Research and Application of Several Error Correction Codes in Communication

Yang Tao *

University of Electronic Science and Technology of China, China, Sichuan Province 610054

* Corresponding Author Email: 2020050906003@std.uestc.edu.cn

Abstract. Error correction code is an important part of contemporary communication engineering, first proposed by Shannon, and has become mature nowadays. This paper analyzes and compares the error correction capabilities of BCH code, cyclic code, and Hamming code using BPSK modulation in AWGN channels. It unfolds in chronological order, introducing the popular codewords of various eras of the last century in turn. Moreover, it introduces the communication process of BPSK modulation and its addition of three codes and compares the bit error rates of the output signals of them when the input signal is a Bernoulli binary sequence. After simulation, it is found that there is a strong correlation between the number of bit errors in BPSK modulation and the code used and its length At low SNR (signal-to-noise ratio),the error rate error of using codewords or not is minimal. Most digital devices exhibit advantages when the SNR exceeds 4 dB. Under the equivalent SNR, the longer the codeword, the lower the error rate, and the best error correction ability of BCH code (31,11,5). This article only discusses the error correction ability of BPSK under modulation, laying a foundation for comparing the error correction ability of higher order PSK modulation and other code words in the future.

Keywords: BPSK modulation, BCH code, cyclic code, Hamming code, SNR(signal-to-noise ratio)

1. Introduction

In the 1940s and 1950s, people entered the electronic information era. "The father of modern informatics" Shannon believed that the two important characteristics of information are effectiveness and reliability. Therefore, improving the effectiveness and reliability of transmitting information has become the goal pursued by all communication workers. In 1948, Shannon first expounded the possibility of achieving reliable communication in noisy channels in his groundbreaking paper "A mathematical theory of communication” and proposed the famous "disturbed channel coding theorem". This epoch-making creative proposal became the "spark" brought by Prometheus in the information field, laying the foundation for the development of error correction codes. Later, Hamming, Hadamard, E.Prange and others designed a series of effective and simple codes based on Shannon's theory . Error correction codes were recognized by more and more communication workers, ushering in a golden era of their development.

From the 1950s to the 1960s, there was a period from the existence of error correction codes to the absence of error correction codes. During this period, the scholars mainly studied various coding algorithms and provided a theoretical basis for linear block codes, whose main achievements include: the sequential decoding of convolutional codes, the compilation of BCH codes and the introduction of the concept of error correction code limits.

The 1960s and 1970s witnessed the most dynamic development of error correction codes Not only have many effective coding and decoding methods been proposed, but attention has been paid to the practical problems of error correction codes, mainly including decoding error probability, invisible error probability, channelization models and so on. During this period, the theory of linear block codes based on finite fields has become mature, such as RS codes.

From the 1970s to the 1980s, the former Soviet scholar V.D. Goppa created the Goppa code. Not only could Goppa codes contain most of the known linear codes at that moment, but it had a good asymptotic property of a certain acyclic code subclass, which can achieve the Shannon limit code mentioned by Shannon in the channel coding theorem. This also proves the correctness of Shannon's theorem.

In the 1990s, Berrou. A. Glavieux and P. Thitmajshima skillfully combined convolutional codes and random interleavers to achieve random coding [1]. So far, as an important means to improve channel reliability, error correction codes have been developed for more than 70 years.

Up to now, error correction codes have formed a mature and effective coding technology, such as Hamming code, Adama code, Reed Muller code, BCH code and RS code, which are widely used in the communication industry. Yufan Wang, Linning Peng et al. used a concatenated code called BCH and RS as codes whose function is to check error for generating keys over a line channel [2]; Shin Jihwan and Ho Kyeong Lee designed concatenated codes using tail biting convolutional codes as internal codes and Hamming codes as external codes. After simulation, the properties of convolutional codes have been significantly improved [3]. Without changing the parity check code bits, LFONSO S M, PEDRO R, JUAN A M et al. proposed two new encoding mechanisms based on Hamming code, SEC-DAED, and SEC-DED-TAED. The former might fix error of one bit and find error of two continuously, and the latter could put right mistake of one bit, discover two-bit as well as detect three-bit misstep continuously [4]. The method proposed by Nandivada Sridevi et al. to expand (8,4) SEC-DED codes to (14,8) SEC-DED-DAEC codes performs neighbor correction for double error detection, reducing the complexity of detection [5]. Minseo Kim et al. proposed a new combination of BCH codes and cyclic redundancy check (CRC) codes. Compared with traditional BCH codes, it improves reliability while greatly saving the required area [6]. Zhong Xiaodong and others proposed an error correction algorithm that combines Hamming codes with quantum keys. This algorithm can change the encoding length for different bit error rates and can also correct random and burst errors in the original key [7].

2. Principle

Error detection is the inspection of noise generated in information from the transmitting end to the receiving end, while error correction is the comparison of initially completely correct data and processed data at the receiving end [8]. Therefore, the function of error correction codes is to detect errors in various channels (in this article, AWGN channels) and restore the original data without errors.

2.1. Modulation and Demodulation of BPSK in AWGN Channels

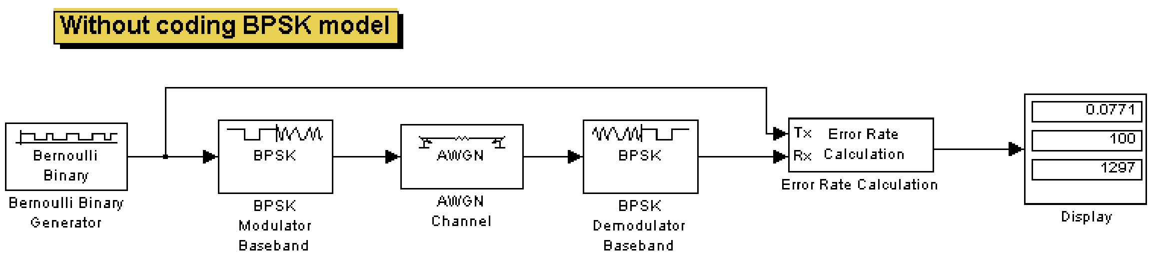


Fig 1. Modulation and Demodulation of BPSK in AWGN Channels

The flowchart shown in Figure 1 clearly shows the communication process involved in BPSK modulation. According to this block diagram, The Bernoulli binary number generator randomly generates binary numbers, obtains modulated signals through a BPSK modulator, passes through a Gaussian channel, and finally obtains binary signals again through a BPSK demodulator. The part responsible for calculating the bit error rate compares the data from the transmit port and the data from the receive port bit by bit, and divides the unequal bits by the total number of bits to obtain the bit error rate/symbol error rate. After the simulation, the error rate will be displayed on the screen, along with a linear image of BER and Eb/No. In terms of modulators, BPSK modulation baseband and BPSK demodulation baseband are used. Simulation is in the channel called AWGN. In the process of simulation, the (Eb/No) in the channel varies from 0 to 10 (dB) to demonstrate the condition of BER.

2.2. Theoretical basiss of three error correction code

2.2.1 BCH code

[9] Matrix BCH code is a special cyclic code that has the ability to correct multiple errors. It can generally be represented by generating polynomial solutions, and its mathematical expression is $g(x)$. Then A cyclic code generated by g (x) is represented by (n, k, t) [10].

2.2.2 Cyclic code

2.2.2.1 Cyclic code coding

[11]Message, generator (coding polynomial), codeword, and received message are represented by m(x)、p(x) and c(x) respectively. These are sequences of functions corresponding to the coefficients of polynomials, where the coefficients are arranged from the lowest to the highest order. Multiplying the message polynomial by the encoding polynomial yields the encoding polynomial $c\ (x) = m\ (x)\, p\ (x)$.

2.2.2.2 Cyclic code coding

Use the generated polynomial of BCH to check whether the data is correct. In other words, use the received code M(x)=C(x)+E(x) divided by G (x), and the number which is remained is E(x)/G(x). If the digit is 0, then the check is exact. Otherwise, the check is incorrect, and error correction is required.

2.2.3 Hamming code

A common method to detect error is to place some extra bits in the message, usually a combination of 1 and 0. The receiver can use the digits on these bits to examine whether the message being delivered is correct and recover the information considered incorrect. Assuming that the length of the detected binary sequence is n bits, if the sequence has the competence to detect and correct errors, it is necessary to add k redundant bits to it to form a (n+k) bit codeword

In order to accurately locate errors and indicate that the code is correct, the newly added detection bit k should meet the following requirements by $2k \geq n + k + 1$. From this relationship, the number of bits k required for detection of different code lengths n can be obtained.

2.3. Process for implementing error correction with three error correction codes

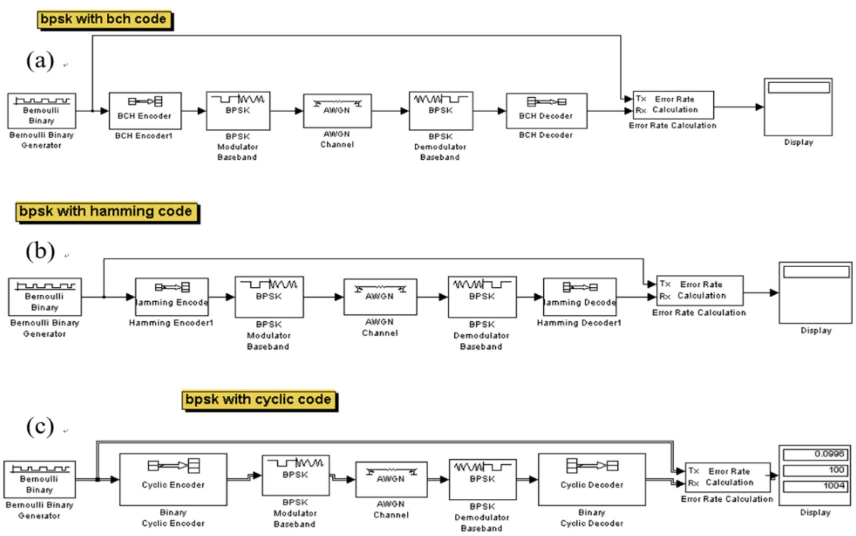
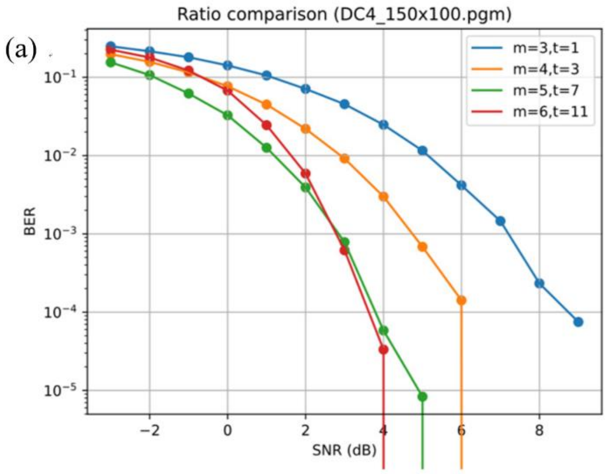


Fig 2. (a)Block diagram of BCH code error correction in AWGN channel under BPSK modulation. (b)Error correction block diagram of Hamming code in AWGN channel under BPSK modulation. (c)Block diagram of cyclic code error correction in AWGN channel under BPSK modulation

By comparing Fig 1 and Fig 2 (a), (b), and (c), it can be seen that the BPSK modulation process of BCH code, Hamming code, and cyclic code is very similar to the uncoded BPSK modulation process, except that the first three add encoders and decoders; According to Fig 2(a), (b) along with(c), the difference in the error correction process between three codes is that they use the corresponding encoder and decoder for their respective codes.

3. Results

3.1. Comparison between variations of BCH code lengths and their error rate compared with uncoded codes



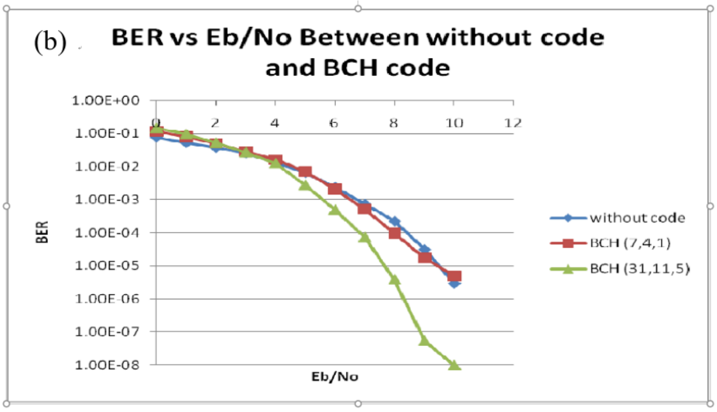


Fig 3. (a)Comparison of error rate of variations for BCH code length (b) Comparison of error rate between uncoded and different lengths of BCH code

As can be seen from Fig 3, under the condition of the small length of code, when it becomes longer, the error rate for the same SNR would be lower. As the SNR gradually increases, the longer the BCH code, the lower the BER, and the better the transmission performance [12].

From Fig 3 (a), it can be seen that BCH (7,5) codes and BCH (11,6) codes have good error correction effects. Before about 2.3 dB, the BER of BCH (7,5) code is better than that of BCH (11,6) code; After 2.3 dB, the BER of the two codes is almost the same. Based on the comprehensive analysis of code length and BER, the BCH (7,5) code has the best coding effect, dropping from 10 ^ (- 1.5) at 0dB to 10 ^ (- 5.1) at 5dB.

As can be seen from Fig 3 (b), when the signal noise is small (less than 2dB), the bit error rate when not coded is slightly lower than that of the two types of coding. Between 2dB and 4dB, the error correction capabilities of these three cases are almost the same. The advantages of BCH (31,11,5) codes are not shown until the bit error rate is greater than 4 dB. A much lower BER than the other two can be observed, decreasing from 1.00E-02 at 4dB to 1.00E-08 at 10dB.

3.2. Comparison between variations of Hamming code lengths and their error rate compared with uncoded codes

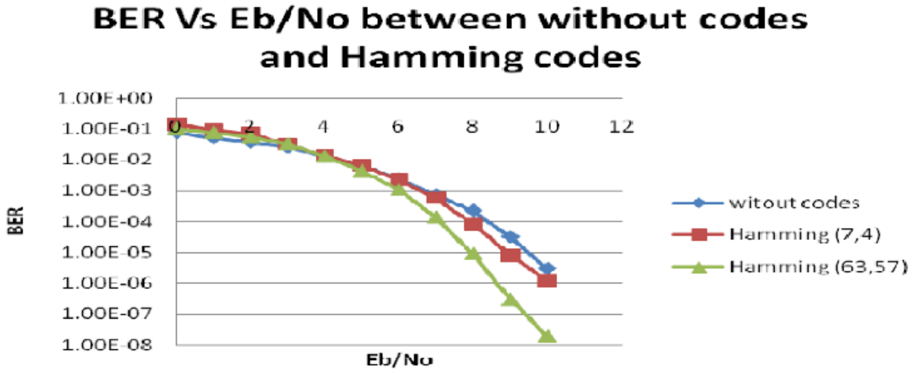


Fig 4. Comparison of error rate between uncoded and different lengths of Hamming code

As can be seen from Fig 4, if the SNR is relatively small, the bit error rate without coding is better than when Hamming code is used. After the SNR surpasses 4dB, hamming code (63,57) begins to exhibit significant coding advantages, with a significant reduction in BER and much smaller than in the case of uncoded or Hamming code (7,4) from 1.00E-02 at 4dB to 1.00E-08 at 10dB.

3.3. Comparison between variations of Cyclic code lengths and their error rate compared with uncoded codes

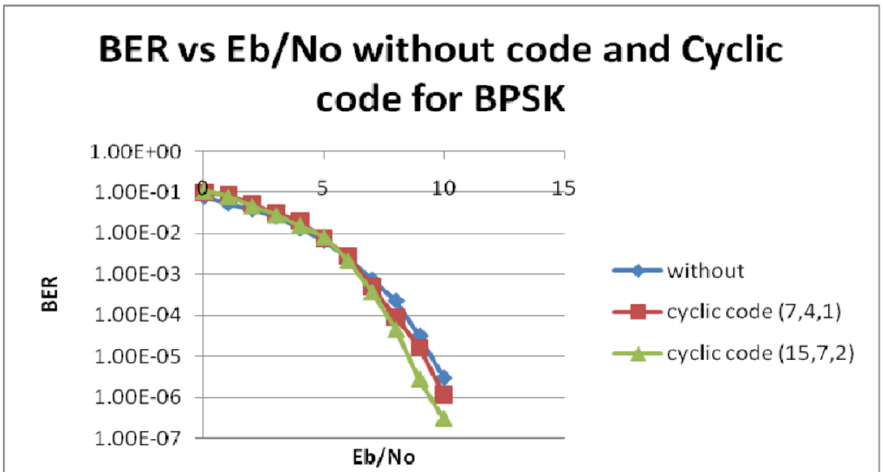


Fig 5. Comparison of error rate between uncoded and different lengths of Cyclic code

Through Fig 5, when the SNR is relatively small (< 5dB), the error rate after modulation without coding is better than that with cyclic code coding. After the SNR outstrips about 7 dB, cyclic code (15,7,2) begin to exhibit coding advantages, but the bit error rate does not differ significantly from that of uncoded or encoded cyclic code (7,4,1); Until the SNR surpasses approximately 9 dB, the cyclic (15,7,2) code shows a significant advantage in error correction ability, decreasing from 1.00E-02 at 5 dB to about 1.00E-7 at 10 dB. Overall, both cyclic (7,4,1) codes and cyclic (15,7,2) codes are good error correction codes. The BER of cyclic (15,7,2) codes is low, However, the redundancy of cyclic (7,4,1) codes is small.

3.4. Comparison of bit error rates of BCH codes,cyclic codes and Hamming codes with lengths of codes varying

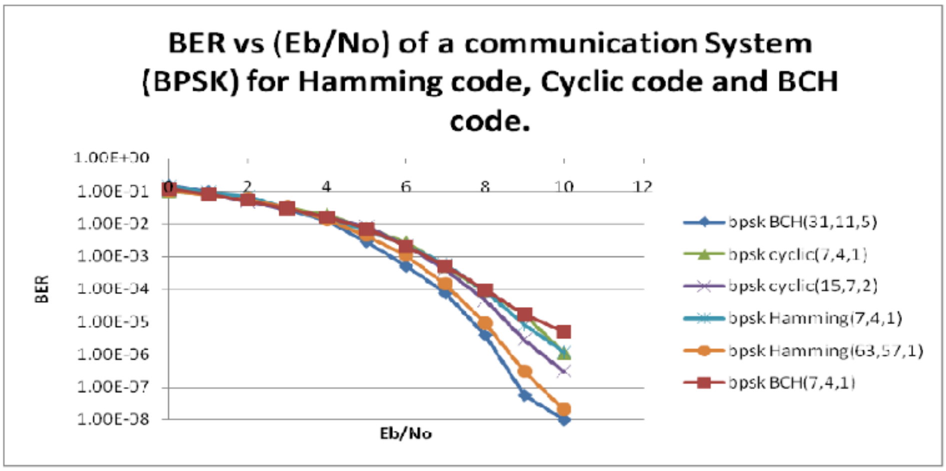


Fig 6. Comparison of bit error rates of BCH codes,cyclic codes and Hamming codes with different code lengths

In Fig 6, when the SNR is less than 4 dB, the error correction capabilities of BCH code, cyclic code, and Hamming code are almost the same. After 4dB, the error rate obtained using BCH code (31,11,5) coding under BPSK modulation is optimal, decreasing from 1.00E-02 at 4dB to 1.00E-8 at 10dB. Generally speaking, when using large redundancy, the error correction effect of BCH codes is better than that of other two codes and could be useful in fixing many faults.

4. Conclusion

The simulation findings demonstrate that the code utilized, and its code length have a significant impact on the bit error rate in BPSK. When the SNR is low, the error rate of using codeword coding or not using codeword coding is very close, with almost no difference. Most codes exhibit advantages only whenever the SNR beyond 4 dB. Under the same SNR, the longer the codeword, the lower the bit error rate generally. The error correcting capability of BCH code is superior to the other two codes when comparing the simulation results of the identical circumstance for the three codes, and the error correction effect of BCH code (31,11,5) is the best[12].

5. Recommendation

This article only explores the impact of error correction codes in the case of BPSK on the error rate of Bernoulli binary signals. In the future, higher order PSK modulation can be expanded, as well as the error correction capabilities of other error correction codes, such as RS code, Turbo code, or concatenated code, in various modulation situations.

References

[1] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," Proceedings of ICC '93 - IEEE International Conference on Communications, Geneva, Switzerland, 1993, pp. 1064-1070 vol.2

[2] Y. Wang, L. Peng, H. Fu, G. Li and A. Hu, "Performance Analysis of Concatenated Error Correction Code in Secret Key Generation System," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 2019, pp. 270-275

[3] S. Jihwan and H. -K. Lee, "Burst Error Correction for Convolutional Code Concatenated with Hamming code with a block interleaver," 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Fukuoka, Japan, 2020, pp. 531-533

[4] Sanchez-Macian, A., Reviriego, P. and Maestro, J.A. (2014) “Hamming Sec-Daed and extended hamming sec-ded-taed codes through selective shortening and bit placement,” IEEE Transactions on Device and Materials Reliability, 14(1), pp. 574–576.

[5] N. Sridevi, K. Jamal and K. Mannem, "Implementation of Error Correction Techniques in Memory Applications," 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2021, pp. 586-595

[6] M. Kim and J. Park, "High Detection Rate BCH Code with CRC Code for Memory Application," 2022 19th International SoC Design Conference (ISOCC), Gangneung-si, Korea, Republic of, 2022, pp. 35-36

[7] X. Zhong and G. Jin, "Application of Hamming Code Based Error Correction Algorithm in Quantum Key Distribution System," 2020 IEEE 3rd International Conference on Electronics Technology (ICET), Chengdu, China, 2020, pp. 857-861

[8] S. Kaur, N. Singh, G. Kaur and J. Singh, "Performance Comparison of BPSK, QPSK and 16-QAM Modulation Schemes in OFDM System using Reed-Solomon Codes," 2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE), Bhubaneswar, India, 2018, pp. 530-533,

[9] C. -D. Lee and Y. -H. Chen, "Algebraic Decoding of Quasi-Reversible BCH Codes Using Band Matrices," in IEEE Transactions on Communications, vol. 69, no. 5, pp. 2800-2811, May 2021

[10] G. Campobello, G. Patane and M. Russo, "Parallel CRC realization," in IEEE Transactions on Computers, vol. 52, no. 10, pp. 1312-1319, Oct. 2003

[11] Y. Jiang, "Analysis of Bit Error Rate Between BCH Code and Convolutional Code in Picture Transmission," 2022 3rd International Conference on Electronic Communication and Artificial Intelligence (IWECAI), Zhuhai, China, 2022, pp. 77-80

[12] S. S. Sarnin, N. F. Nairn and W. N. S. W. Muhamad, "Performance evaluation of phase shift keying modulation technique using BCH code, Cyclic code and Hamming code through AWGN channel model in communication system," The 3rd International Conference on Information Sciences and Interaction Sciences, Chengdu, China, 2010, pp. 60-6