UEP-Optimal Convolutional Encoders with Smallest McMillan Degree

Chung-Hsuan Wang, Wei-Fan Wu, and Jian-Jia Weng
Department of Electrical Engineering, National Chiao Tung University
Hsinchu, Taiwan 30010, R.O.C.
Email: chwang@mail.nctu.edu.tw

***Abstract*—In this paper, convolutional encoders are studied for unequal error protection (UEP) from an algebraic theoretical viewpoint. Given any convolutional code, UEP-optimal encoders with the smallest McMillan degree are constructed to minimize the coding complexity. The noncatastrophic property of encoder is also maintained to avoid the undesired catastrophic propagation of decoding errors.**

I. Introduction

Convolutional codes are conventionally used for equal error protection (EEP). In that case, free distance defined as the minimum weight of nonzero codewords is unarguably an effective parameter for performance evaluation. For a generator matrix of a convolutional code, the external degree and the McMillan degree correspond to the numbers of delay elements in its direct-form encoder and minimal encoder, respectively. Since every generator matrix of a convlutional code contributes the same amount of free distance, canonical and minimal generator matrices which have the minimal external degree and the minimal McMillan degree among all generator matrices, respectively, are desirable for encoding to minimize the complexity of building the encoder and conducting the Viterbi decoding algorithm.

Recent research shows that (n, k) convolutional codes with $k>1$ may possess the intrinsic capability of unequal error protection (UEP) [1]–[9]. Among those studies, the separation vector, originally defined for block codes in [10], has been verified to be an effective UEP measurement for convolutional codes. Different from the case of EEP, generator matrices of a convolutional code may have distinct separation vectors and hence different UEP capabilities. In [6], it was shown that for every convolutional code there exists at least one optimal generator matrix which has the greatest separation vector among all generator matrices. However, counter-examples were also given to demonstrate that in general there may not exist an optimal generator matrix which is canonical or minimal to minimize the coding complexity.

To reduce the coding complexity but still keep the UEP optimality, the generator matrices with the smallest external degree among all optimal ones were constructed in [7]. However, such a generator matrix does not guarantee the minimal complexity unless it happens to be with the smallest McMillan degree. In this paper, we focus on minimizing the McMillan degree of an optimal generator matrix instead of the external degree. Properties of the degrees of generator matrices are further investigated from an algebraic viewpoint. Based on the derived results, procedures are provided to obtain an optimal generator matrix which achieves the smallest McMillan degree among all optimal ones and is also noncatastrophic to avoid the undesired propagation of decoding errors.

The rest of this paper is organized as follows. Section II briefly introduces the algebraic theory of convolutional codes. Some previous results about UEP convolutional encoders are described in Section III. Optimal generator matrices with the smallest McMillan degree are investigated in Section IV. Finally, Section V concludes this work.

II. A Brief Review of the Algebraic Theory of Convolutional Codes

We begin with a review of the terms and definitions used in the algebraic theory of convolutional codes [11]. Let F be a finite field and $F((D))$ be a field consisting of all one-sided formal Laurent series of the form $\sum_{i\geq m} a_i D^i$ with the indeterminate D, where $a_i \in F$ for all i and m can be any integer. The set of all polynomials over F is denoted by $F[D]$. Every rational function $p(D)/q(D)$, where $p(D), q(D) \in F[D]$ and $q(D) \neq 0$, has a unique Laurent series expansion and is called a rational Laurent series. The rational subfield of $F((D))$ consists of all rational Laurent series and is denoted by $F(D)$.

An (n, k) convolutional code C over F can be defined as a k-dimensional subspace of $F(D)^n$. A generator matrix $G(D)$ for C is a $k \times n$ matrix over $F(D)$ whose rows $\boldsymbol{g}_1(D), \boldsymbol{g}_2(D), \cdots, \boldsymbol{g}_k(D)$ form a basis for C. Every codeword $\boldsymbol{c}(D)$ is encoded by $\boldsymbol{c}(D) = \boldsymbol{I}(D)G(D)$, where $\boldsymbol{I}(D)$ = $(I_1(D), I_2(D), \cdots, I_k(D)) \in F(D)^k$. If all the entries of $G(D)$ are in $F[D]$, then $G(D)$ is called a polynomial generator matrix (PGM). Following the definitions in [11], we define the internal and external degrees of a PGM by the maximum degree of its $k \times k$ minors* and the sum of its row degrees, respectively. Let the degree of a convolutional encoder be the number of delay elements in the encoder. The external degree of a PGM corresponds to the degree of its direct-form or controller canonical form encoder. Given a generator matrix $G(D)$ (in general over $F(D)$), its McMillan degree is defined as the minimum degree of all possible encoders of $G(D)$;

*For a $k \times n$ matrix $G(D)$, a $k \times k$ minor of $G(D)$ is the determinant of a $k \times k$ submatrix of $G(D)$.

this quantity is commensurate to the minimum complexity for realizing the encoder and decoder of $G(D)$. Decompose $G(D)$ into the following invariant form over $F(D^{-1})$: [12]

$$G(D) = V(D^{-1})\Lambda(D^{-1})W(D^{-1})$$

where $V(D^{-1})$ is a $k \times k$ unimodular matrix, $W(D^{-1})$ is an $n \times n$ unimodular matrix, and $\Lambda(D^{-1})$ is of the form

$$\begin{pmatrix} \lambda_1(D^{-1}) & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2(D^{-1}) & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k(D^{-1}) & 0 & \cdots & 0 \end{pmatrix}$$

with the invariant factors $\lambda_i(D^{-1})$'s. By expressing $\lambda_i(D^{-1})$ in the form of $a_i(D^{-1})/b_i(D^{-1})$, where $a_i(D^{-1})$ and $b_i(D^{-1})$ are polynomials in D^{-1} which are relatively prime, it follows that

$$a_i(D^{-1}) | a_{i+1}(D^{-1}) \quad \text{and} \quad b_{i+1}(D^{-1}) | b_i(D^{-1}) \qquad (1)$$

$\forall\ 1 \le i < k$. The McMillan degree of $G(D)$ can then be obtained by the sum of the degrees of $b_i(D^{-1})$'s, $\forall\ i$ [12]. In general, for any PGM, we have the following inequality for the degrees defined above: [11]

$$\text{internal degree} \le \text{McMillan degree} \le \text{external degree}.$$

Given a convolutional code, a PGM is called basic if it has the smallest internal degree among all PGMs. If a PGM has the smallest external degree it is called canonical. The degree of a code is defined as the minimal external degree of all its PGMs, which is always the same as the minimal internal degree [11]. Suppose the McMillan degree of a generator matrix is equal to the degree of the code. Such a generator matrix is called minimal. In addition, there exist a class of catastrophic generator matrices [11] for which an infinite-weight $\boldsymbol{I}(D)$ can be encoded as a finite-weight $\boldsymbol{c}(D)$. If a catastrophic generator matrix is used for encoding, a finite number of channel errors can cause an infinite number of decoding errors; this should be avoided at all costs. Basic, canonical, and minimal generator matrices are also noncatastrophic as clarified in [11], [12].

III. Convolutional Encoders for UEP

Similar to the free distance, the UEP capability of a convolutional encoder can be described by the separation vector, originally defined for block codes in [10], or called the free input-distance in [8], defined below.

Definition 1: For an (n, k) convolutional code C over F, denote by $\boldsymbol{s}(G(D)) = (s(G(D))_1, s(G(D))_2, \cdots, s(G(D))_k)$ the separation vector with respect to the generator matrix $G(D)$ for C, where $s(G(D))_i$ is defined as the minimal weight of codewords with nonzero $I_i(D)$, $\forall\ 1 \le i \le k$, and $\boldsymbol{I}(D) = (I_1(D), I_2(D), \ldots, I_k(D))$ stands for the vector of the Laurent series of the input information bits.

By this definition, a large value of $s(G(D))_i$ implies a small BER for the information sequence $I_i(D)$ fed into the ith input of the encoder at high signal-to-noise ratios [4], [5]. The minimum of $s(G(D))_i$'s is then the free distance of the code.

Given a convolutional code, there may exist generator matrices with different separation vectors. For two vectors of real numbers $\boldsymbol{a} = (a_1, a_2, \cdots, a_k)$ and $\boldsymbol{b} = (b_1, b_2, \cdots, b_k)$, define $\boldsymbol{a} \ge \boldsymbol{b}$ if and only if $a_i \ge b_i$, $\forall\ i$. In [6], it has been shown that for every code there always exists an optimal generator matrix which has the greatest separation vector and hence the best UEP capability among all generator matrices. Based on the effectively lower-triangular matrices defined below, Theorem 1 regulates the legitimate transformation between optimal generator matrices.

Definition 2: [7] Let G(D) be a generator matrix of an (n, k) convolutional code. Without loss of generality, assume $\boldsymbol{s}(G(D))$ is in the nondecreasing order, i.e., $s(G(D))_l \le s(G(D))_{l+1}$ $\forall\ 1 \le l < k$, and has α different component values, each with β_i repetitions $\forall\ 1 \le i \le \alpha$. For a $k \times k$ matrix $T(D)$ over $F(D)$, let $t_{u,v}(D)$ be the entry in position (u,v) of $T(D)$, $\forall\ 1 \le u, v \le k$. $T(D)$ is called effectively lower-triangular with respect to $G(D)$ if and only if $t_{u,v}(D) = 0$, $\forall\ \sum_{l=1}^{i-1} \beta_l < u \le \sum_{l=1}^{i} \beta_l$, $v > \sum_{l=1}^{i} \beta_l$, and $1 \le i \le \alpha$.

Theorem 1: [7] Given an (n, k) convolutional code C, let $G(D)$ be an optimal generator matrix of nondecreasing separation vector. For any $k \times k$ nonsingular matrix $T(D)$ over $F(D)$, $T(D)G(D)$ is optimal if and only if $T(D)$ is effectively lower-triangular with respect to $G(D)$.

By Theorem 1, an optimal generator matrix can always been transformed into a basic PGM without sacrificing its UEP optimality [6]. To further reduce the complexity, a procedure was presented in [7] to construct an optimal and basic PGM which has the smallest external degree among all optimal ones.

IV. Reduction of McMillan Degrees for Optimal Generator Matrices

Given a convolutional code, although we can obtain an optimal and basic generator matrix which provides the smallest external degree as demonstrated in [7], such a generator matrix does not guarantee the minimal complexity. For example, consider a binary convolutional code with the following generator matrix of the fewest external degree among all optimal and basic PGMs:

$$G_1(D) = \begin{pmatrix} 1 & 0 & 0 & D^4 \\ 0 & 1 & 1+D^2 & 0 \\ 0 & 0 & 1 & 1+D \end{pmatrix}$$

which has $\boldsymbol{s}(G_1(D)) = (2, 3, 3)$ and the external degree 7. Following the discussion in Section II, we have the invarint factors of $G_1(D)$: $\frac{1}{(D^{-1})^4}$, $\frac{1}{(D^{-1})^2}$, $\frac{(D^{-1})^2}{(D^{-1})^0}$. The McMillan degree is hence 6. However, there exists another optimal and noncatastrophic generator matrix

$$G_2(D) = \begin{pmatrix} 1 & 0 & 0 & D^4 \\ 0 & 1 & 0 & 1+D+D^2+D^3 \\ 0 & 0 & 1 & 1+D \end{pmatrix}$$

with external degree 8 but McMillan degree 4. (Invarint factors of $G_2(D)$ are $\frac{1}{(D^{-1})^4}$, $\frac{1}{(D^{-1})^0}$, $\frac{1}{(D^{-1})^0}$.) $G_2(D)$ can thus be

realized with less complexity than $G_1(D)$ even though it has a greater external degree.

To minimize the McMillan degree of an optimal generator matrix, we first provide some useful properties below.

Lemma 1: Given N polynomials $f_1(D)$, $f_2(D)$, ..., $f_N(D)$ over finite field F, denote by GCD($f_1(D)$, $f_2(D)$, ..., $f_N(D)$) the greatest common divisor of $f_1(D)$, $f_2(D)$, ..., $f_N(D)$. Rewrite $f_i(D)$ into the form of $D^{\omega_i} f_i^*(D)$ where $f_i^*(D)$ is a delay-free polynomial with nonzero constant term, $\forall\, 1 \le i \le N$. Denote by $\deg(\cdot)$ the operator taking the degree of a polynomial. Let $\phi = \max_i \deg(f_i(D))$, $\omega = \min_i \omega_i$, and $\eta = \min_i \deg(f_i^*(D))$. For any integer $m \ge \phi$, we have that the greatest common divisor of $D^{-m} f_1(D)$, $D^{-m} f_2(D)$, ..., $D^{-m} f_N(D)$ (which are now in $F[D^{-1}]$) is

$$D^{-(m-\phi+\eta+\omega)} GCD(f_1(D), f_2(D), \cdots, f_N(D)). \quad (2)$$

Proof:

Since $f_i(D) = D^{\omega_i} f_i^*(D)$, $\forall\, 1 \le i \le N$, it implies that

$$\begin{aligned} & \mathrm{GCD}(f_1^*(D), f_2^*(D), \cdots, f_N^*(D)) \\ = \;& D^{-\omega}\mathrm{GCD}(f_1(D), f_2(D), \cdots, f_N(D)). \end{aligned} \quad (3)$$

Hence, for any $m \ge \phi$, we have

$$\begin{aligned} D^{-m} f_i(D) &= D^{-m} D^{\omega_i} f_i^*(D) \\ &= D^{-(m-\omega_i-\deg(f_i^*(D)))}(D^{-\deg(f_i^*(D))} f_i^*(D)) \\ &= D^{-(m-\deg(f_i(D)))}(D^{-\deg(f_i^*(D))} f_i^*(D)) \end{aligned} \quad (4)$$

$\forall\, 1 \le i \le N$. Since $f_1^*(D), f_2^*(D), \ldots, f_N^*(D)$ are delay-free polynomials, it follows that

$$\begin{aligned} & \mathrm{GCD}(D^{-\deg(f_1^*(D))} f_1^*(D), \cdots, D^{-\deg(f_N^*(D))} f_N^*(D)) \\ = \;& D^{-\eta}\mathrm{GCD}(f_1^*(D), f_2^*(D), \cdots, f_N^*(D)) \\ = \;& D^{-(\eta+\omega)}\mathrm{GCD}(f_1(D), f_2(D), \cdots, f_N(D)). \end{aligned} \quad (5)$$

By (4) and (5), we have

$$\begin{aligned} & \mathrm{GCD}(D^{-m} f_1(D), D^{-m} f_2(D), \ldots, D^{-m} f_N(D)) \\ = \;& D^{-(m-\phi)}\mathrm{GCD}(D^{-\deg(f_1^*(D))} f_1^*(D), \cdots, D^{-\deg(f_N^*(D))} f_N^*(D)) \\ = \;& D^{-(m-\phi+\eta+\omega)}\mathrm{GCD}(f_1(D), f_2(D), \cdots, f_N(D)) \end{aligned}$$

hence completing the proof. ∎

Example 1: Consider $f_1(D) = D^2 + D^3 + D^5$, $f_2(D) = D^3 + D^4 + D^6$, and $f_3(D) = D^3 + D^5 + D^6 + D^7$, which can be rewritten into the forms of $f_1(D) = D^2(1 + D + D^3)$, $f_2(D) = D^3(1 + D + D^3)$, and $f_3(D) = D^3(1 + D)(1 + D + D^3)$. In this case, we have $\phi = 7$, $\omega = 2$, $\eta = 3$, and $\mathrm{GCD}(f_1(D), f_2(D), f_3(D)) = D^2 + D^3 + D^5$. For an integer $m \ge 7$, say $m = 8$, a direct computation shows

$$\begin{aligned} & \mathrm{GCD}(D^{-8} f_1(D), D^{-8} f_2(D), D^{-8} f_3(D)) \\ = \;& D^{-1} + D^{-3} + D^{-4}. \end{aligned} \quad (6)$$

By (2), it follows that

$$\begin{aligned} & D^{-(m-\phi+\eta+\omega)}\mathrm{GCD}(f_1(D), f_2(D), f_3(D)) \\ = \;& D^{-6}(D^2 + D^3 + D^5) \end{aligned}$$

which is exactly the same as (6). ∎

Lemma 1 can then be employed for the calculation of invariant factors as described below.

Theorem 2: Consider a PGM $G(D)$ of an (n, k) convolutional code over finite field F. Let m_i be the maximum degree of $i \times i$ minors of $G(D)$, $\forall\, 1 \le i \le k$, and set $m_0 = 0$. Denote by $\lambda_i(D)$ the ith invariant factor of $G(D)$ over $F(D)$, $\forall\, 1 \le i \le k$. Suppose $G(D)$ is now decomposed into the invariant form over $F(D^{-1})$. The corresponding invariant factors can be obtained by

$$\frac{D^{-\deg(\lambda_i(D))}\lambda_i(D)}{D^{-(m_i-m_{i-1})}},\ \forall\, 1 \le i \le k. \quad (7)$$

Proof:

Denote by $\Delta_i(D)$ the greatest common divisor of all $i \times i$ minors $f_{i,1}(D)$, $f_{i,2}(D)$, $\cdots$, $f_{i,N_i}(D)$ of $G(D)$, where N_i stands for the number of $i \times i$ minors, $\forall\, 1 \le i \le k$. We have $m_i = \max_l \deg(f_{i,l}(D))$, $\forall\, i$. Set $\Delta_0(D) = 1$. It follows that $\lambda_i(D) = \Delta_i(D)/\Delta_{i-1}(D)$ [11], $\forall\, 1 \le i \le k$. Rewrite $f_{i,l}(D)$ as $D^{\omega_{i,l}} f_{i,l}^*(D)$, where $f_{i,l}^*(D)$ is delay free, $\forall\, i$, l. Let $\omega_i = \min_l \omega_{i,l}$ and $\eta_i = \min_l \deg(f_{i,l}^*(D))$, $\forall\, i$.

Denote by $g_{i,j}(D)$ be the entry in the (i, j) position of $G(D)$, $\forall\ 1 \le i \le k$ and $1 \le j \le n$. Let $\rho = \max_{i,j} \deg(g_{i,j}(D))$ and $\tilde{G}(D^{-1}) = D^{-\rho} G(D)$. It is clear that $\tilde{G}(D^{-1})$ is a matrix over $F[D^{-1}]$ since all its entries are now polynomials in D^{-1}. By definition, we have that any $i \times i$ minor of $\tilde{G}(D^{-1})$ is equal to the product of $D^{-\rho i}$ and the $i \times i$ minor of the corresponding submatrix of $G(D)$. It is obvious that the degree of any $i \times i$ minor of $G(D)$ is less than or equal to ρi, i.e., $\rho i \ge m_i$, since any $i \times i$ minor of $\tilde{G}(D^{-1})$ is a polynomial in D^{-1}. By Lemma 1, the greatest common divisor of all $i \times i$ minors of $\tilde{G}(D^{-1})$, denoted by $\tilde{\Delta}_i(D^{-1})$, can thus be obtained by

$$\begin{aligned} & \mathrm{GCD}(D^{-\rho i} f_{i,1}(D), D^{-\rho i} f_{i,2}(D), \ldots, D^{-\rho i} f_{i,N_i}(D)) \\ = \;& D^{-(\rho i - m_i + \omega_i + \eta_i)}\mathrm{GCD}(f_{i,1}(D), f_{i,2}(D), \cdots, f_{i,N_i}(D)) \\ = \;& D^{-(\rho i - m_i + \deg(\Delta_i(D)))}\Delta_i(D) \end{aligned} \quad (8)$$

$\forall\ 1 \le i \le k$. Setting $\tilde{\Delta}_0(D^{-1}) = 1$, we can express the i-th invariant factor of $\tilde{G}(D^{-1})$ as the ratio of $\tilde{\Delta}_i(D^{-1})/\tilde{\Delta}_{i-1}(D^{-1})$, $\forall\, i$. By (8), the ratio can be further deduced as

$$\begin{aligned} & \frac{D^{-(\rho i - m_i + \deg(\Delta_i(D)))}\Delta_i(D)}{D^{-(\rho(i-1) - m_{i-1} + \deg(\Delta_{i-1}(D)))}\Delta_{i-1}(D)} \\ =& \frac{D^{-\rho}}{D^{-(m_i - m_{i-1})}} D^{-(\deg(\Delta_i(D)) - \deg(\Delta_{i-1}(D)))} \frac{\Delta_i(D)}{\Delta_{i-1}(D)} \\ =& \frac{D^{-\rho}}{D^{-(m_i - m_{i-1})}} D^{-\deg(\lambda_i(D))}\lambda_i(D). \end{aligned} \quad (9)$$

Since $G(D) = D^{\rho}\tilde{G}(D^{-1})$, by (9), it follows that the i-th invariant factor of $G(D)$ over $F(D^{-1})$ is

$$D^{\rho}\frac{D^{-\rho}}{D^{-(m_i - m_{i-1})}} D^{-\deg(\lambda_i(D))}\lambda_i(D) = \frac{D^{-\deg(\lambda_i(D))}\lambda_i(D)}{D^{-(m_i - m_{i-1})}}.$$

∎

By Theorem 2, the ith invariant factor of $G(D)$ over $F(D^{-1})$ can be obtained as in (7). Since $D^{-\deg(\lambda_i(D))}\lambda_i(D)$

and $D^{-(m_i-m_{i-1})}$ in (7) are relatively prime, discussion in Section II implies that the ith invariant factor contributes the following amount of degree: $m_i - m_{i-1}$ to the McMillan degree if $D^{-(m_i-m_{i-1})} \in F[D^{-1}]$, i.e., $m_i \geq m_{i-1}$. Define

$$(m_i - m_{i-1})^+ = \max(m_i - m_{i-1}, 0), \forall\ 1 \leq i \leq k.$$

We can thus obtain the McMillan degree of $G(D)$ by

$$\sum_{i=1}^{k} (m_i - m_{i-1})^+ \tag{10}$$

without decomposing $G(D)$ into the invariant form over $F(D^{-1})$. By (10), the condition that a PGM will have same internal and McMillan degrees is investigated in Corollary 1.

Corollary 1: Given a PGM $G(D)$ of an (n, k) convolutional code, let m_k and m_{k-1} be the maximum degrees of $i \times i$ and $(i-1) \times (i-1)$ minors of $G(D)$, respectively. $G(D)$ will have the same internal and McMillan degrees if and only if $m_k \geq m_{k-1}$.

Proof:

Let m_i be the maximum degree of $i \times i$ minors of $G(D)$, $\forall\ 1 \leq i \leq k$, and set $m_0 = 0$. Note that m_k is the internal degree of $G(D)$ by definition and the McMillan degree is $\sum_{i=1}^{k} (m_i - m_{i-1})^+$ by (10). By (1) and (7), we have

$$D^{m_i - m_{i-1}} | D^{m_{i-1} - m_{i-2}},\ \forall\ 2 \leq i \leq k \tag{11}$$

which implies that

$$m_1 - m_0 \geq m_2 - m_1 \geq \cdots \geq m_k - m_{k-1}. \tag{12}$$

In addition, it can be shown that

$$\sum_{i=1}^{k} (m_i - m_{i-1})^+ \geq m_k$$

and the equality holds if and only if $(m_i - m_{i-1})^+ = m_i - m_{i-1}$, i.e., $m_i - m_{i-1} \geq 0$, $\forall\ 1 \leq i \leq k$. By (12), it follows that $\sum_{i=1}^{k} (m_i - m_{i-1})^+ = m_k$ if and only if $m_k - m_{k-1} \geq 0$, hence completing the proof. ∎

In the following, Lemma 2 is given for the necessary and sufficient condition of a PGM which has a specific internal degree.

Lemma 2: Consider a basic PGM $G(D)$ of an (n, k) convolutional code over finite field F with internal degree κ. For a nonnegative integer ω and a $k \times k$ nonsingular matrix over $F(D)$, $T(D)G(D)$ is a PGM with internal degree $\kappa + \omega$ if and only if $T(D)$ is a $k \times k$ polynomial matrix with $\deg(\det(T(D))) = \omega$, where $\det(\cdot)$ stands for the determinant operator.

Proof:

Denote by $f_1(D)$, $f_2(D)$, $\cdots$, $f_N(D)$ the $k \times k$ minors of $G(D)$, where N indicates the number of $k \times k$ minors. The $k \times k$ minors of $T(D)G(D)$ must be of the form:

$$\det(T(D)) f_i(D),\ \forall\ 1 \leq i \leq N$$

since every $k \times k$ submatrix of $T(D)G(D)$ can be expressed as the product of $T(D)$ and the corresponding submatrix of $G(D)$. Let intdeg$(\cdot)$ stand for the operator taking the internal degree of a PGM. If $T(D)$ is a polynomial matrix with $\det(T(D)) = \omega$, it follows that $T(D)G(D)$ is a PGM with

$$\begin{aligned} \text{intdeg}(T(D)G(D)) &= \deg(\det(T(D))) + \text{intdeg}(G(D)) \\ &= \omega + \kappa. \end{aligned} \tag{13}$$

For the other direction, suppose $T(D)G(D)$ is a PGM with internal degree $\kappa + \omega$. Since a basic PGM always has a polynomial right inverse [11], it implies that $T(D)$ is a polynomial matrix. By (13), we also have $\deg(\det(T(D)))$ = intdeg$(T(D)G(D))$ − intdeg$(G(D))$ = ω. ∎

By Theorem 1, Corollary 1, and Lemma 2, Procedure 1 is then proposed to search the optimal PGM which is noncatastrophic and has the smallest McMillan degree among all optimal PGMs.

Procedure 1:

Step 1. Given an (n, k) convolutional code C over finite field F, find a generator matrix $G(D)$ which is basic and optimal. Set i = 0.

Step 2. Set $\Pi = \{T(D) : \forall\ T(D) \in F[D]$ with $\deg(\det(T(D))) = i\}$. If there exists a $T^*(D) \in \Pi$ which is effectively lower-triangular respect to $G(D)$ such that the greatest common divisor of $k \times k$ minors of $T^*(D)G(D)$ is a power of D and m_k and m_{k-1} of $T^*(D)G(D)$ satisfy $m_k \geq m_{k-1}$, go to Step 4; else go to next step. (m_k and m_{k-1} denote the maximum degrees of $k \times k$ and $(k-1) \times (k-1)$ minors of $T^*(D)G(D)$, respectively.)

Step 3. Set i = i+1, and go back to Step 2.

Step 4. $T^*(D)G(D)$ is the desired optimal PGM which is noncatastrophic and has the lowest McMillan degree.

In Step 1, Procedure 1 starts from a basic PGM which has the minimal internal degree, and the internal degree of $T^*(D)G(D)$ is increased only by one once Step 3 is executed. Moreover, it follows that the interanl degree $\leq$ the McMillan degree for every PGM. Together with the checking of the UEP optimality, the noncatastrophic property, and the equality of internal and McMillan degrees in Step 2, we will never miss the desired generator matrix.

Although Procedure 1 can generate the generator matrix with the smallest McMillan degree among all optimal PGMs, it does not guarantee that there is no other non-polynomial optimal generator matrix which has a smaller McMillan degree than the one searched by Procedure 1. To obtain the optimal generator matrix (in general over $F(D)$) with the smallest McMillan degree, Corollary 2 is presented to specify all the generator matrices with a given McMillan degree by generalizing the transformation between minimal generator matrices in [13]. Based on Corollary 2, Procedure 2 is then proposed to search the optimal generator matrix with the smallest McMillan degree.

Corollary 2: Given an (n, k) convolutional code C over finite field F, let $G_c(D)$ be a canonical generator matrix with external degree μ. For any nonnegative integer ω, denote by $T(D)$ the $k \times k$ nonsingular matrix of the following form:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & D^{\omega} \end{pmatrix}. \quad (14)$$

We have that $T(D)G_c(D)$ is a generator matrix with McMillan degree $\mu+\omega$. Suppose $T(D)G_c(D)$ has a minimal encoder with state space description (A, B, K, E), where A, B, K, E are $(\mu+\omega)\times(\mu+\omega)$, $k\times(\mu+\omega)$, $(\mu+\omega)\times n$, $k\times n$, matrices over F, respectively. All generator matrices of C with McMillan degree $\mu+\omega$ must be of the form: $\Phi E+\Phi B(D^{-1}I-A)^{-1}(K+\Psi E)$, where Φ is a nonsingular $k\times k$ matrix over F, Ψ is an arbitrary $(\mu+\omega)\times k$ matrix over F, and I is the $(\mu+\omega)\times(\mu+\omega)$ identity matrix.

Proof:

Given a PGM $G(D)$, let $g_{i,j}(D)$ denote the entry in the (i,j) position of $G(D)$, $\forall\ 1\le i\le k$ and $1\le j\le n$. Let $e_i=\max_j \deg(g_{i,j}(D))$, $\forall\ i$. Define the indicator matrix $\bar{G}$ for the highest degree terms of $G(D)$ by

$$\bar{G}_{i,j} = \text{the coefficient of } D^{e_i} \text{ in } g_{i,j}(D)$$

where $\bar{G}_{i,j}$ stands for the entry in the (i,j) position of $\bar{G}$, $\forall\ i,j$. If $\bar{G}$ is full-rank, the internal, McMillan, and external degrees of $G(D)$ are of same value [11]. Since $G_c(D)$ is a canonical generator matrix, its indicator matrix is always full-rank [11]. With $T(D)$ in (14), it can be shown that the indicator matrix of $T(D)G_c(D)$ is also full-rank. By Lemma 2, we have that the internal degree of $T(D)G_c(D)$ is $\mu+\omega$, which hence implies that the McMillan degree of $T(D)G_c(D)$ is also $\mu+\omega$.

Suppose the minimal encoder of $T(D)G_c(D)$ has the state-space description (A, B, K, E) satisfying the following state-space equations:

$$\begin{cases} \boldsymbol{s}(t+1) &= \boldsymbol{s}(t)A+\boldsymbol{u}(t)B \\ \boldsymbol{y}(t) &= \boldsymbol{s}(t)K+\boldsymbol{u}(t)E \end{cases}$$

where $\boldsymbol{s}(t)$, $\boldsymbol{x}(t)$, and $\boldsymbol{y}(t)$ denote the state vector, input vector, and output vector of the encoder at time t. By [13], all possible encoders of C which has the same dimension of state, i.e., $\mu+\omega$, can be obtained by the following state-space transformation: $(A+\Psi B, \Phi B, K+\Psi E, \Phi E)$, where Ψ is an arbitrary $(\mu+\omega)\times k$ matrix over F and Φ is a nonsingular $k\times k$ matrix over F. Such a new state-space description will result in generator matrix of the following form: $\Phi E+\Phi B(D^{-1}I-A)^{-1}(K+\Psi E)$ which has McMillan degree $\mu+\omega$, hence completing the proof. ∎

Procedure 2:

Step 1. Give an (n,k) convolutional code C over finite field F, find a canonical generator matrix $G_c(D)$ and an optimal PGM $G_o(D)$ for C. Set $\hat{G}(D)=G_c(D)$ and $\Omega(D)$ be the matrix of the form in (14) with $\omega=1$.

Step 2. Let (A, B, K, E) be the state-space description of the minimal encoder of $\hat{G}(D)$. Set $\Pi=\{G(D): G(D)=\Phi E+\Phi B(D^{-1}I-A)^{-1}(K+\Psi E)\}$, where Ψ is a $(\mu+i)\times k$ arbitrary matrix over F and Φ is a $k\times k$ nonsingular matrix over F. If there exists a noncatastrophic generator matrix $G^*(D)\in\Pi$ such that $G^*(D)=T(D)G_o(D)$, where $T(D)$ is an effectively lower-triangular matrix with respect to $G_o(D)$, go to Step 4; else go to next step.

Step 3. Set $\hat{G}(D)=\Omega(D)\hat{G}(D)$. Go back to Step 2.

Step 4. $G^*(D)$ is the desired optimal generator matrix which is noncatastrophic and has the lowest McMillan degree.

In Procedure 2, we start from a canonical generator matrix which has the minimal McMillan degree, and the McMillan degree of $\hat{G}(D)$ is increased only by one in Step 3. Moreover, in Step 2, all possible generator matrices of the same McMillan degree will be checked for the UEP optimality and the noncatastrophic property. It hence guarantees the correctness of Procedure 2.

V. Conclusion

In this paper, convolutional encoders are studied for UEP from an algebraic theoretical viewpoint. We focus on minimizing the McMillan degree of an optimal generator matrix to optimize the trade-off between the complexity and UEP capability. Procedures are provided to obtain an optimal and noncatastrophic generator matrix which achieves the smallest McMillan degree among all optimal ones.

References

[1] R. Palazzo Jr., "Linear unequal error protection convolutional codes," in *Proc. 1985 IEEE Int. Symp. Inform. Theory*, Brighton, U.K., June 1985, pp. 88–89.

[2] R. Palazzo Jr., "On the linear unequal error protection convolutional codes," in *Proc. 1986 IEEE Int. Global Telecom. Conf.*, Houston, TX, Dec. 1986, pp. 1367–1371.

[3] Ph. Piret, *Convolutional Codes*. Cambridge, MA: MIT Press, 1988.

[4] D. G. Mills and D. J. Costello, Jr., "Using a modified transfer function to calculate unequal error protection capabilities of convolutional codes," in *Proc. 1993 IEEE Int. Symp. Inform. Theory*, San Antonio, TX, Jan. 1993, p. 144.

[5] D. G. Mills and D. J. Costello, Jr., "A bound on the unequal error protection capabilities of rate k/n convolutional codes," in *Proc. 1994 IEEE Int. Symp. Inform. Theory*, Trondheim, Norway, June 1994, p. 274.

[6] M.-C. Chiu, C.-C. Chao, and C.-H. Wang, "Convolutional codes for unequal error protection," in *Proc. 1997 IEEE Int. Symp. Inform. Theory*, Ulm, Germany, June 1997, p. 290.

[7] C.-H. Wang and C.-C. Chao, "Further results on unequal error protection of convolutional codes," in *Proc. 2000 IEEE Int. Symp. Inform. Theory*, Sorrento, Italy, June 2000, p. 35.

[8] V. Pavlushkov, R. Johannesson, and V. V. Zyablov, "Unequal error protection for convolutional codes," *IEEE Trans. Inf. Theory*, vol. 52, pp. 700–708, Feb. 2006.

[9] C.-H. Wang and C.-C. Chao, "Canonical convolutional encoders for unequal error protection," in *Proc. 2008 IEEE Int. Symp. Inform. Theory*, Toronto, Canada, June 2008, pp. 2232–2236.

[10] L. A. Dunning and W. E. Robbins, "Optimum encoding of linear block codes for unequal error protection," *Inform. Contr.*, vol. 37, pp. 150–177, 1978.

[11] R. J. McEliece, "The algebraic theory of convolutional codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 1065–1138.

[12] G. D. Forney, Jr., R. Johannesson, and Z. X. Wan, "Minimal and canonical rational generator matrices for convolutional codes," *IEEE Trans. Inf. Theory*, vol. 42, pp. 1865–1880, Nov. 1996.

[13] B. W. Dickinson, "A new characterization of canonical convolutional encoders," *IEEE Trans. Inf. Theory*, vol. IT-22, pp. 352–354, May 1976.