A Fast Method for Blind Identification of Punctured Convolutional Codes

Shu Nan HAN, Min ZHANG, Xin Hao LI

Dept. of Communications Engineering, College of Electronic Engineering, National University of Defense Technology, Huangshan Road 460, 230031 Hefei, China

hsnnong@163.com, piaoyi17@gmail.com, lixinhao1989616@126.com

Submitted October 12, 2017 / Accepted April 22, 2018

Abstract. *The existing method for blind identification of a punctured convolutional code involves searching for dual words and the puncturing pattern exhaustively. As the length of the dual words and the code rate increase, the computational complexity of this method expands exponentially. To address this problem, a fast scheme for blind identification of punctured convolutional codes is proposed. First, a recursive algorithm for solving the parity check equation set is proposed. The dual word and generator polynomial bases of the punctured convolutional code are estimated by using the recursive algorithm. After this, by using the structural properties of the generator matrix of the blocked code, possible generator matrices of the punctured convolutional code are obtained. Finally, since a generator polynomial of the parent convolutional code can be recovered from any column of its polycyclic pseudo-circulant matrix, the corresponding generator matrix of the parent code and the puncturing pattern are reconstructed simultaneously from an estimation of the generator matrix of the punctured code. The reconstructed generator matrix of the parent code with a minimal constraint length is determined to be the identification result. Simulation experiments show the effectiveness of the proposed method. As there is no need to search for the dual word and puncturing pattern exhaustively, the method can achieve fast identification of punctured convolutional codes. Additionally, the method is robust to bit errors in the received sequence.*

Keywords

Punctured convolutional code, blind identification, recursive algorithm, generator matrix, puncturing pattern

1. Introduction

Error correcting codes are widely used in communication systems as a means of enhancing the quality of communication [1]. Since punctured convolutional codes have high code rates and can be decoded flexibly, they are often used by preference in modern communication systems across domains such as satellite communication, deep space communication and mobile communication [2]. This makes blind identification of punctured convolutional codes an important issue in the fields of cognitive radio and information interception.

Blind identification of a punctured convolutional code aims to reconstruct the generator matrices of the punctured and parent codes and identify the puncturing pattern. In the case that the parent code rate is 1/2 and the punctured code rate is $K/(K+1)$ where K is the input dimension of the punctured convolutional encoder, an identification method has been proposed in [3]. The method first of all identifies the parity check matrix of the punctured convolutional code by using Gaussian elimination algorithm to solve the parity check equation. Then, under every possible puncturing pattern, a linear equation set is established according to the orthogonality between the parity check matrix and the generator matrix of the punctured code. The generator matrices of the punctured and parent codes can be reconstructed by solving the linear equation set. The generator matrix of the parent code which has a minimal constraint length, together with the corresponding generator matrix of the punctured code and the puncturing pattern, is determined to be the identification result. However, this method requires that there exist no errors in the received sequence. It also cannot be applied in general cases where the parent code rate is $1/n$ with n being the codeword length of the parent convolutional code.

To address this limitation, an identification method was proposed by Cluzeau [4]. First, the parity check matrix of the punctured convolutional code is estimated by searching for the dual words exhaustively. After this, a canonical generator polynomial matrix of the punctured code can be reconstructed according to the orthogonality between the parity check matrix and the generator matrix. Finally, all the possible parent code lengths and puncturing patterns are tested. Under each hypothesis, the generator matrix of the parent code and the puncturing pattern can be recovered based on the properties of the generator matrix of the blocked code. Similarly, the generator matrix of the parent code with a minimal constraint length is considered to be the identification result. Since the dual words and punctur-

ing pattern are searched for exhaustively, the computational complexity of this method is quite high. If the generator matrix of the punctured code is known a priori, the generator matrix of the parent code and the puncturing pattern can be identified by using the polycyclic pseudocirculant (PCPC) matrix proposed in [5]. Nevertheless, it is difficult to have a priori knowledge of the true generator matrix of a punctured code. Usually, only an equivalent generator matrix can be obtained by employing the methods for identifying convolutional codes put forward variously in [6–12].

In practice, the rates of most punctured and parent convolutional codes are $K/(K+1)$ and $1/n$ respectively [13]. In this case, the identification of a punctured convolutional code by using the existing methods requires either an enormous amount of computation or a priori knowledge of the generator matrix of the punctured convolutional code. In order to solve the limitations of these methods, a fast method for blind identification of a punctured convolutional code is presented in this paper. In our proposed method, there is no need to search for the dual word and puncturing pattern exhaustively. It is also robust against bit errors.

The rest of this paper is organized as follows. In Sec. 2, the construction of a punctured convolutional code is briefly reviewed. In Sec. 3, a recursive algorithm for estimating the dual word and the generator polynomial bases of a punctured convolutional code is proposed. In Sec. 4, the generator matrices of the punctured and parent codes, together with the puncturing pattern, are identified simultaneously. This is done by drawing on the properties of the generator matrix of the blocked code and the PCPC matrix. The method's computational complexity is analyzed and simulation results are shown in Sec. 5. Conclusions are provided in Sec. 6.

2. Construction of a Punctured Convolutional Code

The procedure for constructing a punctured convolutional code is shown in Fig. 1.

A $(n,1,m)$ parent convolutional code, where m is the constraint length of the convolutional code, is equivalent to its Kth blocked code [4]. This Kth blocked code can be denoted by a $K \times nK$ generator polynomial matrix. The construction procedure for the Kth blocked code is as follows.

Let us assume that the generator matrix of a parent code is $\mathbf{G}(D) = [g_1(D), g_2(D), \ldots, g_n(D)]$. Each polynomial $g_i(D)$ can be split into K different polynomials and expressed as

$$g_i(D) = \sum_{j=0}^{K-1} D^j q_{i,j}(D^K), \tag{1}$$

where

$$q_{i,j}(D) = D^{-j/K} g_i^{[j]_K}(D^{1/K}). \tag{2}$$

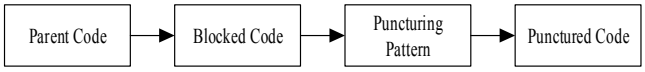

Fig. 1. Construction of a punctured convolutional code.

The polynomial $g_i^{[j]_K}(D)$ consists of the terms of $g_i(D)$ whose degree d modulo K is congruent to j. Thus, the Kth PCPC matrix $\mathbf{Q}_i^{[K]}(D)$ of $g_i(D)$ can be expressed as

$$\mathbf{Q}_i^{[K]} = \begin{bmatrix} q_{i,0}(D) & q_{i,1}(D) & \cdots & q_{i,K-1}(D) \\ Dq_{i,K-1}(D) & q_{i,0}(D) & \cdots & q_{i,K-2}(D) \\ \vdots & \vdots & \ddots & \vdots \\ Dq_{i,1}(D) & Dq_{i,2}(D) & \cdots & q_{i,0}(D) \end{bmatrix}. \tag{3}$$

Incorporating (2) into (3), we obtain that

$$\mathbf{Q}_i^{[K]} = \begin{bmatrix} g_i^{[0]_K}(D^{1/K}) & D^{-1/K} g_i^{[1]_K}(D^{1/K}) & \cdots & D^{-(K-1)/K} g_i^{[K-1]_K}(D^{1/K}) \\ D^{1-(K-1)/K} g_i^{[K-1]_K}(D^{1/K}) & g_i^{[0]_K}(D^{1/K}) & \cdots & D^{-(K-2)/K} g_i^{[K-2]_K}(D^{1/K}) \\ \vdots & \vdots & \ddots & \vdots \\ D^{1-1/K} g_i^{[1]_K}(D^{1/K}) & D^{1-2/K} g_i^{[2]_K}(D^{1/K}) & \cdots & g_i^{[0]_K}(D^{1/K}) \end{bmatrix}. \tag{4}$$

By substituting the corresponding Kth PCPC matrix for each element in $\mathbf{G}(D)$ and interleaving the columns at the depth K, the generator matrix of the Kth blocked code is obtained and denoted as $\mathbf{G}^{[K]}(D)$.

The puncturing pattern $\mathbf{P}$ is a $(n \times K)$ binary matrix where the (i, j) element in $\mathbf{P}$ corresponds to the $[i + n(j-1)]$th column in $\mathbf{G}^{[K]}(D)$. If the value of an element is equal to 0, the corresponding column in $\mathbf{G}^{[K]}(D)$ is deleted. Otherwise, the column is retained. Consequently, the generator matrix $\mathbf{G}_\mathbf{p}(D)$ of the punctured convolutional code is derived from $\mathbf{G}^{[K]}(D)$ by using $\mathbf{P}$.

3. A Recursive Algorithm for Estimation of the Dual Word and the Generator Polynomial Bases

3.1 Estimation of the Dual Word

For a punctured convolutional code with the code rate $K/(K+1)$ there exists a $(K+1) \times 1$ parity check matrix $\mathbf{H}_\mathbf{p}(D)$, which is orthogonal to the generator matrix $\mathbf{G}_\mathbf{p}(D)$ of the punctured code [14], i.e.,

$$\mathbf{G}_\mathrm{p}(D) \cdot \mathbf{H}_\mathrm{p}^\mathrm{T}(D) = 0. \tag{5}$$

The inner product $\boldsymbol{x}\cdot\boldsymbol{y}$ represents $\langle \boldsymbol{x}\cdot\boldsymbol{y} \rangle$ mod 2 in this paper. In order to reconstruct $\mathbf{G}_\mathbf{p}(D)$, the parity check matrix $\mathbf{H}_\mathbf{p}(D)$ has to be estimated first.

Since the punctured convolutional code sequence $\mathbf{C}(D)$ can be expressed as $\mathbf{C}(D) = \mathbf{M}(D) \cdot \mathbf{G}_\mathbf{p}(D)$, with $\mathbf{M}(D)$ being the source bit sequence, then (5) can be used to obtain the following equation

$$\mathbf{C}(D) \cdot \mathbf{H}_\mathrm{p}^\mathrm{T}(D) = 0. \tag{6}$$

According to (6), the following parity check equation set can be established

$$\mathbf{C}\cdot\mathbf{h}^{\mathrm{T}}=0 \tag{7}$$

where $\mathbf{C}$ is the received bit matrix and $\mathbf{h}$ is the dual word. By solving the parity check equation set, the dual word $\mathbf{h}$ can be estimated. Consequently, the parity check matrix $\mathbf{H}_{\mathrm{p}}(D)$ is derived. In this subsection, we proposed a recursive algorithm that can achieve fast estimation of the dual word.

Let $\hat{\mathbf{H}}$ denote the matrix consisting of the values of the elements that were estimated in the dual word, and let $\mathbf{h}'$ denote the vector consisting of the undetermined elements. If the external degree of the punctured convolutional code is d_{p}, the length of the dual word would be $(K+1)(d_{\mathrm{p}}+1)$ [10]. The steps of the recursive algorithm are as follows.

(1) Initialize $\hat{\mathbf{H}}=\boldsymbol{\phi}$ and $\mathbf{h}'=[h_1,\ h_2,\ldots,\ h_{(K+1)(d_{\mathrm{p}}+1)}]^{\mathrm{T}}$ where $\boldsymbol{\phi}$ denotes a blank matrix.

(2) For simplicity, only the general jth recursion of the algorithm is elaborated in this step. Let us assume that the matrix $\mathbf{A}$ is composed of the columns of $\mathbf{C}$ corresponding to the elements that were estimated in $\mathbf{h}$. Let us also assume that the matrix $\mathbf{B}$ is composed of the columns of $\mathbf{C}$ corresponding to the unknown elements in $\mathbf{h}$. Thus, the parity check equation set shown in (7) can now be expressed as

$$\mathbf{B}\mathbf{h}'\oplus\mathbf{A}\hat{\mathbf{H}}=\mathbf{0}. \tag{8}$$

Find the sparsest row in which the number of 1 elements is the smallest in $\mathbf{B}$. If the ith row is the sparsest row, and the 1 elements are the coefficients of the unknowns $h_{k_1},\ h_{k_2},\ldots,\ h_{k_p}$ then according to the ith equation, the modulo 2 summation value of the elements $h_{k_1},\ h_{k_2},\ldots,\ h_{k_p}$ can be obtained as follows

$$h_{k_1}\oplus h_{k_2}\oplus\cdots\oplus h_{k_p}=\mathbf{a}_i\cdot\hat{\mathbf{H}} \tag{9}$$

where $\mathbf{a}_i$ is the ith row of $\mathbf{A}$. From (9), we can get all the possible values of the vector $[\hat{h}_{k_1},\ \hat{h}_{k_2},\ldots,\ \hat{h}_{k_p}]^{\mathrm{T}}$. These vectors can then be used to expand the matrix $\hat{\mathbf{H}}$, and the elements $h_{k_1},\ h_{k_2},\ldots,\ h_{k_p}$ in $\mathbf{h}'$ are deleted. Once this is done, the jth recursion is finished.

If there are errors in the received bit sequence, it is probable to obtain an incorrect summation value of $h_{k_1},\ h_{k_2},\ldots,\ h_{k_p}$ resulting from only one parity check equation. Since there are more correct equations than incorrect ones in practice, we use several parity check equations to jointly determine the summation value in each recursion. Let us assume there are N_{eq} equations which have the same form as (9). The number of equations by which the summation value is estimated to be 1 is N^1_{eq} and the number of equations by which the summation value is estimated to be 0 is N^0_{eq}. Then, the summation value is determined according to the following rule.

When $N_{\mathrm{eq}}\geq th_{\mathrm{eq}}$,

$$\hat{h}_{k_1}\oplus\hat{h}_{k_2}\oplus\cdots\oplus\hat{h}_{k_p}=\begin{cases}1 & ,N^1_{\mathrm{eq}}>N^0_{\mathrm{eq}}\\ 0 & ,N^1_{\mathrm{eq}}<N^0_{\mathrm{eq}}\\ \{0,1\} & ,N^1_{\mathrm{eq}}=N^0_{\mathrm{eq}}\end{cases}. \tag{10}$$

When $N_{\mathrm{eq}}> th_{\mathrm{eq}}$,

$$\hat{h}_{k_1}\oplus\hat{h}_{k_2}\oplus\cdots\oplus\hat{h}_{k_p}=\{0,1\} \tag{11}$$

where th_{eq} is the smallest number of parity check equations required for determining the summation value. Equation (11) denotes that the summation is assigned two possible values, 0 and 1.

The maximum probability of incorrect determination of the summation value under the threshold th_{eq} is

$$p_{\max}=\sum_{i=\lceil th_{\mathrm{eq}}/2\rceil+1}^{2\lceil th_{\mathrm{eq}}/2\rceil}C^{i}_{2\lceil th_{\mathrm{eq}}/2\rceil}p_{\mathrm{e}}^{i}\left(1-p_{\mathrm{e}}\right)^{2\lceil th_{\mathrm{eq}}/2\rceil-i}, \tag{12}$$

$$p_{\mathrm{e}}=\sum_{i=1}^{\lceil w/2\rceil}C_w^{2i-1}\eta^{2i-1}\left(1-\eta\right)^{w-2i+1}. \tag{13}$$

The proof of (12) is shown in the appendix. Equation (13) denotes the error probability for a parity check equation, where η is the bit error ratio and w is the weight of the dual word. According to (12), we can calculate the threshold th_{eq} from the assumed $p_{\max}$. The threshold th_{eq} increases as $p_{\max}$ decreases.

(3) The recursion in step (2) is carried out again until all the elements in $\mathbf{h}$ are estimated.

As the number of estimated elements increases, more and more rows in the matrix $\mathbf{B}$ will contain just a single 1 element. This makes it possible to estimate the unknown elements of $\mathbf{h}$ one by one.

3.2 Verifying the Correct Estimation of the Dual Word

Since there is only one dual word for a punctured convolutional code with the rate $K/(K+1)$ [15], it is essential to choose the correct one among all the estimations. To verify which one is correct, the received bit matrix $\mathbf{C}$ is multiplied by an estimation $\hat{\mathbf{h}}$ of the dual word. 0 elements in the output vector indicate that the corresponding equations hold. 1 elements indicate that the equations do not hold. Define variables ξ_i, $(i=1,2,\ldots,N)$, where N is the number of parity check equations. If the ith equation holds, $\xi_i=1$. Otherwise, $\xi_i=-1$. The testing statistic is defined as $\sum_{i=1}^{N}\xi_i$. Let the hypothesis H_1 denote the estimation of the dual word is correct and the hypothesis H_0 denote the estimation is incorrect. The probability distributions of $\sum_{i=1}^{N}\xi_i$ in the cases of hypotheses H_1 and H_0 are shown as follows [16]

$$\begin{cases} H_1 : \sum_{i=1}^{N} \xi_i \sim N\left(N(1-2p_e), 4Np_e(1-p_e)\right) \\ H_0 : \sum_{i=1}^{N} \xi_i \sim N(0, N) \end{cases}. \quad (14)$$

Let us assume the false alarm probability is p_f. Since $p_f = \frac{1}{\sqrt{2\pi N}} \int_{th}^{+\infty} \exp\left(-x^2/2N\right) dx$, thus based on the constant false alarm criterion, it is straightforward to obtain the detecting threshold $th = \sqrt{N}\Phi^{-1}(1-p_f)$, where $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp\left(-t^2/2\right) dt$. If an estimation has a testing statistic that is larger than both the detecting threshold and the testing statistics of the other estimations, it is recognized as the dual word.

3.3 Estimation of the Generator Polynomial Bases

The parity check matrix $\mathbf{H_p}(D)$ can be obtained from the dual word $\mathbf{h}$. By using (5), a linear equation set can be established. The generator polynomial bases of the punctured convolutional code can be estimated by solving this equation set. If the degree of $\mathbf{H_p}(D)$ is d_p, i.e., $\deg(\mathbf{H_p}(D)) = d_p$, the degree of the ith row of $\mathbf{G_p}(D)$ is $e_{p,i} = \lfloor (d_p + i - 1)/K \rfloor$ [3]. On this basis, we can establish $(d_p + e_{p,i} + 1)$ linear equations with $(K+1)(e_{p,i}+1)$ unknowns, which are the coefficients of the generator polynomial bases. As the number of unknowns is larger than the number of equations, the linear equation set cannot be solved by using the conventional Gaussian elimination algorithm.

The equation set can be solved by our proposed recursive algorithm, but there are some differences from the recursion outlined in Sec. 3.1. First of all, because all of the equations are correct, the summation value of unknowns can be determined by only one equation in each recursion. Additionally, if there are several sparsest rows of $\mathbf{B}$ in which the positions of the 1 elements are identical, to make all equations hold, the dot products of the corresponding rows of $\mathbf{A}$ with any column of $\hat{\mathbf{H}}$ need to be equal. Suppose the indices of these rows of $\mathbf{B}$ are $i_1, i_2, \cdots, i_q$, then

$$\mathbf{a}_{i_1} \cdot \hat{\mathbf{H}} = \mathbf{a}_{i_2} \cdot \hat{\mathbf{H}} = \cdots = \mathbf{a}_{i_q} \cdot \hat{\mathbf{H}}. \quad (15)$$

If any column of $\hat{\mathbf{H}}$ does not satisfy (15), the column is deleted from $\hat{\mathbf{H}}$. The recursion is carried out until all the unknowns have been estimated.

After all the generator polynomial bases have been obtained, any combination of K generator polynomial bases may be the generator matrix $\mathbf{G_p}(D)$ of the punctured code. Using the properties of the generator matrix of the blocked code and the PCPC matrix, we will discuss the identification of $\mathbf{G_p}(D)$ further in Sec. 4.

4. Identification of the Generator Matrices of the Punctured and Parent Codes and the Puncturing Pattern

4.1 Preliminary Reconstruction of the Generator Matrix of the Punctured Code

The mathematical structure of the generator matrix of the blocked code satisfies Property 1.

Property 1 [4]: Let $\mathbf{Z}$ be the $K \times K$ matrix consisting of an upper diagonal of 1, a D in the bottom left corner and 0 everywhere else. The generator matrix $\mathbf{G}^{[K]}(D)$ of the Kth blocked code can be expressed as $\mathbf{G}^{[K]}(D) = [\mathbf{Z}^{K-1}\cdot\mathbf{M}, \mathbf{Z}^{K-2}\cdot\mathbf{M}, \ldots, \mathbf{Z}\cdot\mathbf{M}, \mathbf{M}]$, where $\mathbf{M}$ is a $K \times n$ polynomial matrix.

The generator matrix $\mathbf{G_p}(D)$ of the punctured code is obtained by deleting corresponding columns of the matrix $\mathbf{G}^{[K]}(D)$ according to the puncturing pattern. Since there is no zero vector in the puncturing pattern [3], we can get the following corollary based on Property 1.

Corollary 1: The dot product of $\mathbf{Z}^{-(K-i)}$ with the ith column of $\mathbf{G_p}(D)$, $(1 \le i \le (K-1))$ and the dot product of $\mathbf{Z}^{j-2}$ with the jth column of $\mathbf{G_p}(D)$, $(3 \le j \le (K+1))$ are columns in $\mathbf{G}^{[K]}(D)$, where $\mathbf{Z}^{-1}$ represents the inverse of the matrix $\mathbf{Z}$.

According to Corollary 1, it is possible to determine partial rows of the generator matrix $\mathbf{G_p}(D)$. Then, all the estimations of the generator matrix $\mathbf{G_p}(D)$, denoted as $\hat{\mathbf{G}}_\mathbf{p}(D)$, can be obtained by using the preliminary reconstruction result and the rest of the generator polynomial bases.

4.2 Determination of the Generator Matrices of the Punctured and Parent Codes and the Puncturing Pattern

Property 2 [5]: Define a matrix $\boldsymbol{\beta}$,

$$\boldsymbol{\beta} = \begin{bmatrix} K & K+1 & \cdots & K+(K-1) \\ K-1 & K & \cdots & K+(K-2) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & \cdots & K \end{bmatrix}. \quad (16)$$

Let the vector $\left[q_{i,(1,l)}(D), q_{i,(2,l)}(D), \cdots, q_{i,(K,l)}(D)\right]^{\mathrm{T}}$ denote the lth column of the Kth PCPC matrix of the generator polynomial $g_i(D)$ and then $g_i(D)$ can be expressed as

$$g_i(D) = \sum_{k=1}^{K} D^{\beta(k,l)-K} q_{i,(k,l)}(D^K). \quad (17)$$

According to Property 2, a parent generator polynomial can be recovered from any column of its PCPC matrix. The generator matrix $\mathbf{G_p}(D)$ contains one or more columns of the Kth PCPC matrix of each generator polyno-

mial of the parent code. Thus, the generator polynomial of the parent code can be recovered from $\mathbf{G_p}(D)$. After a parent generator polynomial has been recovered, its Kth PCPC matrix can be obtained. If a column of the PCPC matrix exists in $\mathbf{G_p}(D)$, the element in the corresponding position of the puncturing pattern is 1. Otherwise, the element is 0. Consequently, the puncturing pattern is identified.

The possible generator matrix $\hat{\mathbf{G}}(D)$ of the parent code and the corresponding puncturing pattern $\hat{\mathbf{P}}$ can be derived from $\hat{\mathbf{G}}_\mathbf{p}(D)$. The generator matrix of the parent code with the smallest constraint length, together with the corresponding generator matrix of the punctured code and the puncturing pattern, is the identification result.

5. Computational Complexity Analysis and Simulation Experiment

5.1 Computational Complexity Analysis

The computation of the proposed method is intensive in estimating the dual word and verifying the correctness of the dual word estimations. Let us define one operation as an addition or multiplication between two elements in GF(2). Assume the length of the dual word is L, the number of parity check equations is N and the number of the dual word estimations is n_1. Thus, the upper bound of the computation required for estimating the dual word is $N(2L-3)n_1$ operations. In fact, because the number of unknowns in each estimation differs, the upper bound is very relax. Verifying the correctness of the estimations requires $N(2L-1)n_1$ operations. Combining the computation of these two parts, we derive the computational complexity of the proposed method is $O(NLn_1)$. For comparison, the computational complexity of Cluzeau's method is $O(NL2^L)$ [4]. Since $n_1 << 2^L$, the computational complexity of our method is much lower than Cluzeau's.

5.2 Verification of the Effectiveness of the Proposed Method

The identification of the punctured convolutional code with the generator matrix $\mathbf{G_p}(D) = \begin{bmatrix} 1+D+D^2 & 1+D & 0 & 1 \\ D & 1+D^2 & 1+D+D^2 & 1 \\ D & D & D+D^2 & 1+D+D^2 \end{bmatrix}$ is considered in this experiment. The corresponding parent generator matrix is $\mathbf{G}(D) = \begin{bmatrix} 1+D+D^2+D^3+D^6 \\ 1+D+D^2+D^4+D^6 \\ 1+D^2+D^3+D^5+D^6 \end{bmatrix}^{\mathrm{T}}$ and the puncturing pattern is $\mathbf{P} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$. The estimation results for the dual word of the punctured convolutional code by using our proposed recursive algorithm are shown in Fig. 2.

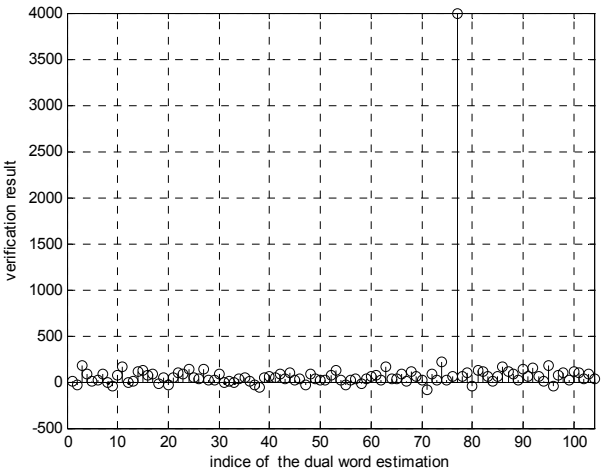

Fig. 2. Estimation of the dual word of the punctured convolutional code.

As shown in Fig. 2, more than one estimation of the dual word are obtained by using our recursive algorithm. However, only one estimation can make all of the parity check equations hold after verifying these estimations. Consequently, the binary vector $[0\,1\,1\,1\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,1\,0]^{\mathrm{T}}$ is regarded as the identification result of the dual word.

By using the identified dual word, the parity check matrix $\hat{\mathbf{H}}_\mathrm{p}(D) = \begin{bmatrix} 1+D^2+D^5 \\ 1+D+D^3+D^4+D^5+D^6 \\ 1+D^2+D^4+D^6 \\ D+D^2+D^4+D^5+D^6 \end{bmatrix}^{\mathrm{T}}$ is obtained. Furthermore, all the generator polynomial bases are derived by using $\hat{\mathbf{H}}_\mathrm{p}(D)$. They are $\left[D, D, D+D^2, 1+D+D^2\right]$, $\left[D, 1+D^2, 1+D+D^2, 1\right]$, $\left[1+D^2, D+D^2, 1+D+D^2, 0\right]$, $\left[0, 1+D+D^2, 1, D+D^2\right]$, $\left[1+D+D^2, D^2, 1, 1+D+D^2\right]$, $\left[1+D+D^2, 1+D, 0, 1\right]$ and $\left[1+D^2, 1, D+D^2, D+D^2\right]$.

Let us define a matrix $\mathbf{Z} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ D & 0 & 0 \end{bmatrix}$. According to Property 1, the dot product of $\mathbf{Z}^{-2}$ with the first column of $\hat{\mathbf{G}}_\mathbf{p}(D)$ and the dot product of $\mathbf{Z}^{-1}$ with the second column of $\hat{\mathbf{G}}_\mathbf{p}(D)$ should be polynomial vectors that do not contain a term with a negative degree. Therefore, we can determine the second and the third rows of $\hat{\mathbf{G}}_\mathbf{p}(D)$ are $\left[D, 1+D^2, 1+D+D^2, 1\right]$ and $\left[D, D, D+D^2, 1+D+D^2\right]$. Since $\deg(\hat{\mathbf{H}}_\mathrm{p}(D)) = 6$, the degree of the ith row of the matrix $\mathbf{G}^{[K]}(D)$ is $e_i = \left\lfloor (d_\mathrm{p} + i - 1)/K \right\rfloor = 2, (1 \le i \le 3)$ [3]. Thus, the degrees of the polynomial vectors obtained by the dot product of $\mathbf{Z}^2$ with the third column of $\hat{\mathbf{G}}_\mathbf{p}(D)$ and the dot product of $\mathbf{Z}$ with the forth column of $\hat{\mathbf{G}}_\mathbf{p}(D)$ cannot be larger than 2. Therefore, we can determine that the first row of $\hat{\mathbf{G}}_\mathbf{p}(D)$ is $\left[1+D+D^2, 1+D, 0, 1\right]$. Consequently, the

reconstruction result of the punctured generator matrix is

$$\hat{\mathbf{G}}_{\mathrm{p}}(D)=\begin{bmatrix}1+D+D^2 & 1+D & 0 & 1\\ D & 1+D^2 & 1+D+D^2 & 1\\ D & D & D+D^2 & 1+D+D^2\end{bmatrix}.$$

Furthermore, according to Property 2, the parent generator polynomial $\hat{g}_1(D)=1+D+D^2+D^3+D^6$ and its PCPC matrix $\hat{\mathbf{Q}}_1^{[3]}(D)=\begin{bmatrix}1+D+D^2 & 1 & 1\\ D & 1+D+D^2 & 1\\ D & D & 1+D+D^2\end{bmatrix}$ is got from the first column of $\hat{\mathbf{G}}_{\mathbf{p}}(D)$. Comparing $\hat{\mathbf{G}}_{\mathbf{p}}(D)$ with $\hat{\mathbf{Q}}_1^{[3]}(D)$, we can determine the first row of the puncturing pattern is [1,0,1]. In the same way, the other generator polynomial of the parent code and rows of the puncturing pattern are obtained by using the other columns of $\hat{\mathbf{G}}_{\mathbf{p}}(D)$. Eventually, the reconstruction results of the parent generator matrix and the puncturing pattern are

$$\hat{\mathbf{G}}(D)=\begin{bmatrix}1+D+D^2+D^3+D^6\\ 1+D+D^2+D^4+D^6\\ 1+D^2+D^3+D^5+D^6\end{bmatrix}^{\mathrm{T}} \quad \text{and} \quad \hat{\mathbf{P}}=\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 0 & 1 & 0\end{bmatrix}.$$

The experimental results indicate the proposed identification method is effective.

5.3 Performance Analysis of the Proposed Method

First, the robustness of the proposed method to bit errors in the received sequence is analyzed. The estimation of the dual word is a key step in the method. The correct identification of the punctured convolutional code depends on the correct estimation of the dual word. The dual word estimations of the (3,2,2) and (4,3,2) punctured convolutional codes are considered respectively. The number of parity check equations is 4000. The threshold th_{eq} in the recursive algorithm is assumed to be 4. In the situations of different bit error ratios, the correct estimation ratios for the dual words of the two punctured convolutional codes by using our recursive algorithm and the matrix analysis algorithm [9] are shown in Fig. 3 and Fig. 4.

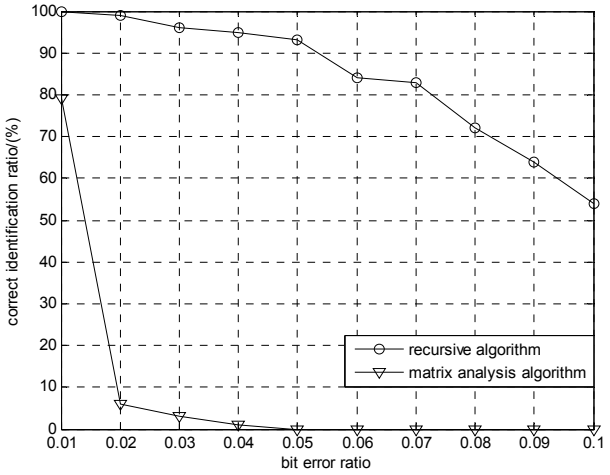

Fig. 3. Correct estimation ratio for the dual word of the (3,2,2) punctured convolutional code.

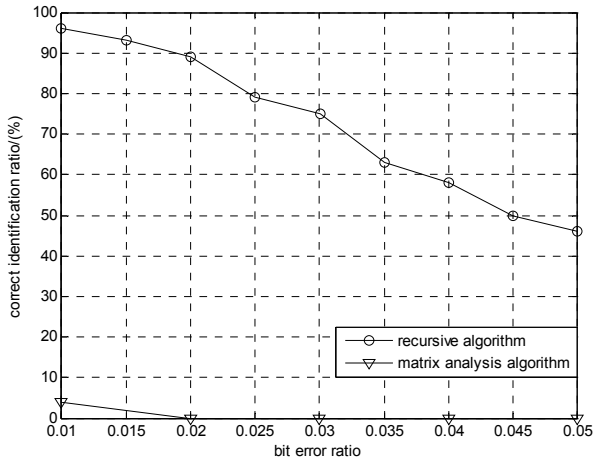

Fig. 4. Correct estimation ratio for the dual word of the (4,3,2) punctured convolutional code.

As illustrated in Fig. 3 and Fig. 4, the robustness of our recursive algorithm to bit errors is much better than that of the matrix analysis algorithm. Additionally, under the same bit error ratio, the correct estimation ratio for the dual word of the (3,2,2) punctured convolutional code is larger than that for the (4,3,2) punctured convolutional code. The reason is that the length of the dual word of the (4,3,2) punctured convolutional code is larger and so there are more unknowns to be estimated.

The second experiment analyzes the relationship between the correct estimation ratio for the dual word and the threshold th_{eq} in the recursive algorithm. The same (3,2,2) punctured convolutional code as that used in the first experiment is considered. Let the value of the threshold th_{eq} be 2, 3, 4 and 5 respectively. The other experimental conditions are the same as those in the second experiment. The correct estimation ratios in the cases of different thresholds are shown in Fig. 5.

Figure 5 shows that under the same bit error ratio, the correct estimation ratio increases along with the increase of the threshold th_{eq}. The experimental result also verifies the correctness of the theoretical analysis in Sec. 3.1.

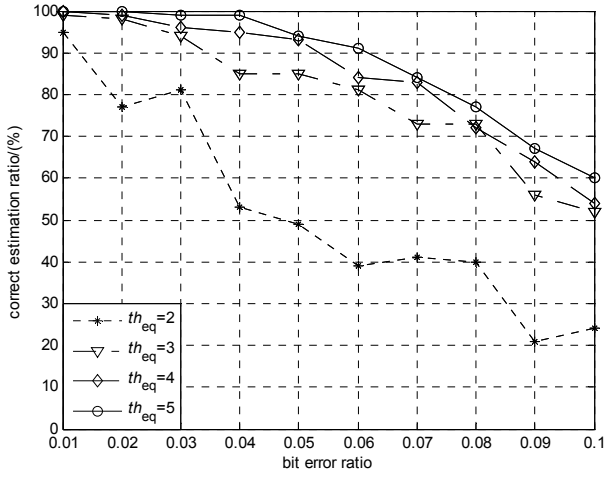

Fig. 5. Correct estimation ratios in the case of different thresholds th_{eq}.

6. Conclusion

A fast method for blind identification of a punctured convolutional code is presented in this paper. First, the dual word and generator polynomial bases are estimated by using the proposed recursive algorithm. Second, based on the structural properties of the blocked matrix, the generator matrix of the punctured convolutional code is reconstructed preliminarily. Finally, using the relationship between a generator polynomial of the parent code and its corresponding PCPC matrix, we can determine the reconstruction result of the generator matrix of the punctured code and recover the generator matrix of the parent code and the puncturing pattern simultaneously. As the dual word and the puncturing pattern do not need to be searched for exhaustively, the computational complexity of the proposed method is much lower than that of Cluzeau's method. Moreover, the method is also robust to bit errors in the received sequence.

References

[1] TODD, K. M. *Error Correction Coding, Mathematical Methods and Algorithms*. 1st ed. Hoboken (USA): John Wiley & Sons, Inc., 2005. ISBN: 0471648000

[2] HAGENAUER, J. Rate compatible punctured convolutional codes and their applications. *IEEE Transactions on Communications*, 1988, vol. 36, no.4, p. 389–400. DOI: 10.1109/26.2763

[3] LU, P. Z., SHEN, L., ZOU, Y., et al. Blind recognition of punctured convolutional codes. *Science in China Ser. E Information Sciences*, 2005, vol. 35, no. 2, p. 173–185. DOI: 10.1360/03yf0480 (in Chinese)

[4] CLUZEAU, M., FINIASZ, M. Reconstruction of punctured convolutional codes. In *Proceedings of Information Theory Workshop*. Taormina (Italy), 2009, p. 75–79. DOI: 10.1109/ITW.2009.5351168

[5] MARAZIN, M., GAUTIER, R., BUREL, G. Algebraic method for blind recovery of punctured convolutional encoders from an erroneous bitstream. *IET Signal Processing*, 2012, vol. 6, no. 2, p. 122–131. DOI: 10.1049/iet-spr.2010.0343

[6] FILIOL, E. Reconstruction of convolutional encoders over GF(p). In *Proceedings of the 6th IMA Conference on Cryptography and Coding*. Heidelberg (Germany), 1997, p. 100–110. DOI: 10.1007/BFb0024454

[7] BARBIER, J., SICOT, G., HOUCKE, S. Algebraic approach for the reconstruction of linear and convolutional error correcting codes. *World Academy of Science, Engineering and Technology*, 2006, vol. 2, no. 3, p. 113–118.

[8] MARAZIN, M., GAUTIER, R., BUREL, G. Dual code method for blind identification of convolutional encoder for cognitive radio receiver design. In *Proceedings of the 5th IEEE Broadband Wireless Access Workshop*. Honolulu (USA), 2009, p. 1–6. DOI: 10.1109/GLOCOMW.2009.5360726

[9] MARAZIN, M., GAUTIER, R., BUREL, G. Blind recovery of k/n rate convolutional encoders in a noisy environment. *EURASIP Journal on Wireless Communications and Networking*, 2011, vol. 2011, no. 168, p. 1–9. DOI: 10.1186/1687-1499-2011-168

[10] COTE, M., SENDRIER, N. Reconstruction of convolutional codes from noisy observation. In *Proceedings of the IEEE International Symposium on Information Theory*. Seoul (South Korea), 2009, p. 546–550. DOI: 10.1109/ISIT.2009.5205729

[11] YANG, X. J., LIU, J. C., ZHANG, Y. Blind recognition of (n,k,m) convolutional codes based on solving check-sequence. *Journal of Astronautics*, 2013, vol. 34, no. 4, p. 568–573. DOI: 10.3873/j.issn.1000-1328.2013.04.017 (in Chinese)

[12] HUANG, L., CHEN, W. G., CHEN, E. H. Blind recognition of k/n rate convolutional encoders from noisy observation. *Journal of Systems Engineering and Electronics*, 2017, vol. 28, no. 2, p. 235–243. DOI: 10.21629/JSEE.2017.02.04

[13] CAIN, J. B., CLARK, G. C. GEIST, J. Punctured convolutional codes of rate (n-1)/n and simplified maximum likelihood decoding. *IEEE Transactions on Information Theory*, 1979, vol. 25, no. 1, p. 97–100. DOI: 10.1109/TIT.1979.1055999

[14] MORIYA, S., KIKUCHI, K., SASANO, H. Construction of high rate punctured convolutional codes through dual codes. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2015, vol. 98, no. 7, p. 1579–1583. DOI: 10.1587/transfun.E98.A.1579

[15] SOTEH, A. G., BIZAKI, H. K. On the analytical solution of rank problem in the convolutional code identification context. *IEEE Communications Letter*, 2016, vol. 20, no. 3, p. 442–445. DOI: 10.1109/LCOMM.2016.2519519

[16] SU, S. J., ZHOU, J., HUANG, Z. P., et al. Blind identification of convolutional encoder parameters. *The Scientific World Journal*, 2014, no. 5, p. 1–9. DOI: 10.1155/2014/798612

About the Authors…

Shu Nan HAN (corresponding author) was born in 1989. He received his B.S. degree and M.S. degree from the Electronic Engineering Institute, China in 2012 and 2015, respectively. He is currently pursuing his Ph.D. degree in the National University of Defense Technology. His research interests include blind identification of channel encoders and sparse reconstruction theory.

Min ZHANG was born in 1966. He received his Ph.D. degree from Anhui University, China. Now he is a professor in the National University of Defense Technology. His research interests include communication signal processing and intelligent computation.

Xin Hao LI was born in 1989. He received his Ph.D. degree from the Electronic Engineering Institute, China in 2016. His research interests include blind identification of channel encoders and frame structures.

Appendix

Proof of the relationship between the threshold th_{eq} and the maximum error probability p_{max} for the determination of the summation value of unknowns.

Proof: When $N_{eq} \geq th_{eq}$ and $N_{eq} = 2n$, $(n \in \mathrm{N}^{+})$, event A denotes that the determination of the summation value of unknowns is incorrect. Thus, the probability that event A occurs is

$$P(A)=\sum_{i=n+1}^{2n} C_{2n}^{i} p_{\mathrm{e}}^{i}(1-p_{\mathrm{e}})^{2n-i} \tag{1}$$

where p_{e} is the error probability for a parity check equation.

When $N_{\mathrm{eq}} \geq th_{\mathrm{eq}}$ and $N_{\mathrm{eq}} = 2n + 1$, event B denotes that the determination of the summation value is incorrect. Thus, the probability that event B occurs is

$$P(B)=\sum_{i=n+1}^{2n+1} C_{2n+1}^{i} p_{\mathrm{e}}^{i}(1-p_{\mathrm{e}})^{2n+1-i}. \tag{2}$$

Each term in (2) is divided by the corresponding term with the same i in (1). Thus we obtain

$$\frac{C_{2n+1}^{i} p_{\mathrm{e}}^{i}(1-p_{\mathrm{e}})^{2n+1-i}}{C_{2n}^{i} p_{\mathrm{e}}^{i}(1-p_{\mathrm{e}})^{2n-i}}=\frac{2n+1}{2n+1-i}(1-p_{\mathrm{e}}),\ \ (n+1 \leq i \leq 2n). \tag{3}$$

Since $p_{\mathrm{e}} > 0.5$, thus

$$\frac{2n+1}{2n+1-i}(1-p_{\mathrm{e}})>1,\ \ (n+1 \leq i \leq 2n). \tag{4}$$

According to (4), it follows that each term in (2) is larger than the corresponding term in (1). Consequently,

$$P(B) > P(A). \tag{5}$$

When $N_{\mathrm{eq}} = 2n + 3$, event C denotes that the determination of the summation value is incorrect. The probability that event C occurs is

$$P(C)=\sum_{i=n+2}^{2n+3} C_{2n+3}^{i} p_{\mathrm{e}}^{i}(1-p_{\mathrm{e}})^{2n+3-i}. \tag{6}$$

Since

$\sum_{i=0}^{2n+1} C_{2n+1}^{i} p_{\mathrm{e}}^{i}(1-p_{\mathrm{e}})^{2n+1-i}=1$ and $\sum_{i=0}^{2n+3} C_{2n+3}^{i} p_{\mathrm{e}}^{i}(1-p_{\mathrm{e}})^{2n+3-i}=1,$

thus

$$\sum_{j=0}^{n}[(\frac{1-p_{\mathrm{e}}}{p_{\mathrm{e}}})^{2n+1-2j}+1] C_{2n+1}^{2n+1-j} p_{\mathrm{e}}^{2n+1-j}(1-p_{\mathrm{e}})^{j}=1, \tag{7}$$

$$\sum_{j=0}^{n+1}[(\frac{1-p_{\mathrm{e}}}{p_{\mathrm{e}}})^{2n+3-2j}+1] C_{2n+3}^{2n+3-j} p_{\mathrm{e}}^{2n+3-j}(1-p_{\mathrm{e}})^{j}=1. \tag{8}$$

Suppose that

$a_j = C_{2n+1}^{2n+1-j} p_{\mathrm{e}}^{2n+1-j}(1-p_{\mathrm{e}})^{j}$ and $b_j = C_{2n+3}^{2n+3-j} p_{\mathrm{e}}^{2n+3-j}(1-p_{\mathrm{e}})^{j}$,

then

$$\begin{cases} P(B)=\sum_{j=0}^{n} a_j \\ P(C)=\sum_{j=0}^{n+1} b_j \end{cases}, \tag{9}$$

$$\sum_{j=0}^{n}[(\frac{1-p_{\mathrm{e}}}{p_{\mathrm{e}}})^{2n+1-2j}+1] a_j=1, \tag{10}$$

$$\sum_{j=0}^{n+1}[(\frac{1-p_{\mathrm{e}}}{p_{\mathrm{e}}})^{2n+3-2j}+1] b_j=1. \tag{11}$$

As $(\frac{1-p_{\mathrm{e}}}{p_{\mathrm{e}}})^{k+1} > (\frac{1-p_{\mathrm{e}}}{p_{\mathrm{e}}})^{k}, k \in \mathrm{N}^{+}$, thus

$$\frac{\sum_{j=0}^{n+1}(\frac{1-p_{\mathrm{e}}}{p_{\mathrm{e}}})^{2n+3-2j} b_j}{\sum_{j=0}^{n+1} b_j} > \frac{\sum_{j=0}^{n}(\frac{1-p_{\mathrm{e}}}{p_{\mathrm{e}}})^{2n+1-2j} a_j}{\sum_{j=0}^{n} a_j}. \tag{12}$$

According to (9), (10), (11) and (12), it follows that

$$P(B) > P(C). \tag{13}$$

Based on above analysis, we derive that if th_{eq} is an odd number, the maximum error probability for the determination is

$$p_{\max}=\sum_{i=\lceil th_{\mathrm{eq}}/2 \rceil+1}^{th_{\mathrm{eq}}+1} C_{th_{\mathrm{eq}}+1}^{i} p_{\mathrm{e}}^{i}\left(1-p_{\mathrm{e}}\right)^{th_{\mathrm{eq}}+1-i}. \tag{14}$$

Otherwise, if th_{eq} is an even number, the maximum error probability for the determination is

$$p_{\max}=\sum_{i=th_{\mathrm{eq}}/2+1}^{th_{\mathrm{eq}}} C_{th_{\mathrm{eq}}}^{i} p_{\mathrm{e}}^{i}\left(1-p_{\mathrm{e}}\right)^{th_{\mathrm{eq}}-i}. \tag{15}$$

Combining (14) and (15), we obtain the relationship between the threshold th_{eq} and the maximum error probability $p_{\max}$ for the determination of the summation value of unknowns is

$$p_{\max}=\sum_{i=\lceil th_{\mathrm{eq}}/2 \rceil+1}^{2\lceil th_{\mathrm{eq}}/2 \rceil} C_{2\lceil th_{\mathrm{eq}}/2 \rceil}^{i} p_{\mathrm{e}}^{i}\left(1-p_{\mathrm{e}}\right)^{2\lceil th_{\mathrm{eq}}/2 \rceil-i}. \tag{16}$$