International Journal of Pure and Applied Mathematics
Volume 97 No. 1 2014, 21-30
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v97i1.3

DECODING OF 2-D CONVOLUTIONAL CODES BASED ON ALGEBRAIC APPROACH

Pramote Jangisarakul[1], Chalie Charoenlarpnopparut[2 §]
[1,2] School of Information
Computer and Communication Technology
Sirindhorn International Institute of Technology
Thammasat University
Klong Luang, Pathum-Thani 12121, THAILAND

Abstract: In this paper, we apply the decoding matrix for 2-D convolution codes to reconstruct information sequences. It is suitable for non-square matrices with multivariate polynomial elements. Next, development of a syndrome decoder for 2-D convolutional codes based on Gröbner bases is introduced. The computation of the syndrome vector employs the computation of the syzygy module, found by means of the Gröbner basis of a certain module. Then, estimated error vector can be identified by using m-variate division algorithm. Simulation results show error-correcting capability of decoding process.

AMS Subject Classification: 94B10, 94B35
Key Words: Groebner bases, convolutional codes, decoding matrix, syndrome decoder

1. Introduction

The representation of codes can be given in terms of either generator matrix or parity-check matrix. In our daily life, there are several applications of channel coding such as image storage in magnetic disks, data storage in silicon memory,

Received: May 11, 2014

§Correspondence author

and data transmission in optical media. These applications require reliable processes in order to correctly recover the original information. These significant processes include encoding, detecting and decoding. In particular, an efficient decoding process is not straightforward to develop, and in general, the decoding process is more difficult and more complex than the encoding process. Theory and application of m-D convolutional codes in last two decades can potentially solve those problems, especially the error-correcting code part. The overview of applications of m-D error-correcting codes given in [2] described potential practical implementations such as transmission of image and video signals over noisy channels.

In a noise-free channel, the decoded information can be retrieved from the convolutional encoded codewords without correcting errors by using a pseudo-inverse encoder, which follows from the non-square polynomial nature of the encoding matrix. One classical pseudo inverse is the Moore-Penrose generalized inverse. However, it is unlikely to assume that most communication channels are noise-free. Methods to find out a solution in the presence of noise are an active research area. In the last decade, research on m-D convolutional decoding with error-correcting capability has been reported in [7, 10], although the theories of m-D signals and systems continue to be a flourishing field. Literature on this field is vast; the attention of this research focuses on 2-D convolutional codes based on an algebraic approach. The path breaking results in this area can be found in Wiener [13], where several fundamental concepts and aspects of m-D convolutional code have been proposed systematically. During past decade, Rosenthal and his research group [11, 12] have developed several fundamental concepts on convolutional coding theory by deriving the relationship between convolutional codes and linear systems theory, using a behavior based approach. Another independent approach [5] is to investigate the problems of m-D convolutional code by using Gröbner basis/module theory. Several results are concerned with m-variate polynomial matrix factorization. An example of such applications was also reported in [6]. Fornasini and Valcher [8] considered 2-D convolutional codes over the Laurent polynomial ring, by using both the behavioral approach and a state-space procedure to construct encoders and decoders. Convolutional code aspects were reported as well.

In this paper, we apply an approach based on [4, 14] for computing the decoding matrix for 2-D cases. The purpose of using this approach is to reconstruct information sequences. An example is carried out to illustrate the approach. It is suitable for non-square matrices with multivariate polynomial elements. Next, the computation of the syndrome vector employs the computation of the syzygy module, found by means of the Gröbner basis of a cer-

tain module. Development of a syndrome decoder for 2-D convolutional codes based on Gröbner bases has some limitations of term orderings. By testing error-correcting capability, reverse lexicographical ordering is the best for this problem. However, using universal Gröbner bases or other term orderings may achieve good accuracy of decoding. The Singular [9] is chosen to implement several algebraic procedures.

2. Decoding Matrix

Let $\mathbb{F} = \mathbb{F}_q$ be the finite field with q elements and let $R = \mathbb{F}[D_1, D_2, \ldots, D_m]$ be the ring of m-variate polynomials whose coefficients belong to the field $\mathbb{F}$. An m-dimensional convolution code of length n over $\mathbb{F}$ is an R-submodule $\mathcal{C} \subseteq R^n$. An element $\mathbf{v} \in \mathcal{C}$ is called a *codeword*.

In 2-D case, there are two directions of delays (shift registers) named horizontal delay (D_1) and vertical delay (D_2) [5]. The realizations of 2-D convolutional encoders illustrate that the correlations between delay elements in generator matrix can be constructed with row and column locations in a circuit diagram. Next, we consider encoder primeness or matrix primeness, a property that is necessary to impose on the m-variate polynomial matrices generating a convolutional code. In the past, many properties of convolutional codes have been introduced based on these primeness, such as the papers [4, 5, 8] that introduced the right inverse of a polynomial matrix, syndrome decoder, and factorization matrices. These papers provided complete descriptions of primeness. Moreover, the paper by Youla and Gnavi [14] about primeness notions is fundamental. It is therefore necessary to discuss and summarize them as follows.

Definition 1. A full row rank convolutional encoder $G(D) \in R^{k\times n}$, $R \in \mathbb{F}_2[D_1, D_2]$ and $k < n$, is said to be:

1. *left zero prime(LZP) if all the $k \times k$ minors of G(D) generate the unit ideal in R;*

2. *left minor prime(LMP) if all the $k \times k$ minors of G(D) have no common divisors in R except for units;*

3. *left factor prime(LFP) if whenever G(D) is factored as $G(D) = T(D)G_1(D)$ with $T(D) \in R^{k\times k}$ and $G_1(D) \in R^{k\times n}$, then T(D) is necessarily a unimodular matrix i.e., det(T) is a unit.*

Generally, the relationship between the codeword sequence represented by vector $\mathbf{v}$ and the corresponding information sequence represented by vector $\mathbf{u}$ can be expressed as: $\mathbf{v} = \mathbf{u} \cdot G$, where G is an $k \times n$ generator matrix, whose elements are m-variate polynomials. If one can find a polynomial matrix Z as $\mathbf{v} \cdot Z = \mathbf{u} \cdot G \cdot Z = \mathbf{u}$, such that $G \cdot Z$ is equal to an identity matrix, then one can directly retrieve the original information sequence under the noise-free environment. The matrix Z is called a right inverse of matrix G or *decoding matrix*. A suitable method for computing Z based on the algebraic approach and Gröbner bases is investigated. By using the constructive proof of Theorem 2 by Youla and Gnavi in [14], the algorithm for finding a right inverse of an m-variate polynomial matrix has been derived by Charoenlarpnopparut [4], and an appropriate example has been provided.

Catastrophic encoders for codes over the m-D polynomial ring

$$R = \mathbb{F}[D_1, D_2, \ldots, D_m]$$

have been studied by Weiner [13]. To test a catastrophic encoder, one needs to evaluate the gcd of the full-size minors of generator matrix. In the 1-D and 2-D cases, a convolutional encoder is noncatastrophic if and only if the gcd of the full-size minors of encoder is in the form D^l, for $l \geq 0$.

Proposition 1. *Let an $k \times n$ polynomial matrix, G whose elements are m-variate polynomials in the ring $\mathbb{F}[D_1, D_2, \ldots, D_m]$ has a right inverse if and only if G is LZP.*

Proof. If G is LZP, all the $k \times k$ minors of G generate the unit ideal in R. We can get

$$\sum_{(j)} d_j(D_1, D_2, \ldots, D_m)\delta_j(D_1, D_2, \ldots, D_m) = 1,$$

where $\delta_j, j = 1, 2, \ldots, \binom{n}{k}$, are all $k \times k$ minors of G. The formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is called a binomial coefficient. Consider the identity $\delta_j I_k = G\frac{1}{k_j}\frac{\partial^n(\Lambda K \mathrm{Adj}(G\Lambda K))}{\partial\lambda_{j_1}\partial\lambda_{j_2},\cdots,\partial\lambda_{j_n}}$, where Λ denotes the diagonal matrix with elements $\{\lambda_1, \lambda_2, \ldots, \lambda_k\}$. A matrix K is any $n \times k$ real constant matrix whose $k \times k$ minors are denoted by $k_j, j = 1, 2, \ldots, \binom{n}{k}$. Note that such a K always exists. Therefore, we can get

$$\begin{aligned} I_k &= \sum_{(j)} d_j(D_1, D_2, \ldots, D_m)\delta_j(D_1, D_2, \ldots, D_m)I_k \\ &= G\sum_{(j)} d_j(D_1, D_2, \ldots, D_m)\frac{1}{k_j}\frac{\partial^n(\Lambda K \mathrm{Adj}(G\Lambda K))}{\partial\lambda_{j_1}\partial\lambda_{j_2}, \cdots, \partial\lambda_{j_n}}. \end{aligned}$$

Then, we imply that a matrix Z is a right inverse of G as follows:

$$Z = \sum_{(j)} d_j(D_1, D_2, \ldots, D_m) \frac{1}{k_j} \frac{\partial^n(\Lambda K \mathrm{Adj}(G\Lambda K))}{\partial\lambda_{j_1}\partial\lambda_{j_2}, \cdots, \partial\lambda_{j_n}}. \qquad \square$$

Example 2. Consider the 2-D generator matrix $G^{(1)}$:

$$G^{(1)} = \begin{bmatrix} 1 + D_1D_2 & D_1 & D_2^2 \\ D_2 & 1 & D_1^2D_2^2 \end{bmatrix}.$$

By referring to Definition 1, $G^{(1)}$ is both LZP and LMP. Also $G^{(1)}$ is noncatastrophic, since the gcd of the full-size minors of $G^{(1)}$ is 1. As a result, one can obtain Z such that $G^{(1)}Z = I_2$, for instance:

$$Z = \begin{bmatrix} 1 & D_1 \\ D_2 & D_1D_2 + 1 \\ 0 & 0 \end{bmatrix}.$$

3. Syndrome Decoder

Due to various kinds of interference in transmission channel, the transmitted codeword is subject to errors and hence it can be written as: $\tilde{\mathbf{v}} = \mathbf{v} + \mathbf{e}$, where $\tilde{\mathbf{v}}$ is called *received codeword*, and $\mathbf{e}$ is called *error vector*. Later, the received codeword goes into the parity-check matrix H for syndrome computation: $\mathbf{s} = \tilde{\mathbf{v}} \cdot H^T$, where $\mathbf{s}$ is called *syndrome vector*. If the syndrome vector is nonzero, the presence of error vector is detected. Zero syndrome implies that $\tilde{\mathbf{v}}$ is a correct codeword and therefore the error vector is assumed to be null, i.e. no error correction. The relationship between the syndrome vector and the error vector can be derived as:

$$\mathbf{s} = (\mathbf{v} + \mathbf{e}) \cdot H^T = \mathbf{e} \cdot H^T.$$

The error-correcting process can be performed by first estimating the error vector for solving $\mathbf{e}$ in above syndrome equation, which has an infinite number of solutions. The *estimated error vector* $\hat{\mathbf{e}}$, that corresponds to the computed syndrome, is, then subtracted from the received vector for correction purposes. In the binary field, addition and subtraction are interchangeable. The decoding process can be performed by the equations: $\hat{\mathbf{v}} = \tilde{\mathbf{v}} + \hat{\mathbf{e}}$ and $\hat{\mathbf{u}} = \hat{\mathbf{v}} \cdot Z$, where $\hat{\mathbf{v}}$ is called *estimated codeword*, $\hat{\mathbf{u}}$ is called *estimated information sequence*, and Z

is the decoding matrix, computed as a pseudo inverse of the generator matrix G by using Proposition 1. If $\hat{\mathbf{e}}$ is determined correctly, i.e. $\hat{\mathbf{e}} = \mathbf{e}$ the decoded information contains no errors, i.e. $\hat{\mathbf{u}} = \mathbf{u}$. A technique is to directly calculate $\hat{\mathbf{e}}$ from the syndrome equation and use it for the error-correcting process to recover the original information. The m-D generalized version of this scheme is proposed in this section, based on the Gröbner bases and the theory of syzygy. The evaluation of $\hat{\mathbf{e}}$ is the main objective of a syndrome decoder.

Gröbner bases are powerful tools to deal with polynomial ideals. The computation of a Gröbner basis is generally done by employing the Buchberger algorithm [1, 3]. The extension of Gröbner bases to the module case can be found in [1]. The syzygy is a module whose members are annihilators of the ideal generator, analogous to the null space of a given matrix. The computation of the syzygy module is generally done by first computing the Gröbner basis.

Definition 3. Let $\mathbf{g}_1,\ \mathbf{g}_2, \ldots,\ \mathbf{g}_k$ be m-variate polynomial row vectors in R^n. A syzygy of the $k \times n$ generator matrix

$$G = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_k \end{bmatrix},$$

is a vector $\mathbf{h} = [h_1, h_2, \ldots, h_k]$ such that $\sum_{i=1}^{k} h_i \mathbf{g}_i = \mathbf{0}$. The set of all such syzygies is called the syzygy module of G and is denoted by $\mathrm{Syz}(\mathbf{g}_1,\ \mathbf{g}_2, \ldots,\ \mathbf{g}_k)$ or $\mathrm{Syz}(G)$.

Definition 4. The bit error probability (P_e) is the probability that an information bit of codeword is erroneously transmitted to the destination.

Definition 5. The correctable percentage of a code is defined as the ratio of the number of detected and corrected codewords ($\hat{\mathbf{v}} = \mathbf{v}$) and the number of received codewords $\tilde{\mathbf{v}}$.

Proposition 2. *If sygyzy module of the parity-check matrix H can be expressed as $Syz(H) = \langle \mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_t \rangle$, where the subscript t denotes a number of syzygies and a polynomial vector $\mathbf{q}$ is a solution of $\mathbf{s} = \mathbf{q} \cdot H^T$, then the estimated error vector can be defined as $\mathbf{q} \xrightarrow[+]{\{\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_t\}} \hat{\mathbf{e}}$.*

Proof. By using the m-variate division algorithm [1], the syndrome vector $\mathbf{s} = \tilde{\mathbf{v}} \cdot H^T$ is reduced to the remainder vector $\mathbf{r}$ modulo H that can be calculated by using $\mathbf{s} \xrightarrow[+]{H} \mathbf{r}$. The computation returns quotients represented by a polynomial vector $\mathbf{q}$ and a remainder $\mathbf{r} = \mathbf{0}$, i.e. $\mathbf{s} = \mathbf{q} \cdot H^T$ since $\mathbf{r}$

is a member of the module generated by H. The $\mathbf{q}$ is a particular solution of the estimated error vector. We find $Syz(H) = \langle \mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_t \rangle$, and then then expression of all possible estimated error vectors can be written as [4]: $\hat{\mathbf{e}} = \mathbf{q} + \alpha_1\mathbf{p}_1 + \alpha_2\mathbf{p}_2 + \cdots + \alpha_t\mathbf{p}_t$, where $\alpha_1, \alpha_2, \ldots, \alpha_t$ are polynomials in $\mathbb{F}[D_1, D_2]$. Also we can express $\mathbf{q} = \alpha_1\mathbf{p}_1 + \alpha_2\mathbf{p}_2 + \cdots + \alpha_t\mathbf{p}_t + \hat{\mathbf{e}}$. Completely reduce the vector $\mathbf{q}$ to $\hat{\mathbf{e}}$ with respect to the module generated by polynomial vectors $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_t$. The computation returns quotients $\alpha_1, \alpha_2, \ldots, \alpha_t$ and the remainder vector $\hat{\mathbf{e}}$ i.e.

$$\mathbf{q} \xrightarrow{\{\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_t\}}_{+} \hat{\mathbf{e}}.$$

□

Example 6. This example is to simulate error-correcting performance of the decoding process based on Proposition 2 for three different polynomial generator matrices $G^{(1)}, G^{(2)}, G^{(3)}$[10]. These matrices are shown as following:

$$G^{(1)} = \begin{bmatrix} 1 + D_1D_2 & D_1 & D_2^2 \\ D_2 & 1 & D_1^2D_2^2 \end{bmatrix},$$

$$G^{(2)} = \begin{bmatrix} 1 + D_1^2 & 0 & D_1 \\ 1 + D_2 & 1 + D_1 + D_2^2 & 0 \end{bmatrix},$$

$$G^{(3)} = \begin{bmatrix} D_1^2D_2 & 0 & D_2 & D_1^2 & 1 & 0 \\ 0 & 1 + D_1^2D_2 & 0 & D_1D_2 & D_1 & 1 + D_1^2 + D_2 \end{bmatrix}.$$

It is assumed that the binary information sequences have 10,000 random symbols, each of them consists of 8 binary bits, and that the transmission channel has a bit error probability P_e, as defined in Definition 4. We assume all bits of transmitted codeword have the same probability, and have $P_e \leq 1$. The generated binary information sequences are transformed into polynomial vectors. The performance of this decoding process can be measured in term of correctable percentage, given in Definition 5.

Table 1 illustrates the correctable percentage of errors in decoding the convolutional codes corresponding to various term orderings. For this decoding problem, the degree reverse lexicographical ordering is the most efficient ordering. However, for every particular problem, one of the term orderings can be the most effective.

Example 7. The original image for testing has 512×512 pixels and each pixel has 8 bits as shown in Fig. 1(a). Using encoder $G^{(1)}$ given in Example 6, $G^{(1)}$ provides the ratio 8/48 for binary input and binary output bits. We assume all bits of transmitted codeword have the same P_e. In Fig. 1(b), many

Table 1: Correctable percentage of errors based on Proposition 2 for $G^{(1)}$, $G^{(2)}$ and $G^{(3)}$ with different term orderings.

Term ordering	$G^{(1)}$	$G^{(2)}$	$G^{(3)}$
Lexicographical ordering	62	50	79
Degree reverse lexicographical ordering	62	68	79
Degree lexicographical ordering	56	63	78

random erroneous bits ($P_e = 0.02$) are imposed on the image, and consequently erroneous pixels have colours different from the original colours. A gray scale colour is used for implementation. Once applied to the encoded image, the decoding procedure is required to retrieve the original image. Consequently, using both the syndrome decoder with lexicographical ordering (this section) and the decoding matrix (previous section), almost all these random erroneous bits on the image are corrected as shown in Fig. 1(c). The peak signal-to-noise ratio (PSNR) is used to evaluate the image quality, and is here defined as $\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}}$. The mean square error (MSE) can be denoted as $\text{MSE} = \frac{\sum_{M,N}[I_{ij}-\overline{I}_{ij}]^2}{M \cdot N}$, where M and N are the number of rows and columns in the images, and I_{ij} and $\overline{I}_{ij}$ are original image and noisy/reconstructed image respectively. The higher the PSNR, the better the quality of the reconstructed image.

Acknowledgment

The authors thank the National Research University(NRU) Project, Commissioner of Higher Education, Thailand for the financial support of this research project.

References

[1] W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, **3** (1994).

[2] S. Basu, M.N.S. Swamy, Editorial Preface to Special Issue on Multidimensional Signals and Systems, *IEEE Trans. Circuits Syst. I, Fun-*

(a) Original image

(b) Noisy image (PSNR=+38.28 dB)

(c) Reconstructed image (PSNR=+45.55 dB)

Figure 1: Decoding image with noise

damental Theory and Applications, **49**, No.6 (2002), 709-714. doi: 10.1109/TCSI.2002.1010026.

[3] B. Buchberger, Gröbner Bases and Systems Theory, *Multidimensional Systems and Signal Processing*, **12** (2001), 223-251. doi: 10.1023/A:1011949421611.

[4] C. Charoenlarpnopparut, *Gröbner Bases in Multidimensional Systems and Signal Processing*, PhD Thesis, Pennsylvania State University, (2000).

[5] C. Charoenlarpnopparut, Applications of Gröbner Bases on the Structural Description and Realization of Multidimensional Convolutional

Code, *Science Asia*, **35** (2009), 95-105. doi: 10.2306/scienceasia1513-1874.2009.35.095.

[6] C. Charoenlarpnopparut, N. K. Bose, Multidimensional FIR filter bank design using Gröbner bases, *IEEE Trans. Circuits Syst. II, Analog Digital Signal Processing*, **46**, No.12 (1999), 1475-1486. doi: 10.1109/82.809533.

[7] A. Dholakia, M. A. Vouk, D. L. Bitzer, Table based decoding of rate one-half convolutional codes, *IEEE Trans. Communications*, **43**, No.2-4 (1995), 681-686. doi: 10.1109/26.380090.

[8] E. Fornasini, M. E. Valcher, Algebraic aspects of two-dimensional convolutional codes, *IEEE Trans. Inform. Theory*, **IT-40**, No.4 (1994), 1068-1082. doi: 10.1109/18.335967.

[9] G.-M. Greuel, G. Pfister, H. Schonemann, SINGULAR 3.0., *Computer Algebra System for Polynomial Computations*, Centre for Computer Algebra, University of Kaiserlautern (2005), http://www.singular.uni-kl.de.

[10] R. Lobo, *On Locally Invertible Encoders and Multidimensional Convolutional Codes*, PhD Thesis, North Carolina State University, (2006).

[11] J. Rosenthal, J. M. Schumacher, E. V. York, On behaviors and convolutional codes, *IEEE Trans. Inform. Theory*, **IT-42**, No.6 (1996), 1881-1891. doi: 10.1109/18.556682.

[12] R. Smarandache, H. G. Luerssen, J. Rosenthal, Constructions of MDS-Convolutional Codes, *IEEE Trans. Inform. Theory*, **IT-47**, No.5 (2001), 2045-2049. doi: 10.1109/18.930938.

[13] P. Wiener, *Multidimensional Convolutional Codes*, PhD Thesis, University of Notre Dame, (1998).

[14] D. C. Youla, G. Gnavi, Notes on n-dimensional system theory, *IEEE Trans. Circuits Systems*, **26** (1979), 105-111. doi: 10.1109/TCS.1979.1084614.