Blind Recognition of Binary Primitive BCH Codes Based on Polynomial Roots Statistic of Finite Fields

Xinran Zhang[1, a], Xiaojing Yang[2, b] and Yuehua Dai1[, c]

[1] School of Electronics and Information Engineering, Anhui University, Hefei 230601, China;

[2] Electronic Engineering Institute, Hefei 230037, China.

[a] mxie_007@sina.com, [b] daiyuehua2014@163.com, [c] mxie_007@sina.com

Keywords: finite fields, polynomial roots, BCH code, blind recognition.

Abstract. We have recently proposed a problem about blind recognition of binary primitive BCH Codes. A model was established based on the polynomial roots statistic of finite fields. The roots probabilities of BCH codes were analyzed and the recognition method for binary BCH codes based on polynomial roots statistic of finite fields was proposed. In the paper we showed that the binary primitive BCH Codes could be completely recognized in theoretical analysis and simulation experiment showed the better performance of the recognition method though in high BER.

1. Introduction

BCH codes are cyclic code which can correct multi-random errors, they have strongly error-correcting ability and strictly algebraic structure with convenient constructing and simple coding at the same time, and BCH codes work importantly in coding theory. So BCH codes have gained more extensive application nowadays.

After BCH codes sequences are intercepted, if we want to achieve information obtained, its coding mode and coding parameters must be blind recognized first.

Nowadays research about the field is centrally focused on blind recognition of convolution code and enhancing the coding performance of different channel coding, but the correlative research about the recognition of coding modes and parameters is few. The recognition about convolution code with 1/2 code rate is achieved by the speedily dual syzygy algorithm [1], but the model can't be applied in convolution code recognition with high code rate; The Euclidean Algorithm [2] is also used to recognize the convolution code with low rate, but it doesn't consider the recognition method of wrong codes. In Literature [3] a new data matrix model is proposed to achieve the blind recognition of linear grouping codes, and the method is generalized to recognize the system convolution code, and it also doesn't consider the recognition method of wrong codes. A recognition method of low code rate linear grouping codes is proposed in Literature [4], the distance of weight distribution function is available to code length recognition at the BER , and following the creating matrix is gained by matrix predigested, thus the blind recognition of binary linear grouping codes is achieved, but the method can't be used in other higher code rate grouping codes recognition. All above methods use great matrix operation, and need lower BER, even some methods need no BER. So in the actual needs, at the higher BER, how correctly recognize the BCH codes become a difficult question.

This paper aims at the question of binary primitive BCH codes, and a method based on polynomial roots statistic of finite fields is proposed, its recognition performance is obvious, and needs no great matrix predigested, the available recognition of high code rate BCH codes at higher BER is achieved.

For the blind recognition of BCH codes, namely no knowing the encoding transcendental information, the creating polynomial is estimated. By analyzing and dealing with the codes sequences, the algebra model is

$$m(x)g(x) = c(x) \tag{1}$$

And $m(x)$ means the information sequences, namely $m(x) = m_{k-1}x^{k-1} + m_{k-2}x^{k-2} + \cdots + m_1x + m_0$, $v(x)$ means the encoding information output, namely $c(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0$, $g(x)$ means the creating polynomial, namely $g(x) = g_{n-k-1}x^{n-k-1} + g_{n-k-2}x^{n-k-2} + \cdots + g_1x + g_0$; $c(x)$ is gained by demodulation of recd signal. So the question of blind recognition of BCH codes is how to gain the creating polynomial $g(x)$ only in precondition of $c(x)$.

2. Recognition Method Research

Define 1 A finite field $GF(q)$ and its expanded field $GF(q^m)$ are enacted, $q = 2$, and m is a positive integer. If symbols of codes are from cyclic codes in $GF(q)$ and its roots of creating polynomial $g(x)$ contain hereinafter power continuous δ 1 roots

$$R\supseteq\{a^{m_0}, a^{m_0+1}, \dots, a^{m_0+\delta-2}\} \tag{2}$$

Thus cyclic codes created by $g(x)$ are binary BCH codes, and code length is $n = 2^m - 1$.

Define 2 The polynomial of lowest degree in all the polynomials with a root q and coefficients from $GF(q)$ is the minimal polynomial, marked as $m(x)$.

The character of binary primitive BCH codes creating polynomial is below

1. The roots of creating polynomial are in $GF(2^m)$, and they contain a set of conjugated roots $\{a^{m_0}, a^{m_0+1}, \dots, a^{m_0+\delta-2}\}$ [5] with$m$elements, a is the primitive root.

2. The roots of binary primitive BCH codes creating polynomial have even continuous roots about the primitive root a.

2.1 Recognition and Flow

After intercepting BCH codes sequences, we search m and group the sequences, gain integer distribution of Statistic roots based on polynomial roots character of BCH codes in finite field $GF(2^m)$, following list the almost equiprobable roots in X, and transform X to Y in $GF(2^m)$. Seeking Y which satisfies the character of binary primitive BCH codes creating polynomial and the number of power continuous roots $L0$, the number of Y is L. If we find the true m, we can get information as follows

Supposing in the condition of m, the primitive polynomial is $P(x)$, after polynomial roots statistic in finite field $GF(2^m)$, according to above method, we gain Y, L and $L0$. So code length is $n = 2^m - 1$, information dimension is $k = n - L = 2^m - 1 - L$, error-correcting capability is $t = L_0/2$, and creating polynomial recognition is achieved by using formula $g(x) = LCM(m_0(x), m_1(x), \dots, m_{2t-1}(x))$ ($m_i(x)$ is the min polynomial). Thus finished to recognize code length, information dimension, error-correcting capability and creating polynomial. The flow chart is below.

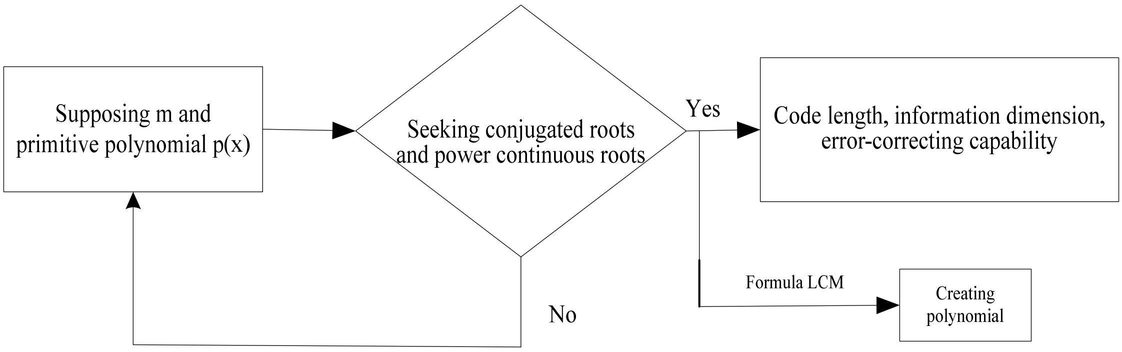
Supposing m and primitive polynomial p(x)
Seeking conjugated roots and power continuous roots
Yes
Code length, information dimension, error-correcting capability
Formula LCM
Creating polynomial
No

Fig. 1 Recognition flow chart of BCH codes

2.2 BER P_e and Code Correct Rate (CCR) P_s

For binary primitive BCH codes which code roots are in $GF(2^m)$, code length $n = 2^m - 1$, the connection between channel BER P_e and CCR P_s is

$$P_s = (1 - P_e)^n \tag{3}$$

So we can see in theory that code roots won't satisfy BCH codes' roots character when code is error. In the condition of random or burst error, the error position is random for every code, so code roots will appear random. If the number of codes is enough, thus the correct codes are more, and the code roots will satisfy the character of primitive BCH codes in every correct code when carrying through roots statistic. For this reason, if we intercept enough data, BCH codes will be recognized in theory.

Proof:

Due to the randomicity of encoding information, if code length is n, let the roots of creating polynomial are in certain muster Y, BCH codes' other roots appear randomly; Meanwhile，the channel bit error positions are random, so error codes' roots are appear random. Supposing the codes correct incident is H_0, the codes error incident is H_1, the existent certain muster incident is D_0, the existent other roots incident is D_1. From probability theory [6], the probability of every code with the certain muster is

$$P_{sc} = P(D_0) = P(D_0 | H_0)P(H_0) + P(D_0 | H_1)P(H_1) \tag{4}$$

The probability of other roots in every code is

$$P_{other} = P(D_1) = P(D_1 | H_0)P(H_0) + P(D_1 | H_1)P(H_1) \tag{5}$$

So in the condition of CCR P_s, we get the roots probabilities of creating polynomial from formulary (4)

$$P_{sc} = 1 \times P_s + \frac{1}{n} \times (1 - P_s) = \frac{1+(n-1)P_s}{n} \tag{6}$$

And other roots probabilities from formulary (5)

$$P_{other} = \frac{1}{n} \times P_s + \frac{1}{n} \times (1 - P_s) = \frac{1}{n} \tag{7}$$

From formulary (6) and (7), we get

$$P_{sc} \gg P_{other}$$

So we can achieve to recognize BCH codes based on the roots statistic.

3. Summary Simulation Experiment and Result Analysis

This paper set BCH codes parameters random in condition of different BER. At certain BER this paper set the gate limit for creating polynomial roots in all roots of BCH codes. The intuitionistic effect chart is given by Monte Carlo experiment simulation.

3.1 Recognition Parameters Setting

BCH codes are random encoding with code length n, and creating 500 codes. The simulation experiment is based on the above recognition method. The code length and BER are chose in table 1 and table 2.

Table 1 Code Length and BER Set (a)

BER SET	Code Length		
	$n = 7$	$n = 15$	$n = 31$
BER	$2.857 \times 10^{-1}, 9 \times 10^{-2}$ $7 \times 10^{-2}, 5 \times 10^{-2}$ $3 \times 10^{-2}, 1 \times 10^{-2}$ $5 \times 10^{-3}, 3 \times 10^{-3}$ $1 \times 10^{-3}, 1 \times 10^{-4}$ 1×10^{-5}	$6.67 \times 10^{-2}, 3.23 \times 10^{-2}$ $1 \times 10^{-2}, 5 \times 10^{-3}$ $3 \times 10^{-3}, 1 \times 10^{-3}$ $1 \times 10^{-4}, 1 \times 10^{-5}$	$6.45 \times 10^{-2}, 3.\times 10^{-2}$ $1 \times 10^{-2}, 5 \times 10^{-3}$ $3 \times 10^{-3}, 1 \times 10^{-3}$ $1 \times 10^{-4}, 1 \times 10^{-5}$

Table 2 Code Length and BER Set (b)

BER SET	Code Length		
	$n = 63$	$n = 127$	$n = 255$
BER	$2 \times 10^{-2}, 1.59 \times 10^{-2}$ $1 \times 10^{-2}, 5 \times 10^{-3}$ $3 \times 10^{-3}, 1 \times 10^{-3}$ $1 \times 10^{-4}, 1 \times 10^{-5}$	$1.57 \times 10^{-2}, 7.9 \times 10^{-3}$ $5 \times 10^{-3}, 3 \times 10^{-3}$ $1 \times 10^{-3}, 1 \times 10^{-4}$ 1×10^{-5}	$7.8 \times 10^{-2}, 5 \times 10^{-3}$ $3 \times 10^{-3}, 1 \times 10^{-3}$ $1 \times 10^{-4}, 1 \times 10^{-5}$

3.2 Gate Limit For Creating Polynomial Roots

From the theory analysis in formulary (8), roots statistic for many codes can achieve BCH codes recognition, but when intercepting a few codes relatively, if recognizing BCH codes, the gate limit must be set.

At the code length of n, code roots probabilities in statistic are $p = (p_1, p_2, \cdots, p_n)$, in this simulation experiment, we set the gate limit is $MX0 = 9/10\max(p)$, there $\max(p)$ means the maximum in p. As we know from the above analysis in formulary (8), a few codes needs a gate limit to recognize the BCH codes.

3.3 Result Analysis

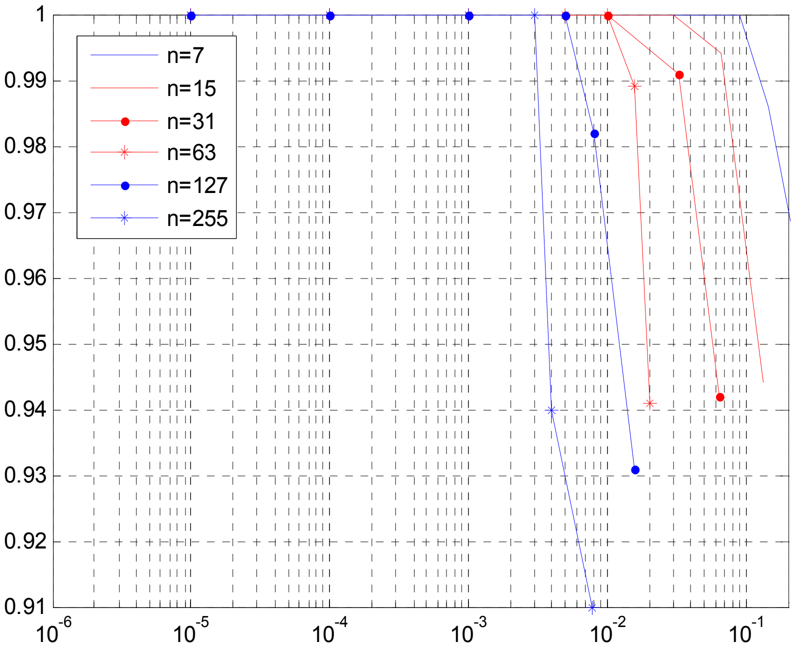

Fig. 2 Recognition probability curve

In figure2, recognition probability changing curve following the BER of binary primitive BCH codes with different code length is provided, six carve express the recognition probability with BCH code length of $n = 7, n = 15, n = 31, n = 63, n = 127, n = 255$. As we analyzing from above theory, BCH codes parameters will be completely recognized by using many codes' code roots. The results of simulation experiments in figure2 show that though in few codes, method in this paper of binary primitive BCH codes recognition is still effectual. As can see from the carve, when $Pe \le 3 \times 10^{-3}$, BCH codes are all recognized with above code length, and when $P_e = 7.8 \times 10^{-3}$, the recognition probability of BCH codes with code length $n = 255$ is 91.4%, code length $n = 127$ is 98.2%, and other BCH codes with different code lengths are 100%.

From the relationship between P_e and P_s, in the definite BER P_e, if code length increases, P_s will fall, the recognition effect will be not good with fewer data; for BCH codes with definite code length, when P_e increases, the recognition effect will be not good also. The analyzing result in this paper gain good proof in figure2.

4. Conclusion

The recognition model is established based on the encoding structure and creating polynomial roots of BCH codes; all the code roots probabilities are analyzed, and the recognition method feasibility with code roots statistic is proved. At the end, the simulation result shows that though in higher BER, BCH codes can be effectually recognized.

References

[1]. ZOU Yan, LU Pei-zhong. A new generalization of key equation [J]. Chinese Journal of Computers, 2006, 29(5):712-718.

[2]. Wang Fenghua, Huang Zhitao. A method of Blind Recognition of Convolution Code Based on Euclidean Algorithm [C]//IEEE Inter Conference on Wireless Com Networking and Mobile Computing, Shanghai, China, 21-25 Sept, 2007:1414-1417.

[3]. XUE Guo-qing, LI Yi1, LIU Wei-ping. Blind Identification of System Convolutional Codes [J]. Information Security and Communications Privacy. 2009, 2.

[4]. ZAN Jun-jun, LI Yan-bin. Blind Recognition of Low Code-rate Binary Linear Block Code [J]. Radio Engineering 2009, 39(1):19.

[5]. Wang Xin-mei. Error-Correcting Codes——theory and method [M]. Xi’an Electronic Science and Technology University Press, 2002, p124.

[6]. Lin Wei-chu. Probability Theory and Data Statistic [M]. Tongji University Press.2008.