East African Scholars Journal of Engineering and Computer Sciences
Abbreviated Key Title: East African Scholars J Eng Comput Sci
ISSN: 2617-4480 (Print) & ISSN: 2663-0346 (Online)
Published By East African Scholars Publisher, Kenya

OPEN ACCESS

Volume-4 | Issue-10 | Dec-2021 |

DOI: 10.36349/easjecs.2021.v04i10.005

Review Article

To Investigate the Performance of CRC-Aided Polar Coding Scheme

Manpreet Singh[1*], Puneet Chopra[1], Prince Jindal[1]
[1]Department of Electrical Engineering, BGIET Sangrur, India

Article History
Received: 25.11.2021
Accepted: 23.12.2021
Published: 30.12.2021

Journal homepage:
https://www.easpublisher.com

Quick Response Code

Abstract: Polar codes are a class of capacity-achieving codes. In the past decade, the interest and research effort on polar codes has been constantly rising in academia and industry alike. The selection of polar codes as the channel coding technique for control channels for 5G NR communications system has proven merits. Also, with better performance than LDPC and turbo codes, polar codes supersede the tail-biting convolutional codes used in LTE systems. In this paper polar coding scheme called CRC-Aided Polar (CA-Polar) coding scheme has been investigated using QPSK modulation over an AWGN channel.

Keywords: Polar Codes, Cyclic Redundancy Check (CRC), Signal to Noise Ratio.

1. INTRODUCTION

Polar codes are a class of capacity-achieving codes introduced in [1]. In the past decade, the interest and research effort on polar codes has been constantly rising in academia and industry alike. Within the ongoing 5th generation wireless systems (5G) standardization process of the 3rd generation partnership project (3GPP), polar codes have been adopted as channel coding for uplink and downlink control information for the enhanced mobile broadband (eMBB) communication service. The construction of a polar code involves the identification of channel reliability values associated to each bit to be encoded. This identification can be effectively performed given a code length and a specific signal-to-noise ratio. However, within the 5G framework, various code lengths, rates and channel conditions are foreseen, and having a different reliability vector for each parameter combination is unfeasible. Thus, substantial effort has been put in the design of polar codes that are easy to implement, having low description complexity, while maintaining good error-correction performance over multiple code and channel parameters.

2. POLAR CODES

Shannon in [1] wrote and derived the mathematical formulation of digital communications systems. In his main work, formulated the acceptable limit of reliable transmission of information. He proved that it is possible to receive the transmitted bits correctly. We add extra bits to the data in order to help us figure out the correct bits with a high rate (R) of probability. He first calculated the channel's capacity C(W) which is considered a high threshold. It means that if R < C(W), information sent at rate bits per channel with no errors or a low number of errors.

Figure 1: The basic communication model

From figure 1 the output from the source is a random process (X). This defined as source entropy H(X). If the system's source entropy H(X) is less than channel capacity C(W) i.e. H(X) < C(W), source input data will be sent through the channel reliably. In contrast, if the system's source entropy H(X) has a value larger than that of channel capacity C(W) i.e. H(X) > C(W), information cannot be sent reliably through the channel and the system loses the information through the channel. Referring to [2] Shannon showed that we can measure the distortion in a system by calculating the difference between two main parameters one is the Xn and the other is source output compressed representation.

Figure 2: Simple communication model

Figure 2 shows a simple communication model as Shannon drew. The source encoder compresses the data input into a suitable form with low quantity of distortion as low as possible then the output data χn goes through a block called channel encoder. In the channel encoder, the system puts extra bits into the data χn in order to improve the system's reliability against noise that comes from different sources. The output from the channel encoder Xn is sent through a channel. At the receiver, the channel decoder receives the data Yn and removes the noise with the help of the extra bits that added in the transmission side. After that, the source decoder decodes the data γn into its original form. In order to reach a safe level of transmission in this system, the blocklength (N) should be large enough, therefore, for designing a practical system we should design a system that works with an acceptable complexity and low space [3].

In the definition of polar codes is introduced and the method of encoding and decoding as well, however, in the first part of this paper, we summarize the definition of polar codes according to all of these references in order to make it easy understanding why these codes are being researched to be used in 5G systems. In [4], a general tutorial of 5G systems is presented and it focuses on the requirements of 5G systems in general nevertheless we study the requirements of 5G systems according to the chosen channel coding scheme. In polar codes are studied in case of 5G systems and they suggest that polar codes are the codes that are suitable to 5G systems and ignoring that these codes have advantages and disadvantages. In this paper, we focus on studying advantages and disadvantages of polar codes in 5G systems and present a comparison between the three suggested codes to be used in 5G systems which are LDPC, turbo, and polar codes. Moreover, we detail the trial encoding and decoding scheme of polar codes in 5G systems and in an overall communication system.

3.1 CYCLIC REDUNDANCY CHECK CODES

Cyclic-redundancy-check codes are a class of cyclic error-detecting codes, commonly used in digital networks. Note that cyclic codes are a kind of linear block codes. Basically, the CRC creates check-bits, which are appended to the message bits or data word. At the reception, it is checked whether or not the redundant bits agree with the received data. A detailed explanation of the CRC method is given next. Let us assume an (n,k) CRC code with k message bits and a block length n . So that there are $n-k$ bits of redundancy, known as checksum, check sequence or CRC. The cyclic-redundancy check employs polynomial arithmetic in Galois Field (GF) of two elements $\{0,1\}$. Message bits are treated as coefficients of a polynomial $U(X)$ with degree $k-1$, as follows:

$$U(X) = u_{k-1}X^{k-1} + u_{k-2}X^{k-2} + \cdots + u_1 X + u_0 \quad (1)$$

Namely $U = (u_{k-1}, u_{k-2}, \ldots u_1, u_0)$ represent the k information bits. Under cyclic codes theory proposed by [5] CRC codes are constructed by a generator polynomial $G(X)$ of degree $n-k$ and a division of polynomials, as follows:

$$\frac{F(X)}{G(X)} = Q(X) + \frac{R(X)}{G(X)} \quad (2)$$

Where $F(X)$ is the dividend, $Q(X)$ is the quotient and $R(X)$ is the remainder. The CRC encoder creates a block polynomial $F(X)$ based on

$U(X)$ and $G(X)$, such that $F(X)$ is divisible by $G(X)$. In other words, the remainder $R(X)$ is equal to zero in (2). This is achieved by multiplying the message $U(X)$ by the factor X^{n-k}, as shown below:

$$F(X) = X^{n-k}U(X) \quad (3)$$

The polynomial multiplication in (3) represents appending n−k 0-bits to the k-bit message. After $F(X)$ is obtained, the encoder performs the polynomial division over $GF(2)$ or modulo- 2 division as shown in (2). The quotient $Q(X)$ is ignored and the remainder $R(X)$ becomes the result. The $n-k$ coefficients of the remainder polynomial $R(X)$ constitute the checksum. The remainder polynomial $R(X)$ has a degree less than $n-k$. The output of the CRC encoder results in the original k-bit message followed by the n−k redundancy bits, i.e. $X^{n-k}U(X)+R(X)$. Take into account that the generator polynomial $G(X)$ is fixed for a given CRC scheme and it must be known by both encoder and decoder. Moreover, note that the degree of the generator polynomial defines the size of the CRC or check sequence. The CRC decoder verifies the correctness of the transmission by repeating the calculation (2). The received codeword represented by polynomial $\hat{F}(X)$ is divided by the generator polynomial $G(X)$. If the remainder polynomial $R(X)$ (or all its $n-k$ coefficients) is zero, then the received message $\hat{F}(X)$ is accepted as the one which was transmitted otherwise $\hat{F}(X)$ has errors. In other words, when $\hat{F}(X)$ is not divisible by $(G(X), R(X) \neq 0)$, an error has occurred. It is evident that CRC method for detecting errors is not foolproof. If the transmitted message is garbled across the communication channel, there is a possibility that the new version of the message $\hat{F}(X)$ is divisible by the generator polynomial $G(X)$, although it is not right. Therefore, when $\hat{F}(X)$ is divisible by $(G(X), R(X) = 0)$, either no error or undetectable error has occurred. The received encoded message with errors can be represented by

$$\hat{F}(X) = F(X) + E(X) \quad (4)$$

Where $F(X)$ is the correct encoded message and $E(X)$ is the error polynomial with nonzero terms in erroneous positions. $E(X)$ is detectable if and only if it is not divisible by the generator polynomial $G(X)$. Hence, the generator polynomial should be carefully chosen to ensure that $E(X)/G(X)$ gives a remainder different of zero, for errors we wish to detect. According with the form of the generator polynomial $G(X)$, it is possible to detect different types of errors such as single, double, triple, odd or burst errors. For example if $G(X)$ contains a factor $1+X$, then any single errors or any odd number of errors will be detected. The implementation of CRC codes is relatively simple using shift registers with feedback connections and modulo-2 adders or exclusive-OR operations, [6].

3.2 Selection of CRC polynomials

Considering that the size of the CRC or check sequence is equal to the degree of the generator polynomial $(r = n-k)$ of an (n,k) CRC code, we refer to this code as CRC-r. The normal representation of a CRC polynomial is the binary or hexadecimal notation of its coefficients.

3.3 Polar Codes

Polar codes are based on the phenomenon of channel polarization, which is developed by recursively combining and splitting individual channels. Some channels become noiseless or perfect while others turn into completely noisy or useless. As the code length N increases, a fraction of reliable channels approaches to the channel capacity. Thus, the data are sent through the reliable channels, [7].

3.4 Channel Polarization

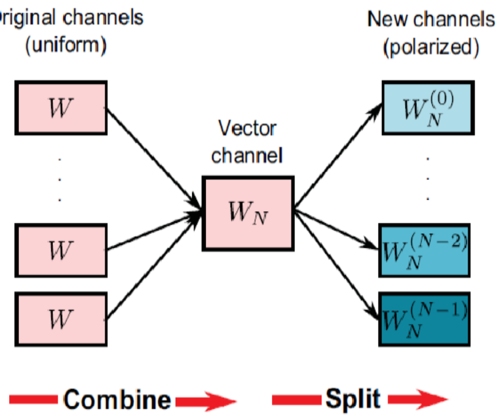
Let be $W: \chi \rightarrow \gamma$ a binary discrete memoryless channel (B-DMC), with input alphabet $\chi = \{0,1\}$, output alphabet $\gamma = \{arbitrary\}$, and the probability of observing y given that x was transmitted defined as the transition probability $W(y|x) \triangleq P(y|x)$, where $x \in \chi$ and $y \in \gamma$. Since the channel W is symmetric, such as a binary symmetric channel (BSC) or a binary erasure channel (BEC), the symmetric capacity $I(W)$ is equal to the Shannon capacity [7]. Symmetric capacity $I(W)$ is the highest rate over W with reliable communication using inputs with equal probability, it takes values inside [0,1] and is given by

$$I(W)=\sum_{y\in y}\sum_{x\in x}\frac{1}{2}W(y|x)\log\frac{W(y|x)}{\frac{1}{2}W\left(y|0+\frac{1}{2}W(y|1)\right)} \quad (5)$$

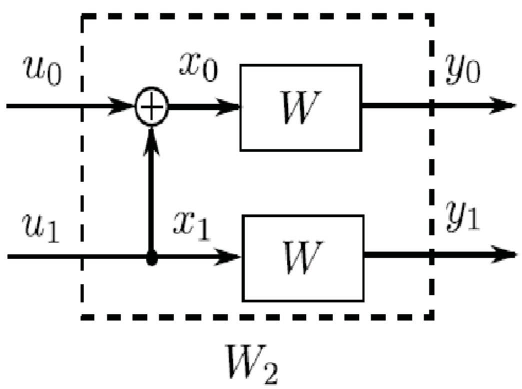
Channel polarization consists of converting n independent copies of B-DMCW into a polarized channel set $W_N^{(i)}$, where $0\le i\le N-1$. Each polarized channel becomes either noisy or noiseless as the code length N goes to infinity and the symmetric capacity terms $I\left(W_N^{(i)}\right)$ tend towards 0 or 1, respectively. Thus, a fraction of noiseless channels goes to I(W) and a fraction of noisy channels goes to $1-I(W)$. Information bits are sent through the noiseless bit-channels in order to achieve the symmetric capacity of B-DMC, and over the noisy bit-channels are fixed values, which are known by the transmitter and the receiver. The channel polarization is divided in two stages, a channel combining and a channel splitting, as is depicted in Figure 3 (a).

3.5 Channel Combining

In this stage, N copies of B-DMC W, denoted as W^N, are combined in a recursive manner to produce a synthesized vector channel $W_N:\chi^N\rightarrow\gamma^N$, where $n=2^p, p\ge 0$. The first level of



(a) Channel combining and splitting



(b) Basic polarizing transformation

Figure 3: Channel Polarization Adapted from [7]

The recursion is $W_2=\chi^2\rightarrow\gamma^2$ as shown in Figure 3 (b), with transition probability

$$W_2(y_0,y_1|u_0,u_1)=W(y_0|u_0\oplus u_1)W(y_1|u_1) \quad (6)$$

In general, the transition probability of the combining operation $\left(W^N\rightarrow W_N\right)$ is

$$W_N\left(y_0^{N-1}|u_0^{N-1}\right)=W^N\left(y_0^{N-1}|u_0^{N-1}G_N\right) \quad (7)$$

Where G_N is the generator matrix of size N, which represents a linear mapping from the input vector u_0^{N-1} to the output vector x_0^{N-1}, so that $x_0^{N-1}=u_0^{N-1}G_N$.

4. PROPOSED WORK

This work highlights the components to enable a polar coding downlink simulation using QPSK modulation over an AWGN channel. Figure 4 shows the schematic block diagrams for the transmitter end i.e., downlink with associated circuitry.

For modelling the downlink, the input bits have been interleaved prior to polar encoding. Then the CRC bits have been appended at the end of the information bits. In polar encoding SNR-independent method has been used where the reliability of each sub-channel is computed offline. The ordered sequence is stored for a maximum code length. This nested property of polar codes allows the sequence to be used for any code rate and for all code lengths less than the maximum code length. This sequence has been computed for given rate matched output length and information length.

Figure 5 shows schematic block diagram for the transmitter side uplink with associated circuitry. The payload size of greater than 19 bits has been used with code-block segmentation.

The polar encoded set of bits has been rate-matched to the output. Then the coded bits have been sub-block interleaved and passed to a circular buffer of size N. Depending on the desired code rate and selected values of message bits K, length of rate-matched output E, and circular buffer of size N; by reading the output bits from the buffer, either of repetition (E >= N), and puncturing or shortening (E < N) has been realized. Note that for puncturing, E bits have been taken from the end, for shortening, E bits have been taken from the start and for repetition, E bits have been repeated by modulo N. In the developed MATLAB test benches, the selected bits are passed on to the modulation mapper for the downlink and they are further interleaved prior to mapping while for the uplink.

At the receiver end, rate recovery has done using the following:

- For puncturing, corresponding LLRs for the bits removed are set to zero
- For shortening, corresponding LLRs for the bits removed are set to a large value
- For repetition, the set of LLRs corresponding to first N bits are selected.

Figure 6 shows the components for polar coding that have been used for Block Error Rate calculation.

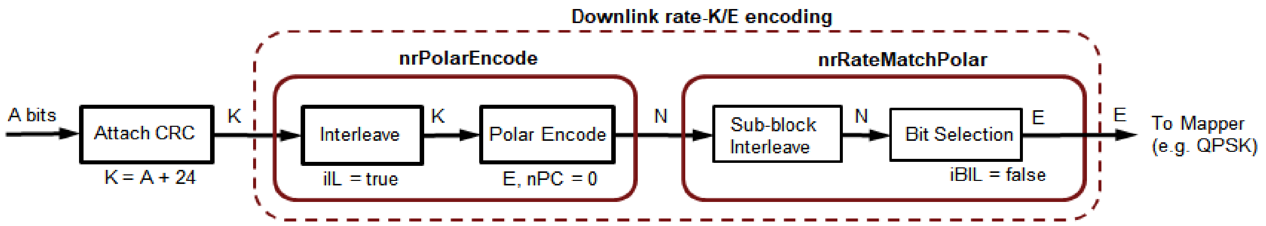


Figure 4: Schematic Diagram for the Transmitter End

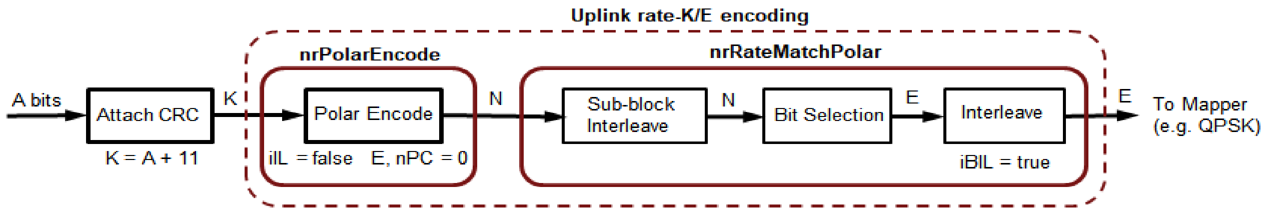


Figure 5: Schematic Diagram for the Transmitter End

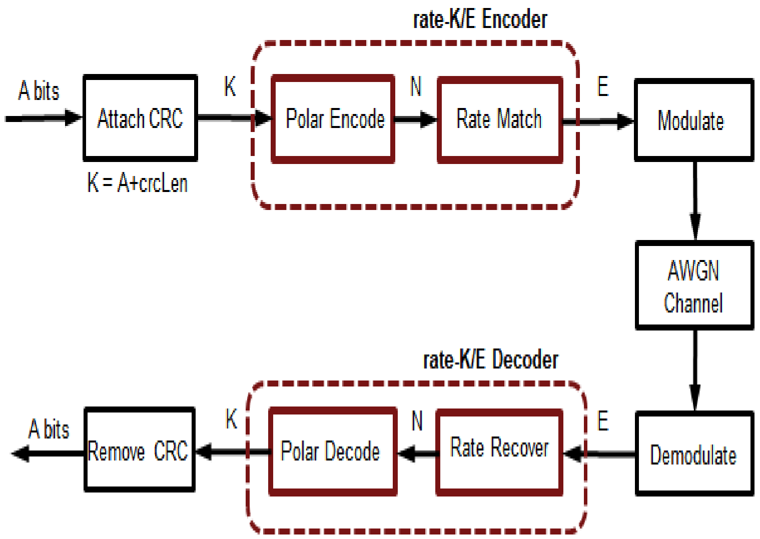


Figure 6: Simulation Set-up for Block Error Rate Simulation

Following steps have been performed for processing each frame. First K random bits are generated and CRC has been computed and appended to these bits. Then the CRC appended bits have been encoded using polar coding. After this rate-matching has been performed to transmit E bits and these E bits are modulated using QPSK modulation. These bits are passed through a AWGN channel and the noisy bits has been demodulated to output LLR values. The rate recovery has been performed which accounts for puncturing, shortening or repetition. Then the recovered LLR values are polar decoded and deinterleaved. From these decoded K bits, the first K bits which have been transmitted have been compared to calculate block error rate.

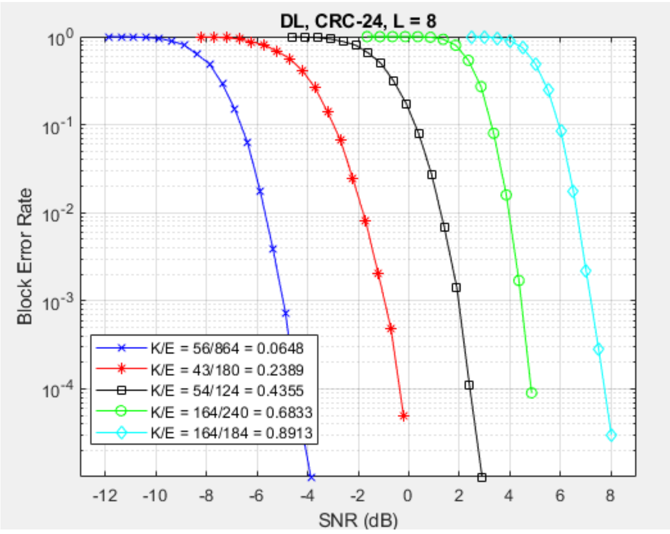


Figure 7: Block Error Rate for Downlink, with CRC=24, L=8 for Different K/E

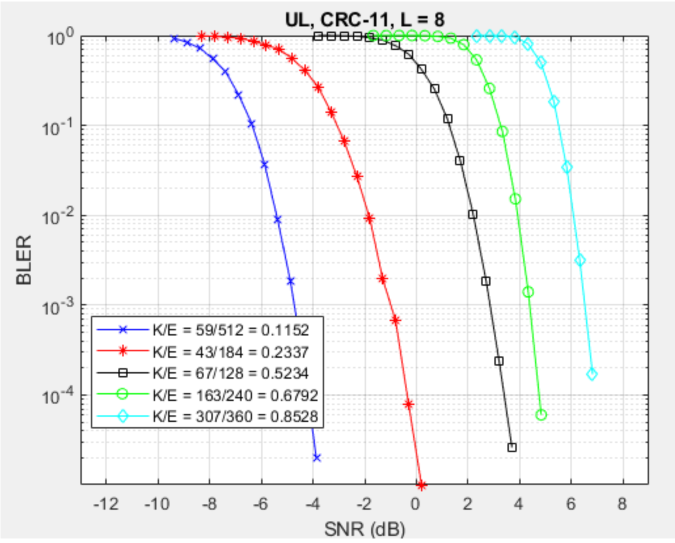


Figure 8: Block Error Rate for Uplink, with CRC=11, L=8 for Different K/E

Figures 7 and 8 shows the block error rate variation for downlink and uplink respectively. From Block error rate variation performance for different code rates and message lengths, it has been concluded that, polar codes are suitable to achieve thigh performance in a communication link. Results also indicate that polar coding functions used for present simulations can also support the parity-check polar coding construction and encoding.

5. CONCLUSION

For the investigation it has been concluded that the use of polar codes has proven merits as a channel coding technique for control channels for a 5G NR communications system. This new coding family i.e., polar coding has the benefit of achieving higher capacity. Polar coding technique has comparable performance with LDPC codes and turbo codes. Results also indicate that polar coding functions could also support the parity-check polar coding construction and encoding. In the future work the actual channel model could be developed and performance of the proposed system can be evaluated for these channel models.

REFERENCES

1. Arıkan, E. (2009). Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inform. Theory*, 55, 3051–3073.
2. Arikan, E. (1988). An upper bound on the cutoff rate of sequential decoding. *IEEE Trans. Inform. Theory*, 34, 55–63.

3. Hassani, S. H., Alishahi, K., & Urbanke, R. (2014). Finite-length scaling for polar codes. *IEEE Trans. Inform. Theory*, 60(10), 5875–5898.
4. Cover, T. M., & Thomas, J. A. (2006). Elements of Information Theory. Wiley Series in Telecommunications, Wiley, 2nd. ed.
5. Peterson, W. W., & Brown, D. T. (1961). Cyclic codes for error detection. *Proceedings of the IRE*, 49(1), 228–235.
6. Sklar, B. (2001). Digital communications. Prentice Hall Upper Saddle River.
7. Arikan, E. (2009). Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Transactions on Information Theory*, 55(7), 3051–3073.

Cite This Article: Manpreet Singh *et al* (2021). To Investigate the Performance of CRC-Aided Polar Coding Scheme. *East African Scholars J Eng Comput Sci*, *4*(10), N/A.