. Fundamenta Informaticae. **84**(1), 51–60 (2008)
10. AV Kelarev, Algorithms for computing parameters of graph-based extensions of BCH codes. J. Discret. Algorithm. **5**(6), 553–563 (2007)
11. AA Andrade, T Shah, A Khan, A note on linear codes over semigroup rings. TEMA Tend. Mat. Apl. Comput. **12**(2), 79–89 (2011)
12. T Shah, AA Andrade, Cyclic codes through $B\left[X; \frac{a}{b}\mathbb{Z}_{\geq 0}\right]$ $\left(\frac{a}{b} \in Q^{+}, b = a + 1\right)$ and Encoding. Discret. Math. Algoritm. Appl. **4**(4) (2012). doi:10.1142/S1793830912500590
13. T Shah, AA Andrade, Cyclic codes through $B[X]$, $B\left[X; \frac{1}{kp}, \mathbb{Z}_{\geq 0}\right]$ and $B\left[X; \frac{1}{p^k}\mathbb{Z}_{\geq 0}\right]$: a comparison. J. Algebra Appl. **11**(4) (2012). doi:10.1142/S0219498812500788
14. T Shah, Amanullah, AA Andrade, A method for improving the code rate and error correction capability of a cyclic code. Comput. Appl. Math. **32**(2), 261–274 (2013)
15. T Shah, Amanullah, AA Andrade, A decoding procedure which improves code rate and error corrections. JARAM. **4**(4), 37–50 (2012)
16. T Shah, A Khan, AA Andrade, Encoding through generalized polynomial codes. Comp. Appl. Math. **30**(2), 349–366 (2011)
17. T Shah, A Khan, AA Andrade, Constructions of codes through semigroup ring $B\left[X; \frac{1}{2^2}, \mathbb{Z}_{\geq 0}\right]$ and encoding. Comput. Math. Appl. **62**, 1645–1654 (2011)
18. T Shah, M Khan, AA Andrade, A decoding method of an *n* length binary BCH code through $(n+1)n$ length binary cyclic code. Anais da Academia Brasileira de Ciê,ncias. **85**(3), 863–872 (2013)
19. SR Nagpaul, Sk Jain, *Topics in Applied Abstract Algebra* (Thomson, Brooks/Cole, USA, 2005)
20. S Gao, D Panario, *Tests and constructions of irreducible polynomials over finite fields, foundations of computational mathematics*. (Foundations of Computational Mathematics, Cucker F, Shub M, eds.) (Springer, 1997), pp. 346–361
21. WW Peterson, EJ Weddon Jr., *Error correcting codes*, 2nd editition. (MIT Press, Cambridge, 1972)