



**Faculté des sciences et des sciences appliquées**

**Département de Génie Electrique**

**Mémoire de Master**

***Option : Technologies des Télécommunications***

Réalisé par :

Imane DEROUICHE

Roumaïssa MIHOUBI

Thème :

---

**Codes correcteurs d'erreurs  
LDPC de communication mobiles  
de la quatrième génération**

---

Le 27/09/2017

Devant les membres de jury :

M· Smail MEDJDOUB

Président

M· Bilal SAOUD

Examineur

M· Mohamed Lamine BOUCENNA

Examineur

M· Skander BENSEGUENI

Encadreur

Année universitaire : 2016/2017

## *Remerciement*

*Je remercie tout d'abord Allah le tout puissant de ses bienfaits, et de son aide sans laquelle je n'aurais pas effectué ce modeste travail.*

*Au terme de ce travail, je tiens à remercier tout spécialement mon encadreur M. BENSEGUINI SKANDER de m'avoir proposé ce sujet,*

*je tiens à*

*leur faire part de ma profonde gratitude pour son aide incessante, ses conseils tout le long de mon travail.*

*Je remercie également le président et les membres de jury d'avoir accepté de m'honorer par leur présence pour juger et évaluer mon travail.*

*Je remercie enfin toutes les personnes qui ont, de près ou de loin, permis la réalisation de ce travail.*

# DÉDICACE

*Au nom de dieu le tout puissant et qui m'a permis d'apprendre et  
d'acquérir le savoir .je dédie ce modeste travail :*

*A ceux qui ont attendu ce jour avec impatience et qui n'ont cessé de  
m'encourager et qui se sont toujours sacrifiés pour mon bonheur*

*A mon modèle de sacrifice, d'amour et de générosité, la lumière de mon  
chemin et l'étoile de m'a vie : **Ma très chère mère***

*A celui m'a offert tout le soutien dont j'ai besoin et sans le quel je ne  
serais pas à ce stade et accomplit ce travail.*

*Mon très cher père*

*Que dieu les protège.*

*A mes très chère sœur : **Razika , Fathia, Wafia** et son mari **Mohammed**  
et sa fille **Ranim.***

*A mes très chers frères : **Kamel et Abou Bakr.***

*Sans oublier " **Nour Al Islam**" mon cher frère dieu bénisse*

*A toute mes amis(es) exceptionnellement: **samira ,houssem.***

*A ma collègue " **Romaissa** " et à sa famille.*

*Tous ceux qui ont contribué de près ou de loin a la réalisation de  
se travail et tous qui ont une place dans cœur.*

**Imane**

# dedicace

*Je dédie ce modeste travail à :*

*À Mes très chers parents,*

*qui me sont les plus chers au monde, dont l'amour  
et les sacrifices n'ont pas cessé de combler ma vie ;*

*que Dieu les protège et les garde pour moi*

*A mes très chers sœurs*

*qui n'ont cessé d'être pour moi des exemples de persévérance,  
de courage et de générosité*

*A mon très cher fiancé*

*Merci pour ton aide, tes conseils et tes encouragements*

*Et à tous ceux qui m'ont aidé de près ou de loin à accomplir ce travail.*

*à tous ceux que j'aime,  
et à tous ceux qui m'aiment ...*

*Roumaïssa*

**Table des matières**

Résumé.....	I
Liste des figures.....	II
Liste des tableaux.....	III
List des abréviations .....	IV

<b>Introduction générale</b>	1
------------------------------	---

**Chapitre 1 : les systèmes de communication mobiles**

1.1. Introduction .....	3
1.2. Définitions et concepts de base .....	3
1.2.1. Réseau Sans fil .....	3
1.2.2. Réseau mobile .....	3
1.2.3. Propriétés des réseaux mobiles .....	3
1.3. Evolution des réseaux de mobile .....	4
1.4. Chaîne de communication .....	6
1.4.1. Source .....	6
1.4.2. Codeur .....	6
1.4.2.1. Source.....	6
1.4.2.2. Canal.....	6
1.5. Technique de modulation .....	7
1.6. Canal radio mobile .....	8
1.6.1. Les classe des canaux radio-mobiles .....	8
1.6.1.1. Canal à évanouissement long terme.....	9
1.6.1.2 Canal à évanouissement à court terme .....	10
1.7 Techniques d'accès multiples.....	11
1.7.1 Technique FDMA .....	11
1.7.2 Technique TDMA .....	11
1.7.3 Technique CDMA.....	12
1.8 La combinaison (Orthogonal Frequency Division Multiples Accès (OFDMA))...	13

1.8.1 OFDM.....	13
1.8.2 OFDMA (Orthogonale Frequency Division Multiple Accès).....	14
1.8.3. SC-FDMA (Signal Carrier Frequency Division Multiple Accès).....	15
1.8.4 Comparaison entre SC-FDMA et OFDMA .....	15
1.9 Conclusion .....	16

**Chapitre 2 : les codes correcteurs d’erreur**

2.1 Introduction .....	17
2.2 Les modèles de canaux de communication.....	17
2.2.1. Le canal binaire symétrique.....	17
2.2.2 Canal Gaussien.....	17
2.3 Codage canal.....	18
2.4 Codes correcteurs d’erreurs.....	18
2.5 Codes linéaires .....	19
2.6 Codes convolutifs.....	20
2.7 Différents codes correcteurs.....	20
2.7.1 Turbo Code.....	20
2.7.2 Code à répétition.....	21
2.7.3 Code de Hamming.....	21
2.7.4 Code cyclique .....	22
2.7.5 Codes de Reed-Solomon.....	23
2.7.6 Codes concatènes.....	23
2.8 Codes LDPC.....	24
2.8.1 Historique.....	24
2.8.2 Caractéristiques et avantages.....	25
2.8.3 Graphes de Tanner .....	25
2.8.4 Codes LDPC irréguliers.....	26
2.8.5 Codes LDPC réguliers.....	27
2.8.6 Encodage LDPC.....	28
2.8.7 Algorithmes de décodage des codes LDPC.....	28
2.8.7.1 Propagation de croyance.....	29
2.8.7.2 Mise à jour des messages sur un noeud de donnée : Data pass.....	29
2.8.7.3 Mise à jour des messages sur un noeud de contrôle : Check pass.....	30

2.9 Conclusion.....	30
<b>Chapitre 3 : Algorithme de code correcteurs LDPC</b>	
3.1 Introduction .....	31
3.2 Algorithme de codage LDPC .....	31
3.3 Codage d'information à 4 bit et à 5 bit.....	32
3.4 Algorithme de décodage LDPC.....	37
3.5 Décodage d'information à 4 bit et à 5 bit.....	37
3.6 Introduction et correction des erreurs .....	38
3.7 L'application sur une image.....	41
3.7.1 Codage.....	41
3.7.2 Décodage.....	42
3.7.3 Introduction des erreurs et correction.....	42
3.8 Conclusion.....	45
<b>conclusion générale</b>	
	46
<b>Bibliographie</b>	
	47

### Résumé

Nous présentons dans ce mémoire, une méthode de codage et de décodage des codes correcteurs d'erreurs pour les transmissions sans fil, basée sur l'utilisation des codes LDPC réguliers. Dans un premier temps, nous avons appliqué un algorithme de codage et décodage des codes correcteurs d'erreur LDPC par la présentation de deux exemples d'information de tailles différentes (de 4 bits et 5 bits) avec l'introduction des erreurs et sans erreurs. Nous avons décodé ces codes en corrigeant toutes les erreurs introduites. Ensuite, nous avons appliqué cet algorithme sur une matrice d'image avec une simulation de plusieurs erreurs. La correction de ces erreurs est effectuée pour le cas d'un seul bit mais, on n'a pas obtenu de corrections pour le cas plusieurs bits d'erreur.

**Mots clés** OFDM, Codes LDPC, Encodage, Décodage

## Liste de figures

**Chapitre 1 : les systèmes de communication mobiles**

<b>Figure 1.1</b> différentes parties de réseaux mobile .....	4
<b>Figure 1.2</b> Evolution d'un réseau mobile .....	5
<b>Figure 1.3</b> modèle de la chaine de communication numérique.....	7
<b>Figure 1.4</b> Diagramme de la constellation de la modulation M-QAM pour M = 4, 16, et 64...8	
<b>Figure 1.5</b> Scénario d'une transmission radio mobile sur un canal .....	9
<b>Figure 1.6</b> fluctuation à petit et à grand échelles de canal .....	10
<b>Figure 1.7</b> Technique d'accès multiple FDMA .....	12
<b>Figure 1.8</b> Technique d'accès multiple TDMA.....	12
<b>Figure 1.9</b> Technique d'accès multiple CDMA .....	13
<b>Figure 1.10</b> La différence entre l'OFDM et l'OFDMA .....	14

**Chapitre 2 : les codes correcteurs d'erreurs**

<b>Figure 2.1</b> Canal binaire symétrique de probabilité d'erreur .....	17
<b>Figure 2.2</b> shama d'un code convolutif .....	21
<b>Figure 2.3</b> schéma de code concaténé .....	24
<b>Figure 2.4</b> Graphe factoriel d'un code LDPC .....	26
<b>Figure 2.5</b> illustration du data pass.....	30
<b>Figure 2.6</b> illustration du check pass.....	30

**Chapitre 3 : Algorithme de code correcteurs LDPC**

<b>Figure 3.1</b> étapes d'un algorithme codage et décodage LDPC.....	32
<b>Figure 3.2</b> Graphe bipartite d'un code LDPC de 7 bit.....	36
<b>Figure 3.3</b> Graphe bipartite d'un code LDPC de 8 bit.....	37
<b>Figure 3.4</b> Construction de l'information et de code .....	43
<b>Figure 3.5</b> Résultat d'introduction de 1 bit d'erreur.....	44
<b>Figure 3.6</b> résultat d'introduction de 2 bit d'erreur.....	44
<b>Figure 3.7</b> Résultat d'introduction de 3 bits.....	45



Liste des tableaux

**Chapitre 1 : les systèmes de communication mobiles**

**Tableau 1.1** : comparaison entre différentes générations mobiles..... 5

**Chapitre 3 : Algorithme de code correcteurs LDPC**

**Tableau 3.1** La table standard de 7 bit..... 39

**Tableau 3.2** La table standard de 8 bit..... 40

**Tableau 3.3** table de syndrome de 7 bit..... 40

**Tableau 3.4** table de syndrome de 8 bit..... 41

**Abréviation**

**1G**(1ème génération)

**2G** (2ème génération)

**3G** (3ème génération)

**4G** (4ème génération)

**5G**(5ème generation)

**A**

**ADSL**: Asymmetric Digital Subscriber Line.

**B**

**BER** : Bit Error Rate.

**BF** : Basse fréquence.

**BPSK** : Binary Phase Shift Keying.

**C**

**CDMA** (Code Division Multiple Access).

**CN**: Core Network.

**D**

**DFT** : Discret Fourier Transform.

**DVB** : Digital Video Broadcast.

**E**

**ESA** : European Spatial Agency.

**F**

**FDMA**(Frequency Division Multiple Access).

**FDM/FDMA** (Frequency Division Multiplexing/Frequency Division Multiple Access) :  
méthode d'accès à la couche physique.

**FDD** (Frequency Division Duplex): technique de multiplexage.

**FFT** (Fast Fourier Transform).

**I**

**IDFT** : Inverse Discrete Fourier Transform.

**IFFT** : Inverse Fast Fourier Transform.

**L**

**LDPC** : (Low Density Parity Check).

**LOS** (Line Of Sight)

**LTE** (Long Term Evolution): technologie de communication radio mobile de longue portée.

## **M**

**MC-CDMA** : Multi-Carriers Code Division Multiple Access.

**MBWA** : Mobile Broadband Wireless Access.

**MLD** (Maximum Likelihood Decoding).

**MIMO** : Multiple Input Multiple Output.

## **N**

**NLOS** (None Line Of Sight).

## **O**

**OFDM** (Orthogonal Frequency Division Multiplexing): procédé de codage des signaux numériques.

**OFDMA** (Orthogonal Frequency Division Multiple Access): méthode d'accès à la couche physique.

## **Q**

**QAM** (Quadrature Amplitude Modulation): méthode de modulation.

**QPSK** (Quadrature phase-shift keying): méthode de modulation.

## **R**

**RAN**: Radio Access Network.

## **S**

**SC-FDMA** : (Signal Carrier Frequency Division Multiple Accès).

## **T**

**TC** : Turbo-Codes

**TDD** (Time Division Duplex): technique de multiplexage.

**TDM/TDMA** (Time Division Mutiplexing/Time Division Multiple Access): méthode d'accès au support physique.

## **U**

**UIT** : Union International des Télécommunications.

**UMTS** (Universal Mobile Telecommunications System): technologie de communication radio mobile de 3ème génération de longue portée.

## **W**

**WLAN** : (Wireless Local Area Network): réseau local sans fil.

**WiMAX** (Worldwide Interoperability for Microwave Access).

**WiMAX** (IEEE 802.16): technologie de communication radio de 3ème génération de longue portée.

**WRAN** : Wireless Rural Area Network

### Introduction générale

L'évolution et la progression technologiques ont connu un sommet avec la création d'internet et sa propagation à travers les quatre coins du monde. Ce dernier joue un rôle efficace dans la distribution et le partage rapide et gratuit de l'information, toutefois, on remarque une lacune dans le mode des communications à grande échelle. La majorité des travaux de recherche dans ce domaine se focalisent sur le déploiement de nouvelles technologies permettant de rendre les réseaux de télécommunication de plus en plus performants. Cette évolution est particulièrement frappante pour les communications radio mobiles avec l'apparition des différentes générations de téléphonie mobile. Parallèlement, les applications pouvant bénéficier de cette évolution technologique n'ont cessé de se diversifier.

Les futures communications mobiles nécessiteront inévitablement des débits élevés de données. Les ressources en temps de spectre radio étant limitées, il est devenu nécessaire d'opter pour de nouvelles techniques qui améliorent l'efficacité spectrale sans engendrer un coût sur l'utilisation du spectre. Dans les applications impliquant les communications sans fil. Les nouvelles générations des réseaux mobiles sont basées sur la technique de modulations multi-porteuses OFDM (Orthogonal Fréquence Division Multiplexing) qui se présente comme une solution contre l'effet de multi-trajet, et représente la base d'une autre technique d'accès OFDMA. L'OFDMA (Orthogonal Frequency Division Multiple Access) est la technique d'accès multiple de l'OFDM combinée avec une technique d'accès multiple par répartition en fréquence FDMA, cette technique a été choisie dans les couches physiques des réseaux mobiles de 4<sup>ème</sup> génération. La séparation des signaux de chaque utilisateur est assurée par le choix d'un code d'étalement spécifique alloué à chaque utilisateur. A la réception, la propriété d'orthogonalité de ses codes sert à la distinction entre les signaux émis par les différents utilisateurs. Les codes de Walsh Hadamard qui possèdent cette propriété d'orthogonalité sont généralement utilisés pour des transmissions synchrones. Néanmoins, cette propriété nécessaire à la séparation des signaux de chaque usager constitue l'une des contraintes majeures de cette technique. En plus, la diversité du canal de transmission à évanouissement est élevée, plus grande est la possibilité d'obtenir des performances proches du cas idéal du canal sans évanouissements. En présence de trajets multiples et d'un signal large bande, le canal devient généralement sélectif en fréquence, ceci dégrade la performance des signaux numériques et limite le débit de données maximum de transmission. Une solution qui a prouvé son efficacité dans une méthode d'optimisation des codes correcteurs d'erreurs pour les

transmissions sur un canal sélectif en fréquence (OFDM) sur la quatrième génération, basée sur l'utilisation des codes LDPC (Low Density Parity Check) réguliers.

Ce mémoire comprend trois chapitres où on a opté pour une présentation graduelle des concepts par ordre de leur apparition dans le mémoire.

Dans le premier chapitre il est question des notions et concepts de communications numériques d'importance dans nos travaux effectués dans le cadre de ce mémoire. Ainsi, les techniques mises en œuvre ou associées avec d'autres au cours de cette recherche sont décrites progressivement. En premier les différents éléments d'une chaîne de transmission numérique de base sont présentés, suivi des différents modèles de canaux de communication auquel les signaux issus de cette chaîne peuvent être soumis sont fournis. Seuls les modèles à plus grand usage sont retenus. Ensuite, la technique multi-porteuse, plus particulièrement l'OFDM, L'OFDMA et sa variante SC-FDMA sont dérivées du codage OFDM, mais contrairement à l'OFDM, l'OFDMA est optimisé pour l'accès multiple, ainsi qu'il est compatible avec la technique des antennes MIMO (Multipl Input Multipl Output).

Le deuxième chapitre a pour objectif d'étude les notions de base sur les codes LDPC en présentant quelques méthodes de construction et différentes méthodes de décodage et de présentation par les graphes de Tanner, qui sont une représentation utile des codes linéaires et particulière des codes LDPC.

Dans le troisième chapitre, nous allons faire une simulation d'un algorithme de code correcteur LDPC sur une image et ajouter des erreurs et essayer de les corriger.

## 1.1 Introduction

Le développement de nouvelles technologies a toujours été dicté par les besoins du moment et la disponibilité de la technique. On est ainsi passé de la radio analogique à la radio numérique avec tous les progrès qui se sont suivis notamment au niveau de la qualité, la rapidité et la fiabilité du transport l'information mais aussi au niveau de la capacité du réseau [1].

Depuis plusieurs années le développement des réseaux mobiles n'a pas cessé d'accroître, plusieurs générations ont vues le jour (1G, 2G, 3G, 4G et prochainement la 5G pas encore mis en œuvre) et connues une évolution remarquable, en apportant un débit exceptionnel et qui ne cesse d'augmenter, une bande passante de plus en plus large et un des avantages d'une telle bande passante est le nombre d'utilisateur pouvant être supportés.

Dans ce chapitre introductif, nous allons présenter quelques généralités sur les réseaux mobiles et leurs techniques d'accès.

## 1.2 Définitions et concepts de base

### 1.2.1 Réseau Sans fil

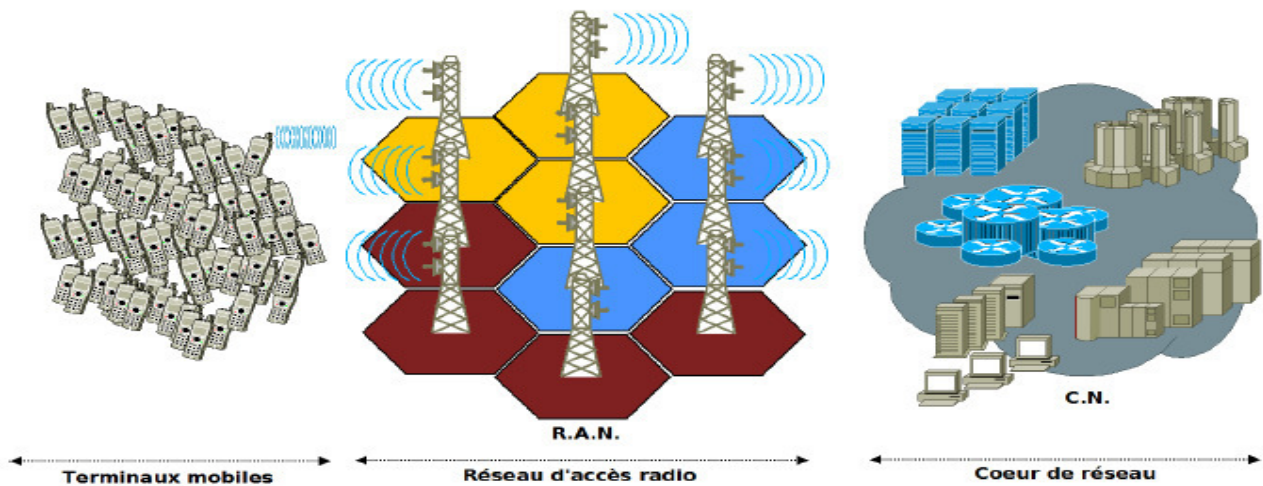
Un réseau sans fil (en anglais Wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fils, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité". Il peut être associé à un réseau de télécommunications pour réaliser des interconnexions entre nœuds [2].

### 1.2.2 Réseau mobile

Le réseau mobile est un réseau de communication composé de cellules, généralement considérées de forme hexagonal .ces cellules sont tous juxtaposées l'une à l'autre afin d'améliorer une meilleure couverture de la zone géographique [2].

### 1.2.3 Propriétés des réseaux mobiles

Les réseaux mobiles sont constitués de deux parties distinctes : le réseau d'accès radio (RAN : Radio Access Network) et le cœur de réseau (CN:Core Network). Le réseau d'accès radio prend en charge la connexion radio avec les terminaux la Figure 1.1, alors que le cœur de réseau permet l'établissement des services quelque soit la localisation et la mobilité du terminal au sein du réseau d'accès radio. Dans les réseaux mobiles, le passage quasi obligatoire de l'information sur l'interface radio restreint les ressources disponibles ainsi que la bande passante dédiée aux utilisateurs .Cette



**Figure 1.1** différentes parties de réseaux mobile [3].

réduction découle de l'étrouitesse de la bande de fréquence qui a été allouée pour le fonctionnement de ces réseaux. Pour une gestion efficace de l'interface radio commune à tous les utilisateurs, de nouvelles technologies ont été créées dans le but de s'adapter aux propriétés des systèmes de mobile [2].

### 1.3 Evolution des réseaux de mobile

Aujourd'hui, les systèmes de communication sans fil sont de plus en plus présents dans notre vie quotidienne et ils tendent à remplacer l'utilisation excessive des câbles. Bien que les connexions à haut-débit de type ADSL se multiplient dans le monde, elles ne permettent pas la souplesse d'utilisation que procure un réseau radio sans fil.

Pour améliorer la qualité de service qu'ils offrent, les chercheurs préparent l'arrivée de la future génération baptisée 4<sup>ème</sup> génération (4G) [4]. Cette évolution est représentée dans la figure.1.2

La première génération des systèmes de communication mobiles sans fil 1G a été introduit Dans les années 70 et la deuxième génération 2G dans les années 80 ont été principalement destinée à la transmission de la voix. Les premières systèmes avaient utilisé la modulation de fréquence analogique alors que la seconde avait utilisé des techniques de communication numérique avec multiplexage temporel (TDM), multiplexage en fréquence (FDM) ou le Code Division Multiple Access (CDMA). Les systèmes sans fil de troisième génération qui sont juste introduites dans la marchés mondiaux offrent des débits de données beaucoup plus élevés, et permet des améliorations significatives par rapport aux systèmes 2G. Les systèmes sans fil 3G ont été proposées pour

fournir des services vocaux ; de radio messagerie et fournir des interactifs multimédias ; y compris l'accès à l'internet, la téléconférence et d'autres services [5].

La norme LTE est faite pour fonctionner sur un très grand nombre de fréquences porteuses : à partir de 400 MHz et jusqu'au-delà de 3 GHz. Cela permet d'utiliser la technologie LTE pour des types de couvertures différents : pour des cellules et des transmissions longue-distance (plusieurs dizaines de kilomètres) aux fréquences les plus basses, ou des cellules à grosse capacité en environnement urbain aux fréquences plus élevées, voire des petites cellules à l'intérieur des bâtiments aux fréquences les plus hautes. Elle a utilisé des bandes de fréquences hertziennes d'une largeur pouvant varier de 1,4 MHz à 20 MHz [6].

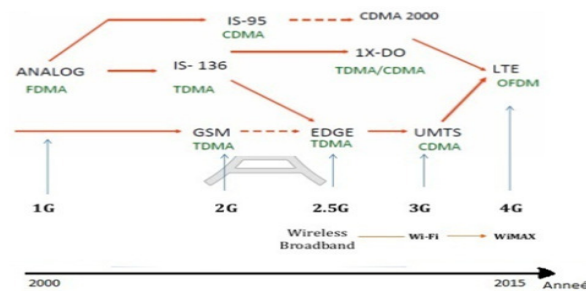


Figure 1.2 Evolution d'un réseau mobile [7].

Tableau 1.1 : comparaison entre différentes générations mobiles.

Technologie/la qualité	1G	2G	3G	4G
<b>Début d'utilisation</b>	1970/1984	1980/1991	1990/2002	2000/2009
<b>La bande passant</b>	1.9 Kbps	14.4 Kbps	2 Mbps	200 Mbps
<b>La bande de fréquence</b>	[450 900]Mhz	[0.9 1.8] GHz	[1.8 2.5] GHz	[2 8] Ghz
<b>Standard</b>	AMPS	TDMA CDMA GSM	WCDMA CDMA-2000	Standard unifié
<b>La technologie</b>	Technologie cellulaire analogique	Technologie cellulaire numérique	WCDMA Technologie IP	Technologie IP Interconnecter avec les réseaux
<b>Les services</b>	Téléphone mobile (la voix)	SMS, la voix numérique	Grande performance audio/vidéo/donnée intégrés	Accès dynamiques aux informations
<b>Multiplexage</b>	FDMA	TDMA, CDMA	CDMA	SC-FDMA, OFDMA

## 1.4 Chaîne de communication

La plupart des signaux que l'on doit être traité et analyser, tel que la parole, les signaux biologique, radar audio et vidéo sont analogique par nature, le but principal de la communication numérique est de transférer l'information de la source vers un ou plusieurs utilisateur à travers un canal de transmission avec la plus grand fiabilité possible. La figure 1.3 représente le schéma synoptique d'une chaîne de transmission numérique. Cette chaîne est constituée de plusieurs éléments, chaque élément jouant un rôle particulier et déterminant, ces rôles pouvant résumer comme suit :

### 1.4.1 Source :

Émet un message numérique sous forme d'une suite d'éléments binaires de transmission numérique

### 1.4.2 Codeur

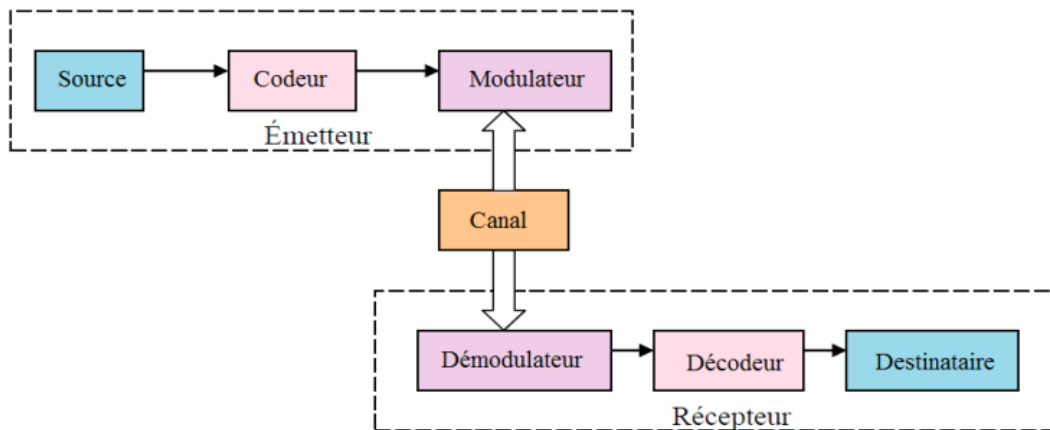
#### 1.4.2.1 Source

Peut éventuellement supprime tous les éléments binaires non significatifs (compression de donnée).

#### 1.4.2.2 Canal

Introduit de la redondance de l'information dans le but de la protéger contre les bruit présent de le canal (adaptation, comprissions).le codage canal n'est possible que c'est le débit de la source est inférieure à la capacité de canal. Suite au processus du codage et avant la transmission de cette information sur le canal doit converti en une forme mieux adaptée à sa transmission .le processus se norme la modulation.

A la réception, les fonctions du démodulateur annule l'effet de la modulation en estimant le symbole transmis et en le convertissant en bits. Le décodeur resitué à partir de la sortie du canal, L'information fournit par la source, il doit aussi comporter un caractère correcteur d'erreur permettent de trouver les donnée transmis avant le codage avec le minimum d'erreur.il existe plusieurs types de codage correcteur d'erreur, dont le codage par blocs et le codage convolutif. Dans le cadre de ce mémoire, nous nous intéresserons exclusivement au codage en bloc.



**Figure 1.3** modèle de la chaîne de communication numérique.

Dans le chapitre deux, nous donnerons plus de détail sur le code LDPC.

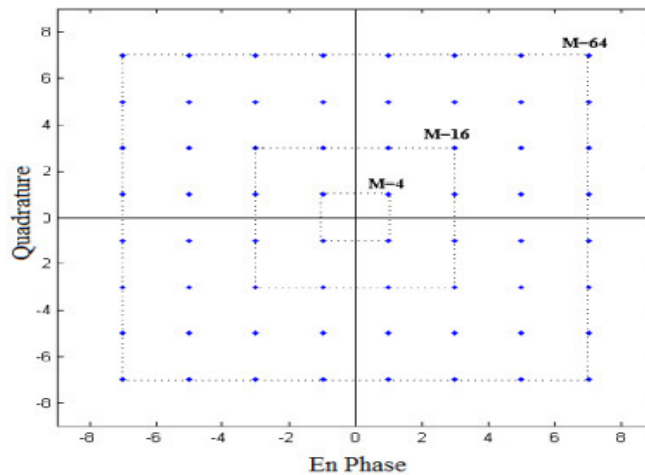
## 1.5 Technique de modulation

La modulation a pour rôle d'adapter le signal à émettre au canal de transmission. La modification peut porter sur un ou plusieurs paramètres d'une onde porteuse tels que l'amplitude, la phase ou la fréquence porteuse. Le spectre du signal généré doit être centré autour de la fréquence porteuse et ne doit pas dépasser la bande disponible. Ce signal peut être représenté par des symboles complexes discrets. L'opération de modulation est alors modélisée par une opération de conversion bits/symboles, appelée aussi mapping. En fait, elle consiste à associer à chaque ensemble de  $n$  éléments binaires de l'information utile un symbole complexe. A partir de  $n$  bits, il est possible de former  $M = 2^n$  symboles différents, appelé aussi alphabet de modulation. La modulation est alors d'ordre  $M$ , ou  $M$  représente le nombre de points de la constellation associée à la modulation. L'efficacité spectrale d'un système de communications est définie comme étant le nombre de bits d'information émis par unité de temps et par unité de bande occupée.

Elle est donnée par l'équation suivante :

$$\eta = \log_2 M (\text{bit} \cdot \text{s}^{-1} \cdot \text{Hz}^{-1}) \quad (1.1)$$

Par exemple les constellations correspondant à certains ordres de modulation pour la M-QAM sont représentées sur la Figure 1.4, lors de l'adoption d'un codage de Gray.



**Figure 1.4** Diagramme de la constellation de la modulation M-QAM pour  $M = 4$ , 16, et 64 [8].

Dans le cadre de cette étude, nous considérons uniquement les conversions bits/symbole par déplacement de phase à ( $M=2$ ) et ( $M = 4$ ) états, respectivement, ce qui correspond aux modulations BPSK et QPSK. Dans le cas de la modulation BPSK, un symbole est associé à  $n = 1$  bit d'information, tandis que pour la modulation QPSK, un symbole est associé à  $n=2$  bits d'information, transmis par les composantes en phase et en quadrature [8].

Avec l'augmentation des débits assurer une transmission fiable des données sur le canal radio devient un véritable défi. Dans ce cas-ci, une bonne compréhension du canal est primordiale pour concevoir des techniques efficaces de transmission et de réception.

## 1.6. Canal radio mobile

Les systèmes de communication sans fil sont limités en capacité et en performance à cause de multiples facteurs liés au canal de transmission. En effet, le signal émis subit des réflexions, de l'émetteur et le récepteur. Il s'en suit qu'au niveau du récepteur une multitude d'ondes est reçue mais arrive avec des amplitudes, des phases, des décalages Doppler et des retards distincts pour les différentes ondes. La combinaison de ces ondes peut se faire de façon constructive ou destructive, ce qui se traduit par des variations dans l'amplitude et la phase du signal reçu appelées évanouissement multi-trajets (voire la figure 1.5) [9].

### 1.6.1. Les classe des canaux radio-mobiles

On peut classer les canaux radio-mobil en deux catégories, à savoir :

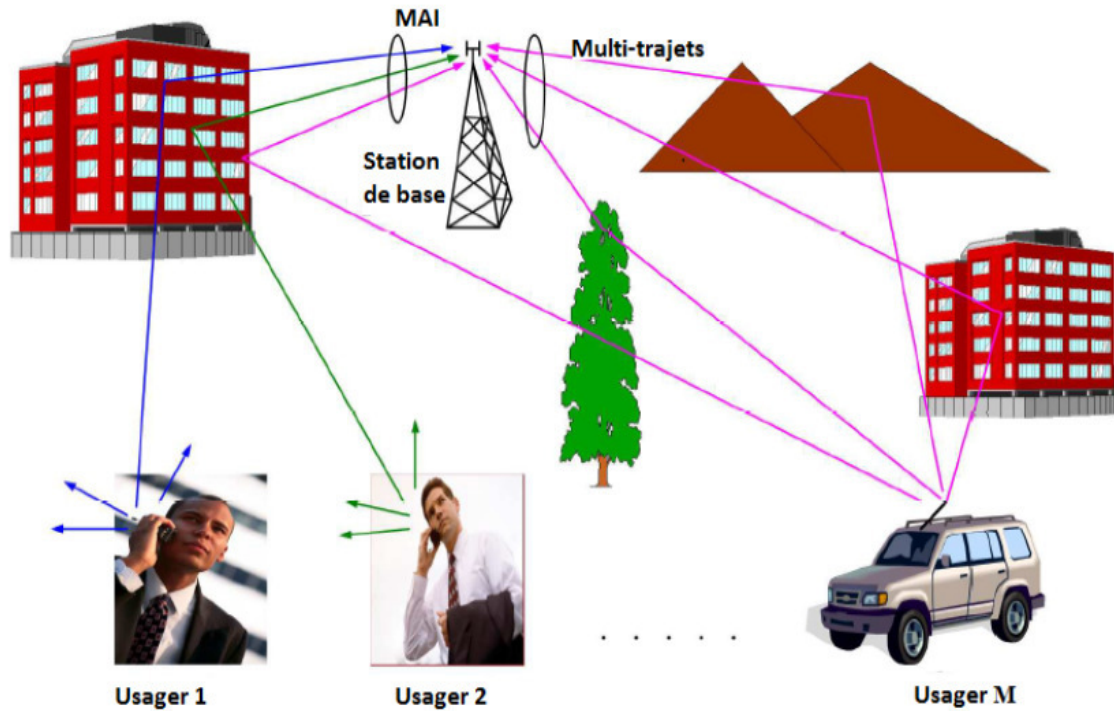


Figure 1.5 Scénario d’une transmission radio mobile sur un canal [9].

**1.6.1.1. Canal à évanouissement long terme**

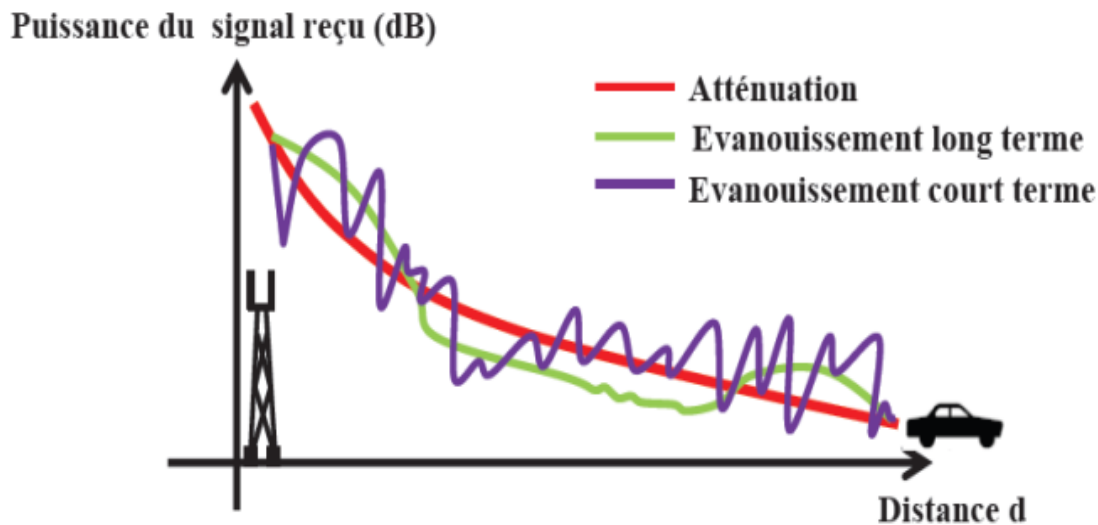
Représentant les atténuations de la puissance moyenne du signal résultant du mouvement sur des grands espaces. Il est généralement causé par l’atténuation moyenne et par le phénomène d’ombrage [10].

**- Atténuation moyenne (Pathloss)**

L’atténuation moyenne indique la façon dont la puissance du signal reçue diminue globalement en Moyenne en fonction de la distance entre l’émetteur et le récepteur. Dans l’espace libre la puissance n moyenne de signal diminue d’une façon inversement proportionnelle au carré de la distance entre la station de base et le mobile. Egalement, dans un canal radio mobile, ou la station de base et le mobile sont en visibilité directe LOS (Line Of Sight), la puissance moyenne du signal diminue en puissance de 2 en fonction de la distance. L’atténuation en puissance est alors donnée par :

$$Att(d) = \left(\frac{2\pi d}{\lambda}\right)^2 \tag{1.2}$$

Où  $\lambda$  est la longueur d’onde du signal transmis. Par contre, lorsque la station de base et le mobile ne sont pas en visibilité directe NLOS (None Line Of Sight), la puissance du signal diminue



**Figure 1.6** fluctuation à petit et à grand échelles de canal [12].

avec un exposant plus grand que 2 en termes de la distance. Cet exposant est alors compris entre 3 et 5 suivant le type d'environnement [11].

#### **-l'effet de l'ombrage (shadowing)**

Est dû à la présence d'obstacles entre l'émetteur et le récepteur. Aux fréquences auxquelles opèrent les systèmes de télécommunication, l'onde électromagnétique traverse ces obstacles, mais subit une atténuation en puissance fonction de la nature du matériau traversé.

Une situation typique est montrée à la figure 1.6 et facilite la compréhension des concepts atténuations moyenne ombrage et évanouissement plat [12], qui est décrit dans la prochaine section.

#### **1.6.1.2. Canal à évanouissement à court terme**

Se réfère à l'évolution rapide de l'amplitude et de la phase du signal sur une petite distance, qui peut être de l'ordre de quelque longueur d'onde, et pour de petites durées qui sont de l'ordre de quelque seconde. Il se manifeste principalement par une dispersion ou étalement du signal dans le temps et la variation du comportement du canal, les variations de puissance observées ont pour origine la présence d'objets dans l'environnement qui engendrent plusieurs réplique du signal transmis pouvant s'additionner de manière constructive ou destructive au niveau du récepteur c'est le fading.

Les signaux multiples qui s'ajoutent de manière constructive, donneront un signal résultant plus puissant que le trajet direct. Il faut noter que les multi-trajets n'ont pas que des inconvénients

puisqu'ils permettent que la communication soit possible même lorsque l'émetteur et le récepteur ne sont pas en vision directe.

### 1.7. Techniques d'accès multiples

Dans un système de communication sans fil multi-usagers, les ressources du système, dont la bande passante et la puissance, doivent être partagées par les différents usagers. Le partage de ses ressources pourra se faire dans des domaines divers : fréquentiel, temporel... etc. Cette allocation de ressources s'appelle l'accès multiple et plusieurs de ses techniques ont été proposées dans la littérature. Dans la conception de tout système de communication radio-mobile le problème de l'accès multiple c'est-à-dire, Celui du partage du support unique entre plusieurs utilisateurs, est une tâche importante. La répartition des ressources entre les différents utilisateurs d'un système de communications radio-mobiles a été réalisée de façon classique par trois techniques différentes [11] :

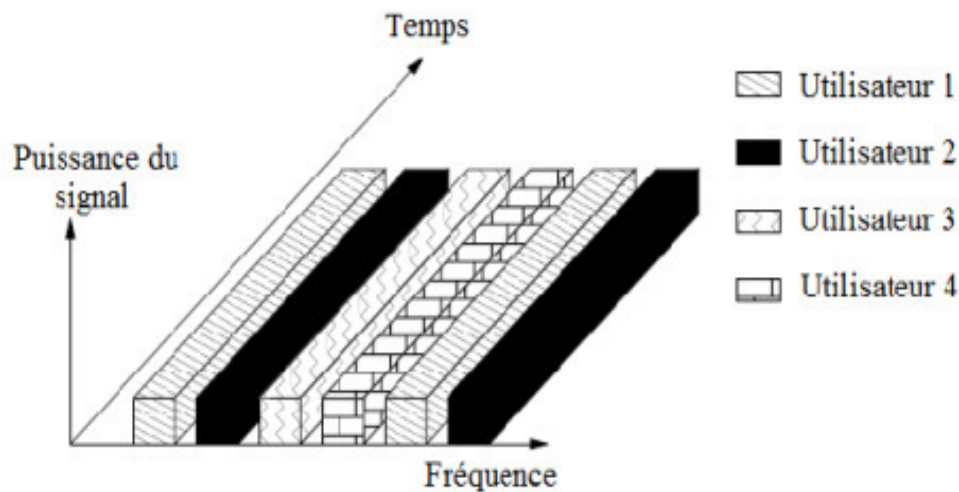
- La technique FDMA (Frequency Division Multiple Accès).
- La technique TDMA (Time Division Multiple Accès).
- La technique CDMA (Code Division Multiple Accès).

#### 1.7.1. Technique FDMA

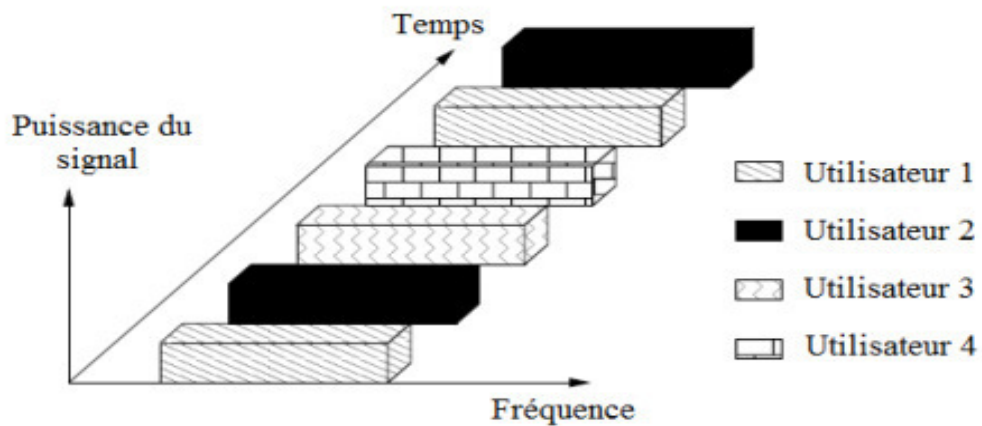
Dans la technique de multiplexage par répartition en fréquences FDMA, la répartition entre usagers est assurée en découpant le spectre en canaux de largeur suffisante et en attribuant chacun de ces canaux à un utilisateur qui désire établir une communication comme illustré à la Figure.1.7 En réception, la dissociation des usagers se fait par des opérations de filtrage. En revanche, son inconvénient majeur est le nombre maximal d'usagers devant partager la bande totale  $B$ . En fait, la largeur de bande allouée à chaque usager diminue avec l'accroissement du nombre total d'usagers admis dans la communication. Cette bande ne doit toutefois pas être trop faible afin d'éviter qu'à un instant donné toutes les composantes spectrales d'un signal ne soient fortement atténuées [13].

#### 1.7.2. Technique TDMA

Avec la technique d'accès multiple TDMA, les utilisateurs sont attribués de courts intervalles de temps, appelées slots temporels, pendant lesquels ils peuvent communiquer sur le canal. Un usager se voit affecter un ou plusieurs slots pour la durée de la communication telle qu'illustré à la Figure 1.8 Cette technique nécessite une synchronisation parfaite entre tous les émetteurs et les récepteurs [14].



**Figure 1.7** Technique d'accès multiple FDMA [13].

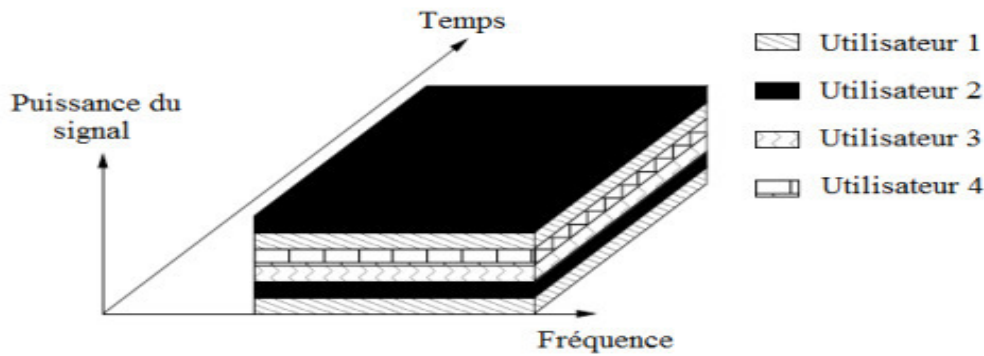


**Figure 1.8** Technique d'accès multiple TDMA [14].

Donc, dans les modes d'accès FDMA ou en TDMA. Le canal est d'composé en sous canaux indépendants, chaque sous-canal étant alloué à un utilisateur. Nous sommes donc confrontés à une approche de transmission assez classique ou la difficulté principale consiste à allouer les ressources libres (sous formes de slots de bandes ou de temps) aux utilisateurs [15, 14]. Pour pallier à cette difficulté, une nouvelle technique d'accès connue sous le nom de CDMA a vu le jour.

### 1.7.3. Technique CDMA

La technique CDMA est essentiellement basé sur la technologie d'étalement de spectre, il est approprié pour les transmissions codées. Avec la technique CDMA, tous les utilisateurs peuvent



**Figure 1.9** Technique d'accès multiple CDMA [17].

émettre simultanément dans une même bande de fréquence, permettant ainsi d'exploiter au maximum les ressources disponibles (voir Figure 1.9) [16]. On assigne une signature, ou code, à chaque utilisateur de manière à pouvoir les identifier au récepteur. L'orthogonalité, ou la quasi-orthogonalité, de ces signatures permet d'isoler chacun des canaux [17].

Diverses méthodes existent pour atteindre l'étalement de spectre, mais seul l'étalement de spectre par séquence directe.

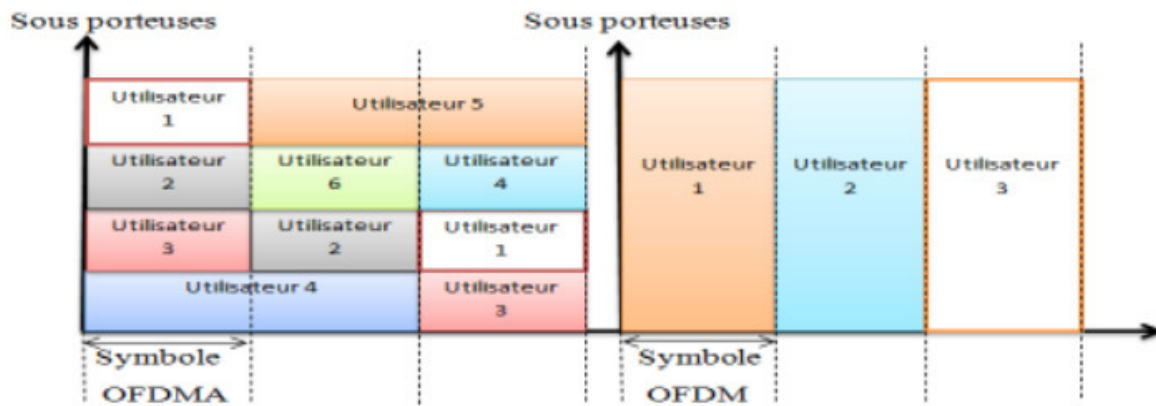
## 1.8 La combinaison (Orthogonal Frequency Division Multiples Accès)(OFDMA)

L'OFDMA est une combinaison de la technique d'accès multiple de le FDMA avec l'OFDM (Orthogonal Frequency Multiples Accès) qui fait partager les sous porteuses qui souvent alloués plusieurs utilisateurs actifs différents et dans un ou plusieurs OFDM [18].

### 1.8.1 OFDM

En général, l'OFDM est une technique de transmission où tous les sous porteuses alloués sont fixés pour la transmission des symboles d'un seul utilisateur, ce n'est pas une technique d'accès multiples. L'OFDM est donne la possibilité d'être associé à d'autres plusieurs techniques d'accès existant, tels que TDMA, FDMA ou CDMA pour devenir un système multi-utilisateurs. Alors l'OFDMA peut être considérée comme une technique hybride des techniques FDMA et TDMA. L'OFDM, le multiplexage à division de fréquence orthogonale, plus connu sous le nom anglophone OFDM, est une technique de modulation par les quelle un flux de données est subdivisée en plusieurs porteuses. L'OFDM est la technique dominante, puisque elle est utilisée par

De plusieurs applications comme la télévision numérique DVB ou la norme ADSL permettent les liaisons internet à haut débit, et aussi elle s'adapte parfaitement aux communications mobiles.



**Figure 1.10** La différence entre l'OFDM et l'OFDMA [19].

### 1.8.2. OFDMA (Orthogonale Frequency Division Multiple Accès)

L'OFDMA est une technologie de codage radio de type « Accès multiple par répartition en fréquence » qui est utilisée notamment dans les réseaux de téléphonie mobile de 4<sup>ème</sup> génération LTE. Elle est également utilisée par d'autres systèmes de radiocommunication, tels les versions évoluées des normes de réseaux locaux sans fil. Comme pour d'autres techniques de codage permettant l'accès multiples (TDMA, FDMA, CDMA), l'objectif est de partager une ressource radio commune (bande de fréquence) et d'en attribuer dynamiquement des parties à plusieurs utilisateurs.

L'utilisation de l'FDMA avec l'OFDM fait partager les  $k$  sous porteuses disponibles, en  $J$  groupes de sous porteuses qui seront allouées à  $J$  utilisateurs actifs différents et dans un ou plusieurs symboles OFDM comme le montre la figure 1.10 [19].

L'OFDM assigne un bloc de données à un utilisateur dans un intervalle de temps, comme on voit sur la figure 1.10, dans le cas où 4 utilisateurs veulent accéder au réseau. L'OFDMA est une méthode qui assigne différents groupes de sous porteuses aux différents utilisateurs, cette façon plus qu'un utilisateur peuvent accéder à l'interface radio en même temps, en se rappelant que dans l'OFDM tous les  $K$  sous porteuses sont consacrées pour apporter les données d'un seul utilisateur, alors que dans l'OFDMA assigne directement les sous porteuses qui sont consacrés pour apporter les données d'un seul porteuse de fréquence aux différents utilisateurs. Cette technique hérite les avantages de l'OFDM et aussi ces d'inconvénients, la différence entre l'OFDM et l'OFDMA c'est qu'en OFDMA la structure de données du symbole OFDMA est établie avant sa constitution dans le bloc IDFT (ou IFFT) c'est-à-dire, les sous porteuses dans un symboles OFDMA sont déjà allouées à plusieurs en forme de sous canaux (groupes de sous porteuses) par le mappeur des sous porteuses

(subporteurs mapper) avant d'être transformées par IDFT(ou IFFT).Le mappeur des sous porteuses Il utilise des schémas d'allocation dessous porteuses qui sont utilisées et préétablis aux différents utilisateurs. Les schémas sont basés sur l'exploitation de la diversité en fréquence ou la diversité utilisateur [19].

L'OFDMA et sa variante SC-FDMA sont dérivés du codage OFDM, mais contrairement à l'OFDM, l'OFDMA est optimisé pour l'accès multiple, ainsi qu'il est compatible avec la technique des antennes MIMO.

### 1.8.3 SC-FDMA (Signal Carrier Frequency Division Multiple Accès)

Le single-carrier FDMA est une technologie de codage radio de type accès multiple par répartition en fréquence utilisée notamment dans les réseaux de téléphonie mobile de 4ème génération LTE.

Comme pour d'autres techniques à schéma d'accès multiples (TDMA, FDMA, CDMA, OFDMA),

Le but est l'attribution et le partage d'une ressource radio commune (bande de fréquence) entre plusieurs utilisateurs. Le SC-FDMA peut être considéré comme une variante linéaire des codages OFDM et OFDMA, dans le sens où il consiste aussi à répartir sur un grand nombre de sous porteuses du signal numérique, mais il utilise en complément, une« **DFT** » (Transformation de Fourier discrète du signal) supplémentaire pour pré-coder l'OFDMA conventionnel [20].

### 1.8.4 Comparaison entre SC-FDMA et OFDMA

La technique de modulation SC-FDMA et la technique OFDMA qui ont été des systèmes concurrents lors de la normalisation des différentes générations. Il s'agit de dresser les points communs et les avantages et inconvénients de chaque technique.

L'OFDMA est une technique d'accès multiple basé sur l'OFDM, et adopté dans la norme 4G LTE pour les communications dans le sens descendant. Comme nous avons pu le constater que le système SC-FDMA a des ressemblances à bien des égards avec le système OFDMA.

On peut observer que le SC-FDMA n'est rien d'autre que de l'OFDMA avec un pré-codage DFT suivi d'un multiplexage particulier dans le domaine fréquentiel. Cette figure permet de relever les points communs entre ces deux techniques qui sont les suivants :

- Une transmission des données en blocs.
- Un multiplexage des données en fréquentiel au sens où ils réparties sur plusieurs sous-porteuses orthogonales.

- Une égalisation de canal réalisé dans le domaine fréquentiel.
- Un intervalle de garde pour prévenir des interférences entre blocs.
- Une complexité globalement équivalente.

La différence majeure entre elles, réside dans le fait que l'OFDMA est une technique de transmission multi-porteuse tandis que le SC-FDMA est une technique mono-porteuse [21].

## **1.9 Conclusion**

Les réseaux mobiles sont des réseaux qui offrent des avantages remarquables évitant les contraintes du câblage en premier lieu et assurant aux utilisateurs un environnement plus souple en effet les usagers restent connectés au réseau tout en se déplaçant dans la zone géographique impartie.

La 4ème génération vise à améliorer l'efficacité spectrale et à augmenter la capacité de gestion du nombre de mobiles dans une même cellule. Elle tente aussi d'offrir des débits élevés en situation de mobilité et à offrir une mobilité totale à l'utilisateur en établissant l'interopérabilité entre différentes technologies existantes.

## 2.1 Introduction

Dans tout système de communication, on cherche à transmettre l'information provenant d'une source vers un récepteur, à travers un canal de transmission. Les perturbations intervenant sur celui-ci induisent des erreurs de transmission que le codage de canal s'efforce de combattre. L'objectif est alors d'assurer un taux d'erreur minimal. La solution est basée sur l'insertion parmi les éléments d'information d'éléments supplémentaires (une redondance) qui suivent une loi connue pour corriger ces erreurs.

Dans ce chapitre nous allons présenter quelques généralités sur les codes correcteurs d'erreurs et leurs différents types et se baser surtout sur le code LDPC.

## 2.2 Les modèles de canaux de communication

### 2.2 Canal binaire symétrique

C'est un canal binaire caractérisé par la probabilité d'erreur  $p$  qu'au cours de la transmission un bit (0 ou 1) soit modifié en son opposé. Ces modifications se produisent indépendamment sur chacun des bits transmis. On représente ce canal par la figure 2.1.

#### 2.2.2. Canal Gaussien

Soit  $x_i \in A = \{0,1\}$  la séquence d'entrée discrète du canal gaussien. On appelle canal gaussien, le canal liant le signal d'entrée au signal de sortie selon la loi.

$$y_i = (-1)^{x_i} + N_i \tag{2.1}$$

Où  $N_i$  est une variable aléatoire suivant une loi normale  $N(0; \sigma_2)$ . La sortie  $y_i$  est une variable continue. Il est possible de définir une loi de décodage au maximum de vraisemblance.

$$\hat{x}_i, \dots, \hat{x}_n = \arg \min_x d(x, y) \tag{2.2}$$

Où chaque  $\hat{x}_i$  suit la loi

$$\begin{cases} \hat{x}_i = 0 & \text{si } y_i > 0 \\ \hat{x}_i = 1 & \text{si } y_i < 0 \end{cases} \tag{2.3}$$

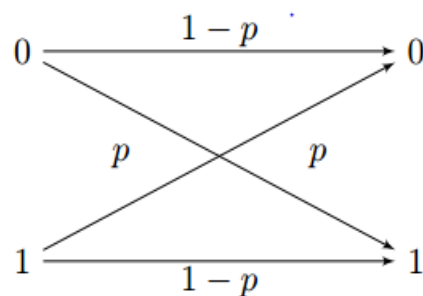


Figure 2.1 Canal binaire symétrique de probabilité d'erreur  $p$ .

Si la probabilité que 0 soit envoyée est la même que la probabilité que 1 soit envoyée. La probabilité que la quantification soit erronée ne dépend pas du bit transmis. On appelle cette probabilité  $P_{err}$ . On vérifie immédiatement que

$$P_{err} = P(N_i > 1) = \int_1^{\infty} \frac{1}{\sqrt{2\pi\delta^2}} e^{-\frac{t^2}{2\delta^2}} dt \quad (2.4)$$

Tel que  $\delta$  est la variance.

### 2.3. Codage canal

Le codage canal est un composant essentiel des systèmes de communication numérique. Bien que les techniques de modulation et d'égalisation avancées existantes permettent de combattre les effets d'interférence et l'ajout de bruit par le canal de propagation, le codage canal reste incontournable pour l'obtention de performances acceptables dans un système réel. En ajoutant de l'information redondante à la trame transmise, le codage canal permet d'assurer une certaine diversité temporelle. Le décodeur sous certaines conditions liées à la structure du code doit être capable d'exploiter cette diversité afin de récupérer l'information originale de l'émetteur.

À part les systèmes de télécommunications, on trouve également le codage canal dans un nombre d'applications comme les systèmes de transfert et de stockage de données pour garantir la fiabilité et l'intégrité de l'information. Suivant l'application visée, les en jeux sont très différents et le codage canal choisi doit s'y adapter. À titre d'exemple, dans un système de télécommunication radio mobile, le décodeur permet durant un temps très petit d'améliorer la qualité perçue de la voix avec un taux d'erreur raisonnable par rapport à la qualité de service requise. Cependant dans un système de stockage, les erreurs sont beaucoup plus critiques, mais la contrainte de temps d'encodage/décodage est moins importante.

### 2.4. Codes correcteurs d'erreurs

Un code correcteur est l'ensemble des mots de code obtenus après le codage. Les systèmes de communication utilisent un support de transmission, aussi appelé «canal de transmission», afin d'échanger de l'information d'un point à un autre. Le canal peut être de différents types : câble, fibre optique, canal radioélectrique : N'étant pas parfait, il introduit des perturbations, affaiblissement, écho, bruit qui détériorent l'information émise et créent des erreurs dans le message. Afin de fiabiliser le message (empêcher la perte de données due aux perturbations, bruit), les systèmes intègrent un processus de protection du message émis. Le principe général de cette protection est l'ajout de redondance, c'est-à-dire d'information supplémentaire, la plus

optimale possible en termes de coût, de volume et de contraintes qui dépendent largement du canal.

Soit un vecteur dont les composantes sont des éléments binaires pouvant avoir pour valeur 0 ou 1 et  $n$  le nombre d'élément binaire contenu dans sous vecteur nous définissons  $n$  comme la longueur du mot nous pouvons avoir  $2^n$  combinaisons différentes parmi lesquelles sont choisies  $2^k$  pour former un code, étant inférieure à  $n$ . Les  $2^k$  combinaisons retenues sont appelées mots de code, le codage est dit par blocs, les  $n$  éléments binaires forment un mot de code se répartissent de la manière suivante :  $K$  bits d'informations,  $n-k$  bits de contrôle. Un code ainsi constitué est désigné par l'expression code  $(n, k)$  on définit le rendement du code par le rapport  $R = k/n$ .

Le poids d'un codeword ou poids de hamming est le nombre de 1 dans un vecteur, l'ensemble des poids des différents mots d'un code est appelé distribution du poids, si tous les mots ont le même poids, le code est appelé code à poids fixe ou constant. La distance de hamming  $d_{ij}$  entre deux mots de code est définie par le nombre de bits en lesquels les deux mots diffèrent-la distance de hamming satisfait la condition  $0 \leq d_{ij} \leq n$  La plus petite valeur de  $d_{ij}$  dans un code est appelé distance minimum de code  $d_{\min}$ .

Pour le choix d'un code : on commence par fixer la longueur  $m$  des mots d'information. On veut un code qui détecte/corrige bien les erreurs, pour cela, il faut ajouter beaucoup de bits de contrôle, donc on a besoin d'une redondance élevée ( $r$  grand). Mais on veut aussi un code le plus économique possible, en vue d'une transmission rapide et/ou courte, donc on a besoin d'un rendement élevé, ce qui se traduit par un  $r$  petit. Par conséquent, on doit faire un compromis entre l'efficacité de la détection/correction et l'efficacité de la transmission, c'est-à-dire entre la redondance et le rendement. L'utilisation de méthodes mathématiques sophistiquées (par exemple l'algèbre sur des corps finis de polynômes) permet de fabriquer des codes efficaces sur ces deux points [22].

Dans ce mémoire nous regroupons les codes selon deux classes qu'ils soient linéaire ou convolutifs. A l'intérieur d'une classe nous distinguerons plusieurs familles de codes, chaque famille se distinguant des autres par ses propriétés structurelles. Nous donnons quelques exemples de familles de codes.

## 2.5. Codes linéaires

Soit  $C_i$  et  $C_j$  deux mots de code,  $\alpha_i$  et  $\alpha_j$  deux constantes binaires quelconques, le code est linéaire si et seulement si  $(\alpha_i C_i + \alpha_j C_j)$  est aussi un mot de code, nous avons les propriétés suivantes :

-Un code linéaire contient le vecteur nul (le vecteur constitué uniquement de 0), donc les codes à poids fixe ne sont pas linéaires.

-Si le vecteur nul possède l'indice 1, la distance de hamming par rapport à cet indice est égale au poids de hamming pour tous les vecteurs  $d_r = W_r$ .

-Les bits de contrôle sont une combinaison linéaire des bits d'information

-Algébriquement,  $k$  vecteurs linéairement indépendants sont nécessaires pour former une base orthogonale et générer un code linéaire le sous-espace complémentaire de dimension  $n - k$  est aussi un code linéaire [22].

## 2.6. Codes convolutifs

Les codes convolutifs ont été introduits en 1955 par p. Elias comme une alternative aux codes en blocs. Les codes convolutifs traitent l'information non plus des séquences de bits  $n$  dépendants, mais sur des blocs successifs avec une propagation du codage (codes à mémoire). nous nous limiterons ici aux cas binaire (le corps à 2 éléments). Un codeur convolutif binaire est défini par à l'aide de trois paramètres,  $n$  le nombre de sortie,  $k$  le nombre d'entrée et  $m$  la taille de la mémoire. A chaque unité de temps, le codeur lit  $k$  bits d'information et produit  $n$  bits codés (nous avons  $n$  supérieure à  $k$ ). les bits d'informations sont introduits dans des registres à décalage à états finis, les bits codés sont générés à partir d'une combinaison linéaire du contenu des registres à états comme le montre la figure 2.2.

On utilise  $k$  registres identiques de  $k$  bits chacun en entrée, et une sortie de  $n$  bits, à chaque arrivée de  $k$  bits en entrée, le contenu de chaque registre est transféré en bloc au registre qui le suit  $k$  bits d'information sont donc codés en  $n$  bits avec un autre paramètre définissant un codeur est son rendement ou taux, il correspond au rapport entre le nombre de bits en entrée et le nombre de bits en sortie  $k/n$  avec longueur de contrainte.

## 2.7. Différents codes correcteurs

### 2.7.1. Turbo Code

Les codes turbo-code ont été inventés en 1991 et présentés à la communauté scientifique en 1993, par une équipe de l'Ecole Nationale Supérieure des télécommunications de Brest dirigée par Claude Berrou et Alain Glavieux[23]. En raison de ses performances, le turbo code a été adopté par plusieurs organismes pour intégrer dans leurs standards c'est ainsi que la NASA a décidé d'utiliser les turbo-codes pour toutes ses sondes spatiales construites à partir de 2003. de son côté l'agence européenne (ESA) a été la première agence spatiale à utiliser le turbo code, avec

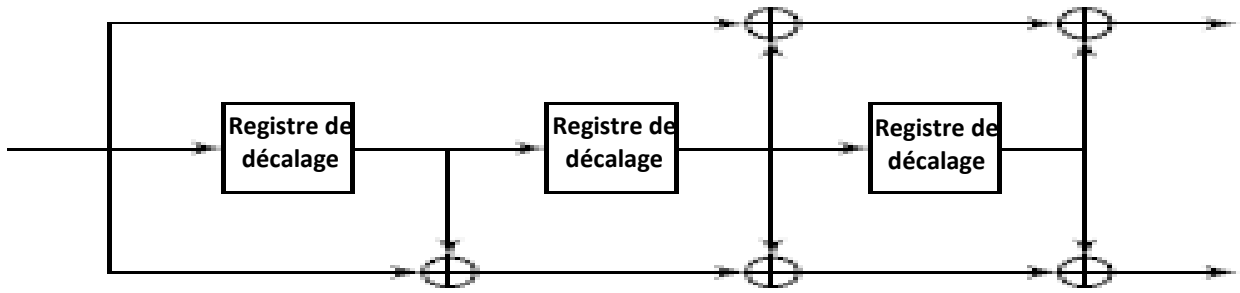


Figure 2.2 schéma d'un code convolutif.

sont de lunaire smart 1. Plus près de nous, le turbo code est utilisé dans la norme UMTS (téléphonique 3G) et l'ADSL<sub>2</sub>.

Les turbo-codes sont des codes en bloc, mais ses mots de code sont constitués de séquence provenant de codeur convolutif. Les codes convolutifs utilisés auront généralement une faible longueur de contrainte (3 ou 4) mais la taille des blocs T sera grand (plusieurs milliers de bit). La permutation n'est pas choisie aléatoirement, car elle a un impact important sur les performances.

En revanche, les « bonne » permutations (celles qui sont utilisées) sont souvent déterminées par tâtonnement (elles évitent les cycles de petite taille dans le graphe de Tanner associé au code), et n'ont a priori pas de propriétés particulières qui permettraient de les retrouver plus facilement. Nous considérons comme aléatoires.

### 2.7.2. Code à répétition

Le code à répétition consiste à répéter  $n$  fois le bit d'information. C'est un code  $[n; 1; n]$ , de dimension 1, de longueur  $n$  et de distance  $n$ . Pour  $n$  impair, ce code est parfait et optimal lorsque l'on protège un seul bit de donnée. En théorie de l'information pour un modèle de bruit blanc (canaux sans mémoire) et à rendement constant on peut avoir une probabilité d'erreur qui tend vers 0. Pour un code à répétition le rendement décroît pour une probabilité d'erreur qui tend vers 0. Ce code ne tire malheureusement pas parti du fait qu'il est plus efficace de protéger simultanément plusieurs bits d'information. Ce code est surtout utilisé en télécommunication pour reconnaître une modulation de signal.

### 2.7.3. Code de Hamming

Le code de Hamming se définit simplement au moyen d'une matrice de parité  $H$  de dimension  $m \times n$  et de longueur  $n = 2^m - 1$  et  $k = 2^m - 1 - m$  et  $n - k = m$ ; Par exemple, pour  $m = 3$  une des matrices de parité s'écrit :

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \quad (2.5)$$

Les colonnes de la matrice de parité étant toutes distinctes, la distance minimale du code est

### 3.2.7.4 Code cyclique

Les codes cycliques sont des codes linéaires stables dans lesquels toute permutation cyclique d'un mot de code est elle aussi un mot de code. À chaque mot de code  $C$  est associé un polynôme  $C(p)$  de degré  $\leq n - 1$

$$C = [C_{n-1}, C_{n-2} \dots C_1, C_0] \quad (2.6)$$

$$C(p) = C_{n-1}p^{n-1} + C_{n-2}p^{n-2} + \dots + C_1p + C_0 \quad (2.7)$$

Dans lequel les coefficients  $C_i$  sont les éléments binaires  $C_i = \{0, 1\}$  et  $p$  représente la variable libre. Soit le polynôme  $pC(p) = C_{n-1}p^n + C_{n-2}p^{n-1} + \dots + C_1p^2 + C_0p$  qui n'est pas un mot de code

$$\frac{pC(p)}{p^n + 1} = C_{n-1} + \frac{C_1(p)}{p^n + 1} \quad (2.8)$$

Avec  $C_{n-2}p^{n-1} + C_{n-3}p^{n-2} + \dots + C_0p + C_{n-1}$  (2.9)

$C = [C_{n-1} \dots C_1 C_0 C_{n-1}]$  Est le mot de code  $C$  par lequel une rotation à gauche d'une position a été effectuée.  $C_1(p)$  est le reste de la division de  $pC(p)$  par  $p^n + 1$  qui peut s'écrire

$$C_1(p) = pC(p) \bmod (p^n + 1) \quad (2.10)$$

On peut généraliser si  $C(p)$  est un mot de code

$$p^i C(p) = Q(p) \cdot (p^n + 1) + C_i(p) \quad (2.11)$$

$Q(p)$  : quotient ;  $C_i(p)$  : reste

On appelle polynôme générateur  $g(p)$  de degré  $n-k$

$$g(p) = p^{n-k} + g_{n-k-1}p^{n-k-1} + \dots + g_1p + 1 \quad (2.12)$$

Qui est un des facteurs du polynôme  $p^n + 1$

On désigne par le polynôme d'information  $X(p)$  de degré  $k - 1$

$$X(p) = x_{k-1}p^{k-1} + x_{k-2}p^{k-2} + \dots + x_1p + x_0 \quad (2.13)$$

Où  $[x_{k-1} x_{k-2} \dots x_1 x_0]$  représentent les  $k$  bits d'information.  $X(p)g(p)$  est un polynôme de degré  $\leq n-1$  qui représente un mot de code. Il ya  $2^k$  mots de codes possibles.

$$C_m(p) = X_m g(p) \quad m = 1, 2, \dots, 2^k \quad (2.14)$$

Une rotation à gauche de  $C(p)$  donne :

$$C_1(p) = pC(p) + C_{n-1}(p^n + 1) \quad (2.15)$$

Comme  $g(p)$  divise aussi bien  $C(p)$  que  $p^n + 1$ , on peut écrire :

$$C_1(p) = X_1(p)g(p) \quad (2.16)$$

$C_1(p)$  est un mot de code ; les mots de codes peuvent être générés à partir de  $g(p)$ .

On peut remarquer que les codes linéaires en général et les codes linéaires cycliques en particulier peuvent être mis sous forme systématique. Un code est dit systématique si on retrouve le message dans le mot de code. Les codes cycliques constituent une classe importante de codes. On trouve dans cet ensemble les codes de Reed Solomon et les codes de Golay. D'autre part la nature de ces codes a permis d'aboutir à des algorithmes de codage et de décodage très performants y compris dans le cas de codes en blocs de grande taille. Le paragraphe suivant présente en détail le fonctionnement d'un code de Reed Solomon.

### 2.7.5 Codes de Reed-Solomon

Les codes de Reed-Solomon sont des codes cycliques  $q$ -aires de longueur  $n = q - 1$ . Le polynôme générateur d'un code de Reed-Solomon est de la forme

$$g(x) = \prod_{i=1}^{d-1} (x - \alpha^i) \quad (2.17)$$

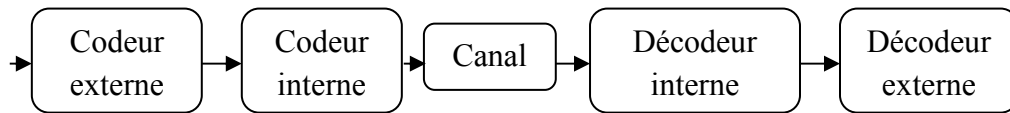
Où  $\alpha$  est un élément primitif du corps fini à  $q$  éléments. Il a pour degré  $d-1$ . Le code correspondant au polynôme générateur ci-dessus a pour longueur  $n = q - 1$ , pour distance minimale  $d$  et pour dimension  $k = n - d + 1$ . Nous avons donc affaire à des codes  $[n; k; n - k + 1]$ .

Ces codes sont efficaces dans les corrections d'erreurs par paquet du fait de leur structure. Ils ont été employés dans les communications spatiales et restent encore utilisés dans les codes concaténés.

### 2.7.6. Codes concaténés

Les codes concaténés ont constitué, et constituent toujours, l'une des constructions les plus utilisées pour obtenir une protection contre des niveaux de bruit importants. Ils risquent d'être supplantés dans les années à venir par les turbo-codes et les codes LDPC.

Dans un schéma concaténé, l'information est codée deux fois séquentiellement. Tels qu'ils ont été décrits initialement par Forney, ils utilisent deux codes en bloc. Le premier, le code externe, est défini sur un alphabet de grande taille  $q$  et le second, le code interne, binaire en général, codera chaque symbole  $q$ -aire afin de fournir une protection supplémentaire. Par la suite,



**Figure 2.3** schéma de code concaténé

le code interne a été remplacé par un code convolutif. Ce schéma concaténé avec un code convolutif interne et un code de Reed-Solomon externe a été standardisé pour les communications spatiales. Si l'on se place à la sortie du canal, tout se passe comme si la séquence codée provenait du code interne seul. Ce codeur permet une forte résistance au bruit.

L'ajout de redondance sur un code en possédant déjà avec le premier codeur offre la possibilité de retrouver l'information là où un seul codeur n'aurait pas suffi pour la retrouver.

Comme le montre dans la Figure 2.3 le schéma de codage d'un code concaténé le décodage s'effectue dans l'ordre inverse du codage. Chacun des codes utilisera un algorithme ad hoc. La construction est efficace car les codes sont complémentaires. Schématiquement, le code interne va corriger les erreurs isolées et le code externe les rafales. De plus, dans les décodeurs les plus élaborés, le résultat du décodage interne pourra être assorti d'une information de fiabilité qui améliore (marginale) les performances du décodeur externe (plus le décodeur interne à corrige d'erreurs, moins l'information fournie est fiable).

## 2.8 Codes LDPC

### 2.8.1 Historique

Bien qu'étant une technique ancienne (ils ont été inventés par Gallager en 1962), les codes LDPC n'ont été sérieusement envisagés pour les applications en télécommunications qu'à partir de l'avènement du décodage itératif dans les années 90. Les codes LDPC sont parmi les codes binaires les plus performants connus, [24, 25]. Ils sont d'ailleurs prévus en option dans les normes IEEE 802.11n (WiFi), 802.16e (802.20 (MBWA)) et 802.22 (WRAN) ainsi que dans les futures normes de téléphonie 4G.

Ils présentent un certain nombre d'avantages et leurs nombreux degrés de liberté rendent facile leur optimisation et adaptation à des contextes applicatifs très différents.

Gallager a également proposé [26] un algorithme de décodage pour ses codes mettant en œuvre des fonctions de vérification de parité. En 1981, Tanner [27] introduit les graphes pour décrire ces codes, et étend les opérations de vérification de parité vers des fonctions plus générales. Ceci a permis le développement d'un algorithme générique « Somme-Produit » puis « Min Sum » par Wiberg [28]. Les graphes factoriels [29] sont aujourd'hui un outil puissant pour

différentes applications en traitement du signal. Les graphes factoriels permettent d'effectuer des calculs complexes d'une manière plus efficace en transformant des fonctions de plusieurs variables en un produit de facteurs localement indépendants.

### 2.8.2 Caractéristiques et avantages

Les codes LDPC forment une famille de codes linéaires obtenus à partir de matrices de parité creuses (Ils sont caractérisés par le faible nombre de « 1 » (densité de « uns ») de leurs matrices de contrôle de parité). Bien que leur définition ne l'impose nullement, les codes LDPC utilisés (et les seuls que nous considérerons pour le moment) sont binaires. Les codes LDPC ont par définition une matrice de parité creuse (le poids de chaque ligne vaut quelques unités, alors que la longueur peut atteindre plusieurs milliers). La performance de l'algorithme de décodage tient essentiellement à la faible densité de la matrice.

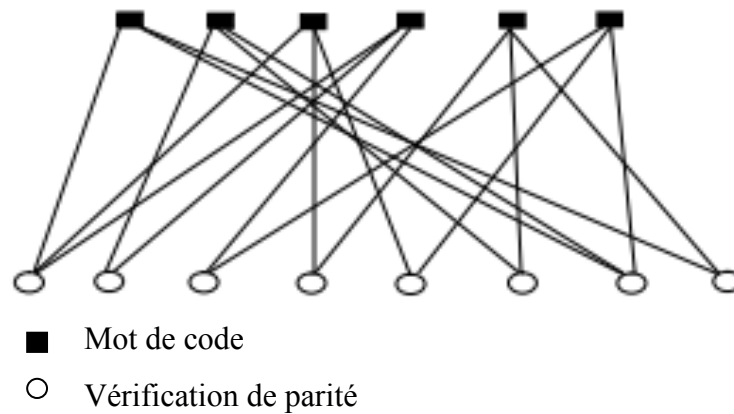
Les codes LDPC sont en grande compétition avec les codes turbo dans les systèmes de communications numériques qui demandent une fiabilité élevée. Aussi, les codes LDPC ont quelques avantages par rapport aux codes turbo :

- (a) ils ne nécessitent pas d'entrelacer pour réaliser une bonne performance d'erreur.
- (b) ils ont une meilleure performance par trame.
- (c) leur plancher d'erreur se produit à un niveau de BER de beaucoup inférieur.
- (d) leur décodage n'est pas basé sur un treillis et peut être réalisé par un processus parallèle.

Pour des grands taux et longueurs, les codes LDPC ont des meilleures performances que les codes turbo. Ils sont appliqués aux systèmes OFDM (Orthogonal Frequency Division Multiplexing) et aux systèmes de codage espace-temps. Récemment, ils ont été sélectionnés pour la norme de transmission vidéo numérique (DVB) et pour des applications en temps réel comme le stockage magnétique, l'Ethernet à 10 GB et les réseaux locaux sans fil avec débit élevé (WLAN).

### 2.8.3 Graphes de Tanner

Les graphes de Tanner [30] sont très utiles pour la représentation des codes en blocs linéaires, parce qu'ils affichent la relation entre les bits des mots-codes et les nœuds de contrôle de parité. Ils ont été proposés pour la première fois par Tanner pour le décodage itératif des codes LDPC. Les codes LDPC sont représentés sous forme de graphes bipartites. Un graphe est bipartite si son ensemble de nœuds ( $V$ ) peut être divisé en deux sous-ensembles disjoints  $V_1$  et  $V_2$ , tels que chaque arête joint un nœud dans  $V_1$  avec un nœud dans  $V_2$  et sans que deux nœuds



**Figure 2.4** Graphe factoriel d'un code LDPC

dans  $V_1$  ou dans  $V_2$  soient connectés. Pour un code LDPC, les deux ensembles de nœuds  $V_1$  et  $V_2$  représentent les  $n$  bits du mot-code (nœuds des variables) et les  $J$  équations de contrôle de parité qui doivent être satisfaites par les bits codés (nœuds de contrôle). Toutes les connexions sont faites entre chaque nœud de bit codé et ses nœuds de contrôle correspondants (qu'on vérifie dans la somme de contrôle).

Un chemin dans un graphe est une séquence de nœuds et d'arêtes, qui commence et finit par des nœuds, tel que chaque arête est incidente avec les nœuds qui la précèdent et la suivent et aucun nœud n'apparaît plus d'une fois. La longueur d'un chemin est donnée par le nombre d'arêtes formant le chemin. Un chemin qui commence et finit avec le même nœud s'appelle cycle. Si un graphe bipartite contient des cycles, ces cycles ont des longueurs paires. La longueur du plus court cycle dans le graphe s'appelle le périmètre du graphe.

Pour un code LDPC régulier, les degrés de tous les nœuds de bits codés sont égaux à 7 (le poids de chaque colonne de la matrice  $H$ ) et les degrés de tous les nœuds de contrôle sont égaux à  $p$  (le poids de chaque rangée de la matrice  $H$ ). Ainsi, le graphe de Tanner est régulier. Il ne peut pas y avoir deux bits codés qui peuvent être vérifiés par deux équations différentes, donc le graphe ne va contenir aucun cycle de longueur 4. Pour décoder un graphe d'un code LDPC avec le décodage itératif, il est important que le graphe de Tanner du code ne contienne aucun cycle de courte longueur (4 ou 6, mais en particulier 4), parce que les cycles courts limitent la performance d'erreur et empêchent le processus de décodage de converger vers la performance obtenue avec le décodage à vraisemblance maximale MLD (Maximum Likelihood Decoding) [31,32].

#### 2.8.4 Codes LDPC irréguliers

Au lieu d'avoir des degrés de connexion fixes, les nœuds du graphe d'un code LDPC peuvent avoir des degrés de connexion différents, d'où l'appellation de « codes irréguliers ».

[33], Luby et al, donnent une extension de l'étude de Gallager sur des graphes irréguliers.

Ils montrent que les performances des codes irréguliers sont meilleures et donnent une première approche de construction de codes irréguliers. Cette approche a été développée plus tard pour obtenir des performances proches de la limite de capacité de Shannon. La structure du code est définie à l'aide des deux polynômes  $\lambda(x)$  et  $\rho(x)$  :

$$\lambda(x) = \sum_{i=2}^{d_c} \lambda_i \cdot x^{i-1} \quad 0 \leq \lambda_i \leq 1 \quad \sum_{i=2}^{d_c} \lambda_i = 1 \quad (2.18)$$

$$p(x) = \sum_{i=2}^{d_c} p_i \cdot x^{i-1} \quad 0 \leq p_i \leq 1 \quad \sum_{i=2}^{d_c} p_i = 1 \quad (2.19)$$

$\lambda_i$  et  $p_i$  sont les proportions des branches du graphe connectées à des nœuds de variable (respectivement de parité) dont le degré de connexion est égal à  $i$ .

Soit  $t$  le nombre total d'arêtes dans le graphe, on note par  $v_i$  (resp  $c_i$ ) le nombre de nœuds de variable (resp de parité) de degré  $i$ . Les égalités suivantes lient alors les paramètres du code à sa structure :

$$v_i = \frac{t - \lambda_i}{i} \quad N = l. \sum_{i=2}^{d_c} \frac{\lambda_i}{i} = l. \int_1^0 \lambda(x) dx \quad (2.20)$$

$$c_i = \frac{t - p_i}{i} \quad M = l. \sum_{i=2}^{d_c} \frac{p_i}{i} = l. \int_1^0 p(x) dx \quad (2.21)$$

$$R = 1 - \frac{\sum_{i=1}^{d_c} \frac{p_i}{i}}{\sum_{i=1}^{d_c} \frac{\lambda_i}{i}} \quad (2.22)$$

### 2.8.5. Codes LDPC réguliers

En utilisant la représentation de Tanner, on définit les nœuds de variable, les nœuds qui représentent les bits (information et redondance) du mot de code. On définit également les nœuds de parité, ceux représentant la contrainte placée sur les nœuds de variable auxquels il est connecté. Les premiers codes LDPC proposés par Gallager [26] ont une structure régulière. Les nœuds de variable et les nœuds de parité ont des degrés de connexion  $d_v$  (respectivement  $d_c$ ) constants. Toutes les colonnes ont alors le même nombre de positions non nulles. Cette condition est valable aussi pour les lignes. Le nombre total de positions non nulles dans la matrice est égal au nombre d'arêtes du graphe. On en dérive :

$$N \cdot d_v = (N - K) \cdot d_c \Rightarrow \frac{K}{N} = R = 1 - \frac{d_v}{d_c} \quad (2.23)$$

Avec le même couple  $(d_v, d_c)$ , plusieurs codes réguliers peuvent être définis selon le choix des positions non nulles dans la matrice  $H$ .

### 2.8.6. Encodage LDPC

L'encodage LDPC est une opération classique qui consiste à engendrer un mot de code  $x = [u, p]$  à partir du mot d'information  $u$ , de la matrice génératrice  $G$  ou de la matrice de contrôle de parité  $H = [H_s, H_p]$ . L'encodage LDPC est très lié à la structure du code, ainsi si la partie  $H_p$  de la matrice possède une structure triangulaire la complexité de l'encodage peut être réduite significativement. En effet le calcul des bits de redondance devient une simple substitution. Plus particulièrement, avec une structure bi-diagonale de  $H_p$ , le code LDPC peut être considéré comme un code de la famille Repeat and Accumulate [34,35] ou une concaténation d'un code de parité et d'un accumulateur [36]. Des codes LDPC de ce type ont été retenus dans les normes WiFi 802.11n et Wimax 802.16e, et leur encodage revient à une simple accumulation de bits. Le résultat est une matrice partiellement triangulaire. Plus la partie triangulaire est grande moins complexe est l'encodage. On note que l'encodage LDPC peut aussi être réalisé en utilisant l'algorithme de décodage somme produit et en remplaçant les bits de parité inconnus par des effacements, mais cette méthode n'est pas intéressante à cause de sa grande complexité.

### 2.8.7 Algorithmes de décodage des codes LDPC

Dans cette section, nous allons présenter un des algorithmes permettant le décodage des codes LDPC. Dès que la taille du mot de code devient importante, ce qui est une hypothèse nécessaire afin d'obtenir des performances convenables, le décodage au sens du maximum de Vraisemblance présente une complexité trop importante pour permettre une réalisation pratique.

Pour pallier à ce type de problème, Gallager présenta un algorithme de décodage itératif sous optimal avec nombre constant d'opération par bit. Cet algorithme a ensuite été revu par MacKay et Kschischang et Al, dans le cadre de la théorie des graphes. L'algorithme résultant est alors connu sous plusieurs noms tels que propagation de croyance (belief propagation). Ou bien encore algorithme, somme-produit (sum-product). Cet algorithme peut être vu comme un algorithme de propagation de messages sur le graphe factoriel associé. Les messages transitant par les branches du graphe peuvent être soit des probabilités, soit les logarithmiques des rapports de vraisemblance. Le principe de la propagation de croyance est l'application de la règle de Bayes localement (soit sur chaque bit) et itérativement afin d'estimer les probabilités a posteriori de chaque bit. Dans le cadre d'un décodage sur un graphe sans cycle (le graphe est alors un arbre)

c'est-à-dire dans le cas où tous les messages sont indépendants, la factorisation locale des règles de Bayes conduit au calcul exact des probabilités a posteriori des nœuds de données.

Dans certains cas incluant cas celui des codes LDPC, le graphe factoriel présente des cycles.

Dans ces conditions, du fait de la dépendance cyclique des différents messages, le calcul exact des probabilités a posteriori n'est plus assuré. Cependant, plus un graphe est creux plus la dépendance entre les différents messages sera faible. De plus, pour minimiser cette dépendance il est nécessaire de calculer plusieurs fois les messages sur les branches ce qui mène à une utilisation itérative de l'algorithme de propagation de croyance.

### 2.8.7.1 Propagation de croyance

Chaque itération de l'algorithme de propagation de croyance est composée de deux étapes [37]:

-Une étape de mise à jour des messages lorsqu'ils passent par un nœud de donnée appelée data passe.

-Une étape de mise à jour des messages lorsqu'ils passent par un nœud de contrôle appelé Check passe

Afin de faciliter la lecture de ce mémoire, les messages utilisés seront des log-rapports de vraisemblance. Notons  $v = \log \frac{p(y'|c'=0)}{p(y'|c'=1)} = \log \frac{v(0)}{v(1)}$  le message de sortie d'un nœud de donnée et  $u = \log \frac{p(y'|c'=0)}{p(y'|c'=1)} = \log \frac{u(0)}{u(1)}$  le message de sortie d'un nœud de contrôle.

### 2.8.7.2 Mise à jour des messages sur un nœud de donnée : Data pass

Lors de la mise à jour sur le nœud de donnée k de degré i à l'itération l, le message envoyé sur la q<sup>ième</sup> branche est donné par la relation suivante :

$$v_q^{(1)} = u_0 + \sum_{n=1; n \neq q}^i u_n^{(l-1)} \quad \forall q = 1, \dots, i \quad (2.24)$$

Où  $u_n, n = 1 \dots i$ , représentent les messages venant des nœuds de contrôle voisins et  $u_0 = \log \frac{p(y_k|c_k=0)}{p(y_k|c_k=1)}$  représente le log-rapport de vraisemblance observé en sortie du canal. A la première itération, tous les messages  $u_n^{(0)}$  venant des nœuds de contrôles sont considérés comme nuls.

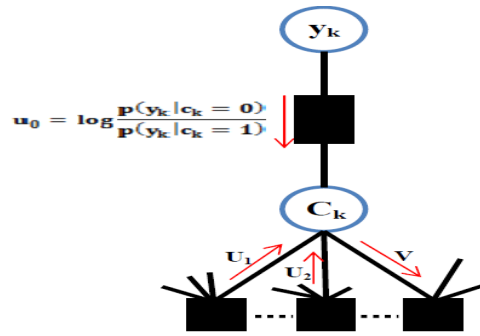


Figure 2.5 illustration du data pass.

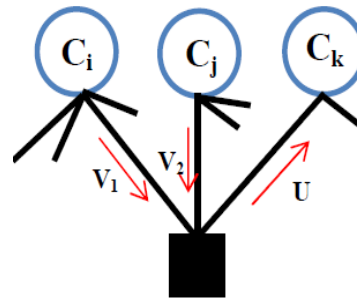


Figure 2.6 illustration du check pass.

### 2.8.7.3 Mise à jour des messages sur un nœud de contrôle : Check pass

Ensuite, lors de la mise à jour sur un nœud de contrôle de degré  $j$ , le message de sortie sur la  $p^{\text{ième}}$  branche est donné par l'expression :

$$\tanh\left(\frac{u_p}{2}\right) = u_0 + \prod_{m=1; m \neq p}^j \tanh\left(\frac{v_m^{(1)}}{2}\right) \quad \forall p = 1, \dots, \dots, j \quad (2.25)$$

Où  $v_m$ ,  $m = 1, \dots, \dots, j$ , sont les messages venant des nœuds de données voisins.

## 2.9 Conclusion

Dans ce chapitre, nous avons décrit les notions de base sur les codes correcteurs d'erreur, nous regroupons les codes selon deux classes : linéaires ou convolutifs. A l'intérieur d'une classe, il existe plusieurs familles de codes, chaque famille se distingue des autres par ses propriétés structurelles. Nous avons donné quelques exemples de familles de codes, en plus d'une explication des graphes de Tanner, qui sont une représentation utile des codes linéaires et en particulier des codes LDPC.

On a expliqué comment on peut construire différents types de codes LDPC, comme les codes LDPC réguliers, les codes LDPC irréguliers. On a présenté à la fin les algorithmes de décodage des codes LDPC.

### 3.1 Introduction

Dans les codes correcteurs d'erreurs, Il existe plusieurs manières pour générer les matrices génératrices comme celles utilisées dans les codes cycliques qui utilisent une matrice génératrice plus complexe basée sur les polynômes générateurs. Notre construction est basée sur une méthode simple des codes LDPC linéairement indépendants le et donnent une matrices génératrices systématique G plus simple.

### 3.2 Algorithme de codage LDPC

Un code LDPC peut être représenté sous forme matricielle ou bien sous la forme d'un graphe bipartite (représentation de Tanner). Les k bits d'information  $X_m$  et qui seront codées dans un mot de code  $C_m$  d'une longueur n.

L'information

$$X_m [x_{m1} \ x_{m2} \ x_{m3} \ \dots \dots] \quad (1 \times k) \quad (3.1)$$

Le code :

$$C_m = [c_{m1} \ c_{m2} \ \dots \dots \ c_{mk} \ c_{mk+1} \ \dots \ c_{mn}] \quad (1 \times n) \quad (3.2)$$

Chaque bit du mot de code est une combinaison linéaire des bits d'information

$$C_m = X_m \cdot G \quad (3.3)$$

Où G est appelé matrice génératrice

$$\begin{bmatrix} g_{11} & g_{12} & \cdot & \cdot & g_{1n} \\ g_{21} & g_{22} & \cdot & \cdot & g_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ g_{k1} & g_{k2} & \cdot & \cdot & g_{kn} \end{bmatrix} = \begin{bmatrix} g_1 \\ g_2 \\ \cdot \\ \cdot \\ \cdot \\ g_k \end{bmatrix} \quad (3.4)$$

Les lignes  $\{g_i\}$  de la matrice G doivent être linéairement indépendantes pour former une base pour le code tel que le rang de G est égal à k. La matrice G n'est pas unique ; Toute matrice G peut être mise sous la forme systématique

$$G = [I_k | P] \quad (3.5)$$

$I_k$  est la matrice identité de dimension  $k \times k$

P est la matrice de contrôle  $k \times m$  (m : est les bits de contrôle)

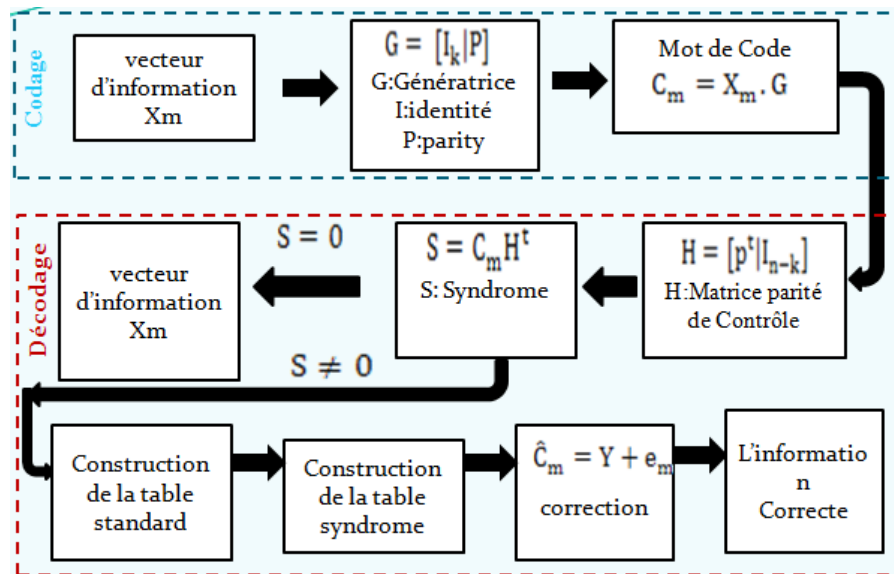


Figure 3.1 étapes d'un algorithme codage et décodage LDPC.

Le code est généré par une matrice  $G$  sous forme systématique est appelé code symétrique Dans chaque mot de code, les  $k$  premiers bits représentent l'information et sont suivis de  $n - k$  bits de contrôle.

### 3.3 Codage d'information à 4 bits et à 5 bits

#### - vecteurs d'information et de code à 4 bits

Nous allons coder les bits d'information représentés par le vecteur  $X_m$  en un mot de code  $C_m$ . Ce vecteur d'information est donné par :

$$X_m = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Les  $n$  éléments binaires formant un mot de code se répartissent de la manière suivante :

$k$  Bits d'information

$n - k$  Bits de contrôle

Un code ainsi constitué a le rendement  $R = \frac{k}{n}$  :

$$k = 4 \quad n = 7 \quad \text{Donc le } R = \frac{K}{n} = 0.57$$

Nous allons utiliser la matrice identité de cette information de (4x4) qui est une matrice diagonale (I) ; on peut voire immédiatement dans cet exemple que les bits de la matrice de parité de 3 bits donnent la matrice génératrice :

$$G = X_m \cdot C_m^{-1} .$$

On donne la matrice de parité et la matrice identité comme suit :

$$\begin{aligned}
 p_1 &= I_1 + I_2 + I_3 \\
 p_2 &= I_2 + I_3 + I_4 \\
 p_3 &= I_1 + I_2 + I_4
 \end{aligned}$$

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad
 P = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad
 G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Le code généré par une matrice G sous forme systématique est appelé code systématique, dans chaque mot de code, les k premières bits représentent l'information et sont suivis de n-k bits de contrôle nous allons trouver le mot de code Cm :

$$C_m = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

**- Vecteur d'information et de code à 5 bit**

Nous allons coder les bits d'information représentés par le vecteur Xm en un mot de code Cm. Ce vecteur d'information est donné par :

$$Xm = \begin{matrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{matrix}$$

### -Matrice génératrice

Les  $n$  éléments binaires formant un mot de code se répartissent de la manière suivante :

$k$  Bits d'information

$n - k$  Bits de contrôle

Un code ainsi constitué a le rendement  $R = \frac{k}{n}$  :

$$K = 5 \quad n = 8 \quad \text{Donc le } R = \frac{K}{n} = 0.625$$

Nous allons utiliser la matrice identité de cette information de (5x5) qui est une matrice diagonale (I) ; on peut voire immédiatement dans cet exemple que les bits de la matrice de parité de 3 bits donnent la matrice génératrice :

$$G = Xm \cdot Cm^{-1} .$$

On donne la matrice de parité et la matrice identité comme suit :

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad p = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Le code généré par une matrice G sous forme systématique est appelé code systématique, dans chaque mot de code, les k premières bits représentent l'information et sont suivis de n-k bits de contrôle nous allons trouver le mot de code Cm :

$$C_m = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

### 3.4 Algorithme de décodage LDPC

La matrice duale de G est appelée la matrice de contrôle de parité

$$H = [p^t | I_{n-k}]$$

Elle possède les propriétés suivantes :

$$C_m H^t = 0$$

$$GH^t = 0$$

Le syndrome est calculé pour vérifier s'il y a des erreurs ou non. Dans ce qui suit, nous allons effectuer le décodage des symboles à 4 bits et à 5 bits.

### 3.5 Décodage d'information à 4 bits et à 5 bits

#### -Matrice de contrôle à 4 bits

La matrice duale de G est appelée matrice de contrôle de parité il constitué la matrice transposé de parité et la matrice identité de dimension  $n - K = 7 - 4 = 3$

On donne la matrice transposé de parité et la matrice identité comme suit :

$$p^t = \begin{matrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{matrix} \quad I_{n-k} = \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{matrix}$$

On a trouvé la matrice comme suit :  $H = [p^t | I_{n-k}]$

Un code LDPC peut être représenté sous forme matricielle ou bien sous la forme d'un graphe bipartite (représentation de Tanner) :

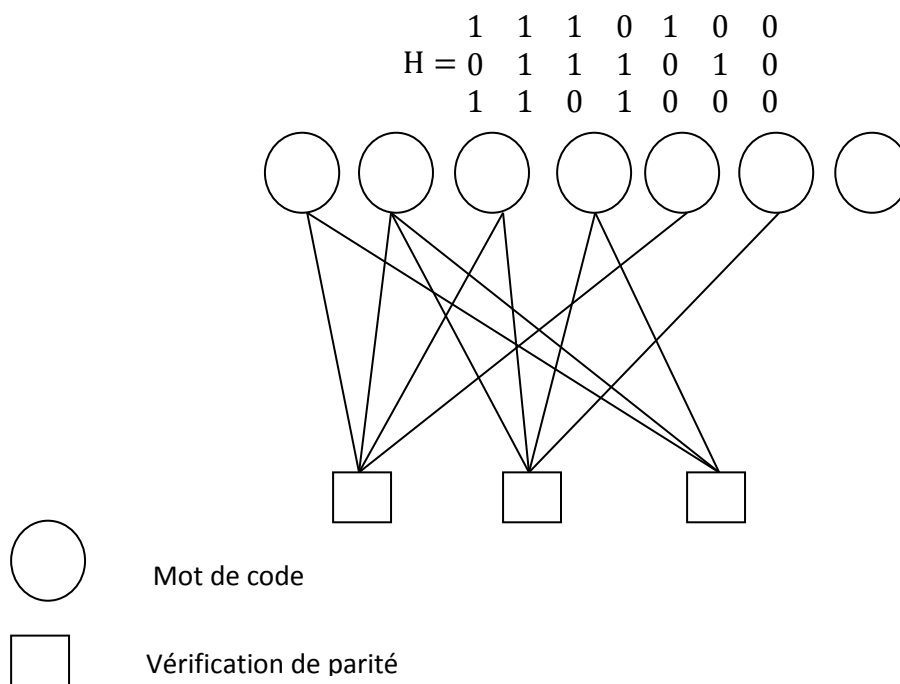


Figure 3.2 Graphe bipartite d'un code LDPC de 7 bit

**-Syndrome**

Le résultat obtenu après la multiplication de la transposée de la matrice de contrôle et le code  $C_m$  est égal à 0 donc le code  $C_m$  a été sans une erreur, car il donne une valeur de syndrome nulle :

$$S = 0 \ 0 \ 0$$

**-Matrice de contrôle à 5 bits**

La matrice duale de  $G$  est appelée matrice de contrôle de parité il constitue la matrice transposée de parité et la matrice identité de dimension  $n - K = 8 - 5 = 3$  On donne la matrice transposée de parité et la matrice identité comme suit :

$$p^t = \begin{matrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{matrix} \quad I_{n-k} = \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$$

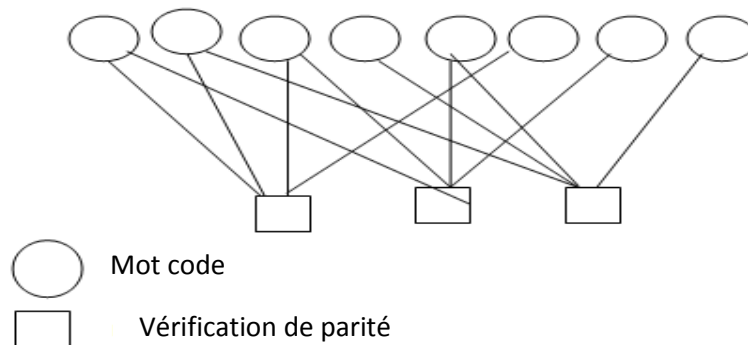
On a trouvé la matrice comme suit :  $H = [p^t | I_{n-k}]$

Un code LDPC peut être représenté sous forme matricielle ou bien sous la forme d'un graphe bipartite (représentation de Tanner) :

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

**- Syndrome**

Le résultat obtenu après la multiplication entre la transposée de la matrice de contrôle et le code  $C_m$  donne un vecteur nul, donc, nous recevons un symbole sans une erreur



**Figure 3.3** Graphe bipartite d'un code LDPC de 8 bit.

**3.6 Introduction et correction des erreurs**

Nous allons introduire une erreur  $e$  et nous vérifierons les vecteurs  $Y$  reçus ; par l'utilisation de :

$$S = Y * H' \neq 0$$

Donc, il y a des erreurs dans le vecteur reçu et pour les corriger nous utilisons les étapes suivantes :

**- Construction de la table standard et les vecteurs d'erreurs**

Qui est construit de la manière suivant :

La première ligne contient le  $2^k$  mot de codes possible en commençant par le mot dont tous les éléments sont des 0. cette ligne représente donc les mots transmis sans erreur  $e_i = 0$ .

La première colonne a  $2^{n-k}$  élément, tel que :  $n - k$  étant la dimension de S qui contient des vecteurs d'erreur  $\{e_i\}$  choisi parmi le  $2^n$ .

- Pour les autres colonnes, on ajoute le vecteur d'erreur représentant la ligne.

$c_1$	$c_2$	$c_3$	...	...	...	...	...	$c_{2^k}$
$c_1 + e_2$	$c_2 + e_2$	$c_3 + e_2$	...	...	...	...	...	$c_{2^k} + e_2$
$c_1 + e_3$	$c_2 + e_3$	$c_3 + e_3$	...	...	...	...	...	$c_{2^k} + e_3$
	.	.						.
	.	.						.
	.	.						.
$c_1 + e_{2^{n-k}}$	$c_2 + e_{2^{n-k}}$	$c_3 + e_{2^{n-k}}$	...	...	...	...	...	$c_{2^k} + e_{2^{n-k}}$

**-La construction de la table standard de 7 bits**

Nous allons utiliser la première ligne qu'il contient le  $2^4$  mot de codes possible en commençant par le mot dont tous les éléments sont des 0. cette ligne représente donc les mots transmis sans erreur  $e_i = 0$

Et la première colonne, linière à  $2^{7-4}$  élément 3 étant la dimension de S contient des vecteurs d'erreur  $\{e_i\}$  choisi parmi les  $2^7$

$c_1$	$c_2$	$c_3$	...	...	...	...	$c_{2^4}$
$c_1 + e_2$	$c_2 + e_2$	$c_3 + e_2$	...	...	...	...	$c_{2^4} + e_2$
$c_1 + e_3$	$c_2 + e_3$	$c_3 + e_3$	...	...	...	...	$c_{2^4} + e_3$
$c_1 + e_4$	$c_2 + e_4$	$c_3 + e_4$	...	...	...	...	$c_{2^4} + e_4$
$c_1 + e_5$	$c_2 + e_5$	$c_3 + e_5$	...	...	...	...	$c_{2^4} + e_5$
$c_1 + e_6$	$c_2 + e_6$	$c_3 + e_6$	...	...	...	...	$c_{2^4} + e_6$
$c_1 + e_7$	$c_2 + e_7$	$c_3 + e_7$	...	...	...	...	$c_{2^4} + e_7$
$c_1 + e_8$	$c_2 + e_8$	$c_3 + e_8$	...	...	...	...	$c_{2^4} + e_8$

Cette construction donne la table standard à 7 bits suivante :

**Tableau 3.1 La table standard de 7 bit**

0000000	0001111	0010110	0011101	0100111	0101100	0110001
0000001	0001110	0010111	0011100	0100110	0101101	0110000
0000010	0001101	0010100	0011111	0100101	0101110	0110011
0000100	0001011	0010010	0011001	0100011	0101000	0110101
0001000	0000111	0011110	0010101	0101111	0100100	0111001
0010000	0011111	0000110	0001101	0110111	0111100	0100001
0100000	0101111	0110110	0111101	0000111	0001100	0010001
1000000	1001111	1010110	1011101	1100111	1101100	1110001

0111010	1000101	1001110	1010011	1011000	1100010	1101001
0111011	1000100	1001111	1010010	1011001	1100011	1101000
0111000	1000111	1001100	1010001	1011010	1100000	1101011
0111110	1000001	1001010	1010111	1011100	1100110	1101101
0110010	1001101	1000110	1011011	1010000	1101010	1100001
0101010	1010101	1011110	1000011	1001000	1110010	1111001
0011010	1100101	1101110	1110011	1111000	1000010	1001001
1111010	0000101	0001110	0010011	0011000	0100010	0101001

1110100	1111111
1110101	1111110
1110110	1111101
1110000	1111011
1111100	1110111
1100100	1101111
1010100	1011111
0110100	0111111

**-La construction de la table standard de 8 bits**

Nous allons utiliser la première ligne qu'il contient le  $2^4$  mot de codes possible en commençant par le mot dont tous les éléments sont des 0.cette ligne représente donc les mots transmis sans erreur  $e_i = 0$

Et la première colonne, limitée à  $2^{8-4}$  élément 4 étant la dimension de S contient des vecteurs d'erreur  $\{e_i\}$  choisi parmi les  $2^8$

$c_1$	$c_2$	$c_3 \dots \dots \dots c_{2^5}$
$c_1 + e_2$	$c_2 + e_2$	$c_3 + e_2 \dots \dots \dots c_{2^5} + e_2$
$c_1 + e_3$	$c_2 + e_3$	$c_3 + e_3 \dots \dots \dots c_{2^5} + e_3$
$c_1 + e_4$	$c_2 + e_4$	$c_3 + e_4 \dots \dots \dots c_{2^5} + e_4$
$c_1 + e_5$	$c_2 + e_5$	$c_3 + e_5 \dots \dots \dots c_{2^5} + e_5$
$c_1 + e_6$	$c_2 + e_6$	$c_3 + e_6 \dots \dots \dots c_{2^5} + e_6$
$c_1 + e_7$	$c_2 + e_7$	$c_3 + e_7 \dots \dots \dots c_{2^5} + e_7$
$c_1 + e_8$	$c_2 + e_8$	$c_3 + e_8 \dots \dots \dots c_{2^5} + e_8$

Cette construction donne la table standard à 8 bits suivante :

Pour la vérification des erreurs, nous calculons la table syndromes basé sur la vérification de la première colonne de la table standard (Tableau 3.2).

**-La correction**

Le mot de code transmis le plus vraisemblable est obtenu en ajoute le vecteur erreur  $e_m$  au mot reçu  $\hat{C}_m = Y + e_m$

Le syndrome du mot reçu est calculé par l'expression :

$$S = Y.H^t$$

**Tableau 3.2 La table standard de 8 bit**

0 0 0 0 0 0 0
0 0 0 0 0 0 1
0 0 0 0 0 1 0
0 0 0 0 1 0 0
0 0 0 1 0 0 0
0 0 1 0 0 0 0
0 1 0 0 0 0 0
1 0 0 0 0 0 0

**-La table de syndrome de 7bit**

Nous construisons la table des syndromes en vérifiant pour chaque vecteur d'erreur l'existence ou là non existence du syndrome correspondant préalablement dans la table. Après, si ce syndrome existe, on le remplace par le syndrome suivant et son vecteur d'erreur correspondant.

**Tableau 3.3 table de syndrome de 7 bit**

Syndrome	Vecteur d'erreur
0 0 0	0 0 0 0 0 0 0
0 0 1	0 0 0 0 0 0 1
0 1 0	0 0 0 0 0 1 0
1 0 0	0 0 0 0 1 0 0
0 1 1	0 0 0 1 0 0 0
1 1 0	0 0 1 0 0 0 0
1 1 1	0 1 0 0 0 0 0
1 0 1	1 0 0 0 0 0 0

On introduire une vecteur d'erreur  $X_m=[0 0 0 0]$  et le vecteur reçu est  $Y = 0 0 0 0 1 1 1$  et le syndrome correspondant est  $S = 1 0 0$  à partir de la

table des syndromes le mot de code transmis le plus vraisemblable est obtenu en ajoute le vecteur erreur  $e_m$  au mot reçu  $\hat{C}_m = Y + e_m$

Le syndrome du mot reçu est calculé par l'expression :  $S = Y \cdot H^t$

$e_m = 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0$  Le mot transmis est :  $\hat{C}_m = 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1$  et l'information correcte est  $X_m = [0 \ 0 \ 0 \ 1]$ .

**La table de syndrome de 8 bit**

Nous allons construire cette table comme déjà expliquai précédemment :

On introduire une vecteur d'erreur  $X_m = [1 \ 0 \ 1 \ 1]$

Et le vecteur reçu est  $Y = 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0$  et le syndrome correspondant est  $S = 1 \ 0 \ 0$  à partir de la table des syndromes le mot de code transmis le plus vraisemblable est obtenu en ajoute le vecteur erreur  $e_m$  au mot reçu  $\hat{C}_m = Y + e_m$

Le syndrome du mot reçu est calculé par l'expression :  $S = Y \cdot H^t$

$e_m = 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0$  Le mot transmis est :  $\hat{C}_m = 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0$

Et l'information correcte est  $X_m = [0 \ 0 \ 0 \ 0]$

**Tableau 3.4 table de syndrome de 8 bit**

Syndrome	Vecteur d'erreur
0 0 0	0 0 0 0 0 0 0 0
0 0 1	0 0 0 0 0 0 0 1
0 1 0	0 0 0 0 0 0 1 0
1 0 0	0 0 0 0 0 1 0 0
0 1 1	0 0 0 0 1 0 0 0
1 1 0	0 0 1 0 0 0 0 0
1 1 1	0 1 0 0 0 0 0 0
1 0 1	1 0 0 0 0 0 0 0

**3.7 L'application sur une image**

**3.7.1 Codage**

**-Vecteur d'information**

Dans cette partie, nous appliquons notre codage LDPC, pour coder une image binaire. Pour cela, nous allons convertir une image en échelle de gris à une image binaire (noire et

blanche), les données de cette image sont représentées par une matrice ayant le nombre de lignes et des colonnes égal au nombre des pixels de l'image et des valeurs représentant les intensités des pixels (1(blanc) ou 0 (noir)); la matrice résultante est partagée en plusieurs vecteurs (8 bits) pour construire le vecteur d'information (Figure 3.4).

### -Matrice génératrice

Nous allons générer le codage de l'image avec la matrice génératrice  $G$  de  $k = 8$ ;  $n = 12$ ;  $R = 2/3$ ; la construction de  $G$  d'une manière systématique comme on a expliqué précédemment :

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

### -Obtention du code correcteur

L'obtention du code correcteur d'erreurs ( $C_m$ ) est comme la loi que déjà dit précédemment

#### 3.7.2 Décodage

### - Matrice de contrôle

La construction de la matrice de contrôle de l'image ( $H$ ) de  $k = 4$ ;  $n = 12$ ;  $R = 1/3$

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

### -Syndrome

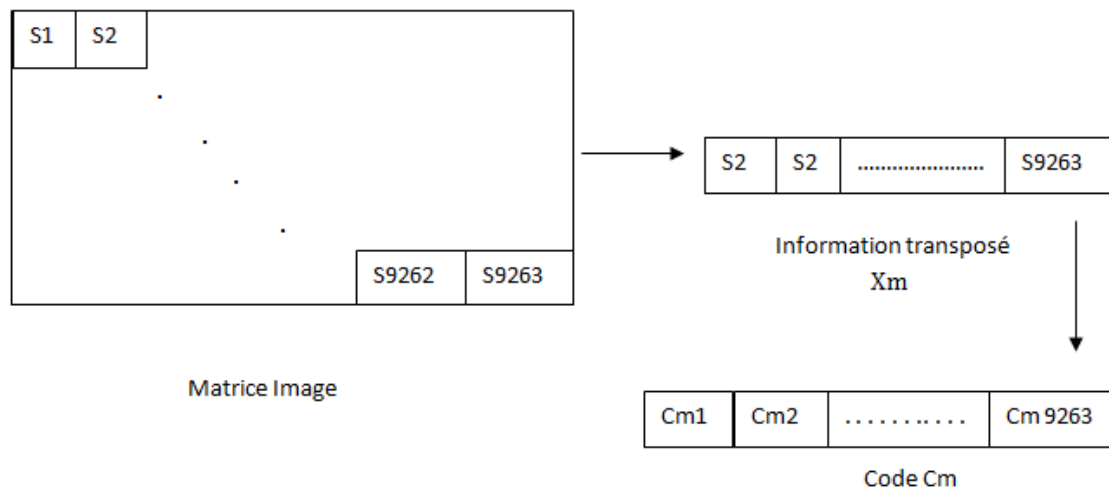
$$s = 0 \quad 0 \quad 0 \quad 0$$

Nous allons obtenir un vecteur de syndrome nul, Donc l'image a été sans erreur.

#### 3.7.3. Introduction des erreurs et correction

Nous allons introduire plusieurs types d'erreurs sur les vecteurs de code ( $C_m$ ) de l'image pour obtenir une image avec erreur et nous essayons de corrigé ces erreurs.

- Calculer les syndromes de ces vecteurs.



**Figure 3.4** construction de l'information et de code

1) En premier lieu, nous introduisons un seul bit d'erreur pour plusieurs vecteurs (Figure 3.4), pour le faire nous allons choisir une série des vecteurs de code et lancer une bit d'erreur pour chaque  $C_m$  puis nous allons essayer de corriger ces erreurs avec les étapes suivantes :

- Trouver les vecteurs d'erreur d'après la comparaison des vecteurs d'erreur et les syndromes obtenues par l'utilisation de la méthode déjà présentée avec les exemples de mot code de 7 bit et 8 bit.
- Faire la somme des vecteurs de code avec leur vecteurs d'erreur déjà trouver pour obtenir la correction des vecteurs de code
- Récupérer les vecteurs d'information  $X_m$  depuis les  $C_m$  par l'élimination des bits de contrôle.
- **Première Résultats :** D'après la comparaison entre les trois images obtenues nous avons remarqué que l'introduction d'un 1 bit d'erreur sur les vecteurs d'un code donne une image résultante sans erreur comme visualisé sur la figure 3.5, l'image obtenues avec erreur n'est pas comme l'image avant le codage mais après la correction nous obtenions une image très semblable à l'image originale.

2) En le deuxième essai, nous introduisons 2 bits d'erreur pour plusieurs vecteurs, et pour le faire nous allons choisir une série des vecteurs de code et lancer 2 bit d'erreur pour chaque  $C_m$ . Puis nous allons essayer de corriger ces erreurs avec les mêmes étapes utilisées pour 1 bit d'erreur.

- **Deuxième Résultats :** D'après la comparaison entre les trois images obtenues nous visualisons sur la figure 3.6 que l'image obtenues avec l'erreur n'est pas comme l'image

avant le codage et après la correction le résultat n'est pas n'est pas identique à l'original, donc la correction de vecteurs  $C_m$  avec 2 bits d'erreur n'est pas vérifiée.

3) En le troisième essai, nous introduisons 3 bits d'erreur pour plusieurs vecteurs, et pour le faire nous allons choisir une série des vecteurs de code et lancer 3 bit d'erreur pour chaque  $C_m$ . Puis nous allons essayer de corriger ces erreurs avec les mêmes étapes utilisées pour 1 bit d'erreur.

- **Troisième Résultats** : D'après la comparaison entre les trois images obtenues nous visualisons sur la figure 3.7 que l'image obtenues avec l'erreur n'est pas comme l'image avant le codage et après la correction le résultat n'est pas n'est pas identique à l'original, donc la correction de vecteurs  $C_m$  avec 3 bits d'erreur n'est pas vérifiée.

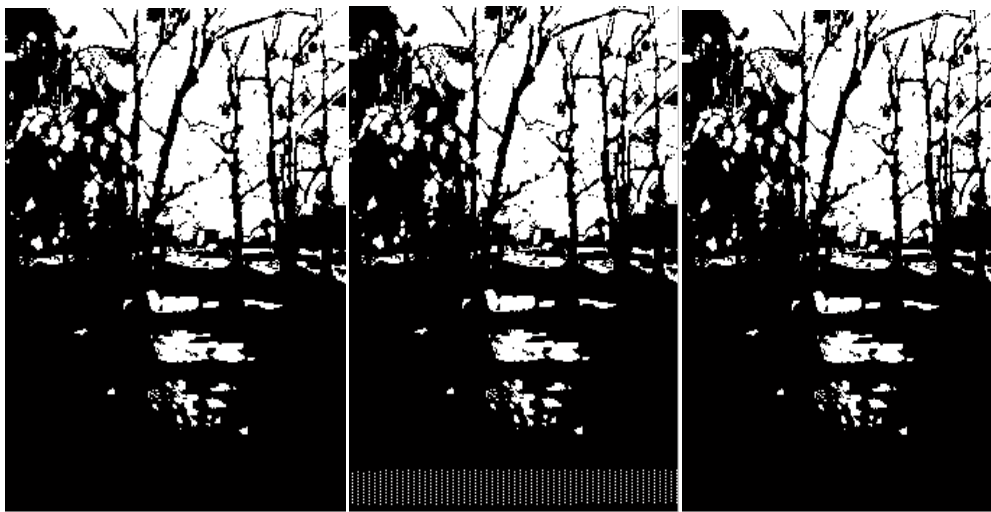


Image sans erreur

Image avec erreur

Image après la correction

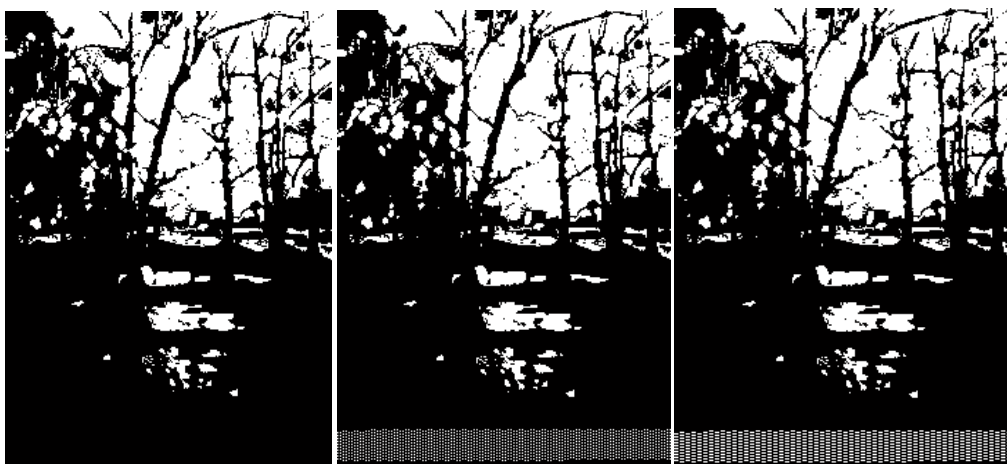
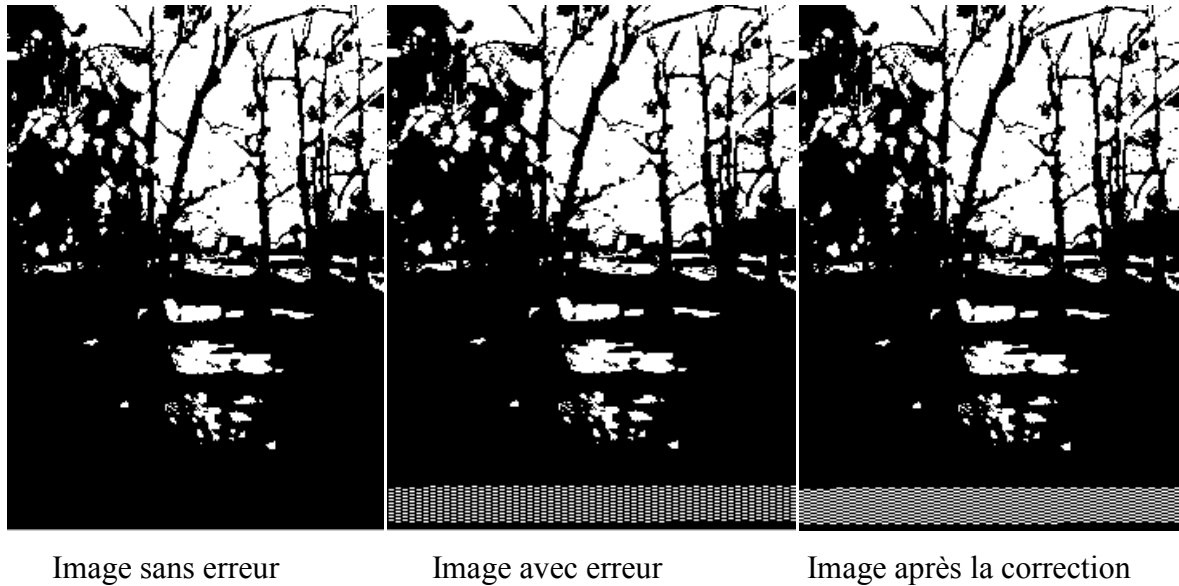
**Figure 3.5** Résultat d'introduction de 1 bit d'erreur

Image sans erreur

Image avec erreur

Image après la correction

**Figure 3.6** résultat d'introduction de 2 bit d'erreur



**Figure 3.7** Résultat d'introduction de 3 bits

### 3.8 Conclusion

Nous avons appliqué dans ce chapitre un algorithme de codage et décodage des codes correcteurs d'erreur LDPC par la présentation de deux exemples d'information de taille différentes (de 4 bit et 5 bit) avec l'introduction des erreurs et sans erreurs. Et puis, nous avons décodé ces codes en corrigeant toutes les erreurs introduites.

Nous avons à la fin, appliqué cet algorithme sur une matrice d'image par la simulation de plusieurs types d'erreurs et nous avons essayé de les corriger. Après visualisation de l'image avant et après correction, nous concluons que la correction des images affectées par des erreurs de 2 et 3 bits erroné n'est pas effectuée, par ce que l'utilisation d'un simple décodage LDPC par la matrice de contrôle de parité ne suffit pas dans le cas de plusieurs bits erronés. Il faut en plus de cette étape revoir les méthodes de construction de la matrice génératrice et utiliser dans l'étape de détection la vérification de la propagation de croyance.

## Conclusion générale

Durant ce mémoire nous avons pu constater que les générations de téléphonie mobile ont été développées pour garantir de meilleures performances en particulier pour les Qualités de Services, tout ça en apportant de nouvelles applications, de nouveaux services, ainsi qu'une meilleure gestion. De nos jours, la dernière génération est la 4G, elle a comme principaux paramètres du réseau, un très haut débit utilisé, une latence beaucoup moins importante que dans le réseau 3G, une large bande passante, une bande de fréquence flexible, et une interopérabilité avec les autres réseaux.

Le but de la théorie des codes correcteurs est de minimiser le plus possible les taux d'erreurs de décodage, en assurant au même temps de très grandes vitesses de transmission. Ces propriétés sont optimales pour le code correcteur d'erreurs largement utilisé dans la 4 G : le LDPC.

Dans notre travail, nous avons appliqué un algorithme de codage et décodage sur deux exemples des mots d'information de 4 et de 5 bits avec l'introduction après le codage d'une erreur et puis une correction de cette dernière au décodage.

Ensuite, nous avons appliqué cet algorithme sur une matrice d'image avec une simulation de plusieurs erreurs. La correction de ces erreurs est effectuée pour le cas d'un seul bit d'erreur, mais on n'a pas obtenu de corrections pour le cas de plusieurs bits d'erreurs, parce que nous n'avons pas fait beaucoup d'investissement dans le choix de la matrice génératrice en choisissant une matrice très simple vérifiant l'indépendance linéaire entre ces vecteurs. En plus, il faut appliquer à la fin de la procédure, les algorithmes de décodage (propagation croyance ...) pour éliminer les bits erronés.

## Bibliographies

---

### Bibliographies

- [1] J. McNair, F. Zhu, "Vertical Handoffs in Fourth-Generation Multinetwork Environment", IEEE Wireless communication, Volume 11, Issue 3, pp.8\_15, June 2004.
- [2] Z. Yan, L. Lei, M. Chen, "WISE-a completely flat and distributed architecture for future wireless communication systems", Wireless world research forum, October 2008.
- [3] E. Tony et L. Ewoussaoua, « Planification Et ingénierie Des Réseau De Télécoms », mémoire pro 2 de télécommunication, Université de Yaounde I, 2011.
- [4] T. Bchini, "Gestion de la Mobilité, de la Qualité de Service et Interconnexion de Réseaux Mobiles de Nouvelle Génération", Thèse de Doctorat, Université de Toulouse, Juin 2010.
- [5] A. H. Khan, A. Mohamed. Qader, A. Juned. Ansari, Sariya Waheed, "4G as a next generation Wireless Network", International conference on futur computer and communication, Aligarh Muslim University, India, pp-334-338, 2009.
- [6] G. Lawton, "4G : Engineering versus Marketing", <http://computingNow,computer.org>, March 2011.
- [7] A. A. GHassen, I. Mahmud et J. Kasmiran, "Modeling and performance Evolution of LTE Networks with Différents Variants, Academie mondiale des sciences, 2011.
- [8] L. Liu, W. Leung et L. Ping, Simple iterative chip-by-chip multiuser detection for cdma systems, dans Vehicular Technology Conference, VTC 2003-Spring. The 57th IEEE Semiannual, ol. 3, (pp. 2157{2161), IEEE, 2003.
- [9] R. v. Nee et R. Prasad, OFDM for wireless multimedia communications, Artech House, Inc. 2000.
- [10] H. Hashemi et D. Tholl, Statistical modeling and simulation of the rms delay spread of indoor radio propagation channels, Transactions on Vehicular Technology, vol. 43, no. 1, pp. 110 120, 1994.
- [11] T. S. Rappaport et al, Wireless communications : principles and practice, vol. 2, prentice hall PTR New Jersey, 2002.
- [12] A. Goldsmith, Wireless communications, Cambridge university press, 2005.
- [13] D. Tse et P. Viswanath, Fundamentals of wireless communication, Cambridge university press, 2005.
- [14] J. G. Andrews, Interference cancellation for cellular systems : a contemporary overview, Wireless Communications, IEEE, vol. 12, no. 2, pp. 19-29, 2005.
- [15] L. Hanzo, C. H. Wong et M.S. Yee, Adaptive wireless transceivers : turbocoded, turbo equalised and space-time coded TDMA, CDMA and OFDM systems, John Wiley & Sons, 2002.

## Bibliographies

---

- [16] J. C. Liberti et T. S. Rappaport, Smart antennas for wireless communications : IS-95 and third génération CDMA application Parentice Halle PTR, 1999.
- [17] M. Theriault, Etude des performances d'un système DS-CDMA avec récepteur Rake dans le contexte UWB, Thèse de doctorat, Université Laval, 2005.
- [18] M. Ergen, Mobile broadband : including WiMAX and LTE, Springer Science & Business Media, 2009.
- [19] D. W. Lee, G. T. Gil et D. H. Kim, A cost-based adaptive handover hysteresis scheme to minimize the handover failure rate in 3gpp lte system, EURASIP Journal on Wireless Communications and Networking, vol. 2010, p. 6, 2010.
- [20] SH. Holma and A. Toskala, LTE for UMTS : OFDMA and SC-FDMA Based Radio Access, Wiley, 2009.
- [21] S. Ragusa, J. Paicot, Y. Louet, and Clipping for Increasing the power Efficiency of OFDM Amplication, in IEEE International Conference on telecommunications, May 2006.
- [22] M. Cote, "Reconnaissance de codes correcteur d'erreurs ", thèse de doctorat, école polytechnique : 2010.
- [23] P. Senellart, "Codes correcteurs d'erreurs la révolution des turbo-codes", Télécom Paris Tech, Département Informatique et Réseaux, Paris Cedex 13 France, 2007.
- [24] Sh. Lin and Daniel J. Costello. Error Control Coding Fundamentals and application. Pearson education Inc, 2004.
- [25] M. Bossert. Channel Coding for telecommunications. John Wiley & sons, 1999.
- [26] R. G. Gallager, "Low-density parity-check codes", Ph. D. dissertation, M. I. T. 1963.
- [27] R. Tanner, "A recursive approach to low complexity codes", IEEE Transactions on Information Theory, vol. 27, no. 5, pp. 533–547, Sep. 1981.
- [28] N. Wiberg, "Codes and decoding on general graphs", Ph. D. dissertation, Département of electrical engineering, Linkoping, Sweeden. Linkoping studies in sciences and technology, 1996.
- [29] H. A. Loeliger, "An introduction to factor graphs", IEEE Signal Processing Magazine, vol. 21, no. 1, pp. 28–41, Jan. 2004.
- [30] R. M. Tanner, "A Recursive Approach to Low Complexity Codes", IEEE Trans. Inform.Theory, vol. IT-27, pp. 533-547, 1981.
- [31] S. Lin et D. Costello, Error control coding. Prentice Hall, 2004.
- [32] 1999 N. Wiberg, H. A. Loeliger et R. Kotter, "Codes and Iterative Decoding on General Graphs", Eur. Trans. Telecommun, vol. 6, pp. 513-26, 1955.
- [33] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. Spielman, "Analysis of low density codes and improved designs using irregular graphs", in Proceeding of 30th ACM Symp. on Theory of Computing, 1998.

## Bibliographies

---

- [34] H. Jin, A. Khandekar, and R. McEliece, “Irregular repeat-accumulate codes”, in Second International Conference on Turbo Codes, 2000.
- [35] D. Divsalar, H. Jin, and R. McEliece, “Coding theorems for turbo-like codes”, in Proceeding of the 36th Allerton conference on communication, control and computing, 1998.
- [36] J. Fan, “Array codes as low-density parity-check codes”, in Second International Conference on Turbo Codes, 2000.
- [37] V. Mannoni, “Optimisation des codes LDPC pour les communication multiporteuses”, Thèse de Doctorat, université de Reims Champagne-Ardenne, Juin 2004.

## Résumé

Nous présentons dans ce mémoire, une méthode de codage et de décodage des codes correcteurs d'erreurs pour les transmissions sans fil, basée sur l'utilisation des codes LDPC réguliers. Dans un premier temps, nous avons appliqué un algorithme de codage et décodage des codes correcteurs d'erreur LDPC par la présentation de deux exemples d'information de tailles différentes (de 4 bits et 5 bits) avec l'introduction des erreurs et sans erreurs. Nous avons décodé ces codes en corrigeant toutes les erreurs introduites. Ensuite, nous avons appliqué cet algorithme sur une matrice d'image avec une simulation de plusieurs erreurs. La correction de ces erreurs est effectuée pour le cas d'un seul bit mais, on n'a pas obtenu de corrections pour le cas plusieurs bits d'erreur.

## Abstract

We present in this paper, a method of coding and decoding error correcting codes for wireless transmissions, based on the use of regular LDPC codes. First, we applied an algorithm for encoding and decoding the LDPC error correcting codes by presenting two examples of different sizes information (4 bits and 5 bits) with the introduction of errors and without errors. We have decoded these codes by correcting all the errors introduced. Then, we applied this algorithm on an image matrix with a simulation of several errors. The correction of these errors is performed for the case of a single bit, but we did not get corrections for the case of several error bits.

## الملخص

نقدم في هذه الأطروحة طريقة لرموز فك تشفير الأخطاء وفك تشفيرها للإرسالات اللاسلكية، استنادا إلى استخدام رموز LDPC. أولا، طبقنا خوارزمية لترميز وفك رموز تصحيح الأخطاء عن طريق تقديم مثالين لمعلومات ذات أحجام مختلفة (4 بت و 5 بت) مع إدخال الأخطاء وبدون أخطاء. لقد تم فك شفرة هذه الرموز عن طريق تصحيح جميع الأخطاء المقدمة. ثم، طبقنا هذه الخوارزمية على مصفوفة صورة مع محاكاة العديد من الأخطاء. تم تصحيح هذه الأخطاء لحالة بت واحد ولكن لم نحصل على تصحيحات لحالة عدة أخطاء.