ISSN 1099-4300
www.mdpi.com/journal/entropy
Article

# Information-Dispersion-Entropy-Based Blind Recognition of Binary BCH Codes in Soft Decision Situations 

Jing Zhou *, Zhiping Huang, Chunwu Liu, Shaojing Su and Yimeng Zhang

School of Mechatronics Engineering and Automation, National University of Defense Technology, Deya Road, Changsha 410073, Hunan Province, China; E-Mails: h.zhiping@hotmail.com (Z.H.); liuchunwu@nudt.edu.cn (C.L.); su_shaojing@163.com(S.S.); zhang_yimeng@nudt.edu.cn(Y.Z.)

* Author to whom correspondence should be addressed; E-Mail: zhou.jing@nudt.edu.cn; Tel.: +86-0731-84576387; Fax: +86-0731-84576387.

Received: 18 March 2013; in revised form: 24 April 2013 / Accepted: 1 May 2013 /
Published: 8 May 2013


#### Abstract

A method of blind recognition of the coding parameters for binary Bose-Chaudhuri-Hocquenghem ( BCH ) codes is proposed in this paper. We consider an intelligent communication receiver which can blindly recognize the coding parameters of the received data stream. The only knowledge is that the stream is encoded using binary BCH codes, while the coding parameters are unknown. The problem can be addressed on the context of the non-cooperative communications or adaptive coding and modulations (ACM) for cognitive radio networks. The recognition processing includes two major procedures: code length estimation and generator polynomial reconstruction. A hard decision method has been proposed in a previous literature. In this paper we propose the recognition approach in soft decision situations with Binary-Phase-Shift-Key modulations and Additive-White-Gaussian-Noise (AWGN) channels. The code length is estimated by maximizing the root information dispersion entropy function. And then we search for the code roots to reconstruct the primitive and generator polynomials. By utilizing the soft output of the channel, the recognition performance is improved and the simulations show the efficiency of the proposed algorithm.


Keywords: information dispersion entropy; blind recognition; channel coding; BCH codes; adaptive coding and modulation (ACM)

PACS Codes: 89.70.+c

## 1. Introduction

Channel coding, applied to reduce the errors in transmissions, is an important part in digital communications [1]. The binary Bose-Chaudhuri-Hocquenghem (BCH) codes are widely used for their powerful error-correcting capability [2], convenient design of encoders [3], and efficiency of decoding algorithms [4,5]. In traditional communication systems, the coding parameters are known by both the transmitters and receivers, but with the development of cognitive radios and intelligent techniques, blind recognition of the channel coding parameters is becoming available and realizable. Cognitive radio (CR) was introduced in [6] as a smart spectrum sharing technology, and it is becoming a hot research topic [7-10]. The adaptive coding and modulations (ACM) technique [11-14] is an important section of the CR to adapt the channel. In an ACM system, the transmitter chooses optimized coding and modulation parameters according to the channel quality. Thus at the reception, the receiver need to recognize those parameters before demodulation and decoding. Another application field of the blind recognition technique is non-cooperative communications [15,16]. In this case, a non-cooperative receiver does not known the modulation and coding parameters before recognizing them. In the future communications, the terminals are required to be as intelligent as possible to adapt themselves to a specific context and to blindly estimate the transmitter parameters for self-reconfiguration purpose, only with knowledge of the received data stream [17].

To the best of our knowledge, most of the blind recognition algorithms proposed in the literature are focused on convolutional codes. In [18], a Euclidean-algorithm-based method was proposed to identify a $1 / 2$ rate convolutional encoder in noiseless cases. However, it is not suitable for noisy channels. In [19], another approach was presented to identify a $1 / \mathrm{n}$ rate convolutional encoder in noisy cases based on the Expectation Maximization algorithm. The authors of [20,21] developed methods for blind recovery of convolutional encoders in turbo code configuration. In [13] and [17], dual code methods for blind identification of $\mathrm{k} / \mathrm{n}$ rate convolutional codes ware proposed for cognitive radio receivers.

In this paper we consider the problem of blind recognition of the coding parameters for a cognitive receiver. The main focus is on the widely used BCH codes. Some previous literature reports [22-24] proposed and developed recognition algorithms for BCH codes in hard decision situations. In [22] and [23], the authors proposed a blind recognition algorithm for BCH codes based on Root Information Dispersion Entropy and Root Statistic (RIDERS). This algorithm can achieve correct recognition with a bit error rate (BER) of $10^{-2}$, but it is computationally intensive, especially when the code length is large. The authors of [24] improved that algorithm proposed in [22,23] to reduce the computational complexity, which made the recognition procedure faster.

However, the previous works on blind recognition of BCH codes are all in hard decision situations, and are based on utilizing the algebraic properties of the codes in Galois Fields (GF). To achieve available recognition results, large amounts of training data are always required. With the development of sampling and signal processing techniques, the soft output of the channel has become available. Many soft-decision-based decoding algorithms have been applied to the error-correcting codes [25-30] and yield better decoding performances than hard decision algorithms. Some blind frame synchronization techniques for error correcting codes also utilize the soft output of the channel to improve the synchronization performances [31-34]. Inspired by the soft decision decoding algorithms, we develop the

RIDERS algorithm introduced by [22-24] in the soft decision situations in this paper. As an example we mainly discuss the problem of the soft decisions of BPSK modulation on AWGN channels.

The remaining of this paper is organized as follows: Section 2 presents the code length and coding starting positions estimation approach. Section 3 gives the code roots recognition method. Section 4 discusses the recognition of the primitive polynomial. In Section 5, we compare the computational complexity between hard decision and soft decision situations. Finally, the simulation results and conclusions are given in Section 6 and Section 7.

## 2. Code Length Estimation and Blind Synchronization

### 2.1. Introduction of the Recognition Algorithm in Hard Decision Situations

In cyclic coding theories, the algebraic model of the encoding operation can be expressed as follows:

$$
\begin{equation*}
c(x)=m(x) \times g(x) \tag{1}
\end{equation*}
$$

or in systematic form [35]:

$$
\begin{equation*}
c(x)=m(x) \times x^{n-k}+\left(\left(m(x) \times x^{n-k}\right) \bmod g(x)\right) \tag{2}
\end{equation*}
$$

Here $g(x)$ is the generator polynomial, $m(x)$ is the input information polynomial and $c(x)$ is the codeword polynomial, which are all defined over an extension field GF $\left(2^{m}\right)(m \geq 1)$. In Equation (2), $n$ and $k$ are the length of the codeword and input information, respectively, and $k / n$ is the code rate. Obviously in Equations (1) and (2), the roots of $g(x)$ are also the roots of $c(x)$. We define the code roots to be the roots of the generator polynomial $g(x)$ in this paper. The number of the elements in an extension field GF $\left(2^{m}\right)$ is $2^{m}-1$. We define the set of these elements as $\mathbf{G}_{m}$. For a binary BCH code defined in GF ( $2^{m}$ ), the possible code roots, which form a root set $\mathbf{A}$, are limited and included in $\mathbf{G}_{m}$. $\mathbf{A}$ is a subset of $\mathbf{G}_{m}$. We consider a sequence of $M$ valid codewords $C_{1}, C_{2}, \ldots, C_{M}$ and let $c_{j}(x)(1 \leq j \leq M)$ be the codeword polynomial of $C_{j}$. Initialize an integer vector $\left[N_{1}, N_{2}, \ldots, N_{M}\right]$ to zeros and get all the roots of each codeword polynomial $c_{j}(x)$ when $j$ increases from 1 to $M$. If the element $\alpha^{i}\left(1 \leq i \leq 2^{m}-1\right)$ in $\operatorname{GF}\left(2^{m}\right)$ is a root of $c_{j}(x)$, we let $N_{i}=N_{i}+1$, where $\alpha$ is a primitive element of GF $\left(2^{m}\right)$. Finally, the value of $N_{i}\left(1 \leq i \leq 2^{m}-1\right)$ reflects the probability of the element $\alpha^{i}\left(1 \leq i \leq 2^{m}-1\right)$ being a code root. Note that not all the roots of a valid codeword polynomial $c(x)$ are the code roots, but all the code roots must be the roots of $c(x)$. The elements, which are the roots of $c(x)$ but not the code roots, appear randomly in different codewords, because the information polynomials are not the same in different encoding operations. According to this fact, the probability of being a code root for an element in $\mathbf{A}$ should be larger than that in $\overline{\mathbf{A}}$, which is a complement of $\mathbf{A}$ in $\mathbf{G}_{m}$, so the values of $\left\{N_{i} \mid \alpha^{i} \in \mathbf{A}\right\}$ corresponding to the elements in $\mathbf{A}$ are generally larger than those corresponding to the elements in $\overline{\mathbf{A}}$, but this property is only true when the considered data blocks are valid codewords, i.e., the code length is correct and the codewords synchronization is achieved. When the code length or the coding starting positions are not correctly estimated, the property described above does not exist and the bits in the codewords can be considered to appear randomly. In this case, the authors of $[22,23]$ proposed the following hypothesis:

Hypothesis 1: When the coding parameters are not correct, the probabilities of being codeword roots of the elements in $\mathbf{G}_{m}$ can be assumed to be uniform, i.e., the values of $N_{i}$ is uniform no matter in $\mathbf{A}$ or $\overline{\mathbf{A}}$.

Therefore, in the correct parameters cases, the entropy of the distribution of the roots should be lower than that in the incorrect parameters cases. Based on this fact, the authors of [22,23] introduced a root information dispersion entropy function (RIDEF) to describe the imbalance degree of the $N_{i}$ on different $\alpha^{i}$ and proposed the correct coding parameters that maximize the RIDEF. The RIDEF is defined to be the difference between the entropy of the uniform distribution and the distribution of the code roots on all the elements in $\mathbf{G}_{m}$ as follows:

$$
\begin{equation*}
\Delta H=-\sum_{i=1}^{n} \frac{1}{n} \log \frac{1}{n}-\left(-\sum_{i=1}^{n} p_{i} \log p_{i}\right)=\sum_{i=1}^{n} p_{i} \log p_{i}+\log n \tag{3}
\end{equation*}
$$

where $n=2^{m}-1$ is the number of the elements in $\mathbf{G}_{m}$. $p_{i}$ is the probability of $\alpha^{i}$ being a root of the code, it is calculated as follows:

$$
\begin{equation*}
p_{i}=\frac{N_{i}}{\sum_{i=1}^{2^{m}-1} N_{i}}, 1 \leq i \leq 2^{m}-1 \tag{4}
\end{equation*}
$$

In the recognition procedure, we traverse all the possible values of code length and coding starting positions to find the ones that make $\Delta H$ be the largest as the estimation of code length and synchronization positions.

The RIDERS algorithm has good performance [22-24] in the parameter recognition of BCH codes. However, there are still some problems in the algorithm. Firstly, it is restricted to hard decision situations, which limits the recognition performance. Secondly, Hypothesis 1, as a basis of the algorithm, is not always true. In the following paragraphs we propose the recognition methods inspired by the RIDERS algorithm in soft decision situations. In the Appendix, we give the proof of the faultiness of Hypothesis 1.

### 2.2. Principles of the Proposed Recognition Algorithm in Soft Decision Situations

### 2.2.1. Calculation of $p_{i}$ in Soft Decision Situations

To develop the application of this algorithm to be suitable for soft decision cases, we should modify Equation (4) to utilize the soft output of the channel. To calculate $p_{i}$ in Equation (4) in soft decision situations, we define the minimal parity check matrix (MPCM) $H_{\text {min }}\left(\alpha^{i}\right)$ corresponding to the element $\alpha^{i}$ in $\mathrm{GF}\left(2^{m}\right)$ as follows:

$$
\begin{equation*}
H_{\min }\left(\alpha^{i}\right)=\left(\left(\alpha^{i}\right)^{l-1},\left(\alpha^{i}\right)^{l-2}, \cdots,\left(\alpha^{i}\right)^{1},\left(\alpha^{i}\right)^{0}\right) \tag{5}
\end{equation*}
$$

where $l$ is the code length. According to the coding theories, if $\alpha^{i}$ is a root of a codeword $C_{j}(1 \leq j \leq M)$, we have:

$$
\begin{equation*}
H_{\min }\left(\alpha^{i}\right) \times C_{j}=0 \tag{6}
\end{equation*}
$$

Soft outputs of the channel can provide more information about the reliability of each decision symbol. Instead of verifying whether $\alpha^{i}$ is a root of a codeword polynomial $c_{j}(x)$, we calculate $p_{j, i}\left(1 \leq i \leq 2^{m}-1,1 \leq j \leq M\right)$, which is the probability of $\alpha^{i}$ being a root of $c_{j}(x)$, and calculate $p_{i}$ in Equation (4) as follows:

$$
\begin{equation*}
p_{i}=\frac{\sum_{j=1}^{M} p_{j, i}}{\sum_{i=1}^{2^{m}-1} \sum_{j=1}^{M} p_{j, i}} \tag{7}
\end{equation*}
$$

To calculate $p_{j, i}$, we transform the MPCM defined in Equation (5) to its binary form by replacing the symbol elements in $H_{\text {min }}\left(\alpha^{i}\right)$ with their binary column vector patterns. For example, $H_{\text {min }}\left(\alpha^{3}\right)$, a BCH code corresponding to the element $\alpha^{3}$ in $\operatorname{GF}\left(2^{3}\right)$ with code length $l=7$, is as follows:

$$
H_{\min }\left(\alpha^{3}\right)=\left(\begin{array}{lllllll}
\alpha^{18} & \alpha^{15} & \alpha^{12} & \alpha^{9} & \alpha^{6} & \alpha^{3} & 1 \tag{8}
\end{array}\right)
$$

Based on the primitive polynomial $p(x)=x^{3}+x+1$, because the symbol $\alpha$ is a root of $p(x)$, we have $\alpha^{3}+\alpha+1=0$, and $\alpha^{3}=\alpha+1$. Other symbols are processed similarly. Finally, we can calculate all the symbols in $H_{\text {min }}\left(\alpha^{3}\right)$ and get their binary vector patterns listed in Table 1. By replacing the symbols in $H_{\text {min }}\left(\alpha^{3}\right)$ with the binary patterns, the MPCM can be written in its binary form as follows:

$$
H b_{\min }\left(\alpha^{3}\right)=\left(\begin{array}{lllllll}
1 & 1 & 1 & 1 & 1 & 0 & 0  \tag{9}\\
1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 1
\end{array}\right)
$$

Table 1. Symbols in $H_{\min }\left(\alpha^{3}\right)$ and their binary vector patterns.

| Symbols | Polynomial expressions | Vector form |
| :---: | :---: | :---: |
| 1 | 1 | 001 |
| $\alpha$ | $\alpha$ | 010 |
| $\alpha^{3}$ | $\alpha+1$ | 011 |
| $\alpha^{6}$ | $\alpha^{2}+1$ | 101 |
| $\alpha^{9}$ | $\alpha^{3}$ | 100 |
| $\alpha^{12}$ | $\alpha^{2}+\alpha+1$ | 111 |
| $\alpha^{15}$ | $\alpha$ | 010 |
| $\alpha^{18}$ | $\alpha^{2}+\alpha$ | 110 |

Note that the number of rows in $H_{\text {min }}\left(\alpha^{i}\right)$ equals to $m$, which is the degree of $\operatorname{GF}\left(2^{m}\right)$. And then the syndromes corresponding to the MPCM $H_{\min }\left(\alpha^{i}\right)$ and codeword $C_{j}(1 \leq j \leq M)$ are calculated in binary forms as follows:

$$
\begin{equation*}
\mathbf{S}_{j, i}=\left[S_{j, 1}, S_{j, 2}, \cdots, S_{j, m}\right]^{T}=H b_{\min }\left(\alpha^{i}\right) \times C_{j} \tag{10}
\end{equation*}
$$

Let $c_{j}(x)$ be the codeword polynomial of $C_{j}$, if the element $\alpha^{i}$ corresponding to $H b_{\text {min }}\left(\alpha^{i}\right)$ in Equation (10) is a root of $c_{j}(x)$, then we have $\mathbf{S}_{j, i}=0$. So the probability of $\mathbf{S}_{j, i}=0$ can be considered as $p_{j, i}$ in Equation (7) and calculated by the mean probabilities of $S_{j, k}=0(1 \leq k \leq m)$ :

$$
\begin{equation*}
p_{j, i}=P_{r}\left(\mathbf{S}_{j, i}=0\right)=\frac{1}{m} \sum_{k=1}^{m} P_{r}\left(S_{j, k}=0\right) \tag{11}
\end{equation*}
$$

In Equation (11) and the remainder of the paper we use $P_{r}(\Psi)$ to depict the probability of the event $\Psi$. We assume that the transmitter is sending a binary sequence of codewords and using a BPSK modulation, i.e., let +1 and -1 be the modulated symbols of 0 and 1 . The modulation operation from coded bit $c_{u}$ to modulated symbol $s_{u}$ can be written as:

$$
\begin{equation*}
s_{u}=1-2 c_{u}, \quad u=1,2,3, \ldots \tag{12}
\end{equation*}
$$

We assume that the propagation channel is a Binary Symmetry Channel (BSC) which is corrupted by an AWGN with the variance $\sigma_{\mathrm{n}}^{2}=N_{0} / 2$. For each configuration, the information symbols in the codes are randomly chosen. A soft decision symbol $r_{u}$ at the reception can be expressed as:

$$
\begin{equation*}
r_{u}=s_{u}+w_{u}, \quad u=1,2,3, \ldots \tag{13}
\end{equation*}
$$

where $\left(w_{1}, w_{2}, w_{3}, \ldots\right)$ is an AWGN sequence. According to [30], it is easy to prove that the probability $P_{r}\left(S_{j, k}=0\right)(1 \leq k \leq m)$ can be calculated as follows:

$$
\begin{equation*}
P_{r}\left(S_{j, k}=0\right)=\frac{1}{2}+\frac{1}{2} \prod_{u=1}^{n_{c}} \tanh \left(r_{u} / \sigma^{2}\right), \quad 1 \leq k \leq m \tag{14}
\end{equation*}
$$

where $n_{e}$ is the number of ones in the $e^{t h}$ row of the binary MPCM $H b_{\min }\left(\alpha^{i}\right)\left(1 \leq i \leq 2^{m}-1\right)$.

### 2.2.2. Adaptive Processing of MPCM

Note that the matrix $H b_{\text {min }}\left(\alpha^{i}\right)$ is not sparse, so a fault decision symbol has negative influences on many syndromes. Considering that the unreliable decision bits have higher probabilities of being error decisions than the reliable decision bits, the authors of [28] proposed an adaptive processing algorithm for the binary MPCM $H b_{\min }\left(\alpha^{i}\right)$ to reduce the influences of the unreliability decision bits when decoding the RS codes by utilizing the belief propagation (BP) algorithm. In this paper, we adopt that idea on the calculation of $P_{r}\left(\mathbf{S}_{j, i}=0\right)$. The detailed adaptive processing steps for a given binary MPCM $H b_{\min }\left(\alpha^{i}\right)$ and a codeword $C_{j}$ with the code length $l$ are listed below:

Step 1: Combine $H b_{\min }\left(\alpha^{i}\right)$ and $C_{j}^{T}$ to form a new matrix $H^{*}\left(\alpha^{i}\right)$ as follows:

$$
H^{*}\left(\alpha^{i}\right)=\left[\begin{array}{cccc}
r_{1} & r_{2} & \cdots & r_{l}  \tag{15}\\
-h_{11} & h_{12} & \cdots & h_{1 l} \\
h_{21} & h_{22} & \cdots & h_{2 l} \\
\vdots & \vdots & \ddots & \vdots \\
h_{m 1} & h_{m 2} & \cdots & h_{m l}
\end{array}\right]
$$

where $r_{1}, r_{2}, \ldots, r_{l}$ are the soft decision bits of the codeword $C_{j},\left\{h_{i j} \mid 1 \leq i \leq m, 1 \leq j \leq l\right\}$ are the elements of $H b_{\text {min }}\left(\alpha^{i}\right)$ in $\operatorname{GF}(2)$.

Step 2: Replace each $r_{u}(1 \leq u \leq l)$ in $H^{*}\left(\alpha^{i}\right)$ with their absolute values to form a matrix $H_{r}^{*}\left(\alpha^{i}\right)$, adjust the positions of the columns in $H_{r}{ }^{*}\left(\alpha^{i}\right)$ to make the first row in $H_{r}{ }^{*}\left(\alpha^{i}\right)$ is ranked from the lowest to the highest and record the indexes. The absolute values of $\left\{r_{u} \mid 1 \leq u \leq l\right\}$ denote the reliability of the received soft decision bits. As shown in Equation (16), $\left|r_{i_{1}}\right| \leq\left|r_{i_{2}}\right| \leq \cdots \leq\left|r_{i_{l}}\right|$ and $i_{1}, i_{2}, \cdots, i_{l}$ are the column indexes of $r_{i_{i}}, r_{i_{i}}, \cdots, r_{i_{i}}$ in $H^{*}\left(\alpha^{i}\right)$.

$$
H_{r}^{*}\left(\alpha^{i}\right)=\left[\begin{array}{cccc}
\left|r_{i_{i}}\right| & \left|r_{i_{2}}\right| & \cdots & \left|r_{i_{i}}\right|  \tag{16}\\
\hdashline h_{1 i_{1}} & h_{1 i_{2}} & \cdots & h_{1 i_{l}} \\
h_{2 i_{1}} & h_{2 i_{2}} & \cdots & h_{2 i_{i}} \\
\vdots & \vdots & \ddots & \vdots \\
h_{m i_{1}} & h_{m i_{2}} & \cdots & h_{m i_{i}}
\end{array}\right]
$$

Step 3: Transform $H_{r}{ }^{*}\left(\alpha^{i}\right)$ by elementary operations to make the last $m$ elements of the first column in $H_{r}^{*}\left(\alpha^{i}\right)$ has only one " 1 " at the top, as shown in Equation (17). The first row does not join the elementary transformation.

$$
H_{r}{ }^{*}\left(\alpha^{i}\right)=\left[\begin{array}{cccc}
\left|r_{r_{1}}\right| & \left|r_{i_{2}}\right| & \cdots & \left|r_{i_{i}}\right|  \tag{17}\\
\hdashline 1 & x & \cdots & x \\
0 & x & \cdots & x \\
\vdots & \vdots & \ddots & \vdots \\
0 & x & \cdots & x
\end{array}\right]
$$

This transformation limits the influences of the most unreliability decision bit to only one syndrome element, which is $S_{j, 1}$ in Equation (10). Furthermore, we continue the elementary transformation on $H_{r}{ }^{*}\left(\alpha^{i}\right)$ to limit the numbers of " 1 " in the following some columns to one (except the first row), as shown in Equation (18):

$$
H_{r}^{*}\left(\alpha^{i}\right)=\left[\begin{array}{cccccc}
\left|r_{i_{1}}\right| & \left|r_{i}\right| & \left|r_{r_{i}}\right| & \cdots & \left|r_{r_{i}}\right| & \left|r_{i_{1}}\right|  \tag{18}\\
\hdashline 1 & 0 & 0 & \cdots & x & x \\
0 & 1 & 0 & \cdots & x & x \\
0 & 0 & 1 & \cdots & x & x \\
\vdots & \vdots & \vdots & \ddots & x & x \\
0 & 0 & 0 & \cdots & x & x \\
0 & 0 & 0 & \cdots & x & x
\end{array}\right]
$$

When the elementary transformation is unavailable, stop the operation. The number available operation times equal to the rank of $H b_{\text {min }}\left(\alpha^{i}\right)$. Then the last $m$ rows in $H_{r}{ }^{*}\left(\alpha^{i}\right)$ form a new matrix. We recovery its original column orders and call it $H b_{\text {min }_{\_} a}\left(\alpha^{i}\right)$. Because the transformation is elementary, the relationship $H b_{\text {min_a }} \times C_{j}=0$, in the hard decision situations still exists if $C_{j}$ is a valid codeword, so
we can calculate the probability $P_{r}\left(S_{j, k}=0\right)$ defined in Equation (14) according to $H b_{\text {min_a }}\left(\alpha^{i}\right)$. This replacement reduces the influences of the unreliable decision bits.

If $\operatorname{rank}\left(H b_{\min \_a}\left(\alpha^{i}\right)\right)=m$, the left $m \times m$ area of $H b_{\min \_a}$ forms an identity matrix. But if $\operatorname{rank}\left(H b_{\min \_a}\left(\alpha^{i}\right)\right)<m, H b_{\min \_a}$ becomes the following style after the elementary transformations:

$$
H b_{\min \_a}\left(\alpha^{i}\right)=\left[\begin{array}{cccccc}
1 & 0 & 0 & \cdots & x & x  \tag{19}\\
0 & 1 & 0 & \cdots & x & x \\
0 & 0 & 1 & \cdots & x & x \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0
\end{array}\right]
$$

In this case, only the first $p$ rows are non-zeros, where $p=\operatorname{rank}\left(H b_{\text {min_a }}\left(\alpha^{i}\right)\right)$. The last $m-p$ rows have no contribution for the calculation of $P_{r}\left(\mathbf{S}_{j, i}=0\right)$ in Equation (11). So we modify Equation (11) and Equation (20):

$$
\begin{equation*}
p_{j, i}=P_{r}\left(\mathbf{S}_{j, i}=0\right)=\frac{1}{r a n k\left(H b_{\text {min_a }}\left(\alpha^{i}\right)\right)} \sum_{k=1}^{r a n k\left(H b_{\text {min }} a\left(\alpha^{i}\right)\right)} P_{r}\left(S_{j, k}=0\right) \tag{20}
\end{equation*}
$$

Now based on Equation (20), Equation (14) and Equation (7), we can calculate the RIDEF defined in Equation (3). However, there is still a problem in the algorithm. Note that the element $\alpha^{2^{m}-1}=1$ is a root of a codeword polynomial only if the code weight is even. This fact severely affects the assumption of uniformity of $p_{i}$. As shown in Figure 1, in the case of recognition of $\mathrm{BCH}(63,51)$, when we assume the code length is 31 , the value of $p_{31}$ is obviously larger than other $p$ values, although the real code length is not 31 and $\alpha^{31}=1$ is not a root of the code.

Figure 1. The problem of $p_{3 l}$.


To avoid that, we drop the calculation of the probability $P_{r}\left(\mathbf{S}_{j, i}=0\right)$ on the element $\alpha^{\alpha^{m}-1}=1$ when recognizing the code length. So we modify Equation (3) and Equation (7) to Equation (21) and Equation (22) respectively as follows:

$$
\begin{gather*}
\Delta H=\sum_{i=1}^{2^{m}-2} p_{i} \log p_{i}+\log \left(2^{m}-2\right)  \tag{21}\\
p_{i}=\frac{\sum_{j=1}^{M} p_{j, i}}{\sum_{i=1}^{2^{m}-2} \sum_{j=1}^{M} p_{j, i}} \tag{22}
\end{gather*}
$$

Considering that not all the rows in the parity check matrix $H b_{\text {min_a }}\left(\alpha^{i}\right)$ have the same value of $n_{e}$ [in Equation (14)], and this affects the comparability of $P_{r}\left(S_{j, k}=0\right)$ among different rows. For the uniformization reasons, so we modify Equation (14) to:

$$
\begin{align*}
P_{r}\left[S_{j, k}=0\right] & =\frac{1}{2}+\frac{1}{2} \operatorname{sign}\left[\prod_{u=1}^{n_{e}} \tanh \left(r_{u} / \sigma^{2}\right)\right]\left|\prod_{u=1}^{n_{e}} \tanh \left(r_{u} / \sigma^{2}\right)\right|^{\frac{1}{n_{e}}} \\
& =\frac{1}{2}+\frac{1}{2} \prod_{u=1}^{n_{e}} \operatorname{sign}\left(r_{u}\right) \times\left|\prod_{u=1}^{n_{e}} \tanh \left(r_{u} / \sigma^{2}\right)\right|^{\frac{1}{n_{e}}} \tag{23}
\end{align*}
$$

### 2.2.3. Summary of the Recognition Steps

According to Equation (20), Equation (21), Equation (22) and Equation (23), we propose the code length estimation and blind synchronization in the following steps for the convenience of computer program automatic processing:

Step 1: According to some prior information, set the searching range of the degree $m$, i.e., set the minimal and maximal degree $m_{\text {min }}$ and $m_{\max }$.

Step 2: Design a window $W$ which has a length $L$ at least $5 \times\left(2^{m_{\text {max }}}-1\right)$, i.e., $M \geq 5$ in Equation (22).

Step 3: Full fill the window $W$ with the received soft decision bits.
Step 4: Set the initial degree $m=m_{\text {min }}$.
Step 5: Set the code length $l=2^{m-1}$.
Step 6: Set the initial synchronization position $t$ at 0 , which is the starting position of $W$.
Step 7: Assume the code length is $l$ and the synchronization position is $t$ and calculate $\Delta H$. Note that the window $W$ has more than one assumed codewords, we calculate the $\Delta H$ on all the codewords and compute the mean of them as $\Delta H(l, t)$.

Step 8: If $t<l$, then let $t=t+1$ and go back to Step 7; if $t=l$, then jump to Step 9.
Step 9: If $l<2^{m}-1$, then let $l=l+1$ and go back to Step 6; if $l=2^{m}-1$, then jump to Step 10.
Step 10: If $m<m_{\max }$, then let $\mathrm{m}=\mathrm{m}+1$ and go back to Step 5; if $m=m_{\max }$, then jump to Step 11.

Step 11: Compare all the calculated $\Delta H(l, t)$, select the maximum one and get the corresponding values of $l, t$ and $m$ as the estimated code length, synchronization position and the degree of the GF of the being recognized codes, respectively.

By traversing all the possible $l$ and $t$, finally we can search out the parameters pair $(\hat{l}, \hat{t})$ that maximizes the RIDEF $\Delta H . \hat{l}$ and $\hat{t}+k \hat{l}(k \in \mathbb{Z})$ are the estimated code length and synchronization positions.

## 3. Code Roots Recognition and Generator Polynomial Reconstruction

### 3.1. Principles of the Code Roots Recognition

As mentioned in Section 2, for a given valid codeword $C_{j}$, the elements in $\mathbf{A}$ have higher probabilities of being the code roots of $C_{j}$ than the elements in $\overline{\mathbf{A}}$, where $\mathbf{A}$ is the set of the roots of the generator polynomial. So after the code length and synchronization position estimation, we can compare the Log-Likelihood Ratios (LLR) of $P_{r}\left(\mathbf{S}_{i}=0\right)$ on different elements in GF ( $2^{m}$ ) from $\alpha^{1}$ to $\alpha^{2^{m}-2}$ and choose the elements which make the LLR of $P_{r}\left(\mathbf{S}_{i}=0\right)$ be obviously higher as the estimated code roots. Finally, we propose a method to judge whether the element $\alpha^{2^{m}-1}=1$, be a root of the code.

In Equation (24), we define the LLR of $P_{r}\left(\mathbf{S}_{i}=0\right)$ as follows, which is also written as $L\left(\alpha^{i}\right)$ :

$$
\begin{equation*}
L\left(\alpha^{i}\right)=L\left[P_{r}\left(\mathbf{S}_{i}=0\right)\right]=\sum_{j=1}^{M} L\left[P_{r}\left(\mathbf{S}_{j, i}=0\right)\right]=\sum_{j=1}^{M}\left[\frac{1}{\operatorname{rank}\left(H b_{\min }\left(\alpha^{i}\right)\right)} \sum_{k=1}^{\operatorname{rank}\left(H b_{\text {min }}\left(\alpha^{i}\right)\right)} L\left(S_{j, k}=0\right)\right] \tag{24}
\end{equation*}
$$

where:

$$
\begin{equation*}
L\left(S_{j, k}=0\right)=\log \frac{P_{r}\left(S_{j, k}=0\right)}{P_{r}\left(S_{j, k} \neq 0\right)}=2 \operatorname{artanh}\left[\prod_{u=1}^{n_{e}} \operatorname{sign}\left(r_{u}\right) \times\left|\prod_{u=1}^{n_{e}} \tanh \left(r_{u} / \sigma^{2}\right)\right|^{\frac{1}{n_{e}}}\right] \tag{25}
\end{equation*}
$$

But for a computer, the "previous higher" is difficult to follow. For the realization of the computer automatic recognition of the code roots, we propose the procedure includes the following steps:

Step1: Let $l$ be the estimated code length, calculate the LLRs to form a vector: $L_{l}=\left[L(\alpha), L\left(\alpha^{2}\right), \cdots, L\left(\alpha^{2^{m}-2}\right)\right]$.

Step2: Rank the vector $L_{l}$ from the lowest to the highest, in order to form a new vector $L_{l R}$, and record the indexes.

Step3: Calculate $d L$, which is the difference of $L_{l R}: d L(i)=L_{l R}(i+1)-L_{l R}(i) \quad(1 \leq i \leq l-1)$.
Step4: Find the maximum of $d L$, record the corresponding value of $i$.
Step5: Select the $(i+1)^{\text {th }}$ to the $l^{\text {th }}$ elements in $L_{I R}$, get their positions in the vector $L_{l}$ and find corresponding GF elements $\left\{\alpha^{j_{1}}, \alpha^{j_{2}}, \cdots\right\}$ as the estimated roots.

As an example, we consider a $\operatorname{BCH}(63,51)$ code which is corrupted by an AWGN with SNR $\mathrm{E}_{\mathrm{s}} / \mathrm{N}_{0}=5 \mathrm{~dB}$, and the corresponding hard decision BER is $10^{-2.19}$. The recognizing procedure is shown in Figure 2.

Figure 2. Code roots recognition of $\operatorname{BCH}(63,51)$. (a) Original LLRs. (b) Rank the vector $L_{l}$ to form $L_{l R}$ (c) $d L$ : the difference of $L_{l R}$ (d) Insert $L\left(\alpha^{2^{m}-1}\right)$ into $L_{l}$.


Figure 2a is the original LLRs calculated in Step 1. By ranking the original LLRs from the lowest to the highest according to Step 2, we can get $L_{l R}$ as shown in Figure 2b. We can see that the change between $L_{I R}(39)$ and $L_{I R}(40)$ is the largest, i.e., the difference $d L(50)$ on $i=50$ in Figure 2c is the largest. Thus, we propose $L_{l R}(i)(i>50)$ as the LLRs of the generator polynomial roots, which are $\alpha^{1}, \alpha^{3}$ and their conjugate roots.

### 3.2. Discussion of the Element $\alpha^{2^{m}-1}$

Up to now, we have estimated the code roots from the set $\left\{\alpha^{1}, \alpha^{2}, \cdots, \alpha^{\alpha^{m}-2}\right\}$ but the element $\alpha^{2^{m}-1}$ is ignored. To verify whether the element $\alpha^{2^{m}-1}=1$ is a root of the code, a method is calculating the LLR $L\left(\alpha^{2^{m}-1}\right)$ according to its MPCM:

$$
\left.H_{\min }\left(\alpha^{2^{m}-1}\right)=\left(\begin{array}{llll}
\left(\alpha^{2^{m}-1}\right.
\end{array}\right)^{n-1-l_{s}} \quad\left(\alpha^{2^{m}-1}\right)^{n-2-l_{s}} \cdots\left(\begin{array}{ll}
\alpha^{2^{m}-1} \tag{26}
\end{array}\right)^{1} \quad 1\right)
$$

But obviously, we have $H_{\min }\left(\alpha^{2^{m}-1}\right)=H b_{\min }\left(\alpha^{2^{m}-1}\right)=H b_{\min a}\left(\alpha^{2^{m}-1}\right)=\left(\begin{array}{llll}1 & 1 & \cdots & 1\end{array}\right)$, because $\alpha^{2^{m}-1} \equiv 1$. The MPCM is an overall-ones vector which provides very little information for the calculation of the LLR. We propose to create a new MPCM for the element $\alpha^{2^{m}-1}$ simply by the NOT of the minimal check matrix of one of the estimated roots. To get high reliability, we choose the root that has the highest LLR.

The parity check matrix of a code, which has $k+1$ roots include $\alpha^{2^{m}-1}$, has a form as shown in Equation (27):

$$
H=\left(\begin{array}{ccccc}
\alpha_{1}{ }^{n-1} & \alpha_{1}{ }^{n-2} & \cdots & \alpha_{1} & 1  \tag{27}\\
\alpha_{2}{ }^{n-1} & \alpha_{2}{ }^{n-2} & \cdots & \alpha_{2} & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
\alpha_{k}{ }^{n-1} & \alpha_{k}{ }^{n-2} & \cdots & \alpha_{k} & 1 \\
1 & 1 & \cdots & 1 & 1
\end{array}\right)
$$

We choose one of its first $k$ rows and its last row to form a new matrix $H^{\prime}$ as follows:

$$
H^{\prime}=\left(\begin{array}{ccccc}
\alpha_{i}^{n-1} & \alpha_{i}^{n-2} & \cdots & \alpha_{i}^{1} & 1  \tag{28}\\
1 & 1 & 1 & 1 & 1
\end{array}\right)
$$

Then we transform $H^{\prime}$ to its binary pattern as follows:

$$
H_{b i n}^{\prime}=\left(\begin{array}{ccccc}
x & x & \cdots & x & 1  \tag{29}\\
x & x & \cdots & x & 1 \\
\vdots & \vdots & \cdots & \vdots & \vdots \\
x & x & \cdots & x & 1 \\
1 & 1 & \cdots & 1 & 1
\end{array}\right)
$$

We define $H_{b i n_{-} f}^{\prime}$ to be any single row of $H_{b i n}^{\prime}$ except the last row, and $H^{\prime}{ }_{b i_{-}-}$to be the last row. For each valid codeword $C$, we have $H_{b i n}^{\prime} \times C=0$. Thus, we have $\left(H_{b i n_{-} f}^{\prime} \oplus H^{\prime}{ }_{b i n_{-} l}\right) \times C=0$. Because all the elements in the last row of $H^{\prime}{ }_{b i n}$ are 1, the XOR and NOT operation is equivalent. Therefore, $\operatorname{NOT}\left(H_{b i_{n} f}^{\prime}\right) \times C=0$. As a result, the NOT of any row in the MPCM of one of the estimated roots is still a valid MPCM when the code has a root $\alpha^{2^{m}-1}$.

Based on the new MPCM, we calculate the LLR on $\alpha^{2^{m}-1}$, and insert it into the vector $L_{l}$ referred in Step1. Then we re-rank the LLRs and estimate the code roots according to the previous steps. Finally, we can write the generator polynomial based on all of the estimated code roots as:

$$
\begin{equation*}
g(x)=\left(x-\alpha_{1}\right)\left(x-\alpha_{2}\right) \cdots\left(x-\alpha_{p}\right) \tag{30}
\end{equation*}
$$

where $\alpha_{1}, \alpha_{2}, \ldots, \alpha_{p}$ are the estimated code roots. In the example of the recognition of $\mathrm{BCH}(63,51)$ code referred previous as shown in Figure 2, we insert $L\left(\alpha^{2^{m}-1}\right)$ into $L_{l}$ and draw the stems of the LLRs in Figure 2(d). Re-execute the code roots recognition steps, it is easy to verify that the element $\alpha^{2^{m}-1}$ is not a root of the code and the case of Figure 1 does not appear in this algorithm. Thus the generator polynomial is as follows:

$$
\begin{align*}
g(x)= & (x-\alpha)\left(x-\alpha^{2}\right)\left(x-\alpha^{4}\right)\left(x-\alpha^{8}\right)\left(x-\alpha^{16}\right)\left(x-\alpha^{32}\right) \\
& \left(x-\alpha^{3}\right)\left(x-\alpha^{6}\right)\left(x-\alpha^{12}\right)\left(x-\alpha^{24}\right)\left(x-\alpha^{48}\right)\left(x-\alpha^{33}\right)  \tag{31}\\
& x^{12}+x^{10}+x^{8}+x^{5}+x^{4}+x^{3}
\end{align*}
$$

## 4. Primitive Polynomial Recognition

In Section 2 and Section 3, the primitive polynomial of the being recognized code is not considered. But in fact, the corresponding primitive polynomial should be given when discussing an extension field $\operatorname{GF}\left(2^{m}\right)$, because there are more than one primitive polynomials in $\operatorname{GF}\left(2^{m}\right)$ and the calculation
rules based on different primitive polynomials are not the same. However, we propose a theorem that a binary cyclic codeword based on a primitive polynomial is also a valid binary cyclic codeword based on another primitive polynomial. According to this, we can choose any one primitive polynomial $p(x)$ randomly and estimate the code length and code roots based on $p(x)$. Then, we can recognize the actual primitive polynomial according to the root properties of the BCH codes.

Theorem 1: A binary cyclic codeword $C_{r}$, which is encoded based on a primitive polynomial $p_{1}(x)$ over $\operatorname{GF}\left(2^{m}\right)$, is also a valid binary cyclic codeword based on another primitive polynomial $p_{2}(x)$ over $\operatorname{GF}\left(2^{m}\right)$ with the same number of code roots.

Proof. The coefficients of a generator polynomial $g(x)$ of a binary cyclic code is in $\mathrm{GF}(2)$ and can be factored into the product of some minimal polynomials over $\mathrm{GF}(2)$ :

$$
\begin{equation*}
g(x)=m_{1}(x) m_{2}(x) \cdots m_{p}(x) \tag{32}
\end{equation*}
$$

Let $\mathrm{GF}_{1}\left(2^{m}\right)$ and $\mathrm{GF}_{2}\left(2^{m}\right)$ be extension fields based on two different primitive polynomials $p_{1}(x)$ and $p_{2}(x)$, respectively, then $\mathrm{GF}_{1}\left(2^{m}\right)$ and $\mathrm{GF}_{2}\left(2^{m}\right)$ have the same structure. Each minimal polynomial $m_{i}(x)(1 \leq i \leq p)$ can be factored in the extension fields $\mathrm{GF}_{1}\left(2^{m}\right)$ and $\mathrm{GF}_{2}\left(2^{m}\right)$ both. We define $\alpha$ and $\beta$ to be the roots of $p_{1}(x)$ and $p_{2}(x)$, respectively. According to Theorem 2.18 in [36], let $e 1$ and $e 2$ be the smallest integers such that $\alpha^{2^{21}}=1$ and $\beta^{2^{c 2}}=1$, respectively, then we have:

$$
\begin{equation*}
m_{i}(x)=\prod_{j=0}^{e l-1}\left(x+\alpha^{2^{j}}\right)=\prod_{j=0}^{e 2-1}\left(x+\beta^{2^{j}}\right) \tag{33}
\end{equation*}
$$

Since a minimal polynomial has only one distinct root, then according to Equation (33), we have $e 1=e 2$, i.e., each minimal polynomial has the same number of conjugate roots, even if it is based on different primitive polynomials. Consequently, a codeword, which is based on a primitive polynomial $p_{1}(x)$, is also a valid codeword based on any other primitive polynomial $p_{2}(x)$, and the number of code roots and error-correcting capabilities are the same. Therefore, when recognizing the parameters of a binary cyclic code, we can just randomly choose a primitive polynomial provisionally. In order to reduce the computational complexity, we recommend choosing the primitive polynomial with the smallest number of terms.

According to the basic character of the BCH codes, a generator polynomial has $2 t$ roots with consecutive degrees (the $2 t$ roots do not form all the code roots, but include all the distinct roots), where $t$ is the correction capability of the codes. In other words, if $\alpha$ is a primitive element in $\operatorname{GF}\left(2^{m}\right)$, the generator polynomial $g(x)$ of a BCH code for correcting $t$ errors has $\alpha, \alpha^{2}, \alpha^{3}, \ldots, \alpha^{2 t}$ as its roots [3]:

$$
\begin{equation*}
g\left(\alpha^{i}\right)=0, \quad i=1,2, \ldots, 2 t \tag{34}
\end{equation*}
$$

After the estimation of code roots based on a randomly chosen primitive polynomial $p(x)$ and the estimated degree $m$, we can calculate the number of roots and the correction capability $t$. Then, we can traverse all the primitive polynomials over $\mathrm{GF}\left(2^{m}\right)$ and get the one that makes the code roots be in accordant with the character of BCH codes as the primitive polynomial of the being recognized code.

As an example, we still consider the $\operatorname{BCH}(63,51)$ code referred in Section 3. The codewords are encoded based on the primitive polynomial $p_{1}(x)=x^{6}+x+1$ and the code roots are $\alpha, \alpha^{2}, \alpha^{4}, \alpha^{8}, \alpha^{16}$, $\alpha^{32}, \alpha^{3}, \alpha^{6}, \alpha^{12}, \alpha^{24}, \alpha^{48}$, and $\alpha^{33}$. The first six ones and the last six ones are two groups of
conjugate roots. Here $\alpha$ is a primitive root in $\operatorname{GF}\left(2^{6}\right)$ based on the primitive polynomial $p_{1}(x)$, i.e., $p_{1}(\alpha)=0$. But in the recognition procedure, we do the calculations over $\operatorname{GF}\left(2^{6}\right)$ with another primitive polynomial $p_{2}(x)=x^{6}+x^{5}+1$ and let the symbol $\beta$ be a root of $p_{2}(x)$. As a result, we can get the code roots $\beta^{15}, \beta^{30}, \beta^{60}, \beta^{57}, \beta^{51}, \beta^{39}, \beta^{31}, \beta^{62}, \beta^{61}, \beta^{59}, \beta^{55}$, and $\beta^{47}$ after the recognition as shown in Figure 3. It is easy to verify that the estimated code roots also form two groups of conjugate roots, thus the error-correction capability $t$ equals two. Now we traverse all the other primitive polynomials and find the one under which the code roots are in accordant with the characters of BCH codes.

Figure 3. Recognizing the $\operatorname{BCH}(63,51)$ codes using a primitive polynomial different from that of the encoder.


## 5. Computational Complexity

In the proposed soft decision recognition algorithm, the most complex computation is the calculation of $p_{i}$. The major computational consumption appears in Equation (23), which includes the $n_{e}^{t h}$ root calculations, productions and tanh function in the real number field. While, the hard decision algorithm only has production and addition calculations over $\operatorname{GF}(2)$. However, our proposed algorithm utilizes the soft decision outputs of the channel, which can provide more information about the reliability decision bits, so require very lower calculation times of $p_{j, i}$ than the hard decision one, which can also reduce the total computational complexity in the recognition procedure.

## 6. Simulations

The simulation results of the proposed blind recognition algorithm are shown in this section. In the simulations, we assume that the propagation channel is a Binary Symmetry Channel (BSC) which is corrupted by an AWGN with the variance $\sigma_{\mathrm{n}}^{2}=N_{0} / 2$. For each configuration, the information symbols in the codes are randomly chosen and the modulation mode is BPSK. All the simulations have the same settings of the observation window with length $L=3,000$ bits and the searching range of the code length is $7-127$.

When applying the algorithm to $\operatorname{BCH}(63,45)$ codes, the simulation results of the code length estimation are shown in Figures 4-6. The signal is corrupted by an AWGN with the $\operatorname{SNR} \mathrm{E}_{\mathrm{s}} / \mathrm{N}_{0}=5 \mathrm{~dB}$.

In Figure 4, we draw the stems of $p_{i}$ on different elements $\alpha^{i}$ taken from $\operatorname{GF}\left(2^{m}\right)$ when the code length and synchronization positions are correct. It is shown in Figure 4 that the values of $p_{i}$ on the code roots are obviously higher than those on the other elements. And we also draw the stems on a fault code length and synchronization position in Figure 5.

Figure 4. Values of $p_{i}$ on correct code length and synchronization positions.


Comparing with Figure 4, the values of $p_{i}$ in Figure 5 is uniform, so the information entropy of $p_{i}$ on correct coding parameters should be lower and the corresponding dispersion entropy function is higher. As shown in Figure 6, we draw the stems of RIDEF on different code length $l$ and coding starting positions $t$ when the start position $t=0$ of the observation window is at the fortieth bit of a codeword. In the figure, the value of $p_{i}$ in the case of $l=63$ and $t=23$ is the highest, thus we consider the parameters $l=63$ and $t=23 k(k \in \mathbb{Z})$ as the estimated code length and synchronization positions. The result is in accordance with the simulation settings.

Figure 5. Values of $p_{i}$ on incorrect code length and synchronization positions.


Figure 6. Code length and synchronization positions estimation of $\mathrm{BCH}(63,45)$ codes.


The performance of the algorithm is affected by the channel quality. In Figure 7, we draw the performance of the proposed algorithm when applied to code length and synchronization positions recognitions for several different binary BCH codes, including the shortened codes. The curves depict the false recognition probabilities (FRP) of the code length and coding starting positions estimations on different SNRs. We also compare the performance of our proposed recognition algorithm with the hard-decision-based RIDERS algorithm proposed in [22-24]. The PFR of our proposed algorithm fall rapidly when SNR increases, and it is much lower than that of the previous hard decision algorithms on each single SNR value.

After the code length and synchronization position estimation, the generator polynomial can be recognized by searching for the code roots according to the steps proposed in Section 3. Figure 8 shows the performance of the proposed generator polynomial recognition algorithm when applied to several different binary BCH codes, which are $\mathrm{BCH}(63,51), \mathrm{BCH}(63,39)$ and $\mathrm{BCH}(30,20)$. The curves show the false recognition probabilities on different noise levels. As $\mathrm{E}_{s} / \mathrm{N}_{0}$ rises, the curves fall rapidly. When $\mathrm{E}_{\mathrm{s}} / \mathrm{N}_{0}$ is above 5 dB , no false recognition occurred during our 200,000 instances of simulation. We also compare our proposed algorithm with the previous hard-decision-based recognition algorithms proposed by [22-24] in the figure. It shows that the recognition performance is improved obviously in soft decision situations. A gap of $1-2 \mathrm{~dB}$ exists between the two groups of curves.

Figure 7. Performances of code length estimations for some binary BCH codes.


Figure 8. Performances of code roots estimations for some binary BCH codes.


## 7. Conclusions

A soft-decision-based blind recognition method for binary BCH codes with BPSK modulations on AWGN channels is proposed aiming at the non-cooperative communications and ACM techniques. The code length estimation and block synchronization are achieved by checking the minimal parity check matrix. After that, the code rate and generator polynomials are reconstructed by searching for the code roots. To the best of our knowledge, this paper is the first publication in literature which introduces an approach for complete-blind recognition of binary BCH codes in soft decision situations. Simulations show that our proposed blind recognition algorithm yields better performance than that of the previous hard-decision-based ones.

## Appendix: Proof of the faultiness of the Hypothesis 1

In this Appendix, we present that the Hypothesis 1 proposed in [22-24] is not always correct. The proof is shown below:

Proof. We can consider a codeword $C$ with length $n$ and the binary pattern of one of the MPCM $H b_{\text {min }}\left(\alpha^{i}\right)$, where $\alpha^{i}\left(0 \leq i \leq 2^{m}-1\right)$ is an element in $\mathbf{G}_{\boldsymbol{m}}$. We let $c(x)$ be the codeword polynomial of $C$. If $\alpha^{i}$ is a root of $c(x)$, then we have $c\left(\alpha^{i}\right)=0$ and $H b_{\text {min }}\left(\alpha^{i}\right) \times C=0$. There are $m$ rows in $H b_{\text {min }}\left(\alpha^{i}\right)$ and we define $\boldsymbol{h}_{j}(1 \leq j \leq m)$ to be the $j^{\text {th }}$ row of $H b_{\text {min }}\left(\alpha^{i}\right)$. Then the equation $H b_{\text {min }}\left(\alpha^{i}\right) \times C=0$ means the productions of all the rows with the codeword $C$ equal to zeros, as shown in Equation (35):

$$
H b_{\min }\left(\alpha^{i}\right) \times C=0 \Leftrightarrow\left\{\begin{array}{c}
\boldsymbol{h}_{1} \times C=0  \tag{35}\\
\boldsymbol{h}_{2} \times C=0 \\
\vdots \\
\boldsymbol{h}_{m} \times C=0
\end{array}\right.
$$

So we can calculate the probability of $\alpha^{i}$ being the root of $c(x)$, i.e., the probability of $H b_{\text {min }}\left(\alpha^{i}\right) \times C=0$ as follows:

$$
\begin{equation*}
P_{r}\left[H b_{\min }\left(\alpha^{i}\right) \times C=0\right]=P_{r}\left(\boldsymbol{h}_{1} \times C=0, \boldsymbol{h}_{2} \times C=0, \ldots, \boldsymbol{h}_{m} \times C=0\right) \tag{36}
\end{equation*}
$$

Let $h_{j l}(1 \leq l \leq n)$ and $C_{l}$ be the $l^{\text {th }}$ element in the vector $\boldsymbol{h}_{j}$ and $C$ and we define the checking indexing set $\mathbf{S}_{j}$ for $\boldsymbol{h}_{j}$ and $C_{l}$ as follows:

$$
\begin{equation*}
\mathbf{S}_{j}=\left\{C_{l} \mid h_{j l}=1\right\} \tag{37}
\end{equation*}
$$

Obviously, when the number of nonzero elements in $\mathbf{S}_{j}$ is even, we have:

$$
\begin{equation*}
\boldsymbol{h}_{j} \times C=0 \tag{38}
\end{equation*}
$$

And when the number of nonzero elements in $\mathbf{S}_{j}$ is odd, we have:

$$
\begin{equation*}
\boldsymbol{h}_{j} \times C=1 \tag{39}
\end{equation*}
$$

When the code length and synchronization positions are not estimated correctly, the restriction among the elements in $C$ does exist. So the elements in the codewords can be considered to appear randomly. In this case, the probabilities of the number of nonzero elements in $\mathbf{S}_{j}$ being odd and even are all about 0.5 . When $H b_{\text {min }}\left(\alpha^{i}\right)$ is full rank, the rows of $H b_{\text {min }}\left(\alpha^{i}\right)$ is linearly independent, so we can calculate Equation (36) as follows:

$$
\begin{equation*}
P_{r}\left[H b_{\min }\left(\alpha^{i}\right) \times C=0\right]=\prod_{j=1}^{m} P_{r}\left(\boldsymbol{h}_{j} \times C=0\right)=(0.5)^{m} \tag{40}
\end{equation*}
$$

But if $H b_{\min }\left(\alpha^{i}\right)$ is not full rank, the calculation of Equation (36) is not correct. We define the maximum linearly independent vector group MI of the row vectors set $\mathbf{H}=\left\{\boldsymbol{h}_{j} \mid 1 \leq j \leq m\right\}$ as follows:
$\mathbf{M I}$ is a subset of $\mathbf{H}$ and meets the following conditions:
(1) The vectors in $\mathbf{M I}$ is linearly independent;
(2) Any vector in $\mathbf{H}$ can be obtained by linear combinations of the vectors in MI.

And it is easy to prove that the number of vectors in MI is the rank of $H b_{\min }\left(\alpha^{i}\right)$.
According to the condition 2 of the definition of MI, if all the vectors in $\left\{\boldsymbol{h}_{j} \mid \boldsymbol{h}_{j} \in \mathbf{M I}\right\}$ make $\boldsymbol{h}_{j} \times C=0$, then also for all the vectors in $\left\{\boldsymbol{h}_{j} \mid \boldsymbol{h}_{j} \in \mathbf{H}\right\}$, we have $\boldsymbol{h}_{j} \times C=0$, so the calculation of Equation (36) should be:

$$
\begin{equation*}
P_{r}\left[H b_{\min }\left(\alpha^{i}\right) \times C=0\right]=\prod_{t=1}^{r a n k}\left(H b_{\text {min }}\left(\alpha^{i}\right)\right) \quad P_{r}\left(\boldsymbol{h}_{j t} \times C=0\right)=(0.5)^{\operatorname{rank}\left(H b_{\min }\left(\alpha^{i}\right)\right)} \tag{41}
\end{equation*}
$$

where $\left\{\boldsymbol{h}_{j t} \mid 1 \leq t \leq \operatorname{rank}\left(H b_{\text {min }}\left(\alpha^{i}\right)\right)\right\}$ are the vectors in MI, i.e., a maximum linearly independent vector group of the rows of $H b_{\text {min }}\left(\alpha^{i}\right)$.

According to Equation (41), Hypothesis 1 is true only if all the $H b_{\text {min }}\left(\alpha^{i}\right)$, where $1 \leq i \leq 2^{m}-1$, have the same rank. But unfortunately, this condition cannot always be met. For example, when considering the $\mathrm{BCH}(63,51)$ codes, we have the following results:

$$
\left\{\begin{array}{c}
\operatorname{rank}\left(H b_{\min }\left(\alpha^{1}\right)\right)=6  \tag{42}\\
\operatorname{rank}\left(H b_{\min }\left(\alpha^{9}\right)\right)=3 \\
\operatorname{rank}\left(H b_{\min }\left(\alpha^{63}\right)\right)=1 \\
\cdots
\end{array}\right.
$$

Therefore, we have:

$$
\left\{\begin{array}{c}
P_{r}\left[H b_{\min }\left(\alpha^{1}\right) \times C=0\right]=\left(\frac{1}{2}\right)^{6}  \tag{43}\\
P_{r}\left[H b_{\min }\left(\alpha^{1}\right) \times C=0\right]=\left(\frac{1}{2}\right)^{3} \\
P_{r}\left[H b_{\min }\left(\alpha^{1}\right) \times C=0\right]=\left(\frac{1}{2}\right)^{1} \\
\ldots
\end{array}\right.
$$

so we find that the Hypothesis $\mathbf{1}$ is not correct.

## References

1. Lin, S.; Costello, D.J. Coding for reliable digital transmission and storage. In Error Control Coding: Fundamentals and Applications, 2nd ed.; Horton, J.M., Riccardi, D.W., Eds.; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2004; pp. 1-23.
2. Wang, X.; Xiao, G.Z. BCH codes and Goppa codes. In Error correcting coding: principles and methods; Li, J., Ed.; Xidian University Press: Xian, China, 2001; pp. 242-317.
3. Moreira, J.C.; Farrell, P.G. BCH Codes. In Essentials of Error-Control Coding; John Wiley \& Sons Ltd.: Chichester, UK, 2006; pp. 97-112.
4. Peterson, W.W. Encoding and error-correction procedures for Bose-Chaudhuri codes. IRE Trans. Inf. Theory 1960, 9, 459-470.
5. Chien, R.T. Cyclic Decoding procedure for the Bose-Chaudhuri-Hocquenghem Codes. IEEE Trans. Inf. Theory 1964, 10, 357-363.
6. Mitola, J.; Maguire, G.Q. Cognitive radio: making software radios more personal. IEEE Personal Commun. 1999, 6, 13-18.
7. Oreay, O.; Ustundag, B. A pattern construction scheme for neural network-based cognitive communication. Entropy 2011, 13, 64-81.
8. Li, M.; Batalama, N.S.; Pados, A.; Melodia, T.; Medley, M.J.; Matyjas, J.D. Cognitive code-division links with blind primary-system identification. IEEE Trans. Wireless Commun. 2011, 11, 3743-3753.
9. Liu, Y.; Tan, X.; Anghuwo, A.A. Joint power and spectrum allocation algorithm in cognitive radio networks. J. Syst. Eng. Electron. 2011, 4, 691-701.
10. Jiang, T.; Grace, D.; Mitchell, P.D. Efficient exploration in reinforcement learning-based cognitive radio spectrum sharing. IET Соттип. 2011, 10, 1309-1317.
11. Marazin, M.; Gautier, R.; Burel, G. Algebraic method for blind recovery of punctured convolutional encoders from an errorneous bitstream. IET Signal Process. 2012, 2, 122-131.
12. Moosavi, R.; Larsson, E.G. A fast scheme for blind identification of channel codes. In Proceedings of 54th GLOBECOM, Houston, TX, USA, 5-9 December 2011; pp. 1-5.
13. Marazin, M.; Gautier, R.; Burel, G. Dual code method for blind identification of convolutional encoder for cognitive radio receiver design. In Proceedings of IEEE Globecom Workshops, Honolulu, HI, USA, 30 November-4 December 2009; pp. 1-6.
14. Goldsmith, A.J.; Chua, S.G. Adaptive coded modulation for fading channels. IEEE Trans. Coттии. 1998, 5, 595-602.
15. Burel, G.; Gautier, R. Blind estimation of encoder and interleaver characteristics in a non cooperative context. Presented at International Conference on Communications, Internet and Information Technology, Scottsdale, AZ, USA, 17-19 November 2003.
16. Choqueuse, V.; Marazin, M.; Collin, L.; Yao, K.C.; Burel, G. Blind reconstruction of linear spacetime block codes: a likelihood-based approach. IEEE Trans. Signal Process. 2010, 3, 1290-1299.
17. Marazin, M.; Gautier, R.; Burel, G. Blind recovery of $\mathrm{k} / \mathrm{n}$ rate convolutional encoders in a noisy environment. EURASIP J. Wireless Commun. Netw. 2011, 168, 1-9.
18. Wang, F.; Huang, Z.; Zhou, Y. A method for blind recognition of convolution code based on Euclidean algorithm. In Proceedings of IEEE WiCom, Shanghai, China, 21-25 September, 2007; pp. 1414-1417.
19. Dignel, J.; Hagenauer, J. Parameter estimation of a convolutional encoder from noisy observations. In Proceedings of IEEE ISIT, Nice, France, 24-29 June 2007; pp. 1776-1780.
20. Marazin, M.; Gautier, R.; Burel, G. Blind recovery of the second convolutional encoder of a turbocode when its systematic outputs are punctured. Military Tech. Acad. Rev. 2009, 2, 213-232.
21. Yongguang, Z. Blind recognition method for the Turbo coding parameters. J. Xidian Univ. 2011, 2, 167-172.
22. Wen, N.; Yang, X. Recognition methods of BCH codes. Electron. Warf. 2010, 6, 30-34.
23. Yang, X.; Wen, N. Recognition method of BCH codes on roots information dispersion entropy and roots statistic. J. Detect. Control. 2010, 3, 69-73.
24. Lv, X.; Huang, Z.; Su, S. Fast recognition method of generator polynomial of BCH codes. J. Xidian Univ. 2011, 6, 187-191.
25. Fossorier, M.; Lin, S. Bit error probability for maximum likelihood decoding of linear block codes and related soft decision decoding methods. IEEE Trans. Inf. Theory. 1998, 11, 3083-3090.
26. Kaneko, T.; Nishijima, T.; Inazumi, H.; Hirasawa, S. An effifient maximum likelihood decoding of linear block codes with algebraic decoder. IEEE Trans. Inf. Theory. 1994, 3, 320-327.
27. Sankaranarayanan, S.; Vasic, B. Iterative decoding of linear block codes: A parity-check orthogonalization approach. IEEE Trans. Inf. Theory 2005, 51, 3347-3353.
28. Jiang, J.; Narayanan, K.R. Iterative soft-input-soft-output decoding of Reed-Solomon codes by adapting the parity check matrix. IEEE Trans. Inf. Theory. 2006, 8, 3746-3756.
29. Ni, L.; Yao, F.; Zhang, L. A rotated quasi-othogonal space-time block code for asynchronous cooperative discovery. Entropy 2012, 14, 654-664.
30. Hagenauer, J.; Offer, E.; Papke, L.; Iterative decoding of binary block and convolutional codes. IEEE Trans. Inf. Theory 1996, 2, 429-445.
31. Imad, R.; Sicot, G.; Houcke, S. Blind frame synchronization for error correcting codes having a sparse parity check matrix. IEEE Trans. Commun. 2009, 6, 1574-1577.
32. Imad, R.; Houcke, S. Theoretical analysis of a MAP based blind frame synchronizer. IEEE Trans. Wireless Commun. 2009, 11, 5472-5476.
33. Imad, R.; Houcke, S.; Jego, C. Blind frame synchronization of product codes based on the adaptation of the parity check matrix. In Proceedings of IEEE ICC2009, Dresden, Germany, 1418 June, 2009; pp. 1574-1577.
34. Imad, R.; Poulliat, C.; Houcke, S.; Gadat, G. Blind frame synchronization of Reed-Solomon codes: Non-binary vs. binary approach. In Proceedings of 2010 IEEE Eleventh International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Marrakech, Morocco, 20-23 June 2010; pp. 1-5.
35. Moreira, J.C.; Farrell, P.G. Cyclic codes. In Essentials of Error-Control Coding; John Wiley \& Sons Ltd.: Chichester, UK, 2006; pp. 81-94.
36. Lin, S.; Costello, D.J. Introduction to algebra. In Error Control Coding: Fundamentals and Applications, 2nd ed.; Horton, J.M., Riccardi, D.W., Eds.; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2004; pp. 25-65.
© 2013 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/).
