Construction of Good Space-Time Trellis Codes Based on Cyclic Codes over Rings

Raquel Dutra Valença, and Reginaldo Palazzo Jr.
Universidade Estadual de Campinas, Campinas SP, Brazil

Abstract— **In this paper, we propose a systematic procedure for constructing good space-time trellis codes derived from cyclic BCH codes over local finite commutative rings. The procedure is based on finding a primitive element in the group of units of the Galois extension ring. For a given design distance, the polynomial generator of a BCH cyclic block code over $\mathbb{Z}_Q$ is determined. Such a generator polynomial must contain no binary factor. Hence, the coefficients of the generator polynomial is used as the tap connections for the Q-ary convolutional encoder. Some examples of these codes were tabulated.**

I. Introduction

SPACE -time codes were proposed by Tarokh *et al*. [2] as an efficient method for transmitting high data rate wireless communication over Rayleigh or Ricean fading channels. Theoretically, these codes provide the best tradeoff between diversity gain, transmission rate, constellation size, signals space dimension and trellis complexity.

In [2], two design criteria for space-time codes construction were established and it was shown that these codes performance is determined by matrices constructed from distinct codeword pairs. More precisely, the minimum rank of these matrices is related to the diversity gain (rank criterion) and the minimum determinant of these matrices is related to the coding gain (determinat criterion).

Space-time codes design is based on both previously mentioned criteria, which were established by considering the channel with fading. These space-time codes were found by an exhaustive search where pairs of codewords have to satisfy the rank and the determinant criteria. Obviously, this search process is very complex.

In this paper a systematic construction of space-time trellis codes over local rings for quasi-static flat fading channel are proposed. This construction provides good space-time trellis codes whose free distance is lower-bounded by the maximum minimum distance achieved by the BCH cyclic codes over local finite commutative rings, however without having binary factors. The reason we have used BCH codes over rings rather than Reed-Solomon codes over rings is that the former is cyclic whereas the latter is not. Although we may use linear block codes for the construction of space-time trellis codes, the complexity of such a procedure is clearly greater than that of using cyclic codes.

This paper is organized as follows. In Section II, we establish the wireless communication system. In Section III, we present some background material on Galois extension of local rings. In Section IV, the technique of generating convolutional codes for the Q-ary discrete memoryless channels is described. In Section V, the construction of trellis codes based on cyclic block codes over Galois extension of local rings is established. Finally, in Section VI the conclusions are drawn.

Raquel D. Valença, and Reginaldo Palazzo Jr. are with the Departamento de Telemática, Faculdade de Engenharia Elétrica e de Computação, 13081-970, Phone: +55 19 3788 3753 Fax: +55 19 3289 1395. E-mails: {raquel, palazzo}@dt.fee.unicamp.br. This work has been supported by FAPESP, under

II. Wireless Communication System

Let us consider the channel is a quasi-static flat fading channel. The wireless communication system model is such that the base station consists of n_T transmitting antennas and the mobile consists of n_R receiving antennas. The information sequence to be transmitted goes through a channel encoder and then it is split into n_T streams which are simultaneously transmitted. Before being transmitted, these sequences go through a pulse shaper and are modulated.

As previously mentioned, two design criteria for space-time codes construction were established in [2]. Based on these criteria and a search for fixed values of the transmission rate, diversity gain, constellation size and trellis decoding complexity, space-time codes were presented in [2] and [3]. Simulations presented in [2] and [4] show these codes achieve good performance under quasi-static flat fading channels.

III. BCH Codes as Cyclic Codes over Finite Local Rings

In this section we describe the construction of BCH codes as cyclic codes over local finite commutative rings A with identity, which is similar to the construction of BCH codes over finite fields. For more details on this subject see for instance [7], [10], [11], [9], and [13].

Recall that a cyclic code with blocklength s over a finite commutative ring A with identity is an ideal in the polynomial ring $A[x]$ modulo a polynomial $x^s - 1$. The first step is to identify an algebraic structure over A containing all the roots of $x^s - 1$. Knowing the structure of the multiplicative group of the units of such a ring leads to the identification of the cyclic subgroup consisting of all the roots of $x^s - 1$.

Let A be a local finite commutative ring with identity. The maximal ideal of A is denoted by $\mathcal{M}$ and its residue field by $\mathbb{K} = \frac{A}{\mathcal{M}} = GF(p^m)$, for some integer $m \geq 1$. Let $A[x]$ be a polynomial ring in the variable x over the ring A. The natural projection is denoted by $\mu : A[x] \rightarrow \mathbb{K}[x]$, with $\mu(f(x)) = \mu(a_0 + a_1x + \cdots + a_nx^n) = \overline{f}(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$, where $\overline{a_i} = a_i + \mathcal{M}, i = 1, \cdots, n$, and $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. Hence, the natural homomorphism $A \rightarrow A/\mathcal{M} = \mathbb{K}$ is simply the restriction of μ to the constant polynomials.

Definition III.1. Let $f(x)$ be a polynomial in $A[x]$. We say that
- $f(x)$ is a *unit* if there exists a polynomial $a(x) \in A[x]$ such that $a(x)f(x) = 1$.
- $f(x)$ is a *zero divisor* if there exists $a(x) \in A[x], a(x) \neq 0$,

- $f(x)$ is *regular* if it is not a zero divisor in $A[x]$.

Theorem III.1. [12] Let $f(x)$ be a regular polynomial in $A[x]$. If $\mu(f(x))$ is irreducible in $\mathbb{K}[x]$, then $f(x)$ is also irreducible in $A[x]$.

Let $f(x)$ be a monic polynomial of degree h in $A[x]$ such that $\mu(f(x))$ is irreducible in $\mathbb{K}[x]$. It follows from Theorem III.1 that $f(x)$ is also irreducible in $A[x]$. Let $\frac{A[x]}{\langle f(x)\rangle}$ denote the quotient ring of the residue classes of the polynomials in x over A, modulo a polynomial $f(x)$. This ring, denoted by $R = GR(|A|, h)$, is a local finite commutative ring with identity and it is called *Galois extension* of A, whose maximal ideal is given by $\overline{\mathcal{M}_1} = \frac{\mathcal{M}_1}{\langle f(x)\rangle}$, where $\mathcal{M}_1 = \langle \mathcal{M}, f(x)\rangle$ and its residue field is given by

$$\mathbb{K}_1 = \frac{R}{\overline{\mathcal{M}_1}} = \frac{A[x]/\langle f(x)\rangle}{\langle \mathcal{M}, f(x)\rangle/\langle f(x)\rangle} = \frac{A[x]}{\langle \mathcal{M}, f(x)\rangle} = \frac{(A/\mathcal{M})[x]}{\langle \mu(f(x))\rangle},$$

with p^{mh} elements. The residue field $\mathbb{K}_1$ is denoted by $GF(p^{mh})$.

An irreducible polynomial $f(x)$ in $A[x]$ is called *basic irreducible* if $\mu(f(x))$ is irreducible in $\mathbb{K}[x]$. A polynomial $f(x)$ in $A[x]$ is called *local* if $\frac{A[x]}{\langle f(x)\rangle}$ is a local extension of A. A regular polynomial $f(x)$ in $A[x]$ is called *separable* if $\frac{A[x]}{\langle f(x)\rangle}$ is a local separable extension of A. If $f(x)$ is a regular polynomial in $A[x]$, then there exists a monic polynomial $g(x)$ such that $\mu(f(x)) = \mu(g(x))$. Furthermore, it is clear that if $f(x)$ is separable, then $\langle f(x)\rangle = \langle g(x)\rangle$, where $g(x)$ is monic and $\mu(f(x)) = \mu(g(x))$. Hence, the separable polynomials are the basic irreducibles. The following conditions are equivalents:

- $f(x)$ is separable;
- $f(x)$ is basic irreducible;
- $\mu(f(x))$ is irreducible.

The next theorem and its corollary characterize the local extensions.

Theorem III.2. [12] A regular polynomial $f(x)$ in $A[x]$ is local if and only if $\mu(f(x))$ is a power of an irreducible polynomial in $\mathbb{K}[x]$.

Corollary III.1. [12] If $f(x)$ is a regular irreducible polynomial in $A[x]$, then $\frac{A[x]}{\langle f(x)^n\rangle}$ is a local ring for some positive integer n.

Let us introduce some notations which will be used in this paper. R^* denotes the multiplicative group of the units of R, and $\mathbb{K}_1^*$ denote the cyclic multiplicative group of $GF(p^{mh})$ with order $p^{mh} - 1$.

Since R^* is an abelian multiplicative group, it can be expressed as the direct product of cyclic groups, [12]. We are interested in the cyclic group of R^*, which we denote by G_s, and whose elements are the roots of $x^s - 1$ for some s such that $mdc(s, p) = 1$ (this guarantees that $x^s - 1$ does not contain repeated factors). Once this group is identified, the problem of constructing BCH codes is reduced to the selection of certain elements of this group to be the input to the parity-check matrix of the code.

Theorem III.3. [12] There is only one maximal cyclic subgroup of R^* whose order is relatively prime to p. This subgroup has

The next theorem provides a method to obtain a cyclic subgroup as stated in Theorem III.3.

Theorem III.4. [13] Assume that α generates a subgroup of order s in R^*, where $mdc(s, p) = 1$. Then the polynomial $x^s - 1$ may be factored as $x^s - 1 = (x - \alpha)(x - \alpha^2)\cdots(x - \alpha^s)$ if and only if $\overline{\alpha}$ has order s in $\mathbb{K}_1^*$.

From Theorem III.4, we denote by G_s the cyclic subgroup of order $s = p^{mh} - 1$ of R^* which has as elements all the roots of $x^s - 1$. Moreover, every polynomial $h(x)$ which divides $x^s - 1$ may be uniquely factored over $\mathbb{K}_1^*$. Thus, by Theorem III.4, we have that the factorization of $h(x)$ over G_s is also unique.

Corollary III.2. A polynomial $h(x)$ which divides $x^s - 1$ with coefficients in A may be factored over G_s as $h(x) = (x - \alpha^{e_1})(x - \alpha^{e_2})\cdots(x - \alpha^{e_l})$ if and only if $\overline{h}(x)$ may be factored over $\mathbb{K}_1$ as $\overline{h}(x) = (x - \overline{\alpha}^{e_1})(x - \overline{\alpha}^{e_2})\cdots(x - \overline{\alpha}^{e_l})$.

The next theorem is of great value in obtaining the generator of G_s.

Theorem III.5. Let $\overline{\alpha}$ be the generator of the cyclic subgroup of order s in $\mathbb{K}_1^*$. Then α generates a cyclic subgroup of order sd in R^*, where d is an integer greater than or equal to 1 and α^d generates a cyclic subgroup G_s of R^*.

Lemma III.1. Let α be an element of G_s with order s. Then the differences $\alpha^{l_1} - \alpha^{l_2}$ are units in R if $0 \le l_1 \ne l_2 \le s - 1$.

Theorem III.6. The minimum Hamming distance of a BCH code satisfies $d \ge 2t + 1$.

The definition of a BCH code as a cyclic code $\mathcal{C}(n, \eta)$ is the following: $c = (c_1, c_2, \cdots, c_n)$ is a codeword if and only if $\sum_{i=1}^{n} c_i \alpha_i^l = 0$ for $l = 1, 2, \cdots, 2t$, where $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is an arbitrary ordered vector of distinct elements of G_s. A permutation applied to this vector does not affect the error correction property of the code. Thus, taking $s = n$ and $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$, where α is a primitive element of G_n and $\alpha_i = \alpha^{i-1}$, we have that the matrix H defines a BCH code having a generator polynomial. Code $\mathcal{C}(n, \eta)$ for which $n = p^{mh} - 1$ is called *primitive*. In this case, η is unique, but for permutation of coordinates.

Theorem III.5 is useful in the determination of the generator of G_n, and Corollary III.2 is useful in the determination of the minimal polynomials of α^i. Thus, we have that $M_i(x)$, the minimal polynomial of α^i over R^* (where α is primitive in G_n), has as roots all the distinct elements of the sequence

$$\alpha^i, (\alpha^i)^q, (\alpha^i)^{q^2}, \cdots, (\alpha^i)^{q^{h-1}},$$

where $q = p^m$. Therefore, $M_i(x)$ may be constructed similarly as the construction of $m_i(x)$, the minimal polynomial of $\overline{\alpha}^i$ over $GF(p^m)$.

From the knowledge of the cyclic group G_n, the construction of the cyclic BCH codes over the ring A reduces to the problem of choosing the elements of this group to be the roots of the generator polynomial $g(x)$. Hence, if α is a primitive element of G_n and if $\alpha^{e_1}, \alpha^{e_2}, \cdots, \alpha^{e_t}$ are the roots of the polynomial $g(x)$ over A given by

where $M_{e_i}(x)$ is the minimal polynomial of α^{e_i} for $i = 1, 2, \cdots, t$, then the polynomial $v(x)$ such that $v(x) = c(x)g(x) \ mod\,(x^n - 1)$, where $c(x) \in A[x]$, defines a cyclic code with block length n over A.

Definition III.2. Let α be a primitive element of G_n. A *BCH* code defined over A is a cyclic code with blocklength n generated by the least degree polynomial $g(x)$ whose roots are $\alpha^{b+1}, \alpha^{b+2}, \cdots, \alpha^{b+2t}$, for some $b \geq 0$, and $t \geq 1$, that is, $g(x) = mmc\{M_1(x), M_2(x), \cdots, M_{2t}(x)\}$, where $M_i(x)$ is the minimal polynomial of $\alpha^{b+i}, i = 1, 2, \cdots, 2t$, over A. Furthermore, $\overline{g}(x) = mmc\{m_1(x), m_2(x), \cdots, m_{2t}(x)\}$ where $m_i(x)$ is the minimal polynomial of $\overline{\alpha}^i,\ i = 1, \cdots, 2t$, generates a BCH code over $GF(p^m)$.

This BCH construction leads to cyclic codes only whereas the construction of Reed-Solomon codes can not be derived from this construction by the fact these codes are not cyclic.

The next theorem establishes a lower bound on the minimum Hamming distance of the code so obtained. This lower bound also applies to cyclic codes in general. However, for the cyclic BCH codes the generator polynomials are chosen such that the minimum distance be guaranteed by it.

Theorem III.7. Let $g(x)$ be the generator polynomial of a cyclic code with blocklength n with symbols in A, and let $\alpha^{e_1}, \alpha^{e_2}, \cdots, \alpha^{e_{n-k}}$ be the roots of $g(x)$ in G_n, where α is an element of order n. Then the minimum Hamming distance of the code is greater than the maximum number of consecutive integers modulo n in the set $E = \{e_1, e_2, \cdots, e_{n-k}\}$.

IV. Q-ary Convolutional Codes

Finding good convolutional codes is a difficult problem to solve due to the fact that its complexity grows exponentially with the input blocklength and memory size. In general, exhaustive search is used in the process despite the efforts devised by many researchers, see for instance [8] and the references therein.

A technique proposed by Trumpis [1] for finding convolutional codes over Q-ary discrete memoryless channels will be used. These codes are called Q-ary convolutional codes with rate $r = 1$ (one binary input digit to one Q-ary output symbol), and constraint length K. The encoder for these codes is similar to the binary input to binary output digits with rate $r = \frac{1}{\log_2 Q}$.

Let $(u_0, u_1, u_2, \ldots, u_{n-m-1})$ be an input sequence, and let us associate to it the following polynomial $U(x) = u_0 + u_1 x + u_2 x^2 + \ldots + u_{n-m-1} x^{n-m-1}$.

To each $(n - m)$-binary input sequence there exists a corresponding Q-ary output symbol from the encoder. Let $(v_0, v_1, v_2, \ldots, v_{n-1})$ be the output sequence, where each $v_i \in \mathbb{Z}_2$. Let us denote the binary output sequence by the polynomial $V(x) = v_0 + v_1 x + v_2 x^2 + \ldots + v_{n-1} x^{n-1}$.

From the shift-register contents and the tap connections $g_0, g_1, \cdots, g_m$ of the convolutional encoder, the coefficients of $V(x)$ are given by

$$\begin{aligned} v_0 &= u_0 g_0, \\ v_1 &= u_0 g_1 + u_1 g_0, \\ &\vdots \end{aligned}$$

or equivalently, as

$$V(x) = U(x)G(x),$$

with $G(x)$, the generator polynomial of the Q-ary convolutional code, defined as

$$G(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_m x^m,$$

where the coefficients $g_0, g_1, ..., g_m$ belong to $R = GR(2^k, h)$, with $Q = 2^k$.

In order to find good Q-ary convolutional codes, some restrictions have to be placed upon $G(x)$. One of them is related to the fact that we have to avoid catastrophic error propagation. In terms of the polynomials so defined, a catastrophic error means that from an infinite input polynomial, $U(x)$, results a finite output polynomial, $V(x)$. This assertion is true if the generator polynomial does contain a binary factor. Therefore, to avoid catastrophic error propagation $G(x)$ can not contain a binary factor.

On the other hand, if $G(x)$ divides $(x^n - 1)$, then $V(x)\ mod\ (x^n - 1)$ defines a codeword of a Q-ary cyclic block code with parameters $(n, n - m)$. This fact can be used to show that there exists a relationship between cyclic block codes with a given minimum distance and convolutional codes with rate $r = 1$ and a given free distance.

Following [1] the free distance is defined as

$$d_{free} = \min_{\substack{V(x)=U(x)G(x) \\ u_0=1}} \{W[V(x)]\},$$

where $W[h(x)]$ denotes the number of nonzero coefficients (or weight) of the polynomial $h(x)$.

Theorem IV.1. [1] Assume that $g(x)$ generates a Q-ary cyclic block code with parameters $(n, n - m, d)$. If $g(x)$ does not contain a binary factor, then $G(x) = g(x)$ generates a non-catastrophic Q-ary convolutional encoder with rate $r = 1$, constraint length $K = m + 1$, and free distance $d_{free} = d$.

Theorem IV.1 provides a definite technique to construct optimum Q-ary convolutional encoders with rate 1, for groups and finite fields because the cyclic codes derived are maximum distance separable (MDS). For Galois extension rings good Q-ary convolutional codes are obtained in general. However, it may be possible in some isolated cases to obtain optimum Q-ary convolutional codes derived from MDS BCH cyclic codes. For more details, examples and a list of such codes, see [5], and [6].

Example IV.1. Consider the construction of 16-ary convolutional codes, whose output consists of quaternary two-tuples. In this direction, we have to determine the generator polynomial of a 16-ary cyclic block code.

The Galois ring $GR\left(2^2, 2\right)$ consists of the residue classes of polynomials in $\mathbb{Z}_{2^2}[x]$ modulo $x^2 + x + 1$, that is,

$$GR\left(2^2, 2\right) \cong \frac{\mathbb{Z}_{2^2}[x]}{\langle x^2 + x + 1 \rangle} = \{a + bx;\ a, b \in \mathbb{Z}_4\}.$$

In order to find a multiplicative group in the ring $GR\left(2^2, 2\right)$, let α be a primitive element in $GR\left(2^2, 2\right)$. Thus, α is a root of $x^2 + x + 1$ or, in other words

where these operations are realized in $\mathbb{Z}_4$.

Hence, the elements of such a multiplicative group in $GR\left(2^2,2\right)$ are:

$$1$$
$$\alpha$$
$$\alpha^2 = 3+3\alpha$$

The minimal polynomials associated to these elements are:

Elements		Minimal polynomial
1	$\longleftrightarrow$	$(x-1)$
α, α^2	$\longleftrightarrow$	$(x+\alpha)(x+\alpha^2) = x^2+x+1$

where

$$x^3-1 = (x-1)(x-\alpha)(x-\alpha^2).$$

The BCH cyclic code has blocklength $n=3$ over $\mathbb{Z}_4$. The minimum distance d of the code is defined as being equal to the number of consecutive factors of $g(x)$ (factors with consecutive powers of the primitive element) plus 1, see Theorem III.7. Consequently, the generator polynomial must have the greatest number of consecutive powers of α, however, without having a complete minimal polynomial (binary factor). Therefore, the possible generators of the 16-ary convolutional code are:
1- $g(x) = (x-\alpha)$. For this case, $d=2$. The corresponding 16-ary convolutional code has free distance $d_{free}=2$.
2- $g(x) = (x-\alpha^2)$. Similarly to 1-, $d=2$.

Example IV.2. Consider the construction of 64-ary convolutional codes.We have two possibilities to consider: Case I - $Q=4^3$ whose output consists of quaternary three-tuples; and, Case II - $Q=8^2$ whose output consists of octary two-tuples. Once more, we have to determine a generator polynomial of a 64-ary cyclic block code.

Case I - The Galois ring $GR\left(2^2,3\right)$ consists of the residue classes of polynomials in $\mathbb{Z}_{2^2}[x]$ modulo x^3+x+1, that is,

$$GR\left(2^2,3\right) \cong \frac{\mathbb{Z}_{2^2}[x]}{\langle x^3+x+1\rangle} = \{a+bx+cx^2;\ a,b,c\in\mathbb{Z}_4\}.$$

Again, we have to determine a multiplicative group in $GR\left(2^2,3\right)$. Thus, let α be a primitive element in $GR\left(2^2,3\right)$. So, α is a root of x^3+x+1 or, in other words

$$\alpha^3+\alpha+1=0 \quad \Rightarrow \quad \alpha^3 = 3+3\alpha,$$

where these operations are over $\mathbb{Z}_4$.

So, the multiplicative group in $GR\left(2^2,3\right)$ consists of the following elements:

1	$\alpha^7 = 3+2\alpha^2$
α	$\alpha^8 = 2+\alpha$
α^2	$\alpha^9 = 2\alpha+\alpha^2$
$\alpha^3 = 3+3\alpha$	$\alpha^{10} = 3+3\alpha+2\alpha^2$
$\alpha^4 = 3\alpha+3\alpha^2$	$\alpha^{11} = 2+\alpha+3\alpha^2$
$\alpha^5 = 1+\alpha+3\alpha^2$	$\alpha^{12} = 1+3\alpha+\alpha^2$
$\alpha^6 = 1+2\alpha+\alpha^2$	$\alpha^{13} = 3+3\alpha^2$

Since the number of elements of the multiplicative group is even, it follows that $x^{14}-1$ can not be uniquely factored. In this case, we have to find another multiplicative group whose order be odd. Defining $\beta=\alpha^2$, results in a multiplicative group whose order is 7. Consequently, the factorization of x^7-1 is unique.

The minimal polynomials associated to the elements of this

Group elements		Minimal polynomial
1	$\longleftrightarrow$	$(x-1)$
β, β^2, β^4	$\longleftrightarrow$	$(x-\beta)(x-\beta^2)(x-\beta^4)$
$\beta^3, \beta^6, \beta^5$	$\longleftrightarrow$	$(x-\beta^3)(x-\beta^6)(x-\beta^5)$

where

$$x^7-1 = (x-1)(x-\beta)(x-\beta^2)(x-\beta^3)(x-\beta^4)(x-\beta^5)(x-\beta^6).$$

The BCH cyclic code has blocklength $n=7$ over $\mathbb{Z}_4$. In order for this code to have the maximum distance possible, its generator polynomial is given by $g(x)=M_1(x)$ with Hamming distance at least 3. Thus, the 64-ary convolutional code is generated by

$$G(x) = x^3+2x^2+x+3.$$

Thus, the BCH cyclic code parameters are $(7,4,3)$. The corresponding convolutional encoder has $K=4$ and free distance at least 3.

Case II - The Galois ring $GR\left(2^3,2\right)$ consists of the residue classes of polynomials in $\mathbb{Z}_{2^3}[x]$ modulo x^2+x+1, that is,

$$GR\left(2^3,2\right) \cong \frac{\mathbb{Z}_{2^3}[x]}{\langle x^2+x+1\rangle} = \{a+bx;\ a,b\in\mathbb{Z}_8\}.$$

Again, we have to determine a multiplicative group in $GR\left(2^3,2\right)$. Thus, let α be a primitive element in $GR\left(2^3,2\right)$. So, α is a root of x^2+x+1 or, in other words

$$\alpha^2+\alpha+1=0 \quad \Rightarrow \quad \alpha^2 = 7+7\alpha,$$

where these operations are over $\mathbb{Z}_8$.

So, the multiplicative group in $GR\left(2^3,2\right)$ consists of the following elements:

$$1$$
$$\alpha$$
$$\alpha^2 = 7+7\alpha$$

The minimal polynomials associated to the elements of this new multiplicative group are:

Group elements		Minimal polynomial
1	$\longleftrightarrow$	$(x-1)$
α, α^2	$\longleftrightarrow$	$(x-\alpha)(x-\alpha^2)$

where

$$x^3-1 = (x-1)(x-\alpha)(x-\alpha^2).$$

The BCH cyclic code has blocklength $n=3$ over $\mathbb{Z}_8$. The minimum distance d of the code is defined as being equal to the number of consecutive factors of $g(x)$ plus 1. As in the previous example, the possible generators of the 64-ary convolutional code are:
1- $g(x) = (x-\alpha)$. For this case, $d=2$. The corresponding 64-ary convolutional code has free distance $d_{free}=2$.
2- $g(x) = (x-\alpha^2)$. Similarly to 1-, $d=2$.

Based on the previous two examples, in the next section we establish a procedure to construct Q-ary convolutional codes over local rings.

V. Construction of Q-ary Convolutional Codes over Local Rings

The following procedure allows the construction of convolutional codes, whose codewords belong to a given local ring $\mathbb{Z}_Q$,

In order to obtain Q^τ-ary convolutional codes consisting of Q-ary τ-tuples, we have initially to determine the generator polynomial of a Q^τ-ary cyclic block code. The Galois ring $GR\left(2^\kappa,\tau\right)$ consists of the residue classes of the polynomials over $\mathbb{Z}_{2^\kappa}[x]$ modulo a primitive ideal of degree τ, also belonging to $\mathbb{Z}_{2^\kappa}[x]$. With the objective of determining a multiplicative group in $GR\left(2^\kappa,\tau\right)$, let α be a primitive element in the ring under consideration. Consequently, α is a root of the primitive polynomial generating the ideal being considered. Therefore, it is possible to express all the elements of the multiplicative group as τ-tuples of α. Note that the operations are over $\mathbb{Z}_{2^\kappa}$. If the order δ of the multiplicative group is even, the term $x^\delta-1$ can not be uniquely factorable. Hence, we have to determine, in the multiplicative group, an element β (a power of α), whose order θ be an odd multiplicity of the order of α in the $GF\left(2^\tau\right)$. In this way, the term $x^\theta-1$ may now be uniquely factored. Once the minimal polynomials associated to each one of the elements of the multiplicative group generated by β, we may establish a generator polynomial of the cyclic block code, not containing a binary factor, will coincide with the generator polynomial of the Q-ary convolutional code over $\mathbb{Z}_Q$. In this direction, we have to select the greatest number of consecutive powers of β, and consequently the corresponding minimal polynomials, however, without containing any binary factor. The minimum distance d of the cyclic block code is defined as being equal to the number of consecutive powers of the primitive element plus 1. The Q-ary convolutional code over $\mathbb{Z}_Q$ so constructed will achieve good free distance as shown in Table I. Table II, shows the free distance which can be achieved if an MDS BCH cyclic code were used. However, the corresponding BCH cyclic codes are not MDS. Therefore, the free distance of the convolutional code is $d_{free}\geq d$.

$GR(p^k,r)$	Alphabet	(n,k,d)
$GR(4,3)$	$\mathbb{Z}_4$	(7,4,3)
$GR(4,4)$	$\mathbb{Z}_4$	(15,5,7)
$GR(8,3)$	$\mathbb{Z}_8$	(7,4,3)

TABLE I
BCH CYCLIC CODES OVER $GR(p^k,r)$

d_{free}	Generator Polynomial
4	$3+x+2x^2+x^3$
9	$1+x+3x^2+3x^4+3x^5+2x^7+x^8+2x^9+x^{10}$
4	$7+5x+6x^2+x^3$

TABLE II
CONVOLUTIONAL CODES

VI. CONCLUSIONS

In this paper, we have proposed a systematic procedure for constructing good Q-ary convolutional codes over rings. The procedure is based on finding a primitive element in the group of units of the Galois extension ring. For a given design distance, the polynomial generator of a BCH cyclic block code over $\mathbb{Z}_Q$ binary factor. Hence, the coefficients of the generator polynomial is used as the tap connections for the Q-ary convolutional encoder. Some examples of these codes were tabulated.

REFERENCES

[1] B.D. Trumpis, *Convolutional Coding for M-ary Channels*, Ph.D. Dissertation, System Science Dept., UCLA, 1975.

[2] V. Tarokh, N. Seshadri, and A.R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction", *IEEE Trans. Inform. Theory*, vol. 44, n^o 2, March 1998, pp. 744-765.

[3] V. Tarokh, A. Naguib, N. Seshadri, and A.R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criteria in the presence of channel estimation errors, mobility, and multipaths", *IEEE Trans. Commun.*, vol. 47, n^o 2, February 1999, pp. 199-207.

[4] V. Tarokh, H. Jafarkhani, and A.R. Calderbank, "Space-time block coding for wireless communications: Performance results", *IEEE J. Select. Areas Commun.*, vol. 47, n^o 3, March 1999, pp. 451-460.

[5] P.R. Barbosa, *Construction of $\mathbb{Z}_{2^k}$-pseudolinear Codes by Isometric Applications and Galois Extensions of Local Rings*, MS Thesis, DT-FEEC-UNICAMP, 2000 (in Portuguese).

[6] R.D. Valença, *Methods for the Construction of Space-Time Codes over Groups, Rings, and Fields for Quasi-static Fading Channels*, MS Thesis, DT-FEEC-UNICAMP, 2001 (in Portuguese).

[7] R. Palazzo Jr., J.C. Interlando, J.R. Gerônimo, A.A. Andrade, O.M. Favareto, T.P. Nóbrega Neto, *Error Correcting Codes over Fields, Rings and Groups*, DT-FEEC-UNICAMP, 1998, (in Portuguese).

[8] R. Palazzo Jr., B.F. Uchôa Filho, e J.P. Arpasi, *Fundamentals and Applications of Convolutional Codes in Communication Systems*, DT-FEEC-UNICAMP, 1999, (in Portuguese).

[9] A.A. Andrade and R. Palazzo Jr., "BCH codes over arbitrary finite commutative rings," *12th Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, June 23-27, 1997, Toulouse, France.

[10] J.C. Interlando, *A Contribution to the Construction and to the Decoding of Linear Codes over Abelian Groups via Concatenation of Codes over Rings of Residue Integers*, PhD Dissertation, FEE-UNICAMP, 1994, (in Portuguese).

[11] J.C. Interlando and R. Palazzo, Jr., "A note on cyclic codes over $\mathbb{Z}_m$", *VI Reunión de Trabajo en Processamiento de la Información y Control*, Bahia Blanca, Argentina, November 1995.

[12] B.R. McDonald, *Finite Rings with Identity*, New York, Marcel Dekker, 1974.

[13] P. Shankar, "On BCH codes over arbitrary integer rings", *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 480-483, July 1979.