2013

Blind LDPC encoder identification

Tian Xia
Louisiana State University and Agricultural and Mechanical College

BLIND LDPC ENCODER IDENTIFICATION

A Thesis

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering

in

The School of Electrical Engineering and Computer Sciences

by
Tian Xia
B.S., University of Electronic Science and Technology of China, 2008
M.S., University of Electronic Science and Technology of China, 2011
December 2013

ACKNOWLEDGEMENTS

First, I would like to express my sincere gratitude to my thesis advisor Dr. Hsiao-Chun Wu. This work cannot be fulfilled without his kind and precious guidance. His profound knowledge and deep insight offer me the timely instructions and indicate the promising directions. Every meeting with Dr. Wu is an enlightening inspiration to me, which elevates me to a yet-higher altitude I would never dream of. His persistent research-interest-driving spirit encourages me to overcome most difficult challenges, one after another. I am very certain that the training and knowledge I gained here in this couple of years will definitely impose a long, positive impact on my future career.

Also, I would like to thank my committee members Dr. Xuebin Liang and Dr. Morteza Naraghi-Pour, who constantly dedicated their invaluable time and provided excellent comments for this work. Beyond the thesis study, I also learned a lot from their outstanding courses, which established indispensable foundations of this work.

Moreover, I am very grateful to my former/current labmates Dr. Yonas G. Debessu and Ms. Hongting Zhang. They not only shared their experience and knowledge but also offered friendship during my study here at Louisiana State University. They made my education here a wonderful and memorable stage in my life.

At last but not least, I would like to express my high gratitude to my parents. No matter what decision I have made or what situation I have to face, they always firmly stand by my side and give me unwavering support. I cannot be any luckier to be raised in such a family full of love and hope. This thesis work is dedicated to my parents.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Nowadays, adaptive modulation and coding (AMC) techniques can facilitate flexible strategies subject to dynamic channel quality. The AMC transceivers select the most suitable coding and modulation mechanisms subject to the acquired channel information. Meanwhile, a control channel or a preamble is usually required to synchronously coordinate such changes between transmitters and receivers. On the other hand, low-density parity-check (LDPC) codes become more and more popular in recent years due to their promising capacity-approaching property. The broad range of variations in code rates and codeword lengths for LDPC codes makes them ideal candidates for future AMC transceivers.

The *blind encoder identification* problem emerges when the underlying control channel is absent or the preamble is not allowed in AMC systems. It would be quite intriguing for one to build a blind encoder identification technique without spectrum-efficiency sacrifice. Therefore, in this thesis, we investigate blind LDPC encoder identification for AMC systems.

Specifically, we would like to tackle the blind identification of binary LDPC codes (encoders) for binary phase-shift keying (BPSK) signals and nonbinary LDPC codes for quadrature-amplitude modulation (QAM) signals. We propose a novel blind identification system which consists of three major components, namely *expectation-maximization (EM) estimator* for unknown parameters (signal amplitude, noise variance, and phase offset), *log-likelihood ratio (LLR) estimator* for syndrome *a posteriori* probabilities, and *maximum average-LLR detector*. Monte Carlo simulation results demonstrate that our proposed blind LDPC encoder identification scheme is very promising over different signal-to-noise ratio conditions.

1. INTRODUCTION

In this chapter, we will facilitate the motivation of adaptive modulation and coding (AMC) technologies. Then some blind signal processing methods are stated for AMC transceivers. Finally, the outline of this thesis work will be presented at the end.

1.1 Background and Motivation

Adaptive modulation and coding (AMC) techniques can adjust the quality-of-service (QoS) for communication sessions transmitted through time-varying channels so as to seek the tradeoff between data-rate (throughput) and bit-error-rate performances. Based on the feedback channel state information (CSI), the AMC transmitter dynamically selects an appropriate combination of modulator and channel encoder from the predefined candidate pool [1–6]. In the conventional AMC techniques, a *control channel* is often necessary to be facilitated to coordinate the changes in modulation/demodulation and coding/decoding mechanisms at both transmitter and receiver. Although this "*control channel*" strategy makes the receiver easy to synchronize with the transmitter's changes, either additional spectral resource or spectral efficiency reduction is definitely required thereupon.

An immediate question arises: do AMC techniques still work if none of the training sequences, the aforementioned control channel, and the preamble is available, i.e., in a *blind* way? This thesis is dedicated to exploiting the potential answer to this interesting and important question. People have been studying this question for a while. In fact, *blind signal processing* techniques would be very useful in this scenario, which have been widely adopted

in modern communication applications. One example is *blind equalization* for cognitive radio receivers [7]. Besides, receivers can rely on *blind classification* techniques to determine the modulation types of the transmitted signals directly from the received signal data [8, 9].

Moveover, *blind identification* of channel encoders was investigated recently by [10–16]. In [10], the frame synchronization was determined by using the log-likelihood ratio (LLR) of the syndrome of error correcting codes. In [11], the blind identification of nonbinary convolutional encoder parameters was investigated for noise-free channels. In [12], three maximum-likelihood (ML)-based classifiers were proposed to distinguish *space-time block codes* (STBCs). In [13], the mathematical structures inferred by the parity-check relations over the *Galois field* $\mathbb{GF}(2)$ were explored for blindly identifying the channel encoder from the predefined candidate set. In [14], a fast algorithm was proposed to detect an *additional lonely bit* (ALB) by identifying two different linear codes. Lately, our group proposed a novel sophisticated algorithm to blindly estimate the parameters for arbitrary turbo codes [15,16].

Since no *a priori* knowledge about the transmitted data is given at the receiver, the receiver has to utilize the redundancy introduced by the channel encoder of the transmitter to identify which kind of encoder the transmitter actually employs. The statistical characteristics, say the *log-likelihood ratios* (LLRs) of the received signals, are usually invoked to extract the essential information in the existing blind channel-encoder identification approaches [12–14]. In addition, for *space-time block codes* (STBCs), which can be considered as a special kind of channel codes, the *space-time redundancy* of the received signal samples is exploited to distinguish coding schemes [12]. For most channel coding schemes involving parity-check symbols, the mathematical structures inferred by the parity-check symbols over the *Galois fields* are explored for identifying the original encoder at the receiver [13].

Obviously, different encoders (codes) may need different blind identification mechanisms. In this thesis, we would like to focus on blind identification of *low-density parity-check* (LDPC) codes. First introduced by pioneer Gallager (see [17]) and then revived after more than thirty years of hibernation (see [18]), LDPC codes have become one of the most favorable codes in both academia and industry [19]. It has been demonstrated that LDPC codes can outperform prevalent turbo codes when codeword block lengths get sufficiently large [20]. On the other hand, unlike binary LDPC codes where the codewords need to be sufficiently long so as to approach Shannon-capacity [21], nonbinary LDPC codes are also devised, which can exhibit promising waterfall and error-floor performances even when the codewords are of short or moderate lengths [22, 23]. The wide range of code rates and codeword lengths also makes LDPC codes ideal choices for AMC systems. Due to these merits, LDPC codes are already adopted in many existing telecommunication standards and remain the top candidates for the future generations of wireless systems. For example, the IEEE 802.11n standard has specified the LDPC codes as a forward error-correction (FEC) option for high-performance, high-throughput networks [24].

1.2 Thesis Outline

The rest of this thesis is organized as follows. In Chapter 2, the basic transceiver system diagram and the signal model involving binary LDPC encoders and binary phase-shift keying (BPSK) modulation are presented and the blind encoder identification problem is formulated. Then, the log-likelihood ratio (LLR) is defined to establish our proposed blind encoder identification scheme. How to blindly estimate the received signal amplitude and the noise variance is also manifested in detail. Specifically, two statistical signal processing

methods, namely the *second-order/fourth-order moment* method (M_2/M_4) (see [25]) and the *expectation-maximization* (EM) algorithm (see [26]) are utilized in our thesis work. The corresponding Cramer-Rao lower bounds (CRLBs) are derived thereupon.

In Chapter 3, we extend our work in Chapter 2 to blindly identify *nonbinary* LDPC codes over the Galois fields $\mathbb{GF}(q)$. There are several important modifications from the binary LDPC codes. First, the signals contain *q-ary quadrature-amplitude modulation* (*q*-QAM) symbols. Consequently, there exists an unknown phase offset in the signal model thereby. Thus, the EM algorithm needs to be developed accordingly to estimate signal amplitude, noise variance, and phase offset altogether. Due to the nonbinary coefficients in the parity-check matrix, the LLRs of syndrome *a posteriori* probabilities (APPs) have to be computed in a recursive manner, which is totally different from the binary counterparts.

In Chapter 4, Monte Carlo simulation results are demonstrated to evaluate the effectiveness of our proposed blind encoder identification schemes for both binary and nonbinary LDPC codes. For binary LDPC codes, the normalized mean-square-error (NMSE) performances for M_2/M_4 and EM algorithms are compared with the corresponding CRLBs. The identification performances are examined for both binary and nonbinary LDPC encoders with various code rates and codeword lengths.

Finally, conclusion will be drawn in Chapter 5. The partial results of this thesis work have been reported in [27–29].

2. BINARY LDPC ENCODER IDENTIFICATION

In this chapter, we will discuss how to blindly identify binary LDPC encoders given a predefined candidate set. The basic communication transceiver system diagram and the signal model will also be introduced.

2.1 Basic Transceiver Model

In this section, we will introduce the basic system model for the transceivers involving binary low-density parity-check (LDPC) coders/decoders. The block diagram of the transceiver involving our proposed new blind binary LDPC encoder identification mechanism is depicted in Figure 2.1. Without loss of generality, let's not consider source encoder/decoder here. Denote the sets $\mathcal{Z}_2 \stackrel{\text{def}}{=} \{0,1\}$ and $\mathcal{B} \stackrel{\text{def}}{=} \{-1,1\}$. At the transmitter, original information bits are grouped into blocks, each of which consists k consecutive bits, say $\mathbf{b}_\nu \in \mathcal{Z}_2^{k\times 1}$, where $\nu \in \mathcal{Z}$ is the *block index*. This block of information bits are passed to the "LDPC encoder θ" to generate a corresponding block of "*codeword*" or "*coded bits*", say $\mathbf{c}_\nu^\theta \in \mathcal{Z}_2^{n\times 1}$, where θ denotes a particular type of LDPC encoder. Obviously the corresponding code rate is $R = k/n$. Then, the codeword $\mathbf{c}_\nu^\theta$ should be modulated by binary phase-shift keying (BPSK) modulator and the corresponding block of modulated symbols are denoted by $\mathbf{s}_\nu^\theta \in \mathcal{B}^{n\times 1}$. These modulated BPSK symbols will undergo a "frequency up-converter" to engender the *pass-band signals* for actual transmission.

The transmitted pass-band signals travel through the channel and arrive at the receiver. They will go through the "frequency down-converter" first to come back to the baseband. In

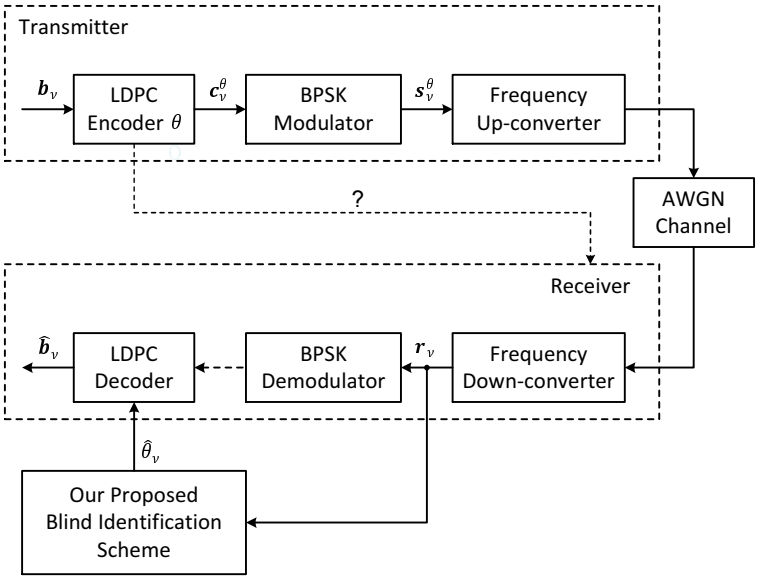

Figure 2.1: The system diagram of a basic transceiver model involving binary LDPC codes.

this thesis, we assume that both frequency and frame synchronizations are properly carried out prior to encoder identification. It is possible that joint frequency synchronization, frame synchronization, and encoder identification can be accomplished blindly using the techniques in [10, 30] as well as the proposed encoder identification scheme in this thesis. Nevertheless, we focus on the new blind encoder identification scheme throughout this thesis.

According to Figure 2.1, the received baseband signal symbols are also collected in blocks, say $\mathbf{r}_\nu \in \mathcal{R}^{n\times 1}$, $\nu \in \mathcal{Z}$. Instead of passing $\mathbf{r}_\nu$ to the "BPSK demodulator" as in the standard receivers, we propose to feed $\mathbf{r}_\nu$ to our new "*blind identification scheme*" to identify θ, the unknown LDPC encoder adopted in the transmitter. Once the encoder type is identified by our proposed scheme as $\hat{\theta}_\nu$ where the subscript ν means that it is estimated from the ν^{th} block of received signal samples, then the appropriate LDPC decoder can be employed to construct the information symbol estimates $\hat{\mathbf{b}}_\nu$.

Consider the additive white Gaussian noise (AWGN) channel here. Each element of the ν^{th} block of received baseband signal samples, $\mathbf{r}_\nu \stackrel{\text{def}}{=} [r_{\nu,0}, r_{\nu,1}, \ldots, r_{\nu,j}, \ldots, r_{\nu,n-1}]^T$, can be

expressed as

$$r_{\nu,j} = a_\nu \, s^{\theta}_{\nu,j} + w_{\nu,j}, \quad j = 0, 1, \ldots, n-1, \tag{2.1}$$

where a_ν is the unknown signal amplitude accounting for the processing gain and the channel gain, $s^{\theta}_{\nu,j} \in \mathcal{B}$ is the modulated BPSK signal generated from the encoder θ, and $w_{\nu,j}$ is the zero-mean AWGN with the variance $\mathbb{E}\{w^2_{\nu,j}\} \stackrel{\text{def}}{=} \sigma^2_\nu$ for the j^{th} signal sample within the ν^{th} block. Consequently, the *signal-to-noise ratio* (SNR) per coded bit for the ν^{th} block of modulated signals is given by

$$\rho_\nu = \frac{a^2_\nu}{\sigma^2_\nu}. \tag{2.2}$$

On the other hand, to take the code rate R into account, the SNR per uncoded bit for the ν^{th} block of modulated signals is given by

$$\eta_\nu = \frac{\rho_\nu}{R} = \frac{a^2_\nu}{R\,\sigma^2_\nu}. \tag{2.3}$$

According to Figure 2.1, the receiver has no idea about the exact encoder θ the transmitter adopts. Therefore, it needs to identify the encoder before any received signal can be decoded. Often, an LDPC encoder would have a very large parity-check matrix, and it is impossible for any receiver to blindly reproduce the exact parity-check matrix without any *a priori* knowledge. In practice, the AMC transceivers would not change their modulators and encoders arbitrarily. Therefore, one may restrict the modulation/encoder options within a given set. In this thesis, we assume that a pre-determined LDPC encoder candidate set, say Θ, which contains multiple encoder candidates, is known to both transmitter and receiver, and obviously $\theta \in \Theta$. We also assume that the encoders in Θ are different from each other so that the parity-check matrices of any two encoders do not have identical row(s). It is the

usual constraint for AMC schemes. Thus, we can pick up its estimate $\hat{\theta}_\nu$ from this given set Θ as well. We will present a new method to blindly identify the LDPC encoder adopted in the transmitter in the subsequent sections.

2.2 Binary LDPC Encoder Identification

Since each LDPC code has a unique parity-check matrix, the encoder θ can be unambiguously identified if we can successfully establish the corresponding underlying *parity-check relations* directly from the received signal data samples. The parity-check relations are manifested by that the sums of certain coded bits in the codeword block over the Galois field $\mathbb{GF}(2)$ are zero. To achieve this, we first formulate the log-likelihood ratio (LLR) of the syndrome *a posteriori* probability (APP) in this section. The similar LLR metric was used for the iterative convolutional decoder in [31]. Henceforth, we propose a novel blind LDPC encoder identification scheme, which is based on this feature, the average LLR of the LDPC syndrome APP. The details are established in the following subsections.

2.2.1 Log-likelihood Ratio

Since we need to rely on the LLR metric for the blind LDPC encoder identification in this thesis, a preliminary introduction on the log-likelihood ratio formulation for a binary random process is provided here. The log-likelihood ratio of a binary random variable X can be facilitated as

$$\mathcal{L}_X(x) \stackrel{\text{def}}{=} \ln \frac{P_r\{x=0\}}{P_r\{x=1\}}, \tag{2.4}$$

which is the natural logarithm of the ratio between the probabilities of X taking values 0 and 1, respectively. Given another random variable, say Y, then the LLR of X conditioned on Y is given by

$$\mathcal{L}_{X|Y}(x|y) \stackrel{\text{def}}{=} \ln \frac{P_r\{x=0\,|\,y\}}{P_r\{x=1\,|\,y\}}. \tag{2.5}$$

According to the Bayes's Theorem, we get

$$\begin{aligned} \mathcal{L}_{X|Y}(x|y) &= \ln \frac{P_r\{y\,|\,x=0\}}{P_r\{y\,|\,x=1\}} + \ln \frac{P_r\{x=0\}}{P_r\{x=1\}} \\ &= \mathcal{L}_{Y|X}(y\,|\,x) + \mathcal{L}_X(x). \end{aligned} \tag{2.6}$$

Without any ambiguity, we hereafter simplify the notations of $\mathcal{L}_X(x)$, $\mathcal{L}_{X|Y}(x|y)$, and $\mathcal{L}_{Y|X}(y|x)$ as $\mathcal{L}(x)$, $\mathcal{L}(x|y)$, and $\mathcal{L}(y|x)$, respectively. Let $\oplus$ denote the addition over Galois field $\mathbb{GF}(2)$ (or exclusive-OR operation). A *box-plus* operation, denoted by $\boxplus$, can be formulated according to [31] as follows:

$$\begin{aligned} \mathcal{L}(x_1 \oplus x_2 \oplus \cdots \oplus x_n) &\stackrel{\text{def}}{=} \boxplus_{j=1}^{n} \mathcal{L}(x_j) \\ &\stackrel{\text{def}}{=} \mathcal{L}(x_1) \boxplus \mathcal{L}(x_2) \boxplus \cdots \boxplus \mathcal{L}(x_n) \\ &= 2\tanh^{-1}\left(\prod_{j=1}^{n} \tanh\Big(\mathcal{L}(x_j)/2\Big)\right). \end{aligned} \tag{2.7}$$

2.2.2 Proposed Blind Encoder Identification Scheme

Given an encoder $\theta' \in \Theta$, one can determine its parity-check matrix $\mathbf{H}_{\theta'} \in \mathcal{Z}_2^{m\times n}$ ($m \geq n-k$), and obtain

$$\mathbf{H}_{\theta'}\,\mathbf{c}_\nu^{\theta} = \mathbf{0}, \text{ if and only if } \theta' = \theta, \tag{2.8}$$

where $\mathbf{c}_\nu^{\theta}$ is the coded sequence from encoder θ with length n, and $\mathbf{0}$ is the $m \times 1$ zero vector. The "only if" implication in Eq. (2.8) holds because the encoders in the candidate set Θ are

assumed to be different from each other as stated in the end of Section 2.1. That is, the candidate LDPC encoder θ' is exactly the encoder θ adopted at the transmitter within the ν^{th} block. Eq. (2.8) describes the so-called *parity-check relations*.

Denote the locations of the non-zero elements at the i^{th} row of the parity check matrix $\mathbf{H}_{\theta'}$ by a vector $\mathbf{l}_i^{\theta'} = [l_{i_1}, l_{i_2}, \ldots, l_{i_{N_i}}]^T$ $(0 \leq l_{i_1} < l_{i_2} < \cdots < l_{i_{N_i}} \leq n-1)$, where N_i is the total number of the non-zero elements in the i^{th} row of $\mathbf{H}_{\theta'}$. Note that the location of the first element in any row of $\mathbf{H}_{\theta'}$ is indexed as "0" instead of "1". Denote $\mathbf{c}_\nu^\theta \stackrel{\text{def}}{=} [c_{\nu,0}, c_{\nu,1}, \ldots, c_{\nu,n-1}]^T$. Thus, we can rewrite Eq. (2.8) as

$$c_{\nu,l_{i_1}} \oplus c_{\nu,l_{i_2}} \oplus \cdots \oplus c_{\nu,l_{i_{N_i}}} = 0, \quad \forall\ 1 \leq i \leq m, \tag{2.9}$$

if and only if $\theta' = \theta$ (the estimated encoder at the receiver is exactly the encoder adopted at the transmitter).

According to Eq. (2.6), we can have

$$\begin{aligned} \mathcal{L}(c_{\nu,j}|r_{\nu,j}) &= \mathcal{L}(r_{\nu,j}|c_{\nu,j}) + \mathcal{L}(c_{\nu,j}) \\ &= \mathcal{L}(r_{\nu,j}|c_{\nu,j}), \quad 0 \leq j \leq n-1, \end{aligned} \tag{2.10}$$

where $\mathcal{L}(c_{\nu,j}) = 0$ because each bit in any LDPC codeword is assumed to have equal probabilities of taking values 0 or 1. Consider $\mathcal{L}(c_{\nu,j}|r_{\nu,j})$ to be the messages which are assumed to be conditionally independent of each other [19]. If an encoder candidate θ' is picked at the receiver, according to Eqs. (2.7)–(2.10), we obtain the LLR of the syndrome *a posteriori* probability (APP) for the i^{th} parity-check bit $(i = 1, 2, \ldots, m)$ in the ν^{th} block as follows:

$$\begin{aligned} \gamma_{\nu,i}^{\theta'} &\stackrel{\text{def}}{=} \mathcal{L}\big(c_{\nu,l_{i_1}} \oplus c_{\nu,l_{i_2}} \oplus \cdots \oplus c_{\nu,l_{i_{N_i}}} | r_{\nu,l_{i_1}} r_{\nu,l_{i_2}} \ldots r_{\nu,l_{i_{N_i}}}\big) \\ &\stackrel{\text{def}}{=} \boxplus_{j=1}^{N_i} \mathcal{L}\big(c_{\nu,l_{i_j}} | r_{\nu,l_{i_j}}\big) = 2\tanh^{-1}\left(\prod_{j=1}^{N_i} \tanh\left(\mathcal{L}(r_{\nu,l_{i_j}}|c_{\nu,l_{i_j}})/2\right)\right). \end{aligned} \tag{2.11}$$

According to the LLR definition given by Eq. (2.4) and the parity-check relations given by Eq. (2.9), the LLR of the syndrome APP, $\gamma_{\nu,i}^{\theta'}$, is expected to be a positive value when $\theta' = \theta$. One may take the average over the individual LLRs $\gamma_{\nu,i}^{\theta'}$, $\forall\, i$, for the entire block ν, and the "positiveness" of the average LLR will be more substantial when $\theta' = \theta$. On the other hand, if $\theta' \neq \theta$, individual LLRs $\gamma_{\nu,i}^{\theta'}$ within the same block ν may be sometimes positive and sometimes negative and they often cancel each other when we calculate the corresponding average LLR. The average LLR for the ν^{th} block of received signal data subject to the encoder candidate θ' is thus given by

$$\Gamma_{\nu}^{\theta'} \stackrel{\text{def}}{=} \frac{1}{m} \sum_{i=1}^{m} \gamma_{\nu,i}^{\theta'}. \tag{2.12}$$

Note that different encoders θ' have different values of n and k so that the values of m (the number of parity-check bits) appear different. Consequently, according to Eqs. (2.11) and (2.12), the underlying LDPC encoder for the ν^{th} block of received signals can be identified as

$$\hat{\theta}_{\nu} = \arg\max_{\theta' \in \Theta} \Gamma_{\nu}^{\theta'}, \tag{2.13}$$

where Θ is the collection of all possible candidates for the LDPC encoders adopted in the transmitter. Note that one needs to carry out $\Gamma_{\nu}^{\theta'}$ for every possible candidate θ' in Θ according to Eq. (2.12). Alternatively, in order to facilitate the relationship between the average LLR and the number of parity-check bits, the average LLR for the first ι parity-check bits of the ν^{th} block of received signal samples subject to the encoder candidate θ' is given by

$$\Gamma_{\nu}^{\theta'}(\iota) \stackrel{\text{def}}{=} \frac{1}{\iota} \sum_{i=1}^{\iota} \gamma_{\nu,i}^{\theta'}, \qquad \iota = 1, 2, \ldots, m. \tag{2.14}$$

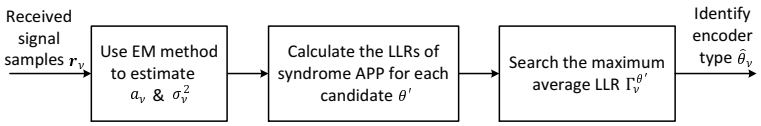

Figure 2.2: The block diagram of our proposed new blind LDPC encoder identification system.

It can be easily seen that Eq. (2.12) is a special case of Eq. (2.14) when $\iota = m$.

According to the system model given by Eq. (2.1), we can write

$$\mathcal{L}\big(r_{\nu,l_{i_j}}|c_{\nu,l_{i_j}}\big) = \frac{2a_\nu r_{\nu,l_{i_j}}}{\sigma_\nu^2}. \tag{2.15}$$

To carry out Eq. (2.13), one needs to calculate Eq. (2.15) first. However, the receiver has no *a priori* knowledge of the signal amplitude a_ν and the noise variance σ_ν^2. Therefore, they need to be *blindly* estimated prior to the calculation of the LLRs of syndrome APP $\gamma_{\nu,i}^{\theta'}$. We propose the blind estimators for a_ν and σ_ν^2 in the following section, which can serve as the frontend mechanism to complete our new blind LDPC encoder identification system, as depicted in Figure 2.2.

2.3 Blind Parameter Estimation

As discussed in Section 2.2.2, signal amplitude and noise variance are two parameters one needs to estimate first for blind LDPC-encoder identification. Since we focus on the blind scheme, the corresponding estimators have to be blind as well. There exist several *non-data aided* methods to estimate signal amplitude and noise variance, such as the M_2/M_4 estimator [25] and the EM (expectation maximization) estimator [26, 32]. The M_2/M_4 method works well for *constant modulus modulations* such as phase-shift keying (PSK). The received signals formulated by Eq. (2.1) constitute a Gaussian mixture where the EM algorithm can

be used to estimate the associated essential parameters. Therefore, we propose to use these two methods to estimate the signal amplitude a_ν and the noise variance σ_ν^2, and then compare their performances with the corresponding CRLBs. In the next subsection, we will present the formulae for the CRLBs of a_ν and σ_ν^2, respectively.

2.3.1 CRLBs

It is well known that for any underlying statistical parameter to be estimated, among all unbiased estimators, the CRLB facilitates the minimum variance. Hence we can use the CRLB as the benchmark to evaluate any estimator. As mentioned in Section 2.2.2, LDPC coded bits can take either 0 or 1 with equal probability and they are assumed statistically independent of each other. According to Eq. (2.1), the probability density function (PDF) of a received signal block $\mathbf{r}_\nu$ can thus be represented by

$$p(\mathbf{r}_\nu) = \prod_{j=0}^{n-1} \frac{1}{2} \frac{1}{\sqrt{2\pi\sigma_\nu^2}} \left[\exp\Big(- \frac{(r_{\nu,j} - a_\nu)^2}{2\sigma_\nu^2} \Big) + \exp\Big(- \frac{(r_{\nu,j} + a_\nu)^2}{2\sigma_\nu^2} \Big) \right]. \tag{2.16}$$

The associated log-likelihood function is thus given by

$$\ln p(\mathbf{r}_\nu) = -\frac{n}{2} \ln(2\pi\sigma_\nu^2) - \frac{1}{2\sigma_\nu^2} \sum_{j=0}^{n-1} \big(r_{\nu,j}^2 + a_\nu^2\big) + \sum_{j=0}^{n-1} \ln\left(\cosh\Big(\frac{a_\nu r_{\nu,j}}{\sigma_\nu^2}\Big) \right). \tag{2.17}$$

Denote $\boldsymbol{\lambda} \stackrel{\text{def}}{=} [a_\nu, \sigma_\nu^2]^T$ the vector of the unknown parameters. According to [33], the inverse of the *Fisher information matrix* can thus be expressed as

$$\mathbf{I}^{-1}(\boldsymbol{\lambda}) = \frac{2\,\sigma_\nu^2}{n\,g(\rho_\nu)} \begin{bmatrix} \frac{1}{2} - \rho_\nu f(\rho_\nu) & -a_\nu f(\rho_\nu) \\ -a_\nu f(\rho_\nu) & \sigma_\nu^2 - \sigma_\nu^2 f(\rho_\nu) \end{bmatrix}, \tag{2.18}$$

where ρ_ν is defined by Eq. (2.2),

$$g(\rho_\nu) \stackrel{\text{def}}{=} 1 - f(\rho_\nu) - 2\rho_\nu f(\rho_\nu), \tag{2.19}$$

and

$$f(\rho_\nu) \stackrel{\text{def}}{=} \frac{\exp\left(-\frac{\rho_\nu}{2}\right)}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \frac{u^2 \exp\left(-\frac{u^2}{2}\right)}{\cosh(u\sqrt{\rho_\nu})}\, du. \tag{2.20}$$

The CRLBs for the signal amplitude a_ν and the noise variance σ_ν^2 are found as the diagonal elements of $\mathbf{I}^{-1}(\boldsymbol{\lambda})$ such that

$$CRLB_{a_\nu} = \frac{\sigma_\nu^2\big(1 - 2\rho_\nu f(\rho_\nu)\big)}{n\, g(\rho_\nu)}, \tag{2.21}$$

$$CRLB_{\sigma_\nu^2} = \frac{2\sigma_\nu^4\big(1 - f(\rho_\nu)\big)}{n\, g(\rho_\nu)}. \tag{2.22}$$

The corresponding *normalized CRLBs* are defined as

$$NCRLB_{a_\nu} \stackrel{\text{def}}{=} \frac{CRLB_{a_\nu}}{a_\nu^2} \tag{2.23}$$

and

$$NCRLB_{\sigma_\nu^2} \stackrel{\text{def}}{=} \frac{CRLB_{\sigma_\nu^2}}{\sigma_\nu^4}, \tag{2.24}$$

respectively.

2.3.2 The M_2/M_4 Estimator

From Eq. (2.1), the second-order moment of the received signal sample $r_{\nu,j}$ is given by

$$M_2 \stackrel{\text{def}}{=} \mathbb{E}\{r_{\nu,j}^2\} = a_\nu^2 + \sigma_\nu^2, \tag{2.25}$$

while the fourth-order moment of $r_{\nu,j}$ is given by

$$M_4 \stackrel{\text{def}}{=} \mathbb{E}\{r_{\nu,j}^4\} = a_\nu^4 + 6a_\nu^2\sigma_\nu^2 + 3\sigma_\nu^4. \tag{2.26}$$

Solving both Eqs. (2.25) and (2.26) together with respect to the two variables a_ν and σ_ν^2, one can get

$$a_\nu = \frac{\sqrt[4]{6M_2^2 - 2M_4}}{\sqrt{2}} \tag{2.27}$$

and

$$\sigma_\nu^2 = M_2 - \frac{\sqrt{6M_2^2 - 2M_4}}{2}, \tag{2.28}$$

where a_ν is assumed to be non-negative. In practice, M_2 and M_4 have to be estimated by the sample averages over the ν^{th} block such that

$$\hat{M}_2 = \frac{1}{n}\sum_{j=0}^{n-1} r_{\nu,j}^2 \tag{2.29}$$

and

$$\hat{M}_4 = \frac{1}{n}\sum_{j=0}^{n-1} r_{\nu,j}^4. \tag{2.30}$$

Substituting Eqs. (2.29) and (2.30) into Eqs. (2.27) and (2.28), we can obtain the M_2/M_4 estimators for a_ν and σ_ν^2.

2.3.3 The EM Estimator

EM estimators have recently been applied for the parameter estimation in wireless communication systems [16, 34, 35]. Here we will establish an EM estimator for determining the signal amplitude a_ν and the noise variance σ_ν^2. According to the system model given by Eq. (2.1), it is obvious that the received signal symbols $r_{\nu,j}$ constitute a dual-modal Gaussian mixture. Upon receiving $r_{\nu,j}, j = 0, 1, \ldots, n-1$, our proposed EM algorithm is presented below.

First, initialize the parameters a_ν and σ_ν^2 using *K-means* clustering method for a few

iterations. The weight of each Gaussian mode is fixed to 1/2 as we assume that each bit in any LDPC codeword has equal probability for taking value of either 0 or 1.

At the E-step, compute

$$\hat{\beta}_{j,\kappa} = \frac{p_\kappa(r_{\nu,j}\,|\,\hat{a}_\nu, \hat{\sigma}_\nu^2)}{\sum_{\kappa=1}^{2} p_\kappa(r_{\nu,j}\,|\,\hat{a}_\nu, \hat{\sigma}_\nu^2)}, \tag{2.31}$$

where

$$p_\kappa(r_{\nu,j}\,|\,\hat{a}_\nu, \hat{\sigma}_\nu^2) \stackrel{\text{def}}{=} \frac{1}{\sqrt{2\pi\hat{\sigma}_\nu^2}} \exp\Big(- \frac{(r_{\nu,j} - \hat{a}_\nu\, x_\kappa)^2}{2\hat{\sigma}_\nu^2}\Big),$$

and

$$x_\kappa \stackrel{\text{def}}{=} \begin{cases} 1, & \kappa = 1 \\ -1, & \kappa = 2 \end{cases}$$

At the M-step, compute the new estimates

$$\hat{a}_\nu = \frac{1}{n} \sum_{j=0}^{n-1} \sum_{m=1}^{2} \hat{\beta}_{j,m}\, x_m\, r_{\nu,j} \tag{2.32}$$

and

$$\hat{\sigma}_\nu^2 = \frac{1}{n} \sum_{j=0}^{n-1} \sum_{m=1}^{2} \hat{\beta}_{j,m}\, (r_{\nu,j} - \hat{a}_\nu x_m)^2. \tag{2.33}$$

Take several iterations of E-step and M-step recursively until the pre-determined convergence criterion is satisfied.

2.3.4 Normalized Mean-Square-Error

To evaluate the performances of the above-mentioned estimators in Sections 2.3.2 and 2.3.3, one may use the *normalized mean-square-error* (NMSE) as the measure. The NMSEs for a_ν

and σ_ν^2 are given by

$$NMSE_{a_\nu} \stackrel{\text{def}}{=} \mathbb{E}\left\{\left(\frac{\hat{a}_\nu - a_\nu}{a_\nu}\right)^2\right\} \approx \frac{1}{N}\sum_{t=1}^{N}\left(\frac{\hat{a}_\nu^{(t)} - a_\nu}{a_\nu}\right)^2 \tag{2.34}$$

and

$$NMSE_{\sigma_\nu^2} \stackrel{\text{def}}{=} \mathbb{E}\left\{\left(\frac{\hat{\sigma}_\nu^2 - \sigma_\nu^2}{\sigma_\nu^2}\right)^2\right\} \approx \frac{1}{N}\sum_{t=1}^{N}\left(\frac{\hat{\sigma}_\nu^{2\,(t)} - \sigma_\nu^2}{\sigma_\nu^2}\right)^2, \tag{2.35}$$

where the superscript (t) indicates the trial index; N is the total number of Monte Carlo trials; a_ν and σ_ν^2 are true values while $\hat{a}_\nu$ and $\hat{\sigma}_\nu^2$ are the corresponding estimates, respectively.

3. NONBINARY LDPC ENCODER IDENTIFICATION

It can be observed from Chapter 2 that the calculation of the log-likelihood ratio of syndrome *a posteriori* probability in our blind encoder identification scheme is very similar to the *check-node* updates in the iterative message-passing decoding process of [19]. It is also known that the iterative *message-passing* decoding process becomes more complicated from binary LDPC codes to nonbinary ones [22, 23]. As a result, how to blindly identify nonbinary LDPC codes is not trivial at all. In this chapter, we would like to extend our proposed blind LDPC encoder identification scheme from binary codes to nonbinary ones.

3.1 Basic Transceiver Model

The block diagram of the transceiver involving our proposed novel blind nonbinary LDPC encoder identification mechanism is depicted in Figure 3.1. At the transmitter, original information symbols are in the Galois filed $\mathbb{GF}(q)$ and grouped into blocks, say $\mathbf{b}_\nu$ with length k, where ν is the *block index*. In this thesis, we assume that the order of the Galois field is represented by $q = 2^\mu$, where μ is an integer greater than 1. This block of information symbols $\mathbf{b}_\nu$ is passed to the "LDPC encoder θ over $\mathbb{GF}(q)$" to generate a corresponding block of "*codeword*" with length n, say $\mathbf{c}_\nu^\theta$, where θ specifies a certain nonbinary LDPC encoder. Then, the codeword $\mathbf{c}_\nu^\theta$ goes through "q-QAM Modulator" where q is assumed known at the receiver[1]. The corresponding block of modulated symbols are denoted by $\mathbf{s}_\nu^\theta$. These modulated q-QAM symbols will undergo a "frequency up-converter" to engender the *pass-*

[1]The modulation type q can be classified blindly according to [8, 36, 37], but it is not the focus of this thesis.

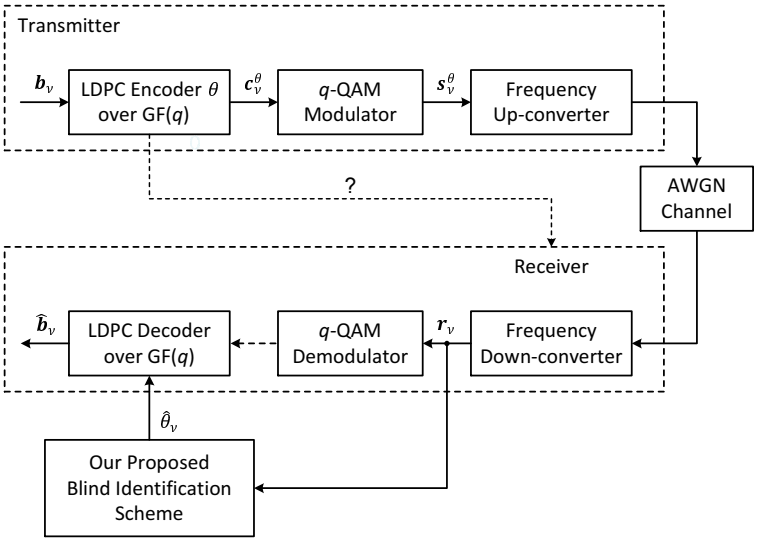

Figure 3.1: The system diagram of a basic AMC transceiver model involving nonbinary LDPC codes.

band signals for actual transmission.

The transmitted pass-band signals travel through the channel to arrive at the receiver. They will go through the "frequency down-converter" first to be converted back to the base-band. In this thesis, we assume that the received baseband signaling experiences perfect time- and frequency-synchronization. The received baseband signal symbols are also collected in codeword blocks of length n, say $\mathbf{r}_\nu$. Instead of simply passing $\mathbf{r}_\nu$ to the "q-QAM demodulator" as in the standard receivers, we propose to feed $\mathbf{r}_\nu$ to our novel "*blind identification scheme*" to identify θ, the unknown *nonbinary* LDPC encoder, from a given candidate set. Once the encoder is identified by our proposed scheme as $\hat{\theta}_\nu$ from the received signal codeword block $\mathbf{r}_\nu$, the appropriate nonbinary LDPC decoder can be employed to construct the information symbol estimates $\hat{\mathbf{b}}_\nu$.

Consider the additive white Gaussian noise (AWGN) channel. Each element of the ν^{th} codeword block of received baseband signal symbols, $\mathbf{r}_\nu \stackrel{\text{def}}{=} [r_{\nu,0},\, r_{\nu,1},\, \ldots,\, r_{\nu,j},\, \ldots,\, r_{\nu,n-1}]^T$,

can be expressed as

$$r_{\nu,j} = a_\nu \, e^{\imath \phi_\nu} \, s^{\theta}_{\nu,j} + w_{\nu,j}, \quad j = 0, 1, \ldots, n-1, \tag{3.1}$$

where $\imath \stackrel{\text{def}}{=} \sqrt{-1}$, a_ν is the unknown signal amplitude accounting for the processing gain and the channel gain, ϕ_ν is the unknown phase offset, $s^{\theta}_{\nu,j}$ is the modulated q-QAM signal generated from the encoder θ with the normalized energy $\mathbb{E}\{|s_{\nu,j}|^2\} = 1$, and $w_{\nu,j}$ is the zero-mean complex AWGN with the variances of its real and imaginary parts both equalling σ_ν^2 for the j^{th} signal sample within the ν^{th} block. Consequently, the *signal-to-noise ratio* (SNR) per coded symbol for the ν^{th} block of modulated signals is given by

$$\rho_\nu = \frac{a_\nu^2}{2\sigma_\nu^2}. \tag{3.2}$$

In order to evaluate the effect of different code rates $R = k/n$, the SNR per uncoded symbol for the ν^{th} block of modulated signals is given by

$$\eta_\nu \stackrel{\text{def}}{=} \frac{\rho_\nu}{R} = \frac{a_\nu^2}{2R\,\sigma_\nu^2}. \tag{3.3}$$

3.2 Nonbinary LDPC Encoder Identification

According to Figure 3.1, the receiver needs to identify the encoder θ before taking any action to decode the received signal symbols. In practice, an AMC transmitter would not change the encoder and modulator arbitrarily and it would establish a specific candidate set beforehand. Assume that the encoder candidate set, say Θ, is known to both transmitter and receiver, and θ can be any encoder in Θ. Hence, $\hat{\theta}_\nu \in \Theta$. In this section, we will present a novel method to blindly identify the *nonbinary* LDPC encoder from a given candidate set.

As each LDPC code has a unique parity-check matrix, the encoder θ can be unambiguously

identified if we can successfully establish the corresponding underlying *parity-check relations* directly from the received signal samples. The parity-check relations are manifested by that the sums of certain coded symbols in the codeword block over $\mathbb{GF}(q)$ are zeros. In this section, we need to formulate the log-likelihood ratio (LLR) of syndrome *a posteriori* probability (APP), which exploits the parity-check relations and indicates if the correct nonbinary LDPC encoder is discovered, for each possible encoder θ in Θ.

3.2.1 Log-likelihood Ratio Vectors

Since our blind LDPC encoder identification scheme relies on the LLR metric, the log-likelihood ratio for random variables over $\mathbb{GF}(q)$ needs to be formulated first. Denote $\mathbb{GF}(q) = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$, where $\alpha_0 = 0$. The $q \times 1$ *log-likelihood ratio vector* (LLRV) of a random variable $X = x$ over $\mathbb{GF}(q)$ is denoted by

$$\mathbf{L}(x) \stackrel{\text{def}}{=} [\mathcal{L}(x = \alpha_0), \mathcal{L}(x = \alpha_1), \ldots, \mathcal{L}(x = \alpha_{q-1})]^T, \tag{3.4}$$

where

$$\mathcal{L}\left(x = \alpha_\beta\right) \stackrel{\text{def}}{=} \ln \frac{P_r\{x = \alpha_0\}}{P_r\{x = \alpha_\beta\}}, \quad \beta = 0, 1, \ldots, q-1, \tag{3.5}$$

which is the natural logarithm of the ratio between the probabilities of x taking values α_0 and α_β, respectively. Apparently, $\mathcal{L}(x = \alpha_0) = 0$. From now on, we simplify the notation $\mathcal{L}(x = \alpha_\beta)$ to $\mathcal{L}(x)_\beta$ without introducing any ambiguity. Note that we place $P_r\{x = \alpha_0\}$ in the numerator (see Eq. (3.5)) rather than the denominator in contrast to the conventional definition given by [22,23]. It is more convenient for us to develop the syndrome *a posteriori* probability this way later on.

Given another random variable, say $Y = y$, we may write the β^{th} element of the LLRV

of x conditioned on y as

$$\mathcal{L}(x|y)_\beta = \mathcal{L}\left(x = \alpha_\beta | y\right) = \ln \frac{P_r\{x = \alpha_0 \,|\, y\}}{P_r\{x = \alpha_\beta \,|\, y\}}. \tag{3.6}$$

According to Bayes's theorem, we obtain

$$\begin{aligned} \mathcal{L}(x|y)_\beta &= \ln \frac{P_r\{y|\, x = \alpha_0\}}{P_r\{y|\, x = \alpha_\beta\}} + \ln \frac{P_r\{x = \alpha_0\}}{P_r\{x = \alpha_\beta\}} \\ &= \mathcal{L}(y|\, x = \alpha_\beta) + \mathcal{L}(x = \alpha_\beta) \\ &= \mathcal{L}(y|\, x)_\beta + \mathcal{L}(x)_\beta. \end{aligned} \tag{3.7}$$

Suppose that we have the LLRV of two random variables x_1, x_2 and two elements a_1, a_2, all in $\mathbb{GF}(q)$. Denote $\oplus$ as the addition operation over $\mathbb{GF}(q)$. The LLRV of $y = a_1 x_1 \oplus a_2 x_2$, defined as the *boxplus* operation, is formulated as (see [38])

$$\begin{aligned} \mathcal{L}(y)_\beta &\stackrel{\text{def}}{=} \boxplus\big(\mathbf{L}(x_1), \mathbf{L}(x_2); a_1, a_2\big)_\beta \\ &= \ln \frac{P_r\{a_1 x_1 \oplus a_2 x_2 = \alpha_0\}}{P_r\{a_1 x_1 \oplus a_2 x_2 = \alpha_\beta\}} \\ &= \ln \frac{\sum\limits_{z \in \mathbb{GF}(q)} \exp\left\{-\mathcal{L}(x_1 = z) - \mathcal{L}(x_2 = a_2^{-1} a_1 z)\right\}}{\sum\limits_{z \in \mathbb{GF}(q)} \exp\left\{-\mathcal{L}(x_1 = z) - \mathcal{L}(x_2 = a_2^{-1}(\alpha_\beta \oplus a_1 z))\right\}}. \end{aligned} \tag{3.8}$$

3.2.2 Our Proposed Novel Blind Encoder Identification Scheme

Given a nonbinary LDPC encoder $\theta' \in \Theta$ over $\mathbb{GF}(q)$, one can determine its parity-check matrix $\mathbf{H}_{\theta'}$, and obtain

$$\mathbf{H}_{\theta'}\, \mathbf{c}_\nu^\theta = \mathbf{0}, \text{ if and only if } \theta' = \theta, \tag{3.9}$$

where $\mathbf{0}$ is the $m \times 1$ zero vector and $m \geq n - k$ is the total number of rows in $\mathbf{H}_{\theta'}$. That is, the candidate LDPC encoder θ' is exactly the encoder θ adopted at the transmitter for the ν^{th} codeword block. Eq. (3.9) describes the so-called parity-check relations.

Denote the locations of the non-zero elements of the i^{th} row of the parity-check matrix $\mathbf{H}_{\theta'}$ by a vector $\mathbf{l}_i^{\theta'} = [l_{i_1}, l_{i_2}, \ldots, l_{i_{N_i}}]^T$ $(0 \leq l_{i_1} < l_{i_2} < \cdots < l_{i_{N_i}} \leq n-1)$, where N_i is the total number of the non-zero elements in the i^{th} row of $\mathbf{H}_{\theta'}$. Note that the location of the first element in any row of $\mathbf{H}_{\theta'}$ is indexed as "0" instead of "1". Thus, the non-zero elements of the i^{th} row of the parity-check matrix $\mathbf{H}_{\theta'}$ can be denoted by a vector $\mathbf{H}_i^{\theta'} = [h_{i,l_{i_1}}, h_{i,l_{i_2}}, \ldots, h_{i,l_{i_{N_i}}}]^T$. Denote $\mathbf{c}_\nu^\theta \stackrel{\text{def}}{=} [c_{\nu,0}, c_{\nu,1}, \ldots, c_{\nu,n-1}]^T$, for $i = 1, 2, \ldots, m$. We can rewrite Eq. (3.9) as

$$h_{i,l_{i_1}} c_{\nu,l_{i_1}} \oplus h_{i,l_{i_2}} c_{\nu,l_{i_2}} \oplus \cdots \oplus h_{i,l_{i_{N_i}}} c_{\nu,l_{i_{N_i}}} = 0, \quad \forall i, \tag{3.10}$$

if and only if $\theta' = \theta$.

Given the received symbols $r_{\nu,j}, j = 0, 1, \ldots, n-1$, according to Eq. (3.7), for $\beta = 0, 1, \ldots, q-1$, the β^{th} element of the LLRV of APP can be expressed as

$$\begin{aligned} \mathcal{L}(c_{\nu,j}|r_{\nu,j})_\beta &= \mathcal{L}(r_{\nu,j}|c_{\nu,j})_\beta + \mathcal{L}(c_{\nu,j})_\beta \\ &= \mathcal{L}(r_{\nu,j}|c_{\nu,j})_\beta, \end{aligned} \tag{3.11}$$

where $\mathcal{L}(c_{\nu,j})_\beta = 0$ because each symbol in any LDPC codeword is assumed to have equal probabilities of taking values α_β, $\forall \beta = 0, 1, \ldots, q-1$. If an encoder candidate θ' is picked at the receiver, according to Eqs. (3.8) and (3.10), the β^{th} element of the LLRV of syndrome APP for the i^{th} parity-check symbol in the ν^{th} codeword block can be formulated in a recursive way [38], that is,

$$\mathbf{L}_j = \boxplus\big(\mathbf{L}_{j-1}, \mathbf{L}(r_{\nu,l_{i_j}}|c_{\nu,l_{i_j}}); 1, h_{i,l_{i_j}}\big), \quad j = 3, 4, \ldots, N_i, \tag{3.12}$$

where $\mathbf{L}_2$ is initialized as

$$\mathbf{L}_2 = \boxplus\big(\mathbf{L}(r_{\nu,l_{i_1}}|c_{\nu,l_{i_1}}), \mathbf{L}(r_{\nu,l_{i_2}}|c_{\nu,l_{i_2}}); h_{i,l_{i_1}}, h_{i,l_{i_2}}\big). \tag{3.13}$$

As j reaches N_i, we obtain the LLRV of syndrome APP and we denote the β^{th} element $\mathbf{L}_j$ as $\gamma^{\theta'}_{\nu,i,\beta}$.

Here we can clearly see that the above procedures to obtain the LLRV of syndrome APP for the nonbinary LDPC codes over $\mathbb{GF}(q)$ are quite different from the procedures to obtain the LLR of syndrome APP for the binary LDPC codes (see [27]). The LLR for binary codes is a scalar; however, it becomes a $q \times 1$ vector for nonbinary codes. The syndrome APP can be calculated in one step for the binary codes, but it needs $N_i - 1$ recursions for the nonbinary codes. As a result, the number of the LLRs of syndrome APP is enlarged by $q-1$ times (the first element of the LLRV is always 0 and thus does not count) and the complexity is greatly increased from the binary to nonbinary cases thereby. These distinctions make the extension of our blind encoder identification scheme from the binary to nonbinary scenarios not straightforward at all.

Based on the LLR definition given by Eq. (3.5) and the parity-check relations given by Eq. (3.10), each nonzero element ($\beta \neq 0$) of the LLRV of syndrome APPs, $\gamma^{\theta'}_{\nu,i,\beta}$, is expected to be a positive value when $\theta' = \theta$. By taking the average of the individual LLRs $\gamma^{\theta'}_{\nu,i,\beta}$ over all i and all nonzero β for the ν^{th} codeword block, the "positiveness" will be more substantial if the correct encoder candidate is selected. On the other hand, if $\theta' \neq \theta$, the LLRs $\gamma^{\theta'}_{\nu,i,\beta}$ within the same codeword block ν may be sometimes positive and sometimes negative, and they often cancel each other so that the average tends to approach 0. This key feature of the LLRs of syndrome APPs reveals which encoder candidate should be the true one. The

average LLR for the ν^{th} codeword block of received symbols subject to the encoder candidate θ' is thus given by

$$\Gamma_{\nu}^{\theta'} \stackrel{\text{def}}{=} \frac{1}{m(q-1)} \sum_{i=1}^{m} \sum_{\beta=1}^{q-1} \gamma_{\nu,i,\beta}^{\theta'}. \tag{3.14}$$

From the above analysis, once computing $\Gamma_{\nu}^{\theta'}$ for all $\theta' \in \Theta$, one can identify the underlying LDPC encoder from the ν^{th} codeword block of received signals as

$$\hat{\theta}_{\nu} = \arg\max_{\theta' \in \Theta} \Gamma_{\nu}^{\theta'}, \tag{3.15}$$

where Θ is the predefined set of all possible nonbinary LDPC encoder candidates adopted by the transmitter.

When one calculates $\mathcal{L}\big(r_{\nu,l_{i_j}} | c_{\nu,l_{i_j}}\big)_{\beta}$ in Eq. (3.11), the unknown parameters, *signal amplitude* a_{ν}, *phase offset* ϕ_{ν}, and *noise variance* σ_{ν}^2, are involved. According to Eq. (3.1), $\mathcal{L}\big(r_{\nu,l_{i_j}} | c_{\nu,l_{i_j}}\big)_{\beta}$ can be expressed as

$$\mathcal{L}\big(r_{\nu,l_{i_j}} | c_{\nu,l_{i_j}}\big)_{\beta} = \ln \frac{\exp\left\{ - \frac{\left| r_{\nu,l_{i_j}} - a_{\nu} e^{\imath \phi_{\nu}} s_{\nu,l_{i_j},0} \right|^2}{2\sigma_{\nu}^2} \right\}}{\exp\left\{ - \frac{\left| r_{\nu,l_{i_j}} - a_{\nu} e^{\imath \phi_{\nu}} s_{\nu,l_{i_j},\beta} \right|^2}{2\sigma_{\nu}^2} \right\}}, \tag{3.16}$$

where $s_{\nu,l_{i_j},\beta}$ is the modulated symbol corresponding to the coded symbol $c_{\nu,l_{i_j}} = \alpha_{\beta}$. Thus, prior to the calculation of the LLRs given by Eq. (3.16), a_{ν}, ϕ_{ν}, and σ_{ν}^2 need to be estimated first. We propose to use the expectation-maximization (EM) algorithm to *blindly* estimate them [39].

In the end of this chapter, we would like to clarify the similarities and the differences of our proposed blind encoder identification schemes between binary LDPC codes and nonbinary ones.

- Similarities: The underlying ideas and procedures are basically the same. We use the

average LLR as the metric to distinguish different LDPC encoders. The EM algorithms are adopted to estimate unknown parameters.

- Differences: The signal is BPSK for binary LDPC codes but QAM for nonbinary ones. For nonbinary LDPC codes, the LLR becomes a vector and the LLR of syndrome APP has to be calculated in a recursive way while the scalar LLR for binary LDPC codes can be calculated at one step. For nonbinary LDPC codes, the EM algorithm has to be changed for QAM signals and one more parameter has to be estimated as well in comparison with binary LDPC codes. The computational complexity of the LLRV calculation for nonbinary LDPC codes is increased by $\mathcal{O}(q^2)$ compared to that of the LLR calculation for binary LDPC codes.

4. SIMULATION RESULTS

The performances of our proposed new blind LDPC-encoder identification schemes are evaluated by computer simulations in this chapter. The performance metric we choose is the *probability of detection*. It is the probability that the receiver can correctly identify the types of the LDPC encoders the transmitter adopts, i.e., $P_D = P_r\{\hat{\theta}_\nu = \theta_\nu\}$.

4.1 Binary LDPC Codes

The binary LDPC parity-check matrices defined in the IEEE 802.11n standard are used in our simulations [24]. Accordingly, three codeword block lengths $n = 648$, 1296, and 1944 are defined therein. For each block length n, four different parity-check matrices are specified corresponding to four different code-rates $R = 1/2$, $2/3$, $3/4$, and $5/6$. Hence, there are totally twelve types of LDPC encoders defined in [24]. The corresponding encoding techniques can refer to [40] for details. The simulation results will be presented in the following subsections.

4.1.1 Comparative Study on Blind Parameter Estimators

In this subsection, at first, we need to evaluate different estimators for signal amplitude and noise variance stated in Section 2.3. Ten thousand Monte Carlo trials ($N = 10,000$) are taken for statistical average. In each trial, we consider only a single signal block. We fix the LDPC encoder θ: $n = 648$ and $R = 1/2$ across all different trials. The modulated BPSK symbols $s^{\theta}_{\nu,j}$ have constant amplitudes, while a_ν varies subject to a uni-variance AWGN $w_{\nu,j}$

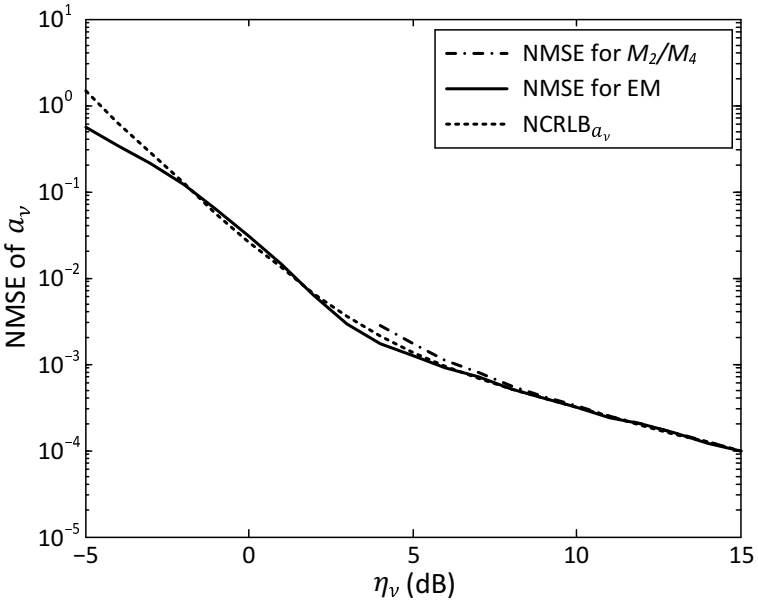

Figure 4.1: The NMSEs of M_2/M_4 and EM estimates of a_ν and the corresponding CRLBs with respect to η_ν.

so as to change the SNR η_ν. For each trial t, we obtain the estimates $\hat{a}_\nu^{(t)}$ and $\hat{\sigma}_\nu^{2\,(t)}$ using either M_2/M_4 or EM method (executed for five iterations) as described in Section 2.3. Then we carry out the NMSE measures for these estimates over 10,000 trials. Besides, we calculate the normalized CRLBs as given by Section 2.3.1.

The NMSEs for the signal amplitude a_ν and the noise variance σ_ν^2 together with the corresponding normalized CRLBs are depicted in Figures 4.1 and 4.2, respectively. It is obvious that the M_2/M_4 estimators can achieve reasonably good performances only when $\eta_\nu > 4$ dB. If $\eta_\nu < 4$ dB, the term $6\hat{M}_2^2 - 2\hat{M}_4$ substituted in Eq. (2.27) is not necessarily always positive so that the resultant estimates would appear to be complex values, which cannot be used as legitimate parameters. Besides, the EM estimates provide us with the lower NMSEs than the M_2/M_4 estimators when $\eta_\nu > 4$ dB.

Note that the NMSEs of the EM estimates sometimes fall below the NCRLBs when $\eta_\nu < 6$ dB. Similar phenomenon was also observed in [26, 32]. As a matter of fact, the estimates

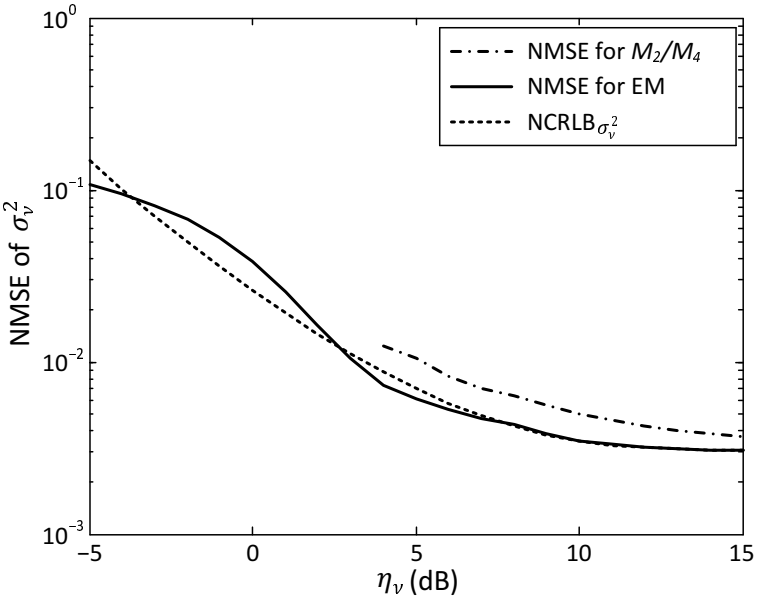

Figure 4.2: The NMSEs of M_2/M_4 and EM estimates of σ_ν^2 and the corresponding CRLBs with respect to η_ν.

produced by the EM algorithm may not always be unbiased. To study the *average biases* of the EM estimates, we have carried out 10,000 Monte Carlo simulations to measure their *normalized biases*, which are

$$NB_{a_\nu} \stackrel{\text{def}}{=} \mathbb{E}\left\{\frac{\hat{a}_\nu - a_\nu}{a_\nu}\right\} \approx \frac{1}{N}\sum_{t=1}^{N}\frac{\hat{a}_\nu^{(t)} - a_\nu}{a_\nu}, \tag{4.1}$$

$$NB_{\sigma_\nu^2} \stackrel{\text{def}}{=} \mathbb{E}\left\{\frac{\hat{\sigma}_\nu^2 - \sigma_\nu^2}{\sigma_\nu^2}\right\} \approx \frac{1}{N}\sum_{t=1}^{N}\frac{\hat{\sigma}_\nu^{2\,(t)} - \sigma_\nu^2}{\sigma_\nu^2}. \tag{4.2}$$

Figure 4.3 demonstrates that the normalized biases NB_{a_ν} and $NB_{\sigma_\nu^2}$ are not negligible when $\eta_\nu < 6$ dB. This explains why the NMSEs of the EM estimates can be lower than the NCRLBs in poor signal quality. Similar trends can be found when different (n, k) encoders are applied for Monte Carlo simulations.

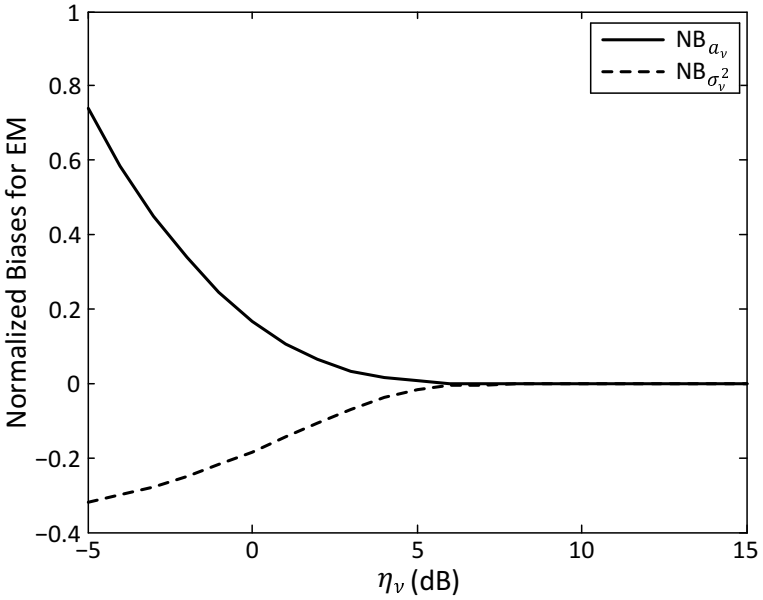

Figure 4.3: The normalized biases for the EM estimates of a_ν and σ_ν^2 with respect to η_ν.

4.1.2 Average LLRs

According to the discussion in Section 4.1.1, we choose the EM estimators in our blind LDPC encoder identification scheme. Based on the estimates $\hat{a}_\nu$ and $\hat{\sigma}_\nu^2$ resulting from the EM method, the LLRs of syndrome APP are calculated and the corresponding average LLRs $\Gamma_\nu^{\theta'}$ can be investigated. The signals and noises are generated in a similar manner to Section 4.1.1 subject to a *fixed* SNR $\eta_\nu = 8$ dB. For illustration, we just fix the codeword block length to $n = 648$ and examine the average LLRs $\Gamma_\nu^{\theta'}$ for four different code-rates $R = 1/2$, $R = 2/3$, $R = 3/4$, and $R = 5/6$. Thus, we have four encoder candidates, i.e., $|\Theta| = 4$. For each received signal block ν, the receiver calculates the average LLR $\Gamma_\nu^{\theta'}$ for each candidate $\theta' \in \Theta$.

To investigate the variations of the average LLRs $\Gamma_\nu^{\theta'}(\iota)$, each of which is constructed from the first ι parity-check bits of the ν^{th} block of received signal samples subject to the encoder candidate θ', as given by Eq. (2.14), we delineate Figure 4.4. Each sub-figure consists of the

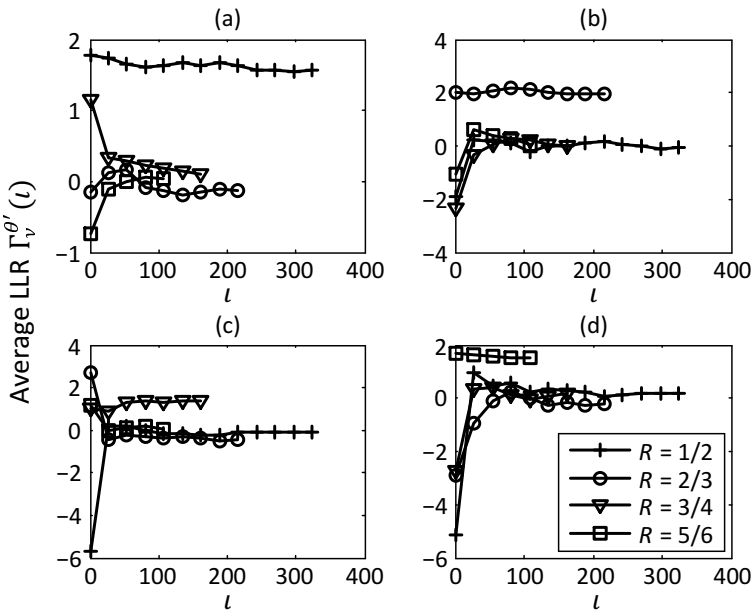

Figure 4.4: The average LLRs $\Gamma_\nu^{\theta'}(\iota)$ with respect to ι when $\eta_\nu = 8$ dB and $n = 648$ for (a) the true LDPC encoder θ: $R = 1/2$, (b) the true LDPC encoder θ: $R = 2/3$, (c) the true LDPC encoder θ: $R = 3/4$, and (d) the true LDPC encoder θ: $R = 5/6$.

average LLRs for four different candidates, namely $\theta' : R = 1/2$, $\theta' : R = 2/3$, $\theta' : R = 3/4$, and $\theta' : R = 5/6$. For different code-rates R, the numbers of parity-check bits, $n - k$, are surely different (the ranges of ι thus vary in these subfigures).

According to Figure 4.4, the average LLRs for $\theta' = \theta$ reach the maximum and always *stay positive* among all candidates $\theta' \in \Theta$, that is, a correct encoder identification can be undertaken. On the contrary, for $\theta' \neq \theta$, the average LLRs fluctuate around zero and tend to be close to 0 as ι increases. In addition, one may desire to use as many parity-check bits (large ι) as possible to reach a satisfactory encoder identification performance. If we may collect the entire received signal block to build the LLRs, the average LLR formula $\Gamma_\nu^{\theta'}$ given by Eq. (2.12) is used for blind encoder identification instead. The average LLRs for the block lengths $n = 1296$ and $n = 1944$ have also been investigated and similar phenomena can be observed.

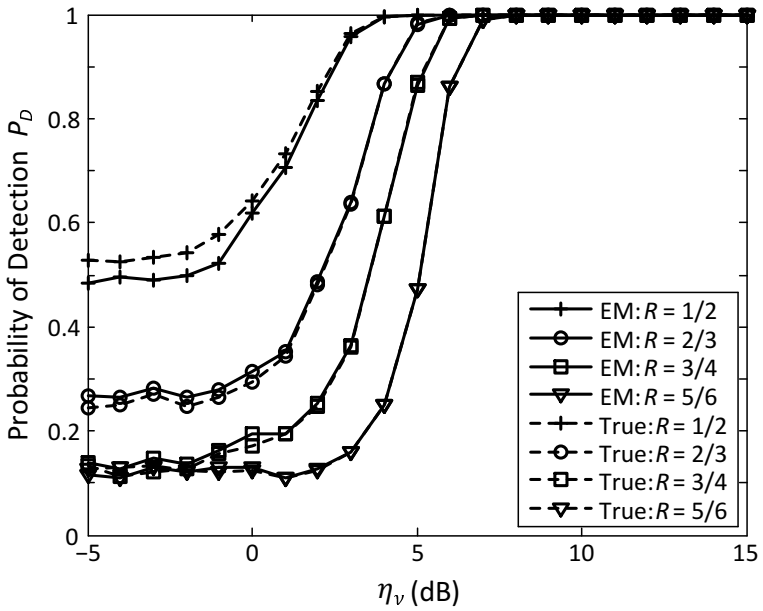

Figure 4.5: The probabilities of detection P_D with respect to η_ν for the codeword block length $n = 648$ and different code-rates R.

4.1.3 Probability of Detection Per Block

The evaluation of the probability of detection P_D per block is carried out in the same simulation set-up as Section 4.1.2. Once the average LLRs are computed, the blind identification can be performed using Eq. (2.13).

Figure 4.5 demonstrates P_D per block versus η_ν for four different code-rates when the codeword length is fixed as $n = 648$. We also investigate the effect of the EM estimators for signal amplitude and noise variance on P_D by comparing the identification results from the estimates (denoted by "EM" in the figure) and the true values of parameters (denoted by "True" in the figure). According to Figure 4.5, the EM estimators perform very well and hence they lead to very similar identification performances to those from the true values of parameters. Moreover, the lower the code-rate, the higher the probability of detection. For example, when $\eta_\nu = 5$ dB, P_D can reach close to 100% for the code-rate $R = 1/2$, while P_D

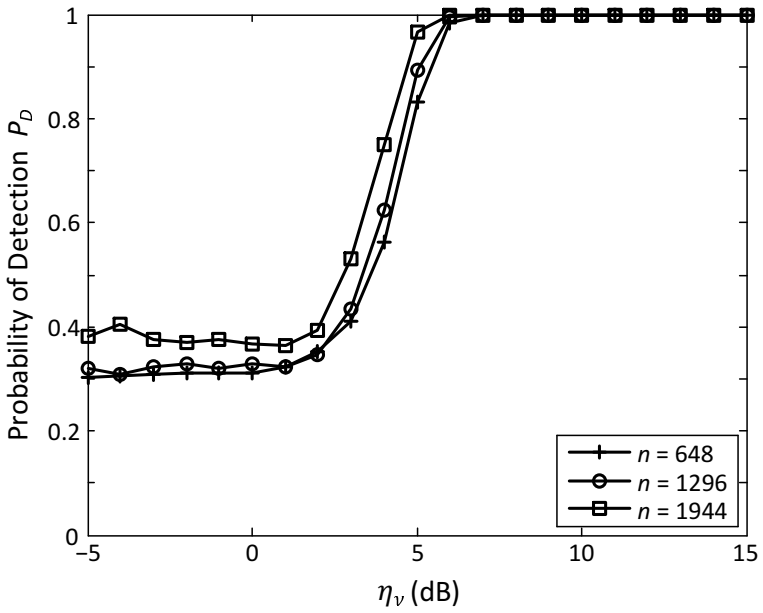

Figure 4.6: The probabilities of detection P_D with respect to η_ν for the code-rate $R = 5/6$ and different codeword block lengths n.

can only attain about 50% for the code-rate $R = 5/6$.

On the other hand, we fix the code-rate $R = 5/6$ and change the codeword block length n to depict Figure 4.6. According to the results shown in Figure 4.5, we use the EM estimators here to facilitate a completely blind encoder identification scheme since they can lead to outstanding performances. Figure 4.6 exhibits P_D per block versus η_ν for three different codeword block lengths n ($|\Theta| = 3$) for the code-rate $R = 5/6$. The larger the codeword block length, the higher the probability of detection P_D. Note that P_D for the codeword block length $n = 648$ depicted in Figure 4.6 is different from P_D for the same code rate $R = 5/6$ shown in Figure 4.5. The reason is simply because these two figures are based on different candidate sets Θ and the encoder identification performance highly depends on the particular candidate set Θ.

4.1.4 Probability of Detection for Multiple Blocks

Both Figures 4.5 and 4.6 demonstrate the fact that the more parity-check bits one uses to construct the average LLRs, the better P_D performance one can expect. Therefore, it is expected that P_D would be yet higher if we collect multiple blocks jointly for blind encoder identification. In practice, the transmitter is likely to retain the same encoder for a while spanning over several consecutive codeword blocks. Assume that each encoder θ lasts for M consecutive blocks ($M \in \mathcal{Z}^+$). It yields

$$\theta_\nu = \theta_{\lfloor \nu/M \rfloor \times M}, \qquad \forall\ \nu \in \mathcal{Z}, \tag{4.3}$$

where $\lfloor\ \rfloor$ denotes the "*integer rounding-down*" operation. For instance, when $M = 5$, one gets $\theta_0 = \theta_1 = \theta_2 = \theta_3 = \theta_4$. According to Eq. (4.3), one can compute a single average LLR $\bar{\Gamma}_M^{\theta'}$ over $\Gamma_\nu^{\theta'}$s for M consecutive blocks, which is given by

$$\bar{\Gamma}_M^{\theta'} \stackrel{\text{def}}{=} \frac{1}{M} \sum_{\nu=\tau}^{\tau+M-1} \Gamma_\nu^{\theta'}, \tag{4.4}$$

where τ specifies the very first block of these M consecutive blocks. Consequently, the encoder can be blindly identified as

$$\hat{\theta}_\nu = \arg\max_{\theta' \in \Theta} \bar{\Gamma}_M^{\theta'}, \qquad \text{for} \quad \nu = \tau, \tau+1, \ldots, \tau+M-1. \tag{4.5}$$

Since the signal amplitude a_ν and the noise variance σ_ν^2 change with the block index ν, the *average SNR per uncoded bit over M received signal blocks*, η_{ave}, is defined as

$$\eta_{\text{ave}} \stackrel{\text{def}}{=} \mathbb{E}\{\eta_\nu\} \approx \frac{1}{M} \sum_{\nu=\tau}^{\tau+M-1} \eta_\nu. \tag{4.6}$$

We retain the same simulation set-up as Figure 4.5 except that we use the new identification method given by Eq. (4.5) to depict the results in Figure 4.7. Figure 4.7 shows P_D

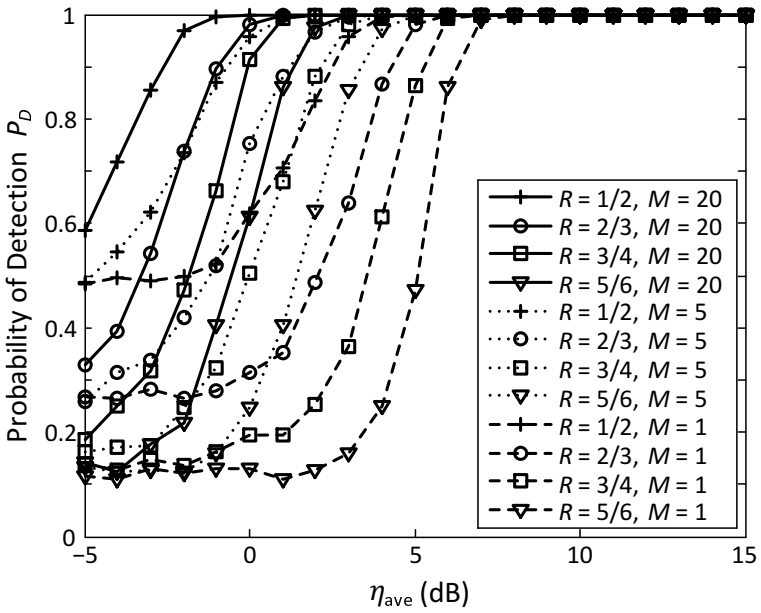

Figure 4.7: The probabilities of detection P_D with respect to η_{ave} for the codeword block length $n = 648$ and different code-rates R when different numbers of blocks, M=1, 5, and 20, are collected jointly for blind encoder identification.

versus η_{ave} for M=1, 5, and 20. The more the number of blocks M, the higher P_D one can expect from the blind identification results.

4.2 Nonbinary LDPC Codes

The nonbinary LDPC parity-check matrices are constructed according to [41]. Specifically, four encoders over $\mathbb{GF}(16)$ are constructed to generate four different (n, k) LDPC codes, namely a $(20, 11)$ code, a $(60, 33)$ code, a $(25, 16)$ code, and a $(75, 48)$ code. The first two codes have the code rate $R = 0.55$, and the last two codes have $R = 0.64$. These four LDPC codes form the candidate set Θ. The phase offset ϕ_ν is randomly chosen from $(-\pi/4, \pi/4)$ for each simulation trial since for square QAM constellations, ϕ_ν can only be blindly estimated within $(-\pi/4, \pi/4)$ due to the *quadrature symmetry* [39]. The phase ambiguity can be greatly eliminated by use of *differential coding*. However, it is out of the focus of this thesis.

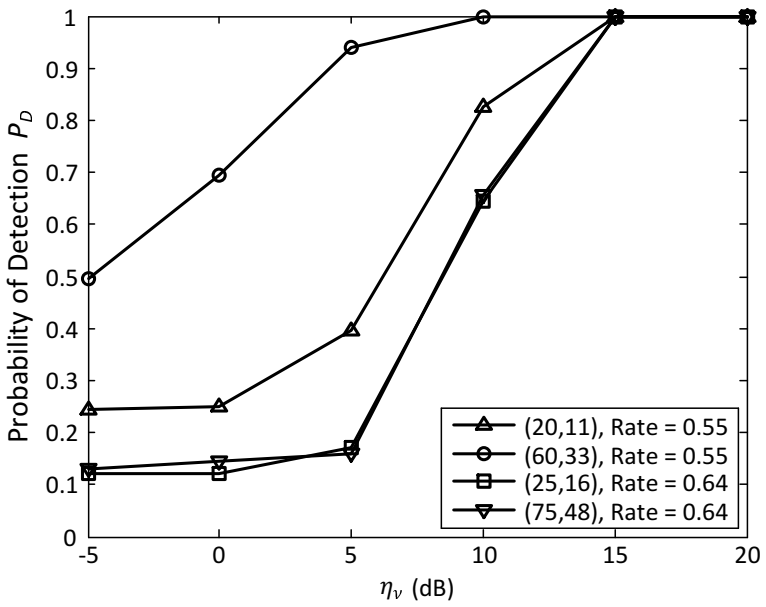

Figure 4.8: The probabilities of detection P_D with respect to η_ν for four different LDPC codes over $\mathbb{GF}(16)$.

Figure 4.8 illustrates the probability of detection P_D versus η_ν for the above four different LDPC codes over $\mathbb{GF}(16)$. The results show that P_D can reach 100% for each code as $\eta_\nu \geq 15$ dB. To have a better insight into the performance of our proposed blind encoder identification scheme, the *frame error rates* (FERs) of these four LDPC coders are investigated using the q-ary sum-product algorithm [22]. The simulation results demonstrate that when $\eta_\nu = 15$ dB, the FERs of $(20, 11)$, $(60, 33)$, $(25, 16)$, and $(75, 48)$ LDPC codes are 4.3×10^{-3}, 5.8×10^{-3}, 4.8×10^{-3}, and 3.1×10^{-3}, respectively. The results manifest that as long as the FER requirement is lower than 10^{-3}, our scheme can work perfectly. Similar trends can also be found by Monte Carlo simulations using LDPC codes over other $\mathbb{GF}(q)$.

5. CONCLUSION

In this thesis, we investigate a crucial problem emerging in adaptive modulation and coding transceivers, namely *blind encoder identification*. Maneuvering advanced statistical signal processing, we propose novel blind identification methods for both binary and non-binary low-density parity-check (LDPC) encoders. Our proposed schemes are based on the log-likelihood ratios (LLRs) of the syndrome *a posteriori* probability. The average LLRs over the entire block of parity-check bits or symbols are used as the essential features to dynamically identify the LDPC encoder adopted at the transmitter.

For binary LDPC codes, signal amplitude and noise variance involved in the construction of the LLRs need to be blindly estimated first. Therefore, we design M_2/M_4 and EM algorithms to estimate them. Furthermore, we establish the Cramer-Rao lower bounds for these two parameters and compare two corresponding blind estimators, namely M_2/M_4 and EM techniques.

For nonbinary LDPC codes, phase offset exists and also needs to be blindly estimated subject to QAM modulations. The log-likelihood ratios of the syndrome *a posteriori* probability have to be carried out in a recursive way instead. The EM estimators for phase offset, signal amplitude, and noise variance turn out to be the most robust techniques for our blind encoder identification schemes according to numerous simulations.

Monte Carlo simulation results by using the binary LDPC codes from the IEEE 802.11n standard and the nonbinary LDPC codes constructed by the finite field method are presented in this thesis to evaluate the effectiveness of our proposed new schemes.

Although our proposed blind encoder identification schemes are developed specifically for LDPC codes, they can be extended and tailored to other types of channel codes according to their various parity-check structures as well.

BIBLIOGRAPHY

[1] A. Goldsmith and S.-G. Chua, "Adaptive coded modulation for fading channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 595–602, May 1998.

[2] X. Huang, H.-C. Wu, and Y. Wu, "Novel pilot-free adaptive modulation for wireless OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3863–3867, Nov. 2008.

[3] X. Wang, A. Marques, and G. Giannakis, "Power-efficient resource allocation and quantization for TDMA using adaptive transmission and limited-rate feedback," *IEEE Trans. Signal Processing*, vol. 56, no. 9, pp. 4470–4485, Sep. 2008.

[4] H.-C. Wu and S. Y. Chang, "Constellation subset selection: Theories and algorithms," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2248–2257, Jul. 2010.

[5] S.-K. Ahn and K. Yang, "Adaptive modulation and coding schemes based on LDPC codes with irregular modulation," *IEEE Trans. Commun.*, vol. 58, no. 9, pp. 2465–2470, Sep. 2010.

[6] S. C.-H. Huang, H.-C. Wu, and S. Y. Chang, "Fast approximation algorithms for symmetric constellation subset selection," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1655–1665, May 2012.

[7] H.-C. Wu, Y. Wu, J. Principe, and X. Wang, "Robust switching blind equalizer for wireless cognitive receivers," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1461–1465, May 2008.

[8] H.-C. Wu, M. Saquib, and Z. Yun, "Novel automatic modulation classification using cumulant features for communications via multipath channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 8, pp. 3098–3105, Aug. 2008.

[9] F. Hameed, O. Dobre, and D. Popescu, "On the likelihood-based approach to modulation classification," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5884–5892, Dec. 2009.

[10] R. Imad, G. Sicot, and S. Houcke, "Blind frame synchronization for error correcting codes having a sparse parity check matrix," *IEEE Trans. Commun.*, vol. 57, no. 6, pp. 1574–1577, Jun. 2009.

[11] Y. Zrelli, M. Marazin, R. Gautier, and E. Rannou, "Blind identification of convolutional encoder parameters over GF(2^m) in the noiseless case," in *Proc. IEEE International Conference on Computer Communications and Networks (ICCCN'2011)*, Maui, Hawaii, Aug. 2011, pp. 1–5.

[12] V. Choqueuse, M. Marazin, L. Collin, K. Yao, and G. Burel, "Blind recognition of linear space-time block codes: A likelihood-based approach," *IEEE Trans. Signal Processing*, vol. 58, no. 3, pp. 1290–1299, Mar. 2010.

[13] R. Moosavi and E. Larsson, "A fast scheme for blind identification of channel codes," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM'2011)*, Houston, TX, Dec. 2011, pp. 1–5.

[14] E. Larsson and R. Moosavi, "Piggybacking an additional lonely bit on linearly coded payload data," *IEEE Wireless Commun. Lett.*, vol. 1, no. 4, pp. 292–295, Aug. 2012.

[15] Y. Debessu, H.-C. Wu, H. Jiang, and S. Y. Chang, "Blind encoder parameter estimation for turbo codes," in *IEEE Global Communications Conference (GLOBECOM'2012)*, 2012, pp. 4233–4237.

[16] Y. Debessu, H.-C. Wu, and H. Jiang, "Novel blind encoder parameter estimation for turbo codes," *IEEE Commun. Lett.*, vol. 16, no. 12, pp. 1917–1920, 2012.

[17] R. G. Gallager, *Low Density Parity Check Codes*. Cambridge, MA: MIT Press, 1963.

[18] D. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.

[19] T. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.

[20] T. Richardson, M. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.

[21] S.-Y. Chung, G. D. Forney, Jr., T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the shannon limit," *IEEE Commun. Lett.*, vol. 5, no. 2, pp. 58–60, Feb. 2001.

[22] M. Davey and D. MacKay, "Low-density parity check codes over GF(q)," *IEEE Commun. Lett.*, vol. 2, no. 6, pp. 165–167, Jun. 1998.

[23] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over GF(q)," *IEEE Trans. Commun.*, vol. 55, no. 4, pp. 633–643, Apr. 2007.

[24] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput*, IEEE Std. 802.11n-2009, 2009.

[25] D. Pauluzzi and N. Beaulieu, "A comparison of SNR estimation techniques for the AWGN channel," *IEEE Trans. Commun.*, vol. 48, no. 10, pp. 1681–1691, Oct. 2000.

[26] A. Wiesel, J. Goldberg, and H. Messer, "Non-data-aided signal-to-noise-ratio estimation," in *Proc. IEEE International Conference on Communications (ICC'2002)*, New York, NY, Apr. 2002, pp. 197–201.

[27] T. Xia and H.-C. Wu, "Novel blind identification of LDPC codes using average LLR of syndrome *a posteriori* probability," in *Proceedings of IEEE International Conference on Intelligent Transport Systems Telecommunications (ITST'2012)*, Taipei, Taiwan, Nov. 2012.

[28] ——, "Novel blind identification of LDPC codes using average LLR of syndrome *a posteriori* probability," will appear in *IEEE Transactions on Signal Processing*.

[29] ——, "Blind identification of nonbinary LDPC codes using average LLR of syndrome *a posteriori* probability," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1301–1304, Jul. 2013.

[30] R. Imad, S. Houcke, and M. Ghogho, "Blind estimation of the phase and carrier frequency offsets for LDPC-coded systems," *EURASIP J. Adv. Signal Process*, vol. 2010, pp. 1–13, Feb. 2010.

[31] J. Hagenauer, E. Offer, and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 429–445, Mar. 1996.

[32] A. Das, "NDA SNR estimation: CRLBs and EM based estimators," in *Proc. IEEE Region 10 Conference (TENCON'2008)*, Hyderabad, India, Nov. 2008, pp. 1–6.

[33] N. Alagha, "Cramer-Rao bounds of SNR estimates for BPSK and QPSK modulated signals," *IEEE Commun. Lett.*, vol. 5, no. 1, pp. 10–12, Jan. 2001.

[34] H.-C. Wu and X. Huang, "Joint phase/amplitude estimation and symbol detection for wireless ICI self-cancellation coded OFDM systems," *IEEE Trans. Broadcast.*, vol. 50, no. 1, pp. 49–55, Mar. 2004.

[35] H.-C. Wu, X. Huang, and D. Xu, "Pilot-free dynamic phase and amplitude estimations for wireless ICI self-cancellation coded OFDM systems," *Broadcasting, IEEE Transactions on*, vol. 51, no. 1, pp. 94–105, 2005.

[36] V. Orlic and M. Dukic, "Automatic modulation classification algorithm using higher-order cumulants under real-world channel conditions," *IEEE Commun. Lett.*, vol. 13, no. 12, pp. 917–919, Dec. 2009.

[37] O. Dobre, M. Oner, S. Rajan, and R. Inkol, "Cyclostationarity-based robust algorithms for QAM signal identification," *IEEE Commun. Lett.*, vol. 16, no. 1, pp. 12–15, Jan. 2012.

[38] H. Wymeersch, H. Steendam, and M. Moeneclaey, "Log-domain decoding of LDPC codes over GF(q)," in *Proc. IEEE International Conference on Communications (ICC'2004)*, Paris, France, Jun. 2004, pp. 772–776.

[39] W. Gappmair, R. Lopez-Valcarce, and C. Mosquera, "Joint NDA estimation of carrier frequency/phase and SNR for linearly modulated signals," *IEEE Signal Processing Lett.*, vol. 17, no. 5, pp. 517–520, May 2010.

[40] Z. Cai, J. Hao, P. Tan, S. Sun, and P. Chin, "Efficient encoding of IEEE 802.11n LDPC codes," *Electron. Lett.*, vol. 42, no. 25, pp. 1471–1472, Dec. 2006.

[41] L. Zeng, L. Lan, Y. Tai, S. Song, S. Lin, and K. Abdel-Ghaffar, "Constructions of nonbinary quasi-cyclic LDPC codes: A finite field approach," *IEEE Trans. Commun.*, vol. 56, no. 4, pp. 545–554, Apr. 2008.

VITA

Tian Xia was born in 1987 in a small town of Shanxi province, China. He received his B. S. and M. S. degrees in electrical engineering from University of Electronic Science and Technology of China, Chengdu, China, in 2008 and 2011, respectively. He came to Louisiana State University in 2012 and is currently a Ph.D. candidate in electrical and computer engineering.