UNIVERSITY OF PUERTO RICO
MAYAGÜEZ CAMPUS

COMPUTER SCIENCE AND ENGINEERING
DEPARTMENT

Computer Networks

CIIC – 4070

Report 2:
Error Correction Codes and Error Detection Codes

Raúl A. Ortiz Rivera ID: 802-18-7733

Professor: Kejie Lu

March 11, 2023

Table of Contents

List of Tables

List of figures

Introduction

In this report on Error Correction Codes and Error Detection Codes different techniques will be investigated to understand how to correct and detect errors in blocks of data received from the network. In addition, the way in which the data is encoded and decoded will be studied. This report will contain knowledge acquired in the bases of correction and detection of errors such as the definition of codeword, complete code, hamming distance techniques and capability of complete code. The techniques of error correction code will be practiced in depth demonstrating how to encode sequences of bits, demonstrating diagrams of how the data is encoded in techniques such as LDPC code and Polar Code. Error detection methods will be approved using procedures such as CRC with a general polynomial provided to encode the data. Also, how the CRC is used from low level areas such as hardware, explaining step by step how the data is passed through a process of mathematical calculations to ensure that the evaluated data is equal to the provided by the sender. The process of coding and decoding using CRC will be demonstrated by diagram. After applying the processes described above, IEEE 802.11 standards will be provided for the polynomials used in CRC error detection and how LDPC, Polar Code and Distributed CRC techniques are used in 5G NR technology.

The Basics

1. Valid Codeword: A valid codeword refers to a sequence of bits which have been successfully transmitted to the network. It is commonly used for error detection and generation of corrections in invalid blocks. There is an inequity that can help us detect blocks of bits with valid patterns and errors patterns, the equation is as follows:

   $$r > 0, 2^m < 2^n = 2^m * 2^r$$

   Where $\boldsymbol{r}$ is the number of redundant blocks, $\boldsymbol{m}$ is the number of bits in each input and $\boldsymbol{n}$ is the number of bits in each output.

2. Complete Code (Codebook): The codebook is defined as a list of valid codewords in a coding scheme. The number of valid codewords is calculated with 2^m.
3. The Hamming distance between two codeworks is the number of different bits (*d*).
4. The Hamming distance of a complete code is defined as the minimal distance between a pair of codewords.
5. The capability to correct errors, the complete code distance must be greater than $\boldsymbol{2k}$. The equation is as follows:

   $$d \geq 2k + 1 \; where \; \boldsymbol{d} \; is \; the \; hamming \; distance \; and \; \boldsymbol{k} \; length \; of \; the \; codeword$$

6. The capability to detect errors, the complete code distance must be greater than $\boldsymbol{k}$. The equation is as follows:

   $$d \geq k + 1 \; where \; \boldsymbol{d} \; is \; the \; hamming \; distance \; and \; \boldsymbol{k} \; length \; of \; the \; codeword$$

Error Correction Code

1. Using Hamming coding to encode bit stream: 10011010010

- To encode the above bit stream we need to select the checking bits. In this case x_1, x_2, x_4 *and* x_8 were used since they go to the power of 2.
- The table below demonstrates the binary values and the final encode value:

Index	b_3	b_2	b_1	b_0	value
1	0	0	0	1	$x_1 = 0$
2	0	0	1	0	$x_2 = 0$
3	0	0	1	1	$x_3 = 1$
4	0	1	0	0	$x_4 = 0$
5	0	1	0	1	$x_5 = 0$
6	0	1	1	0	$x_6 = 0$
7	0	1	1	1	$x_7 = 1$
8	1	0	0	0	$x_8 = 1$
9	1	0	0	1	$x_9 = 1$
10	1	0	1	0	$x_{10} = 0$
11	1	0	1	1	$x_{11} = 1$
12	1	1	0	0	$x_{12} = 0$
13	1	1	0	1	$x_{13} = 0$
14	1	1	1	0	$x_{14} = 1$
15	1	1	1	1	$x_{15} = 0$

Table 1.1 Table to find the encode bit stream.

- To find the x_1 First we get the values 1 that are part of $2^0 = b_0$, Then we add it up and the result should be even. Below shown in the equation:

$$x_1 + x_3 + x_5 + x_7 + x_9 + x_{11} + x_{13} + x_{15}$$

$$x_1 + 1 + 0 + 1 + 1 + 1 + 0 + 0 \ to\ be\ even\ x_1\ must\ be\ 0.$$

- To find the x_2 First we get the values 1 that are part of $2^1 = b_1$, Then we add it up and the result should be even. Below shown in the equation:

$$x_2 + x_3 + x_6 + x_7 + x_{10} + x_{11} + x_{14} + x_{15}$$

$$x_2 + 1 + 0 + 1 + 0 + 1 + 1 + 0 \ to\ be\ even\ x_2\ must\ be\ 0.$$

- To find the x_4 First we get the values 1 that are part of $2^2 = b_2$, Then we add it up and the result should be even. Below shown in the equation:

$$x_4 + x_5 + x_6 + x_7 + x_{12} + x_{13} + x_{14} + x_{15}$$

$$x_4 + 0 + 0 + 1 + 0 + 0 + 1 + 0 \ to\ be\ even\ x_4\ must\ be\ 0.$$

- To find the x_8 First we get the values 1 that are part of $2^3 = b_3$, Then we add it up and the result should be even. Below shown in the equation:

$$x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15}$$

$$x_4 + 1 + 0 + 1 + 0 + 0 + 1 + 0 \ to\ be\ even\ x_4\ must\ be\ 1.$$

- The Encode of the Bit Stream 10011010010 is **<u>001000111010010</u>**.

2. LDPC Code

- The low-density parity check-code is a linear error correcting code created by Robert Gallager in 1963. The main use is to use it as a method to convey a message through a noisy channel. This system essentially used matrices to encode and decode messages. The sparsity of the matrices allows them to be efficiently encoded and decoded to the point of approaching the Shannon Limit.
- The encode of the LDPC method is basically to multiply the message block with a matrix to produce an equation called parity-check equation. Parity bits are bits added to the original message causing the result to end up encoded.
- Diagram of how the basic process for encoding in an LDPC system works:

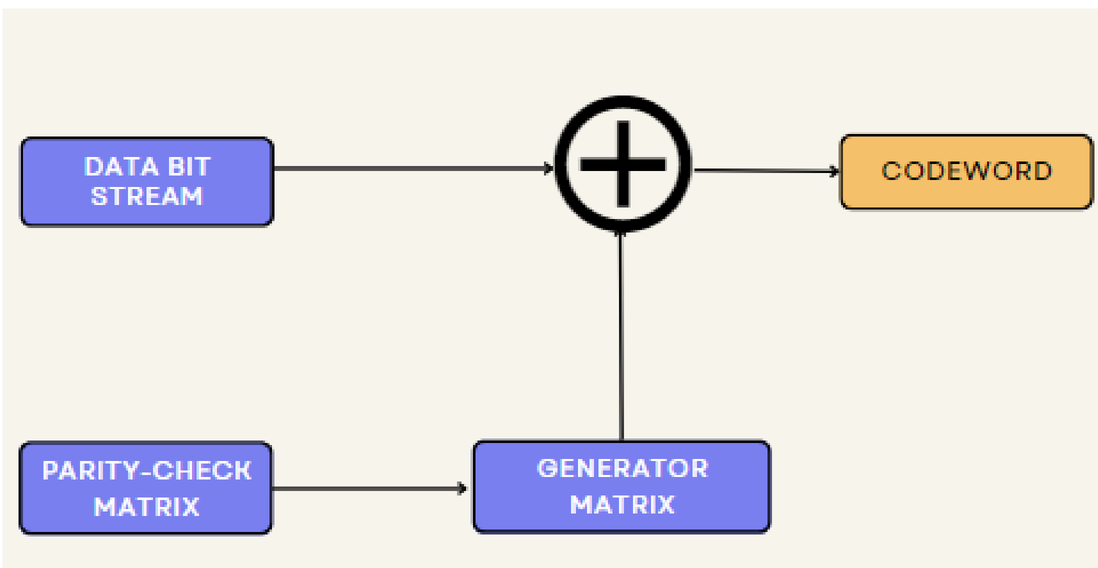

Figure 1.1 LDPC Encoder Block Diagram

3. Polar Code

- Erdal Arikan's model proposed in 2009 states that the polar codes are other linear block correcting code to be able to transmit messages with the least amount of noise possible. This type of encoding uses recursion and handling block sizes that are asymptotically large, is usually efficient and meets its objective. These blocks are divided into good-quality and poor-quality blocks using recursive algorithms. In the end the method sends the data through the channels with good quality while sending the parity bits to those with less quality
- One problem with this system is that with block sizes used in industry, the performance of the successive cancellation is poor and therefore does not usually beat other methods such as LDPC.
- Diagram of how the basic process for encoding in an LDPC system works:

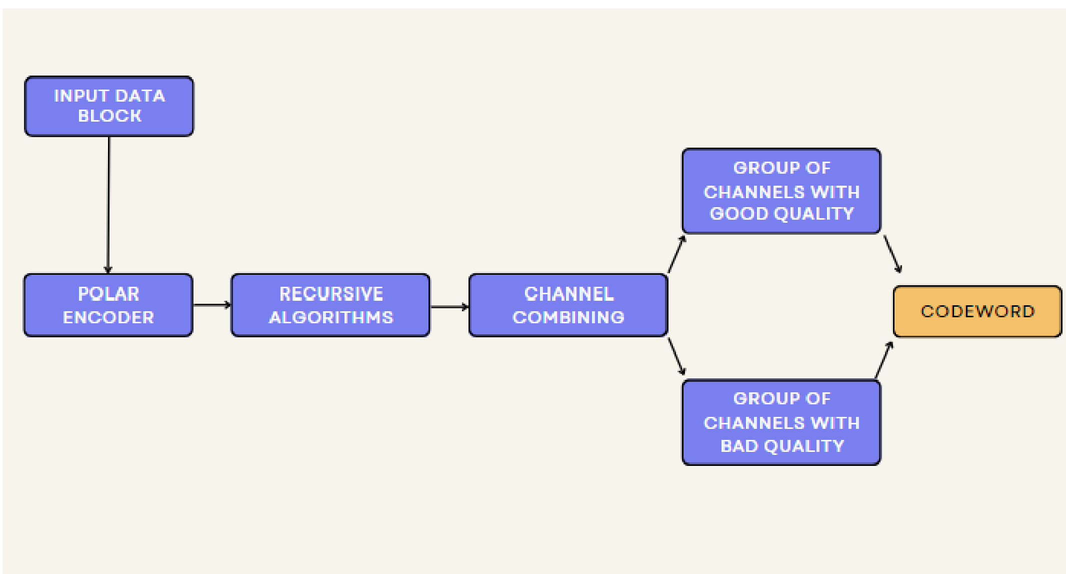

Figure 1.2 Polar Encoder Block Diagram

Error Detection Code

1. Use of CRC (Cyclic Redundant Code) with general polynomial $x^4 + x^3 + 1$ to encode 111011011:

- First, we must find our generator with the polynomial $x^4 + x^3 + 1$ as shown below:

$$x^4 + x^3 + 1 = 11001 \; binary \; sequence$$

$$first \; 1 \; from \; left \; to \; right \; is \; x^4, second \; 1 \; from \; left \; to \; right \; is \; x^3,$$

$$third \; 0 \; from \; left \; to \; right \; is \; x^2, four \; 0 \; from \; left \; to \; right \; is \; x^1,$$

$$final \; 1 \; from \; left \; to \; right \; is \; x^0.$$

- Then you need to apply the division method to obtain the residue remember that this solution uses the exclusive or (XOR) "$\oplus$":

```
         101110111
11001 | 1110110110000
      ⊕ 11001
          10010
        ⊕ 11001
           10111
         ⊕ 11001
            11101
          ⊕ 11001
              10000
            ⊕ 11001
               10010
             ⊕ 11001
                10110
              ⊕ 11001
                  1111
```

- If we want to know what the final frame is, we only must add the residue to the end of the original frame.

- Performing the division by the CRC method, a residue of 1111 was obtained. The encode to the frame 111011011 is **1110110111111.**

2. CRC is performed by hardware:

    - The Cyclic Redundancy Check (CRC) can be extended to the hardware directly. One of the uses is to find irregularities when comparing CRC codes. The process starts by preparing the data, this is usually done by adding zeros to the end of the data stream. This process is necessary since we know that to calculate the CRC, we need to divide the blocks correctly. After the data has been prepared, we move on to the part of the circuits where through the shift register (integrated circuit capable of storing bits and presenting them in their respective pins) and a logic circuit for polynomials. The shift register and the circuit for polynomials are responsible for performing bit-by-bit operations with XOR (exclusive or) between the data that was supplied. These calculations end up delivering the residue of the data that was divided by the logic circuit of polynomials to the shift register. This residue that is kept in the shift register is the CRC code. In the end, the residue is added to the end of the bit stream stored in the hardware. This temporal stream bit is compared to the one received in the data. If the code calculated with the polynomial division circuit is not equal to the CRC supplied by the received data, the block contains an error in the data. If they end up being equal, the data block is error-free and continues with the next block.

- Diagram to explain the encoding process:

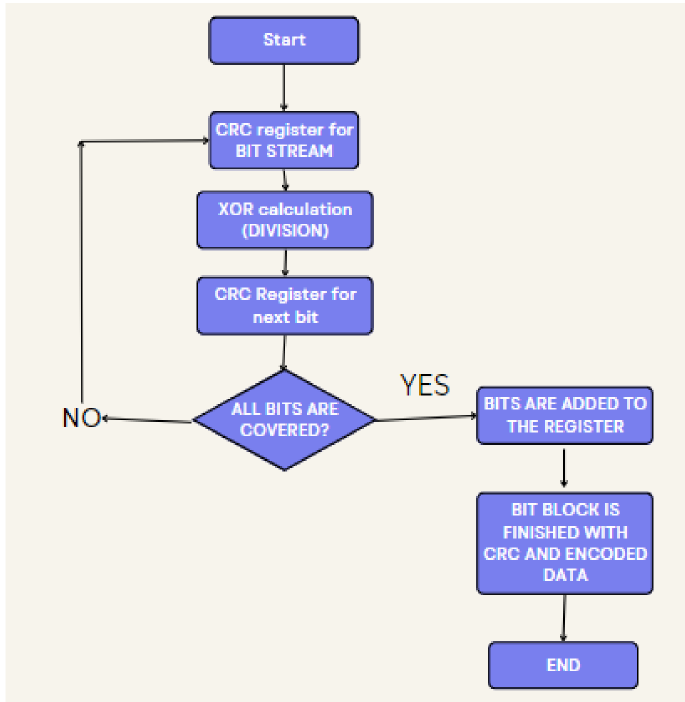

Figure 2.1 Diagram of Encoding with CRC

- Diagram to explain the decoding process:

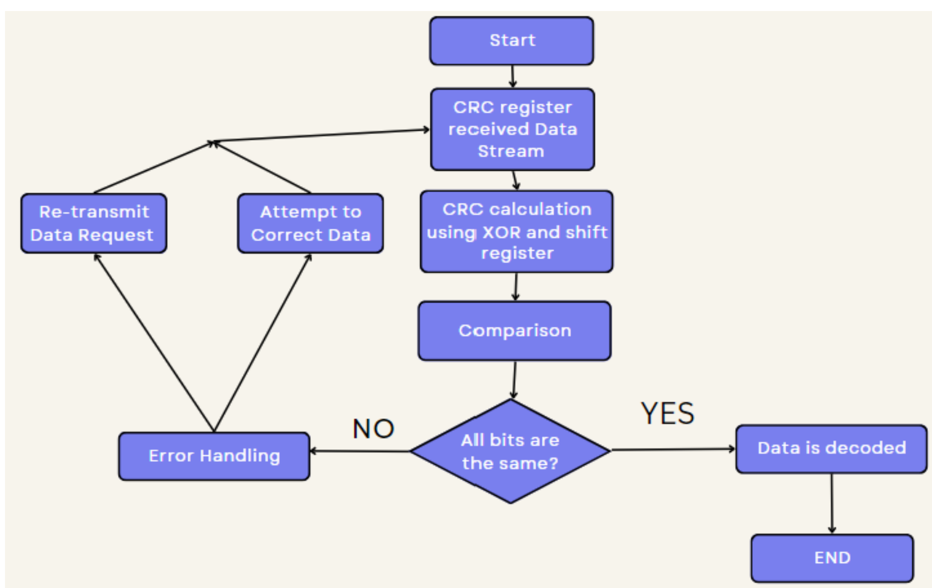

Figure 2.2 Diagram of Decoding with CRC

Codes In Standards

1. The IEEE 802.11 has established several requirements for the CRC error detection. The standards are as follows:

    - The polynomial used for CRC error detection (CH9) is:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

    - The polynomial used for CRC error detection (CH15) is:

$$x^{16} + x^{12} + x^{5} + 1$$

2. 5G NR Standard:

    - LDPC code uses in 5G NR standard: These codes are designed to allow high throughput, a variable code rate and duration, hybrid automatic repeat requests, as well as effective error correcting. Partial adaptation to IEEE standards has been observed. Although they have many references to existing models, it also has unique methods such as the base graph and circular-shift values, as well as the support of rate matching and IR-HARQ.
    - Polar code uses in 5G NR Standard: Control coding technique, is made to work effectively with low block lengths while addressing a successive cancellation decoding delay problem. Its main focus is to have a good complexity-performance. With this model, decoding latency can be reduced due to distributed CRC.

- Use of Distributed CRC: Error detection and correction technique used in communication systems, particularly in the polar codes used in the 5G standard. The bits of information are distributed among them instead of being added at the end. Early error detection reduces decoding time and latency. So in summary the Distributed CRC is used to reduce decoding time and latency.

Conclusion

After making the report of Error Correction Codes and Error Detection Codes I was able to learn the methods to detect and correct Code errors in blocks of data received from the network. I started by learning the basics, understanding what codewords refer to, which are blocks of bits that have been sent correctly through the network. Use the hamming code (different numbers of bits) to encode the 10011010010 stream bit. A table was created where bits were assigned to corroborate the stream of bits obtaining a 001000111010010 encoding. All this was explained step by step and demonstrated. Then, using different sources of information, diagrams were created of how the data is encoded using Low-density Parity Check-code (Figure 1.1) and Polar Code (Figure 1.2). The next phase was to use CRC (Cyclic Redundancy Check) to encode the next block 111011011 with the general polynomial $x^4 + x^3 + 1$. First a generator was found which in this case was 11001, then the CRC division was performed using XOR to obtain the residue. This residue was our CRC which is placed at the end (on the right side) to check if the data was transmitted correctly. In this case the data with the CRC code was 1110110111111. Then in this phase it was explained how the CRC works from the hardware and two diagrams were created of how the coding process (Figure 2.1) and the decoding process (Figure 2.2) are explained. The final part of the report is a compendium of the current IEEE standards for CRC error detection and how the LDPC, Polar Code and Distributed CRC processes are useful for 5G technology and have helped with latency and error detection time issues.

References

A. S. Sing, D. J. says: H. says: and A. S. S. says: “Hamming code with solved problems,” *Electrically4U*, 12-Oct-2022. [Online]. Available: https://www.electrically4u.com/hamming-code-with-a-solved-problem/. [Accessed: 11-Mar-2023].

Author links open overlay panelXiguang Dong a, a, b, c, AbstractOne byte of CRC (Cyclic Redundancy Checks) code is calculated in the general table lookup method each time, S. Wu, A. Monemi, S. Wu, P. Cotret, J. Seo, Y. Huo, J. Mitra, S. Maheshwari, and V. Semerenko, “CRC algorithm for embedded system based on table lookup method,” *Microprocessors and Microsystems*, 22-Feb-2020. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S014193312030096X. [Accessed: 11-Mar-2023].

B. Eater, “Hardware build: CRC calculation,” *YouTube*, 02-Jun-2019. [Online]. Available: https://www.youtube.com/watch?v=sNkERQlK8j8. [Accessed: 11-Mar-2023].

“Cyclic codes,” *Introduction to the Theory of Error-Correcting Codes*, pp. 67–83, 2011.

“Cyclic redundancy check,” *Wikipedia*, 07-Mar-2023. [Online]. Available: https://en.wikipedia.org/wiki/Cyclic_redundancy_check#:~:text=A%20cyclic%20redundancy%20check%20(CRC,polynomial%20division%20of%20their%20contents. [Accessed: 11-Mar-2023].

E. Arikan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

E. Dupraz, F. Leduc-Primeau, and F. Gagnon, “Low-latency LDPC decoding achieved by code and Architecture Co-Design,” *2018 IEEE 10th International Symposium on Turbo Codes & Iterative Information Processing (ISTC)*, 2018.

“Flowchart depicting implementation of R-S with CRC and R-S with cyclic ...” [Online]. Available: https://www.researchgate.net/figure/Flowchart-Depicting-Implementation-of-R-S-with-CRC-and-R-S-with-Cyclic-Codes-for-Randomly_fig7_4290093. [Accessed: 11-Mar-2023].

“Free design tool: Presentations, video, social media | CANVA.” [Online]. Available: https://www.canva.com/. [Accessed: 11-Mar-2023].

“Hamming code,” *Wikipedia*, 05-Mar-2023. [Online]. Available: https://en.wikipedia.org/wiki/Hamming_code. [Accessed: 11-Mar-2023].

IEEE, *Information Technology -- Telecommunications and information exchange between systems -- local and metropolitan area networks -- specific requirements: Part 11:*

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. New York, NY: Institute of Electrical and Electronics Engineers, 1999.

J. H. Bae, A. Abotabl, H.-P. Lin, K.-B. Song, and J. Lee, “An overview of channel coding for 5G NR Cellular Communications,” *APSIPA Transactions on Signal and Information Processing,* vol. 8, no. 1, 2019.

K. Lu, *YouTube*. [Online]. Available: https://www.youtube.com/watch?v=oUkYbf_hjjQ&list=PL_70LDmuP1F8dN7hT_CIW05_TuAqlYTM4&index=3. [Accessed: 11-Mar-2023].

“LDPC encoder block diagram. | download scientific diagram - researchgate.” [Online]. Available: https://www.researchgate.net/figure/LDPC-encoder-block-diagram_fig5_265284106. [Accessed: 11-Mar-2023].

“Low-density parity-check code,” *Wikipedia,* 20-Nov-2022. [Online]. Available: https://en.wikipedia.org/wiki/Low-density_parity-check_code. [Accessed: 11-Mar-2023].

N. Mobini, “New interative decoding algorithms for low-density parity-check (LDPC) codes.”

“NrPolarDecode,” *MATLAB & Simulink*. [Online]. Available: https://www.mathworks.com/help/5g/gs/polar-coding.html. [Accessed: 11-Mar-2023].

“Polar code (coding theory),” *Wikipedia*, 08-Nov-2022. [Online]. Available: https://en.wikipedia.org/wiki/Polar_code_(coding_theory). [Accessed: 11-Mar-2023].

“Shift register,” *Wikipedia*, 28-Dec-2022. [Online]. Available: https://en.wikipedia.org/wiki/Shift_register. [Accessed: 11-Mar-2023].

T. Sinha and J. Bhaumik, “Performance Analysis of NR Polar Codes at short information blocks for control channels,” 2021.

Y. Tian, Y. Bai, and D. Liu, “Low-latency QC-LDPC encoder design for 5G NR,” *Sensors*, vol. 21, no. 18, p. 6266, 2021.