

Blind Recognition of (n, k, m) Convolutional Code Based on Local Decision in a Noisy Environment

Wang Yao, Wang Feng-hua, Huang Zhi-tao

The College of Electronic Science and Engineering, National University of Defense Technology, Changsha, Hunan, P. R. China, 410073.

email:wangyao09a@hotmail.com

Keywords : Noisy environment; Convolution Code; Blind Recognition

Abstract. This paper consider the problem of recognition of (n, k, m) convolutional code from a corrupted bit stream in a reverse-engineering communication system. A new method based on the properties of convolutional encoders and local decision was proposed, which can construct any rate k/n convolutional encoders blindly. Because of the effective utilization of the mathematical properties, this approach presented requires small amount of received bit stream. The validity of algorithm is verified by the simulation result, and the performance is proved to be optimal.

Introduction

In recent years, the code reconstruction problem has been a research hotspot in non-cooperative signal processing field ^[1], which can ensure that the receiver has the ability to select the configuration parameters dynamically. Convolutional code is among the most used error correcting code. Here, we focus on the blind reconstruction of convolutional code.

There is much work which has been done in this domain. B.Rice^[2] proposed the first approach to identify a rate $1/n$. There are a few method based on solving linear equations, Euclidean algorithm^[3] and Key equation^[4]. However, these approaches can't be well adapted in a noisy environment. An method proposed in [5] based on WHT, can adapt to the noisy environment, but it requires a large amount of computing resources and memory. M. Marazin developed a method based on dual codes to estimate a rate k/n convolutional encoder^[6], which calculate the rate by searching. In [7], an approach was also dedicated to the same case base on solving the Check-Sequence, which cannot work effectively in a noisy environment.

In this article, we proposed an approach to recover the parameters of any rate convolutional code, which can calculate the rate directly and adapt to the noisy environment well.

The properties of convolutional code

The mathematical notation of convolutional code was recalled briefly. According to the process of coding, the codewords of (n, k, m) convolutional code, denoted by $C(x)$ can be obtained by:

$$C(x) = M(x)G(x), \quad (1)$$

where $M(x)$ is the input sequence, and $G(x)$ is the polynomial generator matrix of rank k , defined by :

$$G(x) = \begin{bmatrix} g_{1,1}(x) & g_{1,2}(x) & \cdots & g_{1,n}(x) \\ g_{2,1}(x) & g_{2,2}(x) & \cdots & g_{2,n}(x) \\ \vdots & \vdots & & \vdots \\ g_{k,1}(x) & g_{k,2}(x) & \cdots & g_{k,n}(x) \end{bmatrix}. \quad (2)$$

And we denote the memory of the i th input by μ_i : $\mu_i = \max_{j=1,2,\dots,n} \deg g_{i,j}(x)$, $\forall i = 1, 2, \dots, k$, where.

$g_{i,j}(x)$ are the elements of $G(x)$. Let μ be the overall memory of the convolutional code: $\mu = \max_{i=1,\dots,k} \mu_i = m - 1$. Then the total number of memory elements

$$\mu^\perp = \sum_{i=1}^k \mu_i. \quad (3)$$

$H(x)$ is a polynomial generator matrix of rank $(n-k) \times n$, which is a parity check matrix of $C(x)$ only if $H(x)$ satisfy:

$$C(x)H(x)^T = M(x)G(x)H(x)^T = 0. \quad (4)$$

We also can get the linear equations to solve the parity check matrix $H(x)$:

$$C(x)H^i(x)^T = [c_1(x) \ c_2(x) \ \cdots \ c_n(x)] [h_1^i(x) \ h_2^i(x) \ \cdots \ h_{n-1}^i(x) \ h_n^i(x)]^T = 0. \quad (5)$$

Let L be the overall memory of the H , $L = \max(\deg h_i^j(x))$. Then we can get an equation in the following form:

$$\sum_{j=1}^n \sum_{i=0}^L c_{i+(n-1)j} h_{L-i}^j = 0. \quad (6)$$

Moreover, in our article the binary symmetric channel (BSC) with the error probability P_e is considered to model the errors generated by the transmission system, and denote by $e(x)$ the error pattern and by $y(x)$ the received sequence so that: $y(x) = c(x) + e(x)$, where $P_r(e(i)=1) = P_e$, $P_r(e(i)=0) = 1 - P_e$. So the problem of blind recognition of convolutional code is to recover the matrix $G(x)$ from the received code sequence $y(x)$.

The model of reconstruction in a noisy environment

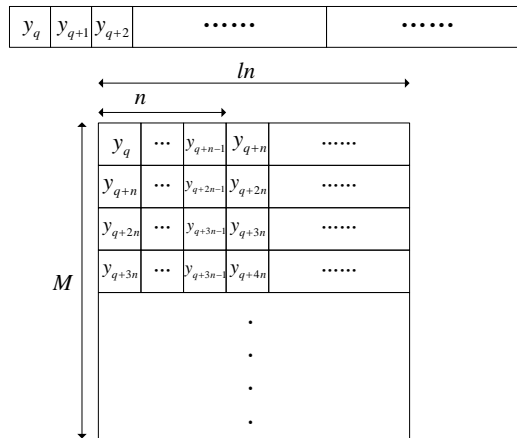


Fig 1 Example of matrix $R(M, ln)$

This section deals with the properties of convolutional code in a noisy environment, which will be used to solve the problem of blind recognition of convolutional encoder.

In the non-cooperative communication, we cannot acquire the start position accurately. We denote the start bit by y_q . According to the equation, we reshape the received code bit stream, y , into the under matrix form in Fig 1, and denoted by $R(M, ln)$. If denote the length of data stream by M' , $M = \lfloor M' / ln \rfloor$.

Then, construct N with ln rows of $R(M, ln)$. And the rank of N can be calculated by the following equation^[8]:

$$rank(N) = \min(\mu^\perp + lk, ln). \quad (7)$$

The size of the first rank deficiency is denoted by $n_a = l_{\min} \cdot n$, where, $l_{\min} = \left\lfloor \frac{\mu^\perp}{n-k} + 1 \right\rfloor$.

In the model proposed, we do not need to have code synchronized. In order to explain the procedure easily, we just deal with the case of synchronization. We denote the first bit of the output at a certain time by y_q , and if we convert the matrix N into a upper triangular matrix denoted by N' , which is illustrated in Fig 2.

$$\begin{bmatrix} I_{\mu^\perp + kl_{\min}} & P^1_{(\mu^\perp + kl_{\min}) \times (n_a - \mu^\perp - kl_{\min})} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I_k & P^2_{(n_a + k) \times (n - k)} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I_k & P^3_{(n_a + n + k) \times (n - k)} \\ 0 & 0 & 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ddots & I_k & P^i_{(n_a + (i-2)n + k) \times (n - k)} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Fig 2 Example of matrix N'

The columns of $P^i_{(n_a + n + k) \times (n - k)}$ ($i \geq 1$) is the non-zero part of the parity check matrix^[7]. Without error bits, take the diagonal elements of N' into consideration, the distribution of “0”, “1” in the diagonal will be written as:

$$\underbrace{11 \cdots 1 0 \cdots 0}_{\mu^\perp + kl_{\min}} \underbrace{1 \cdots 1 0 \cdots 0}_k \underbrace{0 \cdots 0}_{n-k} \cdots \underbrace{1 \cdots 1 0 \cdots 0}_k \underbrace{0 \cdots 0}_{n-k} \underbrace{1 \cdots 1 0 \cdots 0}_k \underbrace{0 \cdots 0}_{n-k} (*)$$

In this case, the parameters of convolutional code can be reached easily. If we denote the order of the first “0” in the diagonal by r , the other parameters can be reached:

$$l_{\min} = \left\lceil \frac{r-1}{n} \right\rceil, \quad \mu^\perp = r-1 - kl_{\min}, \quad L = \left\lceil \frac{r-1}{n} \right\rceil - 1.$$

And generally, the memory of the input μ_i satisfies that $\mu-1 \leq \mu_i \leq \mu$, so μ can be obtained: $\mu = \lceil \mu^\perp / k \rceil$. Nevertheless, in a noisy environment, this regular pattern will be broken. Because of the corrupted data, certain “0” of the diagonal will be replaced by “1”. The possible position of “0” is: $[\mu^\perp + kl_{\min}, n_a - 1] \cup [n_a + k, n_a + n - 1] \cup \dots \cup [n_a + nm + k, n_a + n(m+1) - 1] \cup \dots$. Therefore, we can get the parameters of convolutional code by the statistics of the diagonal.

An optimal code^[9], (4,2,5) convolutional code, is considered, of which the generator matrix in octal form is [17 13 5 2 ; 10 3 17 15], and the polynomial generator matrix is:

$$G = \begin{bmatrix} 1+x+x^2+x^3 & 1+x^2+x^3 & x+x^3 & x^2 \\ 1 & x^2+x^3 & 1+x+x^2+x^3 & 1+x+x^3 \end{bmatrix}$$

When P_e is 2%, we construct the matrix $R(M, ln)$ by the received data. Then construct matrix N_j with ln rows of $R(M, ln)$ successively, and take the diagonal of N_j after linear transformation. The sum of all the diagonals after normalizing, denoted by Q is shown in Fig 3

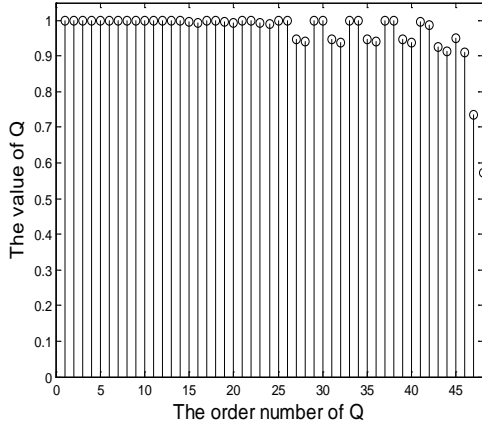


Fig 3 The value of Q

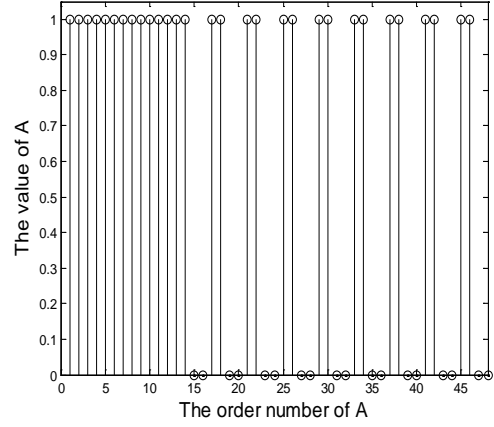


Fig 4 The value of A

If we deal with the vector Q with local decision, which means that when the second sequential “1” was discover, take n elements as a group and make a threshold decision by the mass. And we can get the vector A . We can easily ensure that $n = 4, k = 2, L = 3, m = 3$ according to the recognition model above.

Meanwhile, we can get the matrix $P_{(n_a+n+k) \times (n-k)}^i$ ($i \geq 1$) with the least degree, and get the check matrix H :

$$\begin{aligned} h_1 &= (1+x+x^3 \quad 1 \quad x^3 \quad 1+x^2+x^3) \\ h_2 &= (1+x^2+x^3 \quad 1+x^2+x^3 \quad 1+x^2 \quad x+x^2+x^3) \end{aligned}$$

Then $G(x)$ can be realized by solving the equation $G(x)H(x)^T = 0$:

$$G = \begin{bmatrix} 1+x+x^2+x^3 & 1+x^2+x^3 & x+x^3 & x^2 \\ 1 & x^2+x^3 & 1+x+x^2+x^3 & 1+x+x^3 \end{bmatrix},$$

which is the correct polynomial generator matrix.

The algorithm of parameter estimation

In this section, a new method of estimating the convolutional code blindly is put forward based on procedure proposed above. There are several key parameters will be calculated through the Matrix model, such as the code rate k/n , the overall memory of the convolutional code μ . In the real applications, the parameters of convolutional code are generally quite small, and the parameters typically are such that: $n \in [2, 8]$, $m_{\max} = 10$. The algorithm can be summarized as follow:

Inputs: the received sequence denoted by y ;

Outputs: the code rate k/n and the constraint length K ;

Step1: Take the values of $l = 12$

Step2: Set n from 2 to 8, and construct $R(M, ln)$

Step3: Set j from 1 to $M - 15n + 1$, construct N_j with j th to $(j + ln - 1)$ th rows of $R(M, ln)$, and take the diagonal after linear transformation.

Step4: Repeat **Step3**, and take the sum of all the diagonals, then have it normalize, denoted by P , a calculate A by local decision, which means that take n elements as a group and make a threshold decision by the mass.

Step5: If A is not in the form of (*), return to **Step2** and set n' to be another value; Otherwise, calculate the parameters and get the parity check matrix by the $P_{(n_a+n+k) \times (n-k)}^i$ ($i \geq 1$) with the least degree in **Step3**. Then the whole set of the encoder can be realized based on the Eq. 4

Experiment and performances analysis

In this section, the simulation of Monte Carlo was run. For evaluation of algorithm in various bit error rates (BER), data bits is generated with optimal convolutional codes. The convolutional codewords of size 5000 bits are produced with different code rate and 500 Monte Carlo experiments were executed for each simulation.

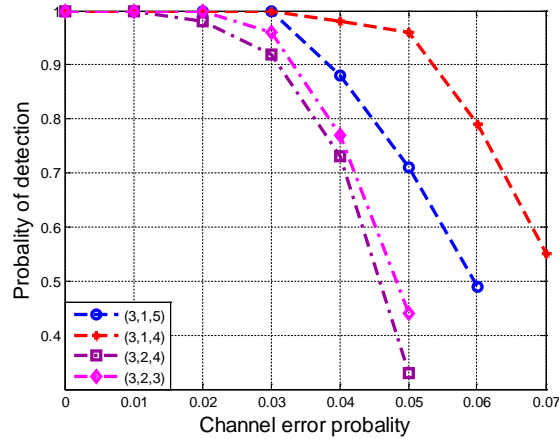


Fig 5 The performances of algorithm in various BER

The performances of the method presented to adapt error rate are illustrated in Fig 5, and it shows that the approach proposed has a good fault tolerance. We can see that the performances are better with the decrease of k and n , which is because that the bigger k or n needs the longer vector A to reflect the properties of the convolutional encoder.

Conclusion

This article dealt with the blind identification of rate k/n convolutional code in a noisy environment. The method is based on the properties of convolutional code and the effect of the corrupted bits on the data matrix of codewords. The performance was proved to be effective with a moderate complexity. Indeed, the probability to detect the true convolutional encoder will be higher with larger amount of received bit stream.

References

- [1] Reza Moosavi, Erik G. Larsson. A fast scheme for blind identification of channel codes [A]. Global Telecommunications Conference 2011 [C]. Linkoping, Sweden: IEEE Press, 1-5, (2011).
- [2] B Rice. Determining the parameters of a rate $1/n$ convolutional encoder over $GF(q)[A]$. In Proceedings of the 3rd International Conference on Finite Fields and Applications[C]. Glasgow, USA: IEEE Press, 1:4, (1995).
- [3] Wang Feng-hua, Huang Zhi-tao, and Zhou Yi-yu, "A method for blind recognition of convolution code based on Euclidean Algorithm," In IEEE International Conference On Wireless Communications, pp. 1414-1417, (2007).
- [4] Peizhong Lu, Yan Zou, "Fast Computations of Gröbner Bases and Blind Recognitions of Convolutional Codes," Lecture Notes in Computer Science, pp. 303-317, (2007).
- [5] Liu Jian, Wang Xiao-jun, Zhou Xi-yuan, "Blind Recognition of Convolutional Coding Based on Walsh-Hadamard Transform," Journal of Electronics & Information Technology, vol. 32, no. 4, pp. 884-888, (2010).
- [6] Melanie Marazin, Roland Gautier, Gilles Burel, "Blind recovery of k/n rate convolutional encoders in a noisy environment," Wireless Communications and Networking, pp. 1186-1687, (2011).
- [7] Yang Xiao-jing, Liu Jian-cheng, Zhang Yu, "Blind Recognition of (n, k, m) Convolutional Codes Based on Solving Check-Sequence," Journal of Astronautics, vol 34, no. 4, pp. 568-573,

(2013).

- [8] Zrelli, Yasamine, Gautier, Roland, Marazin, Melanie, “Focus on Theoretical Properties of Blind Convolutional Codes Identification Methods Based on Rank Criterion”, 9th International Conference on Communications (COMM), Bucharest, ROMANIA, pp. 353-356, (2012)
- [9] Jinn-Ja Chang, Der-June Hwang, Mao-Chao Lin, “Some extended results on the search for good convolutional codes” IEEE Transactions on information theory, Vol. 43, No. 5, (1997).