Some structural properties of convolutional codes over rings

Johannesson, Rolf; Wan, Zhe-Xian; Wittenmark, Emma

Published in:
IEEE Transactions on Information Theory

DOI:
10.1109/18.661532

1998

Some Structural Properties of Convolutional Codes over Rings

Rolf Johannesson, *Fellow, IEEE*, Zhe-Xian Wan, and Emma Wittenmark, *Student Member, IEEE*

***Abstract*— Convolutional codes over rings have been motivated by phase-modulated signals. Some structural properties of the generator matrices of such codes are presented. Successively stronger notions of invertibility of generator matrices are studied, and a new condition for a convolutional code over a ring to be systematic is given and shown to be equivalent to a condition given by Massey and Mittelholzer. It is shown that a generator matrix that can be decomposed into a direct sum is basic, minimal, and noncatastrophic if and only if all generator matrices for the constituent codes are basic, minimal, and noncatastrophic, respectively. It is also shown that if a systematic generator matrix can be decomposed into a direct sum, then all generator matrices of the constituent codes are systematic, but that the converse does not hold. Some results on convolutional codes over $\mathbb{Z}_{p^e}$ are obtained.**

***Index Terms*—Convolutional codes over rings, direct sum decomposition of rings, proper convolutional codes, systematic convolutional codes.**

I. Introduction

Massey and Mittelholzer [1] introduced convolutional codes over rings together with their motivation by phase-modulated signals. They showed that convolutional codes over rings behave very differently than convolutional codes over fields. Some structural properties of convolutional codes over rings were given in [2] and [3]. Further structural properties are presented in this correspondence.

For convolutional codes over rings, there are three successively stronger notions of invertibility of generator matrices. The first is transducer invertibility, which is equivalent to a one-to-one map between information words and codewords. It is shown that this is equivalent to the rows of the generator matrix being free over the ring $R(D)$. The second is right invertibility, which is the existence of a right $R(D)$-inverse to the generator matrix. The last is the existence of a realizable right $R(D)$-inverse to the generator matrix, which is equivalent to systematicity. Systematicity implies right invertibility which implies transducer invertibility, but the converse implications do not hold.

In Section II, we define rings of rational functions and realizable rational functions and some fundamental coding concepts such as generator matrix, equivalence, right invertibility, catastrophicity, and minimality for the ring case. Section III is devoted to systematicity of ring codes. After having defined a systematic convolutional code, we give a new condition for a convolutional code over a ring to be systematic. In Section IV, we prove that our new condition for systematicity is equivalent to a condition given by Massey and Mittelholzer [2]. Section V treats codes over a direct sum of rings. We show that if a systematic generator matrix can be decomposed into a direct sum, then all generator matrices for the decomposed code are systematic, but the converse does not hold. Various examples are given. We also give some results on convolutional codes over $\mathbb{Z}_{p^e}$.

Manuscript received December 20, 1995; revised October 1, 1997. This work was supported in part by the Swedish Research Council for Engineering Sciences under Grant 94-77. The material in this correspondence was presented at the IEEE International Symposium on Information Theory, Ulm, Germany, June 29–July 4, 1997.

The authors are with the Department of Information Technology, Information Theory Group, Lund University, S-221 00 Lund, Sweden.

Publisher Item Identifier S 0018-9448(98)00982-1.

II. Convolutional Generator Matrices over Rings

Let R be a commutative ring with identity and let $R[D]$ be the polynomial ring over R. The *trailing* coefficient of a nonzero polynomial is the coefficient of the smallest power of D with a nonzero coefficient. Let $R(D)$ be the set

$$\left\{ \frac{f(D)}{q(D)} \Big| f(D), q(D) \in R[D], \text{ and the trailing coefficient of } q(D) \text{ is a unit in } R \right\} \tag{1}$$

modulo the equivalence relation

$$\frac{f(D)}{q(D)} \sim \frac{f_1(D)}{q_1(D)} \text{ if and only if } f(D)q_1(D) = f_1(D)q(D). \tag{2}$$

That this is an equivalence relation follows from the assumption that the trailing coefficients of the denominator polynomials are units. The equivalence class of $f(D)/q(D)$ will be denoted by $\overline{f(D)/q(D)}$ or sometimes by the abbreviation $f(D)/q(D)$. It is clear that $R(D)$ is a ring with addition and multiplication defined by

$$\overline{\frac{f(D)}{q(D)}} + \overline{\frac{h(D)}{k(D)}} = \overline{\frac{f(D)k(D) + h(D)q(D)}{q(D)k(D)}}$$

and

$$\overline{\frac{f(D)}{q(D)}}\ \overline{\frac{h(D)}{k(D)}} = \overline{\frac{f(D)h(D)}{q(D)k(D)}}.$$

We call $R(D)$ the *ring of rational functions* over R in the indeterminate D. Each element of $R(D)$ can be expanded into a formal Laurent series in D.

Remark: Without the condition in the definition of the ring of rational functions over R, that the trailing coefficients of the denominator polynomials are units, then

$$\frac{f(D)}{q(D)} \sim \frac{f_1(D)}{q_1(D)} \text{ if and only if } f(D)q_1(D) = f_1(D)q(D) \tag{3}$$

is not always an equivalence relation. For example, let $R = \mathbb{Z}_4$; then $0/2 \sim 2/D$ and $0/2 \sim 2/D^2$, but $2/D$ and $2/D^2$ are not equivalent.

Let $R_r(D)$ be the subring of $R(D)$ consisting of those elements (equivalence classes) which contain a representative $f(D)/q(D)$ with $q(0)$ a unit in R. We call this the *ring of realizable functions* and the elements of $R_r(D)$ *realizable functions*.

Definition 1: A rate-b/c *convolutional transducer* over the ring of rational functions $R(D)$ is a linear mapping

$$\begin{aligned} R(D)^b &\to R(D)^c \\ \boldsymbol{u}(D) &\mapsto \boldsymbol{v}(D) \end{aligned} \tag{4}$$

which can be represented as

$$\boldsymbol{v}(D) = \boldsymbol{u}(D)G(D) \tag{5}$$

where $G(D)$ is a $b \times c$ matrix (called the transfer function matrix) with entries in $R(D)$ whose rows are free over $R(D)$.

Definition 2: The set

$$\mathcal{C} = \{\boldsymbol{u}(D)G(D) | \boldsymbol{u}(D) \in R(D)^b\} \tag{6}$$

where $G(D)$ is the transfer function matrix of a rate-b/c convolutional transducer over $R(D)$, is a *rate-*b/c *convolutional code* over R. The output $\boldsymbol{v}(D) = \boldsymbol{u}(D)G(D)$ is the *code sequence* arising from the *information sequence* $\boldsymbol{u}(D)$.

It follows immediately from Definition 2 that a rate-b/c convolutional code $\mathcal{C}$ over R with transfer function matrix $G(D)$ can be regarded as the $R(D)$ row module of $G(D)$. Hence, it can also be regarded as the rate-b/c block code over $R(D)$ which has $G(D)$ as its (block code) generator matrix.

Obviously, we must be able to reconstruct the information sequence $\boldsymbol{u}(D)$ from the code sequence $\boldsymbol{v}(D)$ when there is no noise on the channel. Therefore, we require that the transducer map be injective, i.e., that the rows of the transfer function matrix $G(D)$ be free over the ring $R(D)$. However, the entries in $G(D)$ need not be realizable functions.

Definition 3: The transfer function matrix $G(D)$ of a rate-b/c convolutional transducer over $R(D)$ is a *generator matrix* of the corresponding rate-b/c code over R if its entries are all realizable functions.

Let $F((D))$ denote the field of formal Laurent series over the field F in the indeterminate D, and let $R((D))$ denote the ring of formal Laurent series over the ring R in the indeterminate D. Since the seminal work by Forney [4], it is customary to regard a convolutional code over a field F as the vector space over $F((D))$ generated by a generator matrix over $F(D)$ or, equivalently, as the rate-b/c block code over the infinite field of formal Laurent series having $G(D)$ as its generator matrix (see also [5]). Massey, however, persists in viewing convolutional codes as the $F(D)$ vector space of the generator matrix [6]. Although we prefer the first view in the field case as being more natural since it does not require information sequences to be ultimately periodic, we have adopted the second view in this correspondence in order not to restrict the generator matrices over $R(D)$ to those whose rows are free over $R((D))$ (see Remark after the proof of Theorem 1). Mittelholzer [7] has recently shown that there indeed exist generator matrices over $R(D)$ whose rows are free over $R(D)$ but not over $R((D))$! The corresponding problem does not arise in the field case. For rings of practical interest for convolutional codes, for example, finite rings, Mittelholzer has also showed that there is no difference between the rows of the generator matrix being free over $R(D)$ or over $R((D))$ [7]. However, other difficulties will be encountered, for example, those concerning equivalence and in results where Theorem 1 is used.

Analogously to the field case we introduce

Definition 4: Two generator matrices are *equivalent* if they generate the same code.

A square matrix $T(D)$ is invertible over $R(D)$ if there exists a square matrix $T'(D)$ of the same size over $R(D)$ such that $T(D)T'(D) = T'(D)T(D) = I$. The inverse is obviously unique and is denoted $T^{-1}(D)$.

Theorem 1: Two rate-b/c generator matrices $G(D)$ and $G'(D)$ are equivalent if and only if there exists a $b \times b$ invertible matrix $T(D)$ over $R(D)$ such that $G(D) = T(D)G'(D)$.

Proof: If $G(D) = T(D)G'(D)$, where $T(D)$ is invertible over $R(D)$, then the generator matrices $G(D)$ and $G'(D)$ are obviously equivalent.

Conversely, assume that $G(D)$ and $G'(D)$ are equivalent. Then we can find input sequences, $\boldsymbol{u}_i(D), \boldsymbol{u}'_i(D) \in R(D)^b, 1 \le i \le b$, such that $G(D) = T(D)G'(D)$ and $G'(D) = S(D)G(D)$ where

$$T(D) = \begin{pmatrix} \boldsymbol{u}_1(D) \\ \vdots \\ \boldsymbol{u}_b(D) \end{pmatrix} \quad \text{and} \quad S(D) = \begin{pmatrix} \boldsymbol{u}'_1(D) \\ \vdots \\ \boldsymbol{u}'_b(D) \end{pmatrix}.$$

Hence,

$$G(D) = T(D)G'(D) = T(D)S(D)G(D)$$

and, thus, since the rows of $G(D)$ are free over $R(D), T(D)S(D) = I_b$ where I_b is the $b \times b$ identity matrix. Similarly, $S(D)T(D) = I_b$ so that $S(D)$ is indeed an inverse of $T(D)$. □

Remark: Let $G(D)$ be a matrix over $R(D)$ whose rows are free over $R(D)$ but not over $R((D))$. Then there exists a $\boldsymbol{u}(D) \in R^b((D))$ such that

$$\boldsymbol{u}(D)G(D) = \mathbf{0} \in R^c(D).$$

If in Definition 1 input sequences over $R((D))$ were allowed, then we could not have transducer invertibility. Moreover, in our proof of the converse part of Theorem 1, both $T(D)$ and $S(D)$ would be matrices over $R((D))$, and from $G(D) = T(D)S(D)G(D)$, or, equivalently, from $(T(D)S(D) - I_b)G(D) = \mathbf{0}$, we could not conclude that $T(D)S(D) = I_b$. A theory for convolutional codes over rings without Theorem 1 would be impoverished.

Definition 5: A convolutional code $\mathcal{C}$ is *right invertible* if it has a generator matrix $G(D)$ which has a right inverse over $R(D)$.

The following theorem shows that this definition is independent of the chosen generator matrix.

Theorem 2: If a convolutional code $\mathcal{C}$ has a generator matrix $G(D)$ which has a right inverse over $R(D)$, so does every generator matrix for this code.

Proof: Let $G'(D)$ be any generator matrix of the code $\mathcal{C}$. Then there exists an invertible $b \times b$ matrix $T(D)$ over $R(D)$ such that $G'(D) = T(D)G(D)$. Let $G^{-1}(D)$ be a right inverse of $G(D)$; then $G^{-1}(D)T^{-1}(D)$ is a matrix over $R(D)$ and is a right inverse of $G'(D)$. □

It is well known that every generator matrix of convolutional codes over a field is right invertible [4], [5]. Over rings R there exist convolutional codes $\mathcal{C}$ which are not right invertible. However, as recently shown by Mittelholzer, this cannot happen if R is commutative and satisfies the descending chain condition (DCC) [7]. Every finite ring satisfies the descending chain condition. Thus for codes over finite commutative rings, every generator matrix has a right inverse.

Example 1: Consider the convolutional code $\mathcal{C}$ over the integers $\mathbb{Z}$ with the 1×1 generator matrix

$$G(D) = (2 + D).$$

The row is free over $\mathbb{Z}(D)$, but $G(D)$ does not have a right inverse over $\mathbb{Z}(D)$ and hence $\mathcal{C}$ is not right invertible.

However, the code over $\mathbb{Z}_4$ (the ring of integers modulo 4), with $G(D) = (2 + D)$ has a right inverse over $\mathbb{Z}_4(D)$, namely, $G^{-1}(D) = ((2 + D)/D^2)$, and hence the convolutional code $\mathcal{C}$ over $\mathbb{Z}_4$ with generator matrix $G(D)$ is right invertible.

Remark: The convolutional code over $\mathbb{Z}$ in Example 1—with bi-infinite code sequences—appears as [8, Example 6], where it was shown that the trellis of $G(D)$ generates an incomplete code. The deep reason why $G(D)$ does not have a right inverse is the lack of the DCC property [7].

Theorem 3: Let $G(D)$ be a $b \times c$ generator matrix. If there exists a $b \times b$ submatrix of $G(D)$ whose determinant is a unit in $R(D)$, then the convolutional code $\mathcal{C}$ generated by $G(D)$ is right invertible.

Proof: Without loss of essential generality, assume that $G(D) = (A(D)\, B(D))$, where $A(D)$ is the $b \times b$ submatrix whose determinant is a unit in $R(D)$. Then, $A(D)$ has an inverse $A^{-1}(D)$ over $R(D)$. Letting

$$G'(D) = \begin{pmatrix} A^{-1}(D) \\ \mathbf{0} \end{pmatrix}$$

gives

$$G(D)G'(D) = (A(D)\; B(D)) \begin{pmatrix} A^{-1}(D) \\ \mathbf{0} \end{pmatrix} = I_b$$

so that $G'(D)$ is a right inverse of $G(D)$ and hence the code $\mathcal{C}$ generated by $G(D)$ is right invertible. □

From Theorem 1 follows immediately

Corollary 4: If a generator matrix $G(D)$ of a convolutional code $\mathcal{C}$ has a $b \times b$ submatrix whose determinant is a unit in $R(D)$, so do all the generator matrices of $\mathcal{C}$.

It is worth noting that the corresponding conclusion for units over the ring of *realizable* rational functions $R_r(D)$ does not hold. That a convolutional code $\mathcal{C}$ has a generator matrix having a $b \times b$ submatrix whose determinant is a unit in $R_r(D)$ does not imply that every generator matrix of $\mathcal{C}$ has a $b \times b$ subdeterminant which is a unit in $R_r(D)$, as the following example shows.

Example 2: Consider the 1×1 generator matrix $G(D) = (1)$ over the ring $\mathbb{Z}_M$. Its determinant, 1, is a unit in $(\mathbb{Z}_M)_r(D)$, but the equivalent generator matrix $G'(D) = (D)$ does not have a realizable inverse.

In connection with Example 2, Forney [9] suggested the notion of causal equivalence.

Definition 6: Two generator matrices $G(D)$ and $G'(D)$ are said to be *causally equivalent* if there exists a $b \times b$ matrix $T(D)$ which is realizable and has a realizable inverse such that $G(D) = T(D)G'(D)$.

From Theorem 1 it is quite easy to show that having a $b \times b$ submatrix whose determinant is a unit in $R_r(D)$ is a property which is preserved between causally equivalent generator matrices.

Theorem 5: If a generator matrix $G(D)$ of a convolutional code $\mathcal{C}$ has a $b \times b$ submatrix whose determinant is a unit in $R_r(D)$, so do all causally equivalent generator matrices of $\mathcal{C}$.

The following example shows that for a generator matrix to have a right inverse over $R(D)$ it is not necessary that it has a $b \times b$ submatrix whose determinant is a unit in $R(D)$.

Example 3: The generator matrix

$$G(D) = (2\ 3)$$

over $\mathbb{Z}_6(D)$ does not have a 1×1 submatrix whose determinant is a unit in $\mathbb{Z}_6(D)$, but it does have a right inverse, viz.,

$$G^{-1}(D) = \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

In the field case, a convolutional generator matrix is said to be *basic* if it is polynomial and has a polynomial right inverse; we use this definition for the ring case as well.

A generator matrix $G(D)$ of a convolutional code in the field case is said to be *catastrophic* if there exists an information sequence $\boldsymbol{u}(D)$ with an infinite number of nonzero symbols that gives a codeword $\boldsymbol{v}(D)$ of finite weight, a definition that we also take over to the ring case.

A convolutional code $\mathcal{C}$ over a ring R can be regarded as a group code. Define

$$\mathcal{C}_{0+} = \{\boldsymbol{v} \in \mathcal{C} | v_i = 0 \quad \forall i < 0\}$$

and

$$\mathcal{C}_{0-} = \{\boldsymbol{v} \in \mathcal{C} | v_i = 0 \quad \forall i \geq 0\}.$$

Then $\mathcal{C}_{0+}$ and $\mathcal{C}_{0-}$ are R-submodules of $\mathcal{C}$. The quotient R-module $\mathcal{C}/(\mathcal{C}_{0-} + \mathcal{C}_{0+})$ is called the *code state space* of $\mathcal{C}$ at time 0 [10].

In the case of convolutional codes over a field, a generator matrix is defined to be minimal when the abstract state space is of minimal dimension. It has been proved that this is fulfilled if and only if the abstract state space is isomorphic to the code state space [3], [11]. It is hence natural in the case of convolutional codes over a ring R to define a generator matrix to be *minimal* when this is fulfilled [3].

Surprisingly enough, there exist convolutional codes over rings which do not have a minimal generator matrix, e.g., the convolutional code over $\mathbb{Z}_4$ generated by $G(D) = (2 \quad 2 + D)$ [3].

III. Systematic Convolutional Codes over Rings

A convolutional generator matrix is said to be *systematic* if it causes the information symbols to appear unchanged among the code symbols, i.e., if some b of its columns form the identity matrix. Here a symbol means an element of $R(D)$.

Systematic rational generator matrices are of prime interest in connection with iterative decoding of convolutional codes [2]. The systematic bits seem to give a "leg up" in decoding. Also, it was recently shown that systematic polynomial generator matrices are superior to other types of generator matrices with list (M-algorithm) decoding of convolutional codes; they support a spontaneous recovery of a lost correct path [13].

For convolutional codes over fields, every code has both systematic and nonsystematic generator matrices. Thus in the field case, being systematic is an encoder property. However, this is not the case for codes over rings. In the ring case, being systematic is a code property [2]. Hence, we have

Definition 7: A convolutional code $\mathcal{C}$ over a ring R is *systematic* if it has a systematic generator matrix.

The following theorem states precisely when a convolutional code over a ring is systematic.

Theorem 6: A convolutional code $\mathcal{C}$ over a ring R is systematic if and only if it has a generator matrix $G(D)$ that has a $b \times b$ submatrix whose determinant is a unit in $R_r(D)$, the ring of realizable functions over R.

Proof: Assume that the generator matrix $G(D)$ is systematic, i.e., $G(D)$ can be written as $G(D) = (I_b\ G'(D))$. The determinant of I_b is a unit in R (and in $R_r(D)$). Conversely, assume that a generator matrix $G(D)$ has a $b \times b$ submatrix $A(D)$ whose determinant is a unit in $R_r(D)$. Without loss of essential generality, let $G(D) = (A(D)\ B(D))$. Then, $A(D)$ has an inverse $A^{-1}(D)$ over $R_r(D)$ and

$$G_{\text{sys}}(D) = A^{-1}(D)G(D) = (I_b\ B'(D))$$

is an equivalent generator matrix for the code $\mathcal{C}$. Hence, $\mathcal{C}$ has a systematic generator matrix. □

An element that is a unit in $R_r(D)$ is also a unit in $R(D)$. Thus Theorem 3 immediately implies

Corollary 7: Let $\mathcal{C}$ be a systematic convolutional code. Then $\mathcal{C}$ is right invertible.

It is not required that *every* generator matrix of a systematic code $\mathcal{C}$ has a $b \times b$ submatrix whose determinant is a unit in $R_r(D)$. For example, the determinant of the generator matrix $G'(D) = (D)$ in Example 2 is not a unit in $R_r(D)$, but the equivalent generator matrix $G(D) = (1)$ is trivially systematic and hence the code generated by $G'(D) = (D)$ is systematic. However, by combining Theorem 6 and Corollary 4 we obtain

Corollary 8: A generator matrix $G(D)$ that does not have a $b \times b$ submatrix whose determinant is a unit in $R(D)$, the ring of rational functions, cannot generate a systematic code.

The generator matrix $G(D) = (2 + D)$ over $\mathbb{Z}_4(D)$ in Example 1 generates a systematic code since it is equivalent to $G'(D) = (1)$, though it has no right inverse over $(\mathbb{Z}_4)_r(D)$. The generator matrix $G(D)$ over $\mathbb{Z}_6(D)$ in Example 3 has a right inverse over $\mathbb{Z}_6[D]$, but no 1×1 submatrix whose determinant is a unit of $\mathbb{Z}_6(D)$, so it generates a right invertible convolutional code $\mathcal{C}$ but $\mathcal{C}$ is not systematic.

IV. An Alternative Condition for Systematicity

Let $\mathcal{C}_0$ be the *start module* of a rate-b/c convolutional code $\mathcal{C}$ over a ring R; i.e., $\mathcal{C}_0$ consists of all c-tuples $\boldsymbol{v}(0)$ for which $\boldsymbol{v}(D)$ is a causal codeword in $\mathcal{C}$. Massey and Mittelholzer [2] defined a convolutional code $\mathcal{C}$ over a ring R to be *proper* if $\mathcal{C}_0$ is a free R-module of rank b and one can select b components such that the c-tuples in $\mathcal{C}_0$, when restricted to these components, form the free module R^b. Then they proved

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

We now prove the following result:

Theorem 9: Proposition 1 is equivalent to Theorem 6.

Proof: Assume that the code $\mathcal{C}$ has a generator matrix $G(D)$ that has a $b \times b$ submatrix whose determinant is a unit in $R_r(D)$. Without loss of essential generality, let $G(D) = (A(D) \;\; B(D))$ where $\det A(D)$ is a unit in $R_r(D)$. Then, $A(D)$ has an inverse $A^{-1}(D)$ over $R_r(D)$ and the matrix

$$G'(D) = A^{-1}(D)G(D) = (I_b \quad A^{-1}(D)B(D))$$

is an equivalent generator matrix of the code $\mathcal{C}$ which is systematic. The rows of $G'(0)$ are free over R and generate the start module. The c-tuples in $\mathcal{C}_0$, when restricted to the first b components, form the free module R^b. Hence, the code is proper.

Conversely, assume that the code $\mathcal{C}$ is proper. We can then find b causal codewords

$$\{\boldsymbol{v}_i(D) = (v_i^1(D) \cdots v_i^c(D)),\ 1 \le i \le b\}$$

such that $\{\boldsymbol{v}_i(0), 1 \le i \le b\}$ is a free basis of $\mathcal{C}_0$ and we can select b components of the codewords such that

$$\{\boldsymbol{v}'_i(0) = (v_i^{j_1}(0) \cdots v_i^{j_b}(0)),\ i = j_1, \cdots, j_b\}$$

form the free module R^b. Without loss of essential generality, we can take

$$\{\boldsymbol{v}'_i(D) = (v_i^1(D), \cdots, v_i^b(D)), 1 \le i \le b\}$$

and

$$\boldsymbol{v}'_i(0) = (0 \cdots 0\ 1\ 0\ \cdots\ 0)$$

where the 1 is in the ith position. We now want to show that the matrix

$$G(D) = \begin{pmatrix} \boldsymbol{v}_1(D) \\ \vdots \\ \boldsymbol{v}_b(D) \end{pmatrix}$$

is a generator matrix for the code $\mathcal{C}$. Consider any causal codeword $\boldsymbol{v}(D)$. Since $\{\boldsymbol{v}_i(0), 1 \le i \le b\}$ generates $\mathcal{C}_0$, there exists a $\boldsymbol{u}_0 \in R^b$ such that

$$\boldsymbol{v}(0) = \boldsymbol{u}_0 G(0)$$

and hence $\boldsymbol{v}(D) - \boldsymbol{u}_0 G(D)$ is a causal codeword with 0 constant term. We write $\boldsymbol{v}(D) - \boldsymbol{u}_0 G(D) = D\boldsymbol{v}'(D)$ where $\boldsymbol{v}'(D)$ is a causal codeword. There exists a $\boldsymbol{u}_1 \in R^b$ such that $\boldsymbol{v}'(0) = \boldsymbol{u}_1 G(0)$ and hence $\boldsymbol{v}(D) - (\boldsymbol{u}_0 + \boldsymbol{u}_1 D)G(D)$ is a causal codeword whose constant term and coefficient of D both are zero. Continuing in the same manner, we can find a sequence $\boldsymbol{u}(D) \in R[[D]]^b$ such that

$$\boldsymbol{v}(D) = \boldsymbol{u}(D)G(D).$$

Let $\boldsymbol{v}_b(D)$ and $G_b(D)$ denote the first b components of $\boldsymbol{v}(D)$ and the first b columns of the matrix $G(D)$, respectively. Then, $\boldsymbol{v}_b(D) = \boldsymbol{u}(D)G_b(D)$. The determinant $\det(G_b(D))$ is a causal rational function and $\det(G_b(0)) = 1$, i.e.,

$$\det(G_b(D)) = 1 + Dr(D)$$

where $r(D)$ is a causal rational function so that $\det(G_b(D))$ is a unit in $R_r(D)$. The sequence $\boldsymbol{u}(D)$ can then be expressed as

$$\boldsymbol{u}(D) = \boldsymbol{v}_b(D)G_b(D)^{-1}$$

which shows that $\boldsymbol{u}(D)$ is a b-tuple of rational functions. Moreover, every causal codeword in $\mathcal{C}$ can be generated by the matrix $G(D)$ and, since $\mathcal{C}$ is time-invariant, so can every codeword of $\mathcal{C}$. It has already been shown that the generator matrix $G(D)$ has a $b \times b$ submatrix whose determinant is a unit in $R_r(D)$ and hence, by Theorem 6, $\mathcal{C}$ is systematic. □

V. Convolutional Codes over $\mathbb{Z}_M$

In this section we mainly consider rate-b/c convolutional codes over rings $\mathbb{Z}_M$ where $M = p_1^{e_1} \cdots p_m^{e_m}$ and $p_1, \cdots, p_m$ are distinct primes. The ring $\mathbb{Z}_M$ is finite and can be decomposed into a direct sum of rings $\mathbb{Z}_M \simeq \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{e_m}}$. The results in this section reduce the study of generator matrices over $\mathbb{Z}_M$ to the study of generator matrices over $\mathbb{Z}_{p^e}$. Apart from the mere results, it simplifies the study of generator matrices, which is especially nice when working with concrete examples. We start more generally as follows.

Theorem 10: Suppose that the ring R can be decomposed into a direct sum of ideals as $R = R_1 \oplus R_2 \oplus \ldots \oplus R_s$. Then

i) the ring $R(D)$ of rational functions can be decomposed into a corresponding direct sum of rings of rational functions, i.e., $R(D) \simeq R_1(D) \oplus R_2(D) \oplus \cdots \oplus R_s(D)$;

ii) the ring $R_r(D)$ of realizable rational functions can be decomposed into a corresponding direct sum of rings of realizable rational functions, i.e.,

$$R_r(D) \simeq (R_1)_r(D) \oplus (R_2)_r(D) \oplus \cdots \oplus (R_s)_r(D);$$

iii) the ring $R[D]$ of polynomials can be decomposed into a corresponding direct sum of rings of polynomials, i.e., $R[D] \simeq R_1[D] \oplus R_2[D] \oplus \cdots \oplus R_s[D]$.

Proof:

i) The identity element of the ring $R(D)$ is the element $1 = 1/1$. We have the following decompositions $1 = e_1 \oplus \cdots \oplus e_s$ where e_i is the identity element of $R_i, i = 1, 2, \cdots, s$, and

$$R(D) = R(D)e_1 \oplus \cdots \oplus R(D)e_s.$$

It remains to prove that $R(D)e_i \simeq R_i(D)$. Define the map γ by

$$\begin{aligned} \gamma\colon \quad & R(D)e_i \to R_i(D) \\ & \frac{f(D)}{q(D)}e_i \mapsto \frac{f(D)e_i}{q(D)e_i} \end{aligned} \tag{7}$$

where

$$f(D)e_i = a_0e_i + a_1e_iD + \cdots + a_ne_iD^n$$

if

$$f(D) = a_0 + a_1D + \cdots + a_nD^n, a_i \in R.$$

The trailing coefficient of $q(D)$ is a unit in the ring R so, for all $i = 1, \cdots, s$, the trailing coefficient of $q(D)e_i$ is a unit in R_i, and hence

$$\frac{f(D)e_i}{q(D)e_i} \in R_i(D).$$

The map γ is well-defined; it preserves addition and multiplication and it is both injective and surjective. Hence, $R(D)e_i \simeq R_i(D)$ and $R(D) \simeq R_1(D) \oplus \cdots \oplus R_s(D)$.

ii) Following the proof of part i), for the ring $R_r(D)$ we have the decomposition

$$R_r(D) = R_r(D)e_1 \oplus \cdots \oplus R_r(D)e_s.$$

For

$$\frac{f(D)}{q(D)} \in R_r(D)$$

the element $q(0)$ is a unit in R so, for all $i = 1, \cdots, s$, the constant term of $q(D)e_i$ is a unit in R_i. Hence, we have $R_r(D)e_i \simeq (R_i)_r(D)$ and

$$R_r(D) \simeq (R_1)_r(D) \oplus \cdots \oplus (R_s)_r(D).$$

iii) Follows from the proof of part i). □

From Theorem 10 we have immediately

Theorem 11: Suppose that the ring R is a direct sum of ideals $R_1, R_2, \cdots, R_s$; i.e., $R = R_1 \oplus R_2 \oplus \cdots \oplus R_s$. Let $G(D)$ be a matrix over $R(D)$. Under the isomorphism

$$R(D) \simeq R_1(D) \oplus R_2(D) \oplus \cdots \oplus R_s(D)$$

denote the image of $G(D)$ in $R_i(D)$ by $G_i(D)$. We write symbolically

$$G(D) = G_1(D) \oplus G_2(D) \oplus \cdots \oplus G_s(D)$$

where $G_i(D)$ is a matrix over $R_i(D)$ for $i = 1, 2, \cdots, s$. Then

i) $G(D)$ is polynomial over $R[D]$ if and only if $G_i(D)$ is polynomial over $R_i[D]$ for $i = 1, 2, \cdots, s$;
ii) $G(D)$ is a generator matrix over $R_r(D)$ if and only if $G_i(D)$ is a generator matrix over $(R_i)_r(D)$ for $i = 1, 2, \cdots, s$;
iii) $G(D)$ has a right inverse over $R(D)$ (or over $R_r(D)$ or over $R[D]$) if and only if $G_i(D)$ has a right inverse over $R_i(D)$ (or over $(R_i)_r(D)$ or over $R_i[D]$) for $i = 1, 2, \cdots, s$.

From Theorem 11 follows

Theorem 12: Suppose that the ring R is a direct sum of ideals $R_1, R_2, \cdots, R_s$; i.e., $R = R_1 \oplus R_2 \oplus \cdots \oplus R_s$ and that a generator matrix $G(D)$ over $R(D)$ has been decomposed into

$$G(D) = G_1(D) \oplus G_2(D) \oplus \cdots \oplus G_s(D).$$

Then

i) $G(D)$ is basic if and only if $G_i(D)$ is basic for $i = 1, 2, \cdots, s$;
ii) $G(D)$ is noncatastrophic if and only if $G_i(D)$ is noncatastrophic for $i = 1, 2, \cdots, s$;
iii) $G(D)$ is minimal if and only if $G_i(D)$ is minimal for $i = 1, 2, \cdots, s$.

Proof:

i) and ii) are obvious; iii) follows from the facts that the abstract state space of $\mathcal{C}$ relative to $G(D)$ is a direct sum of abstract state spaces of $\mathcal{C}_i$ relative to $G_i(D)$ for $i = 1, 2, \cdots, s$ and that the code state space of $\mathcal{C}$ at time 0 is isomorphic to the direct sum of code state spaces of $\mathcal{C}_i$ for $i = 1, 2, \cdots, s$. □

For a generator matrix that can be decomposed into a direct sum, we have the following

Theorem 13: Suppose that the ring R can be decomposed into a direct sum of ideals, $R = R_1 \oplus R_2 \oplus \cdots \oplus R_s$. If a generator matrix

$$G(D) = G_1(D) \oplus G_2(D) \oplus \cdots \oplus G_s(D)$$

of a convolutional code over R is systematic, then $G_i(D)$ is also systematic for $i = 1, 2, \cdots, s$.

Proof: If the generator matrix

$$G(D) = G_1(D) \oplus G_2(D) \oplus \cdots \oplus G_s(D)$$

has a $b \times b$ submatrix whose determinant is a unit in $R_r(D)$, then, since $R(D)$ is a direct sum, $G_i(D)$ must have a $b \times b$ submatrix whose determinant is a unit in $(R_i)_r(D)$ for $i = 1, 2, \cdots, s$. □

The following example shows that the converse of Theorem 13 does not hold.

Example 4: The generator matrices $G_1(D) = (2 \quad 0)$ and $G_2(D) = (0 \quad 3)$ over $\mathbb{Z}_3$ and $\mathbb{Z}_2$, respectively, are both systematic. However, the generator matrix

$$G(D) = G_1(D) \oplus G_2(D) = (2 \quad 3)$$

does not have a $b \times b$ submatrix whose determinant is a unit in $R(D)$ (see Example 3), so that the convolutional code generated by $G(D)$ is not systematic.

Remark: Note that Theorem 13 implies that if a convolutional code $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \cdots \oplus \mathcal{C}_s$ over R is systematic, then $\mathcal{C}_i$ is systematic for $i = 1, 2, \cdots, s$.

Now, if $G(D)$ is a generator matrix over $\mathbb{Z}_M$, then

$$G(D) = G_1(D) \oplus G_2(D) \cdots \oplus G_m(D)$$

where

$$G_i(D) = G(D) \bmod p_i^{e_i}, 1 \le i \le m.$$

By the foregoing discussion, the study of codes over $\mathbb{Z}_M$ can be reduced to the study of codes over $\mathbb{Z}_{p^e}$. This follows also from the fundamental theorem of finite Abelian groups as was already pointed out in [14], cf. also [15]–[19].

Consider a generator matrix $G(D)$ over $\mathbb{Z}_{p^e}$. We can write

$$G(D) = G_0(D) + G_1(D)p + \cdots + G_{e-1}(D)p^{e-1}$$

where the entries of all $G_i(D)$ are over $(\mathbb{Z}_p)_r(D)$. Then, $G(D) \bmod p = G_0(D)$. The relation between the generator matrix $G(D)$ and $G(D) \bmod p$ will be studied next.

Theorem 14: Let $G(D)$ be a generator matrix over $\mathbb{Z}_{p^e}$. Then

i) $G(D)$ is catastrophic if $G(D) \bmod p$ is catastrophic and, for polynomial generator matrices, only if $G(D) \bmod p$ is catastrophic.

ii) Assuming that $G(D)$ is polynomial, $G(D)$ is basic if and only if $G(D) \bmod p$ is basic.

Proof:

i) Assume that $G(D) \bmod p = G_0(D)$ is catastrophic. Then we can find an input sequence $\boldsymbol{u}(D)$ which has infinite weight and where every $u_i \in \mathbb{Z}_p^b$, such that $\boldsymbol{u}(D)G_0(D)$ has finite weight. Then $\boldsymbol{u}(D)p^{e-1}$ also has infinite weight and

$$\begin{aligned}\boldsymbol{u}(D)p^{e-1}G(D) &= \boldsymbol{u}(D)p^{e-1}(G_0(D) \\ &\qquad + G_1(D)p + \cdots + G_{e-1}(D)p^{e-1}) \\ &= \boldsymbol{u}(D)p^{e-1}G_0(D).\end{aligned}$$

This shows that $\boldsymbol{u}(D)p^{e-1}G(D)$ also has finite weight and hence that $G(D)$ is catastrophic.

To prove the converse part when $G(D)$ is polynomial, suppose that $G(D)$ is catastrophic. Then there exists an information sequence $\boldsymbol{u}(D)$ with infinite weight such that $\boldsymbol{u}(D)G(D)$ has finite weight. We can write

$$\boldsymbol{u}(D) = \boldsymbol{u}_0(D) + \boldsymbol{u}_1(D)p + \cdots + \boldsymbol{u}_{e-1}(D)p^{e-1}$$

where each $\boldsymbol{u}_i(D)$ belongs to $\mathbb{Z}_p(D)^b$. Then at least one $\boldsymbol{u}_i(D)$ has infinite weight. Suppose that

$$\boldsymbol{u}_0(D), \boldsymbol{u}_1(D), \cdots, \boldsymbol{u}_{j-1}(D) \qquad (1 \le j \le e)$$

have finite weight and $\boldsymbol{u}_j(D)$ has infinite weight. Then

$$\begin{aligned}\boldsymbol{u}(D)G(D) &= (\boldsymbol{u}_0(D) + \boldsymbol{u}_1(D)p + \cdots + \boldsymbol{u}_{e-1}(D)p^{e-1}) \\ &\qquad \cdot (G_0(D) + G_1(D)p + \cdots + G_{e-1}(D)p^{e-1}) \\ &= \boldsymbol{u}_0(D)G_0(D) + (\boldsymbol{u}_0(D)G_1(D) \\ &\quad + \boldsymbol{u}_1(D)G_0(D))p + \cdots \\ &\quad + (\boldsymbol{u}_0(D)G_{e-1}(D) + \boldsymbol{u}_1(D)G_{e-2}(D) + \cdots \\ &\quad + \boldsymbol{u}_{e-1}(D)G_0(D))p^{e-1}\end{aligned}$$

has finite weight and the coefficients of $p^0, p^1, \cdots, p^{e-1}$ all have finite weight. In particular, the coefficient of p^j, which is

$$\boldsymbol{u}_0(D)G_j(D) + \boldsymbol{u}_1(D)G_{j-1}(D) + \cdots + \boldsymbol{u}_j(D)G_0(D),$$

has finite weight. Since $G(D)$ is polynomial,

$$\boldsymbol{u}_0(D)G_j(D), \boldsymbol{u}_1(D)G_{j-1}(D), \cdots, \boldsymbol{u}_{j-1}(D)G_1(D)$$

all have finite weight. Hence, $\boldsymbol{u}_j(D)G_0(D)$ has finite weight showing that $G_0(D)$ is catastrophic.

ii) If $G(D)$ is basic, then there exists a polynomial matrix $G^{-1}(D)$ such that $G(D)G^{-1}(D) = I_b$ where I_b is the $b \times b$ identity matrix. We can write

$$G^{-1}(D) = G_0^{-1}(D) + G_1^{-1}(D)p + \cdots + G_{e-1}^{-1}(D)p^{e-1}$$

where $G_i^{-1}(D)$ is polynomial, $0 \le i \le e-1$. Then

$$\begin{aligned}&(G_0(D) + G_1(D)p + \cdots + G_{e-1}(D)p^{e-1}) \\ &\qquad \cdot (G_0^{-1}(D) + G_1^{-1}(D)p + \cdots + G_{e-1}^{-1}(D)p^{e-1}) = I_b\end{aligned}$$

which shows that

$$G_0(D)G_0^{-1}(D) = I_b.$$

Thus $G_0(D) = G(D) \bmod p$ has a right polynomial inverse and hence is basic.

Conversely, assume that $G_0(D)$ is basic. Then there exists a $c \times b$ polynomial matrix $G_0^{-1}(D)$ over $\mathbb{Z}_p$ such that

$$G_0(D)G_0^{-1}(D) = I_b \bmod p.$$

We will construct $c \times b$ polynomial matrices $G_1^{-1}(D), \cdots, G_{e-1}^{-1}(D)$ such that $G(D)G^{-1}(D) = I_b$ where

$$G^{-1}(D) = G_0^{-1}(D) + G_1^{-1}(D)p + \cdots + G_{e-1}^{-1}(D)p^{e-1}.$$

Consider the product

$$\begin{aligned}G(D)G^{-1}(D) &= (G_0(D) + G_1(D)p + \cdots + G_{e-1}(D)p^{e-1}) \\ &\qquad \cdot (G_0^{-1}(D) + G_1^{-1}(D)p + \cdots + G_{e-1}^{-1}(D)p^{e-1}) \\ &= G_0(D)G_0^{-1}(D) + (G_0(D)G_1^{-1}(D) \\ &\quad + G_1(D)G_0^{-1}(D))p + \cdots \\ &\quad + (G_0(D)G_{e-1}^{-1}(D) + G_1(D)G_{e-2}^{-1}(D) + \cdots \\ &\quad + G_{e-1}(D)G_0^{-1}(D))p^{e-1}\end{aligned}$$

where the operations are done modulo p^e. We have

$$G_0(D)G_0^{-1}(D) = I_b$$

in $\mathbb{Z}_p$.We can assume that

$$G_0(D)G_0^{-1}(D) = I_b + pK_1(D) + p^2K_2(D) + \cdots + p^{e-1}K_{e-1}(D)$$

in $\mathbb{Z}_{p^e}$. Then

$$\begin{aligned}G(D)G^{-1}(D) &= I_b + (K_1(D) + G_0(D)G_1^{-1}(D) \\ &\quad + G_1(D)G_0^{-1}(D))p + \cdots \\ &\quad + (K_{e-1}(D) + G_0(D)G_{e-1}^{-1}(D) \\ &\quad + G_1(D)G_{e-2}^{-1}(D) + \cdots \\ &\quad + G_{e-1}(D)G_0^{-1}(D))p^{e-1}\end{aligned}$$

and we can choose

$$G_1^{-1}(D) = -G_0^{-1}(D)(K_1(D) + G_1(D)G_0^{-1}(D))$$

where the operations are done modulo p. Clearly, $G_1^{-1}(D)$ is polynomial and

$$K_1(D) + G_0(D)G_1^{-1}(D) + G_1(D)G_0^{-1}(D) = 0$$

in $\mathbb{Z}_p$. We can assume that

$$\begin{aligned}&K_1(D) + G_0(D)G_1^{-1}(D) + G_1(D)G_0^{-1}(D) \\ &\qquad = pL_1(D) + p^2L_2(D) + \cdots + p^{e-1}L_{e-1}(D)\end{aligned}$$

in $\mathbb{Z}_{p^e}$. Then

$$\begin{aligned}G(D)G^{-1}(D) &= I_b + 0p + (K_2(D) + L_1(D) \\ &\quad + G_0(D)G_2^{-1}(D) + G_1(D)G_1^{-1}(D) \\ &\quad + G_2(D)G_0^{-1}(D))p^2 + \cdots \\ &\quad + (K_{e-1}(D) + L_{e-2}(D) \\ &\quad + G_0(D)G_{e-1}^{-1}(D) \\ &\quad + G_1(D)G_{e-2}^{-1}(D) + \cdots \\ &\quad + G_{e-1}(D)G_0^{-1}(D))p^{e-1}\end{aligned}$$

and we can choose

$$\begin{aligned}G_2^{-1}(D) &= -G_0^{-1}(D)(K_2(D) + L_1(D) + G_0(D)G_2^{-1}(D) \\ &\qquad + G_1(D)G_1^{-1}(D) + G_2(D)G_0^{-1}(D))\end{aligned}$$

where the operations are done modulo p. Then $G_2^{-1}(D)$ is polynomial and the coefficient of p^2 in $G(D)G^{-1}(D)$ is 0. Continuing in the same way, we can choose polynomial matrices $G_i^{-1}(D), 1 \le i \le$

$e-1$, in such a way that $G(D)G^{-1}(D)=I_b$. Thus $G(D)$ has a polynomial inverse and is basic. □

Theorem 14 i) implies that, for a polynomial generator matrix $G(D)$ over $\mathbb{Z}_{p^e}$, $G(D)$ is catastrophic if and only if $G(D) \bmod p$ is catastrophic, which was pointed out by Massey and Mittelholzer in [1]. The following example shows that for a nonpolynomial generator matrix $G(D)$ over $\mathbb{Z}_{p^e}$, the catastrophicity of $G(D)$ does not imply catastrophicity of $G(D) \bmod p$.

Example 5: Let $\mathcal{C}$ be a convolutional code over the ring $\mathbb{Z}_{p^2}$ generated by $G(D)=1+(1/(1-D))p$. The infinite weight input sequence

$$u(D)=(1-D)\left(1+\frac{D}{1+p}+\left(\frac{D}{1+p}\right)^2+\left(\frac{D}{1+p}\right)^3+\cdots\right)$$

gives a finite weight output $u(D)G(D)=1+p$ and hence the generator matrix is catastrophic. However, $G(D) \bmod p=(1)$ is noncatastrophic over $\mathbb{Z}_p$.

The following result on systematicity of codes over the ring $\mathbb{Z}_{p^m}$ was stated by Mittelholzer in 1993 [3] and can be proved in the same way as Theorem 14.

Theorem 15: A convolutional code $\mathcal{C}$ is systematic if and only if it has a generator matrix $G(D)$ such that $G(0) \bmod p$ has full rank over $\mathbb{Z}_p$.

There is no correspondingly simple relation between the minimality of the generator matrix $G(D)$ and that of $G(D) \bmod p$. An example is given here of a generator matrix which is not minimal over the ring $\mathbb{Z}_{p^e}$ but is minimal over $\mathbb{Z}_p$.

Example 6: Consider the polynomial generator matrix $G(D)=(1+pD)$ over $\mathbb{Z}_{p^2}$. This generator matrix is not minimal since $G(D)$ is equivalent to the generator matrix $G'(D)=(1)$. However, $G(D) \bmod p=(1)$ is minimal over $\mathbb{Z}_p$.

VI. Comment

For fields we usually define convolutional codes for inputs that are Laurent series, but for general rings we have to restrict the inputs to be rational functions. However, when considering rings satisfying the descending chain condition we could allow Laurent series as inputs. Even for these rings many important properties differ from the field case.

Acknowledgment

Comments on the manuscript by G. D. Forney, Jr., J. L. Massey, and T. Mittelholzer are gratefully acknowledged.

References

[1] J. L. Massey and T. Mittelholzer, "Convolutional codes over rings," in *Proc. 4th Joint Swedish–Soviet Int. Workshop Information Theory* (Gotland, Sweden, Aug. 27–Sept. 1, 1989), pp. 14–18.

[2] ——, "Systematicity and rotational invariance of convolutional codes over rings," in *Proc. 2nd Int. Workshop Algebraic and Combinatorial Coding Theory* (Leningrad, USSR, Sept. 16–22, 1990), pp. 154–158.

[3] T. Mittelholzer, "Minimal encoders for convolutional codes over rings," in *Communications Theory and Applications*. HW Comm. Ltd., 1993, pp. 30–36.

[4] G. D. Forney, Jr., "Convolutional codes I: Algebraic structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720–738, 1970.

[5] R. Johannesson and Z.-x. Wan, "A linear algebra approach to minimal convolutional encoders," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1219–1233, 1993.

[6] J. L. Massey, "Coding theory," in *Handbook of Applied Mathematics*, W. Ledermann, Ed., vol. V, pt. B, *Combinatorics and Geometry*, W. Ledermann and S. Vajda, Eds. Chichester and New York: Wiley, 1985, ch. 16.

[7] T. Mittelholzer, "Convolutional codes over rings and the two chain conditions," in *Proc. IEEE Int. Symp. Information Theory* (Ulm, Germany, June 29–July 4, 1997), p. 285.

[8] H.-A. Loeliger, G. D. Forney, Jr., T. Mittelholzer, and M. D. Trott, "Minimality and observability of group systems," *Linear Algebra and Its Applications*, vol. 205–206, pp. 937–963, July 1994.

[9] G. D. Forney Jr., private communication, Aug. 21, 1997.

[10] G. D. Forney, Jr., and M. D. Trott, "The dynamics of group codes: State spaces, trellis diagrams and canonical encoders," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1491–1513, 1993.

[11] E. Wittenmark and Z.-x. Wan, "Convolutional codes from a dynamical system point of view," in *Proc. 1994 IEEE Int. Symp. Information Theory* (Trondheim, Norway, June 27–July 1, 1994), p. 160.

[12] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes (1)," in *Proc., IEEE Int. Conf. Communications* (Geneva, Switzerland, May 1993), pp. 1064–1070.

[13] H. Osthoff, J. B. Anderson, R. Johannesson, and C.-f. Lin, "Systematic feed-forward convolutional encoders are better than other encoders with an M-algorithm decoder," this issue, pp. 831–838.

[14] I. Ingemarsson, "Commutative group codes for the Gaussian channel," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 215–219, 1973.

[15] C.-J. Chen, T.-Y. Chen and H.-A. Loeliger, "Construction of linear ring codes for 6-PSK," *IEEE Trans. Inform. Theory*, vol. 40, pp. 563–566, 1994.

[16] G. Caire and E. Biglieri, "Linear block codes over cyclic groups," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1246–1256, 1995.

[17] H.-A. Loeliger and T. Mittelholzer, "Convolutional codes over groups," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1660–1686, 1996.

[18] V. V. Vazirani, H. Saran, and B. S. Rajan, "An efficient algorithm for constructing minimal trellises for codes over finite Abelian groups," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1839–1854, 1996.

[19] F. Fagnini and S. Zampieri, "Dynamical systems and convolutional codes over finite abelian groups," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1892–1912, 1996.