

On Unequal Error Protection of Convolutional Codes From an Algebraic Perspective

Chung-Hsuan Wang, *Member, IEEE*, Mao-Ching Chiu, *Member, IEEE*, and Chi-chao Chao, *Member, IEEE*

Abstract—In this paper, convolutional codes are studied for unequal error protection (UEP) from an algebraic theoretical viewpoint. We first show that for every convolutional code there exists at least one optimal generator matrix with respect to UEP. The UEP optimality of convolutional encoders is then combined with several algebraic properties, e.g., systematic, basic, canonical, and minimal, to establish the fundamentals of convolutional codes for UEP. In addition, a generic lower bound on the length of a UEP convolutional code is proposed. Good UEP codes with their lengths equal to the derived lower bound are obtained by computer search.

Index Terms—Basic/canonical/systematic generator matrices, convolutional codes, unequal error protection.

I. INTRODUCTION

IN many practical applications, e.g., broadcast channels, packet-switching networks, and visual/speech communication systems, it is desirable to design an error-correcting code which can provide unequal error protection (UEP) to make the best use of the channel bandwidth. Previous papers about UEP codes were mainly focused on block codes [1]–[19]. Among those studies, the notion of the separation vector was introduced in [4] to measure the UEP capability of block codes and it was shown that given any linear block code there exists an optimal generator matrix with respect to UEP which has the greatest separation vector among all generator matrices. Bounds on the length of linear UEP block codes were extensively studied in [7], [11]. Several optimal linear UEP block codes were given in [7]. Besides, nonlinear UEP block codes of better performance than any linear UEP block codes were investigated in [17]–[19].

Recently, research efforts about UEP have been extended to convolutional codes. Most of the studies are concentrated on developing new UEP schemes, which include using punctured and

path-pruned convolutional codes for UEP [20]–[24] and combining low-rate or short-length convolutional codes by special algebraic structures [25]–[28]. Only a few are about the UEP capability of convolutional codes [29]–[38]. Although several authors have pointed out that the separation vector, originally defined for block codes, also serves as an effective UEP measurement for convolutional codes, unfortunately, most of the available results for UEP block codes can not be directly applied to convolutional codes. Therefore, many important algebraic properties of UEP convolutional codes, such as the existence of optimal generator matrices and the relation between UEP and encoding/decoding complexity, have not been well addressed.

In this paper, a full investigation of the UEP capability of convolutional codes is made from an algebraic theoretical viewpoint. First, the UEP capability of convolutional encoders is combined with several algebraic properties, e.g., systematic, basic, canonical, and minimal, to establish the fundamentals of convolutional codes for UEP. For every convolutional code, we prove that there exists at least one optimal generator matrix which has the greatest separation vector and hence the best UEP capability among all generator matrices. Every optimal generator matrix can always be transformed into a basic matrix, which avoids the undesired catastrophic propagation of decoding errors, without sacrificing its UEP optimality. (Even though this property was proposed in [31], here we give a more well-rounded and detailed exploration.) By a counterexample, however, we show that there may not exist an optimal generator matrix which is also canonical or minimal to minimize both of the encoding and decoding complexity. To optimize the UEP capability while minimize the complexity requirement, several procedures are given for obtaining an optimal generator matrix with the smallest external degree or for searching a canonical generator matrix with the greatest separation vector. Necessary and sufficient conditions for the above desired generator matrices are derived as well. In addition, UEP is combined with systematic generator matrices which are minimal and can provide easy inversion of the encoder operation. Finally, we propose a lower bound on the length of a convolutional code with the given memory distribution and separation vector, based on which optimal (or near optimal) UEP convolutional codes are provided by computer search.

The rest of the paper is organized as follows. Section II gives a brief review of the algebraic theory of convolutional codes. The UEP capability of convolutional encoders is discussed in Section III, where the transformation to make the optimal generator matrices noncatastrophic is also given. The tradeoff between the UEP capability and complexity of convolutional encoders is investigated in Section IV. Section V presents the

Manuscript received December 04, 2008; revised May 04, 2009. Current version published December 23, 2009. This work was supported by the National Science Council of the Republic of China by Grants NSC-88-2213-E-007-081 and NSC-89-2213-E-007-061. The material in this paper was presented in part at the IEEE Symposium on Information Theory, Sorrento, Italy, June 1997, and at the IEEE Symposium on Information Theory, Toronto, ON, Canada, July 2008.

C.-H. Wang is with the Institute of Communication Engineering and the Department of Electrical Engineering, National Chiao Tung University, Hsinchu 30010, Taiwan, R.O.C. (e-mail: chwang@mail.nctu.edu.tw).

M.-C. Chiu is with the Department of Electrical Engineering, National Chung Cheng University, Chia-Yi 621, Taiwan, R.O.C. (e-mail: ieemcc@ccu.edu.tw).

C.-C. Chao is with the Institute of Communications Engineering and the Department of Electrical Engineering, National Tsing Hua University, Hsinchu 30013, Taiwan, R.O.C. (e-mail: ccc@ee.nthu.edu.tw).

Communicated by L. M. G. M. Tolhuizen, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2009.2034821

bound on the length of UEP convolutional codes, where tables of good UEP codes are given. Finally, this work is concluded in Section VI.

II. 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 [39]. 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 $a_i \in F, \forall i$, and m can be any finite 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 $F(D)$. For a Laurent series $x(D)$, the weight $w(x(D))$ is defined as the number of its nonzero coefficients. The weight of a vector of Laurent series $\mathbf{x}(D) = (x_1(D), x_2(D), \dots, x_n(D))$, where $\mathbf{x}(D) \in F(D)^n$ (the n -tuple vector space over $F(D)$), is defined to be the sum of the weights of its components: $w(\mathbf{x}(D)) = \sum_{i=1}^n w(x_i(D))$. If A is a subset of $F(D)^n$, define $w[A] = \min_{\mathbf{x}(D) \in A \setminus \{0\}} w(\mathbf{x}(D))$ as the minimum weight of nonzero elements in A .

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 $\{\mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_k(D)\}$ form a basis for C . Every codeword $\mathbf{c}(D)$ is encoded by $\mathbf{c}(D) = \mathbf{I}(D)G(D)$, where $\mathbf{I}(D) = (I_1(D), I_2(D), \dots, I_k(D)) \in F(D)^k$. 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 [39], we define the internal and external degrees of a PGM $G(D)$ by

$$\begin{aligned} \text{intdeg}(G(D)) &= \text{maximum degree of } G(D)\text{'s } k \times k \text{ minors} \\ \text{extdeg}(G(D)) &= \text{sum of the row degrees of } G(D). \end{aligned}$$

¹ Given a convolutional encoder, the corresponding degree is defined as 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. Denote the minimum degree of all possible encoders of a given generator matrix by the McMillan degree; this quantity is commensurate to the minimum complexity of building the encoder and conducting the Viterbi decoding algorithm for a given generator matrix. With respect to the internal, external, and McMillan degrees, some special generator matrices are introduced.

Definition 1: A $k \times n$ polynomial matrix $G(D)$ is called basic if it has the minimum possible internal degree among all polynomial matrices of the form $T(D)G(D)$, where $T(D)$ is a nonsingular $k \times k$ matrix over $F(D)$.

Definition 2: A PGM is called reduced if its external degree can not be reduced by a sequence of elementary row operations.

Definition 3: A PGM for a given convolutional code C is called canonical if it has the smallest possible external degree

¹ A $k \times k$ minor of $G(D)$ is the determinant of a $k \times k$ submatrix of $G(D)$.

among all PGMs for C . This minimal external degree is called the degree of C , denoted by $\text{deg}(C)$.

Definition 4: A generator matrix for a given convolutional code C is called minimal if its McMillan degree is equal to $\text{deg}(C)$.

A PGM is canonical if and only if it is basic and reduced [39]. Given a convolutional code, the row degrees, called the Forney indices, are the same for all canonical PGMs [39]. The degree of a code can be shown equal to the minimum McMillan degree among all generator matrices [40], which implies that every canonical generator matrix is also minimal. As a result of [41], [42], basic and minimal generator matrices always have polynomial right inverses, for which polynomial codewords imply polynomial inputs; both classes of generator matrices are hence noncatastrophic. There is another class of systematic generator matrices defined as those of the form $(I_k \ X(D))$, under proper permutation of columns, where I_k is the $k \times k$ identity matrix and $X(D)$ is a $k \times (n - k)$ matrix over $F(D)$, which are minimal [39] and possess the advantage of easy inversion of the encoder operation. For further properties of basic, reduced, canonical, minimal, and systematic generator matrices, please refer to [31], [39]–[44].

III. CONVOLUTIONAL ENCODERS FOR UEP

Convolutional codes are conventionally used for equal error protection; in such applications, the free distance defined as the minimum weight of nonzero codewords is unarguably an effective parameter for performance evaluation [39]. However, ordinary (n, k) convolutional codes with $k > 1$ may possess the UEP capability. For example, consider a binary convolutional code with generator matrix

$$G(D) = \begin{pmatrix} 1 & 0 & 1 \\ D^2 + D + 1 & D^2 + 1 & 0 \end{pmatrix}. \quad (1)$$

Denote by $I_i(D)$ (the Laurent series of) the information bit sequence fed to the i th input of the encoder for $i = 1, 2$. Suppose this code is used for transmission over additive white Gaussian noise (AWGN) channels with binary phase-shift keying (BPSK) modulation. The bit error rate (BER) curves of $I_1(D)$ and $I_2(D)$ by Viterbi decoding are plotted in Fig. 1, where $I_2(D)$ is observed to experience a better protection than $I_1(D)$ with a signal-to-noise ratio (SNR) gain around 3 dB at BER 10^{-5} . This code can hence be used for UEP as long as the data of distinct BER requirements are properly fed into the encoder. Similar to the free distance, the UEP capability of a convolutional encoder can be described by the separation vector, originally proposed for block codes in [4], or called the free-input distance in [37], defined here.

Definition 5: For an (n, k) convolutional code C over F , the separation vector $\mathbf{s}(G(D)) = (s(G(D))_1, s(G(D))_2, \dots, s(G(D))_k)$ with respect to a generator matrix $G(D)$ for C is defined by $s(G(D))_i = w[\{\mathbf{I}(D)G(D) : I_i(D) \neq 0\}]$, $\forall 1 \leq i \leq k$, where $\mathbf{I}(D) = (I_1(D), I_2(D), \dots, I_k(D))$ denotes the vector of the Laurent series of the input sequences.

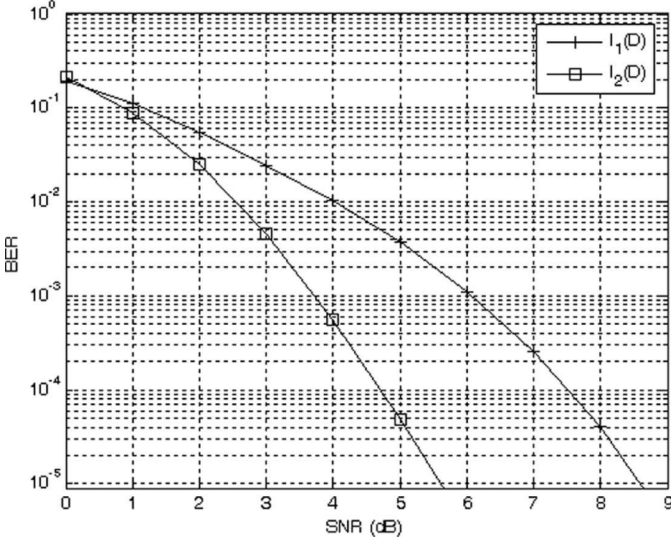


Fig. 1. BER curves of a convolutional code with generator matrix in (1) on AWGN channels with BPSK modulation.

By this definition, the minimum of $s(G(D))_i$'s is hence the free distance of the convolutional code. A large value of $s(G(D))_i$ implies a small BER for the information sequence $I_i(D)$ fed into the i th input of the encoder at high SNRs [32], [33]. For the code with generator matrix in (1), we have $\mathbf{s}(G(D)) = (2, 5)$ by Definition 5; the two distinct values in $\mathbf{s}(G(D))$ thus implies the two-level UEP provided by $G(D)$.

Given a set of vectors $X = \{\mathbf{x}_1(D), \mathbf{x}_2(D), \dots\}$, where $\mathbf{x}_i(D) \in F(D)^n, \forall i$, denote by

$$\langle X \rangle = \left\{ \sum_i a_i(D) \mathbf{x}_i(D) : a_i(D) \in F(D) \right\}$$

the subspace consisting of all linear combinations of elements in X . Without ambiguity, sometimes set brackets are omitted for simplicity, e.g., $\langle \mathbf{x}_1(D), \mathbf{x}_2(D), \mathbf{x}_3(D) \rangle = \langle \{\mathbf{x}_1(D), \mathbf{x}_2(D), \mathbf{x}_3(D)\} \rangle$. Also if a matrix is written inside the span operator $\langle \cdot \rangle$, then the corresponding set is the set of rows of the matrix, e.g., $\langle G(D) \rangle$ means the subspace spanned by the rows of $G(D)$. By Definition 5, it follows that

$$s(G(D))_i = w[C \setminus \langle G(D) \setminus \mathbf{g}_i(D) \rangle], \quad \forall 1 \leq i \leq k. \quad (2)$$

Define $C^\rho = \{\mathbf{c}(D) : \mathbf{c}(D) \in C \text{ and } w(\mathbf{c}(D)) < \rho\}$ and let $G^\rho(D)$ be the matrix consisting of the fewest number of rows of $G(D)$ such that $C^\rho \subseteq \langle G^\rho(D) \rangle$. Lemma 1 gives some further properties of the separation vector.

Lemma 1: Consider a generator matrix $G(D)$ of a convolutional code with rows $\mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_k(D)$.

- a) If the separation vector $\mathbf{s}(G(D))$ is arranged in the non-decreasing order, i.e., $s(G(D))_i \leq s(G(D))_{i+1}, \forall 1 \leq i < k$, we have

$$s(G(D))_i = w[C \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle] \quad (3)$$

$$\forall 1 < i \leq k.$$

- b) $\forall \rho$ and $1 \leq i \leq k$,

$$s(G(D))_i \geq \rho \text{ if and only if } \mathbf{g}_i(D) \notin G^\rho(D).$$

Proof:

- a) By (2) and the fact that

$$\begin{aligned} \{C \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle\} \\ = \{\mathbf{I}(D)G(D) : I_j(D) \neq 0 \text{ for some } j \geq i\} \end{aligned}$$

we have

$$s(G(D))_i \geq w[\{C \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle\}].$$

If $\mathbf{s}(G(D))$ is nondecreasingly ordered, it follows that $s(G(D))_i \leq \dots \leq s(G(D))_j \leq w(\mathbf{I}(D)G(D))$ for every $\mathbf{I}(D)$ with $I_j(D) \neq 0$ for some $j \geq i$ and $s(G(D))_i \leq w[\{C \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle\}]$. The proof is thus completed.

- b) If $\mathbf{g}_i(D) \notin G^\rho(D)$, then $C^\rho \subseteq \langle G(D) \setminus \mathbf{g}_i(D) \rangle$ implies $s(G(D))_i \geq \rho$ by (2). For the reverse direction, suppose $\mathbf{g}_i(D) \in G^\rho(D)$. It is clear that $C^\rho \not\subseteq \langle G(D) \setminus \mathbf{g}_i(D) \rangle$; otherwise, a contradiction that $C^\rho \subseteq \langle G^\rho(D) \setminus \mathbf{g}_i(D) \rangle$ is obtained. Thus, we have $s(G(D))_i < \rho$. \square

A. Optimal Generator Matrix

For two vectors of real numbers $\mathbf{a} = (a_1, a_2, \dots, a_k)$ and $\mathbf{b} = (b_1, b_2, \dots, b_k)$, define $\mathbf{a} \geq \mathbf{b}$ if and only if $a_i \geq b_i, \forall 1 \leq i \leq k$. The two vectors \mathbf{a} and \mathbf{b} are said to be comparable if either $\mathbf{a} \geq \mathbf{b}$ or $\mathbf{b} \geq \mathbf{a}$. In the following, we define an optimal generator matrix which has the greatest separation vector among all generator matrices of a given code.

Definition 6: Given a convolutional code C , a generator matrix $G(D)$ is called optimal (with respect to UEP) if for any other generator matrix $G'(D)$ of C , there exists a permutation of vector components ϕ such that $\mathbf{s}(G(D)) \geq \phi(\mathbf{s}(G'(D)))$.

To achieve the optimal UEP performance, it is desirable to use an optimal generator matrix for encoding. However, given a convolutional code, we observe that there may exist generator matrices with incomparable separation vectors. For example, consider a binary convolutional code with generator matrices

$$\begin{aligned} G_1(D) &= \begin{pmatrix} 0 & 1 & 0 & D \\ 1 + D + D^2 & 1 & D^2 & 1 + D + D^2 \\ 1 + D & 0 & 1 & 1 + D + D^2 \end{pmatrix} \\ &\quad \text{and} \\ G_2(D) &= \begin{pmatrix} D^2 & 0 & 1 + D^2 & D \\ D^2 & 1 & 1 + D^2 & 0 \\ 1 + D & 0 & 1 & 1 + D + D^2 \end{pmatrix} \end{aligned}$$

which result in two incomparable separation vectors $\mathbf{s}(G_1(D)) = (2, 4, 4)$ and $\mathbf{s}(G_2(D)) = (2, 2, 6)$. A question naturally arises that whether there always exists an optimal generator matrix for every convolutional code. Moreover, if the answer is positive, how to find an optimal one? Suppose for the moment there exists at least one optimal generator matrix. We first derive a necessary and sufficient condition for optimal generator matrices in Theorem 1 and then obtain Corollary 1

for the available separation vectors of all generator matrices of a given code.

Theorem 1: For a convolutional code C , define $w(C) = \{w(\mathbf{c}(D)) : \mathbf{c}(D) \in C\}$. A generator matrix $G(D)$ is optimal if and only if $\exists X(D) \subseteq G(D)$ such that

$$\langle C^\rho \rangle = \langle X(D) \rangle, \forall \rho \in w(C) \quad (4)$$

where $X(D) \subseteq G(D)$ means that all rows of $X(D)$ are contained in $G(D)$.

Proof: Without loss of generality, each generator matrix considered in the following is assumed to have a nondecreasingly ordered separation vector. Let $G(D)$ satisfy (4) but suppose $G(D)$ is not an optimal generator matrix. Then, a generator matrix $A(D)$ (with rows $\mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_k(D)$) exists such that $\mathbf{s}(G(D)) \not\geq \mathbf{s}(A(D))$. Let i be the minimal interger in $\{1, 2, \dots, k\}$ such that $s(G(D))_i < s(A(D))_i$. Set $\rho = s(A(D))_i$ and let $X(D) \subseteq G(D)$ such that $\langle C^\rho \rangle = \langle X(D) \rangle$. By Lemma 1, it implies that $\langle C^\rho \rangle \subseteq \langle \mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_{i-1}(D) \rangle$ and $\mathbf{g}_j(D) \in G^\rho(D)$, $\forall 1 \leq j \leq i$. Thus, a contradiction that

$$\langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_i(D) \rangle \subseteq \langle C^\rho \rangle$$

and

$$\langle C^\rho \rangle \subseteq \langle \mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_{i-1}(D) \rangle$$

has been reached, and hence $G(D)$ is optimal.

For the reverse direction, suppose $G(D)$ is an optimal generator matrix for C and consider an integer $\rho \in w(C)$. Denote by $\dim\langle C^\rho \rangle$ the dimension of vector space $\langle C^\rho \rangle$. Let $\{\mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_l(D)\}$ be a basis of $\langle C^\rho \rangle$, where $l = \dim\langle C^\rho \rangle$. Choose $\mathbf{a}_{l+1}(D), \mathbf{a}_{l+2}(D), \dots, \mathbf{a}_k(D)$ from C such that the following matrix forms a generator matrix of C :

$$A(D) = (\mathbf{a}_1^T(D) \cdots \mathbf{a}_l^T(D) \mathbf{a}_{l+1}^T(D) \cdots \mathbf{a}_k^T(D))^T$$

where T denotes transposition. Clearly, $A^\rho(D)$ is the matrix with rows $\mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_l(D)$. By Lemma 1, it follows that $s(A(D))_j \geq \rho, \forall l+1 \leq j \leq k$, because $\mathbf{a}_j(D) \notin A^\rho(D)$. Since $\mathbf{s}(G(D)) \geq \mathbf{s}(A(D))$, we have $s(G(D))_j \geq \rho$ and hence $\mathbf{g}_j(D) \notin G^\rho(D), \forall l+1 \leq j \leq k$, by Lemma 1, which implies

$$\langle C^\rho \rangle \subseteq \langle G^\rho(D) \rangle \subseteq \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_i(D) \rangle.$$

We, thus, have $\langle C^\rho \rangle = \langle G^\rho(D) \rangle$ since $\dim\langle C^\rho \rangle = l$. \square

Corollary 1: Let $G(D)$ be an optimal generator matrix of an (n, k) convolutional code C . For any arbitrary generator matrix $G'(D)$ of C , we have

$$s(G'(D))_j \in \{s(G(D))_i : 1 \leq i \leq k\}, \forall 1 \leq j \leq k.$$

Proof: Suppose there exists an $s(G'(D))_j \notin \{s(G(D))_i : 1 \leq i \leq k\}$ for some j . It means that $\exists \langle C^{s(G'(D))_j} \rangle$ such that

$$\langle X(D) \rangle \neq \langle C^{s(G'(D))_j} \rangle, \forall X(D) \subseteq G(D)$$

which contradicts the necessary and sufficient condition of an optimal generator matrix in Theorem 1, thereby completing the proof. \square

To show the existence of optimal generator matrices of a given convolutional code, we further define a class of monotonically weight-retaining matrices below.

Definition 7: For an (n, k) convolutional code C , a generator matrix $G(D)$ with rows $\mathbf{g}_i(D)$'s, $\forall 1 \leq i \leq k$, is said to be monotonically weight-retaining if and only if

$$w[\langle \mathbf{g}_1(D) \rangle] = w[C]$$

and

$$w[\langle \mathbf{g}_i(D) \rangle] = w[C \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle], \forall 1 < i \leq k.$$

Consider a codeword $\mathbf{c}(D)$ encoded by a monotonically weight-retaining matrix $G(D)$, i.e., $\mathbf{c}(D) = I_1(D)\mathbf{g}_1(D) + I_2(D)\mathbf{g}_2(D) + \dots + I_k(D)\mathbf{g}_k(D)$, where $(I_1(D), I_2(D), \dots, I_k(D)) \in F(D)^k$. If $I_i(D) \neq 0$ for some $i \in \{1, 2, \dots, k\}$, then $\mathbf{c}(D) \notin \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle$, and, hence

$$\begin{aligned} w(\mathbf{c}(D)) &\geq w[C \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle] \\ &= w[\langle \mathbf{g}_i(D) \rangle]. \end{aligned}$$

Define a generator matrix to be weight-retaining if it can be obtained from a monotonically weight-retaining matrix by permutation of rows. Theorem 2 gives some further properties of weight-retaining matrices.

Theorem 2: Let $G(D)$ be a generator matrix of an (n, k) convolutional code C with rows $\mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_k(D)$. Then the following statements are equivalent.

- $G(D)$ is a weight-retaining matrix for C .
- Given any other generator matrix $A(D)$ with rows $\mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_k(D)$ for C ,

$$\sum_{i=1}^k w[\langle \mathbf{g}_i(D) \rangle] \leq \sum_{i=1}^k w[\langle \mathbf{a}_i(D) \rangle].$$

- $s(G(D))_i = w[\langle \mathbf{g}_i(D) \rangle], \forall 1 \leq i \leq k$.

Proof:

a) \Rightarrow b): Suppose that $G(D)$ satisfies Statement a). Without loss of generality, assume that $G(D)$ is monotonically weight-retaining. Suppose there exists a generator matrix $A(D)$ for C with nondecreasingly ordered $(w[\langle \mathbf{a}_1(D) \rangle], w[\langle \mathbf{a}_2(D) \rangle], \dots, w[\langle \mathbf{a}_k(D) \rangle])$ such that $\sum_{i=1}^k w[\langle \mathbf{g}_i(D) \rangle] \not\leq \sum_{i=1}^k w[\langle \mathbf{a}_i(D) \rangle]$. Let i be the smallest integer in $\{1, 2, \dots, k\}$ such that $w[\langle \mathbf{g}_i(D) \rangle] > w[\langle \mathbf{a}_i(D) \rangle]$. Set $\rho = w[\langle \mathbf{g}_i(D) \rangle]$. Since $w[\langle \mathbf{a}_1(D) \rangle] \leq w[\langle \mathbf{a}_2(D) \rangle] \leq \dots \leq w[\langle \mathbf{a}_i(D) \rangle] < \rho$ and $w[C \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle] = \rho$, it follows that $\langle \mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_i(D) \rangle \subseteq \langle C^\rho \rangle$ and $\langle C^\rho \rangle \subseteq \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle$, which implies $i \leq \dim\langle C^\rho \rangle \leq i-1$. A contradiction is thus reached, and we should have $\sum_{i=1}^k w[\langle \mathbf{g}_i(D) \rangle] \leq \sum_{i=1}^k w[\langle \mathbf{a}_i(D) \rangle]$.

b) \Rightarrow c): Suppose $G(D)$ is a generator matrix for C such that Statement c) does not hold for $G(D)$. Then, there exists an integer $i \in \{1, 2, \dots, k\}$ such that $s(G(D))_i \neq w[\langle \mathbf{g}_i(D) \rangle]$. Let $\mathbf{c}(D) \in C \setminus \langle G(D) \setminus \mathbf{g}_i(D) \rangle$ such that $w(\mathbf{c}(D)) = s(G(D))_i$.

It can then be shown that $w(\mathbf{c}(D)) < w[\langle \mathbf{g}_i(D) \rangle]$ and $(\mathbf{g}_1^T(D) \cdots \mathbf{g}_{i-1}^T(D) \mathbf{c}^T(D) \mathbf{g}_{i+1}^T(D) \cdots \mathbf{g}_k^T(D))^T$ forms a generator matrix for C . Therefore, we have

$$\sum_{l=1}^k w[\langle \mathbf{g}_l(D) \rangle] > \sum_{l=1}^{i-1} w[\langle \mathbf{g}_l(D) \rangle] + w[\langle \mathbf{c}(D) \rangle] + \sum_{l=i+1}^k w[\langle \mathbf{g}_l(D) \rangle]$$

and $G(D)$ does not satisfy Statement b).

c) \Rightarrow a): Assume that $G(D)$ satisfies Statement c). Suppose $A(D)$ is a generator matrix obtained from $G(D)$ by permuting the rows of $G(D)$ such that $(w[\langle \mathbf{a}_1(D) \rangle], w[\langle \mathbf{a}_2(D) \rangle], \dots, w[\langle \mathbf{a}_k(D) \rangle])$ is nondecreasingly ordered. Clearly, $A(D)$ satisfies Statement c) and $s(A(D))_1 \leq s(A(D))_2 \leq \dots \leq s(A(D))_k$. Then, Lemma 1 implies $w[\langle \mathbf{a}_1(D) \rangle] = w[C]$ and $w[\langle \mathbf{a}_i(D) \rangle] = w[C \setminus \langle \mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_{i-1}(D) \rangle]$, $\forall 1 < i \leq k$. $A(D)$ is hence monotonically weight-retaining, which implies that $G(D)$ is weight-retaining. \square

By Theorems 1 and 2, we can further obtain that a weight-retaining matrix is an optimal generator matrix.

Corollary 2: Every weight-retaining generator matrix for an (n, k) convolutional code C is an optimal generator matrix for C .

Proof: Suppose $G(D)$ is a weight-retaining generator matrix for C . By Theorem 2, there exists a monotonically weight-retaining generator matrix $A(D)$ whose rows are a permutation of rows of $G(D)$. Denote by $\mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_k(D)$ the rows of $A(D)$. Let $\rho \in w(C)$ and set $X(D) = \{\mathbf{a}_i(D) : w[\langle \mathbf{a}_i(D) \rangle] < \rho\}$. It is clear that $\langle X(D) \rangle \subseteq \langle C^\rho \rangle$. Moreover, there exists an integer $l \in \{1, 2, \dots, k\}$ such that $X(D) = \{\mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_l(D)\}$. If $l = k$, then $\langle X(D) \rangle = C$ and, hence, $C^\rho \subseteq \langle X(D) \rangle$. If $1 \leq l < k$, then $w[C \setminus \langle X(D) \rangle] = w[\langle \mathbf{a}_{l+1}(D) \rangle] \geq \rho$ and, thus, we have $C^\rho \subseteq \langle X(D) \rangle$. Since $\langle X(D) \rangle = \langle C^\rho \rangle$, it also implies the UEP optimality of both $A(D)$ and $G(D)$. \square

By Corollary 2 and Statement b) in Theorem 2, Procedure 1 is proposed for obtaining a monotonically weight-retaining (and hence optimal) PGM for a given convolutional code.

Procedure 1:

- Step 1) Given an (n, k) convolutional code C , choose a polynomial codeword $\mathbf{g}_1(D)$ such that $w(\mathbf{g}_1(D)) = w[C]$. Set $i = 2$. If $i > k$, go to Step 5; else go to the next step.
- Step 2) Choose a polynomial codeword $\mathbf{c}(D) \in C \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle$ such that

$$w(\mathbf{c}(D)) = w[C \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle].$$
- Step 3) Set $\mathbf{g}_i(D) = \mathbf{c}(D)$.
- Step 4) If $i < k$, then replace i by $i + 1$ and go to Step 2; else go to the next step.
- Step 5) Set $G(D)$ to be the generator matrix of rows $\mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_k(D)$, which will be a desired optimal generator matrix for C .

B. Transformation Between Optimal Generator Matrices

To clarify the transformation between optimal generator matrices, consider a binary convolutional code which has an optimal generator matrix

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

with $\mathbf{s}(G(D)) = (2, 4, 6)$. Suppose we choose a transformation matrix

$$T_1(D) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

which is lower triangular; the resulting generator matrix $T_1(D)G(D)$ is still optimal. However, if the following non-lower triangular matrix is selected:

$$T_2(D) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

we have $\mathbf{s}(T_2(D)G(D)) = (2, 2, 2)$ and the optimality is destroyed. Such an interesting observation motivates Lemma 2.

Lemma 2: Let $G(D)$ be an optimal generator matrix of an (n, k) convolutional code C with $\mathbf{s}(G(D))$ in the nondecreasing order, i.e., $s(G(D))_i \leq s(G(D))_j$, $\forall 1 \leq i \leq j \leq k$. For any $k \times k$ nonsingular lower triangular matrix $T(D)$ over $F(D)$, $T(D)G(D)$ is also optimal.

Proof: Denote by $t_{ij}(D)$ the (i, j) th entry of $T(D)$, $\forall 1 \leq i, j \leq k$; we have $t_{ij}(D) = 0$, $\forall 1 \leq i < j \leq k$, since $T(D)$ is lower triangular. Let $G'(D) = T(D)G(D)$, and denote the rows of $G(D)$ and $G'(D)$ by $\mathbf{g}_i(D)$'s and $\mathbf{g}'_i(D)$'s, $\forall 1 \leq i \leq k$, respectively. Since $T(D)$ is nonsingular, it implies that

$$\langle \mathbf{g}'_1(D), \mathbf{g}'_2(D), \dots, \mathbf{g}'_i(D) \rangle = \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_i(D) \rangle$$

$\forall 1 \leq i \leq k$, and thus

$$\langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle \subseteq \langle G'(D) \setminus \mathbf{g}'_i(D) \rangle, \quad \forall 1 < i \leq k. \quad (5)$$

By (2), (3) and (5), it follows that

$$\begin{aligned} s(G'(D))_i &\geq w[C \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle] \\ &= s(G(D))_i, \quad \forall 1 \leq i \leq k. \end{aligned} \quad (6)$$

However, since $G(D)$ is optimal, we have $\mathbf{s}(G(D)) \geq \mathbf{s}(G'(D))$; together with (6), it hence implies that $\mathbf{s}(G(D)) = \mathbf{s}(G'(D))$ and $G'(D) = T(D)G(D)$ is also optimal. \square

By extending the concept of a lower triangular matrix, an effective lower triangular matrix is defined as follows.

Definition 8: Let $G(D)$ be a generator matrix of an (n, k) convolutional code. Without loss of generality, assume $\mathbf{s}(G(D))$ is in the nondecreasing order and has α different component values, each with β_i repetitions, $\forall 1 \leq i \leq \alpha$. For a $k \times k$ matrix

Since $G(D)$ is of full rank, $\Gamma(D)$ and its inverse $\Gamma^{-1}(D)$ are both nonsingular lower triangular matrices over $F(D)$. Thus, $G_b(D)(= \Gamma^{-1}(D)G(D))$ is a generator matrix for C . Then, by Lemma 2, $\mathbf{s}(G_b(D)) = \mathbf{s}(\Gamma^{-1}(D)G(D)) = \mathbf{s}(G(D))$. Hence, $G_b(D)$ is optimal. Let $\Psi'(D)$ be the $n \times k$ matrix formed by the first k columns of $\Psi(D)$. Since $\Psi^{-1}(D)\Psi(D) = I_n$, we have $G_b(D)\Psi'(D) = I_k$, which implies $G_b(D)$ is basic [39]. Therefore, $G(D)$ is successfully transformed into a PGM $G_b(D)$ which is optimal and basic, and we have the following theorem.

Theorem 4: Every convolutional code has at least an optimal PGM which is also basic and hence noncatastrophic.

Remark: This theorem was proposed previously in [31, Section 11.3], but no detailed proof was given.

Example 1: Consider a binary convolutional code C with a canonical generator matrix

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

which has the separation vector $\mathbf{s}(G_1(D)) = (2, 2, 4)$. After Procedure 1, we obtain a monotonically weight-retaining and hence optimal PGM

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

with the separation vector increased to $\mathbf{s}(G_2(D)) = (2, 4, 6)$. Furthermore, by (10), we have

$$G_2(D)\Psi(D) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1+D^2+D^3+D^4+D^5 & D^2 & 0 \end{pmatrix}$$

where

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

and, hence

$$\Psi^{-1}(D) = \begin{pmatrix} 0 & 1 & 0 & D \\ D^2 & 0 & 1+D^2 & D \\ \sum_{i=0}^5 D^i & 0 & D+D^4+D^5 & 1+D^3+D^4 \\ D+D^2+D^4 & 0 & D+D^4 & 1+D^3 \end{pmatrix}.$$

Therefore, the basic generator matrix consisting of the first 3 rows of $\Psi^{-1}(D)$ is

$$G_b(D) = \begin{pmatrix} 0 & 1 & 0 & D \\ D^2 & 0 & 1+D^2 & D \\ \sum_{i=0}^5 D^i & 0 & D+D^4+D^5 & 1+D^3+D^4 \end{pmatrix}$$

which is also an optimal PGM for C . \square

Remark: Note that there existed UEP results for linear block codes [4], [5] parallel to Lemma 1 and all those in Section III-A

except Corollary 1. The transformation between optimal generator matrices by the effectively lower triangular matrices defined in Section III-B is also similar to that between the canonical-form generator matrices for linear UEP block codes [2]. Not only for convolutional codes, in fact it can be shown that Lemma 1, all the UEP results in Section III-A, Lemma 2, and Theorem 3 hold for all linear codes.

IV. RELATION BETWEEN UEP CAPABILITY AND COMPLEXITY OF CONVOLUTIONAL ENCODERS

In Example 1, $G_1(D)$ is transformed into $G_b(D)$ to achieve the optimal UEP performance but at the cost of increasing the external degree from $\text{extdeg}(G_1(D)) = 4$ to $\text{extdeg}(G_b(D)) = 8$. For a PGM, the external degree corresponds to the number of memory elements in its direct-form realization, which dominates the complexity of building the encoder and conducting the Viterbi algorithm. To reduce the hardware/computation complexity while maintain the optimal UEP capability, it is desirable to find an optimal generator matrix which is also canonical or minimal (hence with the minimum degree) for encoding. However, the following example shows that in general there may not exist such a desirable matrix for every convolutional code.

Example 2: Consider a convolutional code C generated by the following canonical PGM:

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

which has $\mathbf{s}(G_1(D)) = (2, 2, 2)$ and $\deg(C) = 2$. By Procedure 1, we obtain an optimal PGM

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

with $\mathbf{s}(G_2(D)) = (2, 2, 3)$, $\text{extdeg}(G_2(D)) = 4$, and the McMillan degree = 3. Obviously, $G_2(D)$ is neither canonical nor minimal, since its external degree and McMillan degree are larger than $\deg(C)$. As a result of [45], there are only a finite number of minimal generator matrices for a convolutional code. Evaluating all the minimal generator matrices for C shows that all of them have separation vectors equal to $(2, 2, 2)$ ($\neq (2, 2, 3)$), and hence no minimal generator matrix is optimal. Since every canonical PGM is also minimal, it indicates that for C there exists no optimal generator matrix which is also canonical or minimal. \square

Since there is no guarantee that an optimal generator matrix can always achieve the degree of the code, the tradeoff between the complexity and UEP capability can then be tackled from two aspects. On the one hand, we can keep the UEP optimality of a generator matrix and try to minimize the corresponding complexity requirement. On the other hand, we can optimize the UEP capability of a generator matrix while still keep the minimal complexity. In the following, we first characterize the PGMs for which the external degree is as small as possible among all optimal generator matrices.

A. Optimal Generator Matrix With Lowest External Degree

For a convolutional code C , define $\mathcal{G}_o(C)$ to be the set of all optimal generator matrices and $\mathcal{G}_{mo}(C)$ to be the set of the optimal PGMs with the smallest external degree among $\mathcal{G}_o(C)$. Let $\rho(C) = \{\rho_1, \rho_2, \dots, \rho_l\}$ be a set of integers such that $\dim\langle C^{\rho_i} \rangle - \dim\langle C^{\rho_{i-1}} \rangle > 0, \forall 1 \leq i \leq l$, and $\langle C^{\rho_l} \rangle = C$. For convenience, define $\langle C^{\rho_0} \rangle = \emptyset$. The subcodes $\langle C^{\rho_1} \rangle, \langle C^{\rho_2} \rangle, \dots, \langle C^{\rho_l} \rangle$ of C are independent of the choice of generator matrices and have the property that $\langle C^{\rho_1} \rangle \subset \langle C^{\rho_2} \rangle \subset \dots \subset \langle C^{\rho_l} \rangle = C$.

Theorem 5: Let $G(D)$ be a PGM of an (n, k) convolutional code C with $\rho(C) = \{\rho_1, \rho_2, \dots, \rho_l\}$; then $G(D) \in \mathcal{G}_{mo}(C)$ if and only if, $\forall 1 \leq i \leq l$,

- a) there exists $X^{\rho_i}(D) \subseteq G(D)$ such that $\langle X^{\rho_i}(D) \rangle = \langle C^{\rho_i} \rangle$, and
- b) the generator matrix $X^{\rho_i}(D)$ for the subcode $\langle C^{\rho_i} \rangle$ has the smallest possible external degree given $X^{\rho_{i-1}}(D)$.

Proof: Condition a) obviously follows from Theorem 1. Let $G(D) \in \mathcal{G}_o(C)$ satisfying Condition b). Suppose $G(D) \notin \mathcal{G}_{mo}(C)$. Then, there exists a PGM $A(D) \in \mathcal{G}_o(C)$ such that $\text{extdeg}(A(D)) < \text{extdeg}(G(D))$. Let $Y^{\rho_j}(D) \subseteq A(D)$ such that $\langle Y^{\rho_j}(D) \rangle = \langle C^{\rho_j} \rangle, \forall 1 \leq j \leq l$. Clearly, $Y^{\rho_{j-1}}(D) \subset Y^{\rho_j}(D)$ and $X^{\rho_{j-1}}(D) \subset X^{\rho_j}(D)$. Denote by i the smallest integer in $\{1, 2, \dots, k\}$ satisfying $\text{extdeg}(Y^{\rho_i}(D)) < \text{extdeg}(X^{\rho_i}(D))$. Then, we have

$$\begin{aligned} \text{extdeg}(Y^{\rho_{i-1}}(D)) + \text{extdeg}(Y^{\rho_i}(D) \setminus Y^{\rho_{i-1}}(D)) \\ < \text{extdeg}(X^{\rho_{i-1}}(D)) + \text{extdeg}(X^{\rho_i}(D) \setminus X^{\rho_{i-1}}(D)) \end{aligned}$$

and hence

$$\text{extdeg}(Y^{\rho_i}(D) \setminus Y^{\rho_{i-1}}(D)) < \text{extdeg}(X^{\rho_i}(D) \setminus X^{\rho_{i-1}}(D)). \quad (11)$$

Let $Z^{\rho_i}(D) = X^{\rho_{i-1}}(D) \cup (Y^{\rho_i}(D) \setminus Y^{\rho_{i-1}}(D))$ which forms a basis of $\langle C^{\rho_i} \rangle$. Extend $Z^{\rho_i}(D)$ to a basis $B(D) = Z^{\rho_i}(D) \cup (G(D) \setminus X^{\rho_i}(D))$ of C . Clearly, $B(D)$ satisfies Condition a), but $\text{extdeg}(Z^{\rho_i}(D)) < \text{extdeg}(X^{\rho_i}(D))$ by (11), which contradicts Condition b) that $X^{\rho_i}(D)$ has the smallest external degree given $X^{\rho_{i-1}}(D)$. The assumption that $G(D) \notin \mathcal{G}_{mo}(C)$ is, hence, false.

Conversely, suppose $G(D) \in \mathcal{G}_{mo}(C)$. Assume that $G(D)$ does not satisfy Condition b) for some i . Then the external degree of $X^{\rho_i}(D)$ can be reduced, and it yields a generator matrix having external degree less than $G(D)$, thereby reaching a contradiction. \square

By Theorem 5, we have the following procedure for obtaining a PGM $G(D) \in \mathcal{G}_{mo}(C)$.

Procedure 2:

- Step 1) Given an convolutional code C with $\rho(C) = \{\rho_1, \rho_2, \dots, \rho_l\}$, find a least-degree codeword $\mathbf{g}_1(D) \in \langle C^{\rho_1} \rangle$.
- Step 2) Set $i = 1, j = 1$, and $r = 2$. Go to Step 5.
- Step 3) Find a least-degree codeword $\mathbf{v}(D) \in \langle C^{\rho_i} \rangle \setminus \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{r-1}(D) \rangle$.
- Step 4) Set $\mathbf{g}_r(D) = \mathbf{v}(D)$ and $r = r + 1$.

Step 5) If $j < \dim\langle C^{\rho_i} \rangle - \dim\langle C^{\rho_{i-1}} \rangle$, then set $j = j + 1$ and go to Step 3; else set $j = 1$ and go to Step 6.

Step 6) If $i < l$, then set $i = i + 1$ and go to Step 3; else stop.

The subcodes $\langle C^{\rho_1} \rangle, \langle C^{\rho_2} \rangle, \dots, \langle C^{\rho_l} \rangle$ can be obtained from an arbitrary optimal generator matrix $G'(D)$ for C , e.g., the optimal generator matrix obtained by Procedure 1. Then, by Theorem 1, there exists $X^{\rho_i}(D) \subseteq G'(D)$ such that $\langle X^{\rho_i}(D) \rangle = \langle C^{\rho_i} \rangle, \forall 1 \leq i \leq l$.

Although Procedure 2 can be used to find an optimal PGM with the smallest external degree among all optimal generator matrices, there is no guarantee that the resulting optimal PGM is noncatastrophic. In the following, we turn to find an optimal PGM which is basic and with the external degree as small as possible. Based on Theorem 3, we can obtain the necessary and sufficient conditions for the transformation of basic and optimal PGMs in Corollary 3.

Corollary 3: Let $G(D)$ be a basic and optimal generator matrix of an (n, k) convolutional code C . For a $k \times k$ nonsingular matrix $T(D)$ over $F(D)$, $T(D)G(D)$ is also basic and optimal if and only if

- a) $T(D)$ is unimodular, and
- b) $T(D)$ is effectively lower triangular with respect to $G(D)$.

Proof: Let $\det(\cdot)$ be the determinant operator. Suppose $T(D)$ is unimodular; by definition, we have

$$\begin{aligned} \text{intdeg}(T(D)G(D)) &= \text{deg}(\det(T(D))) + \text{intdeg}(G(D)) \\ &= \text{intdeg}(G(D)) \end{aligned} \quad (12)$$

since $\det(T(D))$ is a nonzero element in F . Therefore, by Definition 1, $T(D)G(D)$ is also basic.

For the other direction, suppose $T(D)G(D)$ is basic. Since there always exists a polynomial right inverse for a basic generator matrix, it implies that $T(D)$ is also a polynomial matrix. Moreover, since $\text{intdeg}(T(D)G(D)) = \text{intdeg}(G(D))$ and $T(D)$ is nonsingular, by (12), we can have that $\det(T(D))$ is a nonzero element in F and thus $T(D)$ is unimodular. Finally, by Theorem 3, $T(D)$ is effectively lower triangular with respect to $G(D)$, thereby completing the proof. \square

Given an (n, k) convolutional code C with a basic and optimal PGM $G(D)$, suppose $\mathbf{s}(G(D))$ is in the nondecreasing order and of α distinct component values, each with β_i repetitions, $\forall 1 \leq i \leq \alpha$. By Corollary 3, the associated transformation matrix which can still keep the optimality and basic property of $G(D)$ must be of the following form:

$$T(D) = \begin{pmatrix} \Gamma_{1,1}(D) & 0 & \dots & 0 \\ \Gamma_{2,1}(D) & \Gamma_{2,2}(D) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \Gamma_{\alpha,1}(D) & \Gamma_{\alpha,2}(D) & \dots & \Gamma_{\alpha,\alpha}(D) \end{pmatrix} \quad (13)$$

where $\Gamma_{i,j}(D)$ is a $\beta_i \times \beta_j$ polynomial matrix, $\forall i, j$. Since $T(D)$ is unimodular and

$$\det(T(D)) = \det(\Gamma_{1,1}(D)) \det(\Gamma_{2,2}(D)) \dots \det(\Gamma_{\alpha,\alpha}(D))$$

$\Gamma_{i,i}(D)$'s should also be unimodular, $\forall 1 \leq i \leq \alpha$. Let $G'(D) = T(D)G(D)$ and denote the rows of $G'(D)$ and $G(D)$

by $\mathbf{g}'_i(D)$'s and $\mathbf{g}_i(D)$'s, $\forall 1 \leq i \leq k$, respectively. By (13), $\forall 1 \leq i \leq \alpha$, we have

$$\begin{pmatrix} \mathbf{g}'_{\mu+1}(D) \\ \mathbf{g}'_{\mu+2}(D) \\ \vdots \\ \mathbf{g}'_{\mu+\beta_i}(D) \end{pmatrix} = [\Gamma_{i,1}(D), \Gamma_{i,2}(D), \dots, \Gamma_{i,i}(D)] \begin{pmatrix} \mathbf{g}_1(D) \\ \mathbf{g}_2(D) \\ \vdots \\ \mathbf{g}_\nu(D) \end{pmatrix} \quad (14)$$

where $\mu = \sum_{r=1}^{i-1} \beta_r$ and $\nu = \sum_{r=1}^i \beta_r$. Under the constraint of (14), a procedure for obtaining a PGM with the smallest external degree among all the PGMs which are both basic and optimal is proposed here.

Procedure 3:

- Step 1) Given an (n, k) convolutional code C , find a generator matrix $G(D)$ which is basic and optimal based on the discussion in Section III. Suppose that $G(D)$ has rows $\mathbf{g}_i(D)$'s, $\forall 1 \leq i \leq k$, and $\mathbf{s}(G(D))$ is in the nondecreasing order of α distinct component values, each with β_i repetitions, $\forall 1 \leq i \leq \alpha$.
- Step 2) Set $l = 1$, $C^* = \emptyset$, and \hat{C} be the collection of all codewords whose degree is not more than $\text{extdeg}(G(D))$.
- Step 3) Choose β_l independent codewords, say $\mathbf{c}_1(D), \mathbf{c}_2(D), \dots, \mathbf{c}_{\beta_l}(D)$, of the smallest sum of degrees from \hat{C} which are independent to all codewords in C^* and satisfy the following constraints:

$$\begin{pmatrix} \mathbf{c}_1(D) \\ \mathbf{c}_2(D) \\ \vdots \\ \mathbf{c}_{\beta_l}(D) \end{pmatrix} = [\Gamma_{l,1}(D), \Gamma_{l,2}(D), \dots, \Gamma_{l,l}(D)] \begin{pmatrix} \mathbf{g}_1(D) \\ \mathbf{g}_2(D) \\ \vdots \\ \mathbf{g}_\nu(D) \end{pmatrix}$$

where $\Gamma_{l,j}(D)$ is a $\beta_l \times \beta_j$ matrix over $F[D]$, $\forall 1 \leq j \leq l$, $\Gamma_{l,l}(D)$ is unimodular, and $\nu = \sum_{r=1}^l \beta_r$.

- Step 4) Set $C^* = C^* \cup \{\mathbf{c}_1(D), \mathbf{c}_2(D), \dots, \mathbf{c}_{\beta_l}(D)\}$ and $\hat{C} = \hat{C} \setminus \{\mathbf{c}_1(D), \mathbf{c}_2(D), \dots, \mathbf{c}_{\beta_l}(D)\}$.
- Step 5) If $l < \alpha$, then replace l by $l+1$ and go to Step 3; else go to the next step.
- Step 6) Set $G^*(D)$ to be the generator matrix whose rows consist of all codewords in C^* , which will be a desired basic and optimal PGM of the smallest external degree.

Since the degree of each row of $G^*(D)$ never exceeds $\text{extdeg}(G(D))$, the initialization of \hat{C} in Step 2 and the constraints on choosing $\mathbf{c}_1(D), \mathbf{c}_2(D), \dots, \mathbf{c}_{\beta_l}(D)$ in Step 3 can guarantee the correctness of Procedure 3. Moreover, owing to the finite cardinality of \hat{C} , Procedure 3 can be finished in finite steps.

Example 3: Consider the convolutional code in Example 1. By Procedure 3, $G_b(D)$ is converted to the following basic and optimal PGM:

$$G^*(D) = \begin{pmatrix} 0 & 1 & 0 & D \\ D^2 & 0 & 1+D^2 & D \\ 1+D & D & 1 & 1+D \end{pmatrix}.$$

Then, a reduction of 4 in the external degree is obtained. Moreover, since $\text{extdeg}(G^*(D))$ is the same as the degree of the code, it implies that $G^*(D)$ achieves both of the optimal UEP capability and the lowest complexity requirement in this case. \square

B. Relation Between Optimal and Canonical Generator Matrices

In Section IV-B, the discussion is concerned with minimizing the external degree of a basic and optimal PGM. For further investigation of the UEP optimality and canonicity of generator matrices, we are now interested in how much the separation vector can be increased as the generator matrix is required to be canonical. First, if there exists a canonical PGM which has the greatest separation vector among all canonical PGMs, the corresponding necessary and sufficient condition is given in Theorem 6.

Theorem 6: Consider an (n, k) convolutional code C . Without loss of generality, assume the following generator matrices of C are nondecreasingly ordered in terms of their separation vectors. A canonical generator matrix $G(D)$ with rows $\mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_k(D)$ has the greatest separation vector among all canonical generator matrices if and only if, $\forall \rho \in w(C)$, for any canonical generator matrix $A(D)$ with rows $\mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_k(D)$ satisfying $\langle C^\rho \rangle \subseteq \langle \mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_i(D) \rangle$ for some i , we have $\langle C^\rho \rangle \subseteq \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_i(D) \rangle$.

Proof: Suppose $G(D)$ satisfies the condition but $G(D)$ does not have the greatest separation vector, i.e., there exist a canonical generator matrix $A(D)$ such that, for some i , $s(A(D))_j \leq s(G(D))_j$, $\forall j < i$, and $s(A(D))_i > s(G(D))_i$. Since $s(A(D))_i > s(G(D))_i$, it implies that

$$\langle C^{s(A(D))_i} \rangle \subseteq \langle \mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_{i-1}(D) \rangle$$

and

$$\langle C^{s(A(D))_i} \rangle \not\subseteq \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle$$

thereby contradicting the condition.

For the reverse direction, suppose $G(D)$ does not satisfy the condition; it implies that $\exists \rho \in w(C)$ and $A(D)$ such that $\langle C^\rho \rangle \subseteq \langle \mathbf{a}_1(D), \mathbf{a}_2(D), \dots, \mathbf{a}_{i-1}(D) \rangle$ but $\langle C^\rho \rangle \not\subseteq \langle \mathbf{g}_1(D), \mathbf{g}_2(D), \dots, \mathbf{g}_{i-1}(D) \rangle$ for some i . It is clear that $s(A(D))_i \geq w[C \setminus \langle C^\rho \rangle] \geq \rho$ and $s(G(D))_i < \rho$. Therefore, we have $s(A(D))_i > s(G(D))_i$, and $G(D)$ does not have the greatest separation vector. \square

Aided with Theorem 6 and Lemma 1, we further propose Lemma 3 and Theorem 7 to demonstrate the existence of a canonical PGM with the greatest separation vector among all canonical PGMs for every convolutional code.

Lemma 3: Consider an (n, k) convolutional code C . For ρ_1 and $\rho_2 \in w(C)$ with $\langle C^{\rho_1} \rangle \subset \langle C^{\rho_2} \rangle$, if there exist two canonical generator matrices

$$A(D) = \begin{pmatrix} G_1^T(D) & G_1'^T(D) \end{pmatrix}^T$$

and

$$B(D) = \begin{pmatrix} G_2^T(D) & G_2'^T(D) \end{pmatrix}^T$$

where, for $i = 1$ and 2 , $G_i(D)$ and $G'_i(D)$ denote two $k_i \times n$ and $(k - k_i) \times n$ matrices, respectively, with $1 \leq k_1 < k_2 \leq k$ satisfying $\langle G_1(D) \rangle = \langle C^{\rho_1} \rangle$ and $\langle G_2(D) \rangle = \langle C^{\rho_2} \rangle$, then we can always choose a $(k_2 - k_1) \times n$ matrix $G_2^*(D)$ with rows in $G_2(D)$ such that

$$\left(G_1^T(D) \ G_2^{*T}(D) \ G_2'^T(D) \right)^T \quad (15)$$

forms another canonical generator matrix for C .

Proof: For $i = 1$ and 2 , denote the rows of $G_i(D)$ by $\mathbf{g}_j^{(i)}(D)$'s, $\forall 1 \leq j \leq k_i$, respectively. Since $\langle C^{\rho_1} \rangle \subset \langle C^{\rho_2} \rangle$, we can choose k_1 rows from $G_2(D)$ such that $\mathbf{g}_{m_i}^{(2)}(D) = \mathbf{g}_i^{(1)}(D) + \mathbf{v}_i(D)$ where $m_i \in \{1, 2, \dots, k_2\}$ and $\mathbf{v}_i(D) \in \langle C^{\rho_2} \rangle$, $\forall 1 \leq i \leq k_1$, and the remaining rows of $G_2(D)$ are in $\langle C^{\rho_2} \rangle \setminus \langle C^{\rho_1} \rangle$. Let

$$E_1 = \deg(\mathbf{g}_1^{(1)}(D)) + \deg(\mathbf{g}_2^{(1)}(D)) + \dots + \deg(\mathbf{g}_{k_1}^{(1)}(D))$$

and

$$E_2 = \deg(\mathbf{g}_{m_1}^{(2)}(D)) + \deg(\mathbf{g}_{m_2}^{(2)}(D)) + \dots + \deg(\mathbf{g}_{m_{k_1}}^{(2)}(D)).$$

If $E_1 = E_2$, $G_2^*(D)$ can be obtained by deleting the k_1 rows $\mathbf{g}_{m_i}^{(2)}(D)$'s from $G_2(D)$. Denote by $\hat{G}(D)$ the matrix in (15). Then $\hat{G}(D)$ is of full rank because all rows of $G_2^*(D)$ are in $\langle C^{\rho_2} \rangle \setminus \langle C^{\rho_1} \rangle$. We also have $\text{extdeg}(\hat{G}(D)) = \text{extdeg}(B(D))$ since $E_1 = E_2$. It thus implies the canonicity of $\hat{G}(D)$.

Suppose we now have $E_1 > E_2$. Then, rows of $G_1(D)$ can be replaced by $\mathbf{g}_{m_i}^{(2)}(D)$'s to obtain the matrix:

$$\left(\mathbf{g}_{m_1}^{(2)T}(D) \ \mathbf{g}_{m_2}^{(2)T}(D) \ \dots \ \mathbf{g}_{m_{k_1}}^{(2)T}(D) \ G_1'^T(D) \right)^T$$

which is of full rank and has the external degree less than $\text{extdeg}(A(D))$, hence, contradicting the canonicity of $A(D)$. For the remaining case that $E_1 < E_2$, with the same choice of $G_2^*(D)$ as in the case that $E_1 = E_2$, the matrix of the form in (15) is of full rank and with the external degree less than $\text{extdeg}(B(D))$, which also contradicts the assumption that $B(D)$ is canonical, thereby completing the proof. \square

Theorem 7: For every convolutional code, there always exists a canonical generator matrix which has the greatest separation vector among all canonical generator matrices.

Proof: Consider an (n, k) convolutional code C of free distance d_f . To avoid possible ambiguity, ρ^* is referred to $\max_{\rho \in w(C)} \{\rho : \langle C^\rho \rangle = \langle C^{\rho^*} \rangle\}$ as $\langle C^{\rho^*} \rangle$ is mentioned. Consider the set $\{\langle C^{\rho_i} \rangle : \forall 1 \leq i \leq M\}$ containing all the nonempty $\langle C^\rho \rangle$'s which can be spanned by rows of canonical generator matrices except $\langle C^{d_f} \rangle$ consisting of only the all-zero codeword. Without loss of generality, assume that $\rho_1 < \rho_2 < \dots < \rho_M$ and $\langle C^{\rho_i} \rangle = \langle G_i(D) \rangle$, $\forall 1 \leq i \leq M$, where $G_i(D)$ is a $k_i \times n$ submatrix of the canonical generator matrix $\left(G_1^T(D) \ G_2^T(D) \right)^T$; it implies that $\langle C^{\rho_M} \rangle = C$, $k_M = k$, and $\rho_M = \infty$. For any canonical generator matrix $G(D)$, by Theorem 6, we have

$$(d_f, \dots, d_f, \rho_1, \dots, \rho_1, \dots, \rho_{M-1}, \dots, \rho_{M-1}) \geq \phi(\mathbf{s}(G(D))) \quad (16)$$

where ϕ denotes a proper permutation of vector components, d_f has k_1 repetitions, and ρ_i has $k_{i+1} - k_i$ repetitions, $\forall 1 \leq i < M$.

By Lemma 3, it implies that there exists a PGM $G_{i+1}^*(D) \subset G_{i+1}(D)$ such that $(G_i^T(D) \ G_{i+1}^{*T}(D) \ G_{i+1}'^T(D))^T$ is canonical, $\forall 1 \leq i < M$. Repeating the above process with respect to $G_2(D), G_3(D), \dots, G_M(D)$ successively, we can obtain the following canonical PGM $G^*(D)$:

$$\left(G_1^T(D) \ G_2^{*T}(D) \ \dots \ G_M^{*T}(D) \right)^T$$

with

$$\mathbf{s}(G^*(D)) = (d_f, \dots, d_f, \rho_1, \dots, \rho_1, \dots, \rho_{M-1}, \dots, \rho_{M-1})$$

since $\langle C^{\rho_1} \rangle \subset \langle C^{\rho_2} \rangle \subset \dots \subset \langle C^{\rho_M} \rangle$. By (16), $G^*(D)$ is, therefore, a desired canonical generator matrix which has the greatest separation vector among all canonical generator matrices. \square

Since the constructive proof of Theorem 7 can be employed to produce a canonical PGM with the greatest separation vectors among all canonical matrices, a ready-made search procedure will be available as long as we can find all the $\langle C^\rho \rangle$'s which can be spanned by canonical PGMs. In the following, a necessary and sufficient condition is first presented to test whether $\langle C^\rho \rangle$ can be spanned by a canonical PGM. Based on Theorem 7 and Lemma 4, Procedure 4 is then proposed for construction of a canonical PGM with the best UEP capability.

Lemma 4: Consider an (n, k) convolutional code C with an optimal generator matrix $G(D)$. For $\rho \in w(C)$, let $X(D) \subseteq G(D)$ with $\langle X(D) \rangle = \langle C^\rho \rangle$. Let the dimension of $\langle C^\rho \rangle$ be k' . Then $\langle C^\rho \rangle$ is canonically splittable, i.e., there exists a canonical generator matrix $G^*(D)$ and $X^*(D) \subseteq G^*(D)$ such that $\langle X^*(D) \rangle = \langle C^\rho \rangle$, if and only if, for the $k - k'$ codewords of C with the smallest sum of degrees, say $\mathbf{c}_1(D), \mathbf{c}_2(D), \dots, \mathbf{c}_{k-k'}(D)$, which make the matrix $(X^T(D) \ \mathbf{c}_1^T(D) \ \mathbf{c}_2^T(D) \ \dots \ \mathbf{c}_{k-k'}^T(D))^T$ full-rank, we have

$$\deg(\langle X(D) \rangle) + \sum_{t=1}^{k-k'} \deg(\mathbf{c}_t(D)) = \deg(C). \quad (17)$$

Proof: If the condition holds, we first convert $X(D)$ to a canonical generator matrix $X^*(D)$ for $\langle C^\rho \rangle$ by a standard procedure to produce canonical generator matrices [39] and set

$$G^*(D) = \left(X^{*T}(D) \ \mathbf{c}_1^T(D) \ \mathbf{c}_2^T(D) \ \dots \ \mathbf{c}_{k-k'}^T(D) \right)^T.$$

Then $G^*(D)$ is canonical since $\text{extdeg}(X^*(D)) = \deg(\langle X(D) \rangle)$ and $\text{extdeg}(G^*(D)) = \deg(C)$ by (17). It follows that $\langle C^\rho \rangle$ is canonically splittable.

For the reverse direction, suppose $\langle C^\rho \rangle$ is canonically splittable, i.e., there exists a canonical generator matrix $G^*(D)$ with $X^*(D) \subseteq G^*(D)$ such that $\langle X^*(D) \rangle = \langle C^\rho \rangle$. Let $Y^*(D)$ denote the remaining submatrix of $G^*(D)$ by deleting $X^*(D)$. Since $G^*(D)$ is canonical, we have $\deg(\langle X(D) \rangle) = \text{extdeg}(X^*(D))$ and rows of $Y^*(D)$ are

qualified for the candidates of $\mathbf{c}_1(D), \mathbf{c}_2(D), \dots, \mathbf{c}_{k-k'}(D)$.

Therefore, it follows that

$$\begin{aligned} \deg(\langle X(D) \rangle) + \sum_{t=1}^{k-k'} \deg(\mathbf{c}_t(D)) \\ = \text{extdeg}(X^*(D)) + \text{extdeg}(Y^*(D)) \\ = \deg(C) \end{aligned}$$

which completes the proof. \square

Procedure 4:

- Step 1) Given an (n, k) convolutional code C , use Procedure 1 to generate an optimal generator matrix $G(D)$ of rows $\mathbf{g}_i(D)$'s, $\forall 1 \leq i \leq k$. Suppose that $\mathbf{s}(G(D))$ is in the nondecreasing order of α distinct component values s_i 's, each with β_i repetitions, $\forall 1 \leq i \leq \alpha$.
- Step 2) Set $i = 1$ and $M = 1$.
- Step 3) Let $X(D)$ be the $(\sum_{r=1}^i \beta_r) \times n$ matrix of rows $\mathbf{g}_t(D)$'s, $\forall 1 \leq t \leq \sum_{r=1}^i \beta_r$. Convert $X(D)$ to a canonical matrix, say $X^*(D)$, for $\langle C^{s_{i+1}} \rangle$, and choose $\sum_{r=i+1}^{\alpha} \beta_r$ codewords of C , say $\mathbf{c}_1(D), \mathbf{c}_2(D), \dots, \mathbf{c}_z(D)$, where $z = \sum_{r=i+1}^{\alpha} \beta_r$, with the smallest sum of degrees such that the matrix

$$\left(X^{*T}(D) \ \mathbf{c}_1^T(D) \ \mathbf{c}_2^T(D) \ \dots \ \mathbf{c}_z^T(D) \right)^T$$

is of full rank.

- Step 4) If $\text{extdeg}(X^*(D)) + \sum_{t=1}^z \deg(\mathbf{c}_t(D)) = \deg(C)$, then set $G_M(D) = X^*(D)$ and replace M by $M + 1$.
- Step 5) If $i < \alpha - 1$, then replace i by $i + 1$ and go to Step 3; else convert $G(D)$ to a canonical matrix and assign it to $G_M(D)$. Let the rank of $G_i(D)$ be k_i and denote rows of $G_i(D)$ by $\mathbf{g}_j^{(i)}(D)$'s, $\forall 1 \leq i \leq M$ and $1 \leq j \leq k_i$.
- Step 6) Set $i = 2$ and initialize $G^*(D)$ by $G_1(D)$.
- Step 7) Choose k_{i-1} rows $\mathbf{g}_{m_t}^{(i)}(D)$'s from $G_i(D)$, where $m_t \in \{1, 2, \dots, k_i\}$, $\forall 1 \leq t \leq k_{i-1}$, such that remaining rows of $G_i(D)$ are in $\langle G_i(D) \rangle \setminus \langle G^*(D) \rangle$.
- Step 8) Replace $\mathbf{g}_{m_t}^{(i)}(D)$'s in $G_i(D)$ by all rows in $G^*(D)$ and assign the resulting $G_i(D)$ to $G^*(D)$.
- Step 9) If $i < M$, then replace i by $i + 1$ and go to Step 7; else stop and $G^*(D)$ will be a desired canonical generator matrix of the greatest separation vector for C .

In Steps 3 and 4, it is checked whether $\langle C^\rho \rangle$ is canonically splittable or not. Since all $\langle C^\rho \rangle$'s can be specified by an optimal generator matrix by Theorem 1, we never miss any $\langle C^\rho \rangle$ which is canonically splittable after the search in Steps 1 to 5. Also by the constraints on producing $G^*(D)$ in Step 7, the correctness of Procedure 4 is therefore guaranteed.

Example 4: Consider the convolutional code C in Example 1 with an optimal generator matrix $G_2(D)$ of $\mathbf{s}(G_2(D)) = (2, 4, 6)$ and $\text{extdeg}(G_2(D)) = 7$. We have

$$\langle C^1 \rangle = \langle C^2 \rangle = \langle (0 \ 0 \ 0 \ 0) \rangle$$

$$\begin{aligned} \langle C^3 \rangle = \langle C^4 \rangle &= \langle (0 \ 1 \ 0 \ D) \rangle \\ \langle C^5 \rangle = \langle C^6 \rangle &= \left\langle \begin{pmatrix} 0 & 1 & 0 & D \\ D^2 & 1 & 1+D^2 & 0 \end{pmatrix} \right\rangle \\ \langle C^7 \rangle = \langle C^8 \rangle &= \dots = C \\ &= \left\langle \begin{pmatrix} 1+D & 1+D & 1 & 1 \\ 1+D & D & 1 & 1+D \\ 1+D+D^2 & D & D^2 & 1 \end{pmatrix} \right\rangle. \end{aligned}$$

By Lemma 4, it follows that $\langle C^4 \rangle$, $\langle C^6 \rangle$, and C are canonically splittable. By Procedure 4, $G^*(D)$ is updated as follows:

$$\begin{aligned} G^*(D) : (0 \ 1 \ 0 \ D) \\ \Rightarrow \begin{pmatrix} 0 & 1 & 0 & D \\ D^2 & 1 & 1+D^2 & 0 \end{pmatrix} \\ \Rightarrow \begin{pmatrix} 0 & 1 & 0 & D \\ D^2 & 1 & 1+D^2 & 0 \\ 1+D & 1+D & 1 & 1 \end{pmatrix}. \end{aligned}$$

Since $\mathbf{s}(G^*(D)) = (2, 4, 6)$, in this case, the resulting canonical PGM is also optimal but with the external degree reduced to 4. \square

C. Relation Between Optimal and Systematic Generator Matrices

Systematic generator matrices which inherit the lowest McMillan degree and the noncatastrophic property of minimal generator matrices and possess the advantage of easy inversion of the encoder operation have been extensively employed for encoding of convolutional codes in various applications. To optimize the UEP performance by systematic encoding, we intend to find a systematic generator matrix which has the greatest separation vector among all systematic matrices. However, as shown in Example 5, we observe that there may not exist a systematic generator matrix which is also optimal for every convolutional code.

Example 5: Consider the convolutional code C in Example 1 with the optimal separation vector $(2, 4, 6)$. By exhaustive search, there are four kinds of systematic generator matrices for C :

$$\begin{aligned} G_1(D) &= \begin{pmatrix} \frac{D+D^2+D^4}{1+D^3+D^4} & 1 & 0 & 0 \\ \frac{1+D+D^3}{1+D^3+D^4} & 0 & 0 & 1 \\ \frac{D+D^3+D^4}{1+D^3+D^4} & 0 & 1 & 0 \end{pmatrix} \\ G_2(D) &= \begin{pmatrix} 0 & 1 & 0 & D \\ 1 & 0 & 0 & \frac{1+D^3+D^4}{1+D+D^3} \\ 0 & 0 & 1 & \frac{D+D^3+D^4}{1+D+D^3} \end{pmatrix} \\ G_3(D) &= \begin{pmatrix} 1 & \frac{1+D^3+D^4}{D+D^2+D^4} & 0 & 0 \\ 0 & \frac{1}{D} & 0 & 1 \\ 0 & \frac{1+D^2+D^3}{1+D+D^3} & 1 & 0 \end{pmatrix} \\ G_4(D) &= \begin{pmatrix} 0 & 1 & \frac{1+D+D^3}{1+D^2+D^3} & 0 \\ 1 & 0 & \frac{1+D^3+D^4}{D+D^3+D^4} & 0 \\ 0 & 0 & \frac{1+D+D^3}{D+D^3+D^4} & 1 \end{pmatrix} \end{aligned}$$

without considering the possible permutation of rows and multiplication of scalars over $\text{GF}(2)(D)$. Since

$\mathbf{s}(G_i(D)) = (2, 4, 4), \forall 1 \leq i \leq 4$, none of the above systematic generator matrices is optimal. \square

Recall Theorem 6 which presents the necessary and sufficient condition of a canonical generator matrix with the greatest separation vector among all canonical matrices, where the canonicity of generator matrices is surprisingly not used throughout the proof. The same necessary and sufficient condition can then be combined with the following Lemma 5 to yield Theorem 8 for the existence of a systematic generator matrix with the greatest separation vector among all systematic generator matrices for a given code.

Lemma 5: Consider an (n, k) convolutional code C . For ρ_1 and $\rho_2 \in w(C)$ with $\langle C^{\rho_1} \rangle \subset \langle C^{\rho_2} \rangle$, if there exist two systematic generator matrices

$$\left(G_1^T(D) G_1'^T(D) \right)^T \text{ and } \left(G_2^T(D) G_2'^T(D) \right)^T$$

where, for $i = 1$ and 2 , $G_i(D)$ and $G_i'(D)$ denote two $k_i \times n$ and $(k - k_i) \times n$ matrices, respectively, with $1 \leq k_1 < k_2 \leq k$ satisfying $\langle G_1(D) \rangle = \langle C^{\rho_1} \rangle$ and $\langle G_2(D) \rangle = \langle C^{\rho_2} \rangle$, then there exists a $(k_2 - k_1) \times n$ matrix $G_2^{*T}(D) \subseteq G_2(D)$ and we can always choose $k_2 - k_1$ codewords, say $\mathbf{c}_1(D), \mathbf{c}_2(D), \dots, \mathbf{c}_{k_2-k_1}(D)$, generated by

$$\mathbf{c}_i(D) \in \left\langle \left(G_1^T(D) G_2^{*T}(D) \right)^T \right\rangle, \forall 1 \leq i \leq k_2 - k_1$$

such that the resulting matrix

$$\left(G_1^T(D) \mathbf{c}_1^T(D) \mathbf{c}_2^T(D) \cdots \mathbf{c}_{k_2-k_1}^T(D) \right)^T$$

forms a $k_2 \times n$ submatrix of a systematic generator matrix for C .

Proof: Without loss of generality, assume that $G_1(D)$ is of the following form:

$$G_1(D) = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & g_{1,k+1}(D) & \cdots & g_{1,n}(D) \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 & g_{2,k+1}(D) & \cdots & g_{2,n}(D) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 & g_{k_1,k+1}(D) & \cdots & g_{k_1,n}(D) \end{pmatrix} \quad (18)$$

where the left k_1 columns form the $k_1 \times k_1$ identity matrix followed by $k - k_1$ columns of all zero entries, and $g_{i,j}(D)$'s

$\in F(D)$; otherwise, a proper permutation of the components of every codeword can be conducted to make (18) valid. Arbitrarily choose a $(k_2 - k_1) \times n$ submatrix $G_2^{*T}(D)$ consisting of rows in $G_2(D)$ which are linearly independent of rows in $G_1(D)$. (This can always be done because $\langle C^{\rho_1} \rangle \subset \langle C^{\rho_2} \rangle$.) Using the standard procedure to make a generator matrix systematic, we can convert $\left(G_1^T(D) G_2^{*T}(D) \right)^T$ to

$$\left(G_1^T(D) \mathbf{c}_1^T(D) \mathbf{c}_2^T(D) \cdots \mathbf{c}_{k_2-k_1}^T(D) \right)^T$$

which forms a systematic generator matrix for $\langle C^{\rho_2} \rangle$, where

$$\mathbf{c}_i(D) \in \left\langle \left(G_1^T(D) G_2^{*T}(D) \right)^T \right\rangle, \forall 1 \leq i \leq k_2 - k_1.$$

Since $\langle G_1(D) \rangle \subset \langle G_2(D) \rangle$ and both of $G_1(D)$ and $G_2(D)$ are submatrices of systematic generator matrices for C , there are at least $k - k_2$ common columns of $G_1(D)$ and $G_2(D)$ which have all zero entries. Let $k' = k_2 - k_1$. Without loss of generality, the new obtained matrix can be written as shown in (19) at the bottom of the page where the left k_2 columns form the $k_2 \times k_2$ identity matrix, the columns with boldface zeros indicate the common columns of $G_1(D)$ and $G_2(D)$ mentioned above, and $c_{i,j}(D)$'s $\in F(D)$. Obviously, (19) is qualified for a submatrix of a systematic generator matrix for C , hence finishing the proof. \square

Theorem 8: For every convolutional code, there always exists a systematic generator matrix which has the greatest separation vector within the class of systematic generator matrices.

Proof: Following all the same terms defined in the proof of Theorem 7 except that the set $\{\langle C^{\rho_i} \rangle : 1 \leq i \leq M\}$ now contains all the nonempty $\langle C^{\rho} \rangle$'s which can be spanned by rows of systematic generator matrices of C , we continue the proof as follows. By Lemma 5, we can choose $k_2 - k_1$ codewords $\mathbf{c}_j^{(2)}(D)$'s, which are generated by

$$\mathbf{c}_j^{(2)}(D) \in \left\langle \left(G_1^T(D) G_2^{*T}(D) \right)^T \right\rangle, \forall 1 \leq j \leq k_2 - k_1$$

where $G_2^{*T}(D) \subseteq G_2(D)$, such that the resulting matrix

$$\hat{G}_2(D) = \left(G_1^T(D) \mathbf{c}_1^{(2)T}(D) \mathbf{c}_2^{(2)T}(D) \cdots \mathbf{c}_{k_2-k_1}^{(2)T}(D) \right)^T \quad (20)$$

forms a submatrix of a systematic generator matrix for C with $\langle G_1(D) \rangle = \langle C^{\rho_1} \rangle$ and $\langle \hat{G}_2(D) \rangle = \langle C^{\rho_2} \rangle$. Repeating the above procedure with respect to $G_3(D), G_4(D), \dots, G_M(D)$

$$\left(\begin{array}{cccccccccccc} 1 & \cdots & 0 & 0 & \cdots & 0 & \mathbf{0} & \cdots & \mathbf{0} & g_{1,k+1}(D) & \cdots & g_{1,n}(D) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 & \mathbf{0} & \cdots & \mathbf{0} & g_{k_1,k+1}(D) & \cdots & g_{k_1,n}(D) \\ \hline 0 & \cdots & 0 & 1 & \cdots & 0 & \mathbf{0} & \cdots & \mathbf{0} & c_{1,k+1}(D) & \cdots & c_{1,n}(D) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 1 & \mathbf{0} & \cdots & \mathbf{0} & c_{k',k+1}(D) & \cdots & c_{k',n}(D) \end{array} \right) \quad (19)$$

successively, we can obtain $\hat{G}_3(D), \hat{G}_4(D), \dots, \hat{G}_M(D)$ with $\langle \hat{G}_i(D) \rangle = \langle C^{\rho_i} \rangle$ and

$$\hat{G}_i(D) = \left(\hat{G}_{i-1}^T(D) \mathbf{c}_1^{(i)T}(D) \mathbf{c}_2^{(i)T}(D) \cdots \mathbf{c}_{k_i - k_{i-1}}^{(i)T}(D) \right)^T$$

where $\mathbf{c}_j^{(i)}(D)$'s are generated in a similar way to those in (20), $\forall 3 \leq i \leq M$. Since $\langle C^{\rho_1} \rangle \subset \langle C^{\rho_2} \rangle \subset \cdots \subset \langle C^{\rho_M} \rangle$, it implies that

$$\mathbf{s}(\hat{G}_M(D)) = (d_f, \dots, d_f, \rho_1, \dots, \rho_1, \dots, \rho_{M-1}, \dots, \rho_{M-1}).$$

Therefore, $\hat{G}_M(D)$ is a desired systematic generator matrix with the greatest separation vector. \square

Similar to the discussion in Section IV-C, the constructive proof of Theorem 8 can be employed to generate a systematic generator matrix with the largest separation vector as long as we can find all the $\langle C^\rho \rangle$'s which are spanned by systematic generator matrices. In Lemma 6, necessary and sufficient conditions are presented to check whether $\langle C^\rho \rangle$ can be spanned by a systematic generator matrix. Then, Procedure 5 is proposed for obtaining a systematic generator matrix with the best UEP capability.

Lemma 6: Consider an (n, k) convolutional code C with an optimal generator matrix $G(D)$. For $\rho \in w(C)$, let $X(D) \subseteq G(D)$ with $\langle X(D) \rangle = \langle C^\rho \rangle$, and denote by $Y(D)$ the matrix comprising the remaining rows of $G(D)$. Let the dimension of $\langle C^\rho \rangle$ be k' . Then $\langle C^\rho \rangle$ is systematically splittable, i.e., there exists a systematic generator matrix $G^*(D)$ and $X^*(D) \subseteq G^*(D)$ such that $\langle X^*(D) \rangle = \langle C^\rho \rangle$, if and only if the following conditions are satisfied:

- there exist at least $k - k'$ all-zero columns in $X(D)$, and
- there exist $k - k'$ columns of $Y(D)$ in the same positions as the all-zero columns of $X(D)$ which form a nonsingular matrix.

Proof: Suppose both Conditions a) and b) hold. On account of Condition a), without loss of generality, $X(D)$ can be converted to

$$X'(D) = \begin{pmatrix} 1 & \cdots & 0 & 0 & \cdots & 0 & x_{1,k+1}(D) & \cdots & x_{1,n}(D) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 & x_{k',k+1}(D) & \cdots & x_{k',n}(D) \end{pmatrix} \quad (21)$$

by proper row operations, where the left k' columns form the $k' \times k'$ identity matrix followed by $k - k'$ all-zero columns, and $x_{i,j}(D)$'s $\in F(D)$; otherwise, a proper permutation of the columns of $G(D)$ can be conducted to make (21) valid. Due to Condition b), by multiplying a proper transformation matrix, $Y(D)$ can also be transformed to

$$Y'(D) = \begin{pmatrix} 0 & \cdots & 0 & 1 & \cdots & 0 & y_{1,k+1}(D) & \cdots & y_{1,n}(D) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 1 & y_{k-k',k+1}(D) & \cdots & y_{k-k',n}(D) \end{pmatrix} \quad (22)$$

where the left k' columns are with zero entries followed the $(k - k') \times (k - k')$ identity matrix, and $y_{i,j}(D)$'s $\in F(D)$. Since $\langle X'(D) \rangle = \langle C^\rho \rangle$ and $\left(X'^T(D) Y'^T(D) \right)^T$ is systematic for C , $\langle C^\rho \rangle$ is hence systematically splittable.

For the reverse direction, suppose $\langle C^\rho \rangle$ is systematically splittable, i.e., there exists a systematic generator matrix $G^*(D)$ with a $k' \times n$ submatrix $X^*(D) \subseteq G^*(D)$ such that $\langle X^*(D) \rangle = \langle C^\rho \rangle$. Since $G^*(D)$ is systematic, there exist at least $k - k'$ columns of $X^*(D)$ which are of all zero entries. If a codeword $\mathbf{c}(D)$ is generated by $\mathbf{c}(D) \in \langle X^*(D) \rangle$, at least $k - k'$ components of $\mathbf{c}(D)$ are zeros, which implies that there exist at least $k - k'$ all-zero columns in $X(D)$ because $\langle X(D) \rangle = \langle X^*(D) \rangle$. Moreover, if Condition b) does not hold, $G(D)$ will be rank-deficient, thereby contradicting the assumption that $G(D)$ is a generator matrix for C . The proof is then completed. \square

Procedure 5:

- Given an (n, k) convolutional code C , use Procedure 1 to generate an optimal generator matrix $G(D)$ of rows $\mathbf{g}_i(D)$'s, $\forall 1 \leq i \leq k$. Suppose that $\mathbf{s}(G(D))$ is in the nondecreasing order of α distinct component values s_i 's, each with β_i repetitions, $\forall 1 \leq i \leq \alpha$.
- Set $i = 1$ and $M = 1$.
- Let $X(D)$ be the $(\sum_{r=1}^i \beta_r) \times n$ matrix of rows $\mathbf{g}_t(D)$'s, $\forall 1 \leq t \leq \sum_{r=1}^i \beta_r$, and $Y(D)$ denote the matrix containing the remaining rows of $G(D)$. If the following conditions are satisfied:
 - there exist at least $k - k'$ all-zero columns in $X(D)$, and
 - there exist $k - k'$ columns of $Y(D)$ in the same positions as the all-zero columns of $X(D)$ which form a nonsingular matrix,
then convert $X(D)$ to a systematic generator matrix, $G_M(D)$, for $\langle C^{s_{i+1}} \rangle$ and replace M by $M + 1$.
- If $i < \alpha - 1$, then replace i by $i + 1$ and go to Step 3; else convert $G(D)$ to a systematic generator matrix for C and assign it to $G_M(D)$. Denote by $\mathbf{g}_j^{(i)}(D)$'s the rows of $G_i(D)$ and let the rank of $G_i(D)$ be k_i , $\forall 1 \leq i \leq M$ and $1 \leq j \leq k_i$.
- Set $i = 2$ and initialize $G^*(D)$ by $G_1(D)$.
- Choose k_i $-$ k_{i-1} codewords $\mathbf{c}_1(D), \mathbf{c}_2(D), \dots, \mathbf{c}_{k_i - k_{i-1}}(D)$ generated by

$$\mathbf{c}_j(D) \in \left\langle \left(G^{*T}(D) G_i^{*T}(D) \right)^T \right\rangle$$

$\forall 1 \leq j \leq k_i - k_{i-1}$, where $G_i^*(D) \subseteq G_i(D)$, such that the resulting matrix

$$\hat{G}(D) = \left(G^{*T}(D) \mathbf{c}_1^T(D) \mathbf{c}_2^T(D) \cdots \mathbf{c}_{k_i - k_{i-1}}^T(D) \right)^T$$

forms a submatrix of a systematic generator matrix for C . Then set $G^*(D) = \hat{G}(D)$.

- If $i < M$, then replace i by $i + 1$ and go to Step 6; else stop and $G^*(D)$ will be a desired systematic generator matrix of the greatest separation vector for C .

In Step 3, it is checked whether $\langle C^p \rangle$ is systematically splittable. Similar to Procedure 4, none of the $\langle C^p \rangle$'s which are systematically splittable is missed since all $\langle C^p \rangle$'s can be specified by an optimal generator matrix by Theorem 1. Also by the constraints on producing $G^*(D)$ in Step 6, the correctness of Procedure 5 is guaranteed.

Example 6: Consider the convolutional code C which has an optimal PGM $G_2(D)$ with $\mathbf{s}(G_2(D)) = (2, 4, 6)$ in Example 1. By Lemma 6, we observe that only $\langle C^4 \rangle$ and C are systematically splittable with

$$\langle C^4 \rangle = \langle (0 \ 1 \ 0 \ D) \rangle$$

and

$$C = \left\langle \begin{pmatrix} 0 & 1 & \frac{1+D+D^3}{1+D^2+D^3} & 0 \\ 1 & 0 & \frac{1+D^3+D^4}{D+D^3+D^4} & 0 \\ 0 & 0 & \frac{1+D+D^3}{D+D^3+D^4} & 1 \end{pmatrix} \right\rangle.$$

By Procedure 5, $G^*(D)$ is updated as follows:

$$G^*(D) : (0 \ 1 \ 0 \ D) \Rightarrow \begin{pmatrix} 0 & 1 & 0 & D \\ 1 & 0 & 0 & \frac{1+D^3+D^4}{1+D+D^3} \\ 0 & 0 & 1 & \frac{D+D^3+D^4}{1+D+D^3} \end{pmatrix}.$$

Therefore, if the systematic property is preserved, then the greatest separation vector available is $\mathbf{s}(G^*(D)) = (2, 4, 4)$, which is consistent with the observation in Example 5. \square

V. BOUND ON LENGTH OF UEP CONVOLUTIONAL CODES

Besides the above discussion on UEP generator matrices, another basic and significant issue worth investigation is to find a UEP convolutional code with a given memory distribution and a separation vector such that its length is minimized and hence its information rate is maximized. In this section, a lower bound on the length of an (n, k) convolutional code C with the given memory distribution and separation vector is proposed. Let $G(D)$ be a canonical PGM for C and denote the degree of the i th row of $G(D)$ by e_i , $\forall 1 \leq i \leq k$. For any integer $L \geq 0$, define C_L to be the set of polynomial codewords of degree $\leq L$, and then C_L is a vector space over F . We denote the F -dimension of C_L by δ_L and the F -dimension of C_L with respect to the i th message space by δ_L^i . It is clear that $\delta_L = \sum_{i=1}^k \delta_L^i$. The dimension of the polynomial subcode for the i th message space can then be computed from the code's Forney indices (e_1, e_2, \dots, e_k) as shown next.

Lemma 7: Suppose $G(D)$ is a canonical generator matrix of a convolutional code C with Forney indices (e_1, e_2, \dots, e_k) . Denote δ_L^i as the dimension of C_L with respect to the i th message space. Then, $\forall 1 \leq i \leq k$, we have

$$\sum_{L \geq 0} \delta_L^i t^L = \frac{t^{e_i}}{(1-t)^2} \quad \text{and} \quad \delta_L^i = \max(L+1-e_i, 0).$$

Proof: Let $\mathbf{v}(D)$ be any polynomial codeword of degree $\leq L$. Since $\mathbf{v}(D) = \mathbf{I}(D)G(D)$, where $\mathbf{I}(D) = (I_1(D), I_2(D), \dots, I_k(D))$, the inequality $\deg(I_i(D)) + e_i \leq L$ follows from the predictable degree

property [39] of a reduced matrix. Thus, for $i \in \{1, \dots, k\}$, the set $\{D^j \mathbf{g}_i(D) : j + e_i \leq L\}$ is a basis for the F -space C_L with respect to the i th message space. Hence

$$\begin{aligned} \sum_{L \geq 0} \delta_L^i t^L &= \sum_{j \geq 0} (t^{e_i+j} + t^{e_i+j+1} + \dots) \\ &= \frac{t^{e_i}}{(1-t)^2}. \end{aligned}$$

Since $(1-t)^{-2} = \sum_{j \geq 0} (j+1)t^j$, we can obtain

$$\begin{aligned} \sum_{L \geq 0} \delta_L^i t^L &= \frac{t^{e_i}}{(1-t)^2} \\ &= \sum_{j \geq e_i} (j+1-e_i)t^j, \quad \forall 0 \leq i \leq k. \end{aligned}$$

Thus, the coefficient of t^L is $\max(L+1-e_i, 0)$, thereby completing the proof. \square

Denote by $s_i \mathbf{1}_j$ the j -tuple vector with all components equal to s_i . By Lemma 7, a bound on the length of UEP convolutional codes is given in Theorem 9.

Theorem 9: If $G(D)$ is a canonical generator matrix of an (n, k) convolutional code C with Forney indices (e_1, e_2, \dots, e_k) and separation vector $\mathbf{s}(G(D)) = (s_1, s_2, \dots, s_k)$, then we have

$$n \geq \max_{L \geq 0} \left\lceil \frac{\Theta_F(\delta_L, \mathbf{E}_L)}{L+1} \right\rceil \quad (23)$$

where $\Theta_F(\delta_L, \mathbf{E}_L)$ denotes the minimum possible length of a block code over F with dimension δ_L and separation vector $\mathbf{E}_L = (s_1 \mathbf{1}_{\delta_1^1}, s_2 \mathbf{1}_{\delta_2^2}, \dots, s_k \mathbf{1}_{\delta_k^k})$.

Proof: Recall that C_L forms a vector space over F with the basis $D^{j_i} \mathbf{g}_i(D)$'s, $\forall 1 \leq i \leq k$ and $0 \leq j_i < \delta_L^i$. Let $D^{j_i} \mathbf{g}_i(D) = \sum_{l=0}^L \mathbf{v}_{j_i, i}^{(l)} D^l$ with $\mathbf{v}_{j_i, i}^{(l)} \in F^n$, $\forall i, j_i, l$, and denote by $\mathbf{v}_{j_i, i}$ the $1 \times n(L+1)$ vector comprising $(\mathbf{v}_{j_i, i}^{(0)}, \mathbf{v}_{j_i, i}^{(1)}, \dots, \mathbf{v}_{j_i, i}^{(L)})$. It follows that C_L is equivalent to the $(n(L+1), \delta_L)$ block code over F with the following generator matrix:

$$G_L = \left(\mathbf{v}_{0,1}^T \ \mathbf{v}_{1,1}^T \ \dots \ \mathbf{v}_{\delta_1^1-1,1}^T \ \mathbf{v}_{0,2}^T \ \mathbf{v}_{1,2}^T \ \dots \ \mathbf{v}_{\delta_2^2-1,2}^T \ \dots \ \mathbf{v}_{0,k}^T \ \mathbf{v}_{1,k}^T \ \dots \ \mathbf{v}_{\delta_k^k-1,k}^T \right)^T.$$

Let $\mathbf{s}(G_L)$ be the separation vector of G_L . Since $\mathbf{s}(G_L) \geq \mathbf{E}_L$, it implies that

$$n(L+1) \geq \Theta_F(\delta_L, \mathbf{s}(G_L)) \geq \Theta_F(\delta_L, \mathbf{E}_L)$$

and hence

$$n \geq \left\lceil \frac{\Theta_F(\delta_L, \mathbf{E}_L)}{L+1} \right\rceil. \quad (24)$$

Since (24) holds for all possible C_L 's with $L \geq 0$, the proof is thus completed. \square

By Theorem 9, many lower bounds on the length of a linear UEP block code may then be employed to establish lower

TABLE I
CONVOLUTIONAL CODES FOR UNEQUAL ERROR PROTECTION WITH $n = 3$.
(m DENOTES THE EXTERNAL DEGREE OF THE CANONICAL PGM)

n	k	m	Canonical PGM	Forney Indices	Separation Vector
3	2	1	$\begin{bmatrix} 2 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$	1 0	2 3
3	2	2	$\begin{bmatrix} 1 & 0 & 1 \\ 7 & 5 & 0 \end{bmatrix}$	0 2	2 5
3	2	2	$\begin{bmatrix} 0 & 2 & 3 \\ 3 & 3 & 1 \end{bmatrix}$	1 1	3 4
3	2	3	$\begin{bmatrix} 3 & 2 & 1 \\ 5 & 3 & 4 \end{bmatrix}$	1 2	4 5
3	2	3	$\begin{bmatrix} 1 & 0 & 2 \\ 4 & 7 & 5 \end{bmatrix}$	1 2	2 6
3	2	4	$\begin{bmatrix} 0 & 1 & 1 \\ 33 & 31 & 0 \end{bmatrix}$	0 4	2 7
3	2	4	$\begin{bmatrix} 1 & 0 & 7 \\ 4 & 7 & 5 \end{bmatrix}$	2 2	4 6
3	2	5	$\begin{bmatrix} 4 & 1 & 5 \\ 7 & 10 & 13 \end{bmatrix}$	2 3	4 7
3	2	5	$\begin{bmatrix} 4 & 0 & 1 \\ 15 & 13 & 14 \end{bmatrix}$	2 3	2 8
3	2	6	$\begin{bmatrix} 0 & 1 & 1 \\ 133 & 171 & 0 \end{bmatrix}$	0 6	2 10
3	2	6	$\begin{bmatrix} 1 & 11 & 10 \\ 14 & 15 & 7 \end{bmatrix}$	3 3	4 8
3	2	6	$\begin{bmatrix} 17 & 0 & 13 \\ 14 & 13 & 15 \end{bmatrix}$	3 3	6 7
3	2	7	$\begin{bmatrix} 1 & 4 & 0 \\ 60 & 51 & 57 \end{bmatrix}$	2 5	2 10
3	2	7	$\begin{bmatrix} 1 & 2 & 3 \\ 146 & 71 & 171 \end{bmatrix}$	1 6	4 9

bounds on the length of a UEP convolutional code. For example, by the generalized Griesmer bound [7], [11], we have

$$\Theta_F(\delta_L, E_L) \geq \sum_{i=1}^k \sum_{j=1}^{\delta_L^{\phi(i)}} \left\lceil \frac{s_{\phi(i)}}{q \sum_{m=1}^{i-1} \delta_L^{\phi(m)} + j - 1} \right\rceil$$

where q denotes the order of F and $\phi : \{1, \dots, k\} \rightarrow \{1, \dots, k\}$ is a permutation such that $(s_{\phi(1)}, s_{\phi(2)}, \dots, s_{\phi(k)})$ is nonincreasingly ordered.

A canonical PGM with separation vector \mathbf{s} satisfying the lower bound (23) with equality does not mean that it is optimal over all codes of the same Forney indices. We have Definition 9 for ‘‘UEP-optimal’’ convolutional codes.

Definition 9: An (n, k) convolutional code with separation vector \mathbf{s} is said to be UEP-optimal over all codes with Forney indices (e_1, e_2, \dots, e_k) if and only if an (n, k) convolutional code with separation vector larger than \mathbf{s} and Forney indices (e_1, e_2, \dots, e_k) does not exist.

Good UEP convolutional codes with canonical optimal PGMs, obtained by computer search, are shown in Tables I–III with $n = 3, 4$, and 5, respectively. In the tables, every polynomial is expressed in the octal form. For example, the polynomial $1 + D^2 + D^3 + D^6$ is first rewritten as $D^6 + D^3 + D^2 + 1$ and then converted to binary string 1001101 which is 115 in the

TABLE II
CONVOLUTIONAL CODES FOR UNEQUAL ERROR PROTECTION WITH $n = 4$.
(m DENOTES THE EXTERNAL DEGREE OF THE CANONICAL PGM)

n	k	m	Canonical PGM	Forney Indices	Separation Vector
4	2	1	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 3 & 0 & 2 & 3 \end{bmatrix}$	0 1	2 5
4	2	2	$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 7 & 7 & 5 & 0 \end{bmatrix}$	0 2	2 8
4*	2	2	$\begin{bmatrix} 1 & 2 & 3 & 0 \\ 2 & 3 & 1 & 3 \end{bmatrix}$	1 1	4 6
4	2	3	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 13 & 0 & 15 & 17 \end{bmatrix}$	0 3	2 10
4*	2	3	$\begin{bmatrix} 1 & 2 & 3 & 0 \\ 6 & 5 & 1 & 7 \end{bmatrix}$	1 2	4 8
4*	2	3	$\begin{bmatrix} 3 & 3 & 2 & 2 \\ 4 & 7 & 1 & 3 \end{bmatrix}$	1 2	6 7
4	2	4	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 25 & 17 & 32 & 0 \end{bmatrix}$	0 4	4 10
4	2	4	$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 25 & 33 & 37 & 0 \end{bmatrix}$	0 4	2 12
4	2	5	$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 47 & 57 & 55 & 0 \end{bmatrix}$	0 5	2 13
4	2	5	$\begin{bmatrix} 1 & 0 & 7 & 6 \\ 14 & 13 & 15 & 5 \end{bmatrix}$	2 3	6 10
4	2	5	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 37 & 51 & 66 & 0 \end{bmatrix}$	0 5	4 12
4*	2	5	$\begin{bmatrix} 0 & 16 & 3 & 15 \\ 5 & 7 & 6 & 3 \end{bmatrix}$	3 2	8 9
4	2	6	$\begin{bmatrix} 0 & 5 & 7 & 1 \\ 35 & 11 & 35 & 20 \end{bmatrix}$	2 4	6 11
4	2	6	$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 113 & 167 & 165 & 0 \end{bmatrix}$	0 6	2 15
4	2	6	$\begin{bmatrix} 2 & 1 & 2 & 1 \\ 63 & 67 & 25 & 40 \end{bmatrix}$	1 5	4 13

TABLE II (Continued)
CONVOLUTIONAL CODES FOR UNEQUAL ERROR PROTECTION WITH $n = 4$.
(m DENOTES THE EXTERNAL DEGREE OF THE CANONICAL PGM)

n	k	m	Canonical PGM	Forney Indices	Separation Vector
4	2	7	$\begin{bmatrix} 16 & 5 & 1 & 16 \\ 27 & 37 & 24 & 11 \end{bmatrix}$	3 4	9 11
4	2	7	$\begin{bmatrix} 3 & 3 & 2 & 2 \\ 152 & 137 & 71 & 37 \end{bmatrix}$	1 6	6 13
4	2	7	$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 157 & 172 & 21 & 121 \end{bmatrix}$	1 6	4 14
4	2	7	$\begin{bmatrix} 1 & 0 & 0 & 2 \\ 100 & 165 & 145 & 173 \end{bmatrix}$	1 6	2 16
4	2	7	$\begin{bmatrix} 7 & 7 & 1 & 1 \\ 43 & 71 & 46 & 60 \end{bmatrix}$	2 5	8 12
4	3	1	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 2 & 0 & 1 & 0 \end{bmatrix}$	0 0 1	2 2 3
4	3	2	$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 5 & 7 & 0 & 0 \end{bmatrix}$	0 0 2	2 2 5
4	3	2	$\begin{bmatrix} 0 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \\ 3 & 0 & 2 & 3 \end{bmatrix}$	1 0 1	2 3 4
4	3	3	$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 16 & 13 & 0 & 0 \end{bmatrix}$	0 0 3	2 2 6
4	3	3	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 3 & 1 & 0 \\ 5 & 3 & 4 & 0 \end{bmatrix}$	0 1 2	4 4 5
4	3	4	$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 27 & 31 & 0 & 0 \end{bmatrix}$	0 0 4	2 2 7
4	3	4	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 7 & 1 & 4 & 0 \\ 3 & 4 & 7 & 0 \end{bmatrix}$	0 2 2	4 5 5
4	3	4	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 0 \\ 16 & 5 & 15 & 0 \end{bmatrix}$	0 1 3	4 4 6

TABLE II (Continued)
CONVOLUTIONAL CODES FOR UNEQUAL ERROR PROTECTION WITH $n = 4$.
(m DENOTES THE EXTERNAL DEGREE OF THE CANONICAL PGM)

n	k	m	Canonical PGM	Forney Indices	Separation Vector
4	3	5	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 3 & 4 & 7 & 0 \\ 15 & 15 & 6 & 0 \end{bmatrix}$	0 2 3	4 6 6
4	3	5	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 37 & 65 & 0 & 0 \end{bmatrix}$	0 0 5	2 2 8
4	3	5	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 0 \\ 36 & 11 & 31 & 0 \end{bmatrix}$	0 1 4	4 4 7
4	3	6	$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 7 & 6 & 3 & 0 \\ 26 & 13 & 37 & 0 \end{bmatrix}$	0 2 4	2 6 7
4	3	6	$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 135 & 0 & 147 & 0 \end{bmatrix}$	0 0 6	2 2 10
4	3	6	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 3 & 1 & 2 & 0 \\ 57 & 40 & 21 & 0 \end{bmatrix}$	0 1 5	4 4 8
4	3	7	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 13 & 6 & 11 & 0 \\ 34 & 27 & 1 & 0 \end{bmatrix}$	0 3 4	4 7 7
4	3	7	$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 3 & 7 & 2 & 0 \\ 26 & 15 & 53 & 0 \end{bmatrix}$	0 2 5	2 6 8
4	3	7	$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 2 & 3 & 1 & 0 \\ 57 & 135 & 100 & 0 \end{bmatrix}$	0 1 6	2 4 9
4	3	7	$\begin{bmatrix} 1 & 0 & 2 & 3 \\ 3 & 1 & 2 & 0 \\ 6 & 40 & 63 & 23 \end{bmatrix}$	1 1 5	4 4 8
4	3	7	$\begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 2 & 0 & 1 \\ 40 & 63 & 35 & 40 \end{bmatrix}$	1 1 5	2 2 10

the octal form. Note that all the convolutional codes shown in Tables I–III satisfy the lower bound in (23) with equality; those which are further verified to be UEP-optimal are marked by *.

Compared with optimal (n, k) convolutional codes with $k > 1$ which were reported previously without consideration of UEP, we observe that many optimal codes have the intrinsic UEP capability. For those codes, the results presented here can be employed to optimize the protection and complexity requirements. However, for the other optimal codes which can provide equal error protection only, UEP is usually obtained at the cost of a worsened BER performance for some of the information bits. For example, consider the optimal binary $(4, 3)$ convolutional code with generator matrix [39]

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

and $\mathbf{s}(G_1(D)) = (3, 3, 3)$ for equal error protection only. For UEP codes with the same n, k , and degree of the code, the best two in Table II are with the following generator matrices:

$$G_3(D) = \begin{pmatrix} 0 & 0 & 1 & D \\ 0 & 1 & 1 & 1 \\ D+1 & 0 & D & D+1 \end{pmatrix}$$

TABLE III
CONVOLUTIONAL CODES FOR UNEQUAL ERROR PROTECTION WITH $n = 5$.
(m DENOTES THE EXTERNAL DEGREE OF THE CANONICAL PGM)

n	k	m	Canonical PGM	Forney Indices	Separation Vector
5	2	1	$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 3 & 3 & 2 & 0 \end{bmatrix}$	0 1	4 6
5	2	2	$\begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 3 & 5 & 7 & 7 & 0 \end{bmatrix}$	0 2	2 10
5*	2	2	$\begin{bmatrix} 0 & 2 & 3 & 2 & 3 \\ 3 & 1 & 2 & 1 & 3 \end{bmatrix}$	1 1	6 7
5	2	3	$\begin{bmatrix} 0 & 3 & 3 & 1 & 3 \\ 7 & 6 & 5 & 4 & 3 \end{bmatrix}$	1 2	7 8
5	2	3	$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 15 & 13 & 7 & 17 & 0 \end{bmatrix}$	0 3	2 12
5	2	3	$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 13 & 16 & 5 & 0 & 15 \end{bmatrix}$	0 3	4 11
5	2	4	$\begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 27 & 12 & 37 & 15 & 0 \end{bmatrix}$	0 4	2 14
5	2	4	$\begin{bmatrix} 3 & 7 & 2 & 6 & 0 \\ 7 & 1 & 5 & 4 & 7 \end{bmatrix}$	2 2	8 10
5	2	4	$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 22 & 27 & 5 & 37 & 0 \end{bmatrix}$	0 4	4 13
5	2	4	$\begin{bmatrix} 3 & 2 & 3 & 0 & 1 \\ 16 & 17 & 1 & 15 & 10 \end{bmatrix}$	1 3	6 12
5	2	5	$\begin{bmatrix} 5 & 1 & 6 & 4 & 3 \\ 2 & 16 & 1 & 17 & 15 \end{bmatrix}$	2 3	8 12
5	2	5	$\begin{bmatrix} 0 & 3 & 3 & 3 & 1 \\ 27 & 7 & 35 & 22 & 20 \end{bmatrix}$	1 4	7 13
5	2	5	$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 77 & 53 & 73 & 0 & 51 \end{bmatrix}$	0 5	2 18
5	2	5	$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 65 & 46 & 33 & 75 & 0 \end{bmatrix}$	0 5	4 16
5	2	6	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 135 & 0 & 177 & 113 & 145 \end{bmatrix}$	0 6	2 20
5	2	6	$\begin{bmatrix} 3 & 2 & 3 & 0 & 1 \\ 35 & 45 & 51 & 55 & 40 \end{bmatrix}$	1 5	6 15
5	2	6	$\begin{bmatrix} 1 & 3 & 1 & 7 & 7 \\ 25 & 27 & 30 & 34 & 1 \end{bmatrix}$	2 4	10 13
5	2	6	$\begin{bmatrix} 0 & 2 & 1 & 1 & 2 \\ 75 & 45 & 77 & 40 & 27 \end{bmatrix}$	1 5	4 17
5	2	7	$\begin{bmatrix} 21 & 37 & 20 & 6 & 3 \\ 7 & 6 & 13 & 17 & 11 \end{bmatrix}$	4 3	12 14
5	2	7	$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 247 & 331 & 277 & 115 & 0 \end{bmatrix}$	0 7	2 21
5	2	7	$\begin{bmatrix} 2 & 2 & 0 & 1 & 1 \\ 127 & 5 & 147 & 177 & 100 \end{bmatrix}$	1 6	4 18
5	2	7	$\begin{bmatrix} 7 & 2 & 6 & 3 & 3 \\ 43 & 5 & 25 & 74 & 45 \end{bmatrix}$	2 5	10 15
5	2	7	$\begin{bmatrix} 0 & 3 & 1 & 3 & 1 \\ 127 & 75 & 144 & 122 & 100 \end{bmatrix}$	1 6	6 17
5	3	1	$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 2 & 3 & 0 & 0 \end{bmatrix}$	0 0 1	2 4 4
5	3	1	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 3 & 0 & 2 & 3 & 0 \end{bmatrix}$	0 0 1	2 2 5
5	3	1	$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 3 & 2 & 3 & 0 & 0 \end{bmatrix}$	0 0 1	3 3 4
5	3	2	$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 3 & 2 & 0 & 2 \\ 3 & 3 & 1 & 0 & 1 \end{bmatrix}$	0 1 1	2 5 5

and

$$G_3(D) = \begin{pmatrix} 0 & 0 & 1 & D \\ 0 & 1 & 1 & 1 \\ D+1 & 0 & D & D+1 \end{pmatrix}$$

which have $\mathbf{s}(G_2(D)) = (2, 2, 5)$ and $\mathbf{s}(G_3(D)) = (2, 3, 4)$, respectively. For $G_2(D)$, a better performance of $I_3(D)$ is achieved at the cost of some performance loss of $I_1(D)$ and $I_2(D)$ compared with $G_1(D)$ since we have $s(G_2(D))_3 > s(G_1(D))_3$ but $(s(G_2(D))_1, s(G_2(D))_2) < (s(G_1(D))_1, s(G_1(D))_2)$. For $G_3(D)$, $I_1(D)$ experiences worse protection than that for $G_1(D)$ but $I_3(D)$ receives better protection than that for $G_1(D)$ since we have

TABLE III (Continued)
CONVOLUTIONAL CODES FOR UNEQUAL ERROR PROTECTION WITH $n = 5$.
(m DENOTES THE EXTERNAL DEGREE OF THE CANONICAL PGM)

n	k	m	Canonical PGM	Forney Indices	Separation Vector
5	3	2	$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 7 & 5 & 7 & 0 & 0 \end{bmatrix}$	002	228
5*	3	2	$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 \\ 1 & 3 & 2 & 0 & 3 \end{bmatrix}$	011	446
5	3	3	$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 2 & 0 & 3 & 0 & 0 \\ 5 & 7 & 1 & 6 & 3 \end{bmatrix}$	012	337
5*	3	3	$\begin{bmatrix} 2 & 0 & 0 & 1 & 3 \\ 3 & 3 & 2 & 0 & 2 \\ 2 & 1 & 3 & 2 & 1 \end{bmatrix}$	111	466
5	3	3	$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 13 & 17 & 0 & 15 & 0 \end{bmatrix}$	003	2210
5	3	3	$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 3 & 1 & 0 & 3 & 1 \\ 5 & 6 & 0 & 3 & 4 \end{bmatrix}$	012	267
5	3	3	$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 3 & 2 & 0 & 1 & 0 \\ 1 & 7 & 0 & 4 & 7 \end{bmatrix}$	012	248
5	3	4	$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 7 & 0 & 0 & 3 & 7 \\ 2 & 7 & 0 & 7 & 4 \end{bmatrix}$	022	268
5	3	4	$\begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 7 & 4 & 6 & 0 \\ 7 & 3 & 6 & 1 & 0 \end{bmatrix}$	022	277
5	3	4	$\begin{bmatrix} 2 & 1 & 0 & 3 & 0 \\ 3 & 2 & 0 & 3 & 2 \\ 3 & 4 & 7 & 6 & 3 \end{bmatrix}$	112	448
5	3	4	$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 36 & 23 & 15 & 0 & 0 \end{bmatrix}$	004	2410
5	3	4	$\begin{bmatrix} 0 & 1 & 3 & 0 & 3 \\ 2 & 0 & 1 & 3 & 1 \\ 7 & 4 & 3 & 2 & 4 \end{bmatrix}$	112	557
5	3	4	$\begin{bmatrix} 0 & 0 & 3 & 1 & 1 \\ 3 & 1 & 1 & 3 & 0 \\ 7 & 4 & 4 & 1 & 4 \end{bmatrix}$	112	467
5	3	4	$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 33 & 31 & 0 & 0 & 27 \end{bmatrix}$	004	2211
5	3	5	$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 7 & 3 & 7 & 5 & 0 \\ 17 & 17 & 10 & 4 & 0 \end{bmatrix}$	023	488
5	3	5	$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 2 & 3 & 0 & 0 \\ 36 & 13 & 33 & 17 & 0 \end{bmatrix}$	014	4410
5	3	5	$\begin{bmatrix} 5 & 4 & 6 & 1 & 0 \\ 1 & 3 & 3 & 1 & 3 \\ 1 & 2 & 7 & 6 & 0 \end{bmatrix}$	212	677
5	3	5	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 3 & 0 & 7 & 1 & 6 \\ 10 & 0 & 17 & 14 & 5 \end{bmatrix}$	023	289
5	3	5	$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 53 & 71 & 0 & 0 & 67 \end{bmatrix}$	005	2213
5	3	5	$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 3 & 2 & 3 & 2 & 0 \\ 24 & 1 & 37 & 17 & 0 \end{bmatrix}$	014	2610
5	3	5	$\begin{bmatrix} 1 & 4 & 5 & 4 & 1 \\ 1 & 5 & 4 & 2 & 4 \\ 3 & 3 & 1 & 3 & 2 \end{bmatrix}$	221	668

$s(G_3(D))_1 < s(G_1(D))_1$ and $s(G_3(D))_3 > s(G_1(D))_3$. The simulation results of the three codes on AWGN channels with BPSK modulation are shown in Fig. 2, where the BER curves are consistent with the above discussion.

VI. CONCLUSION

In this paper, we study the UEP capability of convolutional codes from an algebraic perspective. For every convolutional

TABLE III (Continued)
CONVOLUTIONAL CODES FOR UNEQUAL ERROR PROTECTION WITH $n = 5$.
(m DENOTES THE EXTERNAL DEGREE OF THE CANONICAL PGM)

n	k	m	Canonical PGM	Forney Indices	Separation Vector
5	3	5	$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 57 & 73 & 24 & 0 & 0 \end{bmatrix}$	005	2412
5	3	5	$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 4 & 7 & 3 & 0 & 0 \\ 7 & 12 & 13 & 13 & 0 \end{bmatrix}$	023	469
5	3	6	$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 10 & 7 & 16 & 0 \\ 11 & 7 & 11 & 13 & 0 \end{bmatrix}$	033	2810
5	3	6	$\begin{bmatrix} 2 & 1 & 2 & 2 & 1 \\ 3 & 2 & 3 & 0 & 0 \\ 6 & 11 & 11 & 33 & 20 \end{bmatrix}$	114	559
5	3	6	$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 15 & 21 & 24 & 1 & 0 \\ 7 & 6 & 3 & 5 & 0 \end{bmatrix}$	042	489
5	3	6	$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 3 & 0 \\ 57 & 40 & 67 & 31 & 0 \end{bmatrix}$	015	4412
5	3	6	$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 175 & 46 & 133 & 0 & 0 \end{bmatrix}$	006	2414
5	3	6	$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 2 & 14 & 7 & 15 & 0 \\ 11 & 17 & 16 & 10 & 0 \end{bmatrix}$	033	299
5	3	6	$\begin{bmatrix} 1 & 2 & 10 & 10 & 5 \\ 2 & 3 & 2 & 3 & 3 \\ 7 & 2 & 1 & 5 & 2 \end{bmatrix}$	312	688
5	3	6	$\begin{bmatrix} 1 & 3 & 3 & 3 & 0 \\ 0 & 4 & 3 & 5 & 6 \\ 10 & 5 & 17 & 15 & 11 \end{bmatrix}$	123	778
5	3	6	$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 3 & 1 & 1 & 0 & 3 \\ 35 & 72 & 40 & 0 & 63 \end{bmatrix}$	015	2611
5	3	6	$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 7 & 7 & 2 & 1 & 0 \\ 25 & 3 & 34 & 30 & 0 \end{bmatrix}$	024	4610
5	3	7	$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 2 & 1 \\ 161 & 165 & 0 & 121 & 100 \end{bmatrix}$	016	3311
5	3	7	$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 141 & 276 & 327 & 0 & 0 \end{bmatrix}$	007	2413
5	3	7	$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 6 & 5 & 7 & 7 & 0 \\ 67 & 16 & 17 & 41 & 0 \end{bmatrix}$	025	21010
5	3	7	$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 137 & 263 & 0 & 331 & 0 \end{bmatrix}$	007	2216
5	3	7	$\begin{bmatrix} 3 & 2 & 1 & 0 & 0 \\ 0 & 7 & 4 & 2 & 1 \\ 11 & 35 & 20 & 25 & 30 \end{bmatrix}$	124	4610
5	3	7	$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 3 & 0 & 3 \\ 132 & 100 & 136 & 0 & 161 \end{bmatrix}$	016	2512
5	3	7	$\begin{bmatrix} 0 & 2 & 3 & 0 & 3 \\ 3 & 1 & 1 & 3 & 3 \\ 34 & 51 & 0 & 51 & 11 \end{bmatrix}$	115	579
5	3	7	$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 26 & 15 & 4 & 0 & 21 \\ 7 & 11 & 15 & 0 & 16 \end{bmatrix}$	043	389
5	4	1	$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}$	0010	2223
5	4	2	$\begin{bmatrix} 0 & 2 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 2 & 3 & 0 & 2 & 0 \end{bmatrix}$	1001	2333
5	4	2	$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 0 & 1 \\ 3 & 1 & 0 & 0 & 2 \end{bmatrix}$	0011	2234

code, we prove the existence of optimal generator matrices for UEP and show that there exists at least one optimal PGM which is basic and hence noncatastrophic with the aid of effective lower triangular matrices. A counterexample shows that in general the set of optimal generator matrices for a given convolutional code may contain neither canonical nor minimal generator matrices which achieve the minimum degree requirement. To optimize the tradeoff between UEP performance and hardware/computation complexity, we turn to find an optimal PGM with the smallest external degree among all

TABLE III (Continued)
CONVOLUTIONAL CODES FOR UNEQUAL ERROR PROTECTION WITH $n = 5$.
(m DENOTES THE EXTERNAL DEGREE OF THE CANONICAL PGM)

n	k	m	Canonical PGM	Forney Indices	Separation Vector
5	4	2	$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 5 & 0 & 7 & 0 & 0 \end{bmatrix}$	0002	2225
5	4	3	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 13 & 0 & 16 & 0 & 0 \end{bmatrix}$	0003	2226
5	4	3	$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 3 & 2 & 0 & 0 \\ 6 & 1 & 5 & 0 & 0 \end{bmatrix}$	0012	2445
5	4	3	$\begin{bmatrix} 3 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 0 & 0 \\ 0 & 3 & 1 & 2 & 0 \end{bmatrix}$	1011	3444
5	4	4	$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 3 & 7 & 0 & 6 & 0 \\ 6 & 1 & 0 & 7 & 0 \end{bmatrix}$	0022	2455
5	4	4	$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 31 & 0 & 27 & 0 & 0 \end{bmatrix}$	0004	2227
5	4	4	$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 0 & 3 \\ 1 & 2 & 0 & 0 & 3 \\ 6 & 5 & 4 & 0 & 5 \end{bmatrix}$	0112	4445
5	4	4	$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 3 & 1 & 0 & 2 & 0 \\ 7 & 10 & 0 & 11 & 0 \end{bmatrix}$	0013	2446
5	4	5	$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 63 & 75 & 0 & 0 & 0 \end{bmatrix}$	0005	2228
5	4	5	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 3 & 1 & 1 \\ 3 & 0 & 5 & 0 & 4 \\ 5 & 0 & 2 & 7 & 0 \end{bmatrix}$	0122	2555
5	4	5	$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 2 & 0 & 3 \\ 3 & 3 & 1 & 0 & 1 \\ 1 & 13 & 10 & 0 & 10 \end{bmatrix}$	0113	4446
5	4	5	$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 6 & 1 & 7 & 0 & 0 \\ 13 & 14 & 1 & 0 & 0 \end{bmatrix}$	0023	2466
5	4	5	$\begin{bmatrix} 1 & 1 & 0 & 2 & 2 \\ 5 & 4 & 0 & 0 & 2 \\ 1 & 2 & 1 & 1 & 2 \\ 2 & 0 & 2 & 3 & 3 \end{bmatrix}$	1211	4455
5	4	5	$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 2 & 3 & 1 & 0 & 0 \\ 11 & 27 & 20 & 0 & 0 \end{bmatrix}$	0014	2447
5	4	6	$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 7 & 0 \\ 2 & 6 & 3 & 1 & 0 \\ 7 & 4 & 7 & 4 & 0 \end{bmatrix}$	0222	2466
5	4	6	$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 3 & 1 \\ 47 & 0 & 0 & 51 & 40 \end{bmatrix}$	0015	2248

TABLE III (Continued)
CONVOLUTIONAL CODES FOR UNEQUAL ERROR PROTECTION WITH $n = 5$.
(m DENOTES THE EXTERNAL DEGREE OF THE CANONICAL PGM)

n	k	m	Canonical PGM	Forney Indices	Separation Vector
5	4	6	$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 6 & 7 & 0 & 0 & 3 \\ 31 & 12 & 0 & 0 & 31 \end{bmatrix}$	0024	2267
5	4	6	$\begin{bmatrix} 2 & 2 & 1 & 2 & 0 \\ 1 & 0 & 0 & 3 & 2 \\ 3 & 1 & 2 & 0 & 0 \\ 10 & 12 & 10 & 15 & 15 \end{bmatrix}$	1113	4446
5	4	6	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 135 & 0 & 147 & 0 & 0 \end{bmatrix}$	0006	22210
5	4	6	$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 2 & 2 & 1 & 2 & 0 \\ 2 & 3 & 0 & 1 & 0 \\ 25 & 13 & 0 & 20 & 0 \end{bmatrix}$	0114	2447
5	4	7	$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 315 & 0 & 0 & 226 & 0 \end{bmatrix}$	0007	2229
5	4	7	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 13 & 3 & 0 \\ 31 & 0 & 2 & 31 & 0 \end{bmatrix}$	0034	2257
5	4	7	$\begin{bmatrix} 0 & 0 & 2 & 3 & 0 \\ 2 & 3 & 3 & 3 & 0 \\ 2 & 1 & 0 & 2 & 1 \\ 7 & 36 & 27 & 27 & 20 \end{bmatrix}$	1114	3446
5	4	7	$\begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 3 & 2 & 0 & 0 \\ 176 & 67 & 67 & 0 & 0 \end{bmatrix}$	0016	2448
5	4	7	$\begin{bmatrix} 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 3 & 4 & 7 & 0 & 0 \\ 26 & 25 & 16 & 0 & 20 \end{bmatrix}$	1024	2466
5	4	7	$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 5 & 1 & 0 & 3 & 7 \\ 7 & 2 & 0 & 6 & 7 \\ 7 & 10 & 0 & 17 & 12 \end{bmatrix}$	0223	2556

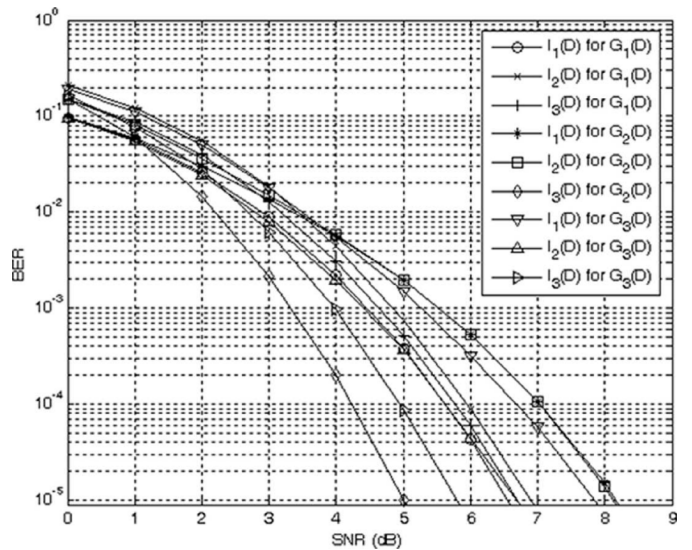


Fig. 2. BER curves of information bits fed to different inputs of $G_1(D)$, $G_2(D)$, and $G_3(D)$.

optimal PGMs or a canonical generator matrix with the greatest separation vector among all canonical PGMs. In addition, UEP is combined with systematic generator matrices. Although the comparison of separation vectors involves a partial ordering, we show the existence of the above desirable generator matrices along with corresponding necessary and sufficient conditions.

Several procedures are also given for obtaining these desirable generator matrices. Finally, we propose a lower bound on the length of a UEP convolutional code with given Forney indices and separation vector. Several convolutional codes that are UEP-optimal or near UEP-optimal are presented with their lengths equal to the derived lower bound.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the Associate Editor for their valuable comments and suggestions which helped to improve the quality of the paper.

REFERENCES

- [1] L. A. Bassalygo, V. A. Zinov'ev, V. V. Zyablov, M. S. Pinskiy, and G. S. Poltyrev, "Bounds for codes with unequal protection of two sets of messages," *Probl. Peredach. Inf.*, vol. 15, no. 3, pp. 40–49, 1979.
- [2] I. M. Boyarinov and G. L. Katsman, "Linear unequal error protection codes," *IEEE Trans. Inf. Theory*, vol. IT-27, pp. 168–175, Mar. 1981.
- [3] I. M. Boyarinov, "Combined decoding methods for linear codes with unequal protection of information symbols," *Probl. Peredach. Inf.*, vol. 19, no. 1, pp. 21–29, 1983.
- [4] L. A. Dunning and W. E. Robbins, "Optimum encoding of linear block codes for unequal error protection," *Inf. Contr.*, vol. 37, pp. 150–177, 1978.
- [5] L. A. Dunning, "Encoding and decoding for minimization of message symbol error rates in linear block codes," *IEEE Trans. Inf. Theory*, vol. IT-33, pp. 91–104, Jan. 1987.
- [6] V. N. Dynkin and V. A. Tognidze, "Cyclic codes with unequal symbol protection," *Probl. Peredach. Inf.*, vol. 12, no. 1, pp. 24–28, 1976.
- [7] W. J. van Gils, "Two topics on linear unequal error protection codes: Bounds on their length and cyclic code classes," *IEEE Trans. Inf. Theory*, vol. IT-29, pp. 866–876, Nov. 1983.
- [8] W. J. van Gils, "Linear unequal error protection codes from shorter codes," *IEEE Trans. Inf. Theory*, vol. IT-30, pp. 544–546, May 1984.
- [9] W. C. Gore and C. C. Kilgus, "Cyclic codes with unequal error protection," *IEEE Trans. Inf. Theory*, vol. IT-17, pp. 214–215, Mar. 1971.
- [10] T. Kasami, S. Lin, V. K. Wei, and S. Yamamura, "Coding for the binary symmetric broadcast channel with two receivers," *IEEE Trans. Inf. Theory*, vol. IT-31, pp. 616–625, Sep. 1985.
- [11] G. L. Katsman, "Bounds on volume of linear codes with unequal information-symbol protection," *Probl. Peredach. Inf.*, vol. 16, no. 2, pp. 25–32, 1980.
- [12] C. C. Kilgus and W. C. Gore, "A class of cyclic unequal-error-protection codes," *IEEE Trans. Inf. Theory*, vol. IT-18, pp. 687–690, Sep. 1972.
- [13] M.-C. Lin, C.-C. Lin, and S. Lin, "Computer search for binary cyclic UEP codes of odd length up to 65," *IEEE Trans. Inf. Theory*, vol. 36, pp. 924–935, Jul. 1990.
- [14] M.-C. Lin and S. Lin, "Cyclic unequal error protection codes constructed from cyclic codes of composite length," *IEEE Trans. Inf. Theory*, vol. 34, pp. 867–871, Jul. 1988.
- [15] B. Masnick and J. K. Wolf, "On linear unequal error protection codes," *IEEE Trans. Inf. Theory*, vol. IT-13, pp. 600–607, Jul. 1967.
- [16] V. A. Zinov'ev and V. V. Zyablov, "Codes with unequal protection of information symbols," *Probl. Peredach. Inf.*, vol. 15, no. 3, pp. 50–60, 1979.
- [17] E. K. Englund, "Nonlinear unequal error-protection codes are sometimes better than linear ones," *IEEE Trans. Inf. Theory*, vol. 37, pp. 1418–1420, Sep. 1991.
- [18] E. K. Englund, "Nonlinear unequal error-protection codes exceeding Katsman bound," in *Proc. IEEE Int. Symp. Inf. Theory*, Trondheim, Norway, Jun. 1994, p. 502.
- [19] M.-C. Chiu and C.-C. Chao, "A new construction of nonlinear unequal error protection codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Whistler, Canada, Sep. 1995, p. 496.
- [20] J. Hagenauer, "Rate-compatible punctured convolutional codes (RCPC codes) and their applications," *IEEE Trans. Commun.*, vol. 32, pp. 389–400, Apr. 1988.
- [21] L. H. C. Lee, "New rate-compatible punctured convolutional codes for Viterbi decoding," *IEEE Trans. Commun.*, vol. 42, pp. 3073–3079, Dec. 1994.
- [22] C.-H. Wang and C.-C. Chao, "Path-compatible pruned convolutional (PCPC) codes," *IEEE Trans. Commun.*, vol. 50, pp. 213–224, Feb. 2002.
- [23] C.-H. Wang, "New table-switching and data-multiplexing schemes of rate-compatible punctured convolutional codes for unequal error protection," *IEEE Commun. Lett.*, vol. 11, pp. 744–746, Sep. 2007.
- [24] C.-H. Wang and Y.-S. Lin, "Combined puncturing and path pruning for convolutional codes and the application to unequal error protection," *IEEE Trans. Commun.*, vol. 56, pp. 1385–1389, Sep. 2008.
- [25] K. Yamaguchi and H. Imai, "Construction of unequal error protecting convolutional codes from low rate convolutional codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Trondheim, Norway, Jun. 1994, p. 275.
- [26] J.-F. Cheng and R. J. McEliece, "Superimposed convolutional codes," in *Proc. Int. Symp. Commun.*, Taipei, Taiwan, Jun. 1995, pp. 105–110.
- [27] R. H. Morelos-Zaragoza and H. Imai, "Binary multilevel convolutional codes with unequal error protection capabilities," *IEEE Trans. Commun.*, vol. 46, pp. 850–853, Jul. 1998.
- [28] C.-H. Wang and C.-C. Chao, "Combined speech and channel coding for wireless communications," *Wireless Pers. Commun.*, vol. 17, pp. 21–43, Apr. 2001.
- [29] R. Palazzo Jr., "Linear unequal error protection convolutional codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Brighton, U.K., Jun. 1985, pp. 88–89.
- [30] R. Palazzo Jr., "On the linear unequal error protection convolutional codes," in *Proc. IEEE Int. Global Telecommun. Conf.*, Houston, TX, Dec. 1986, pp. 1367–1371.
- [31] P. Piret, *Convolutional Codes*. Cambridge, MA: MIT Press, 1988.
- [32] D. G. Mills and D. J. Costello Jr., "Using a modified transfer function to calculate unequal error protection capabilities of convolutional codes," in *Proc. IEEE Int. Symp. Inf. Theory*, San Antonio, TX, Jan. 1993, p. 144.
- [33] D. G. Mills and D. J. Costello Jr., "A bound on the unequal error protection capabilities of rate k/n convolutional codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Trondheim, Norway, Jun. 1994, p. 274.
- [34] M.-C. Chiu, C.-C. Chao, and C.-H. Wang, "Convolutional codes for unequal error protection," in *Proc. IEEE Int. Symp. Inf. Theory*, Ulm, Germany, Jun. 1997, p. 290.
- [35] C.-H. Wang and C.-C. Chao, "Further results on unequal error protection of convolutional codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Sorrento, Italy, Jun. 2000, p. 35.
- [36] T. Danon and S. I. Bross, "Free distance lower bounds for unequal error-protection convolutional codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Sorrento, Italy, Jun. 2000, p. 261.
- [37] 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.
- [38] C.-H. Wang and C.-C. Chao, "Canonical convolutional encoders for unequal error protection," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, Canada, Jul. 2008, pp. 2232–2236.
- [39] 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.
- [40] G. D. Forney Jr., "Convolutional Codes I: Algebraic structure," *IEEE Trans. Inf. Theory*, vol. IT-16, pp. 720–738, Nov. 1970.
- [41] R. Johannesson and Z. X. Wan, "A linear algebra approach to minimal convolutional encoders," *IEEE Trans. Inf. Theory*, vol. 39, pp. 1219–1233, Jul. 1993.
- [42] 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.
- [43] G. D. Forney Jr., "Correction to 'Convolutional Codes I: Algebraic structure'," *IEEE Trans. Inf. Theory*, vol. IT-17, p. 361, May 1971.
- [44] G. D. Forney Jr., "Structural analysis of convolutional codes via dual codes," *IEEE Trans. Inf. Theory*, vol. IT-19, pp. 512–518, Jul. 1973.
- [45] B. W. Dickinson, "A new characterization of canonical convolutional encoders," *IEEE Trans. Inf. Theory*, vol. IT-22, pp. 352–354, May 1976.

Chung-Hsuan Wang (S'94-M'01) received the B.S. and Ph.D. degrees from the National Tsing Hua University, Hsinchu, Taiwan, in 1994 and 2001, respectively, both in electrical engineering.

From August 2001 to July 2004, he held a faculty position with the Department of Electronic Engineering, Chung Yuan Christian University, Chung-Li, Taiwan. From August 2004 to July 2009, he was with the Department of Communication Engineering, National Chiao Tung University (NCTU), Hsinchu, as an Assistant Professor. Since August 2009, he has been with the Institute of Communication Engineering and the Department of Electrical Engineering, NCTU. His current research interests include digital communications, error-correcting codes, information theory, and signal processing.

Mao-Ching Chiu (S'92–A'96–M'08) was born in Chiayi, Taiwan, R.O.C., on April 12, 1968. He received the B.S. degree in electronic engineering from the National Taiwan University of Science and Technology, Taipei, Taiwan, R.O.C. in 1990, and the M.S. and Ph.D. degrees in electrical engineering from the National Tsing Hua University, Hsinchu, Taiwan, R.O.C. in 1992 and 1996, respectively.

After August 1998, he was with the Department of Electrical Engineering, National Chi Nan University, Nantou, Taiwan, as an Assistant Professor. In 2002, he joined the Integrated Programmable Communications, Inc., as a Manager of the Algorithm Department. During this period, he focused on IEEE 802.11a/b/g baseband receiver design, especially on the design of equalization and decoding algorithms. Since August 2003, he has been with the Department of Electrical Engineering, National Chung Cheng University, Chiayi, Taiwan, as an Associate Professor. His current research interests include design of wireless local area networks, digital transmission, error-correcting codes, and spread-spectrum communications.

Chi-chao Chao (S'87–M'89) was born in Taipei, Taiwan, R.O.C., in 1961. He received the B.S. degree from the National Taiwan University, Taipei, in 1983 and the M.S. and Ph.D. degrees from the California Institute of Technology (Caltech), Pasadena, in 1986 and 1989, respectively, all in electrical engineering.

He was an Instructor with the Department of Weapon Command and Control Systems, Naval Weapon School, Kaohsiung, Taiwan, during his military service from 1983 to 1985. Since September 1989, he has been with the National Tsing Hua University (NTHU), Hsinchu, Taiwan, where he is currently a Professor with the Institute of Communications Engineering and the Department of Electrical Engineering. He served as the Director of the Institute of Communications Engineering, NTHU, from August 2005 to July 2008. He held visiting positions at Caltech from September 1995 to March 1996, at Bell Communications Research (now Telcordia Technologies), Morristown, NJ, from March 1996 to August 1996, and at Osaka University, Japan, from April 2009 to September 2009. His current research interests include digital communications, error-correcting codes, information theory, and wireless networks.

Dr. Chao was the Secretary of the IEEE Taipei Section from 1997 to 1998 and the Chair of the IEEE Information Theory Society Taipei Chapter from 1999 to 2001. He served as an Associate Editor for the IEEE COMMUNICATIONS LETTERS from 2002 to 2005. He is currently the Chair of the IEEE Communications Society Taipei Chapter. He received the Distinguished Teaching Awards from NTHU in 1993, 2002, and 2008. In 2008, he became a Tsing Hua Distinguished Professor of NTHU.