People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

Amar Thelidji University - Laghouat

FACULTY OF TECHNOLOGIES

DEPARTEMENT OF ELECTRONIC

MASTER DESERTATION

Presented by:

BENAISSA Mourad **&** ***TEBIB Billal***

DOMAIN : Science and Technology

FIELD : Telecommunicaton

OPTION : Telecommunication System

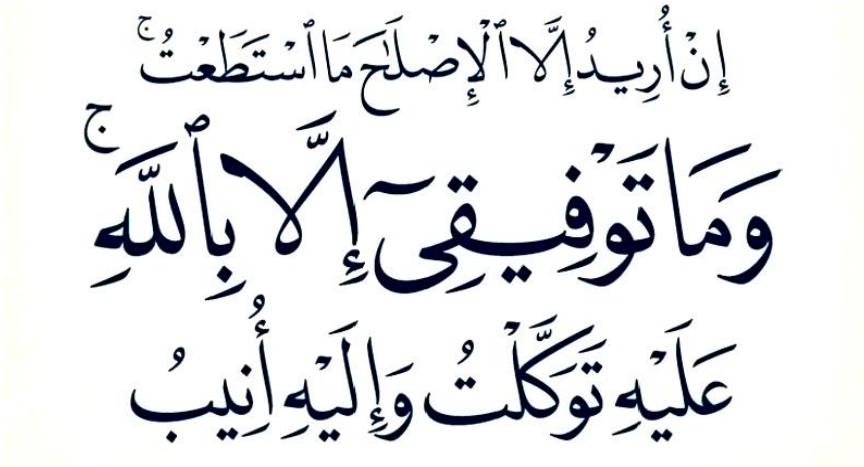
Theme

Study of low density parity-check LDPC codes

Defense jury :

Full Name	Grade	Quality
Challali Safouane	MCA	Supervising
Biran abde-elkader	MCA	President
Reggab Mourad	MCA	Examiner

University year : 2021/2022



سورة هود – 88

ان الحمد لله نحمده سبحانه وتعالى حمدا يليق بجلال وجهه وعظيم سلطانه، فقد سدد الخطى وشرح الصدر ويسر الأمر، فلله الحمد كله واليه يعود الفضل كله والصلاة والسلام على أشرف المرسلين سيدنا محمد صلى الله عليه وسلم.

THANKS

All my praises and thanks to ALLAH the almighty, the clement and merciful, who endowed me with all the faculties and skills and guided me in my works and enlightened my way to carry out this research work.

To my teacher and my supervisor Mr **"Chellali Safouane"**

I had the honor to be among your students and to benefit from your rich teaching.

Please receive my thanks for the great honor you have given me to accept the supervision of this work.

To the members of the jury

Gentlemen of the jury, you do us a great honor by accepting to judge this work.

I would like to warmly thank all my relatives and all those who, from near or far, have brought me their solicitudes to accomplish this work.

Dedication

To the one who taught me success and patience... To the one who taught me to give without waiting... " father ".

To the one who taught me and suffered hardships for me...to whose supplication was one of the reasons for my progress and success to...my "mother".

To all my humble family, wherever they may be.

To my "friends", my "companions" from inside and outside the university.

To the honorable professor, Dr "***safouane chellali***", to my honorable professors who enlightened our paths with science and knowledge.

To everyone who is convinced of an idea and calls for it and works to achieve it, and to ask God for success.

I dedicate this humble work to you in the desire to accept it, God willing.

.....

Billal

Dedication

It is with deep gratitude and sincere words, that I dedicate this modest work of end of studies

To dearest parents, ***BELOUAFA*** *&* ***AICHA****, that may Allah prolongs them life, which have always been them for me,*

I hope that one day I will be able to give back some of what they have done for me, and that God will bless and forgive them.

*To my brother "****Ibrahim****" and my dear sisters*

To all my family ***BENAISSA****.*

To those l've had the pleasure of knowing, may dear friends : Ahmed chaib "Rahimah allah", Billal, Khaled, Mohamed, Rabeh, Khatir, Halima and Wissam.

To all my colleagues of the Telecommunication system promotion

For their sincere friendship and trust, and to whom I owe my gratitude and attachment.

To all of you who have contributed in any way to my success.
To all my other friends,
To all those I love and those who love me.

Moura

Abstract

LDPC codes are currently one of the hottest topics in coding theory they were invented in the early 1960s and have made an incredible comeback in recent years. LDPC codes, unlike many other types of codes, already have very fast encoding and decoding algorithms.

The question is how to design the codes so that these algorithms can recover the original code word even in the presence of lot of noise.

The design problem can now be solved using new analytic and combinatorial tools. As a result, LDPC codes are not only appealing from a theoretical standpoint, but also ideal for practical applications.

In this study, we will provide a brief history of LDPC codes as well as the methods used to analyze and design them.

Résumé

Les codes LDPC sont actuellement des sujets les plus brûlants de la théorie du codage, ils sont inventés au début des années 1960 et ont fait un retour incroyable ces dernières années. Les codes LDPC, contrairement à de nombreux autres types de codes, disposent déjà d'algorithmes de codage et de décodage très rapides.

La question est de savoir comment concevoir les codes pour que ces algorithmes puissent récupérer le mot de code d'origine même en présence de beaucoup de bruit.

Le problème de conception peut désormais être résolu à l'aide de nouveaux outils analytiques et combinatoires. En conséquence, les codes LDPC sont non seulement attrayants d'un point de vue théorique, mais également idéaux pour les applications pratiques. Dans cette étudier, nous fournirons un bref historique des codes LDPC ainsi que les méthodes utilisées pour les analyser et les concevoir.

ملخص

تعد رموز LDPC حاليًا واحدة من أهم الموضوعات في نظرية الترميز التي تم اختراعها في أوائل الستينيات وعادت بشكل لا يصدق في السنوات الأخيرة. تحتوي رموز LDPC على عكس العديد من أنواع الرموز الأخرى بالفعل على خوارزميات تشفير وفك تشفير سريعة جدًا.

السؤال هو كيفية تصميم الرموز بحيث يمكن لهذه الخوارزميات استعادة كلمة المرور الأصلية حتى في وجود الكثير من الضوضاء.

يمكن الآن حل مشكلة التصميم باستخدام أدوات تحليلية وتوافقية جديدة. ونتيجة لذلك، فإن رموز LDPC ليست جذابة فقط من الناحية النظرية، ولكنها أيضًا مثالية للتطبيقات العملية.

في هذه المذكرة، سوف نقدم تاريخًا موجزًا لرموز LDPC بالإضافة إلى الطرق المستخدمة لتحليلها وتصميمها

Glossary

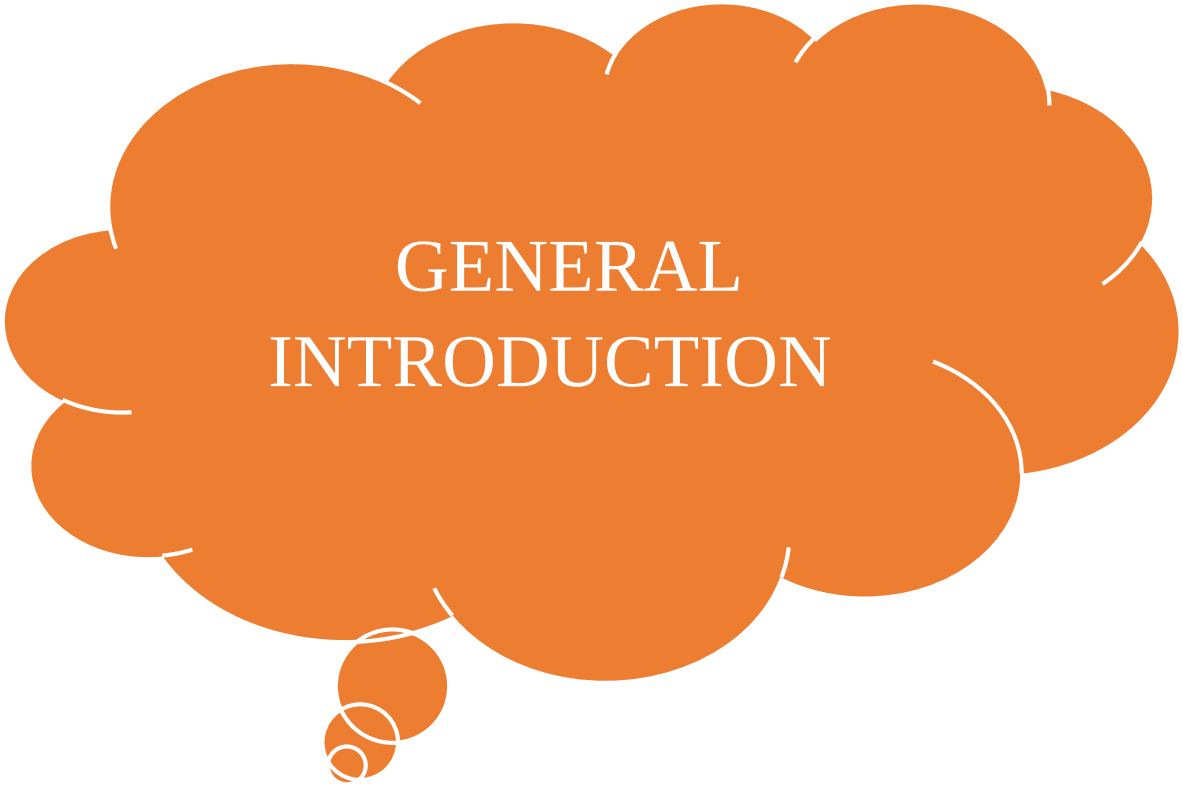
ARQ	Automatic Response Requested
APP	Decoding based on Posterior Probability
AWGN	Additive White Gaussian Noise
BER	Bit Error rate
BF	Bit-Flipping
BSC	Binary symmetric channel
BP	Belief Propagation
CRC	Cyclic Redundancy Check
CPFSK	Continuous Phase Frequency Shift Keying
CPM	Continuous phase modulation
DSP	Digital Signal Processor
DVB-S2	Digital Video Broadcasting - Satellite - Second Generation
FEC	Far word Errer Correction
FER	Frame Error Rate
IEEE	Institute of Electrical and Electronics Engineers
JPEG	Joint Photographic Experts Group
LDPC	Low Density Parity Check
LDPC-QC	Low Density Parity Check Quasi-cyclic
LLR	Logarithmique Likelihood Ration
MLG	Majority logic decoding
MSK	Minimum Shift Keying
MPEG	Moving Picture Coding Expert Group
RII	Remote Ignition Interrupter
PCM	Pulse-Code Modulation
PSK	Shift Keying
W-CDMA	Wide Band Code Division Multiple Access

List of Figures

List of table

Summary

Chapter II : [LDPC codes]


GENERAL
INTRODUCTION

General introduction

The current societies have become different from the rest of the other eras, and in terms of science in particular, everything is in line with telecommunications and information . Digital communications have changed significantly over the past two decades. Today, in most cases, information is transmitted in digital form, whether it is wired media (optical fiber) or radio, cellular or wireless local area networks, or information storage systems. This development is triggered and supported by a strong need for reliable, fast, and efficient transmission and processing of various information (voice, data, or image processing). And this phenomenon exists in every field (military, government, commercial, etc.).In addition, communications are combined with computer-aided data processing techniques.

The elements of a communications system consist of analog /digital transformation of information, redundancy reduction, encryption, and error protection. In analog transmission, the signal is transmitted as it is, which can cause a loss of useful information at the receiving end due to interference and noise on the transmission channel. In addition, the amount of information transmitted is very large and the transmission is done in circuits of great complexity and therefore slow. Digital communications have made it possible to counteract these disadvantages. By applying digital signal processing methods, it is possible to protect the signal more effectively. The challenges are high-speed, real-time, low-error, secure transmission with low energy consumption. In a transmission system, digital signal processing can be applied several times.

Digital channel coding converts sequences of useful information into discrete coded sequences, called code words. Code words can be binary or non-binary. This note only examines binary code. The challenge in encoding digital information is to recover as little as possible at the receiver from the noise of the transmission channel. The receiver converts the encoded received sequence into an estimated information sequence. The sequence should ideally be the same discrete sequence of transmissions, but in practice, it is subject to transmission errors. The discrete sequence is then converted to a continuous sequence and passed to the output.

In 1948, Shannon [1] demonstrated that there is a limit to the information rate transmitted in the presence of noise, called <<channel capacity>>, but did not explain the means of approaching it. From this point on, researchers began to investigate different methods of constructing error-correcting codes and minimizing decoding errors as much as possible.

Even if the asymptotic nature of this limit leaves no hope of reaching it, the information theory community has sought to find ways of getting as close as possible to this famous limit (channel capacity).

Therefore, two families were imposed: linear block codes and convolutional codes achieve good transmission results without errors. These two families have excellent performances, but this revolution has opened up many avenues of research in the field of error-correcting coding and more generally in digital communication systems. This advance has resulted in the rediscovery of GALLAGER codes, also known as LDPC (Low-Density Parity Check) codes, which at that time were not very popular. A commonly accepted reason to explain this oversight is the difficulty at the time to design efficient circuits to process the writing algorithms. In 1995, encouraged by the context that followed the discovery of the turbo principle, MACKEY rediscovered the GALLAGER codes. Thereafter, many works were interested in these two families of codes: Turbo-codes and LDPC codes, and more generally in the application of the iterative principle in a digital communication system, and this will be demonstrated in this study.

This consists of two chapters. The details of each are described below:

Chapter I is devoted to the introduction to the design of a digital transmission chain which we will describe with each basic element starting from the message source to the receiver.

Chapter II is based on LDPC codes which are designed from linear block codes with their encoding and decoding based on iterative decoding.

CHAPTER I

I.1. Introduction

Man has always needed to communicate. In 1794s, CLAUDE CHAPPIE built a telegraph between Paris and Lille. It was then possible to transmit a message over a long distance. Then, thanks to electricity, the telegraph was perfected communication was established in the form of coded messages. The years 1832s and 1876s saw important inventions such as the Morse code thanks to SAMUEL MORSE and the telephone thanks to GRAHAM BELL where the voice could be transmitted [2].

Long-distance communication is now possible with a simple pair of copper wires and a power source. Today, thousands of simultaneous conversations can be transmitted at any distance.

Digital transmission systems carry information between a source and a recipient using a physical medium such as cable, fiber optics, propagation over a radio channel, etc. The signals carried may be either directly digital or analog (speech, image, etc.) but converted into digital form. The task of the transmission system is to carry the signal from the source to the recipient as reliably as possible.

The synoptic diagram of a digital transmission system is given in *figure I.1* where we limit ourselves to the basic functions. The source transmits a digital message in the form of binary elements. The encoder generally encompasses two fundamentally different functions: the first, called source coding, associates a suitable physical medium with the abstract elements emitted by the source, and the second, called channel coding, consists in introducing redundancy into the emitted signal to protect it against noise and interferers present on the transmission channel. The transmission channel includes the transmitter, the physical transmission medium on which the signal will be transmitted, and the receiver. Finally, on the receiver side, the source decoding and channel decoding functions are the respective inverses of the source coding and channel coding functions on the transmitter side.

I.2. The digital transmission chain

The block diagram of a digital transmission system is given in *figure I.1* we limit ourselves to the basic functions:

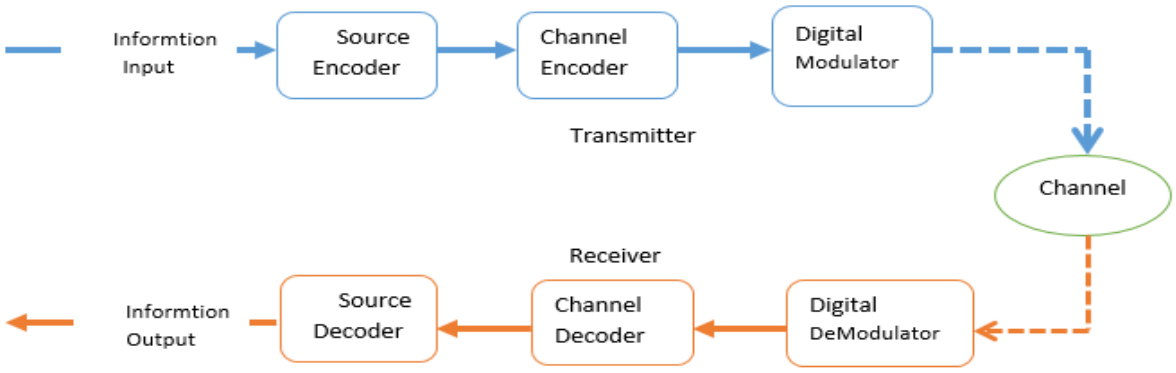


Figure I.1: General diagram of a digital transmission chain.

When detailing the sending part, the following blocks can be distinguished:

- **Information Input**

The source can be an analog signal. Example: A Sound signal

- **Source Encoder**

The source encoder compresses the data into a minimum number of bits. This process helps in the effective utilization of the bandwidth. It removes the redundant bits

Example: unnecessaryexcessbits, i.e.

- **Channel Encoder**

The channel encoder does the coding for error correction. During the transmission of the signal, due to the noise in the channel, the signal may get altered, and hence to avoid this, the channel encoder adds some redundant bits to the transmitted data. These are the error-correcting bits.

- **Digital Modulator**

The signal to be transmitted is modulated here by a carrier. The signal is also converted to analog from the digital sequence, to make it travel through the channel or medium.

- **Channel**

The channel or a medium, allows the analog signal to transmit from the transmitter end to the receiver end.

- **Digital Demodulator**

This is the first step at the receiver end. The received signal is demodulated as well as converted again from analog to digital. The signal gets reconstructed here.

- **Channel Decoder**

The channel decoder, after detecting the sequence, does some error corrections. The distortions which might occur during the transmission, are corrected by adding some redundant bits. This addition of bits helps in the complete recovery of the original signal.

- **Source Decoder**

The resultant signal is once again digitized by sampling and quantizing so that the pure digital output is obtained without the loss of information. The source decoder recreates the source output.

- **Output Signal**

This is the output that is produced after the whole process. Example − the sound signal received.

I.3. Coding

I.3.1. Source coding

Source coding aims to represent the information to be transmitted in the most compact digital form possible see *figure I.2*, by eliminating the redundancy contained in the source messages. On the one hand to digitize the data if they are analog (sound, image, video), on the other hand, to compress the digital data, to reduce the transmission rate or the storage volume[3].

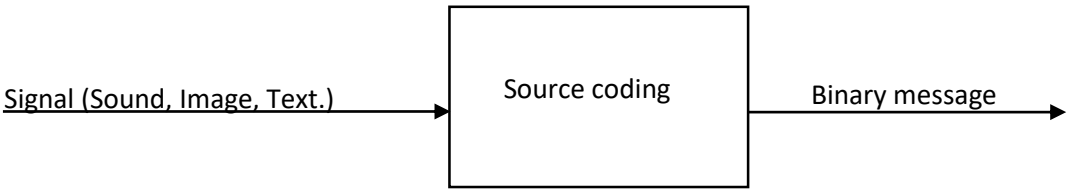


Figure I.2: Source coding

We will distinguish two types of compression:

- Lossless, or conservative, compression allows the original data to be recovered exactly after decompression. Ex: zip compression.

- Lossy or non-conservative, compression leads to a loss of information. It is used for objects intended to be perceived by a human, ensuring that the loss of information is not perceptible.

This is the principle on which the perceptual encoders MPEG (audio and video) and JPEG (image) is based. After digitization and coding,the digital message source is characterized by its bit rate D. defined as the number of bits transmitted per unit time.

The bit rate is equal to:

$$D = \frac{1}{T} \quad \left(\frac{bit}{s}\right) \qquad \textbf{(I.1)}$$

Where T is the duration of one bit.

The digitization of a signal is broken down into two successive operations, sampling, and quantization:

- **Sampling:** an operation performed on the signal to be transmitted to carry out the "analog/digital" conversion. It consists of substituting, for the original signal, a series of instantaneous values taken from the signal and regularly spaced out in time at precise, regularly spaced instants. On reception, a digital RII filter is used to recover the original signal. *figure (1.3).*
- **Quantization:** to reconstitute the signal on reception, it is not necessary to transmit these pulses directly, it is sufficient to transmit information characterizing the amplitude of each of them. This operation consists of matching each sample amplitude with the closest amplitude of a discrete sequence of "standards" called "levels".

Each level of the quantization scale is characterized by a binary number.

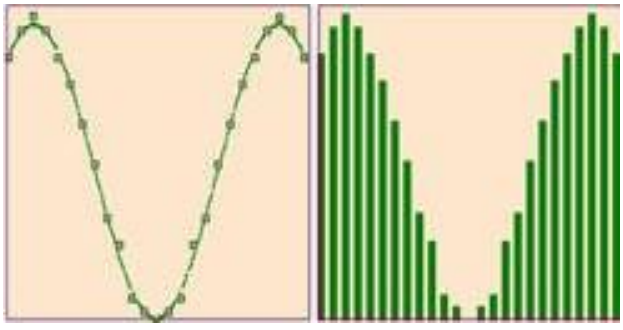


Figure I.3: Signal sampling and quantification.

I.3.2. Channel coding

Channel coding, also known as error-correcting coding, consists of protecting the binary messages provided by the source coding by introducing information redundancy. Bits are added to the original bits, which depend on them. This redundancy can enable error detection and possibly error correction [4].

a) Causes of transmission errors

The causes of errors are numerous and depend mainly on:

- Transmission lines used.

- Type of modulation and coding used.

- Thermal noise due to electronic components can also cause errors if its level becomes quantifiable.

- Pulse noise, is an important source of error since a pulse lasting about ten milliseconds can induce several bits in error and the number of bits in error increases with the transmission speed.

b) Method of correcting transmission errors

These noises produce a large number of clustered errors and therefore error detection and correction systems have been developed to protect the integrity of the transmitted binary information. These systems are based on additional coding of the information at transmission and analysis of the message at reception.

The receiver can distinguish two strategies in case of error detection:

- Either a request to retransmit the erroneous bits: this is the ARQ strategy.
- Or a correction by channel decoding, known as FEC.

We are interested in the first correction strategy (ARQ) See *figure (I.4).*

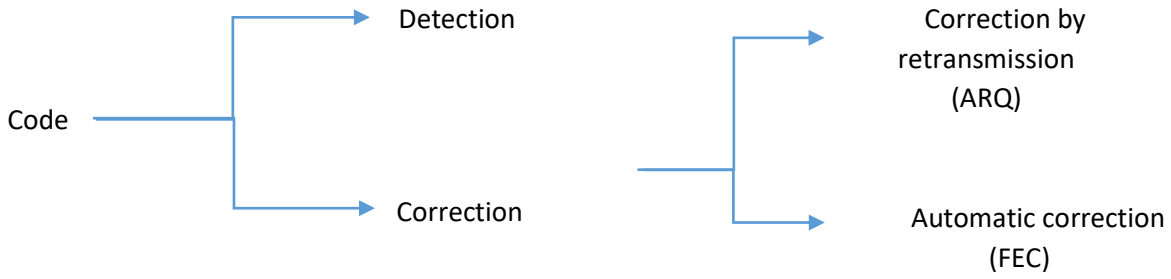


Figure I.4: Error correction method

Traditionally, two types of codes are distinguished, block and convolutional codes. Our study will focus on the Hamming block code.

I.3.2.1. Introduction to block codes HAMMING

The information from the source is put into fixed-length frames, which will be transmitted: this is the message. The channel coding takes this message and makes it into a codeword.

The message consists of k characters, i.e. 2^k possible messages. The codeword

The code word used will also have a fixed length of n characters, i.e. 2^n possible code-words. With $n > k$ there will therefore be n - k characters in the code word which are redundant and will be used to handle any errors.

Moreover, $2^n > 2^k$ so a certain number of codewords do not correspond to a message but only to transmission errors. [5] We thus speak of a block code C (n, k) and the coding ratio or code efficiency R defined by:

$$R = \frac{k}{n} \qquad \textbf{(I.2)}$$

I.3.2.2. Code weight

The weight of a codeword is by definition the number of non-zero characters contained in that word.

Example:

1011001011	Weight =6
0011010100	Weight =4
0000000000	Weight =null

Table I.1. Example of different code weights

I.3.2.3. Hamming distance

The Hamming distance is defined as the number of different bits between two words. It is denoted $dh\ (C, R)$ with C, R two different code words.

To maximize the detection (correction) capability of the code, the Hamming distance between the code words should be as large as possible. The objective is therefore to maximize the minimum distance between codewords, using the linearity property, which implies that the difference between two codewords is one codeword [6].If a code is of minimum distance:

- It will be possible to detect all errors of weight less than or equal to d_{min} - 1.

- We can correct t errors if we can associate (without risk of error) the codeword to erroneous receive the word; this can be done if t is strictly less than $d_{min}/2$.

In summary, if s denotes the number of detectable errors, and t the number of correctable errors, the link to the minimum distance d_{min} is as follows:

$$d_{min} = s + 1 \quad \textbf{(I.3)}$$

$$d_{min} = 2t + 1 \quad \textbf{(I.4)}$$

I.3.2.4. generating a systematic linear block code

We will generate a systematic linear block codeword C_m from a message X_m such that:

$$X_m = [m_0\ m_1\ m_2\ \dots\ \dots\ \dots\ m_k - 1]$$

k Message characters

$$C_m = [R_0\ R_1\ \dots\ \dots\ \dots\ \dots\ \dots\ .. R_n - k - 1\ m_0 m_1\ \dots\ \dots\ \dots\ \dots\ \dots\ .. m_k - 1]$$

but $C_m = [\ R_m\ \ X_m]$ or R_m contains the control characters also called redundancy characters

I.3.2.5. Codeword generation

A- Codeword generation matrix

A matrix which generates the code word C_m from the message X_m is called a generation matrix, denoted G, such that:

$$C_m = G \times X_m \quad \textbf{(I.5)}$$

Turning to systematic codes, the matrix G is of the following form:

$$G = [P_{(k,n-k)}\ \ I_{(k,k)}] \quad \textbf{(I.6)}$$

B- non-systematic code

A non-systematic code noted: $G = [P\ M]$ where the matrix M is a matrix that shuffles the bits of the message to encrypt it. We can of course reduce to a systematic code by combining the rows to gather to involve the matrix I_k. Any block code can thus be reduced to the study of a systematic code. The essential part of the G matrix is therefore the P matrix called the parity matrix [7].

C- Encoder design principle

The principle of the technical implementation is therefore simple, it is sufficient to have two shift registers and an inverter (electronic switch), as shown in figure (I.5).

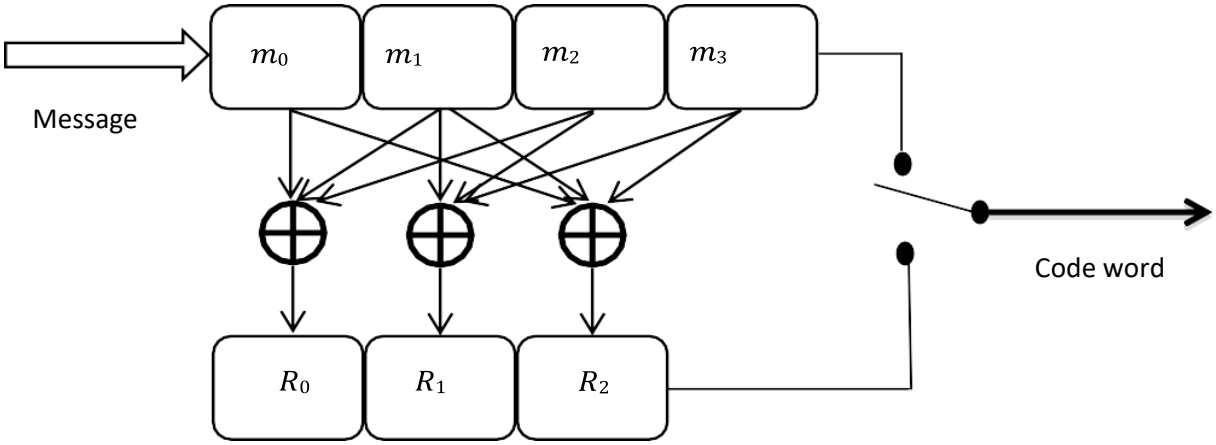


Figure I.5: Principle of the encoder.

- each parity bit is therefore expressed as $R_i = \sum_{j=1}^{k} m_j p_{ji} \bmod 2$
- In binary the P_j,i ∈ {0 ; 1}.
- The P_i are obtained by simple binary addition. See table (1.2)

⊕	0	1
0	0	1
1	1	0

Table I.2. Binary addition

- We take as an example a code $C(7,4)$:
- $G=\begin{bmatrix} 1\,0\,1\,1\,0\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,0\,0\,0\,1\,0 \end{bmatrix} \Rightarrow \begin{cases} R_0 = m_0 + m_1 + m_2 \\ R_1 = m_1 + m_2 + m_3 \\ R_2 = m_0 + m_1 + m_3 \end{cases}$

D- Parity control matrix

Let a systematic code of generating matrix $G\ [P_{(k,n-k)}\ I_k]$, the control matrix H will have the following form:

$$H = [I_{n-k}\ p^T] \quad \textbf{(I.7)}$$

The relation (1.8) makes it possible to determine if a word of n bits noted r belongs or not to the code word, the idea is to define the set of words n bits orthogonal to the code word and to check if r is orthogonal to this set [4].

$$G \times H^T = 0 \quad \textbf{(I.8)}$$

The relationship that controls whether a word belongs to the code or not is given as follows:

$$C \times H^T = 0 \quad \textbf{(I.9)}$$

With c code word.

Example :

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

E- Syndrome

Consider the case where the sender transmits the code word X_m and the receiver receives the word C_m. We call syndrome, the vector :

$$S = C_m \times H^T \quad \textbf{(I.10)}$$

We can also write :

$$S = G \times X_m \times H^T$$

For C_m to to be a code word, the syndrome must be zero.

If the received code mode C_m is tainted with an error, the received Code will be the sum of the transmitted code and the error (equation (I.11).)

$$Y_m = C_m + E_m \quad \textbf{(I.11)}$$

Where Y_m is the error-ridden code word. The syndrome will be deduced by relation (I.12):

$$S = Y_m \times H^T \quad \textbf{(I.12)}$$

Let us take the case of a single error on the i^{th} bit of the error word. The syndrome is then identical to the i^{th} row of H^T (or the ie column of H).

It is possible to correct the error if all columns of H are distinct. The decoding strategy is then very simple: we compare the syndrome with the columns of H. If it is identical to one of them, we correct the corresponding bit of the received word [8].

I.4. Modulation

I.4.1. Introduction

A transmission with prior modification of the spectrum of the signal to be transmitted is called transposed band transmission or modulation. It generally uses two signals:

- The analog or digital message, called the modulating signal or message (LF)
- A carrier or sampling signal (HF) Modulation can be:
- Either a more or less direct transposition of the message spectrum to HF (amplitude modulation, frequency modulation, phase modulation).
- On the other hand, a radical modification of the signal itself using digital means, notably sampling (pulse modulation).
- Alternatively, a combination of the two previous techniques (Wide Band Code Division Multiple Access - W-CDMA).

Example:

- Shift keying modulation.
- Pulse modulation and PCM coding.
- CPM continuous phase modulation.

Now, we will study CPM

I.4.2. General Study of CPM

Continuous phase modulations (CPM) are a family of constant envelope phase modulations. They were introduced in the early 1980s by John B. Anderson and Carl- Erik Sandberg [6]. In addition to a constant envelope, these modulations have other properties that differentiate them from classical linear modulations. These properties include non-linearity with respect to the transmitted sequence and the lattice modeling of CPM signals. Modulations in which the phase of the complex envelope $z\ (t)$ evolves continuously with time but is not constant are called continuous phase

modulations, CPM. Ensuring the continuity of the phase makes it possible to limit the spectral occupation of the modulated signal.

The general expression for the phase $\varphi\ (t)$ of signal $\varphi\ (t)$, in the interval, is $[n^T, (n+\ 1)\ T]$, is as follows:

$$\varphi(t) = 2\pi\ \sum_{i=-\infty}^{n} a_k\ b_{kq(t-kt)} \qquad \textbf{(I.13)}$$

Or the sequence (a_k) the sequence of M-ary amplitudes associated with successive symbols. These symbols are uniformly distributed. The sequence (b_k) is the sequence of modulation indices. Generally, it is constant and the modulation index b is fixed. It can cyclically, and is referred to as multi-index modulation. The elementary pulse $q\ (t)$ is a normalized continuous waveform, which is often the integral of a function $q(t)$.

$$q(t) = \int_{-\infty}^{t} g(r)\ d_r \qquad \textbf{(I.14)}$$

The function $2\pi\ b\ q(t)$ is called the phase elementary pulse, and it is noted hereafter $\varphi\ (t)$. The function $q\ (t)$ is called the frequency elementary pulse.

The most commonly used CPM modulations are described in the following sections. They are the CPFSK continuous phase frequency modulations, with in particular the MSK modulations, and the binary GMSK modulations. These modulations have a constant envelope [9].

- CPFSK is a continuous phase frequency hopping modulation, which associates each symbol with a frequency. The frequency change is made while maintaining phase continuity.
- MSK is a CPFSK modulation with a modulation index, its name comes from the use of the minimum deviation to obtain orthogonal frequencies
- GMSK modulation is an MSK modulation to which a Gaussian low-pass filter has been added to reduce the spectral occupancy of the modulated signal. It is therefore a continuous phase frequency modulation of the index .

I.5. Transmission channel

I.5.1. Definition

Before any transmission chain is designed, and in particular the selection of the waveform, the nature, and properties of the channel used must be studied. Noise strength, channel type, and stationarity are parameters that must be known a priori to make an effective choice of the waveform. This knowledge then allows the capacity of the channel to be evaluated given the waveform adopted. From an operator's point of view, information on propagation conditions is essential for an initial assessment of the system's capacity and the quality and nature of the service it can offer.

The transmission channel represents the link between the transmitter and the receiver and can be of different types depending on the type of data it carries. The transmission channel is characterized by its capacity and bandwidth.

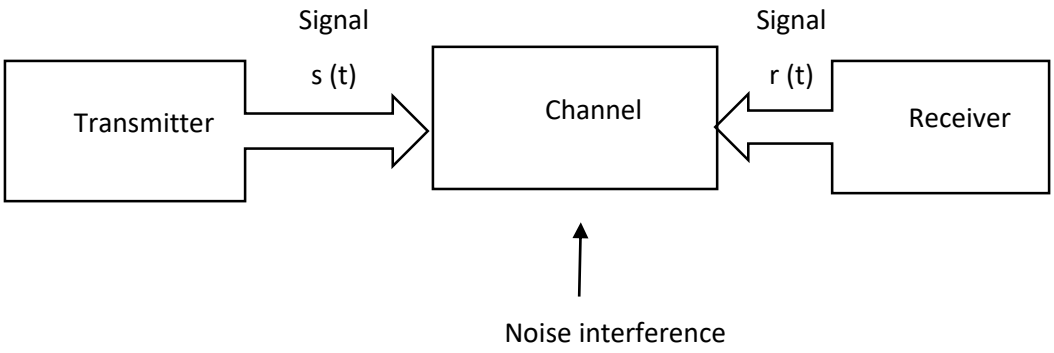


Figure I.6. Transmission channel.

The sources of interference are diverse and depend mainly on the environment in which the transmission channel is located (figure (I.6)). The main types of noise are galactic noise between 20 MHz and 200 MHz due to radiation from various energy sources in space; atmospheric noise up to 20 MHz induced by thunderbolts, industrial noise, urban noise, micro outages corresponding to short interruptions of the signal, phase jumps and flickers related to sudden variations in phase or slow variations caused by electrical power supplies; crosstalk when several links are routed through the same cable [9].

I.5.2. Capacity of a noisy digital channel

A formula specifies the capacity of the transmission channel for a digital signal passing through a real, and therefore noisy, line

$$D = B \log_2(1 + {}^{S}/_{N}) \quad \textbf{(I.15)}$$

Or

- D : Bit rate ($bits/S$).
- B : Bandwidth (HZ).
- S/N : Signal to noise ratio (W/W).

There are several theoretical models of the transmission channel according to the most frequent types of errors:

I.5.3. Symmetric binary channel

The part of the link from the input of the transmitter to the output of the receiver can be considered as a binary channel, which is characterized by input and output of finite and equal bit streams (0, 1). The physical phenomena at work in the real channel are therefore left aside, to connect simply to the binary transformation between the input and the output.

$$P\left(\frac{R_0}{S_1}\right) = P\left(\frac{R_1}{S_0}\right) \quad \textbf{(I. 16)}$$

Where R_i and S_i represent the transmit and receive event of the binary element respectively

At the output of the transmission channel, the noisy signal is demodulated to obtain a sequence of binary elements. It is possible to represent all the parts modulation, transmission channel, and demodulation by a binary channel. The principle of a binary channel, represented in *figure (I.7)*, is to associate to each input bit a certain probability that the received bit is erroneous. This depends on the one hand on the errors generated by the propagation channel and on the other hand on the errors due to the demodulation of the signal.

A- Description of a binary channel

The simplest model is the binary symmetric channel (BSC). A BSC is defined by its probability of error, denoted P. The value of this probability, which depends on the channel and the modulation, corresponds to the (BER) obtained at the output of the demodulator. If we denote c and y as the input and output elements of the BSC, then the probability that the received symbol is erroneous is equal to the P equation (I.17) and conversely, the probability that the received symbol is correct is 1-P equation (I.18):

$$P_r(y = 0, x = 1) = P_r((y = 1, x = 0) = P \quad \textbf{(I.17)}$$

$$P_r(y = 0, x = 0) = P_r((y = 1, x = 0) = 1 - P \quad \textbf{(I.18)}$$

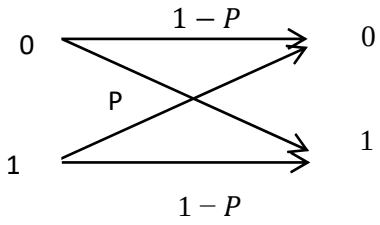


Figure I.7: Symmetric binary channel.

B- The Binary Erasure Channel

Erasure is a special type of error with a known location. The BEC transmits one of the two binary bits 0 and 1. However, an erasure «e» is produced when the receiver receives an unreliable bit. The output of the BEC channel consists of the symbols zero, one and e, as shown in *figure. I.8*. The BEC clears a bit with a probability , called the probability of the erasure channel. Thus, the channel transition probabilities for the BEC are as follows:

$$\begin{cases} \rho(y = 0 \,|x = 0) = 1 - \varepsilon \\ \rho(y = e \,|x = 0) = \varepsilon \\ \rho(y = 1 \,|x = 0) = 0 \\ \rho(y = 0 \,|x = 1) = 0 \\ \rho(y = e \,|x = 1) = \varepsilon \\ \rho(y = 1 \,|x = 1) = 1 - \varepsilon \end{cases}$$

Thus the transition matrix $P_{CH} = \begin{bmatrix} 1-\varepsilon & \varepsilon & 0 \\ 0 & \varepsilon & 1-\varepsilon \end{bmatrix}$

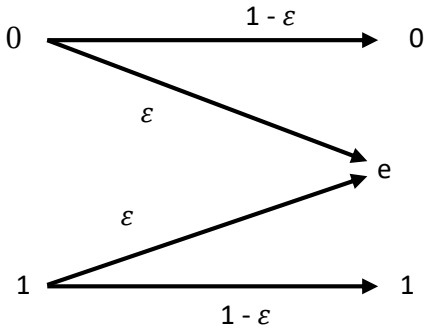


Figure.I.8. Binary erasure channel model

Note that the output random variable of the channel Y takes its values in a ternary alphabet $\{0,1,\varepsilon\}$, where ε represents erasure. This channel is often used as a model for networks. Erasure then models packet losses [10].

I.5.4. The Additive White Gaussian Noise Channel AWGN

the signal is degraded by white noise η, which has a constant spectral density and Gaussian amplitude distribution. A Gaussian amplitude distribution is also included. The channel that we take into consideration and that coding theorists most frequently employ A binary input channel is seen in *figure (I.9)*. It consists of the addition of a white Gaussian noise, of bilateral power spectral density DSP given by equation (I.19) [11].

$$S_b(f) = \frac{N_0}{2} \qquad \textbf{(I.19)}$$

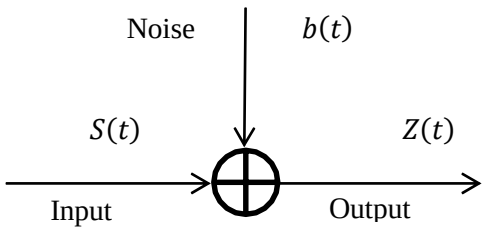


Figure I.9. The additive white Gaussian noise channel AWGN

With additive noise modelled as samples of a distribution [11].

The Gaussian distribution has a probability density function given by:

$$P_{df}(\eta) = \frac{1}{\sqrt{2\,\pi\,\sigma^2}} \exp(-\frac{\eta^2}{2\sigma^2}) \quad \textbf{(I.20)}$$

Where σ^2 is the variance of a Gaussian random process.

The binary input additive white Gaussian noise channel (BI-AWGN) can be described by the equation :

$$y_i = ax_i + \eta_i \quad \textbf{(I.21)}$$

Or $x_i \in \{-1,+1\} is\ the\ i^s$ symbol transmitted, y_i is the is received symbol η_i is the additive noise sampled from η and α is the attenuation.

When transmitting a binary code word on the BI-AWGN channel, the bits of the

Code word $c_i \in \{0,1\}$ can be mapped to the symbols $x_i \in \{-1,+1\}$ in one of two ways by one of the following two ways:$\{0 \to +1,1 \to -1\}$or $\{0 \to -1,1 \to +1\}$.

We will use the traditional convention$\{0 \to +1,1 \to -1\}$, because modulo-2 arithmetic over 0.1 corresponds directly to multiplication with 1.1

When this traditional mapping is used [12].

I.6. The recipient

We've just seen how the transmitter can convert the message into a signal and transmit it over the channel. The receiver, on the other hand, must extract the message from the signal received. It accomplishes this by taking a sequence of decisions on the transmitted message's subsequent symbols in the digital case, or by simple demodulation in the analog case.

Because of the discrepancy between the transmitted and received signals, the receiver's job is complicated. The use of a priori knowledge about the structure of the transmitted signal, as well as the conditions under which the transmission took place, are all tied to the receiver's proper operation.

The receiver incorporates circuits for amplification, frequency change, demodulation (for transmissions on a carrier wave), filtering, sampling, and decision making, with the goal of reconstructing the message broadcast by the source from the received signal [13] .The modulated signal can be brought back to baseband using the frequency change and demodulated. After that, the baseband signal is filtered and sampled at predetermined intervals. Finally, from the received samples, a decision circuit determines the value of the transmitted bits.

I.6. Conclusion

Information transmitted between a source and a recipient is always threatened by interference, disturbances, and transmission errors located along with the transmission medium.

Therefore, a theory of detection and correction of these transmission errors is produced by researchers to address these problems.

CHAPTER II

II.1. Introduction

Gallager invented Low Density Parity Check (LDPC) codes in 1962 [14]. These codes are based on pseudo-random low density parity check matrices. Due to the complexity and hardware means of its encoding and decoding, the code at that time did not attract enough interest in the research community. Theory of coding This monitoring will continue until the code and principles of turbo replication are introduced. For example, in 1996, MacKay and Neal rediscovered LDPC codes [15] and proposed using Pearl's Belief Propagation (BP) algorithm [16] to decode these codes. Then Luby introduced the irregular LDPC code [17] which is characterized by a parity check matrix with a different distribution of the number of elements, and the Null value is not uniform for each row and/or column.

This chapter is devoted to LDPC codes, where the first part introduces the general concepts of these of these codes as well as the construction methods of the parity matrix. The second part presents the decoding techniques.

II.2. Basic concepts [18]

Errors can occur in digital communications regardless of the channel used. To reduce these errors, coding is used during transmission.

There are two types of coding to consider:

- *Source encoder:* It is the analog-digital convention's role to represent the information message on a minimum number of bits (this allows for transmission on a minimum bandwidth).
- *Channel encoder:* Channel coding, also known as detector coding and/or error correction, is a function unique to digital transmissions that does not exist in analog transmission. Analog transmission equivalent this operation consists in appending binary elements known as redundancy elements to a digital information message in accordance with a given law. The channel decoder checks to see if this law is always followed during reception. If this is not the case, it detects a transmission error. This procedure aids in the enhancement of the transmitted signal's quality.

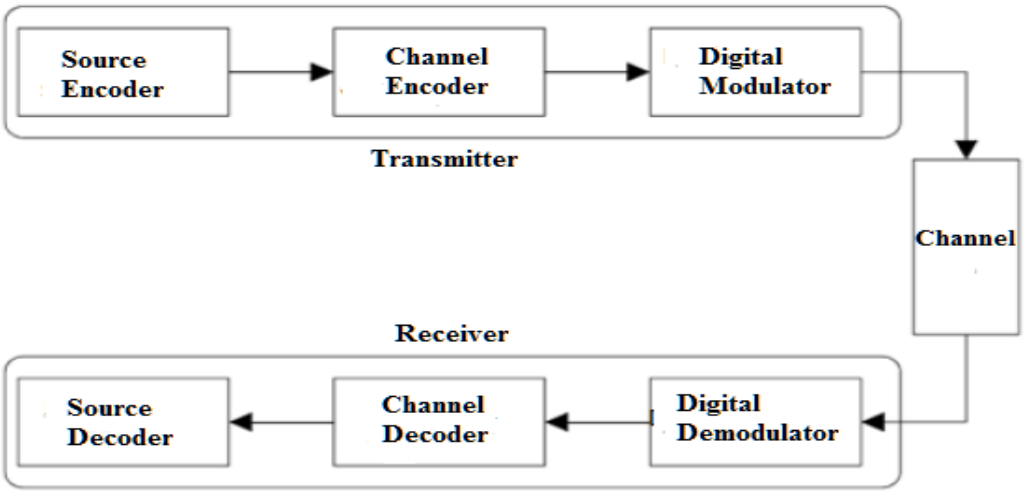


Figure II.1: Block diagram of a digital transmission chain.

II.2.1. Block codes

II.2.1.1. Definitions

The data block m of k symbols from the information source is associated with a block C, which is the code word of n symbols with n > k and (n-k) representing the parity bits.

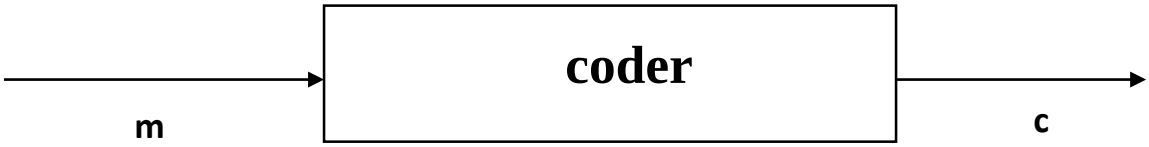


Figure II.2: Simplified diagram of a block encoder, which from an information word m of k bits, generates a code word C of n bits.

II.2.1.2. Generating matrix

The code word ***C*** assigns to each information block a matrix ***G*** of size $\boldsymbol{n} \times \boldsymbol{k}$ such that:

$$C = m \times \mathrm{G} \qquad \textbf{(II.1)}$$

The matrix G can be written in its simplest form:

$$G = [\, p \mid I \,] \qquad \textbf{(II.2)}$$

Where I : The identity matrix of dimension $k \times$ k.

P : The parity matrix of dimension k $\times$ (n $-$ k).

II.2.1.3. Parity check matrix

Each generating matrix of dimension (n × k) is associated with a matrix B of dimension (n − k × n) with rows orthogonal to those of H.

The matrix H can be written:

$$H = [P^T \quad I_{n-k}] \qquad \textbf{(II.3)}$$

II.2.1.4. Properties of block codes

a) Weight of the code

The weight of a code word is defined as the number of non-zero characters in the word.

Example: $C = [\,1\,0\,1\,0\,0\,1\,1\,0\,]$, for this code word the weight is w = 4.

b) Hamming distance

The Hamming distance between two code words is the number of bits by which they differ.

Example: $C1 = [\,1\,0\,1\,0\,0\,1\,1\,0\,]$

$C2 = [\,1\,0\,0\,1\,1\,0\,1\,1\,]$

The Hamming distance for this code C is also defined as:

$$d_{min} = \min\{Wk\} \qquad \textbf{(II.4)}$$

The code word " 0 " is not allowed.

II.2.1.5. Block codes in systematic form

The structure of the code word in a systematic form is shown in Figure II.3. In this form, a code word consists of k information bits followed by (n-k) parity bits.

K: bits of information	(N-K): parity bits

Figure II.3: Systematic form of a code word of a block code.

As a result, the following generating matrix can be used to define a linear block systematic code (n, k) [19]:

$$G = [I_{k\times k} \quad P_{k\times(n-k)}] \qquad \textbf{(II.5)}$$

This means that the information and redundancy bits are not mixed together.

II.2.1.6. Decoding of linear block codes

We can observed in Figure II.4 that following its emission through a noisy channel, a code note may be received containing errors. The resulting vector may therefore be different from the corresponding transmitted Code Word, and it will be noted as:

$$r = (r_1, r_2, r_3 \dots, r_n) \quad \textbf{(II.6)}$$

Error events can be modeled as error vectors or error patterns:

$$e = (e_1, e_2, e_3 \dots, e_n) \quad \textbf{(II.7)}$$

Or : $e = r + c$

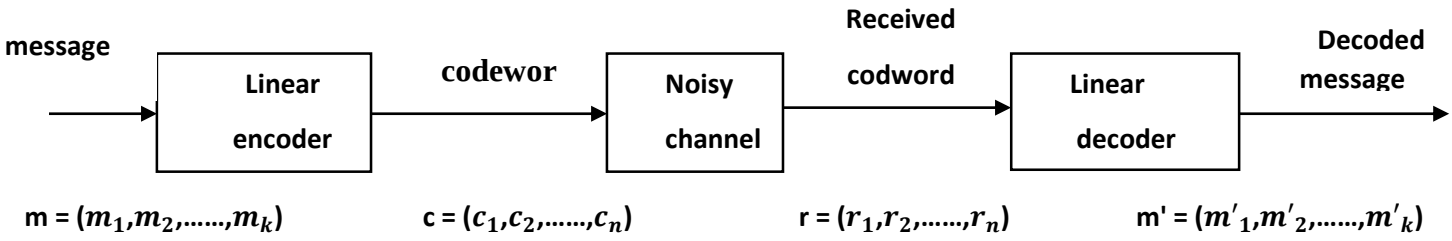


Figure II.4: Diagram of a block encoder.

To detect errors, we use the fact that any valid code word must obey the condition

$$\mathrm{C} \times H^T = 0 \quad \textbf{(II.8)}$$

The error detection tool is based on the above expression, which is of the form:

$$S = \mathrm{r} \times H^T \quad \textbf{(II.9)}$$

Or: $S = (s_1, s_2, s_3, \dots, s_3)$ is known as the syndrome vector. The detection operation is performed on the received vector:

→ **If,** S is the null vector, the received vector is a valid code word.

→ **Otherwise,** the vector received will be wrong. Checking the syndrome table to find the corresponding error pattern ej for j = 1, 2 ,..., n, the decoded message is obtained by:

$$m' = r + e_j \quad \textbf{(II.10)}$$

II.3. LDPC codes

The LDPC (Low-Density Parity-Check) codes are linear block codes with the formulas (n, k) or (n, w_c, w_r), where n is the length of the code word, k is the length of the information word, w_c is the weight of the column (the number of non-zero elements in a column of the parity matrix), and w_r is the weight of the row (i.e., the number of the non-zero elements in a row of the parity-check matrix).

There are two characteristics of LDPC codes:

❖ *Parity-Check:* The LDPC codes are represented by a binary parity check matrix H which satisfies the condition (II.8).

❖ *Low- Density:* the parity check matrix H is a hollow matrix, i.e. of low density (Low density means that there are more "0" than "1" in the matrix H) [19].

Example: Consider the following parity check matrix of a 1/2 efficiency code producing 4 redundancy bits [20]:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

II.3.1. Tanner graph

In addition to its parity check matrix, an LDPC code can be represented graphically. This is referred to as a Tanner graph [21], or, more broadly, a factor graph. A factor graph contains two types of nodes, data nodes and functional nodes. Two nodes are linked together by a branch. In the case of LDPC codes, the data nodes represent the code word, and the functional nodes correspond to the parity constraints. As a result, we will refer to the nodes as functional nodes and parity check nodes. A branch connects a data node *i* to a control node *j* if and only if the element corresponding to the j^{th} row and i^{th} column of the parity check matrix is non-zero. The data nodes will be represented by circles, while the control nodes will be represented by squares. A white circle represents a data node that corresponds to a bit of the transmitted code word. circle. If a code word bit is not transmitted (this is known as a punctured bit), the node is represented by a solid black circle and is known as a punctured node or hidden node.

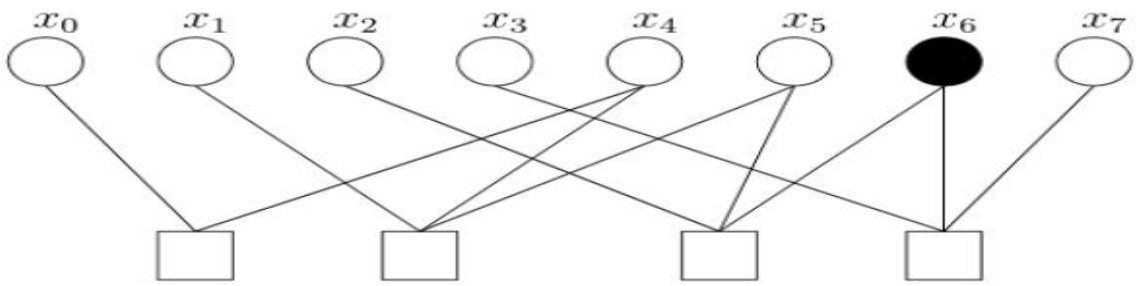


Figure II.5: Factorial graph of an LDPC code

The factor graph is a graphical representation of the code that is very simple. This graph is used to depict the decoding algorithms associated with the LDPC codes that will be presented later.

II.3.1.1. Cycle

In a Tanner graph, a cycle (loop) is a sequence of connected vertices that begins and ends at the same vertex in the graph and contains the other vertices only once. The number of edges in a cycle determines its duration [22].

II.3.1.2. Circumference

The circumference is the minimum length of the cycles in their Tanner graph.

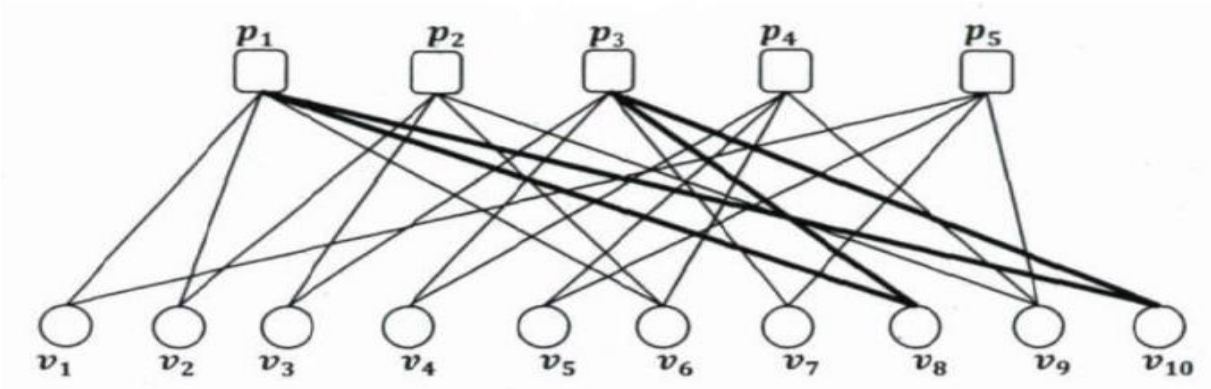


Figure II.6: the cycle in a Tanner graph.

II.3.2. Regular and irregular LDPC code

If all columns or rows of H have the same weight [22], the LDPC code is called regular LDPC code. If not, it is called an irregular LDPC code. Two parameters are defined:

d_v*:* Number of '1' per column,

d_c*:* Number of '1' per row,

Example: Regular code:

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$d_v = 2$; $d_c = 4$.

II.3.3. Construction of LDPC codes

The construction of a binary LDPC code involves assigning a small number of values in a zero-to-one matrix so that the rows and columns have the desired degree distribution.

The construction is based on various design criteria that must be implemented for encoding and decoding in order to achieve a capacity that is close to theoretical capacity. Theoretical ability several methods for creating good LDPC codes can be divided into two categories: random and structural constructions**.**

A random construction is preferred for large LDPC codes [22], [23], whereas a structured construction is used for small or medium size codes. There are primarily two methods in this last class: The first method relies on finite geometries, whereas the second relies on circulating permutation matrices. Matrices of circulating permutation the second method is the one that we are most interested in in this work.

II.3.3.1. Construction of Gallager

Gallager's original LDPC codes are regular and defined by a H band structure. The Gallager matrices' parity check lines are divided into sets w_c, with $\frac{M}{w_r}$ rows in each set. The first set of rows contains w_r number of consecutive '1' ordered across the columns from left to right. (That is, for i $\leq \frac{M}{w_r}$, there is no null entry from the $((i-1)\,w_r+1)^{th}$ to the iwr^{th}column in the i^{th} row.).

Any other set of rows is a randomly chosen column permutation of this first set. Therefore, all columns in *H* have a '1' entry once in each of the sets w_c [24].

Example: A regular parity check matrix (Gallager) M = 12, (w_c = 3, w_r = 4) is:

$$H = \begin{bmatrix} 1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1 \\ -&-&-&-&-&-&-&-&-&-&-&- \\ 1&0&1&0&0&1&0&0&0&1&0&0 \\ 0&1&0&0&0&0&1&1&0&0&0&1 \\ 0&0&0&1&1&0&0&0&1&0&1&0 \\ -&-&-&-&-&-&-&-&-&-&-&- \\ 1&0&0&1&0&0&1&0&0&1&0&0 \\ 0&1&0&0&0&1&0&1&0&0&1&0 \\ 0&0&1&0&1&0&0&0&1&0&0&1 \end{bmatrix}$$

II.3.3.2. MacKay and Neal's construction

A method proposed by MacKay and Neal is another common construction for LDPC codes. Columns of H are added one at a time from left to right in this method. The weight of each column is chosen to achieve the correct distribution, and the locations of the non-zero entries in each column are chosen at random from the rows that are not yet complete [24].

Example: A regular parity control matrix (MacKay and Neal) M = 12 (w_c = 3, w_r = 4) is:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

II.3.3.3. Quasi-cyclic (QC) LDPC code

In comparison to randomly constructed LDPC codes, quasi-cyclic LDPC codes (LDPC-QC) are a class of structured constructs with at least a circumference of 6 that can be encoded with shift registers. LDPC-QC codes are well known for their low coding complexity and low memory requirements, while still achieving high error correction performance [25].

LDPC-QC codes are distinguished by their parity check matrix, which is composed of small square blocks equal to zero, matrices, or circulating circulating permutation matrices [25], [26].

Let an LDPC-QC code be of dimension *(m × n)* with m and n multiples of *q*, and let p^i be the circulant permutation q ×q that shifts the identity matrix I to the right i times for any integer *i*, *0 < i < q*. For simplicity of notation, p^{∞} denotes the all-zero matrix.

The parity check matrix H is defined by:

$$H = \begin{bmatrix} p^{a_{11}} & p^{a_{12}} & \dots & p^{a_{1(n-1)}} & p^{a_{1n}} \\ p^{a_{21}} & p^{a_{22}} & \dots & p^{a_{2(n-1)}} & p^{a_{2n}} \\ . & . & & . & . \\ . & . & & . & . \\ p^{a_{m1}} & p^{a_{m2}} & \dots & p^{a_{m(n-1)}} & p^{a_{mn}} \end{bmatrix} \quad \textbf{(II.11)}$$

Where: $a_{ij} \in \{0, 1, \dots, q-1, \infty\}$. *H* is full rank.

II.3.4. Coding of LDPC codes

Despite their numerous advantages, the coding of LDPC codes can be a challenge for commercial applications due to their high coding complexity and coding delay.

Coding for LDPC codes consists primarily of two tasks:

- Construct a hollow parity check (sparce) matrix.
- Generate the code words using this matrix.

II.3.4.1. Conventional coding based on Gauss-Jordan elimination

To compute the codeword, the classical coding algorithm employs Gauss-Jordan elimination and column reordering. Neal proposed a simple scheme [27] that is similar to the general method of coding codes in linear blocks. We partition a given codeword *C* into message bits *x* and parity check bits *p* using an irregular parity check matrix *H* of size *(m × n)*.

$$C = [x \mid p] \quad \textbf{(II.12)}$$

The parity check matrix *H* is converted to systematic form and then divided into a matrix *A* of size *m × (n - m)* on the left and a matrix *B* of size *m × m* on the right after Gauss-Jordan elimination.

$$H = [A \mid B] \quad \textbf{(II.13)}$$

From condition (II.8), we have:

$$A.\boldsymbol{X^T} + B.\boldsymbol{P^T} = 0 \quad \textbf{(II.14)}$$

Therefore,

$$P^T = \boldsymbol{B^{-1}}.A.X^T \quad \textbf{(II.15)}$$

As a result, (II.15) can be used to compute the control bits if *B* is non-singular[1].

In general, after preprocessing, the parity check matrix H will not be sparse. As a result, the complexity of the traditional processes for coding this LDPC code is quite high. This LDPC code is excellent.

[1] A square matrix is said to be singular if it is not invertible.

II.3.4.2. Coding by lower triangular approximation

The complexity of traditional coding algorithms is inversely proportional to the square of the code length, which becomes a significant issue for long code lengths. To address this issue, Richardson and Urbanke [28] propose an efficient LDPC coding algorithm. In the following section, we will provide a detailed description of this coding algorithm.

The idea is to perform a transformation of the parity check matrix using only row and column permutation to keep H hollow. As shown in Figure II.6, any arbitrary hollow matrix can be converted to a desired parity check matrix H with an approximate lower triangular shape.

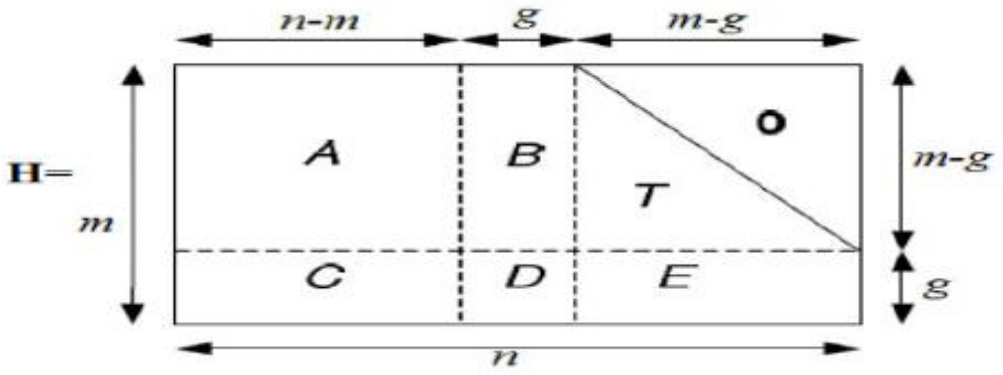


Figure II.7: Lower pseudo-triangular representation of the matrix H.

a) Richardson-Urbanke algorithm [28]:

The steps of this algorithm can be summarized as follows:

1- Perform the row and column permutation to put H in a triangular form approximate lower form:

$$H = \begin{bmatrix} A & B & T \\ C & D & E \end{bmatrix} \qquad \textbf{(II.16)}$$

Where **A** is of size $(m - n) \times (m - g)$, **B** is of size $g \times (m - g)$, **T** is a lower triangular matrix of size $(m - g) \times (m - g)$, **C** is of size $(n - m) \times g$, **D** is of size $g \times g$ and finally **E** is of size $(m - g) \times g$. The g rows of **H** are called the gap of the approximate representation.

2- Once we have obtained the upper triangular format **T**, we use Gauss elimination to empty **E**, which is equivalent to the following per-multiplication:

$$\begin{pmatrix} 1 & 0 \\ -E.T^{-1} & 0 \end{pmatrix} \times \begin{pmatrix} A & B & T \\ C & D & E \end{pmatrix} = \begin{pmatrix} A & B & T \\ -E.T^{-1}.A + C & -E.T^{-1}.B + D & 0 \end{pmatrix}$$

$$= \begin{pmatrix} A & B & T \\ C' & D' & 0 \end{pmatrix} \qquad \textbf{(II.17)}$$

Where we note:

$$C' = -E.T^{-1}.A + C \quad \textbf{(II.18)}$$

$$D' = -E.T^{-1}.A + D \quad \textbf{(II.19)}$$

3- Encoding:

Let us consider the code word **C** consisting of a systematic **x** part and two parity parts $\boldsymbol{p_1}$ and $\boldsymbol{p_2}$, with lengths g and *(m - g)*, respectively. We apply the condition $H.x^T = 0$ to the code

$C = [x\ p1\ p2]$, we obtain:

$$A\,x^T + B\,P_1^T + T\,P_2^T = 0 \quad \textbf{(II.20)}$$

$$\hat{C}\,x^T + \hat{D}\,P_1^T + 0\,P_2^T = \hat{C}\,x^T + \hat{D}\,P_1^T = 0 \quad \textbf{(II.21)}$$

Assuming that **D** is invertible, **p1** can be found from (II.20):

$$P_1^T = -\hat{D}^{-1}\hat{C}\,x^T = -\hat{D}^{-1}(-ET^{-1}A + C)x^T \quad \textbf{(II.22)}$$

Where the low density of A, B and T can be used to keep the complexity of this operation low; since T is upper triangular, P2 can be found by :

$$P_2^T = -T^{-1}(Ax^T + BP_1^T) \quad \textbf{(II.23)}$$

This is the most widely used method for LDPC code encoding, and it has been adopted by the *IEEE 802.11n* and *IEEE 802.16*^{e} standards. The advantage of these codes is that their constructions are performed in a systematic manner, which reduces coding complexity and complexity, as well as the required memory.

II.3.5. Iterative decoding of LDPC codes

In comparison to other types of codes, decoding LDPC codes does not pose as many problems for researchers as their construction. The most difficult task is determining the best methods for creating efficient LDPC codes [29].

Several methods can be used to decode an LDPC code, including:

1. Decoding with firm decisions:

- Decoding with majority logic (MLG).
- Decoding with bit switching (BF).

2. Decoding with weighted decisions:

- Decoding based on a posteriori probability (APP).
- Iterative decoding based on confidence propagation (BP).

3. Mixed decoding (firm and weighted):

- Weighted LF decoding.

In terms of circuit complexity, the MLG method is the most straightforward.

The BF method necessitates slightly more circuit complexity, but it provides better error performance than the MLG method. The APP and BP methods provide better error performance but necessitate greater circuit complexity.

The circuit's complexity Iterative BP decoding is a good compromise between the two properties.

II.3.5.1. Decoding algorithm by belief propagation (BP)

To describe the iterative decoding algorithms for LDPC codes, we will use the notation in Table II.1.

Consider an (n, k) LDPC code with a control matrix H of size $(n - k) \times n$. With $R = k/n$ the coding rate. $c = (c_1, c_2, \ldots, c_n)$ denotes the codeword.

E_b is the average bit energy normalized to 1. N_0 is the average noise density. $r = (r_1, r_2, \ldots r_3)$ is the received vector. $z = (z_1, z_2, \ldots z_n)$ is the estimated vector obtained from r.

s	S = zH^T
p_j^a	An a priori probability of the transmitted code words c_j = a or a is 0 or 1.
f_j^a	A posteriori probability,(App) of q_j^a= p_r(c$_j$ = a | r_j).
$L(cj)$	log likelihood ratio(LLR), $log(f_j^0)/(f_j^1)$
q_{ij}^a	probability that bit j of x is a, given the control information i.
r_{ij}^a	The control probability i being satisfied if bit j of x is considered fixed a, and the other bits have a separate distribution given by q_{ij}.

Table II.1: Message notation - iterative passing LDPC decoders

The belief propagation (BF) algorithm can perform decoding in either the probabilistic or the logarithmic domains [30], [31], [32].

The use of logarithmic probabilities has the advantage of converting a product of several messages to a sum. Because a sum is easier to implement on hardware, this reduces the complexity of the decoding process. Both decoding algorithms have nearly identical bit error rates (BER).

a) Probabilistic BP decoding algorithm:

This is how the algorithm is written:

- **Entrance:** Define a posteriori probability (APP) f_j^0 and f_j^1 for each bit c_j.

$$f_j^1 = p\,(c_j = 1|r_j) = \frac{1}{1+e^{\frac{2r_j}{\sigma^2}}} \quad \textbf{(II.24)}$$

$$f_j^0 = 1 - f_j^1 \quad \textbf{(II.25)}$$

- **Initialisation:** - Set the variables q_{ij}^0 and q_{ij}^1 to the values f_j^0 and f_j^1, respectively.

  - Set the loop counter as well as the maximum number of iterations,i_{max}.

- **Iterative processing:**

1- Operation on lines:

- Define $\delta q_{ij} = q_{ij}^0 - q_{ij}^1$ and calculate for each i, j:

$$\delta q_{ij} = \prod_{j' \in N(i)\setminus j} \delta_{r'_{ij}^a} \quad \textbf{(II.26)}$$

- Then set: $r_{ij}^0 = \frac{1}{2}(1 + \delta r_{ij})$ **et** $r_{ij}^0 = \frac{1}{2}(1 - \delta r_{ij})$

2- Operation on the columns:

- For each j and i and a = 0,1 update :

$$q_{ij}^{a} = \alpha_{ij} f_j^{a} \prod r_{ij}^{a} \quad \textbf{(II.27)}$$

Where α_{ij} is chosen so that $q_{ij}^{0} + q_{ij}^{1} = 1$

3- Decision:

- Update the probabilities q_j^0 and q_j^1 given by:

$$q_j^{a} = \alpha_j f_j^{a} \prod r_{ij}^{a} \quad \textbf{(II.28)}$$

$$\hat{C} = \begin{cases} 1, & q_j^1 > q_j^0 \\ 0, & otherwise \end{cases} \quad \textbf{(II.29)}$$

4- Parity test:

-If $\hat{C}H^T = 0$ then given $\hat{C}$ is stopped the algorithm.

5- Iteration Storyteller:

-Stop if i > i_{max}, n go to 1.

b) Logarithmic BP decoding algorithm

The logarithmic BP decoding algorithm [25] improves on the probabilistic BP algorithm by introducing log likelihood ratios (LLRs), which convert most multiplications to additions.

First, we define:

$$l\,(c_{ij}) = \log\left(f_j^0 / f_j^1\right) \quad \textbf{(II.30)}$$

$$l\,(r_{ij}) = \log\left(r_{ij}^0 / r_{ij}^1\right) \quad \textbf{(II.31)}$$

$$l\,(q_{ij}) = \log\left(q_{ij}^0 / q_{ij}^1\right) \quad \textbf{(II.32)}$$

$$l\,(q_j) = \log\left(q_j^0 / q_j^1\right) \quad \textbf{(II.33)}$$

II.4. Conclusion

In this chapter, we covered the fundamentals of LDPCs as well as their description using Tanner graphs, which are a useful representation of linear block codes, particularly LDPCs.

LDPC codes, in particular, are linear block codes. Some construction methods for these codes have been written, such as the methods of Gallager, Makey, and Neal. In terms of decoding the LDPC codes, we mentioned several methods and detailed an iterative decoding based on the belief propagation algorithm.


General
conclusion

General conclusion

The goal of this study is to examine and evaluate a LDPC code .

The process of canal coding is a key part of our study. It was for this reason that a study of coding and decoding was required in order to clarify the role and effect of an error-correcting code on the signal to be transmitted.

In the first chapter, we presented a brief analysis of the digital transmission chain.

In the second chapter, we looked at a new sort of error-correcting code called LDPC regular codes.

LDPC codes are correction codes close to the Shannon limit. Long LDPC codes with iterative decoding based on belief propagation have been shown to achieve error performance within a fraction of a decibel of the Shannon limit.

LDPC competes fiercely with turbo codes in digital communication systems that require high reliability. In addition, LDPC codes have some advantages over turbo codes.

LDPC code with iterative decoding on a Gaussian channel combined with 2-PSK modulation can well estimate the bit error rate (BER) and FER as a function of the signal-to-noise ratio Eb/N0 (dB).

Thus, LDPCs are now becoming a hot topic in the telecommunications field. For this reason, we will give some perspectives.

These codes have a large number of parameters, so the optimization of their parameters would be a future topic in order to adapt them to many channels. This adaptation offers many perspectives of use.

For example, LDPC codes can be designed for optical communications, magnetic storage, multiple-input and multiple-output channels and satellite transmission.

An LDPC code has been chosen for the DVB-S2 standard, providing a starting point for expressing their potential in industrial uses. Thus, LDPC decoder architectures are now becoming a hot topic in the field of algorithm-architecture matching.

BIBLIOGRAPHY

[1] C. E. SHANNON, «A mathematical theory of communication, » Bell System Technical Journal, vol. 27, pp. 379-423 et 623-656, Juillet et Octobre 1948.

[2] «claude chappe , notice biographique », par Ernest Jacquez, éditeurs Alphonse Picard et fils,1893.

[3] http://creativecommons.org/licenses/by-nc-sa/2.0/ , 'Systèmes de communications numériques'.date of his visited "10/03/2022".

[4] GENEVIEVE BAUDOIN :'radiocommunications numériques', DUNOD, 2002.

[5] 'Yvon Mori','théorie de l'information et du codage,'Hermes Science', 2007.

[6] 'John B. Anderson' , 'Tor Aulin, and Carl-Erik Sundberg'. *Digital Phase Modulation*.Plenum Press, New York, 1986.

[7] 'R. W Hamming ','Error detecting and error correcting codes' The Bell SystemTechnical Journal , April 1950.

[8] 'Gaël Mahé', 'Systèmes de communications numériques', 'UFR de Mathématiqueset Informatique Université Paris Descartes','2010'.

[9] 'Yvon Mori','Filtrage numérique','Hermes Science',2007.

[10] K. D. Rao, *Channel Coding Techniques for Wireless Communications*. s.l.: Springer-Verlag, 2015.

[11] 'http://mediatools.iict.ch/document?url=Cours_de_Telecommunications Modula tions/mod2/Mic.pdf&dpId=15', 'chapitre 8 modulationpar impulsion et codage(MIC,PCM)',

date of his visited "17/03/2022".

[12] S. J. Johnson, *Iterative Error Correction: Turbo, Low-density Parity-check and Repeataccumulate*
Codes. Cambridge University Press, 2009.

[13] A.L. FAWE, L. DENEIRE, «Principe de Télécommunications«, 1995-1996.

[14] R. G. Gallager, "Low-density parity-check codes," Ph.D. dissertation, 1963.

[15] D. MacKay and R. M. Neal, "Near shanon limit performance of low density parity-check codes," Electronic Letter, August 1996.

[16] J. Pearl, Probabilistic reasoning in intelligent systems : networks of plausible inference, S. Mateo, Ed. Morgan Kaufmann Publishers, 1988.

[17] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. Spielman, “Analysis of low density codes and improved designs using irregular graphs,” Proceeding of 30th ACM Symp. On Theory of Computing, 1998.

[18] Cours de transmission numérique.

[19] RUI YANG, « LDPC-coded Modulation for Transmission over AWGN and Flat Rayleigh Fading Channels ». FACULTE DES SCIENCES ET DE GENIE UNIVERSITÉ LAVAL QUÉBEC, 2010.

[20] Jean-Baptiste Doré « Optimisation conjointe de codes LDPC et de leurs architectures de décodage et mise en oeuvre sur FPGA » . Traitement du signal et de l’image. INSA de Rennes, 2007. Français. <Tel-00191155v2>.

[21] R. Tanner, “A recursive approach to low complexity codes,” IEEE Transactions on Information Theory, vol. 27, sept 1981.

[22] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved lowdensity parity check codes using irregular graphs," IEEE Transactions on Information Theory, Vol. 47, pp. 585-598, Feb. 2001.

[23] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, «Design of capacity approaching irregular low-density parity-check codes,» *IEEE Transactions on Information Theory,,* vol. 47, pp. 619-637, 2001.

[24] D. J. C. MacKay, “Good error-correcting codes based on very sparse ma- trices,” IEEE Trans. Inform. Theory, vol. 45, no. 2, pp. 399–431, March 1999.

[25]. M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices", IEEE Transactions on Information Theory, Vol. 50, no. 8, pp. 1788-1794, Aug. 2004.

[26] S. Myung, K. Yang and J. Kim, "Quasi-cyclic LDPC codes for fast encoding", IEEE Transactions on Information Theory, Vol. 51, no.8, pp. 2894- 2900, Aug. 2004.

[27] LDPC Code using MATLAB, http://sites.google.com/site/bsnugroho/ldpc. date of his visited "03/04/2022".

[28] T. J. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity- check Codes", IEEE Transactions on Information Theory, Vol. 47, no. 2, pp. 638- 656, Feb. 2001

[29] I. ADJUDEANU, Codes correcteurs d'erreurs LDPC structurés, QUÉBEC : FACULTE DES SCIENCES ET DE GENIE , 2010.

[30] S. M. Alamouti and S. Kallel, "Adaptive trellis-coded multiple-phase-shift keying for Rayleigh fading channels", IEEE Transactions on Communications, Vol. 42, No. 6, pp. 2305-2314, Jun. 1994.

[31] R. G. Gallager, Low-Density Parity-Check Codes. Cambridge, MA: MIT Press, 1963.

[32] R. G. Gallager, "Low-density parity-check codes", IEEE Transactions on Information Theory, Vol. IT-8, no. 1, pp. 21-28, Jan. 1962