International Journal of Algebra, Vol. 8, 2014, no. 11, 547 - 556
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ija.2014.4657

A BCH Code and a Sequence of Cyclic Codes

Tariq Shah and Mubashar Khan

Department of Mathematics, Quaid-i-Azam University
Islamabad, Pakistan

Antonio Aparecido de Andrade

Department of Mathematics, São Paulo State University at São José do Rio
Preto, São Paulo, Brazil

Abstract

This study establishes that for a given binary BCH code C_n^0 of length n generated by a polynomial $g(x) \in \mathbb{F}_2[x]$ of degree r there exists a family of binary cyclic codes $\{C^m_{2^{m-1}(n+1)n}\}_{m\geq 1}$ such that for each $m \geq 1$, the binary cyclic code $C^m_{2^{m-1}(n+1)n}$ has length $2^{m-1}(n+1)n$ and is generated by a generalized polynomial $g(x^{\frac{1}{2^m}}) \in \mathbb{F}_2[x, \frac{1}{2^m}\mathbb{Z}_{\geq 0}]$ of degree $2^m r$. Furthermore, C_n^0 is embedded in $C^m_{2^{m-1}(n+1)n}$ and $C^m_{2^{m-1}(n+1)n}$ is embedded in $C^{m+1}_{2^m(n+1)n}$ for each $m \geq 1$. By a newly proposed algorithm, codewords of the binary BCH code C_n^0 can be transmitted with high code rate and decoded by the decoder of any member of the family $\{C^m_{2^{m-1}(n+1)n}\}_{m\geq 1}$ of binary cyclic codes, having the same code rate.

Mathematics Subject Classification: 11T71, 14A50, 94A15

Keywords: Cyclic code, BCH code, decoding procedure

1 Introduction

In [4] Cazaran and Kelarev introduce the necessary and sufficient conditions for the ideal to be a principal ideal and describe all finite principal ideal rings

$\mathbb{Z}_m[x_1, x_2, \cdots, x_n]/I$, where I is generated by univariate polynomials. Moreover, in [5], 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 $\mathbb{F}$ is a field and S is a finite semigroup, introduced by Cazaran et al. [6], in which an algorithm is considered for computing the weights of extensions for codes embedded in $\mathbb{F}[S]$ as ideals. Valuable information related to several ring constructions and concerning polynomial codes was given by Kelarev [8] and [9]. Whereas, in [10] and [11], Kelarev discuss 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 [1] elaborated the cyclic, BCH, alternant, 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 et al. [12] and [13], 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 [1] 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 $\frac{1}{2^2}\mathbb{Z}_{\geq 0}$ are taken, respectively. This converts the whole construction of a finite quotient ring of a polynomial ring into a finite quotient ring of monoid rings of particular nature. In [12] and [13], R is considered as a finite unitary commutative ring for the quotient rings $R[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]/((x^{\frac{1}{2}})^{2n} - 1)$ and $R[x; \frac{1}{2^2}\mathbb{Z}_{\geq 0}]/((x^{\frac{1}{2^2}})^{2^2 n} - 1)$, respectively. However, in [2] Andrade et al. describe the decoding principle based on modified Berlekamp-Massey algorithm for BCH, alternant and Goppa codes constructed through monoid rings $R[x; \frac{1}{2}\mathbb{Z}_{\geq 0}]$.

The existence of an $((n+1)^{3^k} - 1, (n+1)^{3^k} - 1 - 3^k r)$ binary cyclic code, where k is a positive integer, corresponding to a $(n, n-r)$ binary cyclic code established in [14] through the monoid ring $\mathbb{F}_2[x; \frac{1}{3^k}\mathbb{Z}_{\geq 0}]$. Furthermore, in [14] a decoding procedure for an $(n, n-r)$ binary cyclic code by an $((n+1)^{3^k} - 1, (n+1)^{3^k} - 1 - 3^k r)$ binary cyclic code is also given, which provides an improvement in the code rate and error corrections capabilities.

Provoked by [14] we initiate the inquiry in support to binary BCH codes alike binary cyclic codes however we observed that; for a binary BCH code of length $n = 2^s - 1$ generated by r degree polynomial $g(x) \in \mathbb{F}_2[x]$ it is not possible to construct a binary BCH code of length $2^{m-1}(n+1)n$ generated by $2^m r$ degree generalized polynomial $g(x^{\frac{1}{2^m}}) \in \mathbb{F}_2[x, \frac{1}{2^m}\mathbb{Z}_{\geq 0}]$. Though, in this study, we instituted that corresponding to an $(n, n-r)$ binary BCH code C_n^0 there is a family $\{(2^{m-1}(n+1)n, 2^{m-1}(n+1)n - 2^m r)\}_{m \geq 1}$ of binary cyclic codes (represented as $\{C^m_{2^{m-1}(n+1)n}\}_{m \geq 1}$) such that C_n^0 is embedded in each $C^m_{2^{m-1}(n+1)n}$. Furthermore, we propose an algorithm which enables in decoding of a received vector of binary BCH code C_n^0 of length n through the decoding of corresponding generalized received vector of any member of the family $\{C^m_{2^{m-1}(n+1)n}\}_{m\geq 1}$ of binary cyclic codes.

2 Cyclic code of length $2^{m-1}(n+1)n$ constructed through $\mathbb{F}_2[x; \frac{1}{2^m}\mathbb{Z}_{\geq 0}]$

Let $D[x;S]$ be a monoid ring. A nonzero element f of $D[x;S]$ 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 D is an integral domain, particularly the binary field $\mathbb{F}_2$, the monoid ring $D[x;S]$ is simply the polynomial ring $D[x]$. Clearly $D[x] = D[x;\mathbb{Z}_{\geq 0}] \subset D[x;\frac{1}{2}\mathbb{Z}_{\geq 0}]$. Since $\frac{1}{2}\mathbb{Z}_{\geq 0}$ is an ordered monoid, it follows that we can define the degree of an element in $D[x;\frac{1}{2}\mathbb{Z}_{\geq 0}]$.

The indeterminate of generalized polynomials in monoid ring $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]$ is $x^{\frac{1}{2^m}}$ and it behave like an indeterminate x in $\mathbb{F}_2[x]$. For instance for a torsion free cancellative monoid S 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 $S \cong \mathbb{Z}_{\geq 0}$ [7, Theorem 8.4]. Corresponding to principal ideal $(f(x^{\frac{1}{2^m}}))$ in $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]$ generated by $f(x^{\frac{1}{2^m}})$ there is a factor ring $\frac{\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]}{(f(x^{\frac{1}{2^m}}))}$ and it is a field if and only if $f(x^{\frac{1}{2^m}})$ is irreducible over $\mathbb{F}_2$. Clearly, it follows the following proposition.

Proposition 2.1 *Let $g(x) \in F_2[x,\mathbb{Z}_{\geq 0}]$ be an r degree polynomial. If $n = 2^s - 1$, where s is a positive integer and $g(x)$ divides $x^n - 1$, then the generalized polynomial $g(x^{\frac{1}{2^m}}) \in \mathbb{F}_2[x,\frac{1}{2^m}\mathbb{Z}_{\geq 0}]$ of degree $2^m r$, where $m \in \mathbb{Z}^+$, divides $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1$ in $\mathbb{F}_2[x,\frac{1}{2^m}\mathbb{Z}_{\geq 0}]$.*

If $f(x^{\frac{1}{2^m}}) = (x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1$, then an element of $\frac{\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]}{((x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n}-1)}$ is $a_0 + a_{\frac{1}{2^m}}\zeta + a_{\frac{2}{2^m}}\zeta^2 + \cdots + a_{\frac{(2^{m-1}(n+1)n-1)}{2^m}}\zeta^{2^{m-1}(n+1)n-1}$, where $a_0, a_{\frac{1}{2^m}}, \cdots, a_{\frac{(2^{m-1}(n+1)n-1)}{2^m}}$ are in $\mathbb{F}_2$ and ζ is the coset $x^{\frac{1}{2^m}} + (f(x^{\frac{1}{2^m}}))$. So $f(\zeta) = 0$, where ζ satisfies the relation $\zeta^{2^{m-1}(n+1)n} - 1 = 0$. If $x^{\frac{1}{2^m}} = \zeta$, then the ring $\frac{\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]}{((x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n}-1)}$ becomes $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$ in which the relation $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1 = 0$ holds, that is $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} = 1$. The multiplication $*$ in the ring $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$ is modulo $((x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1)$. So, given $c(x^{\frac{1}{2^m}}), d(x^{\frac{1}{2^m}}) \in \mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$, we write $c(x^{\frac{1}{2^m}}) * d(x^{\frac{1}{2^m}})$ to denote their product in the ring $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$ and $c(x^{\frac{1}{2^m}})d(x^{\frac{1}{2^m}})$ to denote their product in the ring $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]$. If $\deg(a(x^{\frac{1}{2^m}})) + \deg(b(x^{\frac{1}{2^m}})) < 2^{m-1}(n+1)n$, then $c(x^{\frac{1}{2^m}}) * d(x^{\frac{1}{2^m}}) = c(x^{\frac{1}{2^m}})d(x^{\frac{1}{2^m}})$. Otherwise, $c(x^{\frac{1}{2^m}}) * d(x^{\frac{1}{2^m}})$ is the remainder left on dividing $c(x^{\frac{1}{2^m}})d(x^{\frac{1}{2^m}})$ by

$(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n}-1$. In other words, if $c(x^{\frac{1}{2^m}})*d(x^{\frac{1}{2^m}})=r(x^{\frac{1}{2^m}})$, then $c(x^{\frac{1}{2^m}})d(x^{\frac{1}{2^m}})=r(x^{\frac{1}{2^m}})+((x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n}-1)q(x^{\frac{1}{2^m}})$ for some generalized polynomial $q(x^{\frac{1}{2^m}})$. To get $c(x^{\frac{1}{2^m}})*d(x^{\frac{1}{2^m}})$, we compute the ordinary product $c(x^{\frac{1}{2^m}})d(x^{\frac{1}{2^m}})$ and put $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n}=1$, $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n+1}=x^{\frac{1}{2^m}}$, $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n+2}=(x^{\frac{1}{2^m}})^2$ and so on. Now, consider $x^{\frac{1}{2^m}}*c(x^{\frac{1}{2^m}})$, and it would be $c_{\frac{(2^{m-1}(n+1)n-1)}{2^m}}+c_0x^{\frac{1}{2^m}}+c_{\frac{1}{2^m}}(x^{\frac{1}{2^m}})^2+\cdots+c_{\frac{(2^{m-1}(n+1)n-2)}{2^m}}(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n-1}$. In particular, take the product $x^{\frac{1}{2^m}}*c(x^{\frac{1}{2^m}})$ in $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$. The $\mathbb{F}_2$-space $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$ is isomorphic to $\mathbb{F}_2$-space $\mathbb{F}_2^{2^{m-1}(n+1)n}$; indeed, corresponding to the generalized polynomials $c(x^{\frac{1}{2^m}})=c_0+c_{\frac{1}{2^m}}x^{\frac{1}{2^m}}+\cdots+c_{\frac{(2^{m-1}(n+1)n-1)}{2^m}}(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n-1}$ in $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$ having $2^{m-1}(n+1)n$ terms, there is an $2^{m-1}(n+1)n$-tuple $(c_0,c_{\frac{1}{2^m}},\cdots,c_{\frac{(2^{m-1}(n+1)n-1)}{2^m}})$ in $\mathbb{F}_2^{2^{m-1}(n+1)n}$. Thus, the isomorphism between the vector spaces $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$ and $\mathbb{F}_2^{2^{m-1}(n+1)n}$ is defined by $c\longmapsto c(x^{\frac{1}{2^m}})$.

The multiplication by $x^{\frac{1}{2^m}}$ in the ring $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$ corresponds to cyclic shift σ in $\mathbb{F}_2^{2^{m-1}(n+1)n}$, that is, $x^{\frac{1}{2^m}}*c(x^{\frac{1}{2^m}})=\sigma(c)(x^{\frac{1}{2^m}})$. A subspace C of $\mathbb{F}_2$-space $\mathbb{F}_2^{2^{m-1}(n+1)n}$ is a linear code. As already agreed, we recognize every vector $\mathbf{c}$ in $\mathbb{F}^{2^{m-1}(n+1)n}$ with the polynomial $c(x^{\frac{1}{2^m}})$ in $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$, so $C^m_{2^{m-1}(n+1)n}\subset\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$. The elements of the code $C^m_{2^{m-1}(n+1)n}$ are now referred as codewords or code (generalized) polynomials. By use of the techniques of [14], the following results can easily be established for $2^{m-1}(n+1)n$ instead of $(n+1)^{3^k}-1$.

Theorem 2.2 *[14] If $C^m_{2^{m-1}(n+1)n}, m\geq 1$ is a linear code over $\mathbb{F}_2$, then $C^m_{2^{m-1}(n+1)n}$ is cyclic if and only if $x^{\frac{1}{2^m}}*c(x^{\frac{1}{2^m}})\in C^m_{2^{m-1}(n+1)n}$ for every $c(x^{\frac{1}{2^m}})\in C^m_{2^{m-1}(n+1)n}$.*

Theorem 2.3 *[14] A subset $C^m_{2^{m-1}(n+1)n}$ of $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$ is a cyclic code if and only if $C^m_{2^{m-1}(n+1)n}$ is an ideal of the ring $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$.*

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

Theorem 2.4 *[14] For any $m\geq 1$, if $C^m_{2^{m-1}(n+1)n}$ is a nonzero ideal in $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$, then*

1. *there exists a unique monic polynomial $g(x^{\frac{1}{2^m}})$ of least degree in $C^m_{2^{m-1}(n+1)n}$,*

2. *$g(x^{\frac{1}{2^m}})$ divides $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n}-1$ in $\mathbb{F}_2[x;\frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$,*

3. *$g(x^{\frac{1}{2^m}})$ divides $a(x^{\frac{1}{2^m}})$ for all $a(x^{\frac{1}{2^m}}) \in C^m_{2^{m-1}(n+1)n}$,*

4. *$C^m_{2^{m-1}(n+1)n} = (g(x^{\frac{1}{2^m}}))$.*

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

By Theorem 2.4, if follows that only ideals in the ring $\mathbb{F}_2[x; \frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$ are linear codes which are generated by the factors of $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1$. Thus we can obtain all cyclic codes of length $2^{m-1}(n+1)n$ over $\mathbb{F}_2$ if we find all factors of $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1$ in $\mathbb{F}_2[x; \frac{1}{2^m}\mathbb{Z}_{\geq 0}]$. In the case of trivial factors, we get trivial codes. If $g(x^{\frac{1}{2^m}}) = (x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1$, then $g(x^{\frac{1}{2^m}}) = 0$. Whereas $g(x^{\frac{1}{2^m}}) = 1$ implies $(g(x^{\frac{1}{2^m}})) = \mathbb{F}_2[x; \frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$.

Definition 2.5 *Let $C^m_{2^{m-1}(n+1)n}$ be a nonzero ideal in $\mathbb{F}_2[x; \frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$, where $m \geq 1$. If $g(x^{\frac{1}{2^m}})$ is the unique monic generalized polynomial of least degree in $C^m_{2^{m-1}(n+1)n}$, then $g(x^{\frac{1}{2^m}})$ is called the generator generalized polynomial of the cyclic code $C^m_{2^{m-1}(n+1)n}$.*

If $C^m_{2^{m-1}(n+1)n} = (p(x^{\frac{1}{2^m}}))$ is the ideal generated by $p(x^{\frac{1}{2^m}})$, then $p(x^{\frac{1}{2^m}})$ is the generator generalized polynomial of $C^m_{2^{m-1}(n+1)n}$ if and only if $p(x^{\frac{1}{2^m}})$ is monic and divides $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1$ in $\mathbb{F}_2[x; \frac{1}{2^m}\mathbb{Z}_{\geq 0}]$.

3 Relationship of a BCH code and a cyclic code

Let C^0_n be an $(n, n-r)$ binary BCH code based on the positive integers c, δ_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^0_n has generator polynomial $g(x) = lcm\{m_i(x) : i = c, c+1, \cdots, c+\delta_1 - 2\}$ of degree r, where $m_i(x)$ are minimal polynomials of ζ^i, for $i = c, c+1, \cdots, c+\delta_1 - 2$. Whereas ζ is the primitive n^{th} root of unity in $\mathbb{F}_{2^l}$. Since $m_i(x)$ divides $x^n - 1$ for each i, it follows that $g(x)$ divides $x^n - 1$. This implies $C^0_n = (g(x))$ is a principal ideal in the factor ring $\mathbb{F}_2[x]_n$. As it is established in Proposition 2.1 that the generalized polynomial $g(x^{\frac{1}{2^m}}) \in \mathbb{F}_2[x, \frac{1}{2^m}\mathbb{Z}_{\geq 0}]$ of degree $2^m r$ divides $(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1$ in $\mathbb{F}_2[x, \frac{1}{2^m}\mathbb{Z}_{\geq 0}]$, so there is a family $\{C^m_{2^{m-1}(n+1)n}\}_{m \geq 1}$ of cyclic codes generated by $\{g(x^{\frac{1}{2^m}})\}_{m \geq 1}$, in $\{\mathbb{F}_2[x; \frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}\}_{m \geq 1}$. Since $(x^{\frac{1}{2^m}})^{2^m n} - 1$ divides

$(x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1$ in $\mathbb{F}_2[x, \frac{1}{2^m}\mathbb{Z}_{\geq 0}]$, it follows that $((x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1) \subset ((x^{\frac{1}{2^m}})^{2^m n} - 1)$. By third isomorphism theorem for rings

$$\frac{\mathbb{F}_2[x, \frac{1}{2^m}\mathbb{Z}_{\geq 0}]/((x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1)}{((x^{\frac{1}{2^m}})^{2^m n} - 1)/((x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n} - 1)} \simeq \frac{\mathbb{F}_2[x, \frac{1}{2^m}\mathbb{Z}_{\geq 0}]}{((x^{\frac{1}{2^m}})^{2^m n} - 1)} \text{ and}$$

$$\frac{\mathbb{F}_2[x]}{(x^n - 1)} \hookrightarrow \frac{\mathbb{F}_2[x, \frac{1}{2^m}\mathbb{Z}_{\geq 0}]}{((x^{\frac{1}{2^m}})^{2^m n} - 1)}.$$

Thus C_n^0 is embedded in $C^m_{2^{m-1}(n+1)n}$ under the monomorphism defined as $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mapsto a_0 + a_1(x^{\frac{1}{2^m}}) + \cdots + a_{(n-1)}(x^{\frac{1}{2^m}})^{2^m(n-1)} (= a(x^{\frac{1}{2^m}}))$. Also, if $g(x^{\frac{1}{2^m}})$ is the generator polynomial of the code $C^m_{2^{m-1}(n+1)n}$ in $\mathbb{F}_2[x; \frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$, then $g(x^{\frac{1}{2^{m+1}}})$ is the generator polynomial for the cyclic code $C^{m+1}_{2^m(n+1)n}$ in the monoid ring $\mathbb{F}_2[x; \frac{1}{2^{m+1}}\mathbb{Z}_{\geq 0}]_{2^m(n+1)n}$. Thus $C^m_{2^{m-1}(n+1)n}$ is embedded in $C^{m+1}_{2^m(n+1)n}$ which is defined as $a(x^{\frac{1}{2^m}}) \mapsto a(x^{\frac{1}{2^{m+1}}})$. The above discussion shapes the following theorem.

Theorem 3.1 *For a positive integer s, if C_n^0 is a binary BCH code of length $n = 2^s - 1$ generated by the polynomial $g(x) = \sum_{i=0}^r g_i x^i \in \mathbb{F}_2[x]$ of degree r, then*

1. *there exists a family $\{C^m_{2^{m-1}(n+1)n}\}_{m\geq 1}$ of binary cyclic codes such that for each $m \geq 1$ $C^m_{2^{m-1}(n+1)n}$ has length $2^{m-1}(n+1)n$, generated by the generalized polynomial $g(x^{\frac{1}{2^m}}) = g_0 + g_1(x^{\frac{1}{2^m}})^{2^m} + \cdots + g_{2^m}(x^{\frac{1}{2^m}})^{2^m r} \in \mathbb{F}_2[x, \frac{1}{2^m}\mathbb{Z}_{\geq 0}]$ of degree $2^m r$,*

2. *the binary BCH code C_n^0 is embedded in each binary cyclic code $C^m_{2^{m-1}(n+1)n}$ for $m \geq 1$,*

3. *there are embeddings $C^1_{(n+1)n} \hookrightarrow C^2_{2^1(n+1)n} \hookrightarrow \cdots \hookrightarrow C^m_{2^{m-1}(n+1)n} \hookrightarrow \cdots$ for the members of the family $\{C^m_{2^{m-1}(n+1)n}\}_{m\geq 1}$ of binary cyclic codes.*

Is it possible for a binary BCH code $C_n^0 = (g(x))$ that there is a binary BCH code $C^m_{2^{m-1}(n+1)n}$ generated by polynomial $g(x^{\frac{1}{2^m}})$? The answer is no, 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^0, then $g(x^{\frac{1}{2^m}}) = g_0 + g_1(x^{\frac{1}{2^m}})^{2^m} + \cdots + g_r(x^{\frac{1}{2^m}})^{2^m r} = (g_0 + g_1(x^{\frac{1}{2^m}})^1 + \cdots + g_r(x^{\frac{1}{2^m}})^r)^{2^m}$ is not the least common multiple of irreducible polynomials in $\mathbb{F}_2[x, \frac{1}{2^m}\mathbb{Z}_{\geq 0}]$. Hence, $g(x^{\frac{1}{2^m}})$ is not qualified for a generator of a binary BCH code.

4 General decoding principle

McEliece, Berlekamp and Van Tilborg [3] proved that the maximum likelihood decoding is an NP-hard problem for general linear codes. Though by the principle of maximum likelihood decoding we obtain a codeword after decoding which is closest to the received vector while the errors are corrected. We use the decoding procedure which follows the same principle.

Now, we interpret the decoding terminology for a $2^{m_0-1}(n+1)n$ length binary cyclic code $C^{m_0}_{2^{m_0-1}(n+1)n}$ from the family $\{C^{m}_{2^{m-1}(n+1)n}\}_{m\geq 1}$ of binary cyclic codes. Let parity check matrix of a binary cyclic code $C^{m_0}_{2^{m_0-1}(n+1)n}$ be H. If a vector $\mathbf{b}$ is received, then we obtain the syndrome vector for $\mathbf{b}$ as $S(\mathbf{b}) = \mathbf{b}H^T$. In this way, we calculate syndrome table which is useful in finding the error vector e such that $S(\mathbf{b}) = S(\mathbf{e})$. So the decoding of the received vector $\mathbf{b}$ has done as the transmitted vector $\mathbf{a} = \mathbf{b} - \mathbf{e}$.

The general principle of decoding is; choose the codeword which is closest to the received vector. For this determination, we make a look-up table that gives the nearest codeword for every possible received vector. The algebraic structure of a linear code as a subspace offers a suitable method for making such a table. As $C^{m_0}_{2^{m_0-1}(n+1)n}$ is a subspace of $\mathbb{F}_2$-space $\mathbb{F}_2^{2^{m_0-1}(n+1)n}$. So $C^{m_0}_{2^{m_0-1}(n+1)n}$ is a subgroup of the additive group $\mathbb{F}_2^{2^{m_0-1}(n+1)n}$. Recall that for every $\mathbf{a} \in \mathbb{F}_2^{2^{m_0-1}(n+1)n}$, $\mathbf{a} + C^{m_0}_{2^{m_0-1}(n+1)n} = \{\mathbf{a} + \mathbf{c} : \mathbf{c} \in C^{m_0}_{2^{m_0-1}(n+1)n}\}$ is called a coset of $C^{m_0}_{2^{m_0-1}(n+1)n}$. These cosets form a partition of the space $\mathbb{F}_2^{2^{m_0-1}(n+1)n}$. Hence $\mathbb{F}_2^{2^{m_0-1}(n+1)n}$ is the disjoint union of distinct cosets.

Let $\mathbf{y}$ be any vector in $\mathbb{F}_2^{2^{m_0-1}(n+1)n}$, and suppose $\mathbf{x} \in C^{m_0}_{2^{m_0-1}(n+1)n}$ is the codeword nearest to $\mathbf{y}$. Now $\mathbf{x}$ lies in the coset $\mathbf{y} + C^{m_0}_{2^{m_0-1}(n+1)n} = \{\mathbf{y} - \mathbf{c} : \mathbf{c} \in C^{m_0}_{2^{m_0-1}(n+1)n}\}$. For all $\mathbf{c} \in C^{m_0}_{2^{m_0-1}(n+1)n}$ it follows that $d(\mathbf{y}, \mathbf{x}) \leq d(\mathbf{y}, \mathbf{c})$, i.e., $w(\mathbf{y} - \mathbf{x}) \leq w(\mathbf{y} - \mathbf{c})$. Hence, $\mathbf{y} - \mathbf{x}$ is the vector of least weight in the coset containing y. Writing $\mathbf{e} = \mathbf{y} - \mathbf{x}$, we have $\mathbf{x} = \mathbf{y} - \mathbf{e}$. Thus the following theorem is obtained.

Theorem 4.1 *Let $C^{m_0}_{2^{m_0-1}(n+1)n} \subset \mathbb{F}_2^{2^{m_0-1}(n+1)n}$ be a cyclic code. Given a vector $\mathbf{y} \in \mathbb{F}_2^{2^{m_0-1}(n+1)n}$, the codeword $\mathbf{x}$ nearest to $\mathbf{y}$ is given by $\mathbf{x} = \mathbf{y} - \mathbf{e}$, where $\mathbf{e}$ is the vector of least weight in the coset containing $\mathbf{y}$. If the coset containing $\mathbf{y}$ has more than one vector of least weight, then there are more than one codewords nearest to $\mathbf{y}$.*

Definition 4.2 *Let $C^{m_0}_{2^{m_0-1}(n+1)n}$ be a linear code in $\mathbb{F}_2^{2^{m_0-1}(n+1)n}$. The coset leader of a given coset of $C^{m_0}_{2^{m_0-1}(n+1)n}$ is defined to be the vector with the least weight in the coset.*

Theorem 4.3 *Let $C^{m_0}_{2^{m_0-1}(n+1)n}$ be an $(2^{m_0-1}(n+1)n, 2^{m_0-1}(n+1)n-2^{m_0}r)$ code over $\mathbb{F}_2$, and let H be a parity-check matrix of $C^{m_0}_{2^{m_0-1}(n+1)n}$. Then, $C^{m_0}_{2^{m_0-1}(n+1)n} = \{\mathbf{x} \in \mathbb{F}_2^{2^{m_0-1}(n+1)n} : \mathbf{x}H^T = 0 = Hx^T\}$.*

By Theorem 4.3, it follows that $S(\mathbf{y}) = 0$ if and only if $\mathbf{y} \in C^{m_0}_{2^{m_0-1}(n+1)n}$. For $\mathbf{y}, \mathbf{y}^{/} \in \mathbb{F}^{2^{m_0-1}(n+1)n}$, $S(\mathbf{y}) = S(\mathbf{y}')$ holds if and only if $(\mathbf{y}-\mathbf{y}')H^T = 0$, that is, $\mathbf{y}-\mathbf{y}' \in C^{m_0}_{2^{m_0-1}(n+1)n}$. Hence two vectors have the same syndrome if and only if they lie in the same coset of $C^{m_0}_{2^{m_0-1}(n+1)n}$. Thus there is a one-to-one correspondence between the cosets of $C^{m_0}_{2^{m_0-1}(n+1)n}$ and the syndromes. A table with two columns showing the coset leader $\mathbf{e}_i$ and the corresponding syndromes $S(\mathbf{e}_i)$ is called the syndrome table. To decode a received vector $\mathbf{y}$, we compute its syndrome $S(\mathbf{y})$ and then look at the table to find the coset leader $\mathbf{e}$ for which $S(\mathbf{e}) = S(\mathbf{y})$. Then $\mathbf{y}$ is decoded as $\mathbf{x} = \mathbf{y} - \mathbf{e}$. The syndromes are given by $S(\mathbf{e}_i)$, where $\mathbf{e}_i$ for $i = 1, 2, \cdots, 2^{2^{m_0}r}$ are the coset leaders, $\mathbb{F} = \mathbb{F}_2$ and $S(\mathbf{e}_i) = \mathbf{e}_i H^T$, for $i = 1, 2, \cdots, 2^{2^{m_0}r}$.

Consider a binary BCH code C^0_n based on the positive integers c, δ, $q = 2$ and n such that $2 \leq \delta \leq n$ with $n = 2^s - 1$, where s is a positive integer. Let ζ be a primitive n^{th} root of unity in $\mathbb{F}_{2^l}$. Let $m_i(x) \in \mathbb{F}_2[x]$ denote the minimal polynomial of ζ^i. Let $g(x)$ be the product of distinct polynomials among $m_i(x)$, for $i = c, c+1, \cdots, c+\delta-2$, that is, $g(x) = lcm\{m_i(x) : i = c, c+1, \cdots, c+\delta-2\}$.

Assume that for a fixed $m = m_0$, $C^m_{2^{m-1}(n+1)n}$ is a binary cyclic code of length $2^{m-1}(n+1)n = n')$ with minimum distance d and with generator generalized polynomial $g(x^{\frac{1}{2^m}})$ from the corresponding family $\{C^m_{2^{m-1}(n+1)n}\}_{m\geq 1}$ of binary cyclic codes, which has the check generalized polynomial $h(x^{\frac{1}{2^m}}) = h_{\frac{(n'-2^m r)}{2^m}}(x^{\frac{1}{2^m}})^{n'-2^m r} + h_{\frac{(n'-2^m r-1)}{2^m}} x^{\frac{1}{2^m} n'-2^m r-1} + \cdots + h_{\frac{1}{2^m}} x^{\frac{1}{2^m}} + h_0$, which satisfies $x^{\frac{1}{2^m} n'} - 1 = g(x^{\frac{1}{2^m}}) * h(x^{\frac{1}{2^m}})$. Thus, the matrix H is given by

$$\begin{bmatrix} h_{\frac{(n'-2^m r)}{2^m}} & h_{\frac{(n'-2^m r-1)}{2^m}} & \cdots & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{\frac{(n'-2^m r)}{2^m}} & \cdots & \cdots & h_{\frac{1}{2^m}} & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & h_{\frac{(n'-2^m r)}{2^m}} & h_{\frac{(n'-2^m r-1)}{2^m}} & \cdots & \cdots & h_{\frac{1}{2^m}} & h_0 \end{bmatrix}$$

is the $(2^{m-1}(n+1)n-k) \times 2^{m-1}(n+1)n$ parity-check matrix for $C^m_{2^{m-1}(n+1)n}$ with $k = 2^{m-1}(n+1)n - 2^m r$. Syndrome of the vector $a \in \mathbb{F}_2^{2^{m-1}(n+1)n}$ is denoted as $S(a) = aH^T$. For the vector $\mathbf{a} = (a_0, a_{\frac{1}{2^m}}, a_{\frac{2}{2^m}}, \cdots, a_{\frac{(n-1)}{2^m}}, \cdots, a_{\frac{(2^{m-1}(n+1)n-1)}{2^m}}) \in \mathbb{F}_2^{2^{m-1}(n+1)n}$, the generalized polynomial is $a(x^{\frac{1}{2^m}}) = a_0 + a_{\frac{1}{2^m}} x^{\frac{1}{2^m}} + \cdots + a_{\frac{(n-1)}{2^m}} x^{\frac{1}{2^m}(n-1)} + \cdots + a_{\frac{(2^{m-1}(n+1)n-1)}{2^m}} x^{\frac{1}{2^m} 2^{m-1}(n+1)n-1}$ in $\mathbb{F}_2[x; \frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$, and thus $S(\mathbf{a}) = \mathbf{a}H^T$. Assume that the codeword $\mathbf{v} \in C$ is transmitted and the received vector is $a = v + e$, where $\mathbf{e} = (e_0, e_{\frac{1}{2^m}}, e_{\frac{2}{2^m}}, \cdots, e_{\frac{(2^{m-1}(n+1)n-1)}{2^m}})$ is the error vector having polynomial form $e(x^{\frac{1}{2^m}}) = e_0 + e_{\frac{1}{2^m}} x^{\frac{1}{2^m}} + \cdots + e_{\frac{(2^{m-1}(n+1)n-1)}{2^m}} (x^{\frac{1}{2^m}})^{2^{m-1}(n+1)n-1}$. Thus, $S(\mathbf{e}) = S(\mathbf{a})$. Now, the syndromes for the binary cyclic code $C^m_{2^{m-1}(n+1)n}$ are given by $S(\mathbf{e}_i)$, where $\mathbf{e}_i$ for $i = 1, 2, \cdots, 2^{2^{m-1}(n+1)n-k}$ are the coset leaders, $k = 2^{m-1}(n+1)n - 2^m r$ and $S(\mathbf{e}_i) = \mathbf{e}_i H^T$ for $i = 1, 2, \cdots, 2^{2^{m-1}(n+1)n-k}$.

Now, we introduce a decoding procedure for a binary BCH code of length n through a binary cyclic code of length $2^{m-1}(n+1)n$ in the corresponding family $\{C^m_{2^{m-1}(n+1)n}\}_{m \geq 1}$ of binary cyclic codes. Though, here we sum up the procedure which indicates the steps in decoding a received word of the cyclic code of length $2^{m-1}(n+1)n$ and clarify the method finding the enveloped codeword of a binary BCH code of length n. The decoding procedure is given by

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

Step 2: Construct the Syndrome table for the binary cyclic code $C^m_{2^{m-1}(n+1)n}$.

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

Step 4: Calculate the syndrome vector for the vector

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

corresponding to the received generalized polynomial $b'(x^{\frac{1}{2^m}}) = b_0 + b_{\frac{1}{2^m}} x^{\frac{1}{2^m}} \cdots + b_{\frac{(n-1)}{2^m}} (x^{\frac{1}{2^m}})^{n-1} + \cdots + b_{\frac{(2^{m-1}(n+1)n-1)}{2^m}} x^{\frac{1}{2^m} 2^{m-1}(n+1)n-1}$ in $\mathbb{F}_2[x; \frac{1}{2^m}\mathbb{Z}_{\geq 0}]_{2^{m-1}(n+1)n}$.

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

Step 6: Decode $\mathbf{b}'$ as $\mathbf{b}' - \mathbf{e} = \mathbf{a}'$.

Step 7: The corresponding corrected codeword polynomial $a(x)$ in binary BCH code C^0_n is obtained.

References

[1] A.A. Andrade and R. Palazzo Jr., Linear codes over finite rings, TEMA-Tend. Mat. Apl. Comput., 6(2) (2005), 207-217. Doi 10.5540/tema.2005.06.02.0207

[2] A.A. Andrade, T. Shah and A. Khan, Goppa codes through generalized polynomials and its decoding principle, International Journal of Applied Mathematics, 23(3) (2010) 517-526.

[3] E.R. Berlekamp, R.J. McEliece and H.C.A. van Tilborg, On the inherent intractability of certain coding problem, IEEE Trans. on Inform. Theory, IT-24(3) (1978), 384-386. Doi 10.1109/TIT.1978.1055873

[4] J. Cazaran and A.V. Kelarev, Generators and weights of polynomial codes, Archiv. Math., 69 (1997), 479-486. Doi 10.1007/s000130050149

[5] J. Cazaran and A.V. Kelarev, On finite principal ideal rings, Acta Math. Univ. Comenianae, 68(1) (1999), 77-84.

[6] J. Cazaran, A.V. Kelarev, S.J. Quinn and D. Vertigan, An algorithm for computing the minimum distances of extensions of BCH-codes embedded in semigroup rings, Semigroup Forum, 73 (2006), 317-329. Doi 10.1007/s00233-006-0647-9

[7] R. Gilmer and T. Parker, Divisibility properties in semigroup rings, Michigan Math. J., 21(1) (1974), 65-86.

[8] A.V. Kelarev, Ring constructions and applications, World Scientific, River Edge, New York, 2002.

[9] A.V. Kelarev, Error-correcting codes as ideals in group rings, Contemporary Mathematics, 273 (2001), 11-18. Doi 10.1090/conm/273/04419

[10] A.V. Kelarev, An algorithm for BCH codes extended with finite state automata, Fundamenta Informaticae, 84(1) (2008), 51-60. Doi 10.1006/ffta.1999.0245

[11] A.V. Kelarev, Algorithms for computing parameters of graph-based extensions of BCH codes, Journal of Discrete Algorithms, 5 (2007), 553-563. Doi 10.1016/j.jda.2006.08.002

[12] T. Shah, A. Khan and A.A. Andrade, Encoding through generalized polynomial codes, Comput. Appl. Maths., (30)(2) (2011), 349-366. http://dx.doi.org/10.1590/S1807-03022011000200006

[13] T. Shah, A. Khan and A.A. Andrade, Constructions of codes through semigroup ring $B[x; \frac{1}{2^2}\mathbb{Z}_0]$ and encoding, Computers & Mathematics with Applications, 62 (2011), 1645-1654. http://dx.doi.org/10.1016/j.camwa.2011.05.056

[14] T. Shah, Amanullah and A.A. Andrade, A decoding procedure which improves code rate and error corrections, Journal of Advanced Research in Applied Mathematics, 4(4) (2012), 37-50. Doi 10.5373/jaram

Received: June 1, 2014