Application of LDPC Codes on Networks

A.Agrawal and M.A.Ambroze

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

The current communication systems face many problems these days during the transmission of data, which are network efficiency and congestion. This relates to quality of service of the data transmitted- i.e. data rate, delay, delay variation and packet loss which are provided to the customer. Congestion causes packets to be lost, due to which retransmission of packets takes place and this in turn can increase congestion in the network. From error correction point of view, retransmissions represent an inefficient type of code called as the repetition code, which is known to have high overhead.
This paper investigated the way to reduce the need for retransmission of the lost packet by using efficient error correction codes, such as Low-density parity check (LDPC) codes. They were invented by Gallager in 1963 and had been forgotten until Mackay rediscovered it. They are able to reconstruct the number of lost packets at the receiver end.
This project discusses the iterative decoding and Gaussian elimination decoding methods for their application to decode the received code word with erasures in the binary erasure channel. The information bits will be encoded which is combination of information bits and the redundant bits called as code word which is subjected to noise when transmitted through the binary erasure channel. The error occurs in the form of erasure of the bits from the code word, which is then decoded with the help of the two decoding methods.

Keywords

Error-correcting codes, LDPC codes, Iterative decoding, Gaussian elimination, Binary erasure channel, communication systems, Code word, Retransmission, Generator matirx, Parity check matrix, Channel capacity, Rate of block code.

1 Introduction

C. E. Shannon originated the error-correcting codes in 1940s, which increased the ability and reliability of digital signals. With the help of these error-correcting codes, users can encode the message and transmit over the channel with decoder at the receiving end to decode the message and detect and correct any error in the message. According to Shannon's paper "A Mathematical Theory of Communication" the probability of error in a channel depends on the channel capacity (Shannon, 1948). This project deals with the applications of LDPC (Low-density parity heck) codes, which were first introduced by Robert Gallager in 60's. The LDPC codes needs to be applied on the channel models in order to reduce the error that are created during the data transmission in the channel (Gallager, 1963). The channel that is going to be used in this project is Binary Erasure Channel (BEC), which has the Channel Capacity of 1-p, where p is the erasure probability. Binary erasure channel are not

same like Binary symmetric channel in the sense that if the bit arrives it is always correct and the error occurs only when the bit is erased. The encoding and decoding of the message that will be transmitted over the channel in order to provide a simulation to explain the working of the LDPC codes and the approximate error correction mechanism in the binary erasure channel using Gaussian elimination method and iterative decoding method.

2 Error Correction Code

The main problem faced in today's world is the reliability issues faced while using a digital communication system where we have to expect error at any moment during the connection and should be able to deal with that error. Retransmission of the lost bit is a redundant solution that is time consuming and can also cause congestion in the network. The other approach, called "error detecting and correcting codes" can be used. Error correcting codes are of various types but the one which is used in this project is linear block codes called as Low density parity check (LDPC codes) (Shokrollahi, 2003).

3 Procedure and Methodology

The Process comprises of the encoding of the information bits, transmission of the code word generated through the binary erasure channel and how the information is affected by the noise in the channel. Finally, how the received code words with erasure will be decoded in the decoder with the help of the two decoding process i.e. iterative decoding and the Gaussian elimination process. The encoder will generate the generator matrix with the help of parity-check matrix. After generating the generator matrix, the encoder generates the code word which will be the addition of the information bits and the parity check bits which will be generated with the help of the following formula:

$$\text{Code word } (v) = \text{Information Bits } (u) * \text{Generator Matrix } (G)$$

This received code word is combination of the information bits and the parity check bits. Parity check bits will be helpful in recovering the original information after passing the code word through the noisy channel. This is explained with the help of an example.

Example:

$$\text{Code word } (v) = \text{Information Bits } (u) * \text{Generator Matrix } (G)$$

Where,

$$\text{Generator Matrix } (G) = \begin{pmatrix} 1\,1\,0\,1\,0\,0\,0 \\ 0\,1\,1\,0\,1\,0\,0 \\ 1\,1\,1\,0\,0\,1\,0 \\ 1\,0\,1\,0\,0\,0\,1 \end{pmatrix}$$

Information Bits (u_1) = 0 1 1 0

$$\text{Code word } (v_1) = [0\ 1\ 1\ 0] * \begin{pmatrix} 1\ 1\ 0\ 1\ 0\ 0\ 0 \\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\ 1\ 1\ 1\ 0\ 0\ 1\ 0 \\ 1\ 0\ 1\ 0\ 0\ 0\ 1 \end{pmatrix}$$

As the matrix multiplication is the between 1 x 4 dimension and 4 x 7 dimension matrix the code word will the of 1 x 7 dimension.

Code word (v_1) = [1 0 0 0 1 1 0]

After the encoding is done on the information bits, then the encoded code word is passed through the communication channel. In Binary erasure channel, if there is any error during the transmission due to noise then an erasure is created in the code word which is denoted by ‘e’ n the received code word. So the received code words which initially had two input symbols ‘0’ and ‘1’ before transmission will now contain three output symbols ‘0’, ‘1’ and ‘e’.

As the channel accepts the input as the encoded code word, the first code word will be

Code word (v_1) = [1 0 0 0 1 1 0]

As the channel will create the erasure at the random position, the erasure will be denoted by ‘e’. In this code word the erasure will be at three positions. Hence, the received code word will be,

Received code word (r_1) = [e 0 0 e 1 e 0]

When the erasure is detected in the received code word then it will solve the erasure. It can be done with some specific steps.

1. Firstly it will check for erasure in the received code word (r1) = [e 0 0 e 1 e 0]. It can see that we have erasure in the 1st, 4th and the 6th position.

2. Now it will multiply the parity check matrix and the received code word,

Parity check Matrix (G) * Transpose of received code word (r^T) = 0

Where,

$$\text{Parity check Matrix (H)} = \begin{pmatrix} 1\,0\,0\,1\,0\,1\,1 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \end{pmatrix}$$

Received code word (r_1) = [e 0 0 e 1 e 0]

$$\begin{pmatrix} 1\,0\,0\,1\,0\,1\,1 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \end{pmatrix} * \begin{pmatrix} e \\ 0 \\ 0 \\ e \\ 1 \\ e \\ 0 \end{pmatrix} = 0$$

$$\begin{pmatrix} e\,0\,0\,e\,0\,e\,0 \\ 0\,0\,0\,e\,1\,e\,0 \\ 0\,0\,0\,0\,1\,e\,0 \end{pmatrix} = 0$$

3. After obtaining the matrix, it will consider that there are three equations whose value should be zero when it has all the unknown values.

4. It will check which equation has the less erasure; in this case it will be the third row of the matrix.

$$[0\,0\,0\,0\,1\,e\,0] = 0$$

5. In this equation it will do binary addition and find out the total value of the equation, it will substitute the value as 1 with one unknown.

6. As this equation needs another 1 in the position of ‘e’ to satisfy the condition of being equal to zero, it will substitute the value of unknown as 1.

7. Now it will have one solved erasure with only two unknown in the received code word and the equation matrix will be,

Received code word (r_1) = [e 0 0 e 1 1 0]

$$\begin{pmatrix} e\,0\,0\,e\,0\,1\,0 \\ 0\,0\,0\,e\,1\,1\,0 \\ 0\,0\,0\,0\,1\,1\,0 \end{pmatrix} = 0$$

8. Now it will repeat step no. 4 and check which equation has less erasure, now it will be the second row in the matrix.

$$[0\ 0\ 0\ e\ 1\ 1\ 0] = 0$$

9. In this equation we can do binary addition and find out the total value of the equation, we will get the value as 0 with one unknown.

10. As this equation value is 0, it can say that the value of unknown is also 0, so that it will not affect the equation and its binary addition value.

11. Now it will have two solved erasure with only one unknown in the received code word and the equation matrix will be,

$$\text{Received code word } (r_1) = [e\ 0\ 0\ 0\ 1\ 1\ 0]$$

$$\begin{pmatrix} e\ 0\ 0\ 0\ 0\ 1\ 0 \\ 0\ 0\ 0\ 0\ 1\ 1\ 0 \\ 0\ 0\ 0\ 0\ 1\ 1\ 0 \end{pmatrix} = 0$$

12. This way it will solve the third erasure as well and it will get the received code word which will be

$$\text{Received code word } (r_1) = [1\ 0\ 0\ 0\ 1\ 1\ 0]$$

13. It can now compare the actual code word sent by the user with the solved received erasure for our evaluation purpose.

$$\text{Code word } (v_1) = [1\ 0\ 0\ 0\ 1\ 1\ 0] \text{ and}$$
$$\text{Received code word } (r_1) = [1\ 0\ 0\ 0\ 1\ 1\ 0]$$

14. From above two code words, it can say that we have correctly solved all the three erasure.

The Gaussian elimination decoding depends on the usage of the Gaussian elimination method or also called as Gaussian reduction method, to decode the received LDPC code word with erasure. In this method after the decoder has received the code word with the erasure we try to obtain the three equations by the principle,

$$\text{Parity check Matrix (G)} * \text{Transpose of received code word } (r^T) = 0.$$

Then by applying column transformations and row transformations on the received matrix and try to form an identity matrix at the right hand side of the matrix. After

doing this step it will have only one unknown in each row. Then it can simply do binary additions for each row and find the value of the erasure in each row. This is the most efficient way of decoding.

1. Firstly it will check for erasure in the received code word (r1) = [e 0 0 e 1 e 0]. It can see that it has erasure in the 1st, 4th and the 6th position.

2. Now it will multiply the parity check matrix and the received code word,

3. Parity check Matrix (G) * Transpose of received code word (rT) = 0

Where,

$$\text{Parity check Matrix (H)} = \begin{pmatrix} 1\,0\,0\,1\,0\,1\,1 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \end{pmatrix}$$

Received code word (r_1) = [e 0 0 e 1 e 0]

$$\begin{pmatrix} 1\,0\,0\,1\,0\,1\,1 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \end{pmatrix} \begin{pmatrix} e \\ 0 \\ 0 \\ e \\ 1 \\ e \\ 0 \end{pmatrix} * = 0$$

$$\begin{pmatrix} e\,0\,0\,e\,0\,e\,0 \\ 0\,0\,0\,e\,1\,e\,0 \\ 0\,0\,0\,0\,1\,e\,0 \end{pmatrix} = 0$$

4. After obtaining the matrix, it will now apply row transformations on the matrix so that all the erasures are on the right hand side of the matrix.

$$\begin{pmatrix} 0\,0\,0\,0\,e\,e\,e \\ 0\,0\,1\,0\,0\,e\,e \\ 0\,0\,1\,0\,0\,0\,e \end{pmatrix}$$

5. After obtaining the matrix it will now apply row transformations in such a way that it obtains an identity matrix at the right hand side and the erasures are at the diagonal of that identity matrix.

6. First it will subtract R2 from R1 i.e. R1 – R2, after doing this it will achieve one erasure in the first equation.

$$\begin{pmatrix} 0\,0\,1\,0\,e\,0\,0 \\ 0\,0\,1\,0\,0\,e\,e \\ 0\,0\,1\,0\,0\,0\,e \end{pmatrix}$$

7. Then it will subtract R3 from R2 i.e. R2 – R3, after doing this it will achieve one erasure in the second equation.

$$\begin{pmatrix} 0\,0\,1\,0\,e\,0\,0 \\ 0\,0\,0\,0\,0\,e\,0 \\ 0\,0\,1\,0\,0\,0\,e \end{pmatrix}$$

8. Now the iterative decoding step will be applied once and binary addition will be checked for all the three equations at once and substitute the value of erasure appropriately.

9. For the first erasure the total value of binary addition is 1 so the erasure should be 1. Similarly, the value of second and third erasure will be 0 and 1 respectively.

Received code word (r_1) = [1 0 0 0 1 1 0]

10. It can now compare the actual code word sent by the user with the solved received erasure for our evaluation purpose.

Code word (v1) = [1 0 0 0 1 1 0] and

Received code word (r1) = [1 0 0 0 1 1 0]

11. From above two code words, it can say that we have correctly solved all the three erasure.

4 Results and Discussion

As per Shannon's seminal 1948 paper, capacity C of a Binary erasure channel is an upper bound on the rate *R* of a code that achieves randomly good error control. To

simplify, a reliable code must have $R <= C$. Shannon (1948). So, it the value of R is less than or equal to C then we can solve the erasures in the received code word else it's difficult to solve the received code word. From both the decoding methods explained, we can say that the iterative decoding is a fast method to decode the code word but takes long time as number of iterations is more. On the other hand, the Gaussian elimination method (Liener, 2005) is a slow process but it can be more efficient than the iterative decoding. Even the number of iteration is only once so the time taken for this method will be very less.

5 Conclusion

The main objective of this study is to solve the erasure of the lost packets that were erased during the transmission of the code word in the noisy network. To solve the error of the erased packets a powerful error correcting codes called Low-density parity check (LDPC) codes. It is in the binary erasure channel that the error is introduced in the form of erasing the bits from the actual code word. The study of Binary erasure channel is done to learn about the capacity of the channel and the transmission of the bits. The study of LDPC is done to apply this coding on to the networks to solve the erased bits at the received end. To perform this, a significant level of understanding was achieved and implemented using the knowledge in the C programming language.

Looking at the results, the LDPC code encoding & decoding codes are managed to solve the erasure occurred in the received code word at the receiver end. In the encoding process good results were generated successfully by using the generator matrix. The systematic matrix generation helped in encoding the information sequence simper than encoding with the general matrix. During the transmission of the code word through the binary erasure channel, the channel gets affected by noise to create error in the form of erasure denoted by 'e'.

In decoding process, the erased bits is constructed by applying the equation $H. r^T = 0$. There are two decoding process used to decode the received code word. First one is Iterative decoding, where the received code word is multiplied with the parity check matrix. After the multiplication we receive three equations, which are solved with the help of binary additions and iterations to solve the erasure. This process is fast but it's not accurate and also do not work well with erasure in some position.

The second decoding method is Gaussian elimination method that is more accurate than the iterative decoding. Although the process is slow, it works for more probabilities then the iterative decoding. In Gaussian elimination, the received code word is multiplied with the parity check matrix. After receiving the three equations, the erasures are shifted to the right hand side of the obtained matrix and an identity matrix is formed with erasures at the diagonal position. The erasures are then solved with only one iteration of binary addition.

The program developed cannot take the input through a file, which will be helpful in solving the erasure in the sparse matrix. Also the second method of decoding process, the Gaussian elimination process can be implemented as a C program for both the hamming matrix and the sparse matrix.

6 References

Gallager, R. (1963), "Low-Density Parity-Check Codes", *MIT Press*, Cambridge, MA.

Liener, B.M.J. (2005) "LDPC Codes – a brief Tutorial", Available at: http://www.engr.uvic.ca/~masoudg/upload/ldpc-a%20brief%20tutorial.pdf [Accessed Date: 18th august 2010]

Shannon, CE. (1948), "The Mathematical Theory of Communication", *The Bell System Technical Journal*, 27, pp. 379–423, 623–656.

Shokrollahi, A. (2003), "LDPC codes: An Introduction", *Digital Foundation, Inc.* Available at: *www.ics.uci.edu/~welling/teaching/ICS279/LPCD.pdf [Accessed Date: 28th January 2010]*.