Implementation of Galois Field for Application in Wireless Communication Channels

Dikshita Sarma[1,*], Manash Pratim Sarma[2], Kandarpa Kumar Sarma[3] and Nikos E. Mastorakis[4]

[123] Department of Electronics and Communication Engineering, Gauhati University, Assam

[4] Technical University of Sofia, Sofia, Kilment Ohridski 8, Bulgaria

Abstract. This paper discusses the implementation of Galois Field based codes for application in wireless communication channel. It discusses the use of Galois Fields outlining the basic performance of a digital communication system in terms of BER curves. The work further discusses the performance of these codes in Gaussian and Rayleigh Fading Channels.

Keywords. Coding, Bit Error Rate (BER), Additive White Gaussian Noise (AWGN), Rayleigh Fading Channel, Signal to noise Ratio (SNR), Hamming Code, Bose-Chaudhuri-Hocquenghem (BCH) code, Galois Field.

1 INTRODUCTION

Codes are used for data compression, cryptography, error-correction, and networking. Codes are studied for the purpose of designing efficient and reliable data transmission methods [16]. This typically involves the removal of redundancy and the correction or detection of errors in the transmitted data. In information theory and coding theory with applications in computer science and telecommunication, error detection and correction or error control are techniques that enable reliable delivery of digital data over unreliable communication channels. Many communication channels are subjected to channel noise, and thus errors may be introduced during transmission from the source to a receiver. In digital communications systems, the ultimate function of the physical layer is to as quickly and as accurately as possible transfer data bits in the media. Data can be transmitted over copper cable, optical fibre or free space. Two basic measures of physical performance levels are related to the speed at which data can be transmitted (Data Rate) and data integrity when they arrive at the destination. The primary measure of data integrity is called the Bit Error Ratio, or BER. The bit error ratio can be considered as an approximate estimate of the bit error probability. This estimate is accurate for a long time interval and a high number of bit errors [17]. The remaining part of this paper is systematized in the following way: Section 2 discusses the basic concepts of Wireless Channel Model and its characteristics. Section 3 briefly describes the Galois Field in Hamming Code and Bose-Chaudhuri-Hocquenghem (BCH) code. Section 4 documents the experimental Results. Finally, Section 5 concludes the paper.

.

2 WIRELESS CHANNEL MODEL AND CHARACTERISTICS

Wireless channel is an unguided channel, where the signals not only contain the direct Line of Sight (LOS) waves; but also a number of signals as a result of diffraction, reflection and scattering. This propagation type is termed Multipath, and this results in degradation of the performances of the channel. In the design of communication systems for transmitting information through physical channels, it is convenient to construct mathematical models that reflect the most important characteristics of the transmission medium [2]. schemes in both Gaussian Channel and Rayleigh Fading Channel

2.1. Additive White Gaussian Noise Channel (AWGN)

AWGN is often used as a channel model in which the only impairment to communication is a linear addition of wideband or white noise with a constant spectral density (expressed as watts per hertz of bandwidth) and a Gaussian distribution of amplitude. It does not account for fading, frequency selectivity, interference, non-linearity or dispersion. AWGN is commonly used to simulate background noise of the channel under study. The AWGN channel is represented by a series of outputs

Yi at discrete time event index i. Yi is the sum of the input Xi and noise Zi, where Zi is independent and identically distributed and drawn from a zero-mean normal distribution with variance N (the noise). The Zi are further assumed to not be correlated with the Xi.
Yi = Xi+Zi [1].

2.2 Multi Path Fading Channels (Rayleigh fading channels)

Multipath fading channel is usually modelled as Rayleigh fading channels. Rayleigh fading models assume that the magnitude of a signal that has passed through a communications channel will vary randomly, or fade, according to a Rayleigh distribution-the radial component of the sum of two uncorrelated Gaussian random variables [1].

The channel characteristics are usually modelled as h = α e^jφ , where α is the Rayleigh distributed magnitude and is the phase uniformly distributed in the interval [π; -π]

The BER is an average quantity and not an instantaneous quantity as expressed as BER = Q(√α ² P/σ²)2αe^- α ²/2 dα. The BER is related to the SNR by the expression BER = ½(√SNR=SNR + 2). At high SNR, the expression above reduces to BER = ½ SNR [17].

2.3 Galois Field

Galois fields, named after Evariste Galois, are used in error-control coding, is an algebraic field with a finite number of members. A Galois field that has 2m members is denoted by GF (2m), where m is an integer between 1 and 16. Galois theory helps us understand finite fields. Finite fields have numerous real-life applications in coding theory and combinatorial designs. As a result of applications in a wide variety of areas, finite fields are increasingly important in several areas of mathematics, including linear and abstract algebra, number theory and algebraic geometry, as well as in computer science, statistics, information theory, and engineering [3]. Galois theory originated in the study of symmetric functions the coefficients of a monic polynomial are the elementary symmetric polynomials in the roots. Let K be a field. Given any polynomial f(X) K [X] having distinct roots, the splitting field L of f(X) over K is a finite, normal and separable extension. The essence of Galois theory lies in the association of a group G, known as Galois group, to such a polynomial or more generally, to an extension L/K with the above properties. A main result of Galois Theory establishes a one-to-one correspondence between the subgroups of G and the sub-fields of L containing K. The notion of a solvable group in group theory allows one to determine whether a polynomial is solvable in radicals, depending on whether its Galois group has the property of solvability. In essence, each field extension L/K corresponds to a factor group in a composition series of the Galois group. If a factor group in the composition series is cyclic of order n, and if in the corresponding field extension L/K the field K already contains a primitive nth root of unity, then it is a radical extension and the elements of L can then be expressed using the nth root of some element of K [19]. If all the factor groups in its composition series are cyclic, the Galois group is called solvable, and all of the elements of the corresponding field can be found by repeatedly taking roots, products, and sums of elements from the base field. It is known that a Galois group modulo a prime is isomorphic to a subgroup of the Galois group over the rationals [3].

3 GALOIS FIELD IN HAMMING CODE AND BOSE - CHAUDHURI - HOCQUENGHEM (BCH) CODE IN WIRELESS COMMUNICATION

From the study of abstract algebra, it is known that the most flexible yet the basic system of rules is that of the field. In a field, the operation of addition, subtraction, multiplication and division is performed. To represent each character in a field, a bigger field is needed. In the binary numeral system or base-2 number system, each value are represented with 0 and 1 [25]. To convert a decimal numeral system or base-10 number system into binary system, it is needed to represent a decimal in terms of sums of a 2ⁿ .That is, if x is the said decimal number then we wish to have x = €Na 2ⁿ. The coefficients an is then written in descending order of n and all leading zeros are then omitted. The final result becomes the binary representation of the decimal x. Ultimately, binary system offers an alternative way of representing the elements of a Galois Field. Both the polynomial and binary representation of an element have their own advantages and disadvantages. Since a bit is either 0 or 1, a bit is an element of gf (2). There is also a byte which is equivalent to 8 bits thus is an element of gf (2^8) [3].

There are several types of codes and the major classification is the linear and the non-linear codes. Linear codes may be encoded using the method of linear algebra and polynomial arithmetic. The basic idea lies in breaking information into chunks, appending redundant check bits to each block, these bits being used to detect and correct errors. Each data and the check bits block is called the codeword. A code is linear when each codeword is a linear combination of one or more codewords. This concept is from linear algebra and often the codewords are referred to as vectors for that reason. Again one of the characteristics of some block codes is cyclic nature. That means any cyclic shift of codeword is also a codeword and hence, linear, cyclic, block code codewords can be added to each other and shifted circularly in any way, and the result is a still a codeword. Since the sets of codewords may be considered as a vector space and also may be generated through polynomial division, therefore there are two methods of performing computation-linear algebra and polynomial arithmetic polynomial. In the simplest error detection system, a parity check bits work, say, in a larger field gf (32), by requesting retransmission when one of the

invalid codewords is received. To maximize the chances of guessing the correct codeword, in spite of the errors, there is a need of evenly spacing the codeword and here the concept of Hamming Distance comes to rescue. It measures the minimum number of substitutions required to change one string into the other, or the minimum number of errors that could have transformed one string into the other. In a more general context, the Hamming distance is one of several string metrics for measuring the edit distance between two sequences. A major application is in coding theory, more specifically to block codes, in which the equal-length strings are vectors over a finite field [1].

3.1. HAMMING CODE

The first code developed was hamming code in 1950. The Hamming (7,4) code may be written as a cyclic code over GF(2) with generator 1 + x + x3. In fact, any binary Hamming code of the form Ham (r,2) is equivalent to a cyclic code, and any Hamming code of the form Ham(r,q) with r and q-1 relatively prime is also equivalent to a cyclic code. Given a Hamming code of the form Ham (r,2) with r ≥3, the set of even codewords forms a cyclic [2^r - 1; 2^r - r - 2; 4] -code [24].

It is easy to define Hamming codes for large alphabets of size q. One H matrix with linearly independent columns is needed to be defined. For any word of size q there will be columns who are multiples of each other. So, to get linear independence all non-zero m-tuples with one as a top most non zero element will be chosen as columns. Then two columns will never be linearly dependent because three columns could be linearly dependent with the minimum distance of the code as 3. So, there are (q^m - 1) / (q - 1) non zero columns with one as top most non zero element. Therefore, Hamming code is a [(m-1) / (q- 1); (q^m- 1) / (q- 1) - m] code. B

3.2. BCH CODE OR BOSE-CHAUDHURI-HOCQUENGHEM CYCLIC ERROR-CORRECTING CODES

Cyclic codes are vectors in the field GF (q) and the spectrum given by its inverse fourier transform is over the field GF q^m and are constrained to be zero at certain components. In coding theory, the BCH codes or Bose-Chaudhuri-Hocquenghem-codes form a class of cyclic error-correcting codes that are constructed using polynomials over a finite field also called Galois field. BCH codes were invented in 1959 by French mathematician Alexis Hocquenghem, and independently in 1960 by Raj Bose and D. K. Ray - Chaudhuri and hence the name [4]. One of the key features of BCH codes is that during code design, there is a precise control over the number of symbol errors correctable by the code. In particular, it is possible to design binary BCH codes that can correct multiple bit errors. Another advantage of BCH codes is the ease with which they can be decoded, namely, via an algebraic method known as syndrome decoding. This simplifies the design of the decoder for these codes, using small low-power electronic hardware [4]. BCH codes are used in applications such as satellite communications, compact disc players, DVDs, disk drives, solid-state drives and two dimensional bar codes. For a general BCH code, a finite field GF(q) is fixed, where q is a prime power. Let α be a primitive nth root of unity in GF (q^m), and let m(i) x be the minimal polynomial over GF(q) of α (i) for all i. The generator polynomial of the BCH code is defined as the least common multiple g(x) = lcm (m(c)(x)……m(c)+d-2).

4 EXPERIMENTAL RESULTS

In this section we provide the experimental and the simulation results in order to illustrate the BER performance in AWGN and Rayleigh Channels in

presence of Galois Field. Bit Error Rate (BER) for Hamming Code and BCH code are obtained for different values of SNR ranges and the plots are simulated in MATLAB in presence of Galois field, first in AWGN channel, and then in multipath fading channel like the Rayleigh Fading channel.

The Steps followed for the BCH coding scheme:

- The BCH parameters for a Galois array of GF(2) are set.
- A message is created.
- The error-correction capability is calculated.
- The message is encoded.
- The noisy code is then decoded.
- The message is validated for proper decoding.
- The number of possible errors is increased, and another noisy codeword is generated.
- The new received codeword is decoded.
- The number of corrected errors are examined for determining if the message was properly decoded. Entries of -1 correspond to decoding failures, which occur when the codeword has more errors than can be corrected for the specified pair of message and codeword length.
- From the parameters, the BER is estimated and then plotted for both Gaussian and Rayleigh Fading Channel.

Again for the Hamming Coding Scheme using Galois array, the following steps were followed:

- First the Galois field arrays are created.
- The 4-bit codeword of a (7,4) Hamming code is multiplied by a 47 matrix.
- The information bits are then encoded by multiplying it by the generator matrix.
- The parity-check matrix is used to determine where the error occurred, by multiplying the codeword by it.
- To find the error, the parity-check matrix is looked at

- .From the parameters, the BER is estimated and then plotted for both Gaussian and Rayleigh Fading Channel.

From the Table I, it is seen that as the SNR values ranges from lower to higher, the Bit error rates decreases simultaneously and for the Hamming Coding Scheme, in presence of Galois Field, both in Gaussian and Rayleigh Fading channel, it shows the best result as compared to the other two coding schemes. Here, the BER is calculated at 10 dB, 15 dB and 20 dB and it is observed that the values decreases from 10 dB to 20 dB for all the three coding schemes. When compared, it is found that the Hamming Code in presence of Galois Field shows the best result.

Again, the SNR value is increased from 20 dB to 30 dB and the BER is measured at 20 dB, 25 dB and 30 dB. It is observed that for both Gaussian and Rayleigh Fading Channel, the Hamming Coding Scheme in presence of Galois Field again shows the best result. Here, the BER values decreases simultaneously as the SNR range is increased from 20 dB for both BCH and Hamming Coding Scheme and it is lowest in Hamming Code in presence of Galois Field.

From figure I, it is observed that the plot decreases slowly as the SNR value increases in between the range from 0 dB to 20 dB, in both Gaussian Channel and Rayleigh Fading Channel, thereby showing closeness to values in table I. The Hamming coding schemes in presence of Galois Field shows the best result.

Again, from figure II, the SNR range is increased to 30 dB and it is observed that the curves shows closeness to the values in table II, and the BER is best in case of Hamming Coding Scheme in presence of Galois Field, both in Gaussian Channel and Rayleigh Fading Channel.

Table 1. BER FOR PARITY, BCH AND HAMMING CODING SCHEMES IN GAUSSIAN AND RAYLEIGH FADING CHANNEL

SNR (dB)	**10 dB**	**15 dB**	**20dB**
Even Parity(Gaussian)	0.0348	0.0021	8.9998e-07
Even Parity(Rayleigh)	0.2171	0.1292	0.0612
Odd Parity(Gaussian)	0.0419	0.0022	2.9999e-07
Odd Parity(Rayleigh)	0.2153	0.1229	0.0526
BCH(Gaussian)	0.0022	9.5862e-09	6.1134e-25
BCH(Rayleigh)	0.0302	0.0092	0.0034
Hamming(Gaussian)	1.5004e-05	1.5947e-14	5.7988e-42
Hamming(Rayleigh)	0.0260	0.0094	0.0033

Table 2. BER FOR BCH AND HAMMING CODING SCHEMES IN GAUSSIAN AND RAYLEIGH FADING CHANNEL

SNR (dB)	**20 dB**	**25 dB**	**30dB**
BCH (Gaussian)	6.1134e-25	3.7022e-75	6.5602e-233l
BCH (Rayleigh)	0.0029	0.0010	3.5172e-04
Hamming (Gaussian)	5.792888e-42	1.0495e-127	1.3480e-316
Hamming (Rayleigh)	0.0028	9.0000e-04	2.7568e-04

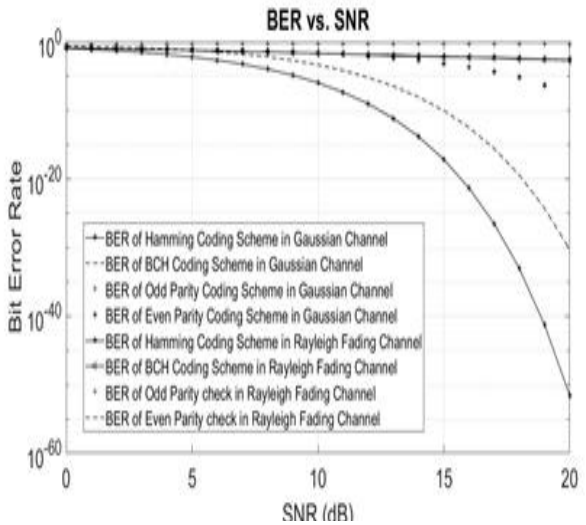

Fig. 1. BER versus SNR plot for Hamming, BCH, Odd Parity check and Even Parity check coding schemes both in Gaussian Channel and Rayleigh Fading Channel Hamming and BCH coding

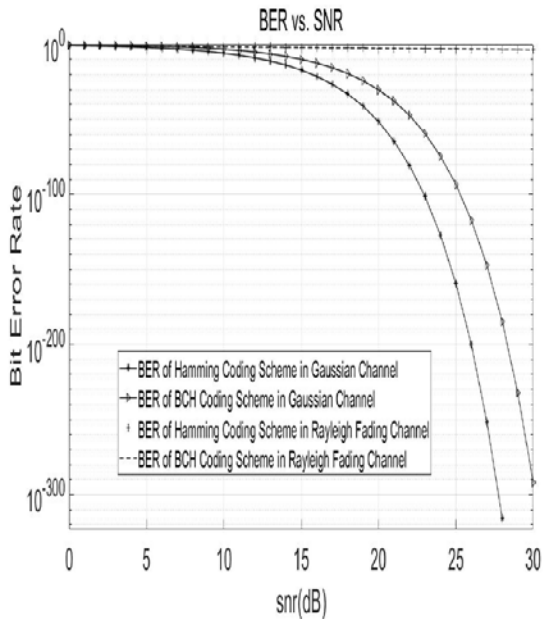

Fig. 2. BER versus SNR plot for Hamming and BCH coding

5 CONCLUSION

Bit error rate (BER) is a powerful parameter in wireless communication systems which provides a measurable and useful indication of the performance of the system that can be directly related to its operational performance. If the BER rises too high then the system performance will noticeably degrade. If it is within limits then the system will operate satisfactorily. Here, we simulate the Bit-error-rate performance of parity, BCH and Hamming coding schemes in MATLAB, first in Gaussian Channel and it can be concluded that in presence of Galois Field, the Hamming Code shows the best result in the various ranges of SNR. The plots are simulated. The error correction capability and the number of correctable errors are also measured. The same is measured by passing it through a Rayleigh Fading Channel, which is a multipath fading Channel. For the different SNR values, the parameter values are different. But for all cases, it can be concluded that the Bit Error Rate slowly decreases from high to low and thus it is suitable even in presence of Galois Field. The Hamming Code shows the best result in presence of Galois Field.

References

1. A. S. Babu, K. V. S. Rao " Evaluation of BER for AWGN, Rayleigh and Rician Fading Channels under Various Modulation Schemes ", International Journal of Computer Applications, no. 9, vol. 26, pp. 0975 8887, 2011.
2. K. Bhargava, Q. Yang and D. J. Peterson, " Coding Theory and its Applications in Communication Systems ", Defence Science Journal, vol. 43, no. 1, pp. 59 - 69, 1993.
3. V. M. Zakharov, B. F. Eminov, S. V. Shalagin, " Representation of Markov's chains functions over finite field based on stochastic matrix lumpability ", 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), IEEE, 978-1-5090-1322-7/ 16/ 31.00, 2016.
4. F. R. Lone, A. Puri and S. Kumar " Performance Comparison of Reed Solomon Code and BCH Code over Rayleigh Fading Channel ", International Journal of Computer Applications, vol. 71, no. 20, pp. 0975 8887, 2013.
5. S. Das, T. S. Sarkar, B. Chakraborty and H. S. Dutta, " A Simple Approach to Design a Binary Coded Absolute Shaft Encoder ", IEEE Sensors Journal, vol. 16, no. 8, pp. 2300 - 2305, 2016.
6. J. D. Gibson, T. R. Fischer, and B. Koo, " Preposterior Analysis for Differential Encoder Design ", IEEE Transaction on Information Theory,

vol. IT-32, no. 3, pp. 375 - 382, 1986.

7. E. Hoekstra, M. Shaaban, R. Czernikowski, and S. Dianat, " Design and Implementation of a DSP based MPEG-1 Audio Encoder ", IEEE Transactions on Consumer Electronics, vol. 45, no. 1, pp. 31 - 35, 1999.
8. H. Kim, S. W. Heo , " Non-systematic RS Encoder Design for a Parity Replacer of ATSC-M/H System ", IEEE Transactions on
9. Consumer Electronics, vol. 56, no. 3, pp. 1270 -1274, 2010.
10. Y. Zhang, L. Ping, and Z. Zhang, " Low Cost Pre-Coder Design for MIMO AF Two-Way Relay Channel ", IEEE Signal Processing Letters, vol. 22, no. 9, pp. 1369 - 1372, 2015.
11. C. Yu, Y.S. Su, " Two - Mode Reed-Solomon Decoder Using A Simplfied Step-by-Step Algorithm ", IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 62, no. 11, pp.1093 - 1097, 2015.
12. D. Chen, P. Chen, Y. Fang , IEEE , " Low-complexity High performance Low-Density Parity-Check Encoder Design for China Digital Radio Standard " ,vol. 5, pp. 20880 - 20886, 2017.
13. C. Zhao, B. T. Wysocki, C. D. Thiem, N. R. McDonald, J. Li, L. Liu, and Y. Yi, " Energy Efficient Spiking Temporal Encoder Design for Neuromorphic Computing Systems ", IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 4, pp. 265 - 276, 2016.
14. M. Zhang, L. Cai, X. Yang, H. Cui, and C. Feng, " Design and Simulation of Turbo Encoder in Quantum-Dot Cellular Automata " , IEEE Transactions on Nanotechnology, vol. 14, no. 5, pp. 820-828, 2015.
15. S. Zhang, F. Yaman, and T. Wanj , " Flexible Transponder Design Aided by Agile Binary Bit Encoder ",Opt. Commun. Netw., vol. 5, no. 7, pp. 722-729, 2013.
16. A. Biasizzo, F. Novak, P. Korosec, " A Multi-Alphabet Arithmetic Coding Hardware Implementation for Small FPGA Devices " ,Journal of Electrical Engineering, vol. 64, no.1, pp. 722 - 729, 2013.
17. B. A. Forouzan, " Data Communications and Networking ", Fifth Edition, McGraw Hill Education (India) Private Limited, 2013.
18. T. S. Rappaport " Wireless communications", Second Edition, Prentice Hall, 2013.
19. S. Haykin, " Digital Communication Systems ", John Wiley and Sons, Inc., 2013.
20. R. B. Wells, " Applied Coding And Information Theory For Engineers" Dorling Kindersley Pvt. Ltd., 2013.
21. V. K. Bhargava, Q. Y. and D. J. Peterson, " Coding Theory and its Applications in Communication Systems", Defence Science Journal, vol. 43, no. 1, pp. 59 - 69, 1993.
22. Lankesh and K .C. Narasimhamurthy, " Hardware Implementation of Single Bit Error Correction and Double Bit Error Detection through Selective Bit Placement for Memory ", International Journal of Computer Applications, pp. 0975 - 8887, 2015.
23. C. K. Ngai, R. W. Yeung and Z. Zhang, " Network Generalized Hamming Weight ", IEEE Transactions on Information Theory, vol. 57, no. 2, pp. 1136 - 1143.
24. Q. L. Rao and Chun He, " A new 2-D parity checking architecture for radiation-hardened by design SRAM ", Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia), pp. 360 - 363, 2009.
25. J. Park and I. Kim, , " Construction of parity - check concatenated polar codes based on minimum Hamming

weight codewords ", H.-Y. Song Electronics Letters, vol. 53, no. 14, pp. 924 - 926, 2017.

26. S. Lin and D. J. Costello, " Error Control Coding ", IEEE Transactions on Information Theory, vol.57, no. 2, pp. 1136 – 1143, 2004.