(Reprint of pp. 154-159 in Proc. 2nd Int. Workshop on Algebraic and Combinatorial coding Theory, Leningrad, Sept. 16-22, 1990)

SYSTEMATICITY AND ROTATIONAL INVARIANCE OF CONVOLUTIONAL CODES OVER RINGS

James L. Massey and Thomas Mittelholzer
Inst. for Signal and Info. Processing
Swiss Federal Institute of Technology
CH-8092 Zürich, Switzerland

Abstract: The necessary and sufficient condition for an (n,k) convolutional code over a finite commutative ring to have a systematic encoder is derived. A sufficient condition for a systematic (n,1) convolutional code over the ring of integers modulo M to be rotationally invariant is derived together with a similar, but not identical, necessary condition.

I. INTRODUCTION

The purpose of this paper is to consider two basic structural properties of convolutional codes over rings. Such codes were introduced in [1] together with their motivation from phase-modulated signals, cf. also [2].

In the sequel, R will always denote a finite commutative ring with multiplicative identity 1, and R[D] will denote the ring of polynomials in the indeterminate D with coefficients in R. By "polynomial", we will always mean an element of R[D]. The leading coefficient (trailing coefficient) of a non-zero polynomial is the coefficient of the largest (smallest) power of D whose coefficient is non-zero. If a(D) and b(D) are polynomials and if the leading coefficient of b(D) is a unit of R, then there exist unique polynomials q(D) and r(D) such that $a(D) = q(D)b(D) + r(D)$ and degree [r(D)] < degree [b(D)].

By a rational function over R we mean a ratio of polynomials $a(D)/b(D)$ in which the trailing coefficient of the denominator polynomial b(D) is a unit of R. As usual, two rational functions $a_1(D)/b_1(D)$ and $a_2(D)/b_2(D)$ are defined to be equal just when $a_1(D)b_2(D) = a_2(D)b_1(D)$. The set of all rational functions over R forms a ring that is denoted by R(D). By formal long division of the denominator polynomial into the numerator polynomial, every rational function can be expressed uniquely as a Laurent series with at most finitely many negative powers of D. For instance, $1/(1-D) = 1 + D + D^2 + \ldots$ and $1/(D-D^2) = D^{-1} + 1 + D + \ldots$.

We will speak interchangeably of the rational function $\alpha(D)$ and the sequence $(\ldots, \alpha_{-1}, \alpha_0, \alpha_1, \ldots)$ where α_i is the coefficient of D^i in the Laurent series for $\alpha(D)$. The

start of a non-zero $\alpha(D)$ is the smallest i such that $\alpha_i = 0$. By way of convention, the sequence $\alpha(D) = 0$ has start $+\infty$. We will say that $\alpha(D)$ is causal (or realizable) if its start is nonnegative.

II. SYSTEMATIC CODES

Let $R(D)^n$ denote the set of all n-tuples with entries in R(D) and note that $R(D)^n$ is a rank-n free module over R(D). We define an (n,k) R-ary convolutional code M to be a rank-k free submodule of $R(D)^n$. By the causal subcode M_c of M, we mean the submodule of M consisting of all codewords having only causal components. By the start module M_0 of M, we mean the R-module consisting of all R-ary n-tuples $[\alpha_1(0), \alpha_2(0), ..., \alpha_n(0)]$ for which $[\alpha_1(D), \alpha_2(D), ..., \alpha_n(D)]$ is a codeword in the causal subcode M_C. We shall say that a convolutional code M is quasi-proper if M_0 is a rank-k free submodule of R^n, and that it is proper if one can select k components so that the n-tuples in M_0 when restricted to these components form the free module R^k.

A generator matrix for M is any $k \times n$ matrix whose rows are a basis for M. An encoding matrix is a generator matrix all of whose entries are realizable. An encoding matrix G(D) is systematic if each column of the identity matrix I_k is also a column of G(D). The convolutional code M is systematic if it has a systematic encoding matrix.

Propositon 1: A convolutional code is systematic if and only if it is proper.

Example 1: The (2,1) convoutional code over $R = Z_4$, the ring of integers modulo 4, having $G(D) = [2+D \quad 2]$ as an encoding matrix is not even quasi-proper because $M_0 = \{ [0,0], [0,2], [2,0], [2,2]\}$ is not a free module.

Example 2: The (2,1) convolutional code over $R = Z_6$ having $G(D) = [2 \quad 3]$ is quasi-proper because M_0 is the free submodule of R^2 with basis [2, 3], but it is not proper because M_0 when restricted to the first component is the R-module {0, 2, 4} and when restricted to the second component is the R-module {0, 3} but neither of these is the free module R.

Example 3: The (2,1) convolutional code over $R = Z_6$ having $G(D) = [5 \quad 2+3D]$ as an encoding matrix is proper because M_0 is the free submodule of R^2 generated by [5, 2] and M_0 restricted to the first component is the free module R generated by 5. Note that scaling the first and only row of the given encoding matrix by 5 gives the systematic encoding matrix $[1 \quad 4+3D]$.

Proof of Proposition 1: Suppose M is systematic and let G(D) be a systematic encoding matrix for M. Then M_0 is the free submodule of R^n having the rows of G(0) as a basis. Moreover, M_0 restricted to some k components where the columns of G(0) contain all columns of I_k is trivially the free module R^k and thus M is proper.

Suppose conversely that M is a proper (n,k) convolutional code. We can then find k codewords $[\alpha_1(D), \alpha_2(D), ..., \alpha_n(D)]$ in the causal subcode M_c such that the corresponding R-ary n-tuples $[\alpha_1(0), \alpha_2(0), ..., \alpha_n(0)]$ are linearly independent over R and remain linearly independent when restricted to some choice of k components. These k codewords form the rows of an encoding matrix G(D) whose columns in the chosen k components form a $k \times k$ matrix A(D) such that the determinant of A(0) is a unit of R. Hence $A(D)^{-1}G(D)$ is a systematic encoder for M, as was to be shown.

If the ring R is in fact a finite field, then every (n,k) convolutional code over R is proper. In particular, **every (n,k) convolutional code over R = Z_p, where p is a prime, is proper.**

If M is the product of two or more distinct primes, then, by the Chinese Remainder Theorem, Z_M is isomorphic to the direct product of the fields Z_p for which p is a prime factor of M. An (n,k) convolutional code over Z_M is thus isomorphic to a direct product of (n,k) convolutional codes over the corresponding fields Z_p. Similarly, the start module M_0 is isomorphic to the direct product of the start modules of the field codes, which modules are vector spaces of dimension k over Z_p. It follows that M_0 has a basis of cardinality k, i. e., it is a free module of rank k. Thus, **when M is the product of two or more distinct primes, every (n,k) convolutional code over Z_m is quasi-proper.** Example 2 shows, however, that such codes need not be proper.

When $M = p^e$ where p is a prime and $e > 1$, then a quasi-proper (n,k) convolutional code over $R = Z_M$ is also proper. To see this, suppose that M is quasi-proper and let G_0 be a k by n matrix over R whose rows are a basis for the free start module M_0. Multiplying each row of G_0 by p^{e-1} gives a k by n matrix G_0 over R, no nontrivial linear combination of whose rows can vanish when the coefficients of the linear combination are restricted to lie in the subset {0, 1, ..., p-1} of R. Equivalently, reducing the entries in G_0 modulo p gives a k by n matrix G_0 over the field Z_p with linearly independent rows. It follows that G_0 must also contain k linearly independent columns over Z_p, and hence that G_0 must also contain k linearly independent columns over R so that the code M is indeed proper. Example 1 shows, however, that a convolutional code over such R need not be quasi-proper.

III. ROTATIONAL INVARIANCE

We have shown elsewhere that convolutional codes over $R = Z_M$ are the "natural" linear codes for use with M-ary phase modulation [1], [2]. We assume hereafter that the element i of Z_M is mapped by the modulator to the signal $e^{j2\pi i/M}$ in the phase modulation signal set. Then the transformation $i \rightarrow i+1$ in Z_M corresponds to the minimum phase shift of the signals that leaves the signal set unchanged. Any "trellis code" for phase modulation is said to be rotationally invariant if this minimum shift, when applied to all components starting at time 0 or later in each codeword, yields a word that differs in at most finitely many positions from another codeword. Because $1/(1-D) = 1 + D + D^2 + ...$, it follows by definition that an (n,k)

convolutional code M over $R = Z_M$ is rotationally invariant if adding $[1/(1-D), 1/(1-D), ..., 1/(1-D)]$ to each codeword in the causal subcode M_c yields an n-tuple that differs from another codeword by a polynomial in each component. The following propositon is then an immediate consequence of the linearity of M.

Propositon 2: A convolutional code over $R = Z_M$ is rotationally invariant if and only if it contains a codeword each of whose components differs from $1/(1-D)$ by a polynomial.

The following simple lemma will be useful in the sequel.

Lemma: A rational function in R(D) differs from $1/(1-D)$ by a polynomial if and only if it can be written as $p(D)/(1-D)$ where $p(D)$ is a polynomial with $p(1) = 1$.

Proof: A rational function differing from $1/(1-D)$ by a polynomial can by definition be written as $q(D) + 1/(1-D)$ where $q(D)$ is a polynomial. But then $q(D) + 1/(1-D) = p(D)/(1-D)$ where $p(D) = (1-D)q(D)+1$ and hence $p(1) = 1$. Conversely, because the leading coefficient of 1-D is a unit of R, any polynomial $p(D)$ with $p(1) = 1$ can be written uniquely as $p(D) =(1-D)q(D)+r$ for some poynomial $q(D)$ and some r in R. But then $r = p(1)$ and hence $p(D)/(1-D) = q(D) + 1/(1-D)$ as was to be shown.

We now consider testing whether or not an (n,1) systematic convolutional code over Z_M is rotationally invariant.

Proposition 3: The (n,1) convolutional code over Z_M with systematic encoding matrix

$$[\,1 \;\; \frac{a_2(D)}{b_2(D)} \;\; \cdots \frac{a_n(D)}{b_n(D)}\,],$$

where $a_i(D)$ and $b_i(D)$ are not both divisible by 1-D for $i = 2, 3,..., n$, is rotationally invariant if $a_i(1) = b_i(1)$ is a unit of Z_M for each i, $2 \le i \le n$. Conversely, the code cannot be rotationally invariant unless $a_i(1) = b_i(1)$ for each i, $2 \le i \le n$.

Remark: The condition that $a_i(1)$ and $b_i(D)$ are not both divisible by 1-D is just the condition that $a_i(1)$ and $b_i(1)$ are not both 0.

Proof: Suppose that $a_i(1) = b_i(1)$ is a unit of R for each i. Consider the information sequence $U(D) = cb_2(D)...b_n(D)/(1-D)$ where $c = (b_2(1)...b_n(1))^{-1}$. It follows from the lemma that U(D) differs from $1/(1-D)$ by a polynomial. The resulting codeword is

$$[\,U(D) \quad U(D)\frac{a_2(D)}{b_2(D)} \;...\; U(D)\frac{a_2(D)}{b_2(D)}\,].$$

The i-th component of this codeword differs from U(D) only in that $b_i(D)$ in the numerator is replaced by $a_i(D)$; hence this i-th component also differs from $1/(1-D)$ by a polynomial because $a_i(1) = b_i(1)$. Thus the code is indeed rotationally invariant.

Conversely, suppose the code is rotationally invariant. Then, by the lemma, the information sequence that yields some codeword each of whose components differs from $1/(1-D)$ by a polynomial must have the form $U(D) = p(D)/(1-D)$ where $p(D)$ is a polynomial with $p(1) = 1$. The i-th component of the resulting codeword, $(p(D)a_i(D))/((1-D)b_i(D))$, can then by the lemma be written as $q(D)/(1-D)$ where $q(D)$ is a polynomial with $q(1) = 1$. Thus, $p(D)a_i(D) = q(D)b_i(D)$ from which it follows that $a_i(1) = b_i(1)$, as was to be shown.

Example 4: The (2,1) code of Example 3 is rotationally invariant since $a_2(1) = b_2(1) = 1$ is a unit of Z_6.

Unfortunately, the values of $a_i(1)$ and $b_i(1)$ do not suffice to determine whether or not the code is rotationally invariant when $a_i(1) = b_i(1)$ is a non-zero non-unit, as the following examples show.

Example 5: The (2,1) code over Z_6 with encoding matrix $G(D) = \left[\, 1 \quad \frac{5+3D}{1+D} \,\right]$,

which has $a_2(1) = b_2(1) = 2$, a non-unit, is rotationally invariant since the information sequence $U(D) = (5+2D)/(1-D)$ produces the codeword $\left[\, \frac{5+2D}{1-D} \quad \frac{1}{1-D} \,\right]$ each of whose components, by the lemma, differs from $1/(1-D)$ by a polynomial.

Example 6: The (2,1) code over Z_6 with encoding matrix $G(D) = \left[\, 1 \quad \frac{2}{1+D} \,\right]$,

which also has $a_2(1) = b_2(1) = 2$, is not rotationally invariant. To see why, note that the second entry of this matrix is just 4 times the corresponding entry of the matrix in Example 5. Thus, because 4 is not a unit, it is impossible that there be any 1's whatsover in the Laurent series of the second component of a codeword for the code of this example, much less that there be all 1's after some finite number of terms.

Finally, we consider the case of polynomial encoders for (n,1) systematic codes to show that our condition for rotational invariance reduces to the well-known (cf. [3, p. 255]) condition for a "transparent code" for binary phase modulation when $M = 2$ so that Z_M is a field.

Corollary to Propositon 3: The (n,1) convolutional code over Z_M with polynomial encoding matrix $G(D) = [a_1(D) \; a_2(D) \; ... \; a_n(D)]$, where $a_1(0)$ is a unit of Z_M and where $a_i(1)$ is not 0 for at least one i, $1 \le i \le n$, is rotationally invariant if $a_1(1) = a_2(1) = ... = a_n(1)$ is a unit of Z_M. Conversely, the code cannot be rotationally invariant unless $a_1(1) = a_2(1) = ... = a_n(1)$.

Proof: Dividing each entry of $G(D)$ by $a_1(D)$ gives a systematic encoding matrix as in Propositon 3 where now $b_i(D) = a_1(D)$ for $i = 2,3,..,n$. The corollary follows immediately.

REFERENCES

[1] J.L. Massey and T. Mittelholzer, "Convolutional Codes over Rings", pp. l4-l8 in Proc. 4th Joint Swedish-USSR Workshop on Info.Th., Gotland, Sweden, Aug. 27 - Sept. 1, l989.

[2] J.L. Massey, "A Short Introduction to Coding Theory and Practice", pp. 6.29 - 6.33 in Proc. Int. Symp. on Signals, Systems and Electronics (ISSSE '89), Erlangen, Germany, Sept. l8 - 20, l989.

[3] G.C. Clark Jr. and J.B. Cain, Error-Correction Coding for Digital Communications. New York: Plenum, l98l.