Blind recognition of punctured convolutional codes

LU Peizhong[1], LI Shen[2], ZOU Yan[1] & LUO Xiangyang[2]

1. Department of Computer Science and Engineering, Fudan University, Shanghai 200433, China;
2. Institute of Information Engineering, Information and Engineering University, Zhengzhou 450002, China
Correspondence should be addressed to Lu Peizhong (email: pzlu@fudan.edu.cn)
Received August 9, 2004

Abstract This paper presents an algorithm for blind recognition of punctured convolutional codes which is an important problem in adaptive modulation and coding. For a given finite sequence of convolutional code, the parity check matrix of the convolutional code is first computed by solving a linear system with adequate error tolerance. Then a minimal basic encoding matrix of the original convolutional code and its puncturing pattern are determined according to the known parity check matrix of the punctured convolutional code.

Keywords: **blind recognition, punctured convolutional code, generator matrix, puncturing pattern.**

DOI: 10.1360/03yf0480

1 Introduction

Adaptive modulation and coding (AMC) can remarkably improve bandwidth-efficiency, information-rate and robustness in time-varying channel (fading channel)[1,2]. Therefore the techniques will be considered to be used in communication systems, especially 3G mobile communication system, software radio system and multimedia service system[3]. But, how to recognize the demodulation and decoding method quickly, only by the received data information in the receiver, is a very important problem. This paper addresses the problem. Obviously, this problem is also one of the key problems in the field of information interception.

Utilizing RCPC codes (Rate-Compatible Punctured Convolutional) to realize AMC is a simple and efficient method[3,4]. RCPC codes, presented by Hagenauer[5], having good performance, form a subclass of punctured convolutional codes[6]. Begin and Haccoun[7] studied the construction technique of punctured codes, showed that any punctured code can be obtained by means of an orthogonal puncturing pattern, and also gave lots of good punctured codes. McEliece[8] researched the method of puncturing. Recently, Shen et al.[9] constructed the generator matrix of the punctured convolutional code on the condition that the original convolutional code and puncturing pattern are given, and also gave the necessary and sufficient condition on the inverse problem: representing a known

convolutional code as a punctured convolutional code.

This paper solves the problem of blind recognition of punctured convolutional codes. For a given finite sequence of a convolutional code, the parity check matrix of the convolutional code is first computed by solving a linear system with adequate error tolerance. Then a minimal basic encoding matrix of the original convolutional code and its puncturing pattern are determined according to the known parity check matrix of the punctured convolutional code. In practical applications, an original rate-$1/2$ convolutional code is usually used to generate a rate-$(n-1)/n$ punctured convolutional code. Thus we simply focus on the punctured convolutional codes with rate $(n-1)/n$.

2 Problem descriptions

For detailed treatment of punctured convolutional codes, readers can refer to refs. [5, 7, 8, 10]. We introduce some basic concepts for conveniently describing the main problem of this paper.

Let $F=\{0,1\}$ be the binary field, Z the set of all integers, and $Z_k=\{0,1,\cdots,k-1\}$, where k is a positive integer. Let $F[D]$ be the polynomial ring, $F(D)$ the rational function field.

A rate k/n convolutional code $\mathcal{C}$ is a k-dimensional subspace of $F(D)^n$. A generator matrix $G(D)$ for $\mathcal{C}$ is a $k\times n$ matrix over $F(D)$ whose rows form a basis for $\mathcal{C}$. If $G(D)$ is a polynomial matrix with full rank, then $G(D)$ is an *encoding matrix*. If $G(D)$ is an encoding matrix with right inverse, then $G(D)$ is a *basic encoding matrix*.

For a k/n-rate convolutional code $\mathcal{C}$, when k information bits $\boldsymbol{u}_t=(u_{0,t},u_{1,t},\cdots,u_{k-1,t})$ are input at time t, then $\mathcal{C}$ will output n bits $\boldsymbol{v}_t=(v_{0,t},v_{1,t},\cdots,v_{n-1,t})$. We call $\boldsymbol{u}_t$ the *information word* at t, and $\boldsymbol{v}_t$ the *code word* at t.

The following describes a simple procedure for constructing a high rate-l/n punctured code from an original rate-$1/2$ convolutional code.

Let $\mathcal{C}$ be a $1/2$-convolutional code, $U(D)=\sum_{j=0}^{\infty}u_jD^j$ the input information sequence, and $V(D)=\left(\sum_{j=0}^{\infty}v_{j,0}D^j,\sum_{j=0}^{\infty}v_{j,1}D^j\right)$ the output code sequence in $\mathcal{C}$. If we block the input information sequence and the output code sequence into l and $2l$ subsequences respectively as follows:

$$U'(D)=(U_0,U_1,\cdots,U_{l-1}),$$
$$V'(D)=(V_{0,0},V_{0,1},V_{1,0},V_{1,1},\cdots,V_{l-1,0},V_{l-1,1}),$$

where $U_i=\sum_{j=0}^{\infty}u_{lj+i}D^j$, $V_{i,k}=\sum_{j=0}^{\infty}v_{lj+i,k}D^j$, $i=0,1,\cdots,l-1,k=0,1$, then the set of all kinds of $V'(D)$ is an $l/2l$-rate convolutional code $\mathcal{C}'$ which is equivalent to $\mathcal{C}$.

Hence, for the code $\mathcal{C}'$, at time t, the input information word and the corresponding

output code word are

$$\boldsymbol{u}'_t = (u_{lt}, u_{lt+1}, \cdots, u_{lt+l-1}),$$
$$\boldsymbol{v}'_t = (v_{lt,0}, v_{lt,1}, v_{lt+1,0}, v_{lt+1,1}, \cdots, v_{lt+l-1,0}, v_{lt+l-1,1}).$$

Let $P \in F^{2l}$. P has n components of value 1, and $2l-n$ components of value 0. In every output code word $\boldsymbol{v}'_t$ of the code $\mathcal{C}'$, $2l-n$ bits are deleted according to the positions of 0 in P. The remaining n bits form a code word $\boldsymbol{c}'_{Pt}$ of the punctured convolutional code $\mathcal{C}_P$ at t. Here P is called the puncturing pattern. Clearly, the punctured convolutional code $\mathcal{C}_P$ has rate l/n. Therefore, the procedure of construction can be simply described as follows:

$$\mathcal{C} \overset{\text{block}}{\Longrightarrow} \mathcal{C}' \overset{\text{puncture}}{\Longrightarrow} \mathcal{C}_P.$$

Let $G(D)'$ be a generator matrix of $\mathcal{C}'$, P a puncturing pattern. After deleting the columns of $G^{'}(D)$ according to the positions of 0 in P, the remaining matrix $G_P(D)$ is a generator matrix of the punctured convolutional code $\mathcal{C}_P$.

Let $\alpha_P = (\alpha_P(0), \alpha_P(1), \cdots, \alpha_P(n-1))$ be a position vector of P, where $\alpha_P(i)$ is the position of the i-th 1 in P. For example, if $P = (0,1,1,0,0,0,1)$, then $\alpha_P = (1,2,6)$.

Let $\beta = (\beta_0, \beta_1, \cdots, \beta_{k-1}) \in Z_n^k$. Let $[G(D)]_\beta$ denote the matrix deduced from $G(D)$ with columns of β, namely

$$[G(D)]_\beta = \left[G^{(\beta_0)}(D), G^{(\beta_1)}(D), \cdots, G^{(\beta_{k-1})}(D)\right],$$

where $G^{(\beta_i)}(D)$ is the β_i-th column of $G(D)$.

In design of punctured code, the puncturing pattern should satisfy the following conditions:

1) In order for $\mathcal{C}_P$ to have uniquely decoding property, the generator matrix $G_P(D)$ should be a basic encoding matrix. Hence there exists an $n \times l$ polynomial matrix Q, such that $G_P(D) \cdot Q = I_l$.

2) The puncturing pattern should not delete all the bits of the output code word $\boldsymbol{v}_t$ of the source code $\mathcal{C}$ at each time t. Therefore, P must satisfy that $(P(2i), P(2i+1)) \neq (0,0), i = 0, 1, \cdots, l-1$.

In this paper, we default that the puncturing patterns P to be blind recognized satisfy the previous conditions. In fact, the punctured convolutional codes with nice properties constructed by Begin and Haccoun[7] satisfy the conditions.

If $G(D)$ and P are known, it is easy to construct the generator matrix $G_P(D) = [G(D)']_{\alpha_P}$ of the punctured code $\mathcal{C}_P$. In this paper, we want to solve the inverse problem as follows:

Mail problem. Let $\boldsymbol{r}_i, i = 0, 1, \cdots, N$ be a received sequence of signal words of a transmitted sequence of code words of an unknown punctured convolutional code $\mathcal{C}_P$

through a noise channel, where $\boldsymbol{r}_i = (r_{i,0}, r_{i,1}, \cdots, r_{i,n-1})$, $r_{i,j} \in F_2$. Find the generator matrix $G(D)$ of the source code $\mathcal{C}$ and the corresponding puncturing pattern P.

We will solve the main problem in this paper in two steps. In the first step, the parity check matrix $H_P(D)$ of $\mathcal{C}_P$ will be solved from a linear system constructed by the sequence of signal words $\boldsymbol{r}_i, i = 0, 1, \cdots, N$. In the second step, the generator matrix $G(D)$ of the source code $\mathcal{C}$ and the corresponding puncturing pattern P will be computed according to the matrix $H_P(D)$.

3 Blind recognition of parity check matrix

For convenience in description, we only consider to recognize the binary punctured convolutional codes $\mathcal{C}_P$ of rate $\frac{n-1}{n}$. Let $G_P(D)$ be an $(n-1) \times n$ encoding matrix of $\mathcal{C}_P$. Let $H_P(D)$ be the parity check matrix of $\mathcal{C}_P$. Then

$$G_P(D) \cdot H_P(D) = 0.$$

Since the rank of $G_P(D)$ is full, $H_P(D)$ is an $n \times 1$ polynomial matrix. We want to compute the matrix $H_P(D)$. Let $H_P(D)^T = (h_0(D), h_1(D), \cdots, h_{n-1}(D))$.

Let $\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_N$ be a sequence of code words of the punctured convolutional code $\mathcal{C}_P$ such that

$$\Pr(r_{i,j} = v_{i,j}) = 1 - p, i = 0, 1, \cdots, N, j = 0, 1, \cdots, n-1.$$

3.1 Noiseless case

To compute the polynomials $h_i(D)$, we first estimate the maximum degree $k = \max_{0 \leqslant i \leqslant n-1}(\deg h_i(D))$, and let $h_i(D) = h_{i,0} + h_{i,1}D + \cdots + h_{i,k}D^k$.

If $N > (n+1) \times (k+1) - 1$, we can construct the following linear system:

$$\sum_{j=0}^{k} \sum_{i=0}^{n-1} r_{i,k-j+s} h_{i,j} = 0, s = 0, 1, \cdots, N-k. \tag{1}$$

The minimal matrix $H_P(D)$ can be obtained by selecting a nonzero solution of (1).

Rules of selection for minimal matrix $H_P(D)$ are as follows. Since the parity check matrix $H_P(D)$ is an $n \times 1$ matrix, we need to find a suitable nonzero solution of linear equation (1). Let the $n(k+1)$ unknown variables of eq. (1) be

$$(h_{0,0}, h_{1,0}, \cdots, h_{n-1,0}, h_{0,1}, h_{1,1}, \cdots, h_{n-1,1}, \cdots, h_{0,k}, h_{1,k}, \cdots, h_{n-1,k}),$$

and a canonical basis of the subspace of solutions be the rows of the following matrix

$$\begin{pmatrix} q_{0,0} & q_{0,1} & \cdots & q_{0,n(k+1)-1-r-1} & q_{0,n(k+1)-1-r} & 1 & 0 & \cdots & 0 \\ q_{1,0} & q_{1,1} & \cdots & q_{1,n(k+1)-1-r-1} & q_{1,n(k+1)-1-r} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ q_{r-1,1} & q_{r-1,1} & \cdots & q_{r-1,n(k+1)-1-r-1} & q_{r-1,n(k+1)-1-r} & 0 & 0 & \cdots & 1 \end{pmatrix}, \tag{2}$$

where r is dimension of subspace of solutions. Let J_i be the first column in i-th row with nonzero component value. Let $j_i = \left\lfloor \frac{J_i}{n} \right\rfloor, i = 0, 1, \cdots, r-1$. Find a minimal integer i_0

such that $0 \leqslant i_0 \leqslant r-1$, and

$$j_{i_0} + \left\lfloor \frac{r-i_0}{n} \right\rfloor = \max_{0 \leqslant i \leqslant r-1} \left\{ j_i + \left\lfloor \frac{r-i}{n} \right\rfloor \right\}.$$

Then the best solution we want is

$$h_{i,j} = q_{i_0,(j+j_{i_0})n+i}, i = 0, 1, \cdots, n-1, j = 0, 1, \cdots, k - \left(j_{i_0} + \left\lfloor \frac{r-i_0}{n} \right\rfloor \right). \quad (3)$$

The selected polynomials $h_i(D), i=0, 1, \cdots, n-1$ satisfy that $\max_{0 \leqslant i \leqslant n-1}\{\deg h_i(D)\}$ is minimal.

Remark 1. If the source information sequence has a very low linear complexity, the dimension of subspace of the solutions of (1) will be so large that the nonzero solution selected by the previous rules is not only a parity check, but also a scrambling polynomial or some padding pattern with short period for information sequence .

Usually, we need N received signal words, where $N \approx (n+1) \times (k+1)$. The number of unknown variables is $n \times (k+1)$. To guarantee the solvability of the linear equation (1), the estimated maximum degree k of the component polynomials of $H_P(D)$ should be large enough. But, if the k is overlarge, the number of signal words to be acquired, N, will be too large, which results in the remarkable increase of the computing complexity, and decrease of possibility of noiseless condition. The computing complexity of solving linear system (1) by the well-known Gaussian method is $O(N^3)$.

From the form of linear system (1), we can find an important fact that the problem of blind recognition of parity check matrix of a convolutional code is a natural generalization of the problem of sequence synthesis which is a very important problem in cryptography, algebraic coding, and linear systems. The famous BM algorithm[11] is used to solve the problem of sequence synthesis. Recently, based on theory of Gröbner basis, we find a fast algorithm to compute the syzygy of homogeneous ideal generated by some polynomials in $F[x, y]$. The algorithm is a generalization of the BM algorithm, and can be used to solve eq. (1) with computing complexity $O(N^2)$. Limited by the space, it is impossible to give a detailed introduction to the fast algorithm of syzygy computation, which needs a plentiful background of commutative algebra. Fortunately, in practical applications, usually $k < 15$ and $n \leqslant 8$. Thus it is fast enough to find the solutions of (1) by Gaussian method.

3.2 Noise case

If the error probability $p < 5 \times 10^{-3}$, we deal with the problem with two different methods.

In the case of broad band communications, since a great deal of signal words can be obtained in a moment, we can repeatedly compute eq. (1) by trial and error with different sequences of signal words.

In the case of narrow band communications without admission of long delay, since the volume of received signal words is limited in a short time, we should adopt an avoiding

error strategy. Since, in practice, $n \times (k+1) < 60$, the number of errors in the received $N+1$ signal words may be less than 2. We can exhaust all the combination of two errors to find the best solution of (1).

If the error probability is a little larger, for example, $p = 2 \times 10^{-2}$, we further assume that the number of unknown variables of eq. (1) is less than 60. Then, we have the following computation of probability:

$$\Pr\left(\sum_{j=0}^{k}\sum_{i=0}^{n-1} r_{i,k-j+s}h_{i,j} = 0\right) \approx 0.65, s = 0, 1, \cdots, N-k. \tag{4}$$

Based on eq. (4), we can use a method of correlation attack in cryptanalysis to solve eq. (1). More details of correlation attack can be found in ref. [12].

4 Generator matrices of punctured codes and properties

Shen et al.[9] gave the expression of a generator matrix of a punctured convolutional code. We present a more detailed description in this section.

Lemma 1[9]**.** Let $\mathcal{C}$ be a parent rate-$1/m$ convolutional code with polynomial generator matrix $G(D) = (g_1(D), \cdots, g_m(D))$, where $g_k(D) = \sum_{j=0}^{\infty} g_{k,j}D^j \in F[D], k = 1, \cdots, m$. Let $\hat{g}_{k,i}(D) = \sum_{j=0}^{\infty} g_{k,lj+i}D^j$, $i = 0, 1, \cdots, l-1, k = 1, \cdots, m$. Then the generator matrix $G'(D)$ of the rate-l/ml convolutional code $\mathcal{C}'$ equivalent to $\mathcal{C}$ is $G'(D) =$

$$\begin{pmatrix}
\hat{g}_{1,0}(D) & \cdots & \hat{g}_{m,0}(D) & \hat{g}_{1,1}(D) & \cdots & \hat{g}_{m,1}(D) & \cdots & \hat{g}_{1,l-1}(D) & \cdots & \hat{g}_{m,l-1}(D) \\
D\hat{g}_{1,l-1}(D) & \cdots & D\hat{g}_{m,l-1}(D) & \hat{g}_{1,0}(D) & \cdots & \hat{g}_{m,0}(D) & \cdots & \hat{g}_{1,l-2}(D) & \cdots & \hat{g}_{m,l-2}(D) \\
D\hat{g}_{1,l-2}(D) & \cdots & D\hat{g}_{m,l-2}(D) & D\hat{g}_{1,l-1}(D) & \cdots & D\hat{g}_{m,l-1}(D) & \cdots & \hat{g}_{1,l-3}(D) & \cdots & \hat{g}_{m,l-3}(D) \\
\vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \ddots & \vdots & \cdots & \vdots \\
D\hat{g}_{1,1}(D) & \cdots & D\hat{g}_{m,1}(D) & D\hat{g}_{1,2}(D) & \cdots & D\hat{g}_{m,2}(D) & \cdots & \hat{g}_{1,0}(D) & \cdots & \hat{g}_{m,0}(D)
\end{pmatrix}.$$

Example 1. Let $m = 2$, $\mathcal{C}$ an original rate-$1/2$ convolutional code with generator matrix $G(D) = (g_1(D), g_2(D))$, where $g_1(D) = 1 + D^2 + D^3 + D^5 + D^6, g_2(D) = 1 + D + D^2 + D^3 + D^6$. If $l = 3$, we have $\hat{g}_{1,0}(D) = 1 + D + D^2$, $\hat{g}_{1,1}(D) = 0$, $\hat{g}_{1,2}(D) = 1 + D$, $\hat{g}_{2,0}(D) = 1 + D + D^2$, $\hat{g}_{2,1}(D) = \hat{g}_{2,2}(D) = 1$. Then the generator matrix $G'(D)$ of the rate-$3/6$ convolutional code $\mathcal{C}'$ equivalent to $\mathcal{C}$ is

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

Example 2. Conditions are the same as Example 1. The rate of the punctured code is $3/4$, and the puncturing pattern is $P = (0, 1, 1, 0, 1, 1)$ with its corresponding position vector $\alpha_P = (1, 2, 4, 5)$. The generator matrix $G'(D)$ of the rate-$3/6$ convolutional code

$\mathcal{C}'$ equivalent to $\mathcal{C}$ is the same as in Example 1. Thus the generator matrix of the punctured code is

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

Lemma 2. Let $G(D) = (g_1(D), \cdots, g_m(D))$ be a polynomial generator matrix of a $1/m$ rate convolutional code $\mathcal{C}$. Then $G(D)$ is an encoding matrix if and only if $G'(D)$ is an encoding matrix, where $G'(D)$ is defined as in Lemma 1.

Proof. If $G(D)$ is an encoding matrix, then $G(0) \neq 0$. Without loss of generality, let $g_1(0) = 1$. Then the $m \cdot j$-columns, $j = 0, 1, \cdots, m$ of $G(0)$ consist of a triangle matrix with $g_1(0)$ in diagonals. Thus $G(0)$ has full rank. Conversely, if $G(0)$ has full rank, then $g_i(0) \neq 0$, for some i, and $G(0)$ has full rank.

Let $G(D)$ be a $k \times n$ polynomial matrix. Let $G_i(D) = (g_{i1}(D), ..., g_{in}(D))$ denote the i-th row of $G(D)$, and we define the degree e_i of $G_i(D)$ as the maximum degree of its components, namely, $e_i = \deg G_i(D) = \max_j\{\deg g_{i,j}(D)\}$. In a similar way we define the degree of any n-tuple of polynomials as the maximum degree of any component.

McEliece[8] defined the *internal degree* and *external degree* of $G(D)$ as follows:

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

Let $G_1(D), G_2(D)$ be generator matrices of $\mathcal{C}$. If there exists a nonsingular polynomial matrix $T(D)$ such that $G_1(D) = T(D)G_2(D)$, we say $G_1(D)$ and $G_2(D)$ are equivalent. Equivalent matrices generate the same convolutional code.

Lemma 3[10]**.** Let $G_1(D)$ be a rational generator matrix of $\mathcal{C}$. Then there exists a basic encoding matrix $G_2(D)$ of $\mathcal{C}$ such that $G_1(D)$ and $G_2(D)$ are equivalent.

Let $G[D]_h$ be constructed by the coefficients of the row degrees, namely, $G[D]_h = (g_{ijh})_{k\times n}$, where

$$g_{ijh} = \begin{cases} 1, & \deg g_{ij}(D) = e_i, \\ 0, & \deg g_{ij}(D) < e_i. \end{cases}$$

If $G(D)$ is a basic encoding matrix, and $G[D]_h$ has full rank, then $G(D)$ is called a minimal basic encoding matrix.

Lemma 4[8]**.** A $k \times n$ polynomial matrix $G(D)$ is minimal if and only if extdeg $G(D) =$ intdeg$G(D)$.

Lemma 5[8]**.** If $G(D) = (g_1(D), \cdots, g_m(D))$ is a minimal basic encoding matrix of $\mathcal{C}$, then $G'(D)$ is a minimal basic encoding matrix of $\mathcal{C}'$.

Lemma 6[10]**.** Let $G_1(D), G_2(D)$ be equivalent minimal basic encoding generator

matrices of a rate-k/n convolutional code $\mathcal{C}$, $e_{1,i}, e_{2,i}$ the i-th row degrees of $G_1(D)$, $G_2(D)$. If they are ordered from small to large, without loss of generality, we get $(e_{1,0}, e_{1,1}, \cdots, e_{1,k-1})$ and $(e_{2,0}, e_{2,1}, \cdots, e_{2,k-1})$. Then $(e_{1,0}, e_{1,1}, \cdots, e_{1,k-1}) = (e_{2,0}, e_{2,1}, \cdots, e_{2,k-1})$.

Lemma 7[8]**.** Let $G(D)$ be a polynomial generator matrix of a rate-k/n convolutional code $\mathcal{C}$, e_i the i-th row degree of $G(D)$. Then the $(lj+i)$-th row degree of $G'(D)$ is $\left\lfloor \frac{e_j+i}{l} \right\rfloor$, $i = 0, 1, \cdots, l-1$, $j = 0, 1, \cdots, k-1$.

Corollary 1. Let $G(D) = (g_1(D), \cdots, g_m(D))$ be a polynomial generator matrix and

$$\max\{\deg g_1(D), \cdots, \deg g_m(D)\} = d.$$

Then the i-th row degree of $G^{'}(D)$ is $\lfloor \frac{d+i}{l} \rfloor$, $i = 0, 1, \cdots, l-1$. Moreover, the sum of all row degrees of $G'(D)$ is d.

Theorem 1. Let $G(D) = (g_1(D), \cdots, g_m(D))$ be a polynomial generator matrix of an original rate-$1/m$ convolutional code $\mathcal{C}$, P a puncturing pattern. Let $e_{P,i}$ be the i-th row degree of $G_P(D)$, and $d = \max\{\deg g_1(D), \cdots, \deg g_m(D)\}$. Then

$$\sum_{i=0}^{l-1} e_{P,i} \leqslant d.$$

Moreover, if $\deg g_1(D) = \cdots = \deg g_m(D)$ and P satisfies that $(P(mi), P(mi+1), \cdots, P(mi+m-1)) \neq (0, 0, \cdots, 0), i \in Z_l$, then $e_{P,i} = \lfloor \frac{d+i}{l} \rfloor$, $i = 0, 1, \cdots, l-1$, and $\sum_{i=0}^{l-1} e_{P,i} = d$.

Proof. Let e'_i be the i-th row degree of $G'(D)$. Then

$$e_{P,i} \leqslant e'_i.$$

By Corollary 1, we have

$$e'_i = \left\lfloor \frac{d+i}{l} \right\rfloor, i = 0, 1, \cdots, l-1.$$

Therefore

$$e_{P,i} \leqslant \left\lfloor \frac{d+i}{l} \right\rfloor.$$

Since we have the

$$\sum_{i=0}^{l-1} \left\lfloor \frac{d+i}{l} \right\rfloor = d,$$

it implies that

$$\sum_{i=0}^{l-1} e_{P,i} \leqslant d.$$

Moreover, if $\deg g_1(D) = \cdots = \deg g_m(D) = d$, then there are m consequent columns, from the ms-th column to the $(ms+m-1)$-th column for some $s \in Z_l$, in the i-th row of $G'(D)$ with polynomial degrees equal to the i-th row degree of $G'(D)$. Since P satisfies that $(P(mj), P(mj+1), \cdots, P(mj+m-1)) \neq (0, 0, \cdots, 0)$, $j \in Z_l$, we

can see that these m polynomials cannot be deleted at all when we construct $G_P(D)$ from $G'(D)$ by P. Thus $e_{P,i} = e'_i, i = 0, 1, \cdots, l-1$, and $\sum_{i=0}^{l-1} e_{P,i} = d$.

Corollary 2. Let $G(D) = (g_1(D), \cdots, g_m(D))$ be a polynomial generator matrix of an original rate-$1/m$ convolutional code, where $\deg g_1(D) = \cdots = \deg g_m(D) = d$. Let P_1, P_2 be puncturing patterns, and $e_{P_1,i}$ and $e_{P_2,i}$ be the i-th row degrees of $G_{P_1}(D)$ and $G_{P_2}(D)$ respectively. If $(P_k(mi), P_k(mi+1), \cdots, P_k(mi+m-1)) \neq (0, 0, \cdots, 0)$, $k = 1, 2$, we have

$$e_{P_{1,i}} = e_{P_{2,i}} = \left\lfloor \frac{d+i}{l} \right\rfloor. \tag{5}$$

5 Recognition of punctured codes

In this section, we realize the blind recognition of rate-$(n-1)/n$ punctured codes. Different original rate-$1/2$ convolutional codes and different puncturing patterns may generate the same punctured code. Our task is to find the optimal among those original convolutional codes and their puncturing patterns.

Let $g(D) = \sum_{j=0}^{\infty} g_j D^j$ be a power series(or possibly just a polynomial), $\hat{g}_i(D) = \sum_{j=0}^{\infty} g_{lj+i} D^j$, $i = 0, 1, \cdots, l-1$. The matrix $g^{[l]}(D)$ is defined by

$$g^{[l]}(D) := \begin{pmatrix} \hat{g}_0(D) & \hat{g}_1(D) & \cdots & \hat{g}_{l-1}(D) \\ D\hat{g}_{l-1}(D) & \hat{g}_0(D) & \cdots & \hat{g}_{l-2}(D) \\ D\hat{g}_{l-2}(D) & D\hat{g}_{l-1}(D) & \cdots & \hat{g}_{l-3}(D) \\ \vdots & \vdots & \ddots & \vdots \\ D\hat{g}_1(D) & D\hat{g}_2(D) & \cdots & \hat{g}_0(D) \end{pmatrix}. \tag{6}$$

Let π_l be a permutation on Z_{ml} such that

$$\pi_l(mi+j) = jl+i,\ j = 0, 1, \cdots, m-1, i = 0, 1, \cdots, l-1. \tag{7}$$

Then we have the following results.

Corollary 3[9]**.** Let $G(D) = (g_1(D), \cdots, g_m(D))$ be a basic encoding generator matrix of an original rate-$1/m$ convolutional code $\mathcal{C}$ and P a puncturing pattern. Then the corresponding generator matrix $G_P(D)$ of the punctured code $\mathcal{C}_P$ is

$$G_P(D) = [G(D)']_{\alpha_P} = [g_1^{[l]}(D), \cdots, g_m^{[l]}(D)]_{\pi_l(\alpha_P)}.$$

Theorem 2. Let $H(D) = (h_0(D), h_1(D), \cdots, h_{n-1}(D)) \in F^n[D]$ be a parity-check matrix of an arbitrary rate-$(n-1)/n$ convolutional code. Then there exists a rate-$1/2$ convolutional code $\mathcal{C}$ and a puncturing pattern P such that $H(D)$ is a parity check matrix of the corresponding punctured code $\mathcal{C}_P$. Moreover the generator matrix of $\mathcal{C}$ is $G(D) = (g_1(D), g_2(D))$, where

$g_1(D) = h_{n-1}(D^{n-1}), g_2(D) = h_{n-2}(D^{n-1}) + Dh_{n-3}(D^{n-1}) + \cdots + D^{n-2}h_0(D^{n-1})$.

The puncturing pattern $P = (1, 0, 1, 0, \cdots, 1, 0, 1, 1) \in Z_2^{2(n-1)}$.

Proof. Let $g_1(D) = h_{n-1}(D^{n-1})$, $g_2(D) = h_{n-2}(D^{n-1}) + Dh_{n-3}(D^{n-1}) + \cdots + D^{n-2}h_0(D^{n-1})$. By (6), we have

$$g_1^{[n-1]}(D) = h_{n-1}(D)I_{n-1}, g_2^{[n-1]}(D) = \left(A_{(n-1)\times(n-2)}, B_{(n-1)\times 1}\right),$$

where I_{n-1} is an $(n-1)$-order identity matrix, $B_{(n-1)\times 1} = (h_0(D), h_1(D), \cdots, h_{n-2}(D))^T$.

Let $P = (1, 0, 1, 0, \cdots, 1, 0, 1, 1) \in Z_2^{2(n-1)}$. Then $\alpha_P = (0, 2, \cdots, 2(n-2), 2(n-2)+1)$. By (7), we have $\pi_{n-1}(2j) = j, j = 0, 1, \cdots, n-2$, and $\pi_{n-1}(2(n-2)+1) = n-1+n-2 = 2n-3$. Thus $\pi_{n-1}(\alpha_P) = (\pi_{n-1}(0), \pi_{n-1}(2), \cdots, \pi_{n-1}(2(n-2)), \pi_{n-1}(2(n-2)+1)) = (0, 1, \cdots, n-2, 2n-3)$. By Corollary 3, the generator matrix of punctured code $\mathcal{C}_P$ is

$$G_P(D) = \left[g_1^{[n-1]}(D), g_2^{[n-1]}(D)\right]_{\pi_{n-1}(\alpha_P)} = \left[g_1^{[n-1]}(D), B_{(n-1)\times 1}\right].$$

$G_P(D)$ is the following matrix

$$G_P(D) = \begin{pmatrix} h_{n-1}(D) & 0 & \cdots & 0 & h_0(D) \\ 0 & h_{n-1}(D) & \cdots & 0 & h_1(D) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & h_{n-1}(D) & h_{n-2}(D) \end{pmatrix}. \tag{8}$$

It is clear that

$$G_P(D)H(D)^T = 0.$$

Theorem 2 shows that an arbitrary rate-$(n-1)/n$ convolutional code can be generated from an original rate-$1/2$ convolutional code by puncturing. Moreover the degree of the minimal basic encoding generator matrix of the original rate-$1/2$ convolutional code is $\leqslant (n-1)d + n - 2$, where d is the degree of $H(D)$. Although, by Theorem 2, we can find a generator matrix of the original rate-$1/2$ convolutional code and a puncturing pattern corresponding to a given rate-$(n-1)/n$ convolutional code, the constraint length of the original rate-$1/2$ convolutional code may be too large to be suitable for a Viterbi decoding algorithm. The search for an original convolutional code with as low degree as possible is the main task to be carried out in this section. Note that, the matrix $G_P(D)$ in (8) is a basic encoding matrix if and only if $h_{n-1}(D) = 1$.

Lemma 8[10]**.** Let $G(D)_{k\times n}$ be a basic encoding matrix of a convolutional code $\mathcal{C}$, $H(D)_{(n-k)\times n}$ a basic encoding generator matrix of the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$. Let e_i be the i-th row degree of $G(D)_{k\times n}$, $i = 0, 1, \cdots, k-1$, and $e_{H,j}$ the j-th row degree of $H(D)_{(n-k)\times n}$, $j = 0, 1, \cdots, n-k-1$. Then

$$\sum_{i=0}^{k-1} e_i = \sum_{j=0}^{n-k-1} e_{H,j}.$$

Lemma 9[10]**.** Let $G_1(D)_{k\times n}$ be a minimal basic encoding matrix of a convolutional code $\mathcal{C}$, $G_2(D)_{k\times n}$ a polynomial generator matrix of $\mathcal{C}$, and $e_{1,i}, e_{2,i}$ the i-th row degrees

of $G_1(D)_{k\times n}$, $G_2(D)_{k\times n}$ respectively, $i = 0, 1, \cdots, k-1$. If $G_1(D)_{k\times n}$ and $G_1(D)_{k\times n}$ are equivalent, we have

$$\sum_{i=0}^{k-1} e_{1,i} \leqslant \sum_{i=0}^{k-1} e_{2,i}.$$

Lemma 10. Let $H(D)_{(n-k)\times n}$ be a basic encoding matrix of the dual code $\mathcal{C}^{\perp}$, and $G(D)_{k\times n}$ a basic encoding matrix of $\mathcal{C}$, i.e. $G(D)\cdot H(D)^t = 0$, and $G(D)$ has a right inverse. Then $G(D)$ is a minimal basic encoding matrix.

Proof. By Corollary 2.24 of ref. [10], there is a minimal basic encoding matrix $S(D)$ equivalent to $G(D)$. Thus, by Theorem 2.20 of ref. [10], there exists a $k \times k$ invertible polynomial matrix $Q(D)$ such that

$$G(D) = Q(D)S(D). \tag{9}$$

Thus both $S(D)$ and $G(D)$ are basic encoding matrices of $\mathcal{C}$. By Lemma 8, we know that

$$\begin{aligned}\sum_{j=0}^{n-k-1} e_{H,j} &= ext\deg G(D)\\ &\geqslant int\deg G(D)\\ &= int\deg S(D)\\ &= ext\deg S(D)\\ &= \sum_{j=0}^{n-k-1} e_{H,j}.\end{aligned}$$

Thus $ext\deg G(D) = int\deg G(D)$. It implies that $G(D)$ is a minimal basic encoding matrix.

Theorem 3. Let $G(D) = (g_1(D), \cdots, g_m(D))$ be a polynomial generator matrix of an original rate-$1/m$ convolutional code $\mathcal{C}$, P a puncturing pattern, and $G_P(D)$ is a basic encoding matrix of the punctured code $\mathcal{C}_P$. Let $H(D) = (h_0(D), h_1(D), \cdots, h_{n-1}(D))$ be a polynomial parity check matrix of $\mathcal{C}_P$ and $\gcd(h_0(D), h_1(D), \cdots, h_{n-1}(D)) = 1$. Then

$$\max\{\deg(g_1(D)), \cdots, \deg(g_m(D))\} \geqslant \max_{0\leqslant i\leqslant n-1}\{\deg h_i(D)\}. \tag{10}$$

Moreover, if $\deg(g_1(D)) = \cdots = \deg(g_m(D)) = d$, and punctured pattern satisfies

$$(P(mi), \cdots, P(mi+m-1)) \neq 0, i \in Z_{n-2},$$

then

$$d = \max_{0\leqslant i\leqslant n-1}\{\deg h_i(D)\}. \tag{11}$$

Proof. Let $\max\{\deg(g_1(D)), \cdots, \deg(g_m(D))\} = d$, where d is a positive integer. Let $G'(D)$ be the polynomial generator matrix of the rate-$(n-1)/k(n-1)$ convolutional code $\mathcal{C}'$ equivalent to $\mathcal{C}$, e'_i the i-th row degree of $G'(D)$, and $e_{P,i}$ the i-th row degree of $G_P(D)$, $i = 0, 1, \cdots, n-2$. By Corollary 1, we have

$$e'_i = \left\lfloor \frac{d+i}{n-1} \right\rfloor, i = 0, 1, \cdots, n-2.$$

Thus

$$\sum_{i=0}^{n-2} e'_i = d.$$

Since $G_P(D)$ is constructed by some columns of $G'(D)$, we have

$$\sum_{i=0}^{n-2} e_{P,i} \leqslant \sum_{i=0}^{n-2} e'_i = d.$$

By Lemma 3, there exists a minimal basic encoding matrix $G_{PM}(D)$ of $\mathcal{C}_P$ equivalent to $G_P(D)$. Let $e_{PM,i}$ be the ith row degree of $G_{PM}(D)$, $i = 0, 1, \cdots, n-2$. By Lemma 9,

$$\sum_{i=0}^{n-2} e_{PM,i} \leqslant \sum_{i=0}^{n-2} e_{P,i} \leqslant d.$$

Since $H(D)$ is a parity check matrix of $\mathcal{C}_P$ and the rate of $\mathcal{C}_P$ is $(n-1)/n$, $H(D)$ is a generator matrix of $\mathcal{C}_P^{\perp}$. Since $\gcd(h_0(D), h_1(D), \cdots, h_{n-1}(D)) = 1$, there exists polynomials $h'_0(D), h'_1(D), \cdots, h'_{n-1}(D)$ such that

$$\sum_{i=0}^{n-1} h_i(D) h'_{n-i}(D) = 1.$$

Let $H'(D) = (h'_0(D), h'_1(D), \cdots, h'_{n-1}(D))^T$. Then $H(D)H'(D) = 1$. Thus $H(D)$ is a basic encoding matrix of $\mathcal{C}_P^{\perp}$. By Lemma 6,

$$\begin{aligned} \max_{0 \leqslant i \leqslant n-1} \{\deg h_i(D)\} &= \sum_{i=0}^{n-2} e_{PM,i} \\ &\leqslant d. \end{aligned}$$

Therefore (10) holds.

Moreover, if $\deg(g_1(D)) = \cdots = \deg(g_m(D)) = d$ and P satisfies: $(P(mi), \cdots, P(mi+m-1)) \neq 0, i \in Z_{n-2}$, then by Theorem 2

$$e_{P,i} = \left\lfloor \frac{d+i}{n-1} \right\rfloor, i = 0, 1, \cdots, n-2.$$

Hence

$$\sum_{i=0}^{n-2} e_{P,i} = d.$$

Since $G_P(D)$ is a basic polynomial encoding matrix of $\mathcal{C}_P$, by Lemma 10, $G_P(D)$ is a minimal basic encoding matrix of $\mathcal{C}_P$. Thus, by Lemma 8, we have

$$\begin{aligned} d &= \sum_{i=0}^{n-2} e_{P,i} \\ &= \operatorname{ext}\deg(G_P(D)) \\ &= \max_{0 \leqslant i \leqslant n-1} \{\deg h_i(D)\}. \end{aligned} \tag{12}$$

If a parity check matrix of a rate-$(n-1)/n$ punctured code is known, we can further determine a generator matrix of an original rate-$1/2$ convolutional code. Theorem 2 and

Theorem 3 give respectively the upper and lower bounds of the degree of generator matrix of the optimal original convolutional code. By Theorem 2, we can compute an original rate-$1/2$ convolutional code and a puncturing pattern. But the code may be not the optimal. we need to search original rate-$1/2$ convolutional codes with the minimal degree and puncturing patterns. By Theorem 2 and Theorem 3, we present the following algorithm:

Algorithm 2. Find original generator matrix and puncturing pattern P

INPUT :$H(D) = (h_0(D), h_1(D), \cdots, h_{n-1}(D))$
$d = \max_{0 \leqslant i \leqslant n-1} (\deg h_i(D))$, $S = \{P \in F_2^{2n-2} | w(P) = n\}$, $k = (n-1)(d+1)-1$,
$GP = \{\}$,
$M = k+1$, $g_1(D) = \sum_{i=0}^{k} a_i D^i$, $g_2(D) = \sum_{i=0}^{k} b_i D^i$.
Construct a formal matrix $G'(D)$
WHILE $(S \neq \Phi)$ DO

$P \in S$. Construct the matrix $G_P(D) = [G'(D)]_{\alpha_P}$.

According to $G_P(D)H(D)^T = 0$, rearrange the linear system

$$G \cdot (a_0, a_1, \cdots, a_k, b_0, b_1, \cdots, b_k)^T = 0, \tag{13}$$

where G is an $(n-1) \times 2(k+1)$ matrix over F.

Let Ω be the set of nonzero solutions of eq. (13).

Represent each element in Ω as $(\bar{a}, \bar{b})$, where $\bar{a} = (a_0, a_1, \cdots, a_k) \in F^k$,

and denote $\bar{a}(D) = a_0 + a_1 D + \cdots + a_k D^k$ a polynomial.

IF $(\Omega \neq \emptyset)$

DegP$= \min_{(\bar{a},\bar{b}) \in \Omega} \{\max\{\deg(\bar{a}(D)), \deg(\bar{b}(D))\}\}$

IF (DegP$= M$)

$GP = \{(\bar{a}, \bar{b}) \in \Omega | \text{DegP} = \max\{\deg(\bar{a}(D)), \deg(\bar{b}(D))\}\}$,

$S = S \backslash P$, CONTINUE.

IF (DegP$< M$)

$M =$DegP, $GP = \{(\bar{a}, \bar{b}) \in \Omega | \text{DegP} = \max\{\deg(\bar{a}(D)), \deg(\bar{b}(D))\}\}$

$S = S \backslash P$, CONTINUE.

ELSE $S = S \backslash P$.
OUTPUT: All the minimal solutions in GP.

Remark 2. 1) There are $\binom{2n-1}{n}$ punctured patterns to be searched in Algorithm 2. Since n is a small positive integer, usually $n \leqslant 8$, $\binom{2n-1}{n}$ may not be a big integer. 2) The main computation is to solve the linear system (13). The linear system has $2(n-1)(d+1)$ unknown variables of $a_i, b_i, i = 0, 1, \cdots, (n-1)d + n - 2$ over F. Since n is a small integer, solving the linear system in F is very fast. 3) By Theorem 2, our algorithm can

find a generator matrix $(g_1(D), g_2(D))$ with minimal degree and a punctured pattern P.

We can improve Algorithm 2 by considering the conditions on the puncturing pattern P. Since P should satisfy the conditions in Theorem 1, the number of punctured patterns to be searched can be largely reduced. Moreover, by Theorem 3, the degree of generator of the optimal original convolutional code is equal to the degree of parity check matrix. Hence, Algorithm 2 can be improved in the two aspects:

a) Determine whether P satisfies the conditions in Theorem 3. Thus the number of patterns to be searched is $2^{n-2}\,(n-1)$, which is much less than $\binom{2n-1}{n}$.

b) Only search the original generator matrices with degree equal to the degree of the parity check matrix, namely, let $k = d$ as an initial value, and $g_1(D) = \sum_{i=0}^{d} a_i D^i$, $g_2(D) = \sum_{i=0}^{d} b_i D^i$. Therefore the unknown variables to be determined are $2(d+1)$. Since $2(d+1) < 2(n-1)(d+1)$, the improved algorithm will be much faster.

Example 3. Suppose a parity check matrix obtained is

$$H(D) = \left(D^5, 1+D^4+D^5, 1+D^2+D^3+D^5+D^6, 1+D+D^2+D^4+D^6\right).$$

By Algorithm 2, we can easily recognize the optimal generator matrix $G(D) = (g_1(D), g_2(D))$, where $g_1(D) = 1+D^2+D^3+D^5+D^6$, $g_2(D) = 1+D+D^2+D^3+D^6$, and $P = (1,0,1,0,1,1)$.

Example 4. Let

$$H(D) = (1+D^3+D^4+D^5, 1+D+D^5, 1+D+D^2+ D^5+D^6, 1+D^2+D^4+D^6)$$

be the parity check matrix. By Algorithm 2, we find the minimal generator matrix $G(D) = (g_1(D), g_2(D))$ where $g_1(D) = 1+D+D^6+D^7+D^8+D^9+D^{10}+D^{12}+D^{13}+D^{17}$, $g_2(D) = 1+D^3+D^6+D^7+D^8+D^9+D^{10}+D^{11}+D^{12}+D^{13}+D^{14}+D^{16}+D^{17}$, and $P = (0,1,1,0,1,1)$. Note that $\deg G(D) = 17 > \deg H(D) = 6$. Theorem 3 implies that $G_P(D)$ is not a basic encoding matrix , namely $G_P(D)$ has no right inverse.

6 Conclusions

We study the construction and properties of punctured codes. Punctured codes from original rate-$1/2$ convolutional codes are the emphasis. An algorithm is presented to solve the problem of blind recognition of rate-$(n-1)/n$ punctured codes.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant Nos. 10171017, 90204013), Special Funds of Authors of Excellent Doctoral Dissertation in China (Grant No. 200084), and Shanghai Science and Technology Funds (Grant No. 035115019).

References

1. Alouini, M. S., Goldsmith, A. J., Capacity of Rayleigh fading channels under different adaptive transmission and diversity-combining techniques, IEEE Trans. Veh. Technol., 1999, 48(4): 1165–1181.
2. Goldsmith, A. J., Chua, S. G., Variable-rate variable-power MQAM for fading channels, IEEE Trans. Comm., 1997, 45(10): 1218–1230.

3. Lee, J. M., Song, I., Jung, S. et al., A rate adaptive convolutional coding method for multicarrier DS/CDMA systems, MILCOM 2000, Los Angeles,October 2000, 932–936.
4. Barton, M., Punctured convolutional codes for supporting PCS access to ATM networks, ICC'99, Vanconver, June 1999, 1880–1884.
5. Hagenauer, J., Rate-compatible punctured convolutional codes (RCPC Codes) and their application, IEEE Trans. Comm., 1988, 36(4): 389–400.
6. Cain, J. B., Clark, G. C., Geist, J. M., Punctured convolutional codes of rate$(n-1)/n$ and simplified maximum likelihood decoding, IEEE Trans Inform Theory, 1979, 25(1): 97–100.
7. Begin, G., Haccoun, D., High-rate punctured convolutional codes: structure properties and construction techniques, IEEE Trans. Comm., 1989, 37(11): 1381–1385.
8. McEliece, R. J., The algebraic theory of convolutional codes, in Handbook of Coding Theory, Amsterdam: Elesevier, 1999.
9. Shen, B. Z., Patapoutian, A., McEwen, P. A., Punctured recursive convolutional encoders and their applications in turbo codes, IEEE Trans. Inform. Theory, 2001, 47(6): 2300–2320.
10. Johannesson, R., Zigangirov, K. S., Fundamentals of Convolutional Codes, Priscataway, NJ: IEEE Press, 1999.
11. Berlekamp, E. R., Algebraic Coding Theory, New York: McGrw-Hill, 1968.
12. Chose, P., Joux, A., Mitton, M., Fast correlation attacks: An algorithmic point of view, EUROCRYPT 2002, LNCS 2332, Berlin: Spinger-Verlag, 2002, 209–221.