Reliability Analysis of the Sum-Product Decoding Algorithm for the PSK Modulation Scheme

Hadi Khodaei Jooshin
Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran
hadikhodaei.j@gmail.com

Mahdi Nangir *
Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran
nangir@tabrizu.ac.ir

Received: 04/Apr/2020 Revised: 24/Aug/2020 Accepted: 08/Oct/2020

Abstract
Iteratively decoding and reconstruction of encoded data has been considered in recent decades. Most of these iterative schemes are based on graphical codes. Messages are passed through space graphs to reach a reliable belief of the original data. This paper presents a performance analysis of the Low-Density Parity-Check (LDPC) code design method which approach the capacity of the Additive White Gaussian Noise (AWGN) model for communication channels. We investigate the reliability of the system under Phase Shift Keying (PSK) modulation. We study the effects and advantages of variation in the codeword length, the rate of parity-check matrix of the LDPC codes, and the number of iterations in the Sum-Product Algorithm (SPA). By employing an LDPC encoder prior to the PSK modulation block and the SPA in the decoding part, the Bit Error Rate (BER) performance of the PSK modulation system can improve significantly. The BER performance improvement of a point-to-point communication system is measured in different cases. Our analysis is capable for applying any other iterative message-passing algorithm. The code design process of the communication systems and parameter selection of the encoding and decoding algorithms are accomplished by considering hardware limitations in a communication system. Our results help to design and select paramours efficiently.

Keywords: LDPC Codes; BER Performance; SPA; Channel Decoding Algorithm; Rate; Channel Capacity.

1- Introduction
Berrou et al. introduced Turbo Codes in 1993 and made it possible that by utilizing these error correction codes, one can approach the Shannon limit of the channel capacity [1-2]. A few years later in 1996, Mackay and Neal rediscovered the Shannon limit performance of the Low-Density Parity-Check (LDPC) codes [3-5], that were introduced by Gallager in 1963 [6]. The LDPC codes could compete with the Turbo Codes successfully. Nowadays, there is an increasing demand for the reliable communication systems, which can handle a large amount of data rate with high-speed equipment. It requires cheap, fast, and very small size communication and storage devices.

The performance of all communication and storage systems has some limitations. One of these limitations is the channel capacity concept that has been introduced by Claude Shannon in 1948. Channel Capacity is the maximum possible value of rate, which can be achieved by using a specific communication system with an arbitrary small enough BER value.

Some applicable error correction codes are the Hamming codes, the LDPC codes, the Turbo codes, and Polar codes, which have been employed in the real world communication systems. The LDPC codes are a kind of linear block codes that strongly contrasts the channel noise effect. The LDPC code is one of the hot research topics in the coding and information theory due to its high speed encoding and decoding algorithms, it’s capability to achieve the channel capacity providing a reliable communication for an arbitrary transmission rate. It is a progressive coding scheme and is proper in a wide range of applications such as signal processing, cryptography, compressed sensing, wireless communications, and data compression.

The LDPC codes utilize a parity-check matrix $H$, in which the proportion of ones to zeros is very low; in other words, the matrix $H$ is sparse. These codes are classified into the regular and the irregular codes. A code is regular if the number of ones in each column (say $w_c$) and the number of ones in each row (say $w_r$) in the parity-check matrix $H$ are

* Corresponding Author
fixed values. Obviously, if a code is not regular, then it is irregular code. An LDPC code of length $n$ can be indicated with $(n, w_c, w_v)$, where $w_v$ and $w_c$ are generally two vectors, respectively showing the degree of the variable nodes and the check nodes of $H$. Thus, each information bit in a variable node is involved with $w_v$ check bits, and similarly each check bit in a check node is involved with $w_c$ information bits. The decoder in the receiver side employs the parity-check matrix $H$ for accomplishing its task. It reconstruct the original data with a BER utilizing a decoding algorithm.

In this work, we consider SPA and evaluate its reliability. The LDPC codes are very efficient codes in several communication scenarios, such as wireless communications [7], optical communication systems [8], satellite communication systems [9], digital video broadcast (DVB) systems [10], and terrestrial multimedia broadcasting (TMB) systems [11]. Furthermore, it’s applications in high-density data storage systems, such as digital electronic memories are now considerable. These codes have capacity-approaching performance and can be achieved using practical and implementable iterative decoding algorithms. The LDPC codes have been adopted to use in the next generation of communication systems [12-13] such as 5G due to the low BER. As an example, $\text{BER}=10^{-13}$ is achievable with an acceptable complexity of encoding and decoding schemes.

In this paper, we investigate SPA, which is one of the fast, implementable, and simple iterative message-passing algorithms that have been utilized for decoding of the LDPC codes [14-16].

Through this paper, we follow three main goals for a designed parity-check matrix $H$. First, we show that by increasing the size of parity-check matrix $H$, the performance improves and BER value decreases. Second, we illustrate that the BER performance improves by increasing the iteration numbers in the SPA. Our third finding is that the performance or BER decreases by decreasing the rate of parity-check matrix $H$. For instance, for the LDPC code with parity-check matrix $H$ (768, 1024, irregular), rate=$1/4$, and iteration=10 in the SPA, we achieve $\text{BER}=10^{-9}$ for $\text{Eb/N0}=6\text{dB}$, while for the LDPC code with $H$ (384, 512, irregular), rate=$1/4$, and iteration=10, we achieve $\text{BER}=10^{-7}$ for $\text{Eb/N0}=6\text{dB}$. Hence, the advantage of increasing the size of the parity-check matrix $H$ is concluded. The effect of parameter variations is desirable in this work.

The rest of this paper is organized as follows: In section II, the system model and definitions are proposed. Furthermore, the details of the encoding and decoding schemes are provided in this section. Simulation results and discussions are presented in section III. Finally, section IV concludes this paper.

2- System Model and Definitions

In this section we present system model and provide some fundamental tools for iterative decoding schemes. Specifically, we study the SPA because it can be simply modified and extended to get other message-passing algorithms for other communication system tasks.

2-1-System model

The task of a point-to-point communication system is conveying information from a source to a destination. In Fig. 1, a simplified block diagram a point-to-point communication system is depicted. A brief description of each block is presented.

![Fig. 1: Block Diagram of Communication System.](image)

In the source encoder, the information symbols of the source are mapped to codewords. The main reasons of using a source encoder is reduction of redundancy from information symbols, which can significantly reduce the size of transmitted data. For instance, the Lempel-Ziv 77 (LZ77), the Lempel-Ziv 78 (LZ78), and the LZ-Storer-Szymanski (LZSS) are some source encoding algorithms based on text compression algorithms. They use a sliding window over the sequence of symbols, with two sub-windows for the source coding [17-19].

If source information can be completely recovered from codewords, this coding is called lossless compression, otherwise it is called lossy compression. For the sources with unknown distributions, we use universal source coding algorithms [20]. Furthermore, multi-terminal source coding algorithms can be applied for the case of single binary source [21].

The second block is a channel encoder. Some intentional redundancy is added to the vector of the information symbols to increase reliability of the transmission via the noisy channel, which causes a rate reduction [22].

The channel coding methods can be categorized into two main classes. First, the linear block codes maps a sequence of $m$ information bits into a codeword with $n$ bits ($n>m$). The Hamming codes, LDPC codes, BCH codes, and cyclic
codes are some examples of this category. Second, the convolutional codes which maps a vector of $m$ information bits into a codeword with $n$ bits, depending on the current and previous information bits. For instance, the turbo codes is in this category. In this work, the LDPC codes and the SPA are exploited for the channel encoding and the channel decoding, respectively. Finally, the third block is modulator, which prepares the encoded data to send via communication channel.

Modulation superimposes data on a carrier signal, which its frequency is higher than the bandwidth of the information signal [23]. The $M$-PSK (phase-shift keying), the $M$-FSK (frequency-shift keying), and $M$-ASK (amplitude-shift keying) are fundamental digital modulation schemes. In this paper, the BPSK ($M=2$) is exploited for accomplishing the modulation.

The modulated data is transmitted by noisy channel such as a wire, an antenna, an optical fiber, etc. In this paper, the channel noise is assumed to be the Adaptive White Gaussian Noise (AWGN). Furthermore, an amplification of the modulated data is done before transmitting over the noisy channel due to channel debilitation and fading phenomena.

In the receiver side, all performed operations at the transmitter should be accomplished on the received data reversely. Therefore, first, data is being demodulated then the demodulated data is being decoded by the SPA to get source codewords. Finally, these codewords are being decoded to obtain the information source symbols. All of the methods and procedures for the encoding in transmitter and the decoding in receiver should be the same, and they should be done in a reverse order.

2-2- Graphical Representation of The LDPC Codes

A bipartite Tanner graph that has been illustrated in Fig. 2 is a graphical representation of the parity-check matrix $H$, made of two types of nodes, the variable nodes (VN) denoted by $v_j$ and the check nodes (CN) denoted by $c_i$ [24]. The $j$-th VN ($v_j$) and $i$-th CN ($c_i$) in the Tanner graph are connected with each other if and only if $h_{ij}=1$, in the matrix $H$. The following matrix is a parity-check matrix $H$ (5,10,regular). It’s corresponding Tanner graph is shown in Fig. 2.

\[
H = \begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1
\end{pmatrix}
\]

Fig. 2: Graphical representation (Tanner graph) of $H$ (5,10, regular) with $w_v=2$, $w_i=4$ .

A loop or cycle is a close path of nodes that crosses over the edges of the Tanner graph. The shortest cycle in a Tanner graph is called the girth of graph. A cycle of the length $6$ is illustrated in Fig. 2, by the bold edges. Hence, there is no cycle of length $4$ in this graph, the length of its girth is $6$. We investigate the BER performance of LDPC codes over AWGN channels from different points of view caused by the parameter variation.

We implement and decode the noisy corrupted codewords by utilizing iterative belief propagation decoding algorithm based on LDPC codes, which its performance strongly depends on the length of girth. As the length of girth increases, the computability of decoding algorithm increases. Furthermore, the BER performance can be improved by removing lower length cycles (i.e., increasing the length of girth). In our implementations, the minimum length of girth is assumed to be $6$.

2-3- The LDPC Encoding Algorithm

A sequence of blocks each of them having $k$ information bits are encoded by using the generator matrix $G$, which can be derived from the parity-check matrix $H$ in different ways. Reader can refer to [25] for further explanation about deriving generator matrix $G$. For the obtained generator matrix $G$, we have $GH^T=0$.

Let consider $C$ is the codeword of length $n$ obtained from multiplying the information bit of length $k$ and the generator matrix $G$ with the size of $k \times n$. Thus, $C$ forms the data that is modulated before transmission. $C$ is a valid codeword if and only if $CH^T=0$. Therefore, the $C$ is as follows,

\[
C_{i,n} = D_{i,k}G_{k,n}, \quad (1)
\]

where,

\[
D = \{d_1, d_2, d_3, ..., d_k\},
\]

and

\[
C = \{c_1, c_2, c_3, ..., c_n\}.
\]
Furthermore, \( k \) and \( n \) are respectively the length of the information packet bits and the length of the codeword \( C \). Note that, \( n-k \) is the length of the redundancy which is added to the information bits for providing protection.

Besides, there is another encoding algorithm using LDPC codes which is called syndrome generation method. This method has a source coding and compression goal. A syndrome generated by using the parity-check matrix of an LDPC code is sent to the decoder as a lossless compressed data. Thus, for data \( n \)-tuple \( u \), we send \( s = uH^t \) to the decoder.

In this method, the decoder finds an estimation of \( u \) based on the received syndrome \( s \) by utilizing a syndrome decoding scheme. An efficient scheme for the syndrome decoding is SPA algorithm. In this scheme, in addition to the syndrome, a side information is needed. Actually, side information is a corrupted version of the original data \( u \) affected by the channel noise. Here, we briefly describe syndrome decoding scheme based on the SPA.

In this scheme, first the syndrome \( s \) is located in the CNs and the side information is located in VNs. Then, the message-passing SPA is run. For a given number of iterations, Log-Likelihood-Ratio (LLR) values are calculated and passed between CNs and VNs. The VN values are updated in each iteration based on the calculated LLR values. Finally, one can find the decoded data which are located in the VNs of the Tanner graph of the LDPC code with parity-check matrix \( H \).

### 2-4- The Sum-Product Decoding Algorithm

The message-passing algorithms are iterative decoding procedures, in which some messages are passed back and forward between the VNs and CNs until the process is stopped. The bit-flipping decoding algorithm is one of the message-passing algorithms in which the received symbols are hard decoded into 1’s and 0’s.

The SPA is similar to the bit-flipping algorithm, but the bit-flipping decoding is a kind of hard decisions while the SPA is a soft decision message-passing algorithm that utilizes the probability of each bit instead of its value. The extrinsic data between \( j \)-th CN and \( i \)-th VN which is the probability of \( c_i = 1 \) is denoted by \( E_{ji} \) as the \( j \)-th parity check equation is satisfied.

The probability that a parity-check equation is established for the bit \( c_i \) to be 1 is represented by \( P \) that is calculated as follows:

\[
E_{ji} = L(P_{ji}^e) = \log \frac{1 - p_{ji}^e}{p_{ji}^e}.
\]

By using the following relation,

\[
\tanh \left( \frac{1}{2} \log \frac{1-p}{p} \right) = 1-2P,
\]

it can be concluded that,

\[
E_{ji} = \log \frac{1 + \prod_{i \in B_j, j' \neq i}(1 - 2P_{ji}^{e_j})}{1 - \prod_{i \in B_j, j' \neq i}(1 - 2P_{ji}^{e_j})},
\]

and by using the relation,

\[
2 \tanh \frac{1}{p} = \log \frac{1+p}{1-p},
\]

we can write,

\[
E_{ji} = 2 \tanh \frac{1}{p} \prod_{i \in B_j, j' \neq i} \tanh \frac{L(P_{ji}^e)}{2}.
\]

The value of \( L(P_{ji}^e) \) takes its sign and its magnitude as follows:

\[
L(c) = \log \frac{p(c=0)}{p(c=1)}.
\]
\[ L(P_{i,j}) = S_{i,j} \cdot M_{i,j} \cdot \] 

where,

\[ S_{i,j} = \text{sign}(L(P_{i,j})) \] 

\[ M_{i,j} = |L(P_{i,j})| \] 

Thus, equation (11) can be rewritten as

\[ \tanh \left( \frac{1}{2} L(P_{i,j}) \right) = \prod_{i \neq j} S_{i,j} \cdot \prod_{i \in B_i, j \neq i} \tanh(\frac{1}{2} M_{i,j}) \] 

Therefore,

\[ E_{i,j} = \prod_{i \neq j} S_{i,j} \cdot 2 \tanh^{-1}(\prod_{i \neq j} \tanh(\frac{1}{2} M_{i,j})) \]

\[ = \prod_{i \neq j} S_{i,j} \cdot 2 \tanh^{-1}(\log(\prod_{i \neq j} \tanh(\frac{1}{2} M_{i,j}))) \]

\[ = \prod_{i \neq j} S_{i,j} \cdot \sqrt{\sum_{i \neq j} \log(\tanh(\frac{1}{2} M_{i,j})))} \]

where \( \Theta(x) \) is defined as follows:

\[ \Theta(x) = -\log(\tanh(\frac{x}{2})) = \log \left( \frac{e^x + 1}{e^x - 1} \right) \] 

In the SPA, each VN has access to the initial LLR and LLRs from connected CNs because probability passes between nodes. The total LLR in the i-th bit is as follows:

\[ L_{i,\text{total}} = L_i + \sum_{j \in A_i} E_{j,i} \] 

where \( A_i \) is the set of CNs connected to i-th VN.

The decoder is initialized by setting VN information \( L(P_{i,j}) \), for which \( h_{ij} = 1 \), as follows:

\[ L_i = L(c|y_i) = \log \left( \frac{P(c=i|y_i)}{P(c=\bar{i}|y_i)} \right) \] 

where \( y_i \) is the i-th bit information value that has been received. \( L_i \) can be calculated for the binary input AWGN channel as follows:

\[ P(x_i = x|y_i) = \frac{1}{1 + \exp(-4y_i x/N_0)} \] 

from equation (20),

\[ L_i = L(c|y_i) = -4y_i N_0 \] 

where \( N_0 \) is the noise power spectrum density.

After calculating total LLR for every VN, \( \hat{C} \) is obtained as follows:

\[ \hat{C}_i = \begin{cases} 1 & \text{if } L_{i,\text{total}} < 0, \text{ for } i=1, 2, ..., N; \\ 0 & \text{else}, \end{cases} \]

where \( N \) is the length of codewords.

The accuracy of decoded data \( \hat{C} \) can be obtained by multiplying \( \hat{C} \) and \( H^T \). If \( \hat{C}H^T = 0 \), then the decoded data is correct, else LLRs should update as follows:

\[ L(P_{i,j}) = \sum_{i \neq j} E_{j,i} + L_i \] 

These operations continue until the parity-check equations are satisfied \( (\hat{C}H^T = 0) \), or the number of iteration equals the maximum limit which has been considered.

3- Simulation Results

In this section, we report some simulation results which are obtained from implementation of the described communication system. All BER values are averaged over 50 tests for randomly generated binary sequences as an information source.

The BER performance of a PSK modulated communication is presented with respect to the number of iterations, the code length, and coding rate. A fair comparison is done for various values of the signal to noise ratio.

After decoding received data in receiver the number of bits that have not received correctly can be simply obtained by comparing the received bits in the receiver and transmitted bits of the transmitter. The BER is calculated by dividing the number of incorrect received bits to the number of total received bits.

In Fig. 3, it is depicted that the BER decreases by increasing the number of iterations in the SPA with a same parity-check matrix \( H \) (384,512,irregular) with the rate of \( \frac{1}{4} \). This observation is because of increasing the number of runs in update equations of the SPA.

Based on the results, which is reported in Fig. 4, it is obvious that the BER decreases by increasing the size of the parity-check matrix \( H \). This fact stems from the direct effect of increasing length. Note that, by increasing the size of \( H \), complexity of implementations increases. For example, the BER is 5.46×10^{-6}, 3.91×10^{-6}, and 2.8×10^{-6} respectively for the cases of iteration=10, iteration=20, and iteration=50 in SNR=6db.

The effect of increasing the number of added redundancy to a same information block with a constant length to the BER performance is presented in Fig. 5. As it is seen, the BER value decreases by increasing redundancy or equivalently by decreasing coding rate.
As an example, the BER is $2.97 \times 10^{-3}$, $6.72 \times 10^{-4}$, $8 \times 10^{-7}$, and $8 \times 10^{-11}$ respectively for rate=$\frac{2}{3}$, rate=$\frac{1}{2}$, rate=$\frac{1}{4}$, and rate=$\frac{1}{8}$ in SNR=7db.

Based on the reported results, it is seen that the SPA is reliable with respect to parameter changes and can be utilized for the BPSK modulation scheme with an acceptable performance. In the design process, one can choose proper rate, number of iterations and length to reach a required quality of service.

**Conclusions**

In this paper, a point-to-point communication system is investigated. Our focus is on the channel encoder and the channel decoder blocks and their BER performances. The LDPC codes are employed for the channel encoder block and the SPA with the same parity-check matrix of encoder are exploited for the channel decoding. The BER performance of the system under AWGN communication channel model with PSK modulation scheme is derived from implementations for various cases. Our simulation results show the effect of the parameter changes in order to achieve lower BER values. This provide the direction of parameter changes to a system designer to improve the performance.

**Appendix**

Here, we present the degree distributions of the parity-check matrices, which have been used in our implementations for some rates. Note that the parity-check matrices are obtained from these degree distributions by using progressive edge growth method with some approximations.

For the rate of 0.75, we have:

$$
\lambda(x) = 0.2911x + 0.1892x^2 + 0.0408x^3 + 0.0873x^4 + 0.0074x^5 + 0.1126x^6 + 0.0925x^7 + 0.0186x^8 + 0.124x^9 + 0.016x^{10} + 0.0202x^{11},
$$

and

$$
\rho(x) = 0.8x^4 + 0.2x^5.
$$
For the rate of 0.66, we have:
\[ \lambda(x) = 0.2177x + 0.1634x^2 + 0.0985x^3 + 0.1018x^4 + 0.0538x^5 + 0.0301x^6 + 0.0566x^7 + 0.0109x^8 + 0.0809x^9 + 0.1863x^{10}, \]
and
\[ \rho(x) = 0.9x^5 + 0.1x^7. \]

For the rate of 0.5, we have:
\[ \lambda(x) = 0.1528x + 0.2825x^2 + 0.0062x^3 + 0.5586x^{19}, \]
and
\[ \rho(x) = x^9. \]

For the rate of 0.25, we have:
\[ \lambda(x) = 0.1118x + 0.1479x^2 + 0.0721x^5 + 0.2464x^6 + 0.0021x^8 + 0.4195x^{29}, \]
and
\[ \rho(x) = x^{23}. \]

For the rate of 0.125, we have:
\[ \lambda(x) = 0.1154x + 0.1846x^2 + 0.1872x^6 + 0.0107x^7 + 0.0107x^8 + 0.0298x^9 + 0.0676x^{17} + 0.0713x^{21} + 0.0311x^{22} + 0.0523x^{25} + 0.194x^{55} + 0.0148x^{69} + 0.0192x^{72} + 0.0021x^{89} + 0.0086x^{99}, \]
and
\[ \rho(x) = 0.5x^{45} + 0.5x^{46}. \]

References

Hadi Khodaei Jooshin received the B.S. degree in Telecommunication, Electrical Engineering from University of Tabriz, Tabriz, Iran in 2020. Currently he is working on extending iterative channel decoding algorithms for special applications. His area research interests include Channel Coding and Information Systems, Image Processing, Machine Learning and Signal Processing.

Mahdi Nangir received the B.Sc. degree with first rank in Electrical Engineering from University of Tabriz and M.Sc. degree in Communication System Engineering from Sharif University of Technology, Tehran, Iran, in 2010 and 2012, respectively. He received the Ph.D. degree from K. N. Toosi University of Technology, Tehran, Iran, in 2018. He was a finalist of the Mathematics Olympiad and owner of bronze medal in 2005 from Young Scholar Club. He received high ranks in Iranian National Electrical Engineering Student Olympiads of 2009 and 2010. In 2017, he joined McMaster University, Hamilton, Ontario, Canada as a research visiting student. He is now an assistance professor in Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran. His research interests include coding and information theory, distributed source coding, data compression algorithms and optimization.