UNIVERSITÉ DE LIMOGES
ÉCOLE DOCTORALE Science – Technologie – Santé
FACULTÉ des SCIENCES et TECHNIQUES

Année 2005 **Thèse N° 36 - 2005**

Thèse

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Discipline : Mathématiques et ses applications

présentée et soutenue publiquement

par

Laurent DUBREUIL

le 11 octobre 2005

Amélioration de l'étalement de spectre par l'utilisation de codes correcteurs d'erreurs

Thèse dirigée par Thierry BERGER

Jury

Président :	
Raymond QUÉRÉ	Professeur à l'université de Limoges
Rapporteurs :	
Danièle FOURNIER-PRUNARET	Professeur à l'INSA de Toulouse
Nicolas SENDRIER	Directeur de recherche à l'INRIA Rocquencourt
Examinateurs :	
Thierry BERGER	Professeur à l'université de Limoges
Jean-Pierre CANCES	Maître de conférence à l'ENSIL, Limoges
Alban DUVERDIER	Ingénieur au CNES de Toulouse

A Marcel,
A ma famille, mes proches, mes amis,

Remerciements

Je souhaite remercier Raymond Quéré d'avoir accepté de présider mon jury de thèse ainsi que Danièle Fournier-Prunaret et Nicolas Sendrier qui ont bien voulu en être les rapporteurs.

Je remercie Jean-Pierre Cances de sa participation à mon jury.

Je remercie Alban Duverdier de sa participation à mon jury et de ces remarques constructives.

Je remercie Thierry Berger d'avoir été mon directeur de thèse tout au long de ces quatre années de recherche.

Je tiens à exprimer toute ma gratitude à Thierry Berger et Raymond Quéré pour leur aide, leur apport scientifique et culturel et toutes les discussions que nous avons eues tout au long de cette recherche. Je tiens aussi à les remercier pour m'avoir proposé le stage initial de DEA qui m'a permis d'effectuer cette thèse.

Je remercie les secrétaires Hélène Breuzard, Martine Guerletin, Sylvie Laval, Marie-Claude Lerouge, Nadine Tchefranoff, Patricia Vareille et Yolande Vieceli pour leur gentillesse et leur disponibilité, et pour avoir facilité mon travail en s'occupant des soucis administratifs.

Merci aussi à Anne Bellido, Abdelkader Necer, Marc Rybowicz, Stéphane Vinatier et Henry Massias pour leur aide, leur disponibilité et leur gentillesse.

Je remercie aussi tous les doctorants et docteurs que j'ai côtoyé pendant ces quatre années pour leur joie et leur bonne humeur : Thomas Cluzeau, Samuel Maffre, Carmen Nedeloaia, Mikaël Lescop, Guilhem Castagnos, Adrien Poteaux et Mathieu Le Floc'h. Et plus particulierement à Philippe Segalat, Ayoub Otmani, Mériem Héraoua et Nicolas Le Roux, qui étaient mes voisins de bureau, pour les discussions endiablées que nous avons eues.

Je remercie aussi tous les membres du Laboratoire que je n'ai pas nommé explicitement.

Je souhaite remercier mes fidèles lecteurs et correcteurs Anne Bellido, Chrystèle Lacombe, Philippe Ségalat et Vincent Virefléau.

Un grand merci à ma famille au grand complet, à mes amis Pierre Ardiller, Manuel Louchart, Simon Polizzi, Manuel Virefléau et Vincent Virefléau qui m'ont apporté joie et bonne humeur et qui ont su me distraire de diverses manières tout au long de cette recherche. Merci aussi à Céline Muckli pour sa gentillesse, sa disponibilité, son amitié et son écoute attentive.

Je fais un énorme bisou à *"Ma puce"* Chrystèle pour son aide, son soutien,

son enthousiasme et son amour tout au long de ces deux dernières années.

Et pour finir, je voudrais faire un petit clin d'œil à mon *"petit zèbre"*, ma filleule, Célia, ainsi qu'à sa sœur, Julie, en leur souhaitant un parcours universitaire équivalent au mien.

Table des matières

Table des figures

Liste des tableaux

Notations et abréviations

Notations

Code $[n, k, d]$	Code en bloc de longueur n, de dimension k et de distance minimale d
d_{min} ou d	Distance minimale
E_b	Energie d'un bit d'information
$\frac{E_b}{N_0}$	Rapport entre l'énergie d'un bit d'information et la densité spectrale de puissance du bruit
E_s	Energie d'un symbole
$\mathbb{F}_q$	Corps fini à q éléments
N_0	Densité spectrale de puissance du bruit
$\mathcal{RM}(r, m)$	Code de Reed Muller d'ordre r à m variables

Abréviations

BAM	Bruit d'Accès Multiple
BPSK	Binary Phase Shift Keying
dB	Décibels
CDMA	Code Division Multiple Access
LRV	Logarithme du Rapport de Vraisemblance
M-PSK	M-ary Phase Shift Keying
MAI	Multiple Access Interference
QPSK	Quadrature Phase Shift Keying
RM	Reed Muller
RS	Reed Solomon
TEB	Taux d'Erreur Binaire

Introduction

Ce manuscrit est le fruit de trois années de recherche au sein du Laboratoire d'Arithmétique de Calcul formel et d'Optimisation en collaboration avec L'Institut de Recherche en Communications Optiques et Microondes de Brive la Gaillarde et le Centre National d'Etudes Spatiales de Toulouse sur le thème "Développement de nouvelles techniques pour des télécommunications spatiales".

Depuis une dizaine d'année, les communications personnelles sont en pleine expansion. Le nombre d'utilisateurs ne fait que croître et le type de données à transmettre n'arrête pas de se diversifier. Désormais, à la transmission de la voix s'ajoute de plus en plus la transmission de données diverses et variées allant de la photo à la vidéo en passant par la musique. Ces besoins nécessitent donc d'augmenter toujours plus les capacités des systèmes, que ce soit en terme de nombre d'utilisateurs ou en débit des données, tout en minimisant les coûts. Il est donc nécessaire de repousser les limites des applications déjà existantes, d'où l'étude que nous avons faite sur les améliorations de l'étalement de spectre par l'utilisation de codes correcteurs d'erreurs.

L'objectif de notre recherche est d'étudier un système pour lequel le nombre d'utilisateurs pouvant interagir sur une même bande de fréquence, pour un débit donné, est maximal. Dans cette étude, nous avons imposé que, pour chaque utilisateur, le TEB en sortie de l'étalement de spectre soit inférieur ou égal à 10^{-3}, et que le facteur d'étalement soit fixé à 31. De plus, nous avons supposé que l'émetteur et le récepteur étaient synchronisés, sauf mention contraire.

Dans le premier chapitre, nous présentons quelques généralités concernant les communications, plus particulièrement celles concernant la théorie de l'information, le décodage ainsi que les séquences de Gold. Nous présentons notamment des rappels sur la capacité des différents modèles de canaux : ces résultats seront utilisés par la suite pour déterminer la limite de Shannon. Cette limite permet, en effet, d'évaluer des codes de même rendement et ainsi de déterminer lequel de ces codes est le plus proche de cette limite. Nous présentons ensuite, un décodage souple, utilisé lors des simulations pour décoder des codes ayant une petite dimension. Ce chapitre s'achève alors par

la présentation des séquences de Gold utilisées comme séquence d'étalement dans le CDMA. Nous donnons certaines propriétés de ces séquences ainsi que leur construction.

Le second chapitre présente le système CDMA qui est le centre de notre étude théorique et pratique. Nous y décrivons l'étalement de spectre et l'accès multiple à répartition par les séquences d'étalement plus communément appelé, dans la littérature anglo-saxonne, CDMA pour Code Division Multiple Access. Cette description présente brièvement la technique de l'étalement de spectre qui est l'élément principal du CDMA. Puis, nous rappelons l'une des techniques utilisées dans l'étalement de spectre, l'étalement de spectre par séquences directes, et nous donnons les avantages et les inconvénients de cette technique. Ensuite vient la description du CDMA proprement dit avec ses avantages et ses inconvénients et enfin, pour finir, deux modélisations du CDMA : l'une du point de vue de l'émetteur, l'autre du point de vue du récepteur. Ces modélisations sont la base de cette étude.

Le troisième chapitre définit un étalement de spectre à déphasage multiple utilisant, en modulation de phase, des séquences d'étalement aléatoires à déphasage multiple. Après cette définition, nous montrons, de manière théorique et pratique, que l'utilisation de séquences d'étalement aléatoires à déphasage multiple dans l'étalement de spectre est meilleure en terme de TEB que l'utilisation de séquences aléatoires binaires ou de Gold. De plus, l'utilisation des séquences d'étalement aléatoires à déphasage multiple dans le cas d'un étalement de spectre asynchrone est meilleure que l'utilisation des séquences de Gold dans le cas synchrone. Ce résultat est le point fort de notre étude et justifie l'utilisation de séquences d'étalement aléatoires à déphasage multiple pour atteindre nos objectifs.

Le quatrième chapitre intitulé "Etalement de spectre, cryptographie et information cachée" rappelle brièvement l'étalement de spectre. Ensuite, nous présentons la cryptographie symétrique et nous montrons comment l'étalement de spectre peut être utilisé comme moyen cryptographique. La dernière section de ce chapitre présente une méthode se basant en particulier sur un avantage de l'étalement de spectre pour cacher de l'information dans une communication. Cette méthode a toutefois un problème majeur qui est la synchronisation de l'émetteur et du récepteur. Nous proposons un schéma utilisant deux communications au lieu d'une dans le cas précédent pour corriger ce problème. Cette section conclut sur le fait que l'étalement de spectre peut servir comme algorithme de chiffrement et comme canal caché pour transmettre des informations.

Le cinquième chapitre, quant à lui, présente l'étalement de spectre en tant que code correcteur d'erreurs. Toutefois, le code correcteur utilisé de base n'est

pas le plus approprié car il n'y a pas de gain de codage avec ce code, comme le montre le calcul du TEB d'une liaison à spectre étalé. Ce chapitre ensuite donne des limites théoriques et physiques concernant le CDMA. Les limites théoriques données portent sur la limite de Shannon et le nombre maximum d'utilisateurs pouvant interagir ensemble. La limite de Shannon est de $-1,49$ dB pour tout code de rendement 1/31. Le nombre maximum d'utilisateurs est fonction du facteur d'étalement et tend vers l'infini lorsque ce dernier tend lui aussi vers l'infini. Les limites physiques quant à elles portent sur l'utilisation des décodeurs et sur le facteur d'étalement. En effet, le décodage du code ayant un système fonctionnant en temps réel doit être le plus rapide possible. Quant au facteur d'étalement, il ne peut tendre vers l'infini car la fréquence de fonctionnement du système est fonction de ce facteur, et des systèmes fonctionnant à très haute fréquence sont peu nombreux et très onéreux.

Le sixième chapitre apporte des solutions pour atteindre nos objectifs, en présentant principalement deux codes. L'un des codes est un code de petite dimension n'excédant pas 10, l'autre est un code concaténé, résultant d'un code de Reed Solomon et d'un code de petite dimension. L'utilisation de ces codes permet d'avoir un nombre maximum d'utilisateurs simultanés allant jusqu'à 23 alors qu'avec le code à répétition, ce nombre n'est que de 7 pour un TEB fixé à 10^{-3}.

Le septième chapitre expose les résultats de simulation du couplage dans la chaîne de transmission des blocs "codage canal" et "étalement de spectre" pour un TEB fixé à 10^{-6} au lieu de 10^{-3} comme précédemment. Dans les chapitres antérieurs, les résultats de notre recherche montrent l'utilisation de codes correcteurs d'erreurs dans l'étalement de spectre. Il est donc envisageable de regrouper les deux blocs, qui utilisent des codes correcteurs, en un seul. De plus, l'utilisation du code concaténé présenté dans le chapitre précédant n'est pas concluante, lorsque nous le regardons par rapport au reste de la chaîne de transmission. Dans le cadre de ce chapitre, l'utilisation est plus intéressante et adaptée au reste de la chaîne une fois les deux blocs regroupés. Les résultats de simulations sont présentés pour deux codes : l'un est un code concaténé pris sur la base du code concaténé présenté dans le chapitre précédent, l'autre est un code de Reed Muller du premier ordre.

L'annexe A présente les codes CORTEX et l'utilisation que nous en faisons dans cette étude. Toutefois les résultats obtenus ne sont pas les résultats escomptés.

L'annexe B liste les matrices génératrices des codes binaires utilisés lors de cette étude.

L'annexe C donne les principaux programmes utilisés lors de cette étude.

Chapitre 1

Quelques éléments de communications et de décodage

Dans ce chapitre, nous rappelons des généralités concernant la théorie de l'information et le décodage. Dans un premier temps, nous définissons la capacité d'un canal comme quantité maximale d'information mutuelle moyenne apportée par chaque bit reçu. Dans un second temps, étant donné que le système de communication étudié utilise des modulations M-PSK avec un bruit parasite gaussien, nous allons nous intéresser au calcul de la probabilité d'erreur pour des modulations M-PSK en présence d'un bruit gaussien. Puis, nous présenterons un algorithme de décodage souple que nous utiliserons ultérieurement lors de nos simulations et nous définirons les séquences de Gold.

1.1 Capacité d'un canal

Dans ce paragraphe, nous allons nous intéresser à la capacité d'un canal. Tout d'abord, nous définirons divers modèles de canaux, puis nous donnerons la capacité de ces canaux ([1] pp. 380-386 [2, 3]).

1.1.1 Modèles d'un canal

Définissons quatre modèles de canaux : le canal binaire symétrique, le canal M-aire, le canal continu en sortie et le canal caractérisé par des formes d'ondes.

Canal binaire symétrique

On considère un canal incluant le canal physique, les modulateurs et les démodulateurs comme représentés à la figure (1.1).

Le canal binaire symétrique est défini par un alphabet binaire d'entrées $X = \{0, 1\}$ et un alphabet de sortie $Y = \{0, 1\}$ associés aux probabilités conditionnelles d'avoir un symbole donné y_i sachant que le symbole x_j a été émis. Cette association peut se représenter par le diagramme (1.2). On note

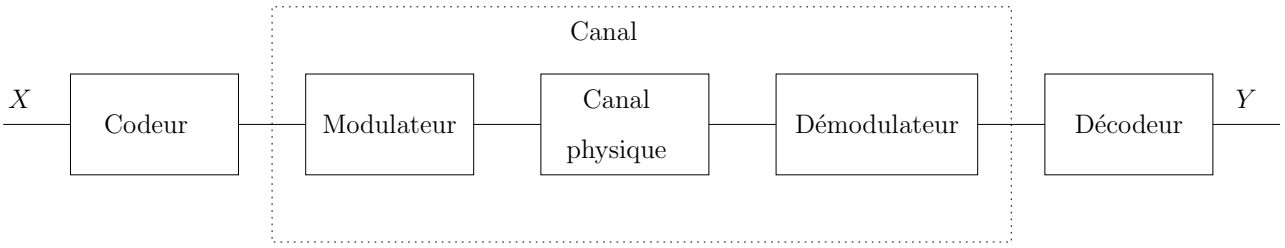


FIG. 1.1 – Modèle général d'un canal incluant le modulateur et le démodulateur

$P(y_i|x_j)$ pour $P(Y = y_i|X = x_j)$. Pour le canal binaire symétrique, on pose p la probabilité d'erreur du canal ayant pour valeur

$$p = P(0|1) = P(1|0).$$

On peut traduire le fonctionnement du canal binaire par une matrice de transition de probabilité :

$$P(Y) = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \cdot P(X).$$

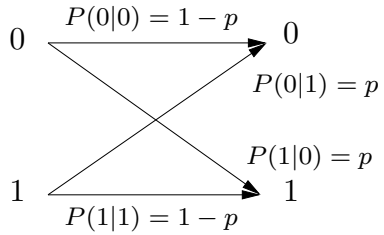


FIG. 1.2 – Diagramme de transition pour un canal binaire.

Canal M-aire

Dans le cas général, l'alphabet d'entrée peut comprendre q symboles et l'alphabet de sortie Q symboles. On a donc $X = \{x_0, \cdots, x_{q-1}\}$ et $Y = \{y_0, \cdots, y_{Q-1}\}$. Le diagramme de transition est représenté par celui de la figure (1.3). La matrice de transition est alors donnée par :

$$P(Y) = \begin{pmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,q-1} \\ p_{1,0} & p_{1,1} & \cdots & p_{1,q-1} \\ \vdots & & \ddots & \vdots \\ p_{Q-1,0} & p_{Q-1,1} & \cdots & p_{Q-1,q-1} \end{pmatrix} \cdot P(X)$$

avec $p_{i,j} = P(y_i|x_j)$ et pour $i = 0, 1, \cdots, Q-1 \quad \sum_{k=0}^{q-1} p_{i,k} = 1.$

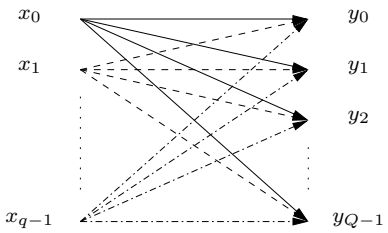


FIG. 1.3 – Diagramme de transition pour un canal M-aire avec q entrées et Q sorties.

Canal continu en sortie

Dans le cas d'un canal bruité, la superposition du bruit au symbole transmis entraîne le fait que la variable de sortie prend ses valeurs dans un continuum. On a donc la situation suivante :

- q symboles discrets en entrée $\{x_0, , x_1, \cdots x_{q-1}\}$;
- $y \in \mathbb{R}$ en sortie.

Le canal sera alors caractérisé par les probabilités conditionnelles :

$$P(y|x_k) \quad \text{pour } k = 0, 1, \cdots q-1.$$

Dans le cas d'un bruit gaussien additif, on aura $Y = X + G$ où G est la variable aléatoire caractérisant le bruit gaussien. Ainsi :

$$p(y|x_k) = \frac{1}{\sigma\sqrt{2\pi}}\, e^{-\frac{(y-x_k)^2}{2\sigma^2}}. \tag{1.1}$$

Canal caractérisé par des formes d'ondes

Dans le cas où l'on sépare le canal physique du modulateur et du démodulateur, le canal peut être caractérisé par les formes d'ondes d'entrée $x(t)$ et de sortie $y(t)$ et par le processus de bruit $n(t)$. Si ce canal a une largeur de bande W, on le caractérise par un ensemble d'échantillons d'entrée et de sortie définis respectivement par $x_i = x(iT_e)$ et $y_i = y(iT_e)$ avec $T_e = \frac{1}{2W}$. En effet, d'après le théorème de Nyquist ([1] pp. 542-547), le signal de bande W est correctement décrit si $T_e = \frac{1}{2W}$. Si T est le temps d'observation du signal, on obtiendra N échantillons tels que

$$N = 2WT. \tag{1.2}$$

Lorsque le bruit $n(t)$ est gaussien, on montre aisément que les échantillons $y_i = x_i + n_i$, avec $n_i = n(iT_e)$, sont des variables aléatoires gaussiennes indépendantes. Ainsi,

$$p(y_i|x_i) = \frac{1}{\sigma_i\sqrt{2\pi}}\, e^{-\frac{(y_i-x_i)^2}{2\sigma_i^2}} \tag{1.3}$$

où $\sigma_i^2 = \frac{1}{2}N_0$. En reportant cette valeur dans (1.3), on obtient :

$$p(y_i|x_i) = \frac{1}{\sqrt{\pi N_0}}\, e^{-\frac{(y_i - x_i)^2}{N_0}}. \tag{1.4}$$

1.1.2 Capacité d'un canal

Nous allons donner dans un premier temps la définition de la capacité d'un canal. Nous donnerons ensuite la capacité des divers canaux définis précédemment.

Définitions

Considérons un canal muni d'un alphabet d'entrée $X = \{x_0, x_1, \cdots x_{q-1}\}$ et d'un alphabet de sortie $Y = \{y_0, y_1, \cdots y_{Q-1}\}$. Supposons que le symbole x_i ait été transmis et que le symbole y_j ait été reçu ; *l'information mutuelle*, notée $I(x_i; y_j)$, procurée par cet événement est définie par :

$$I(x_i; y_j) = \log_2 \left[\frac{P(x_i, y_j)}{P(x_i)P(y_j)}\right] = \log_2 \left[\frac{P(y_j|x_i)}{P(y_j)}\right] \tag{1.5}$$

avec $P(y_j) = \sum_{k=0}^{q-1} P(y_j|x_k)P(x_k)$.

L'*information mutuelle moyenne* dans le canal, notée $I(X;Y)$, est alors définie par :

$$I(X;Y) = \sum_{i=0}^{q-1}\sum_{j=0}^{Q-1} I(x_i; y_j)P(x_i, y_j) = \sum_{i=0}^{q-1}\sum_{j=0}^{Q-1} I(x_i; y_j)P(x_i)P(y_j|x_i). \tag{1.6}$$

La *capacité du canal*, notée C, est définie comme étant le maximum de l'information mutuelle moyenne lorsque la densité de probabilité des symboles d'entrée varie. On a donc :

$$C = \underset{P(x_i)}{Max}\,[I(X;Y)] = \underset{P(x_i)}{Max}\left[\sum_{i=0}^{q-1}\sum_{j=0}^{Q-1} I(x_i; y_j)P(x_i)P(y_j|x_i)\right] \tag{1.7}$$

avec $P(x_i) \geq 0$ et $\sum_{i=0}^{q-1} P(x_i) = 1$.

Exemples

⋆ Canal binaire symétrique

Dans le cas d'un canal binaire symétrique, on a $P(0|1) = P(1|0) = p$ et

$P(0|0) = P(1|1) = 1-p$. L'information mutuelle est alors maximale lorsque la densité de probabilité sur X est uniforme, soit $P(X=0) = P(X=1) = \frac{1}{2}$. On a donc :

$$C = P(X=0)\left[P(1|0)\log_2\left(\frac{P(1|0)}{P(Y=1)}\right) + P(0|0)\log_2\left(\frac{P(0|0)}{P(Y=0)}\right)\right] + P(X=1)\left[P(1|1)\log_2\left(\frac{P(1|1)}{P(Y=1)}\right) + P(0|1)\log_2\left(\frac{P(0|1)}{P(Y=0)}\right)\right].$$

Or, d'après le théorème des probabilités totales, on a

$$\begin{aligned} P(Y=0) &= P(X=0)P(Y=0|X=0) + P(X=1)P(Y=0|X=1) \\ &= \frac{1}{2}(p+1-p) \\ &= \frac{1}{2}. \end{aligned}$$

De même $P(Y=1) = \frac{1}{2}$. Ainsi, la capacité d'un canal binaire symétrique est égale à

$$\begin{aligned} C &= P(X=0)\left[P(1|0)\log_2\left(\frac{P(1|0)}{P(Y=1)}\right) + P(0|0)\log_2\left(\frac{P(0|0)}{P(Y=0)}\right)\right] \\ &\quad + P(X=1)\left[P(1|1)\log_2\left(\frac{P(1|1)}{P(Y=1)}\right) + P(0|1)\log_2\left(\frac{P(0|1)}{P(Y=0)}\right)\right] \\ &= \frac{1}{2}\left[p\log_2\left(\frac{p}{\frac{1}{2}}\right) + (1-p)\log_2\left(\frac{1-p}{\frac{1}{2}}\right)\right] + \frac{1}{2}\left[(1-p)\log_2\left(\frac{1-p}{\frac{1}{2}}\right) + p\log_2\left(\frac{p}{\frac{1}{2}}\right)\right] \\ &= \frac{p}{2}\log_2(2p) + \frac{(1-p)}{2}\log_2(2(1-p)) + \frac{(1-p)}{2}\log_2(2(1-p)) + \frac{p}{2}\log_2(2p) \\ &= p\log_2(2p) + (1-p)\log_2(2(1-p)) \\ &= 1 + p\log_2(p) + (1-p)\log_2(1-p). \end{aligned}$$

dont la variation en fonction de p est donnée à la figure (1.4).

⋆ **Canal binaire gaussien** (Canal binaire continu en sortie)

Dans ce cas, l'alphabet d'entrée est $X = \{-A\ ,\ +A\}$ avec

$$P(X=A) = P(X=-A) = \frac{1}{2}.$$

Ainsi $p(y|A) = \dfrac{1}{\sigma\sqrt{2\pi}}\, e^{-\frac{(y-A)^2}{2\sigma^2}}$ et $p(y|-A) = \dfrac{1}{\sigma\sqrt{2\pi}}\, e^{-\frac{(y+A)^2}{2\sigma^2}}$ et donc

$$\begin{aligned} p(y) &= p(y|A)P(A) + p(y|-A)P(-A) \\ &= \frac{1}{2\sigma\sqrt{2\pi}}\left[\, e^{-\frac{(y-A)^2}{2\sigma^2}} + \, e^{-\frac{(y+A)^2}{2\sigma^2}}\right]. \end{aligned}$$

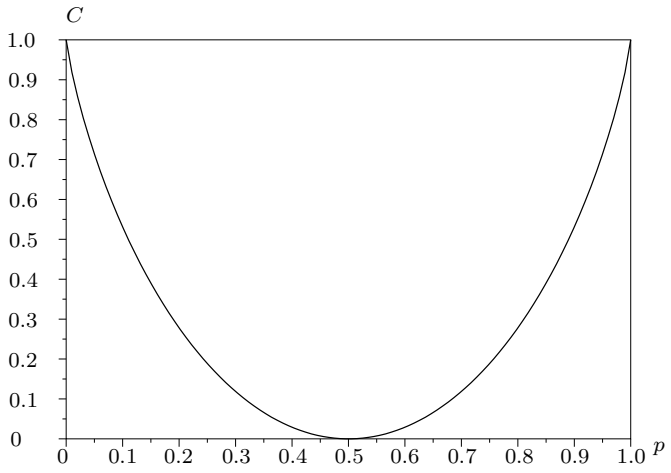


FIG. 1.4 – Capacité C d'un canal binaire symétrique en fonction de la probabilité d'erreur p sur un symbole.

La capacité d'un canal binaire gaussien est alors égale à

$$\begin{aligned}
C &= P(X=A)\int_{-\infty}^{+\infty} P(y|A)\log_2\left(\frac{P(y|A)}{P(y)}\right)dy \\
&\quad +P(X=-A)\int_{-\infty}^{+\infty} P(y|-A)\log_2\left(\frac{P(y|-A)}{P(y)}\right)dy \\
&= \frac{1}{2}\int_{-\infty}^{+\infty}\frac{1}{\sigma\sqrt{2\pi}}\,e^{-\frac{(y-A)^2}{2\sigma^2}}\log_2\left(\frac{\frac{1}{\sigma\sqrt{2\pi}}\,e^{-\frac{(y-A)^2}{2\sigma^2}}}{\frac{1}{2\sigma\sqrt{2\pi}}\left[\,e^{-\frac{(y-A)^2}{2\sigma^2}}+\,e^{-\frac{(y+A)^2}{2\sigma^2}}\right]}\right)dy \\
&\quad +\frac{1}{2}\int_{-\infty}^{+\infty}\frac{1}{\sigma\sqrt{2\pi}}\,e^{-\frac{(y+A)^2}{2\sigma^2}}\log_2\left(\frac{\frac{1}{\sigma\sqrt{2\pi}}\,e^{-\frac{(y+A)^2}{2\sigma^2}}}{\frac{1}{2\sigma\sqrt{2\pi}}\left[\,e^{-\frac{(y-A)^2}{2\sigma^2}}+\,e^{-\frac{(y+A)^2}{2\sigma^2}}\right]}\right)dy \\
&= \frac{1}{2\sigma\sqrt{2\pi}}\int_{-\infty}^{+\infty}e^{-\frac{(y-A)^2}{2\sigma^2}}(1-\log_2\left(1+e^{-\frac{2yA}{\sigma^2}}\right))dy \\
&\quad +\frac{1}{2\sigma\sqrt{2\pi}}\int_{-\infty}^{+\infty}e^{-\frac{(y+A)^2}{2\sigma^2}}(1-\log_2\left(1+e^{\frac{2yA}{\sigma^2}}\right))dy.
\end{aligned}$$

En effectuant le changement de variable $y=-y$ dans la seconde intégrale, nous obtenons le fait que la capacité du canal binaire gaussien est

$$C=\frac{1}{\sigma\sqrt{2\pi}}\int_{-\infty}^{+\infty}e^{-\frac{(y-A)^2}{2\sigma^2}}\left[1-\log_2\left(1+e^{-\frac{2yA}{\sigma^2}}\right)\right]dy. \tag{1.8}$$

Capacité d'un canal à bande limitée

La capacité d'un canal d'alphabets d'entrée X et de sortie Y à bande limitée a été définie par Shannon [4] en 1948. Elle est égale à

$$C = \lim_{T \to +\infty} \underset{p(x)}{Max} \frac{1}{T} I(X;Y). \tag{1.9}$$

Dans cette définition :

- C représente la capacité par unité de temps. Elle s'exprime en bits/s.
- $I(X;Y)$ est l'information mutuelle moyenne entre les formes d'ondes $x(t)$ et $y(t)$ à l'entrée et à la sortie du canal. Elle est donnée par

$$I(X;Y) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} p(x)p(y|x) \log_2 \frac{p(y|x)}{p(y)} dx\, dy.$$

Pour calculer la capacité du canal à bande limitée, on s'intéresse à la suite d'échantillons d'entrée et de sortie prélevés au rythme de Nyquist ([1] pp. 542-547), soit à la période $T_e = \frac{1}{2W}$. Dans l'intervalle de temps d'observation T, on dispose donc de N échantillons tels que $T = NT_e$ et on a

$$N = 2WT. \tag{1.10}$$

Les échantillons d'entrée et de sortie du canal sont respectivement x_i et $y_i = x_i + n_i$. L'hypothèse d'un bruit additif gaussien de variance $\sigma^2_{n_i} = \frac{1}{2}N_0$ fournit l'expression de la densité de probabilité conditionnelle suivante

$$p(y_i|x_i) = \frac{1}{\sqrt{\pi N_0}}\, e^{-\frac{(y_i - x_i)^2}{N_0}}. \tag{1.11}$$

On montre que l'information mutuelle $I(X;Y)$ est maximale lorsque la répartition des x_i est gaussienne centrée. En notant σ_x la variance de chaque x_i, on a

$$p(x_i) = \frac{1}{\sigma_x \sqrt{2\pi}}\, e^{-\frac{x_i^2}{2\sigma_x^2}}. \tag{1.12}$$

Les variables aléatoires X et Y sont alors décrites par les vecteurs d'échantillons $\mathbf{X}_N = [x_1, \ldots, x_N]$ et $\mathbf{Y}_N = [y_1, \ldots, y_N]$. L'information mutuelle est donc donnée par :

$$\begin{aligned} I(\mathbf{X}_N; \mathbf{Y}_N) &= \int_{\mathbf{X}_N} \cdots \int \int_{\mathbf{Y}_N} \cdots \int p(\mathbf{Y}_N|\mathbf{X}_N) p(\mathbf{X}_N) \log_2 \frac{p(\mathbf{Y}_N|\mathbf{X}_N)}{p(\mathbf{Y}_N)} d\mathbf{X}_N d\mathbf{Y}_N \\ &= \sum_{i=1}^{N} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} p(y_i|x_i) p(x_i) \log_2 \frac{p(y_i|x_i)}{p(y_i)} dx_i dy_i. \end{aligned} \tag{1.13}$$

On va calculer le terme d'ordre i. On définit I_i par

$$I_i = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} p(y_i|x_i)p(x_i) \log_2 \frac{p(y_i|x_i)}{p(y_i)} dx_i dy_i.$$

Ainsi

$$I_i = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \frac{1}{\pi\sigma_x\sqrt{2N_0}}\, e^{\left(-\frac{(y_i-x_i)^2}{N_0} - \frac{x_i^2}{2\sigma_x^2}\right)} \log_2 \left[\frac{\frac{1}{\sqrt{\pi N_0}}\, e^{-\frac{(y_i-x_i)^2}{N_0}}}{\frac{1}{\sqrt{\pi N_0'}}\, e^{-\frac{y_i^2}{N_0'}}} \right] dx_i dy_i. \tag{1.14}$$

En effet, on montre que l'on a :

$$\begin{aligned} p(y_i) = \int_{-\infty}^{+\infty} p(y_i|x_i)p(x_i)dx_i &= \int_{-\infty}^{+\infty} \frac{1}{\pi\sigma_x\sqrt{2N_0}}\, e^{\left(-\frac{(y_i-x_i)^2}{N_0} - \frac{x_i^2}{2\sigma_x^2}\right)} dx_i \\ &= \frac{1}{\sqrt{\pi N_0'}}\, e^{-\frac{y_i^2}{N_0'}} \end{aligned}$$

en notant $N_0' = N_0\left(1 + \dfrac{2\sigma_x^2}{N_0}\right)$.
On peut décomposer (1.14) en trois intégrales notées I_i^1, I_i^2, I_i^3 :

$$\begin{aligned} I_i^1 &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \frac{-\log_2 \mathrm{e}}{\pi\sigma_x\sqrt{2N_0}}\, \frac{(y_i - x_i)^2}{N_0}\, e^{\left(-\frac{(y_i-x_i)^2}{N_0} - \frac{x_i^2}{2\sigma_x^2}\right)} dx_i\, dy_i, \\ I_i^2 &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \frac{y_i^2 \log_2 \mathrm{e}}{N_0'}\, \frac{1}{\pi\sigma_x\sqrt{2N_0}}\, e^{\left(-\frac{(y_i-x_i)^2}{N_0} - \frac{x_i^2}{2\sigma_x^2}\right)} dx_i\, dy_i, \\ I_i^3 &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \frac{1}{2} \log_2 \left(\frac{N_0'}{N_0}\right) \frac{1}{\pi\sigma_x\sqrt{2N_0}}\, e^{\left(-\frac{(y_i-x_i)^2}{N_0} - \frac{x_i^2}{2\sigma_x^2}\right)} dx_i\, dy_i. \end{aligned}$$

Après simplification

$$\begin{aligned} I_i^1 &= -\frac{1}{2} \log_2 \mathrm{e}, \\ I_i^2 &= \frac{1}{2} \log_2 \mathrm{e}, \\ I_i^3 &= \frac{1}{2} \log_2 \left(1 + \frac{2\sigma_x^2}{N_0}\right). \end{aligned}$$

Ainsi

$$I_i = I_i^1 + I_i^2 + I_i^3 = \frac{1}{2} \log_2 \left(1 + \frac{2\sigma_x^2}{N_0}\right). \tag{1.15}$$

La capacité du canal C est donnée par

$$\begin{aligned} C &= \lim_{T\to+\infty} \underset{p(x)}{Max} \frac{1}{T} I(X;Y) \\ &= \lim_{T\to+\infty} \underset{p(x)}{Max} \frac{1}{T} I(X_N;Y_N) \\ &= \lim_{T\to+\infty} \underset{p(x)}{Max} \frac{1}{T} \sum_{i=1}^{N} I_i \\ &= \lim_{T\to+\infty} \underset{p(x)}{Max} \frac{N}{2T} \log_2\left(1+\frac{2\sigma_x^2}{N_0}\right) \\ C &= \lim_{T\to+\infty} \frac{N}{2T} \log_2\left(1+\frac{2\sigma_x^2}{N_0}\right). \end{aligned}$$

On peut exprimer σ_x^2 en fonction de la *puissance moyenne du signal* P_{moy} qui est définie par

$$P_{moy} = \frac{1}{T}\int_0^T E\left[x^2(t)\right] dt = \frac{1}{T}\sum_{i=1}^{N} E\left[x_i^2\right] = \frac{1}{T} N\sigma_x^2. \tag{1.16}$$

En considérant (1.10), on obtient

$$\sigma_x^2 = \frac{P_{moy}}{2W}. \tag{1.17}$$

Finalement, la capacité C du canal est donnée par

$$C = W\ \log_2\left(1+\frac{P_{moy}}{WN_0}\right). \tag{1.18}$$

Cette expression peut être exprimée en fonction de l'énergie par bit, notée E_b. En effet $P_{moy} = CE_b$ où C est le débit en bits/s. Ainsi,

$$\frac{C}{W} = \log_2\left(1+\frac{C\,E_b}{W\,N_0}\right). \tag{1.19}$$

On obtient donc

$$\frac{E_b}{N_0} = \frac{2^{C/W}-1}{C/W}. \tag{1.20}$$

La représentation de la capacité, en fonction du rapport signal à bruit par bit, est donnée à la figure (1.5). En effet, lorsque $C/W = 1$, $E_b/N_0 = 1$ (0 dB), et quand $C/W \to +\infty$ on a

$$\begin{aligned} \frac{E_b}{N_0} &\approx \frac{2^{C/W}}{C/W} \\ &\approx e^{(\frac{C}{W}\ln(2) - \ln\frac{C}{W})}. \end{aligned}$$

Ainsi E_b/N_0 croît de manière exponentielle quand $C/W \to +\infty$. Et lorsque $C/W \to 0$ nous avons

$$\lim_{C/W \to 0} \frac{E_b}{N_0} = \ln(2) = 0.693 = 10^{\frac{-1,6}{10}}.$$

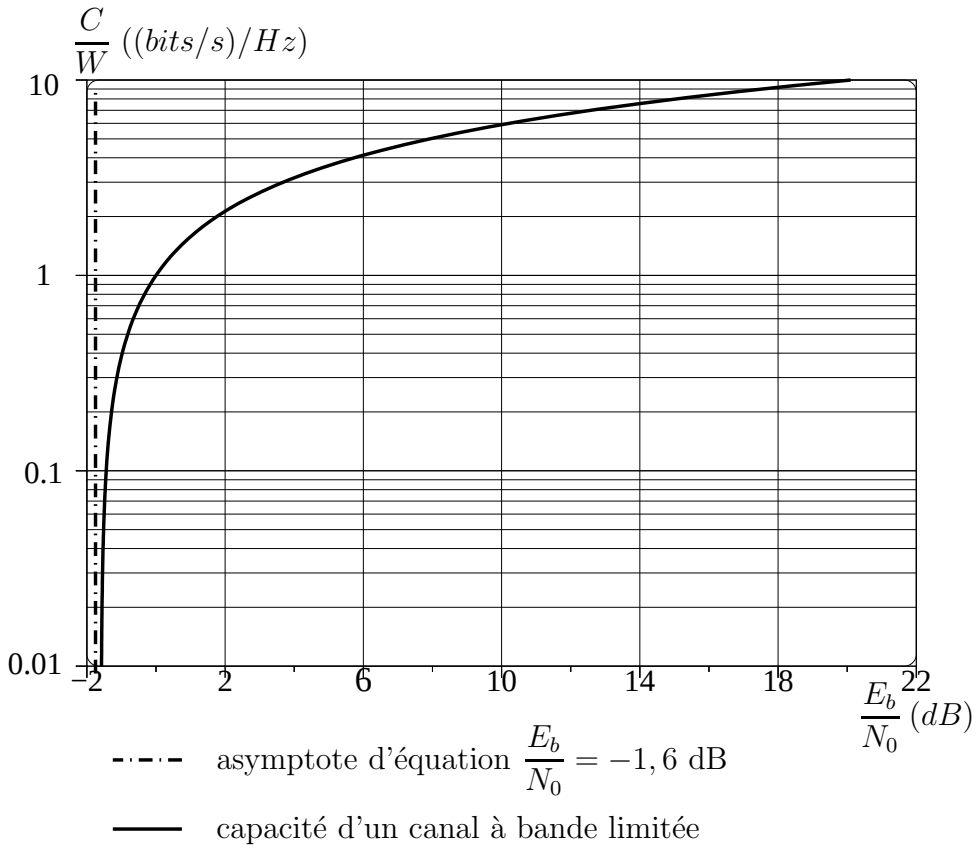


FIG. 1.5 – Capacité d'un canal à bande limitée en fonction du rapport signal à bruit par bit E_b/N_0.

1.2 Calcul de la probabilité d'erreur pour des modulations M-PSK en présence d'un bruit blanc additif gaussien

Dans ce paragraphe, nous allons calculer la probabilité d'erreur pour des modulations à M états de phase en présence d'un bruit blanc additif gaussien ([1] pp. 269-274).

On considère un signal modulé, $s_m(t)$, à M états de phase. Il se modélise sous la forme

$$s_m(t) = g(t)\,\cos\left(2\pi f_c t\, + \frac{2\pi}{M}\,(m-1)\right),\ \text{avec } m = 1, 2, \cdots, M$$

où $t \in [0, T_s]$, T_s est la durée d'émission d'un symbole, f_c la fréquence de la porteuse et $g(t)$ est la fonction définissant l'enveloppe du signal émis. Cette enveloppe est non nulle sur l'intervalle $[0, T_s]$.

Si T_b est la durée d'émission d'un bit, la durée d'émission du symbole est donnée par

$$T_s = \log_2(M) T_b.$$

La puissance instantanée de l'onde modulée est égale à

$$P_{sm} = \frac{1}{2} g^2(t)$$

et l'énergie par symbole émis est donnée par

$$E_s = \int_0^{T_s} \frac{1}{2} g^2(t)\, dt.$$

L'amplitude de l'impulsion constante sur $[0, T_s]$ d'énergie E_s est égale à $\sqrt{\frac{2E_s}{T_s}}$.
A la réception, la suppression de la porteuse à la pulsation ω_c est obtenue par la multiplication de l'onde modulée $s_m(t)$ par

$$e_1(t) = \sqrt{\frac{2}{T_s}}\cos(2\pi f_c t) \text{ et } e_2(t) = -\sqrt{\frac{2}{T_s}}\sin(2\pi f_c t),$$

suivant le schéma du corrélateur de la figure (1.6). Le vecteur reçu en sortie $\mathbf{r_m}$ du corrélateur est donc

$$\mathbf{r_m} = \left(\sqrt{E_s}\,\cos\left(\frac{2\pi}{M}(m-1)\right)\ , \sqrt{E_s}\sin\left(\frac{2\pi}{M}(m-1)\right)\right),\ \text{avec } m = 1, 2, \cdots, M. \tag{1.21}$$

Le vecteur reçu $\mathbf{r_m}$ en l'absence de bruit a donc pour module $\sqrt{E_s}$ et pour phase à l'origine $\frac{2\pi}{M}(m-1)$.

Le diagramme de Fresnel des vecteurs émis et reçus est représenté à la figure

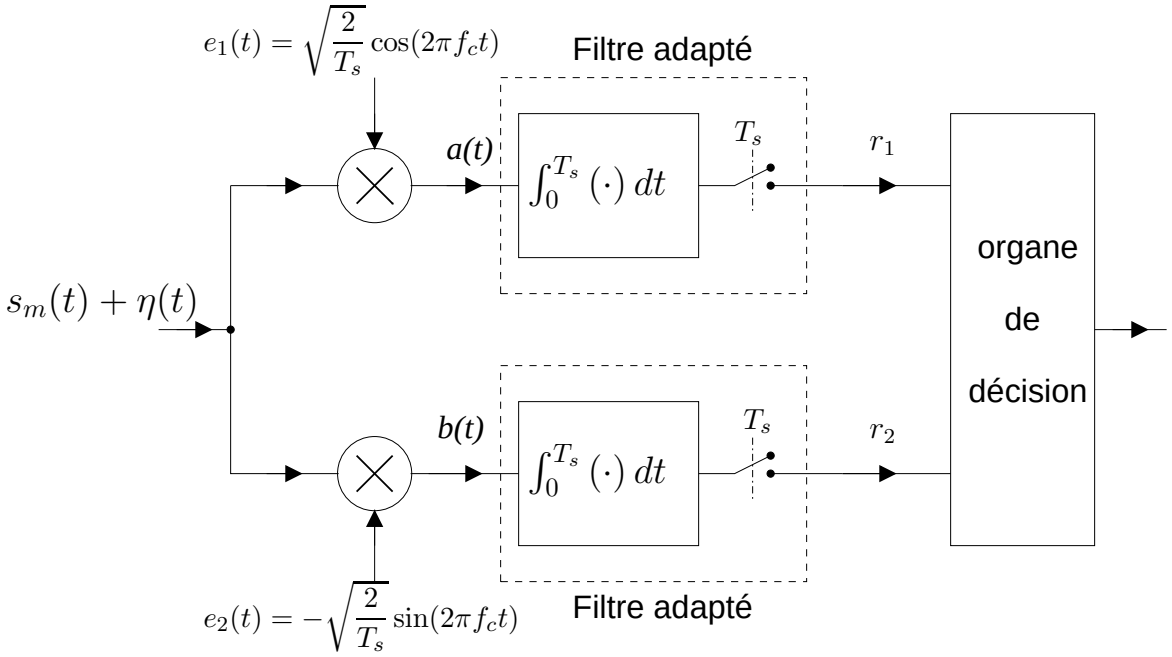


FIG. 1.6 – Forme générale d'un corrélateur pour la démodulation de signaux.

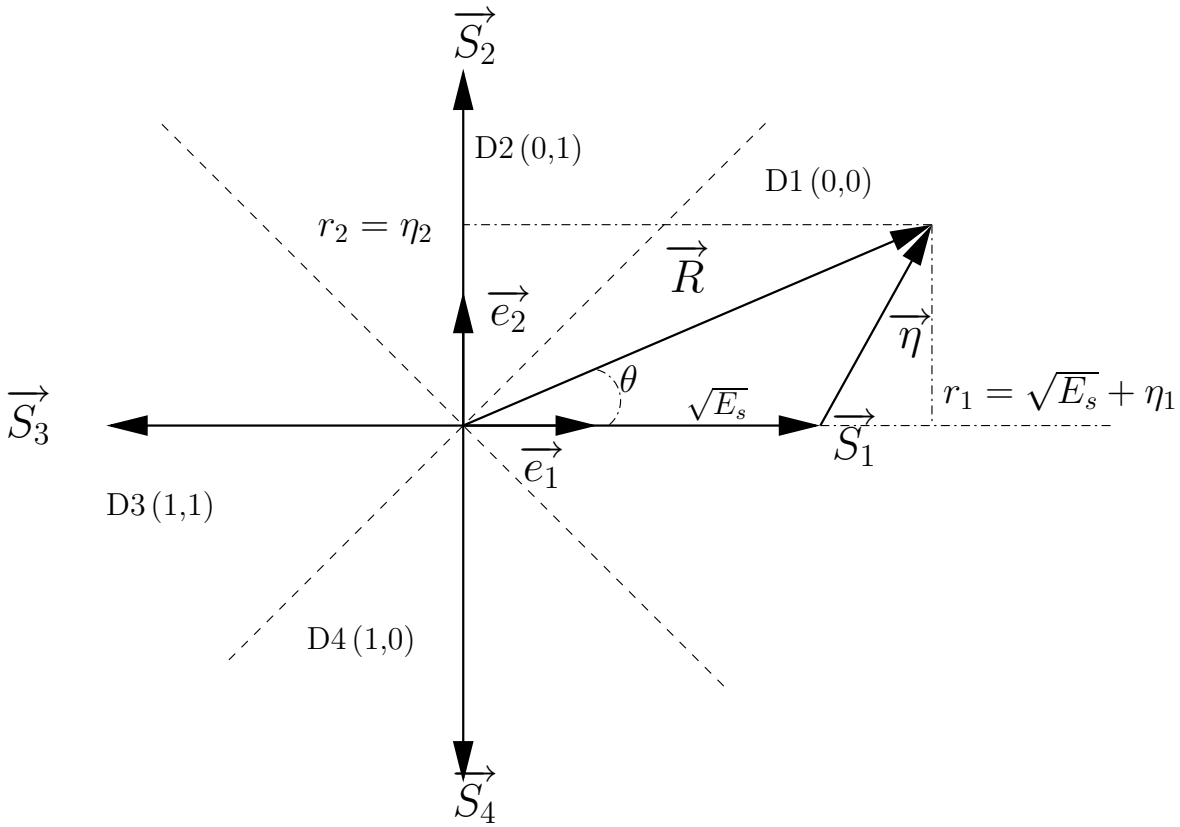


FIG. 1.7 – Diagramme de Fresnel en réception lorsque le symbole S_1 a été émis.

(1.7) lorsque le symbole $S_1 = (\sqrt{E_s},\ 0)$ a été émis dans le cas d'une modulation QPSK. Le bruit $\eta(t)$ vient alors s'additionner au signal émis S_1 pour former le signal reçu R, comme indiqué à la figure (1.7). Le vecteur bruit $\overrightarrow{\eta}$ est caractérisé par ses composantes $(\eta_1,\ \eta_2)$ qui sont des variables gaussiennes de moyenne nulle et de variance $\sigma_n^2 = N_0/2$. Si le symbole S_1 a été émis, les composantes reçues à la sortie du filtre adapté sont $(r_1,\ r_2) = (\sqrt{E_s} + \eta_1,\ \eta_2)$, avec $E(r_1) = \sqrt{E_s}$, $E(r_2) = 0$ et $\sigma_{r_1}^2 = \sigma_{r_2}^2 = N_0/2 = \sigma_n^2$. La probabilité jointe d'avoir à la fois r_1 et r_2 est égale au produit des probabilités de r_1 et r_2 car ces deux variables aléatoires sont indépendantes. On a donc

$$p(r_1, r_2) = \frac{1}{2\pi\sigma_n^2} e^{-\frac{(r_1-\sqrt{E_s})^2+r_2^2}{2\sigma_n^2}}. \tag{1.22}$$

Pour calculer la probabilité d'avoir un symbole erroné, nous allons d'abord calculer la probabilité de réception correcte. La réception est correcte si l'angle du vecteur reçu noté $\Theta = \arg \overrightarrow{R}$ est tel que $|\Theta| \leq \dfrac{\pi}{M}$. Pour obtenir cette inégalité, il nous faut d'abord obtenir la densité de probabilité de Θ. En faisant le changement de variable $A = \sqrt{r_1^2 + r_2^2}$ on a $\Theta = \tan^{-1}\left(\dfrac{r_2}{r_1}\right)$. Ainsi,

$$p_{A,\Theta}(A, \Theta) = \frac{A}{2\pi\sigma_n^2}\, e^{-\frac{A^2+E_s-2A\sqrt{E_s}\cos\Theta}{2\sigma_n^2}}. \tag{1.23}$$

En intégrant la probabilité jointe précédente par rapport à A, et en posant $\gamma_s = \dfrac{E_s}{N_0}$, on obtient

$$\begin{aligned} p_\Theta(\Theta) &= \int_0^{+\infty} p_{A,\Theta}(A, \Theta) dA & (1.24)\\ &= \frac{e^{-\gamma_s \sin^2\Theta}}{2\pi} \int_0^{+\infty} A\, e^{-\frac{(A-\sqrt{2\gamma_s}\cos\Theta)^2}{2}} dA. & (1.25) \end{aligned}$$

Par intégration formelle de l'équation (1.25) à l'aide du logiciel Maple [5, 6], on obtient

$$\int_0^{+\infty} A \exp\left[-\frac{(A-\sqrt{2\gamma_s}\cos\Theta)^2}{2}\right] dA = \sqrt{\gamma_s\pi}\, \cos\Theta\, [1 + \mathrm{erf}(\gamma_s \cos\Theta)] + e^{-\gamma_s \cos^2\Theta},$$

avec $\mathrm{erf}(x) = \dfrac{2}{\sqrt{\pi}} \displaystyle\int_0^x e^{-t^2} dt$.
Finalement,

$$p_\Theta(\Theta) = \sqrt{\gamma_s\pi}\, \cos\Theta\, [1 + \mathrm{erf}(\gamma_s \cos\Theta)]\, \frac{e^{-\gamma_s \sin^2\Theta}}{2\pi} + \frac{e^{-\gamma_s}}{2\pi}. \tag{1.26}$$

Cette égalité permet de représenter la densité de probabilité $p_\Theta(\Theta)$ (cf. figure (1.8)). Dans le cas où γ_s est grand et $\Theta \leq \pi/2$, la densité de probabilité $p_\Theta(\Theta)$

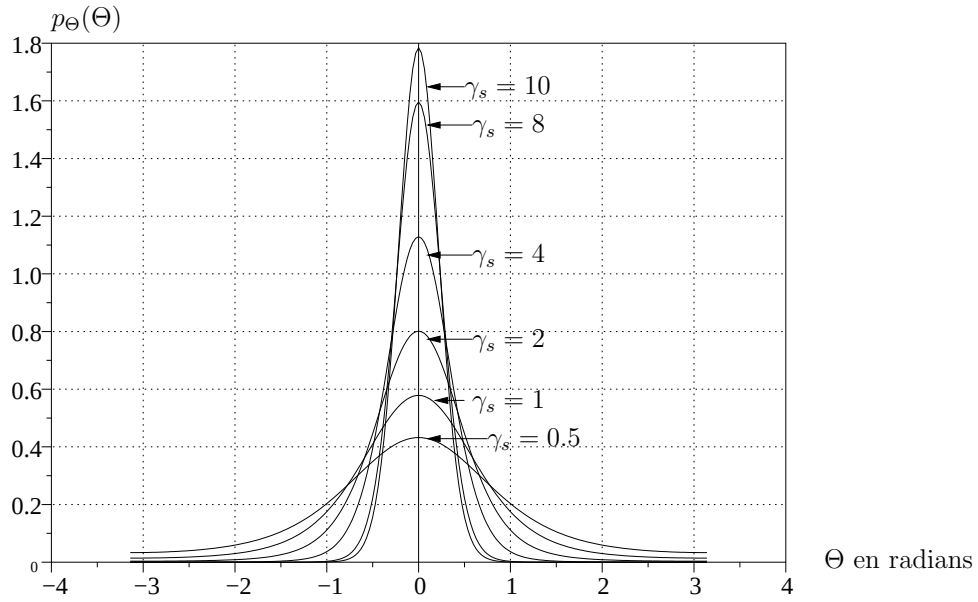


FIG. 1.8 – Densité de probabilité de l'angle Θ du vecteur reçu.

est bien approchée par

$$p_\Theta(\Theta) \approx \sqrt{\frac{\gamma_s}{\pi}}\, e^{-\gamma_s \sin^2\Theta}\ \cos\Theta. \tag{1.27}$$

La probabilité d'erreur par symbole P_{es} est alors donnée par

$$\begin{aligned} P_{es} &= 1 - \int_{-\pi/M}^{\pi/M} p_\Theta(\Theta) d\Theta & (1.28)\\ &\approx 1 - \sqrt{\frac{\gamma_s}{\pi}} \int_{-\pi/M}^{\pi/M} e^{-\gamma_s \sin^2\Theta} \cos\Theta\, d\Theta. & (1.29) \end{aligned}$$

En effectuant le changement de variable $u = \sqrt{\gamma_s}\sin\Theta$, l'intégrale devient

$$\begin{aligned} P_{es} \approx 1 - \frac{1}{\sqrt{\pi}} \int_{\sqrt{\gamma_s}\sin -\frac{\pi}{M}}^{\sqrt{\gamma_s}\sin\frac{\pi}{M}} e^{-u^2}\, du &= 1 - \frac{2}{\sqrt{\pi}} \int_0^{\sqrt{\gamma_s}\sin\frac{\pi}{M}} e^{-u^2}\, du & (1.30)\\ &= 1 - \mathrm{erf}\left(\sqrt{\gamma_s}\sin\frac{\pi}{M}\right) & (1.31)\\ &= \mathrm{erfc}\left(\sqrt{\gamma_s}\sin\frac{\pi}{M}\right), & (1.32) \end{aligned}$$

avec $\mathrm{erfc}(x) = 1 - \mathrm{erf}(x) = \dfrac{2}{\sqrt{\pi}} \displaystyle\int_x^{+\infty} e^{-t^2} dt$.

On a aussi $k = \log_2(M)$, $\gamma_s = k\,\gamma_b$ où $\gamma_b = \dfrac{E_b}{N_0}$, et $E_b = \dfrac{E_s}{k}$ qui est l'énergie par bit.

Si le code associé à la modulation à M états est un code de Gray, la probabilité d'erreur par bit, P_{eb}, est égale à

$$P_{eb} = \frac{P_{es}}{k}.$$

Ainsi, d'après (1.32), on a,

$$P_{es} = \operatorname{erfc}\left(\sqrt{\gamma_s}\sin\frac{\pi}{M}\right),$$

et finalement

$$P_{eb} = \frac{P_{es}}{k} = \frac{1}{k}\operatorname{erfc}\left(\sqrt{k\,\gamma_b}\sin\frac{\pi}{M}\right). \tag{1.33}$$

La figure (1.9) représente les résultats obtenus avec le calcul exact de l'intégrale et l'approximation de l'équation (1.32). On peut constater la très bonne qualité d'approximation, ce qui justifie son utilisation pour calculer les taux d'erreur par symbole (représentés à la figure (1.10)) pour des modulations M-PSK.

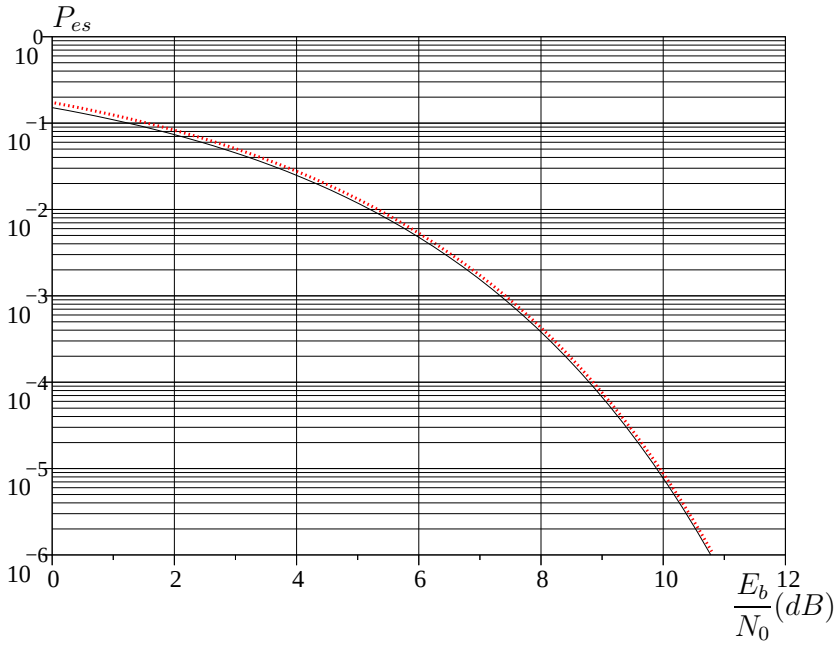


FIG. 1.9 – Comparaison des taux d'erreur par symbole entre l'approximation de l'équation (1.32) et le calcul exact de l'intégrale (1.28) à l'aide de l'équation (1.26).

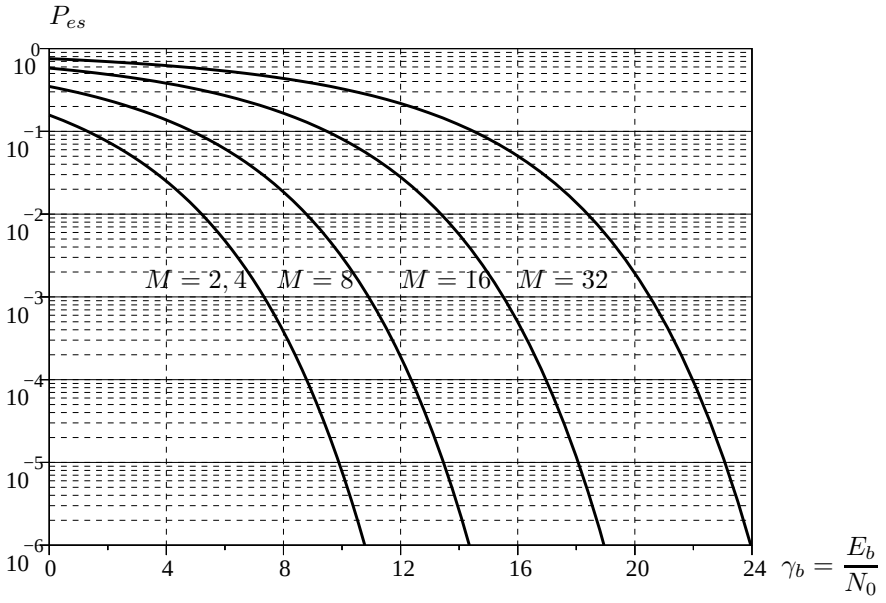


FIG. 1.10 – Taux d'erreur symbole en fonction de $\frac{E_b}{N_0}$ donné par la formule (1.32) pour une modulation M-PSK.

1.3 Décodage souple

Dans ce paragraphe, nous nous intéressons à un algorithme de décodage souple d'un code binaire pouvant s'étendre aux codes M-aires [7]. Notre intérêt est motivé par le fait que le décodage souple est plus performant que le décodage dur en terme de TEB, en fonction du rapport signal à bruit [8].

Soit un code en bloc binaire $\mathcal{C}$ $[n, k, d]$ de longueur n, de dimension k et de distance minimale d. Notons $c_i = (c_{i1}, \ldots, c_{ij}, \ldots, c_{in})$ pour i variant de 1 à 2^k les mots du code $\mathcal{C}$. Pour simplifier les notations, nous considèrerons que c_{ij} appartient à $\{-1, +1\}$, au lieu de $\{0, 1\}$. Le schéma simplifié d'un système de transmission est présenté par la figure (1.11), où les e_j désignent les symboles binaires codés émis et les r_j les données reçues, perturbées par un bruit blanc additif gaussien n_j. L'entrée du décodeur pondéré reçoit, pour chaque échantillon reçu r_j, le couple (y_j, α_j) où y_j est le symbole binaire obtenu par seuillage de r_j (y_j est le signe de r_j) et α_j représente la fiabilité de y_j. Enfin, les d_j représentent les symboles binaires décodés. Notons $\mathbf{E} = [e_1, \ldots, e_j, \ldots, e_n]$ la transmission d'un mot du code $\mathcal{C}$ et $\mathbf{R} = [r_1, \ldots, r_j, \ldots, r_n]$ les données reçues.

La fiabilité de l'élément binaire (voir [7] chapitre 2) y_j ne dépend que de

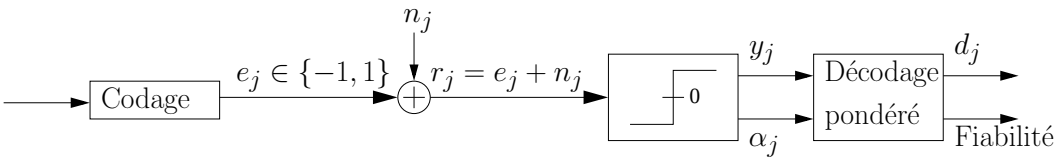


FIG. 1.11 – Schéma simplifié du système de transmission considéré.

l'échantillon r_j du vecteur $\mathbf{R}$, et est donnée par

$$\alpha_j = \frac{\sigma^2}{2} \left| \ln \left(\frac{P(e_j = +1|r_j)}{P(e_j = -1|r_j)} \right) \right| = |r_j|$$

où σ^2 est la variance des échantillons de bruit blanc additif gaussien n_j. A partir de $\mathbf{Y} = [y_1, \ldots, y_j, \ldots, y_n]$ et $\alpha = [\alpha_1, \ldots, \alpha_j, \ldots, \alpha_n]$, la décision optimale est le mot de code $\mathbf{D} = [d_1, \ldots, d_j, \ldots, d_n]$ qui se trouve à la distance euclidienne minimale du vecteur $\mathbf{R}$.

La décision binaire d_j, en sortie du décodeur, dépend de $\mathbf{Y}$ et de α, et donc de $\mathbf{R}$, du fait de la relation de dépendance introduite par le codage. Une mesure de la fiabilité associée à d_j peut ainsi être obtenue à partir du Logarithme du Rapport de Vraisemblance (LRV) qui est défini par

$$LRV_j = \ln \left(\frac{P(e_j = +1|\mathbf{R})}{P(e_j = -1|\mathbf{R})} \right). \tag{1.34}$$

Calculons les probabilités $P(e_j = +1|\mathbf{R})$ et $P(e_j = -1|\mathbf{R})$, afin de développer l'expression (1.34). On a

$$P(e_j = +1|\mathbf{R}) = \sum_{c_i \in \mathcal{C}} P(e_j = +1, \mathbf{E} = c_i|\mathbf{R}). \tag{1.35}$$

En utilisant la formule de Bayes [9], l'expression précédente devient

$$P(e_j = +1|\mathbf{R}) = \sum_{c_i \in \mathcal{C}} P(e_j = +1|\mathbf{E} = c_i, \mathbf{R}) P(\mathbf{E} = c_i|\mathbf{R}). \tag{1.36}$$

En tenant compte du fait que

$$P(e_j = +1|\mathbf{E} = c_i, \mathbf{R}) = \begin{cases} 1 & \text{si} \quad c_{ij} = +1 \\ 0 & \text{si} \quad c_{ij} = -1, \end{cases} \tag{1.37}$$

nous avons la relation

$$P(e_j = +1|\mathbf{R}) = \sum_{\substack{c_i \in \mathcal{C} \\ c_{ij} = +1}} P(\mathbf{E} = c_i|\mathbf{R}). \tag{1.38}$$

Notons $S^{+1(j)}$ l'ensemble des mots de codes c_i tels que $c_{ij} = +1$, l'expression (1.38) devient

$$P(e_j = +1|\mathbf{R}) = \sum_{c_i \in S^{+1(j)}} P(\mathbf{E} = c_i|\mathbf{R}). \tag{1.39}$$

Par un calcul similaire à $P(e_j = +1|\mathbf{R})$ on obtient

$$P(e_j = -1|\mathbf{R}) = \sum_{c_i \in S^{-1(j)}} P(\mathbf{E} = c_i|\mathbf{R}), \tag{1.40}$$

où $S^{-1(j)}$ est l'ensemble des mots de codes c_i tels que $c_{ij} = -1$.

Nous montrons à l'aide de la formule de Bayes [9] que

$$P(\mathbf{E} = c_i|\mathbf{R}) = \frac{f(\mathbf{R}|\mathbf{E} = c_i)P(\mathbf{E} = c_i)}{f(\mathbf{R})}. \tag{1.41}$$

Si $P(\mathbf{E} = c_i) = \dfrac{1}{2^k}$, et si nous supposons que les mots du code sont émis de manière équiprobable, la densité de probabilité notée $f(.)$ est donnée par

$$f(\mathbf{R}|c_i) = \frac{1}{(\sigma\sqrt{2\pi})^n} \quad e^{-\frac{1}{2\sigma^2}\sum_{l=1}^{n}(r_l - c_{il})^2}$$

car $R|c_i$ est un vecteur aléatoire gaussien de moyenne c_i et de matrice de covariance σId_n. En notant $\|\mathbf{R} - c_i\| = \sum_{l=1}^{n}(r_l - c_{il})^2$, les relations (1.39) et (1.40) deviennent respectivement :

$$P(e_j = +1|\mathbf{R}) = \sum_{c_i \in S^{+1(j)}} \frac{1}{2^k f(\mathbf{R})} \frac{1}{(\sigma\sqrt{2\pi})^n} \quad e^{-\frac{1}{2\sigma^2}\|\mathbf{R} - c_i\|} \tag{1.42}$$

et

$$P(e_j = -1|\mathbf{R}) = \sum_{c_i \in S^{-1(j)}} \frac{1}{2^k f(\mathbf{R})} \frac{1}{(\sigma\sqrt{2\pi})^n} \quad e^{-\frac{1}{2\sigma^2}\|\mathbf{R} - c_i\|}. \tag{1.43}$$

En reportant ces expressions dans l'égalité (1.34), nous obtenons pour le LRV associé à la décision du bit d_j la formule suivante :

$$LRV_j = \ln\left(\frac{\displaystyle\sum_{c_i \in S^{+1(j)}} e^{-\frac{1}{2\sigma^2}\|\mathbf{R} - c_i\|}}{\displaystyle\sum_{c_i \in S^{-1(j)}} e^{-\frac{1}{2\sigma^2}\|\mathbf{R} - c_i\|}}\right). \tag{1.44}$$

1.4 Séquences de Gold

Les séquences de Gold, qui sont des séquences binaires, sont utilisées dans le système CDMA comme séquences d'étalement. En effet, comme nous allons le décrire dans la partie suivante, ces séquences ont des propriétés d'autocorrélation et d'intercorrélation qui conviennent parfaitement pour l'étalement de spectre. De plus, l'ensemble des séquences utilisables est assez conséquent.

Dans un premier temps, nous définirons les séquences binaires à longueur maximale, aussi appelées m-séquences, et nous donnerons leurs propriétés principales. Puis dans un second temps, nous définirons les séquences de Gold en tant que m-séquences particulières et nous donnerons leurs propriétés.

1.4.1 Séquences binaires à longueur maximale (m-séquences)

Intéressons-nous dans un premier temps à la génération des m-séquences.

Notons la séquence $(u_n)_{n\in\mathbb{Z}}$ de période N par $\mathbf{u} = (\dots, u_{-1}, u_0, u_1, \dots)$ et sa période par $u = (u_0, u_1, \dots, u_{N-1})$. De même, notons $\mathbb{T}$ l'opérateur de décalage à gauche cyclique sur u, vérifiant la relation

$$\mathbb{T}u = (u_1, u_2, \dots, u_{N-1}, u_0).$$

Les m-séquences sont faciles à générer et très connues [10, 11]. Elles sont générées à l'aide de registres à décalage, connus sous le nom de LFSR (Linear Feedback Shift Register) dans la littérature anglo-saxonne, sur le corps $\mathbb{F}_2$.

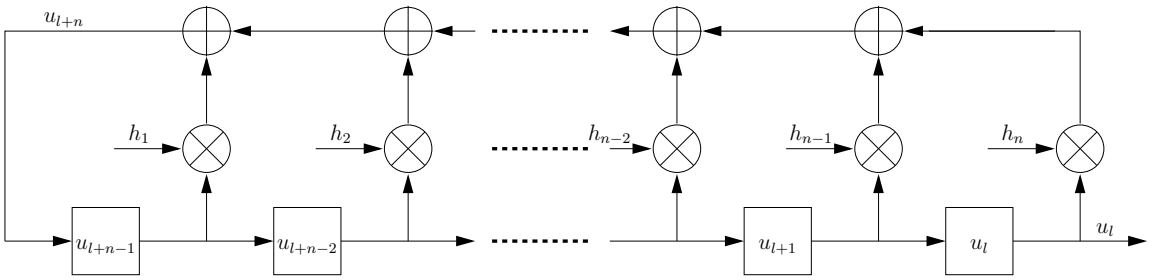


FIG. 1.12 – Registre à décalage linéaire

La figure (1.12) représente le schéma général d'un registre linéaire à décalage, bouclé sur une fonction booléenne linéaire, décrite par les pondérations h_0, $h_1, \dots, h_{n-1}$. L'opérateur $\oplus$ est l'opérateur modulo 2 et les multiplications considérées sont des multiplications modulo 2, définies sur $\mathbb{F}_2$.

Les coefficients h_i prennent la valeur 1 s'il y a la connexion et 0 sinon. Ainsi, le registre à décalage est construit par la mise en cascade d'éléments à retard, reliés par une fonction booléenne linéaire, elle-même réalisée par des

opérations linéaires entre les sorties des éléments à retard u_l et le coefficient correspondant noté h_{l-n+1}.

La séquence **u**, ainsi générée, vérifie la relation de récurrence suivante sur $\mathbb{F}_2$:

$$u_{l+n} = h_n u_l \oplus h_{n-1} u_{l+1} \oplus \cdots \oplus h_1 u_{l+n-1}. \tag{1.45}$$

Lorsque l'on étudie la sortie u_l du LFSR schématisé en figure (1.12), nous pouvons représenter de manière usuelle la récurrence (1.45) par

$$u_l D^n = h_n u_l \oplus h_{n-1} u_l D \oplus \cdots \oplus h_1 u_l D^{n-1} \tag{1.46}$$

où D est l'élément de retard usuel. La séquence nulle est alors obtenue par

$$(h_n \oplus h_{n-1} D \oplus \cdots \oplus h_1 D^{n-1} \oplus D^n) u_l = 0. \tag{1.47}$$

La séquence binaire **u** est donc entièrement décrite par le polynôme générateur $h(x)$ qui est donné en fonction des coefficients h_l par

$$h(x) = x^n + h_1 x^{n-1} + \cdots + h_{n-1} x + h_n. \tag{1.48}$$

Les coefficients du polynôme $h(x)$ satisfont la relation de récurrence (1.45).

Les coefficients du polynôme générateur $h(x)$ sont généralement donnés sous forme octale [12]. Par exemple, le polynôme $h(x) = x^5 + x^2 + 1$ est représenté en notation octale par $\langle 45 \rangle$.

Propriété 1 *Toute séquence binaire u issue d'un registre à décalage est périodique, sa période est au maximum $N = 2^n - 1$ où n est le degré du polynôme générateur de la séquence u.*

La borne supérieure sur la période étant connue, il reste à déterminer les polynômes générateurs permettant d'atteindre cette borne. En effet, la propriété (1) ne donne qu'une borne supérieure pour la période. La période des séquences générées par le polynôme $h(x)$ de degré n dépend de la divisibilité du polynôme $(x^{2^n-1} - 1)$ par $h(x)$ et des propriétés du polynôme $h(x)$, voir [13]. Ainsi les m-séquences sont les séquences générées par un polynôme générateur $h(x)$ primitif et irréductible de degré n. Elles ont pour période $N = 2^n - 1$.

Définition 1 *Le polynôme f(x) est un polynôme irréductible de degré n s'il n'existe pas un couple de polynôme $(f_1(x), f_2(x))$ respectivement de degré $n_1 \geq 1$ et $n_2 \geq 1$ avec $n = n_1 + n_2$ tel que $f(x) = f_1(x) f_2(x)$.*

Définition 2 *Soit f un polynôme de degré n ; f est un polynôme primitif si le plus petit entier l pour lequel f(x) divise $x^l - 1$ est égal à $2^n - 1$.*

Maintenant que nous connaissons les conditions pour obtenir des m-séquences, nous allons nous intéresser aux propriétés de celles-ci.

Propriété 2 *Si la séquence* $\mathbf{u}$ *est générée par un registre à décalage de polynôme générateur h(x), alors toute séquence* $\hat{\mathbf{u}} = \mathbb{T}^i\mathbf{u}$ *est générée par le même polynôme générateur.*

Cette propriété montre que toutes les séquences issues de registres à décalage sont obtenues les unes par rapport aux autres par des décalages cycliques. La propriété suivante est un résultat de la propriété (2) :

Propriété 3 *Si les séquences* $\mathbf{u}$ *et* $\mathbf{v}$ *sont générées par un même registre à décalage de polynôme générateur* $h(x)$ *alors la séquence* $\mathbf{w} = \mathbf{u} \oplus \mathbf{v}$ *est générée par le même registre à décalage.*

Soit Ξ l'ensemble des m-séquences issues du registre à décalage ayant pour polynôme générateur $h(x)$ de degré n. La propriété suivante donne le cardinal de Ξ.

Propriété 4 *Il y a* $N = 2^n - 1$ *séquences à longueur maximale générées par un registre à décalage de polynôme générateur* $h(x)$ *primitif, irréductible et de degré n, c'est à dire* $card(\Xi) = N$*. La famille de séquences ainsi générée est constituée des différents décalages cycliques à gauche d'une séquence fondamentale* $\mathbf{u}$*, c'est à dire* $\Xi = \{\mathbf{u}, \mathbb{T}\mathbf{u}, \mathbb{T}^2\mathbf{u}, \ldots, \mathbb{T}^{N-1}\mathbf{u}\}$.

Cette propriété montre que les séquences à longueur maximale sont obtenues les unes à partir des autres par des applications successives de l'opérateur $\mathbb{T}$.

Propriété 5 Décalage et Addition
Une séquence $\mathbf{u}$ *de période* N *est une séquence à longueur maximale si et seulement si, pour chaque couple d'entiers distincts* i *et* j *tels que* $i, j \in \{0, 1, 2, \ldots, N-1\}$*, il existe un unique* $k \in \{0, 1, 2, \ldots, N-1\} \backslash \{i, j\}$ *tel que* $\mathbb{T}^i\mathbf{u} \oplus \mathbb{T}^j\mathbf{u} = \mathbb{T}^k\mathbf{u}$.

La propriété suivante, appelée dans la littérature premier postulat de Golomb, illustre le caractère aléatoire des séquences binaires à longueur maximale [14].

Propriété 6 *Le poids de Hamming d'une période u d'une séquence* $\mathbf{u}$ *à longueur maximale est* $w_H(u) = 2^{n-1} = \frac{N+1}{2}$.

Cette propriété montre que les m-séquences sont des séquences équilibrées ; en effet il y a 2^{n-1} uns pour $2^{n-1} - 1$ zéros.

La propriété la plus importante des m-séquences est la propriété d'autocorrélation. En effet, la nature aléatoire des séquences à longueur maximale se traduit par une fonction d'autocorrélation périodique s'annulant pour tous retards $k > 0$; c'est le troisième postulat de Golomb [14].

Définissons tout d'abord l'intercorrélation périodique et l'autocorrélation périodique dans un cadre général puis dans le cas de séquences binaires.

Définition 3 Intercorrélation périodique (cas complexe)
Soient $\mathbf{u}$ *et* $\mathbf{v}$ *deux séquences, à valeurs complexes, périodiques de période N. L'intercorrélation périodique* $\theta_{\mathbf{u},\mathbf{v}}(l)$ *de ces séquences est définie par*

$$\theta_{\mathbf{u},\mathbf{v}}(l) = \sum_{i=0}^{N-1} u_i v_{l+i}^*,$$

où v_{l+i}^* *est le conjugué de* v_{l+i}.

Définition 4 Autocorrélation périodique (cas complexe)
Soit $\mathbf{u}$ *une séquence à valeurs complexes, périodique de période N. L'autocorrélation périodique* $\theta_{\mathbf{u}}(l)$ *de cette séquence est définie par*

$$\theta_{\mathbf{u}}(l) = \theta_{\mathbf{u},\mathbf{u}}(l).$$

Dans le cas binaire ces définitions deviennent :

Définition 5 Intercorrélation périodique (cas binaire)
Soient $\mathbf{u}$ *et* $\mathbf{v}$*, deux séquences binaires, périodiques de période N. L'intercorrélation périodique* $\theta_{\mathbf{u},\mathbf{v}}(l)$ *de ces séquences est définie par*

$$\theta_{\mathbf{u},\mathbf{v}}(l) = N - 2w_H(u \oplus \mathbb{T}^l v).$$

Définition 6 Autocorrélation périodique (cas binaire)
Soit $\mathbf{u}$ *une séquence binaire, périodique, de période N. L'autocorrélation périodique de* $\theta_{\mathbf{u}}(l)$ *de cette séquence est définie par*

$$\theta_{\mathbf{u}}(l) = N - 2w_H(u \oplus \mathbb{T}^l u).$$

Définissons aussi les paramètres d'intercorrélation pic et d'autocorrélation pic notés respectivement θ_c et θ_a. Ces paramètres donnent en valeur absolue une borne supérieure sur les valeurs prises respectivement par les fonctions d'intercorrélation et d'autocorrélation périodiques.

Définition 7 Intercorrélation pic
Le paramètre d'intercorrélation pic sur l'ensemble Ξ *est défini par*

$$\theta_c = \max\{|\theta_{\mathbf{u},\mathbf{v}}(k)| / 0 \leq k \leq N-1, (\mathbf{u},\mathbf{v}) \in \Xi^2, \mathbf{u} \neq \mathbf{v}\}.$$

Définition 8 Autocorrélation pic
Le paramètre d'autocorrélation pic sur l'ensemble Ξ *est défini par*

$$\theta_a = \max\{|\theta_{\mathbf{u},\mathbf{u}}(k)| / 1 \leq k \leq N-1, \mathbf{u} \in \Xi\}.$$

En plus de connaître les propriétés de corrélation des séquences, il est important pour certaines applications, tel le CDMA, de connaître le spectre d'intercorrélation des séquences, comme l'ont défini Sarwate et Pursley dans [10].

Définition 9 *On appelle spectre d'intercorrélation des séquences* $\mathbf{u}$ *et* $\mathbf{v}$*, l'ensemble des valeurs prises par la fonction d'intercorrélation périodique* $\theta_{\mathbf{u},\mathbf{v}}(k)$ *pour les différents retards* $0 \leq k \leq N-1$.

En utilisant les propriétés (5), (6) et la définition (6) nous obtenons la propriété suivante sur l'autocorrélation périodique des m-séquences.

Propriété 7 *La fonction d'autocorrélation périodique des m-séquences est donnée par la relation suivante :*

$$\theta_{\mathbf{u}}(k) = \begin{cases} N & k \equiv 0 \ [N] \\ -1 & k \not\equiv 0 \ [N] \end{cases}$$

où N est la longueur des m-séquences.

Les m-séquences sont parfaites du point de vue de la fonction d'autocorrélation périodique. Mais du point de vue de l'intercorrélation, ces séquences ne le sont pas, voir [10]. En effet, les m-séquences sont obtenues par applications successives de l'opérateur $\mathbb{T}$, cf propriété (4). Il existe donc un entier k tel que $\mathbf{v} = \mathbb{T}^k\mathbf{u}$ et pour lequel la valeur de l'intercorrélation périodique $\theta_{\mathbf{u},\mathbf{v}}(k)$ est maximale, c'est à dire $\theta_{\mathbf{u},\mathbf{v}}(k) = N$.

Cela a motivé le développement de familles de séquences obtenues par combinaisons de m-séquences particulières, ou encore par décimation, comme le définissent Sarwate et Pursley dans [10]. Afin d'utiliser ces séquences dans les applications CDMA, il est important de minimiser le paramètre d'intercorrélation pic associé aux m-séquences. Pour cela, nous présenterons une méthode basée sur la décimation des m-séquences puis nous parlerons de la construction d'ensembles connectés [10] et des paires préférées de m-séquences.

Définition 10 *On définit la q-décimation d'une m-séquence* $\mathbf{u}$ *comme la séquence* $\mathbf{u}[q]$ *telle que* $u[q]_l = u_{ql}$.

La q-décimation d'une m-séquence vérifie la propriété suivante.

Propriété 8 *Si la séquence* $\mathbf{u}[q]$*, n'est pas identiquement nulle alors la séquence* $\mathbf{u}[q]$ *est périodique et de période* $n_q = \dfrac{N}{pgcd(N,q)}$.

Ainsi, si le facteur de décimation q est premier avec la période de la m-séquence, la séquence $\mathbf{u}[q]$ est une m-séquence de période N. La décimation est alors appelée décimation propre de la m-séquence $\mathbf{u}$. Le théorème suivant nous donne le spectre d'intercorrélation des séquences suivant la valeur de la décimation.

Théorème 1 *Soient* $\mathbf{u}$ *et* $\mathbf{v}$ *deux m-séquences de période* $N = 2^n - 1$*. Si la séquence* $\mathbf{v}$ *est la q-décimation de la séquence* $\mathbf{u}$ *avec* $q = 2^k + 1$ *ou* $q = 2^{2^k} - 2^k + 1$ *et si* $e = pgcd(n,k)$ *tel que le rapport* $l = \frac{n}{e}$ *soit impair, alors*

le spectre d'intercorrélation des séquences $\mathbf{u}$ *et* $\mathbf{v}$ *est constitué de trois valeurs dans les proportions suivantes :*

$$\begin{array}{lll} -1+2^{\frac{n+e}{2}} & \textit{apparaît} & 2^{n-e-1}+2^{\frac{n-e-2}{2}} \quad \textit{fois}, \\ -1 & \textit{apparaît} & 2^n+2^{n-e}-1 \quad \textit{fois}, \\ -1-2^{\frac{n+e}{2}} & \textit{apparaît} & 2^{n-e-1}-2^{\frac{n-e-2}{2}} \quad \textit{fois}. \end{array}$$

Nous constatons que les amplitudes ainsi que le nombre d'apparitions des différentes valeurs du spectre d'intercorrélation dépendent du paramètre e. Une approche conventionnelle pour l'optimisation des séquences d'étalement en terme de minimisation du paramètre θ_c peut se formuler comme suit : prendre le paramètre e le plus faible possible lorsque n est impair : par exemple, $e = 1$ et une valeur faible pour le paramètre k, voir références [10, 15]. Lorsque le degré du polynôme générateur est $n \equiv 2$ [4] on choisit $e = 2$ et $k = 2$.

Nous pouvons regrouper ces propositions dans la propriété suivante.

Propriété 9 *Soit* $t(n) = 1 + 2^{\lfloor \frac{n+2}{2} \rfloor}$. *Si* $n \not\equiv 0$ [4]*, il existe des paires de m-séquences ayant un spectre de corrélation à trois valeurs données par l'ensemble* $\{-t(n), -1, t(n) - 2\}$.

On appelle *paires préférées* de m-séquences, les paires de séquences vérifiant la propriété (9).

Nous venons de voir une méthode pour générer et trouver des paires préférées de m-séquences ayant de bonnes propriétés d'intercorrélation. Toutefois, dans l'objectif d'utiliser ces séquences dans une application CDMA, il est important de construire un ensemble de séquences, de cardinal le plus grand possible, ayant, de préférence, les mêmes propriétés de corrélation que celles des paires préférées les constituant. Nous parlerons alors d'ensembles connectés.

Définition 11 *On appelle ensembles connectés les ensembles de séquences binaires* Ξ *tels que tout couple de séquences* $(\mathbf{u}, \mathbf{v}) \in \Xi^2$ *soit une paire préférée. Un ensemble maximal connecté est l'ensemble connecté de cardinalité maximale.*

Le problème de la recherche d'ensembles de séquences connectées et connectées maximales est un problème difficile en général. La table (1.1) que nous avons reprise de [10] montre quelques exemples de ces constructions. M_n représente la taille de l'ensemble maximal connecté, M_s représente le nombre de m-séquences, $t(n)$ est le paramètre d'intercorrélation maximal défini dans la proposition (9), N est la longueur de la période de la séquence et n est le degré du polynôme générateur correspondant.

Notons que dans cette table, si n a pour valeur 4 ou 8, il n'existe pas de paires préférées. Dans ces cas, il est possible de construire des paires de m-séquences ayant un spectre d'intercorrélation pouvant prendre 4 valeurs.

n	$N = 2^n - 1$	M_s	M_n	$t(n)$
3	7	2	2	5
4	15	2	0	9
5	31	6	3	9
6	63	6	2	17
7	127	18	6	17
8	255	16	0	33
9	511	48	2	33
10	1023	60	3	65

TAB. 1.1 – Ensembles maximaux connectés de m-séquences [10].

Théorème 2 *Soient* $\mathbf{u}$ *et* $\mathbf{v}$ *deux* m*-séquences de période* $N = 2^n - 1$*, où* n *est un multiple de* 4*. Si* $\mathbf{v} = \mathbf{u}[-1 + 2^{\frac{n+2}{2}}] = \mathbf{u}[t(n) - 2]$*, alors le spectre d'intercorrélation des séquences* $\mathbf{u}$ *et* $\mathbf{v}$ *est constitué de quatre valeurs dans les proportions suivantes :*

$$\begin{array}{lll} -1 + 2^{\frac{n+2}{2}} & \textit{apparaît} & \dfrac{2^{n-1} - 2^{\frac{n-2}{2}}}{3} \quad \textit{fois}, \\ -1 + 2^{\frac{n}{2}} & \textit{apparaît} & 2^{\frac{n}{2}} \quad \textit{fois}, \\ -1 & \textit{apparaît} & 2^{n-1} - 2^{\frac{n-2}{2}} - 1 \quad \textit{fois}, \\ -1 - 2^{\frac{n}{2}} & \textit{apparaît} & \dfrac{2^n - 2^{\frac{n}{2}}}{3} \quad \textit{fois}. \end{array}$$

Les relations précédentes ont montré qu'il est possible de construire par des décimations choisies de m-séquences des ensembles de séquences avec de faibles paramètres d'intercorrélation pic. Cependant, ces ensembles ont en général une cardinalité faible. Ce nombre faible de paires préférées ainsi que la difficulté associée à leur construction constituent des problèmes majeurs lors de leur application à l'accès multiple en général et au système CDMA en particulier.

Les séquences de Gold offrent une solution à ce problème en développant des familles de séquences de grande cardinalité et ayant de faibles paramètres de corrélation pour les applications CDMA.

1.4.2 Définitions et propriétés des séquences de Gold

Les séquences de Gold ont été développées par R.A. Gold [16, 17] pour augmenter la cardinalité des ensembles connectés décrits dans la section précédente. Ces séquences optimisent le paramètre d'intercorrélation pic θ_c et procurent un nombre suffisant de séquences à disposition du système CDMA.

Les deux propriétés suivantes permettent de bien comprendre les séquences de Gold.

Propriété 10 *Soit un polynôme générateur d'un registre à décalage donné par* $f(x) = h(x)\hat{h}(x)$ *où les polynômes* $h(x)$ *et* $\hat{h}(x)$ *n'ont pas de facteur en commun. L'ensemble des séquences générées par le polynôme* $f(x)$ *est l'ensemble de toutes les séquences de la forme* $\mathbf{u} \oplus \mathbf{v}$ *où* $\mathbf{u}$ *et* $\mathbf{v}$ *sont des séquences binaires générées par les polynômes* $h(x)$ *et* $\hat{h}(x)$ *respectivement.*

Propriété 11 *Supposons que* $f(x) = h(x)\hat{h}(x)$ *où* $h(x)$ *et* $\hat{h}(x)$ *sont des polynômes primitifs de degré n. Si* $\mathbf{w}$ *est une séquence non nulle générée par f(x), alors pour toutes séquences* $\mathbf{u}$ *et* $\mathbf{v}$ *générées par les polynômes* $h(x)$ *et* $\hat{h}(x)$ *respectivement, il existe* i *et* j *entiers avec* $0 \leq i, j \leq N-1$*, tel que la séquence* $\mathbf{w}$ *s'écrit sous l'une des formes suivantes :*

$$\begin{aligned} \mathbf{w} &= \mathbb{T}^i\mathbf{u}, \\ \mathbf{w} &= \mathbb{T}^j\mathbf{v}, \\ \mathbf{w} &= \mathbb{T}^i\mathbf{u} \oplus \mathbb{T}^j\mathbf{v}. \end{aligned}$$

La propriété (11) montre que l'ensemble de toutes les séquences générées par $f(x)$ est l'ensemble $G(u,v) = \{\mathbf{u}, \mathbf{v}, \mathbf{u} \oplus \mathbf{v}, \mathbf{u} \oplus \mathbb{T}\mathbf{v}, \ldots, \mathbf{u} \oplus \mathbb{T}^{N-1}\mathbf{v}\}$. Cet ensemble $G(u,v)$ contient $N+2 = 2^n+1$ séquences d'étalement de période N. Nous avons donc pu construire à partir de deux séquences $\mathbf{u}$ et $\mathbf{v}$ un ensemble de séquences linéaires sur $\mathbb{F}_2$, obtenues par additions modulo 2 et applications successives de l'opérateur de décalage $\mathbb{T}$. La propriété suivante décrit le paramètre de corrélation des séquences construites de cette façon.

Propriété 12 *Lorsque les séquences* $\mathbf{u}$ *et* $\mathbf{v}$ *sont des séquences de longueur maximale, les paramètres de corrélation des séquences de l'ensemble G(u,v) satisfont :*

$$\theta_c = \theta_a = \max\{|\theta_{\mathbf{u},\mathbf{v}}(l)| : 0 \leq l \leq N-1\}.$$

La propriété (12) montre que pour toute paire de séquences à longueur maximale générées respectivement par les polynômes $h(x)$ et $\hat{h}(x)$ ayant des paramètres de corrélation donnés par $\theta_m = \max\{\theta_a, \theta_c\}$, on peut construire une famille de $N+2$ séquences ayant des paramètres d'intercorrélation et d'autocorrélation donnés par $\theta_c = \theta_a = \theta_m$.

En particulier, lorsque la paire de séquences utilisée pour construire $G(u,v)$ est une paire préférée, les paramètres de corrélation vont être donnés par $\theta_c = \theta_a = t(n)$. Les séquences de cet ensemble sont les *séquences de Gold*, voir [16, 17]. Les séquences de Gold ainsi définies vérifient la propriété suivante :

Propriété 13 *Si* $(\mathbf{u}, \mathbf{v})$ *est une paire préférée de séquences à longueur maximale générées par les polynômes primitifs* $h(x)$ *et* $\hat{h}(x)$ *respectivement, alors, pour chaque couple de séquences* $(\mathbf{u}', \mathbf{v}') \in G(u,v)$*, l'autocorrélation et l'intercorrélation des séquences vérifient la relation :*

$$\forall k \in \mathbb{N},\ k \not\equiv 0\ [N] \quad \theta_{\mathbf{u}',\mathbf{u}'}(k) \in \{-1, -t(n), t(n)-2\} \tag{1.49}$$

$$\forall k \in \mathbb{N} \quad \theta_{\mathbf{u}',\mathbf{v}'}(k) \in \{-1, -t(n), t(n)-2\} \tag{1.50}$$

La propriété (13) montre que l'on peut construire à partir d'une paire préférée de séquences à longueur maximale une famille de séquences ayant des propriétés de corrélations prédictibles, avec une égalité des paramètres θ_a et θ_c. La figure (1.13) représente un schéma de génération des séquences de Gold à partir de deux séquences à longueur maximale. Les registres à décalage sont initialisés avec différentes valeurs non nulles pour obtenir toutes les séquences de l'ensemble $G(u, v)$.

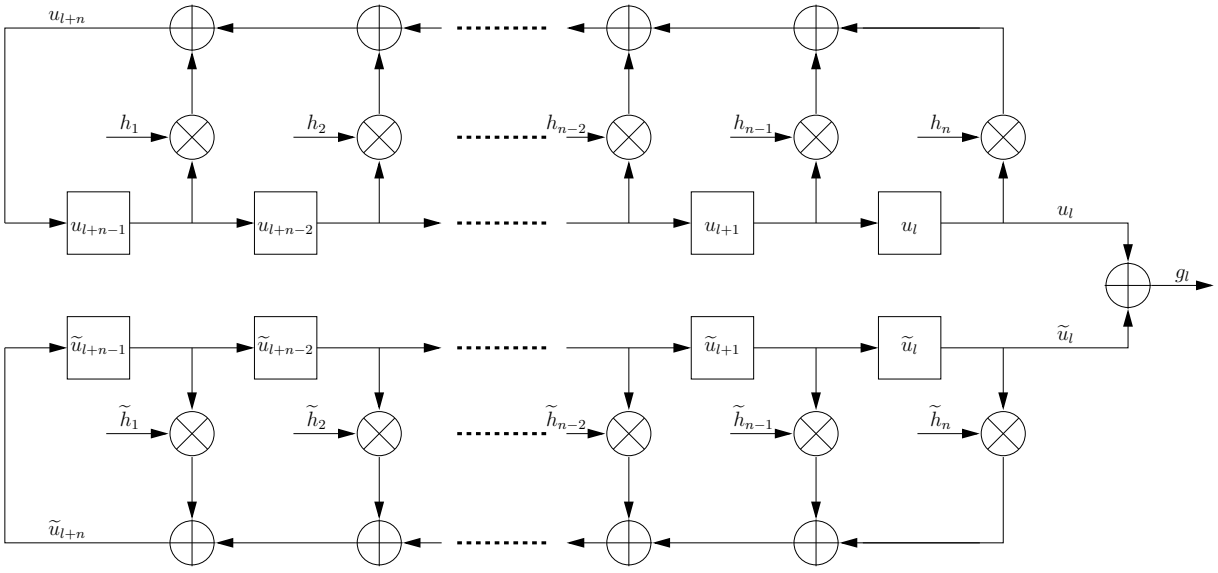


FIG. 1.13 – Génération des séquences de Gold

La table (1.2) récapitule le nombre de séquences de Gold pouvant être générées par rapport aux m-séquences. M_n représente la taille de l'ensemble des séquences maximum connectées, M_s représente le nombre de m-séquences, M_G représente le nombre de séquences de Gold pouvant être générées, $t(n)$ est le paramètre d'intercorrélation maximal défini dans la proposition (9), N est la longueur de la période de la séquence et n est le degré du polynôme générateur correspondant.

Les couples de m-séquences qui donnent des paires préférées se trouvent assez facilement dans la littérature. Par exemple Dixon, dans [18], donne une sélection de paires préférées pour des degrés de polynômes compris entre 5 et 13.

D'autres types de séquences binaires peuvent être utilisés en CDMA comme les séquences de Kasami [19] qui présentent, elles aussi, une très faible intercorrélation, ou les séquences orthogonales [20] dans le cas d'un CDMA synchrone.

n	$N = 2^n - 1$	M_s	M_n	M_G	$t(n)$
3	7	2	2	18	5
4	15	2	0	0	9
5	31	6	3	99	9
6	63	6	2	130	17
7	127	18	6	774	17
8	255	16	0	0	33
9	511	48	2	1026	33
10	1023	60	3	3075	65

TAB. 1.2 – Paires préférées et valeur maximale de l'intercorrélation.

Chapitre 2

Étalement de spectre et accès multiple à répartition par les séquences d'étalement

Les systèmes de communication à accès multiples se décomposent en trois catégories, voir figure (2.1) :

La première utilise le multiplexage temporel [21, 22] (TDMA : Time Division Multiple Access) où chaque utilisateur émet dans la même bande de fréquence mais à des instants différents.

La seconde utilise le multiplexage fréquentiel [22, 23] (FDMA : Frequency Division Multiple Access). Ici, les utilisateurs émettent simultanément mais dans des bandes de fréquence différentes.

La dernière catégorie utilise un multiplexage par les séquences d'étalement (CDMA : Code Division Multiple Access). Avec cette méthode "tout le monde parle en même temps et au même endroit, mais chacun dans sa langue".

Nous nous sommes intéressés à cette dernière catégorie de système car c'est la plus intéressante parmi les trois citées du fait qu'elle n'impose pas de contrainte de temps ni de fréquence. En effet, la première catégorie impose une contrainte de temps : une seule bande de fréquence est utilisée et chaque utilisateur a un temps limité pour communiquer. La seconde catégorie impose une contrainte sur le nombre de bandes de fréquences utilisables : les utilisateurs ont un temps illimité pour communiquer, mais chaque utilisateur émet dans une bande de fréquence différente. Or la bande de fréquence n'est pas illimitée et est onéreuse, ce système a un nombre restreint d'utilisateurs. Dans la catégorie qui nous intéresse, tous les utilisateurs émettent dans la même bande de fréquence et sans contrainte de temps. Cette catégorie utilise les avantages des deux autres sans leurs inconvénients.

Dans un premier temps, nous nous intéresserons à la technique de l'étalement de spectre, qui est la base du CDMA. Nous nous intéresserons ensuite au CDMA proprement dit.

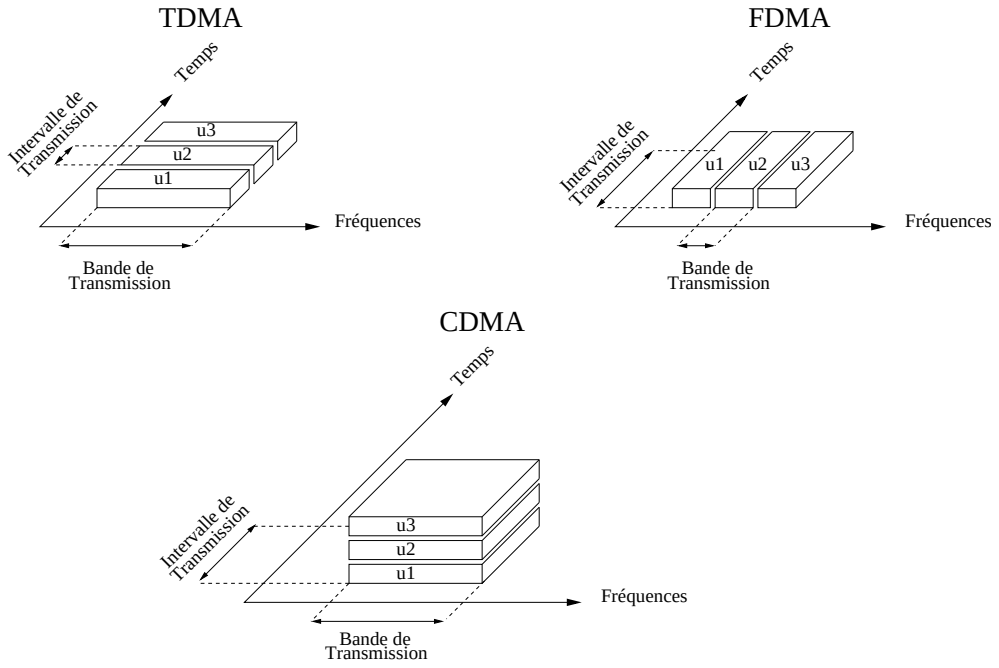


FIG. 2.1 – Les différents types de multiplexage

2.1 Étalement de spectre

Depuis les années 1940, les techniques d'étalement de spectre sont utilisées pour des applications militaires. Ces techniques fournissent une excellente immunité aux interférences et permettent à la transmission d'être cachée dans le bruit de fond. Récemment, les systèmes à étalement de spectre ont été adaptés pour des applications civiles et plus particulièrement dans les systèmes de téléphonie sans fil [22].

Dans la chaîne de transmission des données, le bloc "étalement de spectre" se trouve entre le bloc "codage canal" et le bloc "canal" comme le montre le schéma (2.2). Le bloc "reconstruction signal" est le bloc inverse du bloc "étalement de spectre". Il transforme le signal large bande en signal bande étroite et donne, en sortie, les bits probablement émis.

Le principe de l'étalement de spectre [24] consiste à répartir l'énergie du signal à émettre sur une bande de fréquence plus large que celle réellement nécessaire à la transmission du signal utile. Les deux principales techniques de modulation par étalement de spectre sont la séquence directe [21, 22] (Direct Sequence Spread Spectrum) et le saut de fréquence [21, 22] (Frequency Hopping Spread Spectrum). Dans le cas de la séquence directe, l'énergie du signal est répartie sur toute la bande de fréquence disponible, alors que pour le saut de fréquence, la bande de fréquence disponible est divisée en un grand nombre de sous-canaux. La fréquence porteuse se déplace alors d'un sous-canal à l'autre par des sauts discrets pseudo-aléatoires.

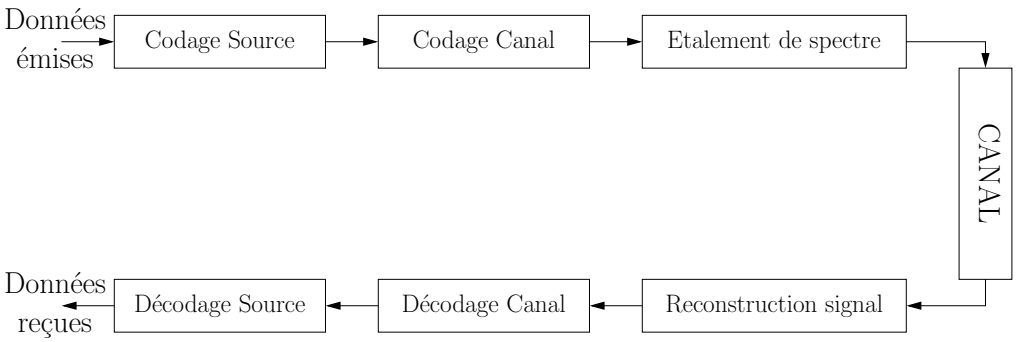


FIG. 2.2 – Schéma d'une chaîne de transmission

Nous nous sommes principalement intéressés à l'étalement de spectre par séquences directes. Nous présentons en détail cette technique pour en décrire ensuite les avantages et les inconvénients.

2.1.1 Étalement de spectre par séquence directe

Cette technique consiste à multiplier chaque bit d'information par une séquence pseudo-aléatoire binaire, notée PN, de rythme très supérieur à celui des données à transmettre, voir figure (2.3). En supposant que le rythme de la séquence d'étalement est N fois plus grand que le débit de données, il en résulte, en notant T_b la durée d'un bit d'information et T_c la durée d'un bit de la séquence d'étalement, que

$$T_b = N\ T_c \tag{2.1}$$

où N est appelé gain de traitement du système à étalement de spectre.

La figure (2.3) présente cette technique d'étalement de spectre par séquence directe sur l'émission du message binaire $d = (0, 1, 0)$ avec la séquence d'étalement $PN = (0, 1, 0, 0, 1, 0, 1, 1)$. Pour simplifier les notations, nous considérons que les bits du message à transmettre d sont à valeurs dans $\{-1, 1\}$ au lieu de {0,1}. Les données à transmettre $(d_1, d_2, d_3) = (1, -1, 1)$, représentées par le premier graphique, ont une durée d'émission de T_b. La séquence d'étalement PN est, quant à elle, représentée par le second graphique. Elle est répétée trois fois car, contrairement aux données à transmettre, les bits de la séquence PN ont une durée d'émission T_c plus petite que T_b. Dans notre exemple, nous avons $T_b = 8T_c$. Le facteur d'étalement est donc $N = 8$. Ainsi, 8 bits de la séquence d'étalement PN sont nécessaires pour transmettre un bit de donnée d_i. Les bits transmis sur le canal sont donnés par le troisième graphique qui représente la multiplication des données par la séquence d'étalement PN ; ces bits ont une durée d'émission identique à celui des bits de la séquence PN, notée T_c.

Ainsi, à chaque bit d'information peut correspondre, suivant la valeur du facteur d'étalement, soit une période de la séquence PN, soit une partie

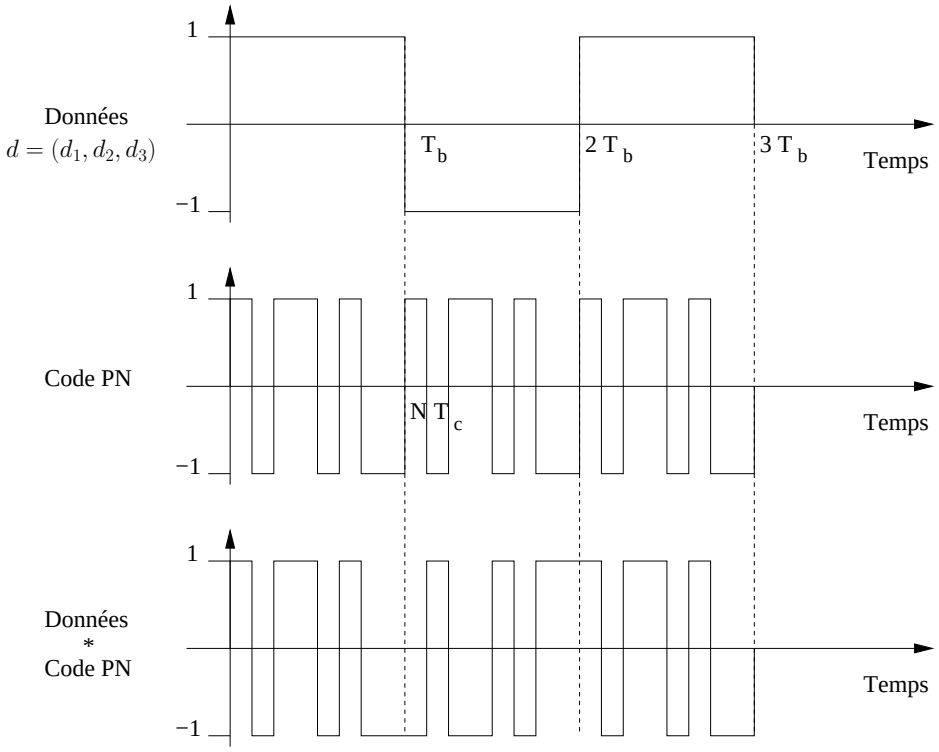


FIG. 2.3 – Étalement de spectre par séquence directe

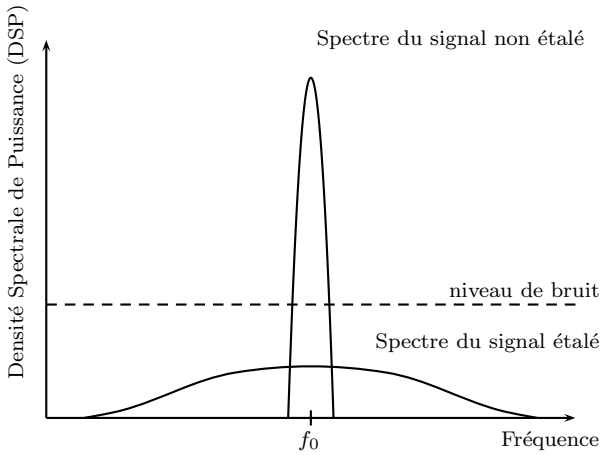


FIG. 2.4 – Comparaison signal bande étroite / signal étalé.

tronquée de cette période, soit plusieurs périodes.

Dans le domaine fréquentiel, la notion d'étalement de spectre est représentée par la figure (2.4). La puissance du signal étalé, émis par étalement de spectre, est la même que celle du signal non étalé, émis sans étalement de spectre. Toutefois, elle n'est pas répartie sur la même largeur de bande de fréquence. On appelle alors un signal non étalé, un signal bande étroite, et un signal étalé, un signal large bande.

En réception, le signal est reconstruit en multipliant, dans un synchronisme parfait, le signal reçu par une séquence PN locale identique à celle utilisée à l'émission. La synchronisation de ces deux signaux est plus ou moins délicate suivant la technique utilisée pour le calcul de la corrélation.

2.1.2 Avantages et Inconvénients

Comme nous l'avons vu, la technique de l'étalement de spectre consiste à moduler le signal contenant l'information puis à *"l'étaler"* de manière à ce que le spectre du signal émis occupe une bande de fréquence très supérieure à celle nécessaire à la transmission de l'information. L'étalement de spectre, par rapport aux modulations à bande étroite, présente de nombreux avantages, voir [25] :

- *bonne résistance aux perturbations bande étroite* : lors de l'émission, des perturbations bande étroite peuvent s'ajouter au signal étalé. Le récepteur réalise l'opération inverse de l'étalement. Le signal étalé est ainsi transformé en signal bande étroite alors que les perturbations à bande étroite sont étalées. De cette façon, la puissance des perturbations devient négligeable devant celle du signal utile reconstitué, voir figure (2.5).

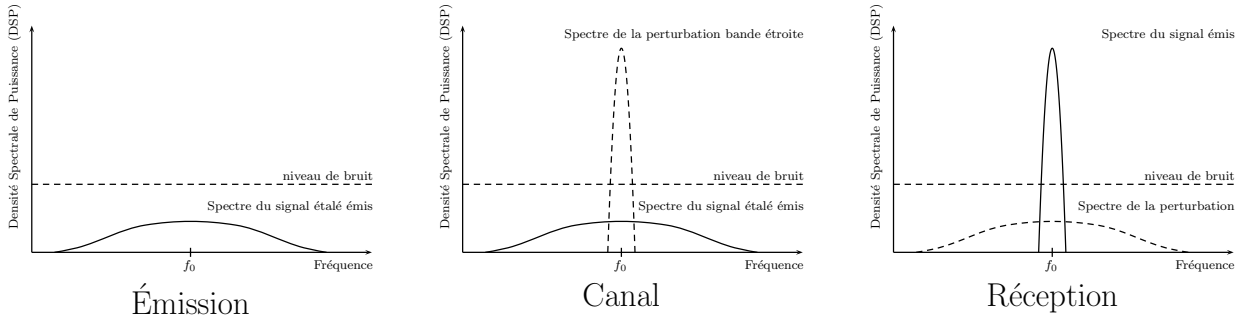


FIG. 2.5 – Exemple d'émission avec une perturbation bande étroite.

- *faible brouillage des émissions classiques à bande étroite* : les signaux à bande étroite peuvent cohabiter sur la même bande de fréquence que ceux générés par un système à étalement de spectre, sans perturber de façon importante un système par rapport à l'autre. La puissance de ces signaux est étalée sur une bande de fréquence importante. Leur densité

spectrale de puissance est donc très faible comparée à celle des signaux à bande étroite.

- *insensibilité aux effets des trajets multiples* : contrairement aux transmissions bande étroite, l'étalement de spectre permet de lutter efficacement contre l'effet des trajets multiples de propagation. Les creux de Fading [26] résultant de ces trajets multiples peuvent absorber complètement le spectre d'une modulation bande étroite. Dans le cas d'une modulation large bande, sous réserve que cette bande soit supérieure à la bande de cohérence du canal radio, seule une partie du signal disparaît.

- *faible probabilité d'interception* : le signal ayant les caractéristiques d'un bruit aléatoire dont le niveau peut être inférieur à celui du bruit thermique, la communication est difficilement détectable. De plus, si le signal était détecté, seuls les récepteurs possédant les paramètres de la séquence d'étalement pourront accéder à l'information.

- *multiplexage et adressage sélectif* : plusieurs émissions peuvent cohabiter dans la même bande de fréquence dans la mesure où les codes d'étalement relatifs à chacun des signaux sont orthogonaux, c'est à dire dans la mesure où ils présentent une intercorrélation voisine de zéro (code de Hadamard, code de Walsh [27], code de Gold [10]). La séquence d'étalement affectée à chaque signal constitue sa *clé de codage*. Ce signal ne peut être exploité que si le récepteur possède la même *clé de codage*. Cette propriété se nomme l'Accès Multiple à Répartition par les séquences d'étalement, appellation que l'on trouve dans la littérature anglo-saxonne sous le terme CDMA (Code Division Multiple Access), voir [20, 21, 22, 23].

Quelques inconvénients sont liés à cette technique :

- encombrement spectral important qui rend souvent l'attribution de fréquences difficile. En effet, le signal a toujours la même puissance mais celle-ci est répartie différemment.

- complexité accrue des systèmes qui rend leur coût plus élevé par rapport à celui des systèmes bande étroite.

- nécessité d'avoir de bonnes méthodes de synchronisation permettant, à la réception, de reconstruire le signal émis.

Ce type d'émetteur-récepteur, utilisant l'étalement de spectre, est principalement utilisé dans les systèmes CDMA, c'est à dire dans un environnement multi-utilisateurs. Il se distingue aussi d'autres systèmes, comme le MBOK (M-

ary Bi-Orthogonal Keying) [27, 28] et le CCK (Complementary Code Keying) [29, 30, 31], qui sont contraints de fonctionner simplement en mono-utilisateur pour avoir des performances optimales.

2.2 Accès Multiple à Répartition par les séquences d'étalement

Les systèmes CDMA sont une extension des systèmes à étalement de spectre par séquences directes, DS-CDMA (Direct Sequence CDMA), et par sauts de fréquences, FH-CDMA (Frequency Hopping CDMA).

Chaque utilisateur du système possède sa propre séquence d'étalement pseudo-aléatoire. La discrimination des utilisateurs dans le système dépend des propriétés d'auto et d'intercorrélation de la famille de séquences considérées. En effet, la fonction d'autocorrélation fixe la capacité du système à se synchroniser dans le cas mono-utilisateur et l'intercorrélation, quant à elle, détermine le Bruit d'Accès Multiples (BAM ou MAI pour Multiple Access Interference). Le choix de la famille de codes d'étalement est donc un critère important dans la réalisation d'un système CDMA. Nous verrons dans le chapitre suivant les familles de séquences les mieux adaptées à ce système.

Un autre critère important est le contrôle de la puissance émise par les utilisateurs. Chaque utilisateur doit émettre avec la même puissance (problème de Near Far Effect [32]). Dans le cas contraire, seul l'utilisateur possédant la plus forte puissance sera correctement démodulé.

La figure (2.6) présente le principe du CDMA : les signaux provenant de M utilisateurs sont transmis autour d'une porteuse de fréquence f_0. Nous avons à l'émission "l'empilement" des M spectres des signaux émis autour de la fréquence f_0 . En réception, seul le spectre du signal utile de l'utilisateur A, par exemple, est "désétalé", les $M-1$ autres signaux sont à nouveau étalés par la séquence pseudo-aléatoire de l'utilisateur A.

Il existe deux types de CDMA : le CDMA synchrone (S-CDMA) et le CDMA asynchrone (A-CDMA). Dans le cas d'une communication satellite/ utilisateur de télévision à péage, le CDMA synchrone correspond à une communication du satellite vers les utilisateurs, tandis que le CDMA asynchrone correspond à une communication de l'utilisateur vers le satellite.

Dans le cas du CDMA synchrone, l'orthogonalité des codes d'étalement est exploitée au maximum, tandis que dans le second cas, CDMA asynchrone, les décalages temporels existant entre les utilisateurs ne permettent pas l'utilisation de l'orthogonalité des codes d'étalement.

Les avantages du CDMA sont les mêmes que ceux de l'étalement de spectre :

- bonne résistance aux perturbateurs bande étroite ;
- faible brouillage des émissions classiques à bande étroite ;

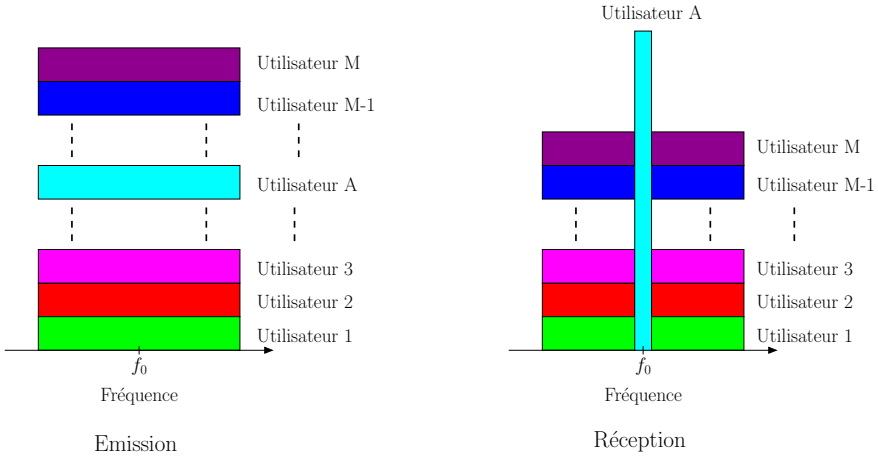


FIG. 2.6 – Principe du CDMA

– insensibilité aux effets des trajets multiples ;

– faible probabilité d'interception ;

– multiplexage et adressage sélectif.

Les principaux inconvénients sont :
– la puissance d'émission est la même pour chaque utilisateur. Il faut alors utiliser un sous-système permettant de contrôler la puissance.

– la synchronisation de la séquence d'étalement de l'utilisateur concerné, dans le récepteur, avec celle de l'émetteur dans un environnement perturbé par les autres utilisateurs, cela afin de démoduler correctement les données utiles. Suivant la technique utilisée pour résoudre cette synchronisation, le récepteur sera plus ou moins complexe.

Parmi les méthodes permettant la synchronisation de l'émetteur et du récepteur, la meilleure est l'orthogonalité des séquences mais celle-ci n'est performante que dans le cas du S-CDMA. On s'intéresse donc à une autre méthode : la corrélation des séquences d'une même famille. Pour cela, définissons l'autocorrélation d'une séquence et l'intercorrélation de deux séquences.

Définition 12 Autocorrélation
Soit $(x_n)_n$ une séquence d'entiers naturels inférieurs strictement à m. L'autocorrélation, $\theta_{x,x}(l)$, est définie de la manière suivante :

$$\theta_{x,x}(l) = \frac{1}{P}\sum_{n=0}^{P-1} e^{\frac{i2\pi x_n}{m}} e^{-\frac{i2\pi x_{n+l}}{m}}. \tag{2.2}$$

Définition 13 Intercorrélation
Soient $(x_n)_n$ et $(y_n)_n$ deux séquences d'entiers naturels inférieurs strictement à m. L'intercorrélation, $\theta_{x,y}(l)$, est définie de la manière suivante :

$$\theta_{x,y}(l) = \frac{1}{P}\sum_{n=0}^{P-1} e^{\frac{i2\pi x_n}{m}} e^{-\frac{i2\pi y_{n+l}}{m}}. \tag{2.3}$$

La partie réelle de l'autocorrélation permet de synchroniser un émetteur donné avec le récepteur correspondant. Les valeurs prises par $\Re e(\theta_{x,y}(.))$ sont comprises entre -1 et 1.

Lorsque la valeur de $\Re e(\theta_{x,y}(.))$ est maximale pour un décalage l, c'est à dire $\Re e(\theta_{x,y}(l)) = \theta_{x,y}(l) = 1$, la séquence $(x_n)_n$ est une partie de la séquence $(y_n)_n$ sur les P termes considérés. Donc, au lieu de considérer deux séquences $(x_n)_n$ et $(y_n)_n$, nous considérons simplement la séquence $(x_n)_n$. Nous avons ainsi synchronisé notre émetteur et notre récepteur. En effet, en décalant la séquence du récepteur de l valeurs, nous retrouvons les mêmes valeurs que la séquence utilisée par l'émetteur, car ce décalage est un multiple de la période de la séquence considérée. Ce sont les pics de corrélation qui sont recherchés pour synchroniser chaque émetteur avec le récepteur correspondant.

Cependant, pour que cette méthode de synchronisation soit efficace, il est nécessaire que pour tout autre décalage l différent de la période de la séquence, cette autocorrélation soit la plus faible possible de telle manière que les pics de corrélation soient très facilement détectables. De plus, comme l'intercorrélation symbolise le BAM dû aux autres utilisateurs, ce bruit doit être le plus faible possible pour chaque intercorrélation, quel que soit le décalage l entre les deux séquences.

Ainsi, pour que les systèmes CDMA aient de bonnes performances, il est nécessaire de trouver une famille, $F = ((u_n^1)_n, (u_n^2)_n, \cdots, (u_n^k)_n)$ de séquences, de période T. Cette famille F doit être de cardinal k le plus grand possible tel que :

- $\forall i \in \{1,..,k\}, \quad \theta_{(u_n^i,u_n^i)}(0) = 1$ et $\forall l \;\; 0 < l < T, \quad |\theta_{(u_n^i,u_n^i)}(l)| \leq \varepsilon$;
- $\forall (i,j) \in \{1,..,k\}^2, \;\; i \neq j, \;\; \forall l \in \{0,\ldots,T\}, \quad |\theta_{(u_n^i,u_n^j)}(l)| \leq \varepsilon$

avec ε de l'ordre de 10^{-2} ou 10^{-3}.

Pour pouvoir utiliser au mieux les définitions précédentes d'auto et d'intercorrélation, nous schématisons le CDMA par les figures (2.7) et (2.8) qui représentent sa modélisation du point de vue respectivement de l'émetteur et du récepteur .

Le système étudié est un système fonctionnant bit à bit, de la manière suivante : chaque bit d'entrée noté $d_j(t)$ crée un déphasage $e^{i\pi d_j(t)}$ sur la porteuse du signal, de valeur 0 ou π, pendant une durée $T_b = N\ T_c$ (durée d'émission du bit). Ce signal déphasé sera ensuite émis mais en étant déphasé tous les T_c par une valeur de la séquence d'étalement de l'utilisateur, $e^{\frac{i2\pi y_j(l)}{m}}$.

Nous avons envisagé d'utiliser des déphasages car c'est un des moyens les plus appropriés pour utiliser la corrélation que nous avons définie précédemment car le système fonctionne en modulation de phases.

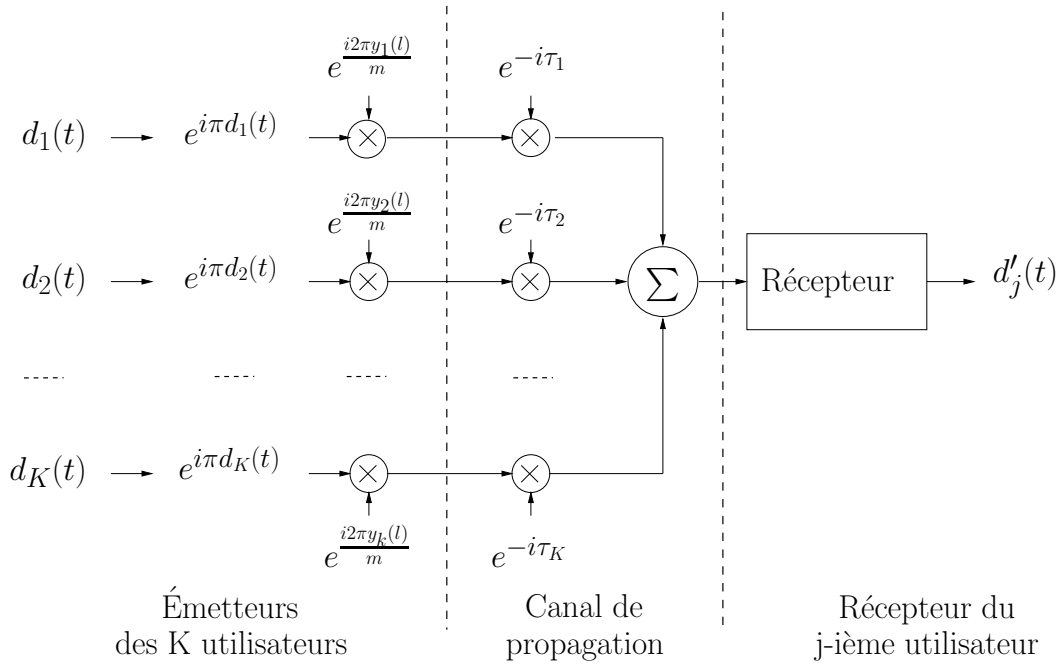


FIG. 2.7 – Modélisation du CDMA du point de vue de l'émetteur

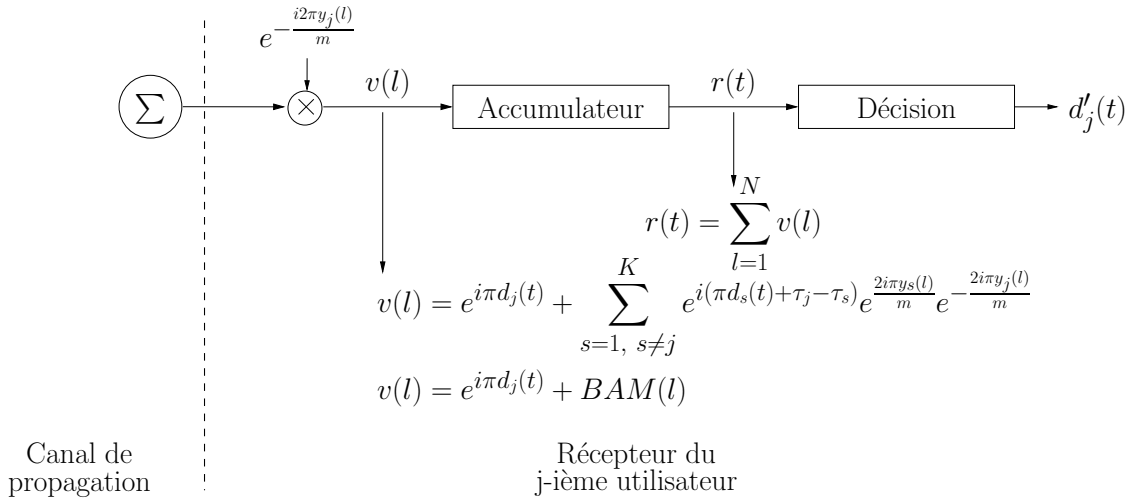


FIG. 2.8 – Modélisation du CDMA du point de vue du récepteur

A la réception, après synchronisation par exemple du récepteur de l'utilisateur numéro 1, nous appliquons la corrélation, multiplication par $e^{-\frac{i2\pi y_1(l)}{m}}$, aux données reçues, $\sum_{j=1}^{K} e^{i\pi d_j(t)} e^{\frac{i2\pi y_j(l)}{m}} e^{i(\tau_1-\tau_j)}$. Ainsi d'une part, nous avons le bit émis $e^{i\pi d_1(t)}$ et, d'autre part, nous avons l'intercorrélation

$$\sum_{j=2}^{K} e^{i(\pi d_j(t)+\tau_1-\tau_j)} e^{\frac{2i\pi y_j(l)}{m}} e^{-\frac{2i\pi y_1(l)}{m}},$$

que nous noterons par BAM pour Bruit d'Accès Multiple. Comme ce calcul s'effectue N fois, nous en faisons la somme. C'est ensuite l'organe de décision qui détermine, suivant le signe de la somme, si le bit émis est le bit 0 ou le bit 1.

Dans les chapitres suivants, nous montrerons que la séquence d'étalement de spectre de l'utilisateur peut être à déphasage multiple et qu'elle est plus performante que la séquence d'étalement classique. Nous déterminerons aussi que ce système peut fonctionner avec en entrée un bloc de bits au lieu de bit à bit. Nous montrerons enfin en utilisant un code correcteur d'erreur que le déphasage dû au bit d'entrée peut ne pas être constant durant le temps d'émission T_b et qu'il peut varier tous les T_c.

Chapitre 3

Étalement de spectre à déphasage multiple

Des séquences d'étalement de spectre multi-niveaux sont utilisées à la place des séquences d'étalement de spectre binaires pour faire de l'étalement de spectre mais aussi du CDMA dans [33, 34]. Dans le cadre de notre étude, ces séquences multi-niveaux sont des séquences à déphasage multiple puisqu'elles permettent différents déphasages sur la porteuse, le système fonctionnant en modulation de phase. L'utilisation de séquences d'étalement de spectre aléatoires à déphasage multiple est motivée par le fait qu'elles sont plus performantes du point de vue des simulations que les séquences aléatoires binaires.

Nous démontrons donc, dans ce chapitre, ce fait, sachant que le système utilisé est celui défini par les figures (2.7) et (2.8). Pour cela, nous nous sommes intéressés à la valeur moyenne du BAM ajoutée à chaque top d'horloge par le système.
Nous allons ainsi démontrer qu'en moyenne le BAM ajouté lors de l'utilisation de séquences aléatoires à déphasage multiple est plus petit que lors de l'utilisation de séquences aléatoires binaires.
Dans le cas d'un étalement de spectre *classique*, comme représenté en figure (2.3), nous avons une séquence aléatoire binaire de la forme $(e^{i\pi y_j})_{j\in\mathbb{N}}$ avec $y_j \in \{0, 1\}$.
Dans le cas d'un étalement de spectre *à déphasage multiple* à m états, $m > 2$, comme représenté en figure (3.1), nous avons une séquence aléatoire de symboles de la forme $(e^{\frac{2i\pi y_j}{m}})_{j\in\mathbb{N}}$, où $y_j \in \{0, \ldots, m-1\}$.

La figure (3.1) représente les différents déphasages successifs de la porteuse suivant le bit émis et les valeurs de la séquence d'étalement. Dans cette figure, la séquence d'étalement $\mathbf{y}$ est définie sur huit états et $\mathbf{y} = (3, 6, 7, 4, 1, 0, 2)$. Les déphasages successifs de la porteuse sont $\{\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_7\} = \{\frac{3\pi}{4}, -\frac{\pi}{2}, -\frac{\pi}{4}, \pi, \frac{\pi}{4}, 0, \frac{\pi}{2}\}$ si le bit émis est 0 et

$\{\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_7\} = \{-\frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}, 0, -\frac{3\pi}{4}, \pi, -\frac{\pi}{2}\}$ si le bit émis est 1. Nous constatons que les deux séquences de déphasage issues respectivement du bit émis 0 et 1 sont distinctes de π, pour chaque valeur de la séquence. Cela est dû au fait que le bit émis crée lui aussi un déphasage de 0 dans le cas d'émission du bit 0 et de π dans l'autre cas.

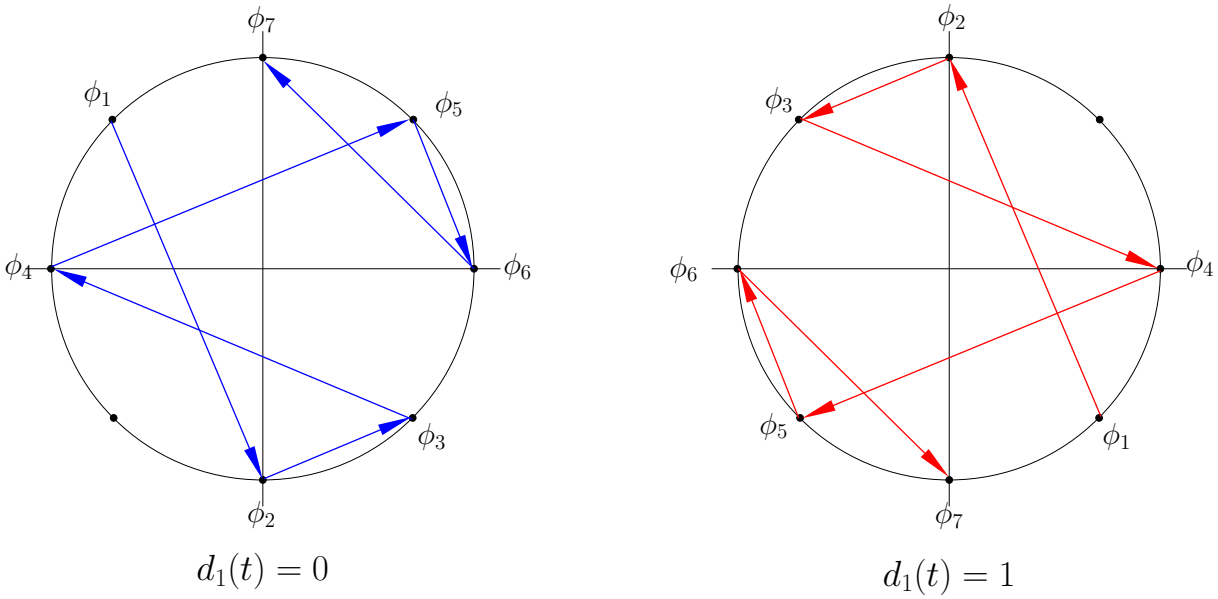


FIG. 3.1 – Étalement de spectre utilisant des séquences aléatoires à déphasage multiple suivant le bit émis, $\mathbf{y} = (3, 6, 7, 4, 1, 0, 2)$

3.1 Cas classique

Dans cette section, nous considérons le cas classique de l'étalement de spectre avec l'utilisation de séquences aléatoires binaires. Nous supposons de plus, que tous les utilisateurs sont synchronisés ou, tout du moins, que le décalage temporel est un multiple de T_c durée d'un bit de la séquence d'étalement d'un utilisateur. La séquence de l'utilisateur que nous observons est notée $(x_n)_n$, celles des utilisateurs perturbateurs $(y_n^p)_n$ et leurs bits d'information respectifs, d_x et d_{y^p}.

Dans un premier temps, nous allons calculer la valeur moyenne ajoutée par le BAM dans le cas d'un utilisateur perturbateur. Nous calculerons ensuite cette valeur moyenne ajoutée dans le cas de plusieurs utilisateurs perturbateurs.

3.1.1 Cas d'un utilisateur perturbateur

A l'instant l, en réception du canal de transmission après décorrélation nous avons la valeur $v(l)$ définie par :

$$v(l) = e^{i\pi d_x} + e^{i\pi y^1_{l+\tau}}\ e^{i\pi d_{y^1}}\ e^{-i\pi x_l}.$$

Nous nous intéressons à la valeur qui symbolise le BAM, générée ici par l'autre utilisateur : $e^{i\pi y^1_{l+\tau}}\ e^{-i\pi x_l}$. Nous allons regarder la valeur moyenne qui est ajoutée à chaque top d'horloge par le BAM. Notons X la variable aléatoire définie par $X = e^{i\pi y^1_{l+\tau}}\ e^{-i\pi x_l}$ qui correspond au BAM. Elle est équivalente à :

$$X = (-1)^\nu$$

où $\nu \in \{0, 1\}$ est une variable aléatoire, puisque y^1_n et x_n sont des variables aléatoires indépendantes.

Calculons l'espérance et la variance de cette variable aléatoire pour connaître la valeur moyenne ajoutée à chaque top d'horloge. L'espérance $E(X)$ nous est donnée par

$$E(X) = \sum_{\nu=0}^{1} p_\nu (-1)^\nu$$

où p_ν est la probabilité d'avoir la valeur $(-1)^\nu$. On a

$$p_0 = p_1 = \frac{1}{2}$$

car la variable X est le produit de deux séquences aléatoires uniformes, donnant donc une nouvelle séquence aléatoire. La probabilité des symboles est uniforme. Ainsi

$$E(X) = 0.$$

Considérons maintenant la variance de cette variable aléatoire :

$$\begin{aligned}
V(X) &= \sigma^2 \\
&= E((X - E(X))^2) \\
&= E(X^2) - E(X)^2 \\
&= E(X^2) \\
&= \sum_{\nu=0}^{1} p_\nu ((-1)^\nu)^2 \\
&= \sum_{\nu=0}^{1} p_\nu (-1)^{2\nu} \\
&= \sum_{\nu=0}^{1} p_\nu 1 \\
&= 1.
\end{aligned}$$

L'écart type, aussi appelé rayon moyen, est la racine carrée de la variance : c'est ce que nous ajoutons ou retranchons à l'espérance pour avoir la valeur moyenne qu'un *utilisateur perturbateur* ajoute à chaque top d'horloge. Dans notre cas, la valeur moyenne ajoutée par un *utilisateur perturbateur*, notée Ω_1^b, est égale à

$$\Omega_1^b = E(X) \pm \sqrt{V(X)} = 0 \pm 1 = \pm 1.$$

Cette valeur moyenne peut être améliorée dans le cas d'un étalement de spectre à déphasage multiple.

3.1.2 Cas de plusieurs utilisateurs perturbateurs

Considérons le cas où nous avons p *utilisateurs perturbateurs*, $p \in \mathbb{N} \setminus \{0, 1\}$. Nous avons, en réception de canal, à l'instant l après décorrélation

$$v(l) = e^{i\pi d_x} + \sum_{k=1}^{p} e^{i\pi y_{l+\tau}^k} e^{-i\pi x_l} e^{i\pi d_{y^k}}.$$

Intéressons-nous à la variable aléatoire (X_p) définie par

$$\begin{aligned} X_p &= \sum_{k=1}^{p} e^{-i\pi x_l} e^{i\pi y_{l+\tau}^k} \\ &= \sum_{k=1}^{p} (-1)^{-x_l} (-1)^{y_{l+\tau}^k} \\ &= \sum_{k=1}^{p} (-1)^{x_l} (-1)^{y_{l+\tau}^k} \end{aligned}$$

où $x_l, y_{l+\tau}^1, ..., y_{l+\tau}^p \in \{0, 1\}$. Notons $H(t)$ la variable aléatoire $H(t) = (-1)^t$ où $t \in \{0, 1\}$. Les séquences $x, y^1, \ldots, y^p$ sont indépendantes car aléatoires. Les variables aléatoires $H(x)$ et $H(y_{l+\tau}^i)$, pour $i = 1, \ldots, p$, le sont donc aussi. Calculons comme précédemment l'espérance et la variance de X_p.

$$\begin{aligned} E(X_p) &= E(\sum_{k=1}^{p} H(x) H(y_{l+\tau}^k)) \\ &= \sum_{k=1}^{p} E(H(x) H(y_{l+\tau}^k)) \\ &= \sum_{k=1}^{p} E(H(x)) E(H(y_{l+\tau}^k)) \\ &= 0. \end{aligned}$$

En effet $E(H(x)) = E(H(y_i)) = 0$.
Calculons la variance :

$$\begin{aligned} V(X_p) &= E((X_p - E(X_p))^2) \\ &= E(X_p^2) = E\left((\sum_{k=1}^{p} H(x)H(y_k))^2\right) \\ &= \underbrace{\sum_{k=1}^{p} E((H(x)H(y_k))^2)}_{p} - \underbrace{2\sum_{1\leq i<j\leq p} cov(H(x)H(y_i), H(x)H(y_j))}_{0} \\ &= p. \end{aligned}$$

On en déduit que la valeur moyenne notée Ω_p^b ajoutée par p *utilisateurs perturbateurs* est égale à

$$\Omega_p^b = E(X_p) \pm \sqrt{V(X_p)} = 0 \pm \sqrt{p} = \pm\sqrt{p}.$$

Ainsi, dans le cas d'un étalement de spectre utilisant des séquences d'étalement aléatoires binaires, la valeur moyenne du BAM ajoutée par p utilisateurs perturbateurs est égale à $\Omega_p^b = \pm\sqrt{p}$.

Nous allons ci-après montrer que, dans le cas où les séquences d'étalement aléatoires binaires sont remplacées par des séquences aléatoires à déphasage multiple, la valeur moyenne est divisée par un facteur $\sqrt{2}$.

3.2 Cas du déphasage multiple

Dans le cas d'un étalement de spectre à déphasage multiple, nous n'imposons aucune condition sur la synchronisation des utilisateurs. Ainsi, seule la partie réelle de notre corrélation nous intéresse, car le système ne fonctionne que bit à bit et la partie imaginaire n'apporte pas d'information sur le bit émis.
On définit le nombre d'états m par $m = 2^r$ où $r \in \mathbb{N} \setminus \{0, 1\}$.
Nous allons tout d'abord calculer la valeur moyenne ajoutée par le BAM dans le cas d'un utilisateur perturbateur. Puis nous calculerons la valeur moyenne ajoutée dans le cas de plusieurs utilisateurs perturbateurs.

3.2.1 Cas d'un utilisateur perturbateur

En réception et après synchronisation, nous avons à l'instant l :

$$v(l) = e^{i\pi d_x} + e^{\frac{2i\pi y_l^1}{2^r}} e^{-\frac{2i\pi x_l}{2^r}} e^{-i\tau_{y_1}} e^{i\pi d_{y^1}}$$

où τ_{y_1} est le déphasage de *l'utilisateur perturbateur.*
Considérons la variable aléatoire Y définie par

$$Y = \Re e\left(e^{\frac{2i\pi y_l^1}{2^r}} e^{-\frac{2i\pi x_l}{2^r}} e^{-i\tau_{y_1}}\right).$$

Nous remarquons qu'elle prend ses valeurs sur le cercle complexe de rayon 1. En effet, les déphasages des deux utilisateurs sont sur le cercle unité, et le retard d'émission τ_{y_1} entre les deux utilisateurs est lui aussi sur ce cercle. De plus, ce retard τ_{y_1} est une variable aléatoire continue uniforme sur le cercle unité. Ainsi, après simplification, on obtient

$$Y = cos(\theta)$$

où θ est une variable aléatoire uniforme sur $[0, 2\pi]$. En effet, cette dernière est la composée de deux variables aléatoires discrètes, x_l et y_l^1, et d'une variable aléatoire continue uniforme, τ_{y_1}, de fonction de répartition f définie par

$$f(\theta) = \begin{cases} \frac{1}{2\pi} & \text{pour } \theta \in [0, 2\pi] \\ 0 & \text{sinon.} \end{cases}$$

La variable aléatoire Y a donc pour fonction de répartition la fonction g définie par

$$g(y) = \begin{cases} \frac{1}{\pi}\frac{1}{\sqrt{1-y^2}} & \text{pour } y \in [-1, 1] \\ 0 & \text{sinon.} \end{cases}$$

Calculons l'espérance et la variance de la variable aléatoire Y :

$$\begin{aligned} E(Y) &= \int_{-\infty}^{+\infty} yg(y)dy \\ &= \int_{-1}^{1} y\frac{1}{\pi}\frac{1}{\sqrt{1-y^2}}dy \\ &= [-\frac{1}{2\pi}\sqrt{1-y^2}]_{-1}^{1} \\ &= 0, \end{aligned}$$

et

$$\begin{aligned} V(Y) &= \int_{-\infty}^{+\infty} y^2 g(y)dy \\ &= \int_{-1}^{1} \frac{1}{\pi}\frac{y^2}{\sqrt{1-y^2}}dy \\ &= \left[-\frac{1}{2\pi}\sqrt{1-y^2} + \frac{1}{2\pi}\arcsin(y)\right]_{-1}^{1} \\ &= \frac{1}{2}. \end{aligned}$$

La valeur moyenne notée Ω_1^m ajoutée par un *utilisateur perturbateur* est égale à

$$\Omega_1^m = E(Y) \pm \sqrt{V(Y)} = 0 \pm \frac{1}{\sqrt{2}} = \pm\frac{1}{\sqrt{2}}.$$

Nous remarquons que cette valeur moyenne Ω_1^m est plus petite que la valeur moyenne Ω_1^b. Ainsi la valeur moyenne notée r_{multi} en sortie de l'accumulateur est égale à

$$\begin{aligned} r_{multi} &= \sum_{l=1}^{N} v(l) \\ &= \sum_{l=1}^{N} \left(e^{i\pi d_x} + e^{\frac{2i\pi y_l^1}{2^r}} e^{-\frac{2i\pi x_l}{2^r}} e^{-i\tau_{y_1}} e^{i\pi d_{y^1}} \right) \\ &= N e^{i\pi d_x} + \sum_{l=1}^{N} \left(e^{\frac{2i\pi y_l^1}{2^r}} e^{-\frac{2i\pi x_l}{2^r}} e^{-i\tau_{y_1}} e^{i\pi d_{y^1}} \right) \\ &= N e^{i\pi d_x} + \sum_{l=1}^{N} \pm\frac{1}{\sqrt{2}}. \end{aligned}$$

La valeur moyenne de sortie notée r_{bin} de l'accumulateur dans le cas de l'utilisation de séquences aléatoires binaires est égale à :

$$r_{bin} = N e^{i\pi d_x} + \sum_{l=1}^{N} \pm 1.$$

C'est suivant cette valeur, en sortie de l'accumulateur, que l'organe de décision décide du bit supposé émis. Supposons que le bit émis soit le bit 0. Nous avons alors

$$r_{multi} = N + \sum_{l=1}^{N} \pm\frac{1}{\sqrt{2}}$$

et

$$r_{bin} = N + \sum_{l=1}^{N} \pm 1.$$

Pour que la décision se fasse sur le bit 0, il faut que la somme, r_{multi} ou r_{bin}, soit positive. Or la valeur r_{bin} peut être positive ou nulle tandis que la valeur r_{multi} est toujours positive. En effet, dans le pire des cas envisageables, on soustrait la valeur moyenne à chaque étape, ainsi r_{multi} a pour valeur

$$r_{multi} = N - \sum_{l=1}^{N} \frac{1}{\sqrt{2}} = N(1 - \frac{\sqrt{2}}{2}) > 0,$$

tandis que r_{bin} a pour valeur

$$r_{bin} = N - \sum_{l=1}^{N} 1 = 0.$$

Si la valeur reçue par l'organe de décision est zéro alors celui-ci est dans l'impossibilité de décider. En effet, la valeur 0 se trouve à la même distance de la valeur 1 que de -1, symbolisant respectivement les bits 0 et 1. Il y a donc la même probabilité que ce soit le bit 0 que le bit 1 qui soit émis. Dans ces conditions, la décision est fausse une fois sur deux en moyenne. Ainsi, lorsque nous sommes dans le pire des cas, seul l'étalement à déphasage multiple permet de retrouver le bit émis avec une probabilité de 1, tandis que dans le cas classique, cette probabilité n'est que de 0,5.

Ainsi l'utilisation de séquences d'étalement aléatoires à déphasage multiple rend le système plus performant en terme de TEB par rapport à l'utilisation de séquences d'étalement aléatoires binaires.

3.2.2 Cas de plusieurs utilisateurs perturbateurs

Considérons maintenant le cas où nous avons p *utilisateurs perturbateurs*, $p \in \mathbb{N} \setminus \{0, 1\}$. Après décorrélation, à l'instant l nous avons en réception de canal,

$$v(l) = e^{i\pi d_x} + \sum_{k=1}^{p} e^{-i\frac{\pi x_l}{2^r}} e^{i\frac{\pi y_l^k}{2^r}} e^{-i\tau_k} e^{i\pi d_{y^k}}.$$

Comme précédemment, définissons la variable aléatoire Y_p par

$$\begin{aligned} Y_p &= \Re e\left(\sum_{k=1}^{p} e^{-i\frac{\pi x_l}{2^r}} e^{i\frac{\pi y_l^k}{2^r}} e^{-i\tau_k}\right) \\ &= \sum_{k=1}^{p} \Re e\left(e^{-i\frac{\pi x_l}{2^r}} e^{i\frac{\pi y_l^k}{2^r}} e^{-i\tau_k}\right) \\ &= \sum_{k=1}^{p} \cos(\theta_k) \end{aligned}$$

nous posons $\cos(\theta_k) = \Re e\left(e^{-i\frac{\pi x_l}{2^r}} e^{i\frac{\pi y_l^k}{2^r}} e^{-i\tau_k}\right)$ pour les mêmes raisons que dans le cas d'un utilisateur perturbateur. Les variables $\theta_1, .., \theta_p \in [0, 2\pi]$ sont des variables aléatoires continues uniformes indépendantes. Ce sont des séquences aléatoires, car composées des séquences aléatoires $x, y^1, \ldots, y^p$. Les variables aléatoires $\cos(\theta_i)$ sont aussi des variables aléatoires continues uni-

formes indépendantes. Calculons comme précédemment l'espérance de Y_p :

$$\begin{aligned} E(Y_p) &= E(\sum_{k=1}^{p} \cos(\theta_k)) \\ &= \sum_{k=1}^{p} E(\cos(\theta_k)) \\ &= 0. \end{aligned}$$

Calculons maintenant la variance de Y_p :

$$\begin{aligned} V(Y_p) &= E((Y_p - E(Y_p))^2) \\ &= E(Y_p^2) = E((\sum_{k=1}^{p} cos(\theta_k))^2) \\ &= \underbrace{\sum_{k=1}^{p} E((\cos(\theta_k))^2)}_{\frac{p}{2}} - \underbrace{2 \sum_{1 \leq i < j \leq p} cov(\cos(\theta_i), \cos(\theta_j))}_{0} \\ &= \frac{p}{2}. \end{aligned}$$

La valeur moyenne notée Ω_p^m ajoutée par p *utilisateurs perturbateurs* est égale à

$$\Omega_p^m = E(Y_p) \pm \sqrt{V(Y_p)} = 0 \pm \sqrt{\frac{p}{2}} = \pm\sqrt{\frac{p}{2}}.$$

Comme nous venons de le montrer dans la section précédente, les séquences d'étalement aléatoires à déphasage multiple rendent le système plus performant en terme de TEB. Remarquons que le nombre d'états de ces séquences n'apporte en revanche aucune amélioration. Cela est dû au simple fait que lorsque l'on utilise des séquences aléatoires binaires, les deux états utilisés sont réels, tandis que dans le cas de séquences aléatoires à déphasage multiple, les valeurs sont complexes et seule la partie réelle nous intéresse.

La figure (3.2) représente le TEB en fonction du nombre d'utilisateurs pour différentes séquences d'étalement. Nous remarquons que les séquences aléatoires à déphasage multiple dans le cas asynchrone sont plus performantes que les séquences de Gold, aussi bien dans le cas synchrone que dans le cas asynchrone. Pourtant ces dernières, comme nous l'avons décrit dans le chapitre 1, ont de très bonnes propriétés de corrélation. Toutefois, l'utilisation que nous pouvons en faire est réduite. En effet, ces propriétés ne sont vérifiées que dans le cas où les deux séquences sont synchrones. Dans le cas asynchrone, ces propriétés sont fortement dégradées. De plus, les séquences aléatoires à déphasage multiple sont meilleures que les séquences de Gold. Nous remarquons que les

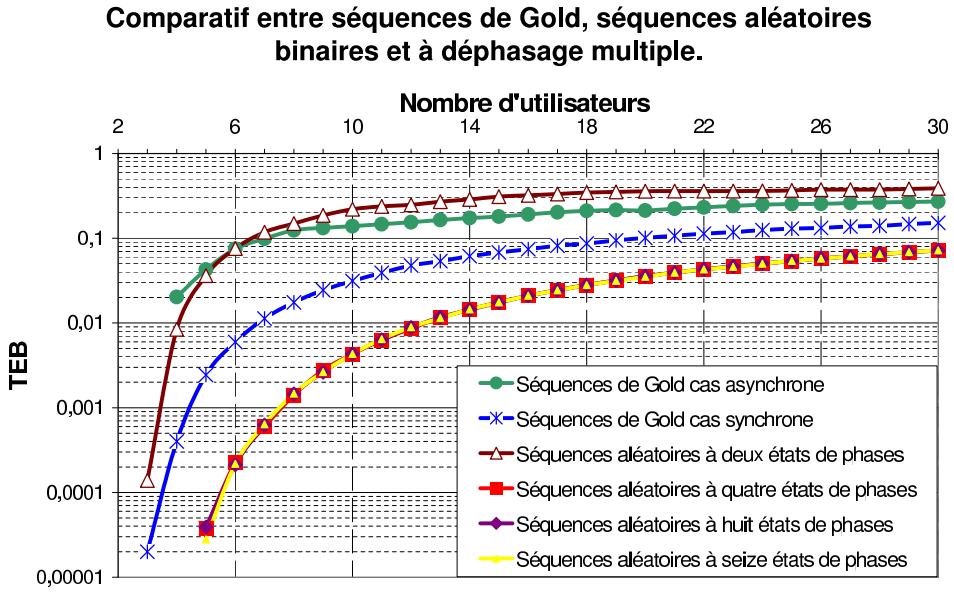


FIG. 3.2 – TEB fonction du nombre d'utilisateurs et des séquences d'étalement utilisées

courbes des séquences d'étalement aléatoires à déphasage multiple à 4, 8 et 16 états sont confondues : comme nous l'avions déjà dit, le nombre d'états n'intervient pas dans l'amélioration du TEB. Pour un TEB de 10^{-3}, le gain entre séquences de Gold et séquences aléatoires à déphasage multiple est de 3 utilisateurs, ce qui n'est pas négligeable sachant que le nombre maximum d'utilisateurs pour les séquences aléatoires à déphasage multiple est de 7.

Dorénavant, lorsque nous ferons référence aux séquences d'étalement, ce sera aux séquences d'étalement aléatoires à déphasage multiple.

Chapitre 4

Étalement de spectre, cryptographie et information cachée

Ce chapitre a fait l'objet d'une publication [35] qui fut présentée à International Workshop on Algebraic and Combinatorial Coding Theory (ACCT) en Juin 2004.

Comme nous l'avons vu dans le chapitre 2, l'étalement de spectre est une méthode de communication bien connue. Elle utilise une large bande de fréquence et une faible densité de puissance pour transmettre le signal. L'intérêt le plus important de cette méthode est de transformer le bruit non-gaussien ambiant en bruit blanc gaussien.

Sans la connaissance de l'existence d'une communication par étalement de spectre, il n'est pas facile de détecter celle-ci. C'est pour cette raison que certaines communications sont souvent considérées comme cachées. Comme nous venons de le voir, l'étalement de spectre utilise des séquences pseudo-aléatoires périodiques ayant de bonnes propriétés de corrélation, telles que les séquences de Gold (voir chapitre 1), etc, voir aussi [1, 23]. Comme nous l'avons vu dans les chapitres 1 et 2, ces propriétés sont utilisées pour détecter et synchroniser la communication entre l'émetteur et le récepteur. Ainsi, pour détecter et retrouver le message, la fréquence de la porteuse de la communication doit être connue et la corrélation doit être faite avec toutes les séquences potentiellement utilisables avec différents décalages, cela afin de déterminer la bonne séquence et de permettre ensuite la synchronisation.

Dans ce chapitre, nous proposons de remplacer la séquence d'étalement par une séquence pseudo-aléatoire notée PNS, cryptographiquement sûre, verifiant au moins les tests présentés en [36] et [37]. Cette communication n'est pas seulement cachée (car difficile à détecter), mais cryptographiquement sûre. En effet, même si quelqu'un connaît l'existence de cette communication, cette

personne ne peut pas retrouver le message clair si elle ne connaît pas la séquence PNS.

Toutefois, l'utilisation d'une séquence PNS entraîne des difficultés importantes pour la synchronisation. En effet, cette séquence est soit apériodique, soit périodique avec une très grande période, beaucoup plus grande que le facteur d'étalement utilisé. Ainsi cette séquence ne peut pas être utilisée pour synchroniser la communication et maintenir cette synchronisation. C'est pour cette raison que nous préconisons l'utilisation d'une autre communication, dite publique, pour résoudre ce problème. Le message caché est considéré comme une légère altération de la transmission publique.

Dans la première section de ce chapitre, nous reparlerons brièvement du principe de l'étalement de spectre. Nous expliquerons ensuite comment utiliser une séquence PNS pour chiffrer le message. Enfin, dans la troisième section nous décrirons comment utiliser une communication QPSK classique avec message pour cacher et synchroniser la communication secrète avec message secret. Cette dernière section sera accompagnée de résultats de simulations pour montrer que cette méthode est effective.

4.1 Principe de l'étalement de spectre

Comme défini précédemment, la technique de l'étalement de spectre par séquence directe prend un bit de la séquence de données, en entrée, et le multiplie par une séquence pseudo-aléatoire binaire à un rythme très supérieur à celui des données à transmettre.

Si T_b est la durée d'émission d'un bit de donnée, la forme d'onde des données est alors $d(t) = d_n$ avec $nT_b \leq t < (n+1)T_b$ et $d_n \in \{1, -1\}$, où (d_n) est la séquence de donnée binaire (par commodité $d_n \in \{1, -1\}$ au lieu de $\{0, 1\}$).

Soit T_c la durée d'un chip, qui est la durée de vie d'un bit de la séquence pseudo-aléatoire binaire PN. Pour les applications pratiques, les horloges des données et de la séquence PN doivent être synchronisées. Plus précisément, la durée d'émission d'un bit T_b est un multiple de la durée d'un chip T_c. Le rapport $N = T_b/T_c$ est défini comme le facteur d'étalement.

La figure (4.1) présente le résultat de l'étalement de spectre de la séquence de données $(d_n) = (1, -1, -1)$, par la séquence d'étalement PN $(1, -1, -1, 1, -1, 1, 1, -1)$, de facteur d'étalement $N = 8$.

Pour simplifier le principe, considérons la séquence de données $D = (d_t)$ transmise avec une durée d'émission de bits égale à T_b comme la séquence de données $D' = (d'_t)$ transmise avec une durée d'émission de bit égale à T_c. La séquence D' est obtenue à partir de la séquence D en répétant chaque bit de cette dernière N fois. Les données transmises sont alors $C = D' \times PN$ au temps chip T_c.

Afin d'obtenir le message original, D, le récepteur multiplie C par la séquence PN pour retrouver D'. La séquence D, quant à elle, est retrouvée à partir de D' par vote majoritaire.

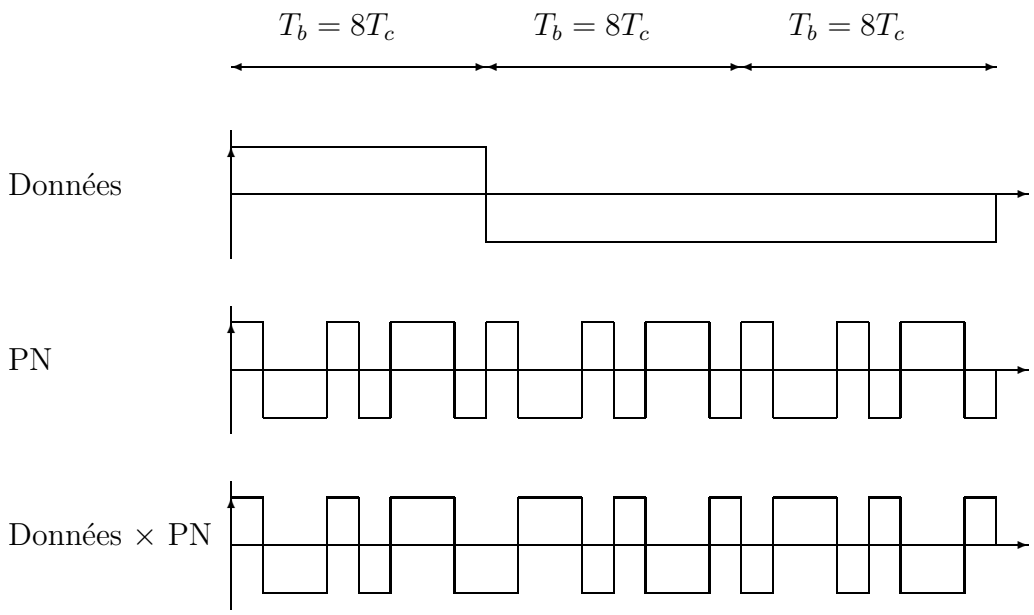


FIG. 4.1 – Principe de l'étalement de spectre par séquences directes

L'étalement de spectre a beaucoup d'avantages, voir [23] et chapitre 2. La bande de fréquence est notamment plus large mais avec une densité spectrale de puissance plus faible que celle d'une communication classique. Le signal est plus résistant aux interférences, et après multiplication par la séquence PN, celles-ci se comportent comme un bruit blanc gaussien. La densité spectrale de puissance de l'étalement de spectre est en dessous du niveau de bruit. Nous pouvons constater tout cela sur la figure (4.2). Sous ces conditions, le signal est difficile à détecter sans la multiplication par la séquence PN.

Un autre avantage de l'étalement de spectre est qu'il peut être utilisé dans un espace ambiant très bruité, c'est à dire avec un rapport signal à bruit faible, en augmentant la valeur du facteur d'étalement N. Le signal peut devenir indétectable si la séquence PN n'est pas connue pour calculer l'intercorrélation.

4.2 L'étalement de spectre utilisé en cryptographie

La cryptographie symétrique est axée essentiellement sur deux méthodes : le chiffrement par bloc et le chiffrement par flot. Dans cette section, nous nous intéressons au second type de chiffrement. En effet, ce dernier est le plus propice pour l'étalement de spectre. Le principe du chiffrement par flot est

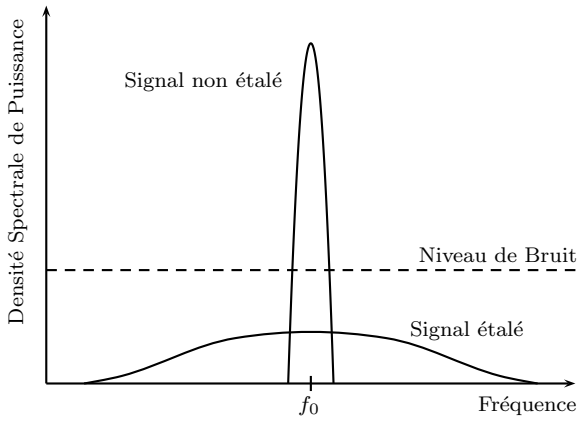


FIG. 4.2 – Densité spectrale de puissance d'une communication classique et d'une communication par étalement de spectre.

très simple : un symbole aléatoire k_t est ajouté modulo 2 à chaque symbole de données d_t, $d_t \in \{0, 1\}$.

Message : $M = (d_t)_{t=1}^n$.
Clé secrète partagée : $K = (k_t)_{t=1}^n$.
Cryptogramme : $C = (d_t \oplus k_t)_{t=1}^n$.

Pour retrouver le message initial, le récepteur calcule $C \oplus K$.

Si la clé secrète est choisie aléatoirement et utilisée une seule fois, cette méthode est inconditionnellement sûre. C'est la méthode du masque jetable (One time pad method) [38]. Pour des applications pratiques, il n'est pas possible d'utiliser une clé ayant la même taille que le message. Ainsi la séquence aléatoire K est remplacée par une séquence issue d'un générateur pseudo-aléatoire initialisé par une petite clé.

Au lieu d'ajouter une séquence pseudo-aléatoire ayant de bonnes propriétés cryptographiques, [36, 37], notée PNS aux données avant la transmission, nous proposons d'utiliser directement la séquence PNS comme séquence d'étalement. Elle remplace ainsi la séquence PN utilisée habituellement qui a de bonnes propriétés de corrélation. Remarquons aussi que dans le principe cryptographique proposé précédemment, nous utilisons l'opération $\oplus$ dans le cas où les bits sont à valeurs dans $\{0, 1\}$. Dans le cas où ils seraient à valeurs dans $\{1, -1\}$, nous utilisons l'opération $\times$, qui correspond au produit utilisé dans l'étalement de spectre.

Une telle méthode est théoriquement aussi sûre que la précédente. Dans notre cas, supposons que nous voulions transmettre le message $M = (d_t)$ avec un facteur d'étalement $N = T_b/T_c$ et la séquence PNS notée $S = (s_t)$. Du fait de la différence entre les temps d'émission des bits de données et les temps des bits de la séquence PNS, notre méthode consiste à ajouter la séquence S au message $M' = (d'_t)$, où M' est le message M avec N répétitions de chaque bit

$(d'_t = d_{\lceil t/N \rceil})$. Le cryptogramme est donc

$$C' = M' \oplus S.$$

Nous venons de construire une communication chiffrée qui est cachée dans le bruit ambiant et nous avons aussi atteint notre objectif. En effet, la séquence S sert à la réception pour synchroniser le récepteur avec l'émetteur par l'intermédiaire d'un calcul de corrélation. Or, comme nous le savons, l'énergie du signal étalé est plus petite que l'énergie du bruit ambiant. Il est donc impossible de retrouver le cryptogramme $C' = M' \oplus S$ sans la connaissance de la séquence S.

Toutefois, pour une application pratique, il existe quelques problèmes de synchronisation si on utilise la séquence PNS. En effet, les séquences PN classiques utilisées dans l'étalement de spectre sont des séquences de périodes très courtes et répétées autant de fois que nécessaire. De plus, ces séquences PN ont de bonnes propriétés de corrélation. Ces propriétés et le fait qu'elles soient périodiques, permettent de synchroniser la transmission en cherchant le pic de corrélation. Or, dans le cas des séquences PNS, qui sont des séquences PN ayant de bonnes propriétés cryptographiques, cette méthode de synchronisation n'est plus possible car les séquences PNS n'ont pas les mêmes propriétés de corrélation que les séquences PN. Et même si la séquence PNS est périodique, la synchronisation ne peut se faire, car la période de la séquence est très grande et pratiquement hors d'intérêt. Nous verrons dans la section suivante comment pallier cet inconvénient.

4.3 Information cachée dans une communication QPSK

Généralement, en cryptographie, le fait qu'un cryptogramme soit envoyé ne constitue pas un secret. Dans la situation qui nous intéresse, les avantages obtenus en utilisant notre technique de chiffrement par flot, directement sur le mécanisme de l'étalement de spectre, ne sont pas aussi clairement définis que dans le cas d'une utilisation classique. En effet, notre transmission, en plus d'être chiffrée, est indétectable sans la connaissance de la séquence d'étalement qui est aussi la clé secrète du schéma de chiffrement. Toutefois, pour quelques applications particulières, il est intéressant d'avoir non seulement une sécurité cryptographique, mais aussi de cacher la transmission du secret, d'où l'intérêt de notre méthode.

Ainsi, la première méthode naturelle consiste à employer notre système avec un grand facteur d'étalement N pour masquer le message à l'intérieur du bruit ambiant. En effet, plus le facteur d'étalement N est grand, plus la bande de fréquence est conséquente et l'amplitude maximale de la densité spectrale de puissance en est d'autant plus faible. Cependant, le problème

de synchronisation n'est pas résolu, comme nous l'avons noté dans la section précédente.

Une deuxième solution consiste à masquer la transmission secrète, utilisant l'étalement de spectre, avec une communication classique sans importance. Le signal secret est alors synchronisé avec la communication classique. Cette méthode est plus robuste que la stéganographie classique, voir [39], puisque même si le signal secret est détecté, il n'est pas possible de récupérer le message secret initial sans connaissance de la séquence PNS.

Comme premier exemple d'application, considérons une transmission classique BPSK. Soit $D = (D_n)$, le message de la communication non-secrète ($D_n \in \{0,1\}$). La forme d'onde du signal transmis est $\Phi(t) = A cos\,(\omega t + D(t)\pi)$ où A est l'amplitude, $1/\omega$ est la fréquence du signal et $D(t) = D_n$ avec $n = \lfloor t/T_b \rfloor$ et T_b la durée d'émission d'un bit du message. Le message caché est $m = (d_n)$, $d_n \in \{0,1\}$ transmis avec l'amplitude a, au temps chip T_c, un diviseur de T_b. Le temps d'émission de chaque bit de cette transmission t_b est un multiple de T_b. La séquence pseudo-aléatoire PNS est notée (k_n), $k_n \in \{0,1\}$. Soit $\phi(t) = a cos\,(\omega t + (m(t) + k(t))\pi)$ la forme d'onde de la communication secrète, avec $m(t) = d_n$ et $n = \lfloor t/t_b \rfloor$ et $k(t) = k_{n'}$ avec $n' = \lfloor t/T_c \rfloor$.

La forme de cette transmission est alors $\Phi(t) + \phi(t)$ avec $a \ll A$.

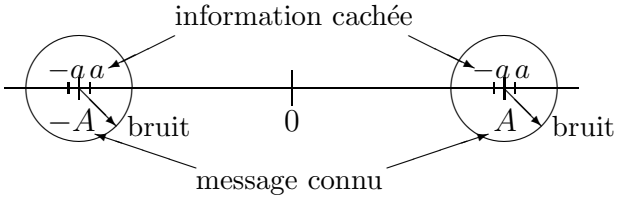
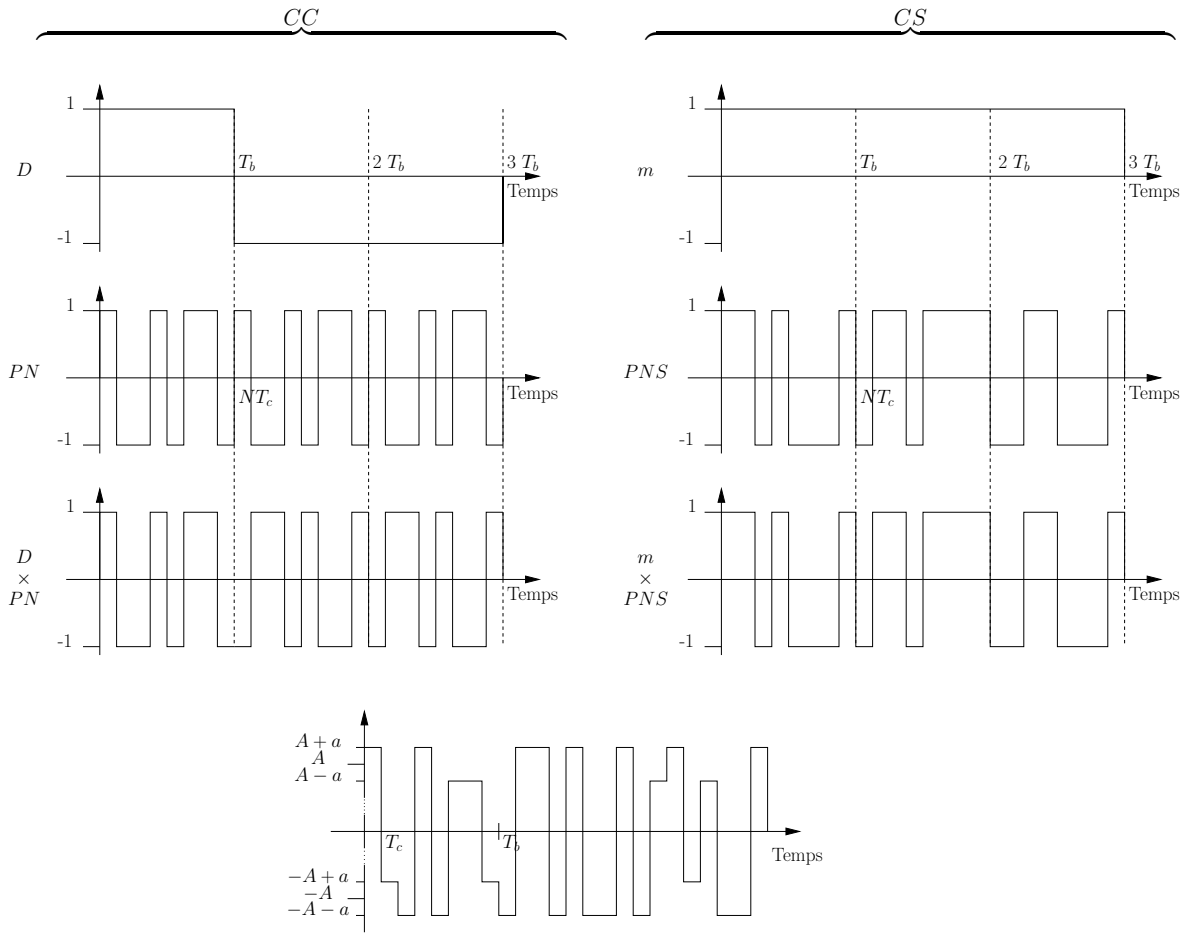


FIG. 4.3 – Diagramme de Fresnel de la transmission

Les figures (4.3) et (4.4) représentent respectivement ce principe dans le diagramme de Fresnel et dans le domaine temporel. Dans la figure (4.4), trois diagrammes temporels sont représentés. Le premier noté CC représente celui de la communication classique qui dans ce cas est une communication par étalement de spectre. Le second noté CS représente celui de la communication secrète. Le troisième est l'addition des deux diagrammes précédents mais avec une amplitude différente. Dans le cas de la communication CC, le message transmis est $D = (1,-1,-1)$ de durée $T_b = 8T_c$. Le facteur d'étalement a donc pour valeur $N_{CC} = 8$ et la séquence d'étalement PN est

$$(1,-1,-1,1,-1,1,1,-1).$$

Pour la communication secrète CS, le message transmis est $m = (1)$ de durée $t_b = 3T_b = 24T_c$, le facteur d'étalement a pour valeur $N_{CS} = 24$ et la séquence



Message transmis $A \times CC + a \times CS$ avec $a \ll A$

FIG. 4.4 – Diagramme de la transmission dans le domaine temporel

d'étalement PNS est

$$(1, 1, -1, 1, -1, -1, -1, 1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, -1, -1, 1).$$

Le récepteur utilise la séquence d'étalement de la communication classique pour la synchroniser. Une fois le message D récupéré, on retrouve le signal $\phi(t)$ en soustrayant le signal reçu par le signal classique supposé émis. Le message secret est ensuite retrouvé en utilisant les méthodes classiques de l'étalement de spectre puisque les deux communications sont synchronisées grâce à la communication classique.

Notons que le message secret est plus petit que le niveau de bruit et n'est pas détectable si la séquence PNS n'est pas utilisée pour calculer la corrélation.

Pour un observateur extérieur, la transmission classique ressemble à une transmission BPSK mais avec de légères perturbations d'amplitude, ce que nous pouvons constater sur le troisième diagramme de la figure (4.4). En effet, le signal transmis est de la forme

$$\Phi(t) = (A \pm \epsilon(t))cos\,(\omega t + D(t)\pi)$$

avec $0 \leq \epsilon(t) \leq a$.

Cependant, dans cette méthode, si une erreur se produit sur un symbole du message D, elle induit un bruit très élevé sur T_b/T_c chips. Ceci peut conduire à introduire quelques erreurs sur le message secret m.

Pour éviter un tel problème, il est possible d'utiliser un signal QPSK qui ressemble à un signal BPSK : le message D est émis sur la phase (voie I) et le message secret m sur la quadrature (voie Q), avec toujours la condition $a \ll A$.

Avec les notations ci-dessus, le message transmis est alors $\Phi(t) + \phi(t)$, où $\Phi(t) = Acos\,(\omega t + D(t)\pi)$ et $\phi(t) = asin\,(\omega t + (m(t) + k(t))\pi)$. Ainsi la transmission classique se situe sur la partie réelle du signal tandis que le signal secret se situe sur la partie imaginaire. La figure (4.5) représente le principe de cette méthode.

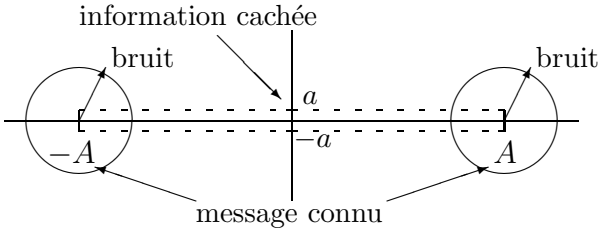


FIG. 4.5 – Diagramme de Fresnel de la transmission complexe

Puisque le signal secret est orthogonal au signal non secret, une erreur sur le message connu n'induit pas d'erreur sur le message secret. Le signal caché peut être récupéré directement sans soustraction du message original comme précédemment. La communication non secrète sert ici uniquement pour la

synchronisation et ne perturbe pas la transmission secrète comme c'est le cas pour la première méthode.

De plus, pour un observateur extérieur, cette transmission ressemble à un signal BPSK classique mais avec de légères perturbations de phases. En effet, le signal résultant est de la forme

$$\Phi'(t) = Acos\left(\omega t + D(t)\pi \pm \epsilon(t)\right)$$

avec $\epsilon(t) \simeq a/A$.

Résultats de nos simulations

Nous donnons maintenant quelques résultats de nos simulations. La différence entre les deux méthodes n'est pas significative, puisque très peu d'erreurs se produisent sur le message connu.

Le message connu est envoyé en utilisant la méthode classique d'étalement de spectre avec le facteur $N_{CC} = T_b/T_c$ et l'amplitude A. Le message secret est envoyé avec un facteur d'étalement de spectre $N_{CS} = t_b/T_c$ et d'amplitude a. L'amplitude de bruit est B. Les taux d'erreur binaire du message connu et caché (quelle que soit la méthode présentée) sont respectivement notés TEB et *teb*.

L'amplitude B du bruit n'est pas fixée par l'utilisateur. L'amplitude A du message non-secret et le facteur N_{CC} sont fixés simultanément pour pouvoir récupérer ce message avec un TEB choisi. Dans notre exemple, nous choisissons pour le signal non-secret, utilisé pour la synchronisation, les paramètres suivants $N_{CC} = 32$ $B/A = 50\%$ et $TEB \leq 10^{-6}$ et nous regardons le TEB de la communication secrète ainsi que la manière dont elle se comporte par rapport à la communication classique et au bruit ambiant. De plus, nous ne parlons pas ici de l'utilisation d'un code correcteur d'erreurs pour diminuer le TEB du signal secret.

N_{CS}/N_{CC}	a/A	a/B	TEB	teb
10	13%	26%	$\leq 10^{-6}$	$\leq 10^{-6}$
100	5%	10%	$\leq 10^{-6}$	$\leq 10^{-6}$
1000	2%	4%	$\leq 10^{-6}$	$\leq 10^{-6}$

TAB. 4.1 – Taux d'erreur binaire de la communication secrète en fonction du rapport des facteurs d'étalement utilisés.

Le tableau (4.1) nous donne les résultats du *teb* en fonction du rapport N_{CS}/N_{CC} utilisé. Parmi les trois rapports N_{CS}/N_{CC} présentés, le rapport le plus intéressant est le second. En effet, pour avoir un *teb* inférieur à 10^{-6} il faut que l'amplitude du signal secret soit égale à 5% de l'amplitude du message clair A, ce qui est très négligeable devant A, et correspond à ce que nous souhaitions. Notons aussi que, pour transmettre un bit secret, il faut 100 bits du message classique.

Le rapport $N_{CS}/N_{CC} = 100$ est également le plus intéressant des trois car pour le premier rapport, $N_{CS}/N_{CC} = 10$, l'amplitude du signal secret est trop importante, tandis que pour le troisième rapport, $N_{CS}/N_{CC} = 1000$, l'amplitude du signal secret convient, mais le nombre de bits utiles est multiplié par 10 par rapport à notre choix, ce qui est considérable en temps comme en coût, surtout pour ne diviser l'amplitude que par 2,5.

En conclusion, la propriété la plus importante de ces deux méthodes permettant de cacher de l'information est le fait que, si la séquence utilisée pour étaler le signal n'est pas connue, il n'est possible ni de récupérer le message secret, ni de distinguer le signal secret du bruit ambiant.

Chapitre 5

Utilisation de codes correcteurs d'erreurs dans l'étalement de spectre

Dans ce chapitre, nous allons montrer que les performances de l'étalement de spectre peuvent être améliorées en utilisant un code correcteur d'erreurs autre que le code à répétition pour la transmission des données. Dans un premier temps, nous montrons que le code à répétition est utilisé dans l'étalement de spectre, nous regardons les propriétés de ce code et nous en déduisons que ce n'est pas le code le plus adapté pour cette utilisation. Nous regardons ensuite le TEB d'une liaison à spectre étalé et nous déterminons que ce taux d'erreur est principalement fonction de trois facteurs, dont le facteur de gain de codage, qui est lié au code utilisé. Nous donnons enfin les limites théoriques de cette méthode ainsi que ses limites physiques. Nous montrons tout d'abord que la limite de Shannon pour un code de rendement 1/31 est de $-1,49$dB. Ensuite, nous déterminons le nombre maximum théorique d'utilisateurs pouvant cohabiter sur une même bande de fréquence, nombre qui est uniquement fonction du facteur d'étalement N. Ainsi, lorsque le facteur d'étalement tend vers l'infini, le nombre maximum d'utilisateurs tend lui aussi vers l'infini. Dans le cas d'un facteur d'étalement égal à 31, 45 utilisateurs peuvent interagir sur une même bande de fréquence. Quant aux limites physiques, elles nous imposent l'utilisation d'un code ayant une petite dimension, pour avoir un décodage en temps réel et un coût de réalisation moindre, ainsi qu'un facteur d'étalement ne tendant pas vers l'infini.

5.1 Analyse du code $[N, 1, N]$

Comme nous l'avons vu au chapitre 2, la technique de l'étalement de spectre par séquence directe consiste à multiplier chaque bit d'information par une séquence pseudo-aléatoire binaire de rythme très supérieur à celui des données à transmettre, voir figure (5.1).

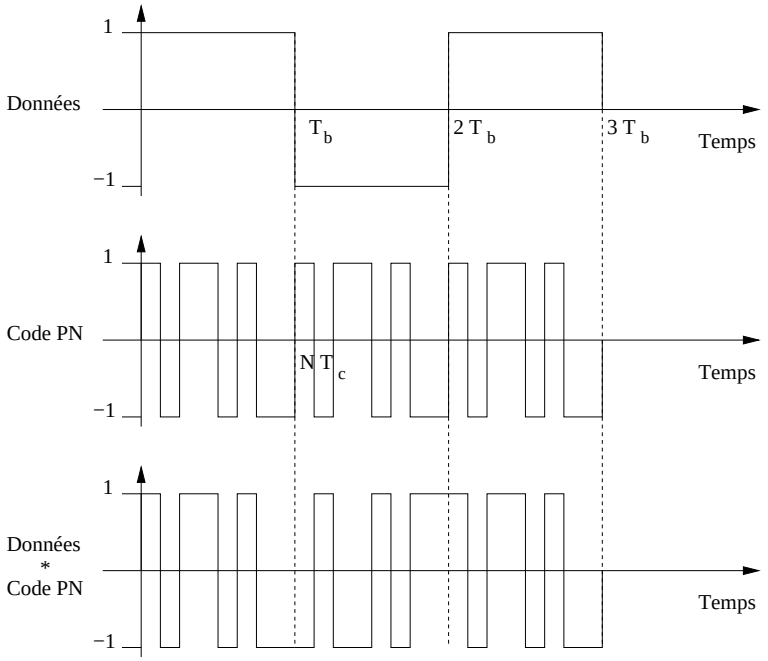


FIG. 5.1 – Étalement de spectre par séquence directe

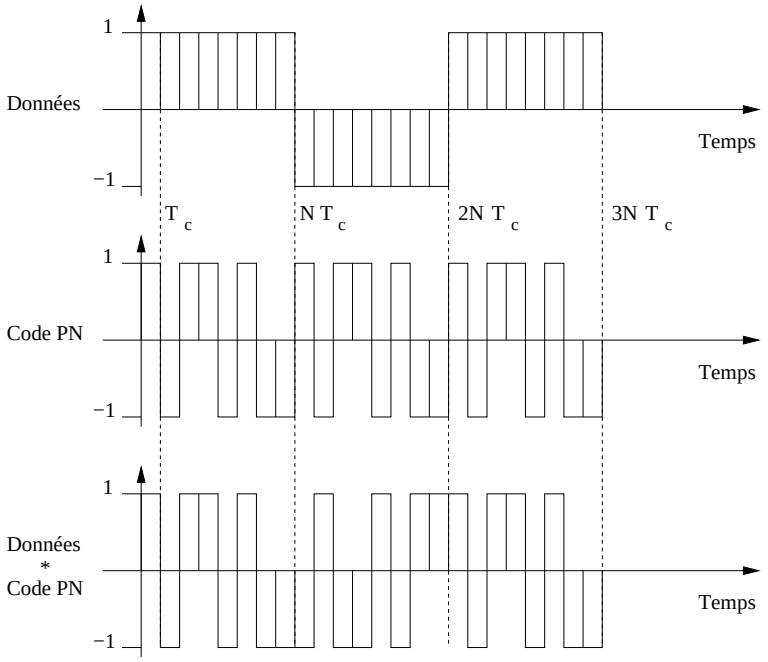


FIG. 5.2 – Étalement de spectre par séquence directe discrétisé à T_c

Discrétisons les graphiques de la figure (5.1) : nous obtenons la figure (5.2). Le fait d'établir cette discrétisation fait apparaître dans le graphique nommé "Données", un code de longueur N et de dimension 1. En effet, avant cette discrétisation, nous avions, dans le graphique nommé "Données", l'émission d'un symbole d'une durée T_b. Maintenant, nous pouvons considérer qu'à la place, nous avons l'émission de N symboles de durée T_c, d'où l'utilisation sous-jacente d'un code de longueur N et de dimension 1. Notons que ce code est utilisé pour chaque bit d'information transmis. A la réception, une fois la décorrélation effectuée avec la séquence étalante de l'utilisateur, un décodage sera effectué pour retrouver le bit d'information. Ce décodage sera fait en temps réel car l'application qui l'utilise fonctionne elle-même en temps réel, il doit être le plus simple et le plus rapide possible.

Le code qui apparaît dans la figure (5.2) est le code à répétition de paramètres $[N, 1, N]$: c'est un code MDS (Maximum Distance Separable). Rappelons qu'un code $\mathcal{C}$ binaire de paramètres $[n, k, d]$ est MDS s'il vérifie $d + k = n + 1$. C'est le meilleur code de dimension 1 et de longueur N, du point de vue du TEB, de par sa structure de code MDS. Ce code est utilisé pour une transmission bit à bit et convient parfaitement pour cette utilisation. Par contre, si nous nous plaçons dans le cas d'une transmission par blocs de bits, nous allons voir que ce n'est plus le cas.

Prenons le cas d'une transmission par blocs de l bits, $l \in \mathbb{N}^*$. Puisque pour chaque bit, le code à répétition est utilisé, le code résultat, noté $\mathcal{C}_{RR}$, est le code concaténé ayant pour paramètres $[lN, l, N]$. De par la définition de la Borne de Singleton et le résultat précédent, nous savons qu'il est possible de trouver un code de longueur lN, de dimension l et de distance minimale d tel que $N \leq d \leq lN - l + 1$.

Soit C_{max} un code binaire de dimension l et de longueur lN ayant la plus grande distance minimale : ce code est plus performant, en terme de TEB, que tout autre code de même dimension et de même rendement (voir [3, 40, 41]). Dans le cas binaire, pour une longueur de code inférieure à 256, $\mathcal{C}_{max}$ peut être trouvé à l'aide de la table de A.E. Brouwer [42]. Ainsi, en dehors du cas $l = 1$, le code $\mathcal{C}_{max}$ est différent du code $\mathcal{C}_{RR}$. Donc, pour $l \neq 1$, le code $\mathcal{C}_{RR}$ n'est pas le code le plus performant en terme de TEB.

5.2 Taux d'erreur d'une liaison à spectre étalé

Dans ce paragraphe, nous allons nous intéresser au taux d'erreur d'une transmission à spectre étalé avec et sans codage de l'information. Nous montrons ainsi que la probabilité d'erreur par symbole est fonction du poids des mots du code et du rendement. Ensuite, nous regarderons quels sont les gains de traitement et de codage de cette transmission ([1] pp. 702-709) en fonction du code utilisé.

5.2.1 Transmission avec codage

Nous considérons un système de transmission à spectre étalé avec codage de l'information, comme représenté en figure (5.3). Nous considérons aussi que le taux des données entrant dans le bloc *codeur canal* est de R bits par seconde et que la largeur de bande du canal est de W Hz. La modulation utilisée est une modulation BPSK. De plus, de manière à utiliser toute la largeur de bande disponible du canal, la porteuse du signal sera déphasée de façon pseudo-aléatoire sur le même modèle que le générateur pseudo-aléatoire, défini au bloc *Séquence Pseudo aléatoire PN*, au rythme de W fois par seconde.

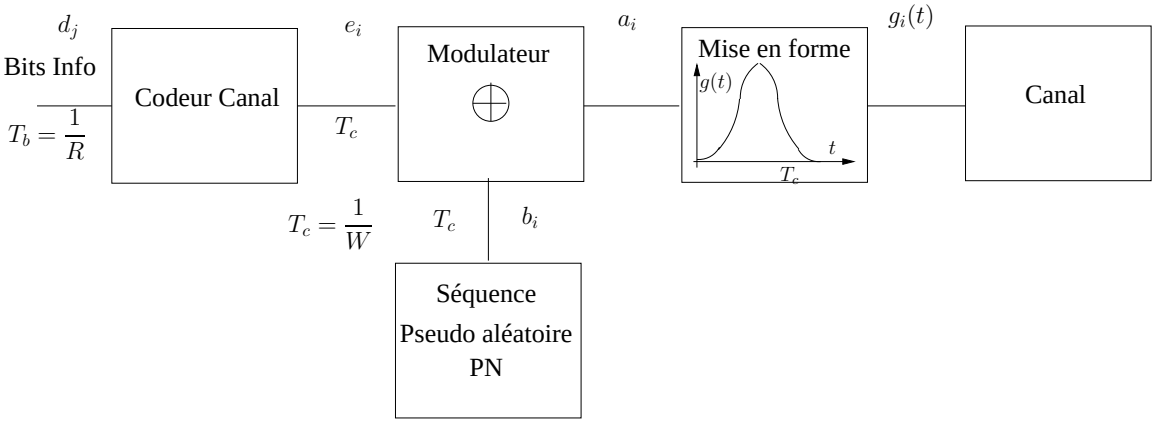


FIG. 5.3 – Schéma d'un système de transmission à étalement de spectre

Le bloc *Codeur Canal* est constitué d'un encodeur d'un code $\mathcal{C}$ de paramètres $[n, k]$ qui encode donc k bits d'entrée en n bits de sortie. Soit T_b la durée d'un bit d'entrée et T_c celle d'un bit de sortie de l'encodeur. On a :

$$kT_b = nT_c. \tag{5.1}$$

On définit le facteur d'étalement L_c par

$$L_c = \frac{T_b}{T_c} = \frac{n}{k} = \frac{W}{R} = \frac{1}{R_c}, \tag{5.2}$$

où R_c est le rendement du code $\mathcal{C}$. Nous notons $(e_i)_{1\leq i\leq n}$ la suite obtenue à la sortie de l'encodeur et $(b_i)_{1\leq i\leq n}$ la suite issue du bloc *Séquence Pseudo aléatoire PN*.

Le bloc *Modulateur* a donc pour entrée les suites (b_i) et (e_i) et pour sortie la suite (a_i) qui est le "ou exclusif bit à bit". Ainsi, nous avons la relation $a_i = b_i \oplus e_i$, où $\oplus$ désigne le "ou exclusif bit à bit".

Le bloc *Mise en forme* consiste à générer une forme d'onde $g_i(t)$ telle que si $g(t)$ est la fonction représentée à la figure (5.3) avec $\int_0^{T_c} g(t)g^*(t)dt = 2E_c$,

où E_c est l'énergie d'un bit e_i, du mot de code, on a

$$g_i(t) = \begin{cases} g(t - iT_c) & a_i = 1 \\ -g(t - iT_c) & a_i = 0, \end{cases} \tag{5.3}$$

ce qui s'écrit aussi

$$g_i(t) = (2b_i - 1)(2e_i - 1)g(t - iT_c). \tag{5.4}$$

Le signal à la réception est défini par $r_i(t) = g_i(t) + z(t)$ où $z(t)$ est le signal de bruit. A la réception, le signal reçu est filtré par le filtre adapté de réponse impulsionnelle $g^*(t)$. Après multiplication du signal de sortie du filtre par le signal pseudo-aléatoire, nous obtenons le vecteur $M = (y_1, \ldots, y_n)$ où $y_i = (2b_i - 1) \displaystyle\int_0^{T_c} r_i(t)g^*(t)$. Un décodeur souple calcule ensuite la corrélation entre le vecteur M reçu et les mots de code C_i, notés C_iM, par

$$C_iM = \sum_{j=1}^{n} (2c_{ij} - 1)y_j \text{ pour } i = 1, 2, \cdots, 2^k \tag{5.5}$$

où c_{ij} est le $j^{ème}$ bit du $i^{ème}$ mot de code.
Sans restreindre la généralité, considérons que le mot tout à zéro

$$C_1 = \underbrace{(0, \cdots, 0)}_{n\ bits}$$

est émis. Alors la corrélation C_1M est donnée par :

$$\begin{aligned} C_1M &= \sum_{j=1}^{n} (2c_{1j} - 1)^2 (2b_j - 1)^2 \int_0^{T_c} g_j(t)g_j^*(t)dt \\ &+ \sum_{j=1}^{n} (2c_{1j} - 1)(2b_j - 1) \int_0^{T_c} z(t)g_j^*(t)dt. \end{aligned}$$

En posant $\nu_j = \displaystyle\int_0^{T_c} z(t)g_j^*(t)dt$, on obtient

$$C_1M = 2nE_c - \sum_{i=j}^{n} (2b_j - 1)\nu_j. \tag{5.6}$$

De la même façon, si le mot de code C_m a un poids w_m, on a

$$C_mM = 2E_cn(1 - \frac{2w_m}{n}) + \sum_{j=1}^{n} (2c_{mj} - 1)(2b_j - 1)\nu_j. \tag{5.7}$$

Nous devons désormais calculer la probabilité pour que $C_mM > C_1M$ qui est la probabilité d'erreur au décodage. Soit $P(m)$ cette probabilité d'erreur.

$P(m) = P(C_m M > C_1 M) = P(C_1 M - C_m M < 0)$. Soit D_m la différence entre les deux corrélations $C_1 M$ et $C_m M$, on a

$$D_m = C_1 M - C_m M = 4E_c w_m - 2\sum_{j=1}^{n} c_{mj}(2b_j - 1)\nu_j. \tag{5.8}$$

Sous la condition que la distance minimum du code est suffisamment grande pour pouvoir utiliser le théorème central limite [2, 43], la somme/différence des composantes de bruit se comporte comme une variable aléatoire gaussienne. Ainsi l'espérance mathématique du second membre est nulle car $E[2b_j - 1] = 0$ et $E[\nu_j] = 0$. D'autre part, la variance est donnée par

$$\sigma_m^2 = 4\sum_{j=1}^{n}\sum_{i=1}^{n} c_{mj}c_{mi}E[(2b_j - 1)(2b_i - 1)]E[\nu_j\nu_i] \tag{5.9}$$

où $E[(2b_j - 1)(2b_i - 1)] = \delta_{ij}$. Ainsi $\sigma_m^2 = 4w_m E[\nu^2]$.
La variance $E[\nu^2]$ du terme de bruit est égale à

$$\begin{aligned} E[\nu^2] &= \int_0^{T_c}\int_0^{T_c} g(t)g^*(t)\phi_{zz}(t-\tau)dt\,d\tau \\ &= \int_{-\infty}^{+\infty} |G(f)|^2 \Phi_{zz}(f)df \end{aligned} \tag{5.10}$$

où $\phi_{zz}(\tau) = \frac{1}{2}E\left[z^*(t)z(t+\tau)\right]$ est la fonction d'autocorrélation et $\Phi_{zz}(f)$, la densité spectrale de puissance de l'interférence $z(t)$. Si la densité spectrale de bruit est constante et vaut J_0, on obtient

$$E[\nu^2] = 2E_c J_0 \text{ et donc } \sigma_m^2 = 8w_m E_c J_0. \tag{5.11}$$

Ainsi D_m suit une distribution gaussienne d'espérance $4E_c w_m$ et de variance $8w_m E_c J_0$. Finalement la probabilité pour que D_m soit négative est égale à, voir [1] (pp. 486-488),

$$P(m) = Q\left(\sqrt{\frac{16E_c^2 w_m^2}{8w_m E_c J_0}}\right) = Q\left(\sqrt{\frac{2E_c w_m}{J_0}}\right) \tag{5.12}$$

où $Q(x) = \dfrac{1}{\sqrt{2\pi}}\displaystyle\int_x^{+\infty} e^{-t^2/2}dt = \frac{1}{2}\,\text{ercf}\left(\frac{x}{\sqrt{2}}\right)$.
Comme $E_b = E_c/R_c$, on a

$$P(m) = Q\left(\sqrt{\frac{2E_b}{J_0}R_c w_m}\right). \tag{5.13}$$

Pour calculer la probabilité d'erreur P_m par symbole, il faut faire la somme de toutes les distances D_m. On obtient la borne suivante

$$P_m \leq \sum_{m=2}^{2^k} Q\left(\sqrt{\frac{2E_b}{J_0}R_c w_m}\right). \tag{5.14}$$

On remarque que la probabilité d'erreur par bit est liée à la probabilité d'erreur par symbole suivant la formule donnée dans [1] (pp. 486-488).

5.2.2 Gain de traitement et gain de codage

Déterminons les gains de codage et de traitement d'une telle communication.

On peut exprimer la probabilité donnée dans (5.14) en fonction du rapport signal à bruit des puissances. En effet, soit P_{moy} la puissance moyenne émise par bit d'information, on a alors $E_b = P_{moy}T_b = \dfrac{P_{moy}}{R}$. Par ailleurs, la puissance de bruit dans la bande W est donnée par $J_{moy} = J_0 W$.
Le rapport $\dfrac{E_b}{J_0}$ est alors donné par

$$\frac{E_b}{J_0} = \frac{P_{moy}}{J_{moy}} \frac{W}{R}. \tag{5.15}$$

En remplaçant $\dfrac{E_b}{J_0}$ dans (5.14), la probabilité d'erreur P_m est majorée par

$$P_m \leq \sum_{m=2}^{2^k} Q\left(\sqrt{\frac{2W/R}{J_{moy}/P_{moy}} R_c w_m}\right). \tag{5.16}$$

La probabilité d'erreur dépend des rapports $\dfrac{W}{R}$ et $\dfrac{J_{moy}}{P_{moy}}$ mais aussi du produit $R_c w_m$. Le rapport $\dfrac{W}{R}$ est le gain de traitement apporté par l'étalement de spectre. Le rapport $\dfrac{J_{moy}}{P_{moy}}$ est l'inverse du rapport signal à bruit. Le produit $R_c w_m$ est le gain de codage.
La borne inférieure du produit $R_c w_m$ est $R_c d_{min}$, avec d_{min} la distance minimum du code, et comme la fonction Q est décroissante nous pouvons donc majorer P_m par

$$P_m \leq \sum_{m=2}^{2^k} Q\left(\sqrt{\frac{2W/R}{J_{moy}/P_{moy}} R_c w_m}\right) \leq (2^k - 1) Q\left(\sqrt{\frac{2W/R}{J_{moy}/P_{moy}} R_c d_{min}}\right). \tag{5.17}$$

Supposons que l'émission se fasse sans codage. Dans ce cas $k = 1$ et le facteur d'étalement est N. Le poids d'un mot de code différent de 0 est alors $w = N$. On a donc $R_c w = 1$ et la probabilité d'erreur par symbole est

$$P_m = Q\left(\sqrt{\frac{2W/R}{J_{moy}/P_{moy}}}\right). \tag{5.18}$$

Dans ce cas, nous ne bénéficions pas du gain de codage qui est $R_c w_m \geq R_c d_{min}$.

En conclusion l'utilisation du code à répétition fait perdre le gain de codage que l'on a en utilisant un code ayant le même rendement. C'est pourquoi nous proposons un système à étalement de spectre n'utilisant pas de code à répétition mais un autre code ayant le même rendement et la distance minimale la plus grande possible.

5.3 Limites Théoriques

Dans cette section, nous allons définir deux limites théoriques. La première limite repose sur la théorie de l'information, c'est la limite de Shannon d'un code pour un rendement donné [4]. La seconde sera la limite sur le nombre maximum d'utilisateurs pouvant interagir dans une même bande de fréquence.

5.3.1 Limite de Shannon

Dans son article "A Mathematical Theory of Communication" de 1948 [4], Shannon fabrique les outils de la théorie de l'information. Comme nous l'avons vu dans le chapitre 1, il est à l'origine de la notion de capacité d'un canal ainsi que des notions d'entropie et d'information mutuelle. Le point de départ de son travail est le théorème suivant, souvent appelé théorème du codage de canal bruité [4, 8].

Théorème 3 *Tout canal a une capacité C, et pour tout $R < C$, il existe des codages de canal de taux R qui, à l'aide d'un décodage à maximum de vraisemblance, permettent d'atteindre des taux d'erreurs de transmission arbitrairement petits.*

A l'aide de ce résultat, nous allons déterminer, pour un rendement de code donné, la limite de Shannon en fonction du rapport signal à bruit. Pour cela, définissons tout d'abord le rapport signal à bruit. Nous donnerons ensuite la relation liant la capacité C du canal au rapport signal à bruit.

Soient E_b et E_s respectivement l'énergie par bit d'information et l'énergie par symbole transmis. L'énergie par bit d'information E_b est l'énergie par symbole transmis E_s divisée par le taux de codage R, c'est à dire

$$E_b = E_s/R.$$

Le rapport signal à bruit E_b/N_0, exprimé en décibel (dB), est le rapport de l'énergie par bit d'information à l'énergie du bruit. On a :

$$E_b/N_0 \text{ (dB)} = 10\log_{10}(E_b/N_0) = 10\log_{10}(E_s/N_0) - 10\log_{10}(R).$$

Nous appelons *rapport utile signal à bruit* le rapport E_b/N_0 et *rapport brut signal à bruit* le rapport E_s/N_0. En effet, l'énergie émise par l'émetteur est l'énergie symbole E_s, quel que soit le rendement du code, tandis que l'énergie

qui nous intéresse pour faire des comparaisons avec d'autres codes n'ayant pas le même rendement est l'énergie par bit d'information E_b. La capacité du canal gaussien à entrée binaire et sortie réelle en fonction du rapport brut signal à bruit est donnée par la formule suivante, déjà présentée dans le chapitre 1 (voir équation (1.8), en posant $E_s/N_0 = 1/2\sigma^2$ et $A = 1$) :

$$C = \sqrt{\frac{E_s}{\pi N_0}} \int_{-\infty}^{+\infty} e^{-\frac{E_s}{N_0}(y-1)^2} (1 - \log_2 \left(1 + e^{-\frac{E_s}{N_0} 4y} \right)) dy.$$

Cette capacité est tracée en figure (5.4) en fonction du rapport brut signal à bruit ainsi que la capacité du canal binaire symétrique [8]. Comme nous

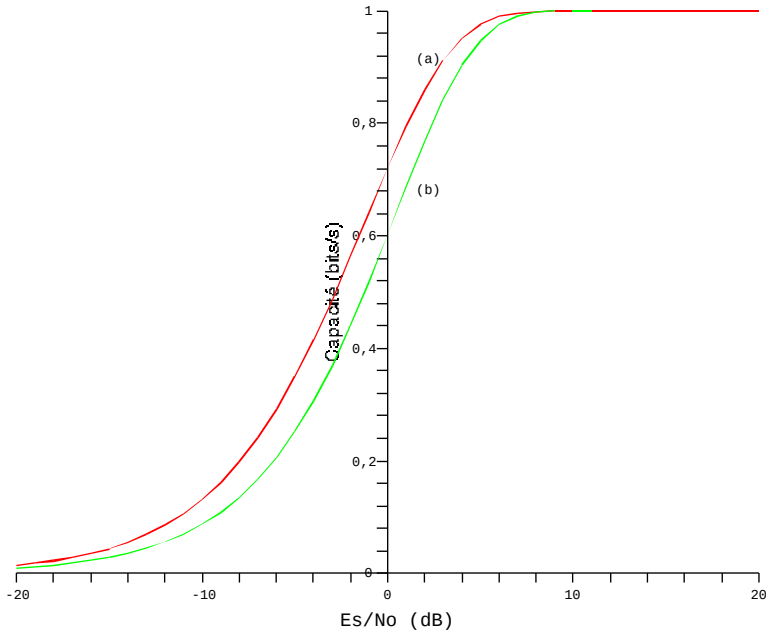


FIG. 5.4 – Capacité des différents canaux : (a) canal gaussien à entrée binaire et sortie réelle ; (b) canal binaire symétrique.

venons de le voir, la capacité du canal est fonction du rapport brut signal à bruit. D'après le théorème du codage de canal bruité, nous pouvons trouver des codes (et des décodeurs) ayant un rendement aussi proche que l'on veut de la capacité du canal et pouvant avoir des taux d'erreurs aussi petits que l'on veut. Pour un rendement R supérieur à C, il est impossible de trouver des codes ayant un TEB aussi petit que l'on veut. La condition limite s'applique donc à un rendement de code égal à la capacité du canal. Cette limite nous donne par conséquent une limite inférieure sur le rapport utile signal à bruit pour lequel nous sommes certains d'avoir un TEB arbitrairement petit. Elle est

appelée la *limite de Shannon* [4, 8]. Dans le cas où le rendement est fixé, il s'agit de déterminer pour quelle valeur de rapport brut signal à bruit nous avons la capacité du canal qui est égale au rendement, puis de calculer le rapport utile signal à bruit correspondant.

Exemple

La figure (5.5) représente le TEB d'un signal BPSK utilisant le code de paramètres [186,6,94], de rendement $R = 1/31$, ayant pour algorithme de décodage un algorithme à maximum de vraisemblance, d'un signal BPSK sans codage et la limite de Shannon. Pour obtenir un TEB de 10^{-3} à l'aide du code de paramètres [186,6,94], il suffit d'un rapport utile signal à bruit d'environ $4,09$ dB. Donc il faut un rapport brut signal à bruit E_s/N_0 de

$$4,09 \text{ dB } + 10\log_{10}(1/31) \approx -10,82 \text{ dB}.$$

Sans codage, il faut un rapport signal à bruit de $6,82$ dB. On a donc un gain de codage de $2,73$ dB.
La capacité de ce canal est tracée en figure (5.4) courbe (a). Nous avons pour un rapport brut signal à bruit de $-10,82$ dB, une capacité de canal $C = 0,11 = -9,56$ dB. On dit que l'on transmet à $10\log_{10}(C/R) = 5,34$ dB de la capacité.
Pour transmettre à 0 dB de la capacité, il faut que $C = R = 1/31$, donc avoir un rapport brut signal à bruit de $-16,4$ dB, c'est à dire un rapport utile signal à bruit de -1.49 dB, représenté en figure (5.5) par la droite verticale. C'est la limite de Shannon pour tout code de rendement 1/31.

La limite de Shannon pour tout code de rendement 1/31 est pour un rapport utile signal à bruit de $-1,49$ dB.

5.3.2 Nombre maximum d'utilisateurs

Dans cette partie, nous déterminons le nombre d'utilisateurs maximum pouvant interagir sur une fréquence donnée, [20, 21, 33, 44]. Considérons le système CDMA ayant les paramètres suivants

- M : le nombre maximum d'utilisateurs,
- W : la largeur de bande de fréquence du signal étalé en hertz (Hz),
- T_c : le temps chip, $T_c = \dfrac{1}{W}$,
- R_τ : le taux de transfert en bits/s,
- T_b : le temps bit, $T_b = \dfrac{1}{R_\tau}$,
- P : la puissance de chaque utilisateur en watts,
- E_b : l'énergie par bit reçu, $E_b = \dfrac{P}{R_\tau}$,

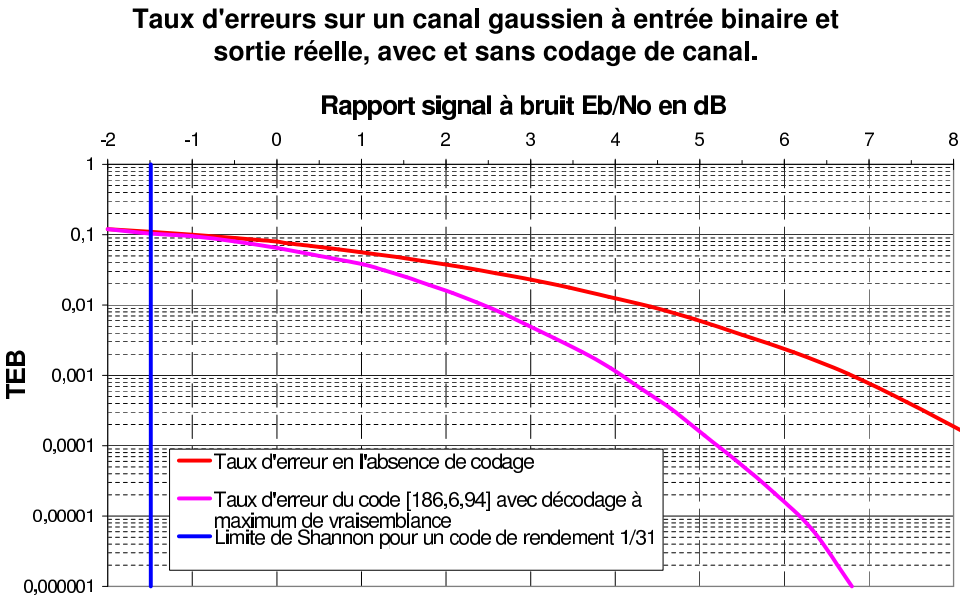


FIG. 5.5 – Taux d'erreurs sur un canal gaussien en modulation BPSK, avec et sans codage de canal.

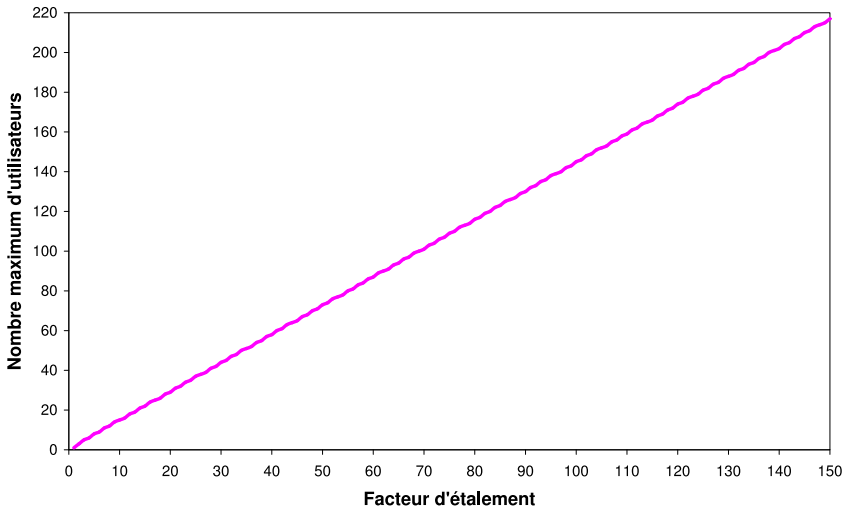


FIG. 5.6 – Nombre maximum d'utilisateurs pouvant interagir en fonction du facteur d'étalement.

- I : la puissance des interférences engendrées par les autres utilisateurs, $I = (M-1)P$,
- I_0 : la densité de bruit reçu par chaque utilisateur, $I_0 = \dfrac{I}{W}$,
- N : le facteur d'étalement, $N = \dfrac{T_b}{T_c} = \dfrac{W}{R}$.

En utilisant la définition de la puissance des interférences engendrées par les autres utilisateurs, nous savons alors que le nombre maximum d'utilisateurs a pour valeur

$$M = \frac{I}{P} + 1. \tag{5.19}$$

Or, par définition de la densité de bruit I_0, l'équation (5.19) devient

$$M = \frac{I_0 W}{P} + 1. \tag{5.20}$$

En remplaçant P, la puissance de chaque utilisateur, par $E_b R_\tau$ l'équation (5.20) s'écrit

$$M = \frac{I_0 W}{E_b R_\tau} + 1. \tag{5.21}$$

En regroupant les rapports $\dfrac{W}{R_\tau} = N$ et $\dfrac{E_b}{I_0}$, l'équation devient

$$M = \frac{\dfrac{W}{R_\tau}}{\dfrac{E_b}{I_0}} + 1 = \frac{N}{\dfrac{E_b}{I_0}} + 1. \tag{5.22}$$

Le rapport $\dfrac{E_b}{I_0}$ est le rapport de l'énergie par bit sur la densité de bruit nécessaire pour que le récepteur de l'étalement de spectre de chaque utilisateur puisse fonctionner. Dans notre étude, le facteur d'étalement N est l'inverse du rendement du code utilisé. Ainsi pour le rapport $\dfrac{E_b}{I_0}$, nous prendrons la limite de Shannon d'un code ayant pour rendement 1/N, puisque c'est la borne inférieure du rapport utile signal à bruit pour lequel nous sommes certains d'avoir un TEB arbitrairement petit. Notons que le nombre maximum d'utilisateurs est fonction principalement du facteur d'étalement. La figure (5.6) représente le nombre d'utilisateurs maximum pouvant interagir en fonction de la valeur du facteur d'étalement. Nous constatons que plus le facteur d'étalement est grand plus le nombre de personnes pouvant interagir est grand. Et lorsque N tend vers l'infini, le nombre maximum d'utilisateurs tend lui aussi vers l'infini.

Pour un facteur d'étalement $N = 31$, la limite de Shannon se situe à un rapport utile signal à bruit $E_b/N_0 = -1.49$ dB. Ainsi le nombre maximum

d'utilisateurs M pouvant interagir a pour valeur

$$M = \left\lceil \frac{31}{10^{\frac{-1.49}{10}}} + 1 \right\rceil = 45. \tag{5.23}$$

Cette valeur est à mettre en parallèle avec les valeurs que nous obtenons dans le chapitre suivant concernant les améliorations que nous proposons.

5.4 Limites Physiques

La première limite physique concerne le décodeur du code correcteur. Comme nous l'avons déjà dit, le système à étalement de spectre est un système fonctionnant en temps réel. Il est donc nécessaire pour avoir le débit de données d'information le plus intéressant possible que le décodeur utilisé soit à la fois le plus rapide et le plus performant possible. Notons $\mathcal{C}$ le code de paramètres $[n, k]$, et $c_i = (c_{i1}, \ldots, c_{ij}, \ldots, c_{in}) \in \{-1, 1\}^n \subset \mathbb{N}^n$ un mot du code $\mathcal{C}$ et $r \in \mathbb{R}^n$ le mot reçu. Le décodeur le plus adapté pour cette utilisation est le décodage à maximum de vraisemblance. Il consiste à déterminer quel est le mot c_i du code $\mathcal{C}$ qui est le plus proche, pour la distance euclidienne, du mot reçu r. Pour cela, les 2^k distances doivent être calculées pendant une durée de temps égale au temps d'émission d'un mot de code. Ceci est possible car ces 2^k calculs peuvent se faire en parallèle.

En effet, nous devons calculer $||c_i - r|| = \sqrt{\sum_{j=1}^{n}(c_{ij} - r_j)^2}$ pour $i = 1, \ldots, 2^k$ et déterminer pour quelle valeur de i cette distance est la plus petite. Afin de faciliter ces calculs, nous ne nous intéressons pas à la distance, qui demanderait un calcul de racine carrée ayant un coût non négligeable en temps, mais nous prenons en compte le carré de la distance défini par

$$||c_i - r||^2 = \sum_{j=1}^{n}(c_{ij} - r_j)^2.$$

Dans ce cas de figure, nous n'avons plus que des additions, soustractions et des élévations au carré à effectuer. Ces dernières ont toutefois un coût en temps non négligeable par rapport aux deux premières et comme nous ne pouvons nous en passer nous allons en minimiser le nombre. A priori, en calculant les distances les unes indépendamment des autres, pour chaque calcul de distance, n élévations au carré, n différences et $(n-1)$ additions sont nécessaires. Et donc, pour calculer les 2^k distances, $n2^k$ élévations au carré, $n2^k$ différences et $(n-1)2^k$ additions sont nécessaires.

Toutefois, nous remarquons qu'à chaque étape j $c_{ij} \in \{-1, 1\}$ d'où $(c_{ij} - r_j)^2$ prend deux valeurs distinctes :

$$(c_{ij} - r_j)^2 = \begin{cases} (1 - r_j)^2 \\ (-1 - r_j)^2 = (1 + r_j)^2 \end{cases} \tag{5.24}$$

Seules deux élévations au carré sont nécessaires à chaque étape j et ce calcul sera effectué dès réception du r_j correspondant. Ensuite pour $l = 1, \ldots, 2^k$, la valeur $(c_{lj} - r_j)^2$ correspondant à l'état c_{lj} sera envoyée à l'accumulateur numéro l qui calcule la valeur $||c_l - r||^2$. Cette répartition dans les accumulateurs se fait en parallèle, ce qui permet d'effectuer également le calcul des 2^k distances en parallèle. Toutefois, 2^k accumulateurs sont nécessaires ce qui n'est pas à négliger pour une réalisation pratique et le choix de la dimension du code devra être judicieux. En conclusion, dans cette configuration, $2n$ élévations au carré, n différences et $(2^k + 1)n - 2^k$ additions sont nécessaires ainsi que 2^k accumulateurs, ce qui constitue un gain de temps important par rapport au cas de figure a priori. Pour ajouter à chaque accumulateur l la bonne valeur $(c_{lj} - r_j)^2$ correspondante suivant la valeur c_{lj}, il suffit simplement de mettre avant chaque accumulateur une porte logique qui définit, suivant l'entrée c_{ij}, la valeur à ajouter, c'est à dire soit $(r_j + 1)^2$ soit $(r_j - 1)^2$, voir figure (5.7).

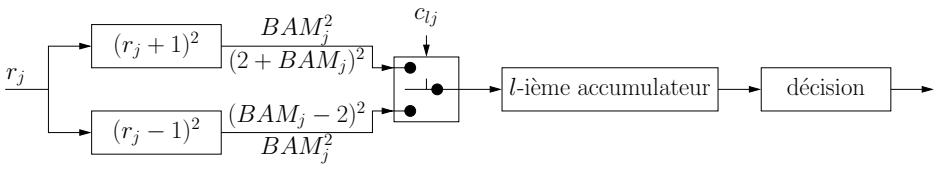


FIG. 5.7 – Système récepteur, partie décodage

Cette utilisation, telle que nous l'avons décrite, nécessite donc de stocker tous les mots du code dans une mémoire pour qu'à l'instant j la porte logique de l'accumulateur l, par exemple, sache quelle entrée elle doit utiliser. Cela nécessite également un câblage assez conséquent entre la mémoire et les portes logiques. Ainsi, le fait d'utiliser des accumulateurs en parallèle fait gagner du temps de calcul puisque toutes les sommes se font en même temps, mais ce gain de temps peut être très onéreux. En effet le nombre d'accumulateurs doit être égal à 2^k et le câblage doit aller de la mémoire à chaque porte logique, sans tenir compter de l'espace mémoire nécessaire pour stocker tous les mots du code. Il s'agit donc de faire un compromis entre gain de temps et coût financier : dans notre cas, nous nous sommes limités à des codes ayant une dimension égale à 6 ou 8. Nous avons ainsi un gain de temps conséquent et une minimisation du coût financier.

Nous avons également une autre limite physique qui concerne le facteur d'étalement N. En effet, nous avons remarqué, dans la section "limites théoriques" de ce chapitre, que plus le facteur d'étalement est grand, plus le nombre d'utilisateurs pouvant cohabiter sur une même bande de fréquence est grand. Ainsi, dans l'objectif de faire cohabiter le maximum d'utilisateurs sur une même bande de fréquence, la solution la plus simple est d'utiliser un facteur d'étalement le plus grand possible tendant vers l'infini. Cependant pour un débit d'information fixé à, par exemple, 1 Mégabit/s, la durée d'émission

d'un bit d'information T_b est égale à $\frac{1}{10^6}$ seconde et le temps chip $T_c = \frac{T_b}{N}$ est de $\frac{1}{N10^6}$ seconde. Comme tout le système, émetteur et récepteur, est cadencé sur ce temps chip T_c cela signifie qu'il doit fonctionner à une fréquence, qui est l'inverse de la période T_c, de $N10^6$ Hz soit N MHz pour satisfaire la contrainte de débit d'information. Or, plus la fréquence des composants est élevée, plus ces composants coûtent chers : de nos jours, la plus grande fréquence d'utilisation pour des composants est de 100 GHz, cette valeur est assez conséquente mais ne tend pas vers l'infini. De plus, avec une telle fréquence, le facteur d'étalement pour le débit envisagé est d'au plus $N = 100000$. Ce facteur d'étalement est donc limité par la fréquence d'utilisation des composants mais aussi par le débit de donnée qui divise d'autant la valeur du facteur d'étalement. Comme dans les normes de télécommunication, les débits d'information sont exprimés en Mégabits par seconde. Cela signifie que la fréquence de fonctionnement du système est au moins un milliard de fois plus grande que le facteur d'étalement comme nous venons de le voir. Cela limite d'autant la valeur maximum du facteur d'étalement.
Ainsi pour ces deux raisons, contraintes physiques et coût financier, le facteur d'étalement ne peut tendre vers l'infini.

Chapitre 6

Synthèse et applications

Nous proposons un système faisant la synthèse des résultats que nous avons observés précédemment. Les TEB que nous donnons dans ce chapitre sont ceux obtenus à la sortie du bloc "Reconstruction signal" du schéma de transmission donné au chapitre 2 en figure (2.2). Dans un premier temps, nous faisons une présentation du système utilisé. Ce dernier est un peu différent de celui proposé en fin de chapitre 2, puisque nous prenons en compte les résultats trouvés dans le chapitre 5 concernant l'utilisation de codes correcteurs d'erreurs. Nous donnons ensuite les résultats que nous avons obtenus en fonction du code utilisé. Nous nous sommes intéressés à des codes de petite dimension, 6 ou 8, satisfaisant aux contraintes physiques définies dans le chapitre 5, puisque, comme nous l'avons vu précédemment, le décodeur utilisé doit fonctionner en temps réel. 0r, l'algorithme de décodage, ayant un fonctionnement en temps réel, est l'algorithme de décodage à maximum de vraisemblance car la plupart des calculs se font en parallèle. Toutefois, cette parallélisation demande une augmentation de la taille du circuit et donc un surcoût financier. Ainsi, pour limiter cela, nous imposons que la dimension de ces codes ne soit pas supérieure à 8. Nous nous sommes ensuite intéressés à des codes concaténés ayant pour code interne des codes de petite dimension.

6.1 Présentation du système

Le système utilisé est le même que celui défini en fin de chapitre 2 et présenté sur les figures (2.7) et (2.8), avec toutefois certaines modifications mineures pour la partie émettrice et plus importantes pour la partie réceptrice. Comme nous l'avons vu dans le chapitre 5, l'émission des bits peut se faire par blocs de l bits, et dans ce cas, le code à répétition n'est pas le code le plus approprié. Il est alors nécessaire d'utiliser le code ayant la plus grande distance minimale pour une dimension l et un rendement $1/N$ donnés. Ainsi durant la durée de temps d'émission d'un symbole constitué de l bits, notés $T_s = l\ T_b = l\ N\ T_c$, ce n'est pas le bit 0 ou 1 qui sera émis durant la période de temps T_s mais une succession de lN bits de 0 et de 1, de durée T_c chacun.

Cette succession de bits est fonction du symbole à émettre.

Pour l'émission, voir figure (6.1), en entrée de l'émetteur, les bits d'informations sont regroupés par blocs de l bits formant ainsi un symbole. Ce symbole correspond à un mot de code particulier. Les l bits d'informations entrant dans l'émetteur activent l'entrée de la table d'adressage qui correspond au symbole formé par les l bits. La sortie de cette table est la succession de lN bits. Ceux-ci forment le mot du code correspondant au symbole à émettre. Ensuite, ces lN bits sont stockés dans un convertisseur parallèle/série. Ce dernier délivrera les bits à chaque top d'horloge T_c. Ainsi, chaque bit issu du convertisseur est émis pendant une durée T_c. Il crée un déphasage sur la porteuse du signal. Ce signal, avant d'être émis, est déphasé une nouvelle fois par la séquence d'étalement de l'utilisateur.

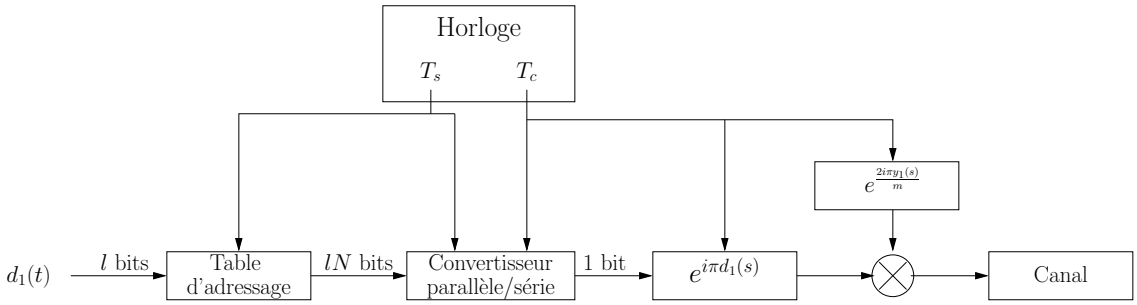


FIG. 6.1 – Système utilisé du point de vue de l'émetteur numéro 1.

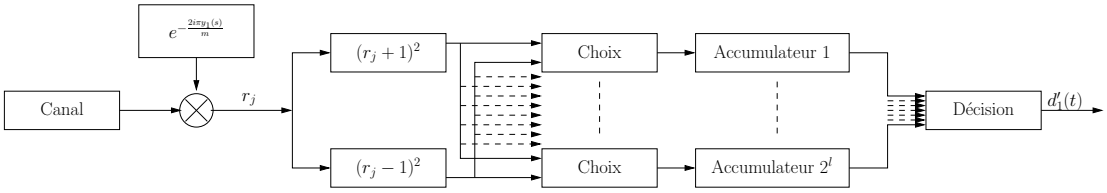


FIG. 6.2 – Système utilisé du point de vue du récepteur numéro 1.

A la réception, figure (6.2), nous appliquons la décorrélation pour éliminer le déphasage dû à la séquence de l'utilisateur. D'un côté, nous avons un bit du mot de code émis et, de l'autre côté, nous avons l'intercorrélation, due aux autres utilisateurs, notée BAM. Ensuite, il s'agit de déterminer le symbole émis à l'aide d'un décodage à maximum de vraisemblance. Pour cela, nous devons déterminer quel symbole est le plus proche du symbole reçu pour la distance euclidienne. Ainsi, nous calculons les valeurs $(r_j + 1)^2$ et $(r_j - 1)^2$, comme nous l'avons vu dans le chapitre 5. Puis, les 2^l accumulateurs ajoutent à leurs valeurs déjà existantes l'une des deux valeurs qui vient d'être calculée. Une fois le calcul des 2^l distances effectué, l'organe de décision détermine quel est le symbole qui fut probablement émis en déterminant quel est l'accumulateur

qui a la plus petite valeur, cette valeur étant le carré de la distance euclidienne entre le symbole reçu et l'un des symboles pouvant être émis.

6.2 Résultats expérimentaux

Lors de l'utilisation d'un code correcteur d'erreur, la partie la plus contraignante est le décodage. En effet, si on connaît la matrice génératrice du code, l'encodage est simple. Le décodage en revanche n'est pas aussi simple que cela si on souhaite que ce dernier soit rapide et peu onéreux en temps et en coût matériel. Plusieurs décodages existent : décodage exhaustif, décodage itératif, etc et ils sont plus ou moins coûteux et utilisables suivant le code utilisé du fait de leurs particularités structurales. Dans cette section, nous présenterons les résultats de notre recherche pour améliorer les performances du CDMA en utilisant des décodages qui sont appropriés pour notre utilisation.

6.2.1 Codes de petite dimension

Dans un premier temps, notre intérêt s'est porté sur des codes de petites dimensions, 6 voire 8, ayant la distance minimale la plus grande connue à ce jour, en faisant un décodage à maximum de vraisemblance. Ces codes, qui ont un décodage en temps réel, ont une dimension inférieure ou égale à 8. Ils satisfont aux contraintes physiques que nous nous sommes imposées dans le chapitre précédent.

Dans le cadre de notre étude, l'émetteur et le récepteur sont synchronisés. Cette synchronisation est maintenue tout le long de la transmission. Le facteur d'étalement est $N = 31$. Les codes utilisés sont les suivants : $[31, 1, 31]$, $[62, 6, 31]$ répété trois fois équivalent au code $[186, 6, 93]$, $([62 \times 3, 6, 31 \times 3])$. Le code ayant la plus grande distance minimale connue à ce jour de dimension 6 et de longueur 186 a pour paramètres $[186, 6, 94]$. Les tables de Brouwer permettent de déterminer de tels codes [42]. Les matrices génératrices de ces codes sont données en annexe B. Pour notre système, ces deux derniers codes sont quasiment équivalents. En effet, les courbes de TEB en fonction du rapport utile signal à bruit sont confondues, voir figure (6.3). Ceci n'est pas étonnant puisque la différence entre les deux distances minimales est de 1. Le gain de codage de ces deux codes a pour borne inférieure 3 tandis que le gain de codage du code à répétition est de 1.

En ce qui concerne les codes de dimension 8 que nous avons utilisés, la différence entre les distances minimales sera plus grande et le résultat s'en ressentira puisque les courbes de résultat sont espacées. En dimension 8, les codes que nous avons utilisés sont les suivants : $[62, 8, 28]$ répété quatre fois, comme pour celui de dimension 6, le code équivalent a pour paramètres $[248, 8, 112]$. Le code ayant la plus grande distance minimale connue à ce jour de dimension 8 et de longueur 248 a, quant à lui, pour paramètres $[248, 8, 124]$, voir [42]. La différence des deux distances minimales est de 12 et cela s'en ressent sur les

résultats, voir figure (6.3). Le gain de codage de ces deux codes est respectivement minoré par 3,61 et 4, ce qui conforte les résultats de simulations.

Pour un TEB fixé à 10^{-3}, nous constatons qu'avec le code à répétition nous pouvons avoir au maximum 7 utilisateurs pouvant interagir ensemble. Par contre si les bits ne sont pas émis bit à bit mais par blocs de 6 bits alors le nombre maximum d'utilisateurs est de 13. Pour une émission par blocs de 8 bits, le nombre maximum d'utilisateurs pouvant interagir ensemble a pour valeur 15. Cette amélioration est due au gain de codage de chaque code. Nous avons ainsi doublé le nombre maximum d'utilisateurs pouvant interagir ensemble. Toutefois le nombre maximum théorique d'utilisateurs pouvant être actifs ensemble est de 45. Nous sommes donc au tiers de la borne théorique. Pour pouvoir progresser, nous utiliserons un code concaténé résultat d'un code de petite dimension tel que nous venons de le décrire, concaténé avec un code de Reed Solomon et divers rendements pour ces deux codes de telle sorte que les codes concaténés obtenus aient un rendement voisin de 1/31, soit un facteur d'étalement voisin de 31.

En ce qui concerne le TEB en fonction du rapport utile signal à bruit pour une liaison à spectre étalée, il est représenté en figure (6.4). Ainsi, pour un TEB fixé à 10^{-3}, il faut, pour le code à répétition, un rapport utile $\frac{E_b}{N_0}$ de 6,75 dB ; tandis que pour le code de paramètres $[186, 6, 94]$, il faut un rapport de 4,05 dB. Ce qui fait un gain de 2,7 dB. Et pour le code de paramètres $[248, 8, 112]$, ce rapport est de 3,65 dB, ce qui fait un gain par rapport au code à répétition de 3,1 dB. Ces gains sont très intéressants mais doivent être mis en parallèle avec la limite de Shannon qui, dans ce cas, est de -1,49 dB, car rappelons-le, cette limite est pour tout code de rendement 1/31. Ainsi, les codes de dimension 6 et 8 sont respectivement à 5,54 dB et 5,14 dB de la limite de Shannon. Nous pouvons trouver des codes plus proches de cette limite et qui satisfont à nos contraintes, comme nous allons le voir avec l'utilisation d'un code concaténé résultat d'un code de petite dimension et d'un code de Reed Solomon.

6.2.2 Code Reed Solomon concaténé avec des codes de petite dimension

Pour que l'étalement de spectre soit le plus performant possible, il est nécessaire de regrouper les bits d'informations, comme nous l'avons vu dans le chapitre 5. Mais le décodage utilisé a ses limites, qui sont soit des limites de temps, soit des limites physiques. En effet, le décodage doit être un décodage en temps réel de par la nature de l'application. Cela impose une contrainte de temps. Il est donc envisageable de paralléliser le décodage pour satisfaire la contrainte de temps. Toutefois, cette parallélisation a un coût matériel non négligeable, qui impose une contrainte sur la dimension du code utilisé. Ainsi, pour satisfaire à ces contraintes nous utilisons un code de Reed Solomon concaténé avec un code de dimension inférieure ou égale à 8.

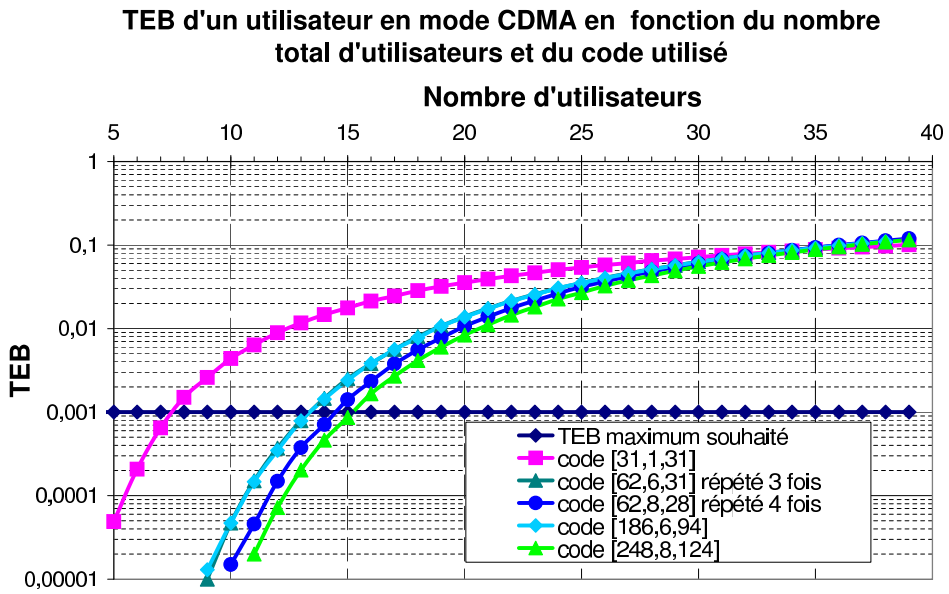


FIG. 6.3 – TEB d'un utilisateur en mode CDMA en fonction du nombre total d'utilisateur et du code utilisé.

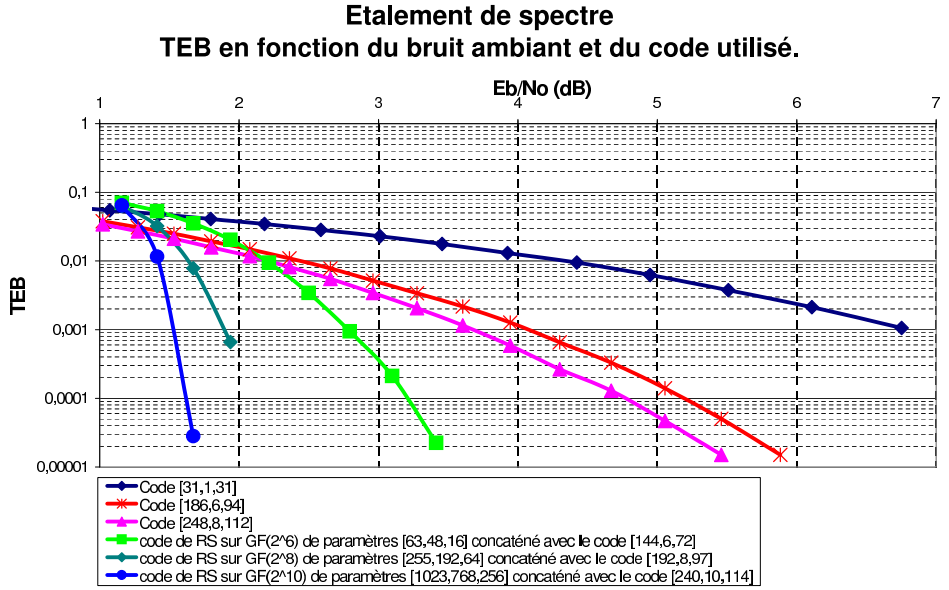


FIG. 6.4 – Taux d'erreur binaire en fonction du bruit et du code utilisé

Les codes de Reed Solomon sont définis sur des corps finis $\mathbb{F}_q$ et ont pour paramètres $[M = q-1, K, D = M-K+1]$ (voir [40, 41]). Nous nous sommes intéressés à des codes de Reed Solomon sur $\mathbb{F}_{2^6}$, c'est à dire le corps fini à 64 éléments, et sur $\mathbb{F}_{2^8}$. Étant donné que la construction de ces codes est similaire, nous nous limitons à la présentation de la construction du code de Reed Solomon sur le corps $\mathbb{F}_{2^6}$.

Le corps $\mathbb{F}_{2^6}$ peut être vu comme un $\mathbb{F}_2$-espace vectoriel de dimension 6. En effet, ce corps est défini à partir d'un polynôme primitif de degré 6, que nous notons $P_6(X) = \sum_{i=0}^{6} a_i X^i$, avec $\forall i \in \{1, \ldots, 5\},\ a_i \in \{0, 1\}$ et $a_0 = a_6 = 1$, irréductible sur $\mathbb{F}_2$. Le corps $\mathbb{F}_{2^6}$ est isomorphe à $\mathbb{F}_2$ quotienté par l'idéal engendré par $P_6(X)$, c'est à dire :

$$\mathbb{F}_{2^6} \backsimeq \mathbb{F}_2/(P_6(X)).$$

La matrice génératrice du code de Reed Solomon sur $\mathbb{F}_{2^6}$ est définie à l'aide d'une racine primitive de $P_6(X)$, notée α , c'est à dire :

$$\forall i \in \{1, .., 62\} \quad \alpha^i \not\equiv\ 1\ [a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5],$$

qui engendre $\mathbb{F}_2/(P_6(X))$. Elle est de la forme :

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{M-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & \cdots & (\alpha^2)^{M-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^K & (\alpha^K)^2 & (\alpha^K)^3 & \cdots & (\alpha^K)^{M-1} \end{pmatrix}.$$

Cette matrice peut se mettre sous forme systématique, voir théorème 1 de [45], et c'est sous cette forme que nous l'utilisons dans notre application, d'une part, pour limiter la mémoire utilisée et, d'autre part, pour retrouver facilement les symboles d'information.

Les codes internes qui sont concaténés avec le code de Reed Solomon sont des codes de petites dimensions. Ils sont de dimension 6 si nous utilisons le code de Reed Solomon sur le corps $\mathbb{F}_{2^6}$, ou de dimension 8 si nous utilisons le code de Reed Solomon sur le corps $\mathbb{F}_{2^8}$. Le fait de prendre des codes internes qui ont la même dimension que le degré d'extension du corps est la manière la plus simple de ne pas avoir à couper les symboles des mots du Reed Solomon. En effet, les symboles du code de Reed Solomon sont des blocs de q bits, ici $q = 6$ ou $q = 8$.Donc pour plus de simplicité de manipulation, nous utilisons un code interne ayant pour dimension le nombre de bits constituant un symbole du code de Reed Solomon. De plus, comme nous l'avons déjà dit, ces corps peuvent être considérés comme des $\mathbb{F}_2$-espaces vectoriels. Ainsi, tout se passe comme si nous travaillions sur des bits qui sont par blocs de 6 pour $\mathbb{F}_{2^6}$ et de 8 pour $\mathbb{F}_{2^8}$, d'où l'intérêt d'utiliser des codes internes de petite dimension, ayant

une dimension égale au degré de l'extension. Nous faisons également ce choix dans un souci d'efficacité en terme de décodage. En effet, après décodage du code interne, certains bits d'information peuvent être erronés. Etant donnés qu'ils sont issus d'un seul symbole du code de Reed Solomon, seul un symbole sera erroné quelque soit le nombre de bits d'information faussés issus du code interne. Par contre, si les bits d'information du code interne sont issus de plusieurs symboles du code de Reed Solomon, alors au moins un symbole sera faussé et, suivant la place des erreurs, ce seront tous les symboles considérés qui seront erronés. Ce qui limite la capacité de correction du décodeur.

Le principe de l'encodage, pour une émission par blocs de 6 bits, est le suivant :

- les bits d'information sont encodés par le code de Reed Solomon dans un premier temps ;
- après cet encodage, nous avons M symboles de 6 bits qui sont, à leur tour, encodés par le code de petite dimension correspondant, voir figure (6.5) ;
- le code concaténé résultant des deux codes a pour paramètres $[Mn, Km]$, où $[n, m]$ sont les paramètres du code de petite dimension, et a pour facteur d'étalement $\frac{Mn}{Km}$.

Dans notre étude, M=63 ou 255. Comme $K \in \{1, \ldots, M-1\}$, il est nécessaire de trouver pour quelle valeur de K le code concaténé résultat du code de Reed Solomon et du code de petite dimension est le plus performant. Il y a effectivement un point d'équilibre à trouver car, si le facteur d'étalement du code de petite dimension est petit (par exemple 4 ou 8), alors le décodage est moins performant en terme de TEB. En effet, pour un rapport signal à bruit utile fixé, le TEB d'un code ayant un facteur d'étalement petit, N=4 ou 8, est plus grand que le TEB d'un code ayant un facteur d'étalement grand. Ainsi, il y a une forte probabilité d'erreur pour que le symbole en sortie du décodeur du code de petite dimension ne soit pas le même que le symbole rentrant. De ce fait, le symbole correspondant pour le mot du code de Reed Solomon peut être faux, et la probabilité que ces symboles soient faux est grande pour tous les symboles. Donc, le décodage du Reed Solomon a une forte probabilité de retourner des bits d'informations faux. Toutefois, si le facteur étalement du code de petite dimension est grand, la probabilité d'erreur est plus faible, d'où une probabilité d'erreur pour le code de Reed Solomon plus faible et, finalement, un bon décodage des bits d'informations. Il est donc nécessaire, pour un rendement du code concaténé fixé, de trouver pour quels rendements du code de Reed Solomon et du code de petite taille le TEB est le plus faible possible pour un même rapport utile signal à bruit.

Lors de notre étude, nous avons trouvé les meilleurs résultats lorsque $\frac{K}{M+1} = \frac{3}{4}$. Nous avons donc considéré le code de Reed Solomon sur $\mathbb{F}_{2^6}$ de paramètres $[63, 48, 16]$ concaténé avec le code de paramètres $[144, 6, 72]$, le fac-

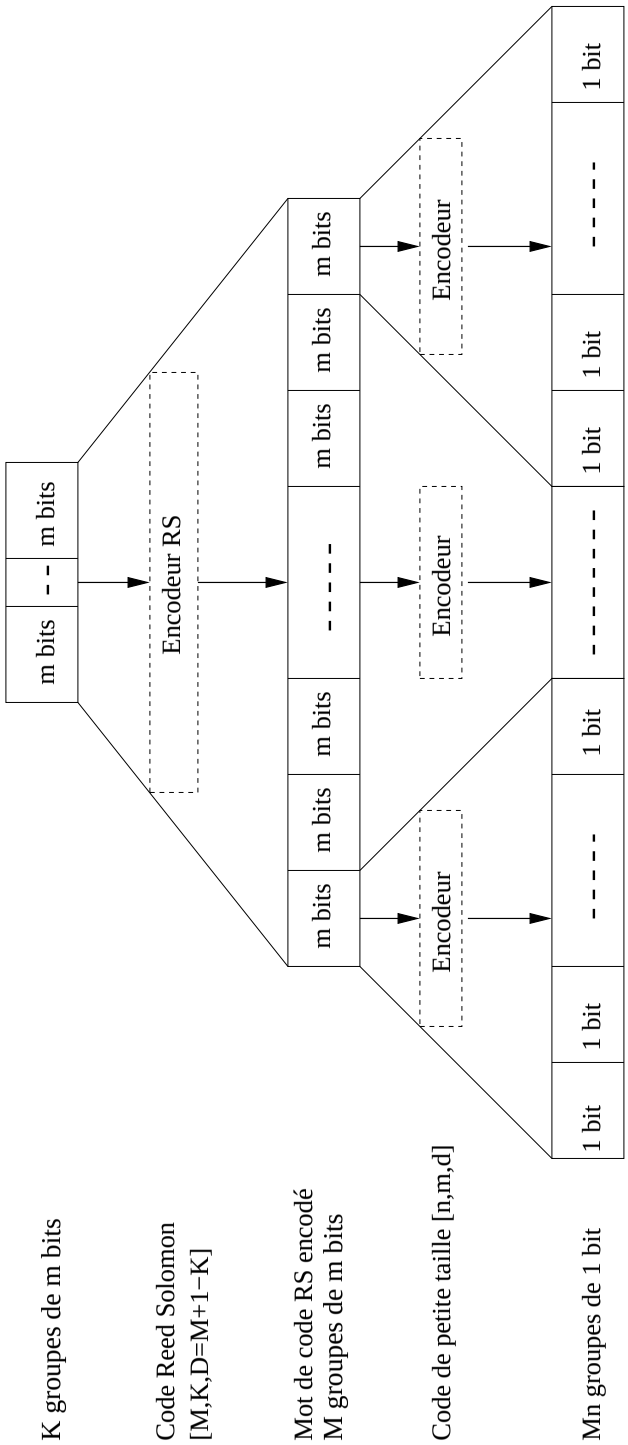


FIG. 6.5 – Principe de la concaténation du code de Reed Solomon avec un autre code

teur d'étalement étant de

$$N = \frac{Mn}{Km} = \frac{63 \times 144}{48 \times 6} = 31,5.$$

Le code concaténé résultant de ces deux codes a pour paramètres $[9072, 288]$.

Pour le code de Reed Solomon sur $\mathbb{F}_{2^8}$, le code utilisé a pour paramètres $[255, 192, 64]$ et le code de petite dimension a pour paramètres $[192, 8, 96]$. Le code concaténé issu de ces deux codes a pour paramètres $[48960, 1536]$ et pour facteur d'étalement

$$N = \frac{Mn}{Km} = \frac{255 \times 192}{192 \times 8} = 31,875.$$

Le décodage de ce code concaténé se fait, d'une part, en décodant le code de petite dimension de manière exhaustive, d'autre part, en décodant le code de Reed Solomon. Le décodage de ce dernier se fait en s'appuyant sur la structure algébrique du code et utilise les polynômes localisateurs et évaluateurs, ainsi que l'algorithme d'Euclide étendu, voir la thèse de N. Sendrier [46] pour le détail de l'algorithme. Il est à noter que le décodage du code de Reed Solomon est un décodage dur.

La figure (6.6) représente le TEB d'un utilisateur en mode CDMA en fonction du nombre total d'utilisateurs interagissant et du code utilisé. Pour un TEB maximum fixé a 10^{-3}, nous avons alors au maximum 7 utilisateurs qui peuvent interagir dans le cas de l'utilisation du code à répétition. Dans le même temps, pour l'utilisation du code de Reed Solomon sur $\mathbb{F}_{2^6}$ avec son code de petite dimension correspondant, nous avons au maximum 18 utilisateurs qui peuvent interagir et, dans le cas du Reed Solomon sur $\mathbb{F}_{2^8}$, nous en avons 21, soit trois fois plus que dans le cas du code à répétition. Notons que nous avons atteint la moitié de la limite théorique concernant le nombre maximum d'utilisateurs pouvant interagir pour un TEB aussi petit que l'on veut.

Nous présentons le TEB d'une liaison à spectre étalé en fonction du rapport utile signal à bruit sur la figure (6.4). Ainsi, pour un TEB fixé à 10^{-3}, un rapport signal à bruit de 6,75 dB est nécessaire pour atteindre cette borne lors de l'utilisation du code à répétition, tandis qu'un rapport utile de 2,81 dB est nécessaire pour le code de Reed Solomon sur $\mathbb{F}_{2^6}$ concaténé avec le code de petite dimension. Le gain est de 3,94 dB ; toutefois la limite de Shannon pour un code de rendement de 1/31 étant à -1,49 dB, ce code se trouve donc à 4,3 dB de la borne de Shannon. En ce qui concerne le code de Reed Solomon sur $\mathbb{F}_{2^8}$, il nécessite un rapport utile signal à bruit de 1,92 dB, ce qui fait un gain par rapport au code à répétition de 4,83 dB. Mais ce code se trouve encore à 3,41 dB de la borne de Shannon.

Le code permettant d'avoir un nombre d'utilisateurs maximum pouvant interagir, supérieur à la moitié de la borne théorique et étant à près de 3 dB de la limite de Shannon, est le code concaténé résultat du code de Reed Solomon sur $\mathbb{F}_{2^{10}}$ ayant pour paramètres [1023, 768, 256] avec le code binaire

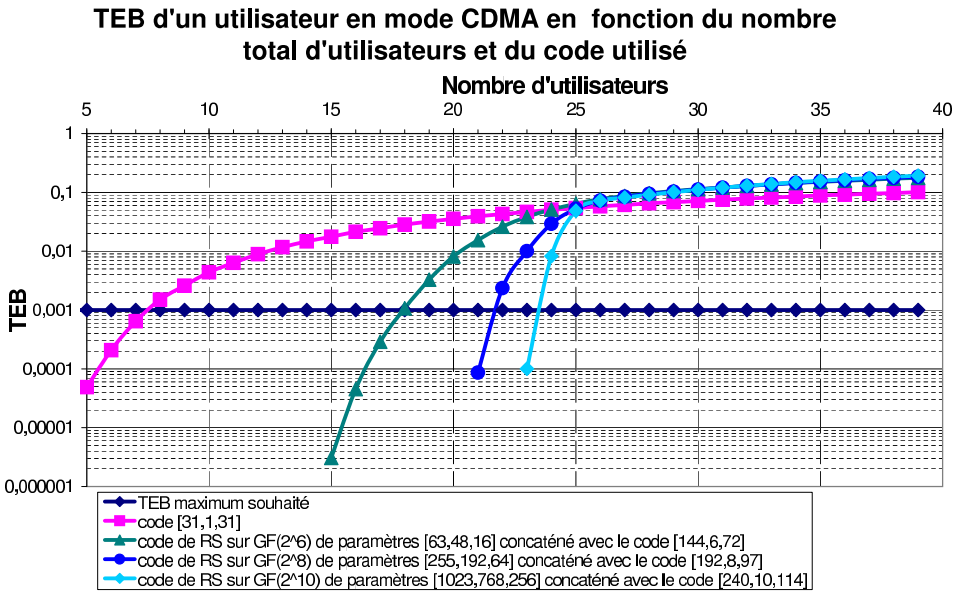


FIG. 6.6 – Taux d'erreur binaire en fonction du nombre d'utilisateurs et du code utilisé

[240,10,114]. En effet, comme nous pouvons le voir sur la figure (6.4), le nombre maximum d'utilisateurs pouvant interagir avec un TEB résiduel de 10^{-3} est de 23 et il se trouve à 3,06 dB de la limite de Shannon. Toutefois, pour décoder ce code, $2^{10} = 1024$ accumulateurs et portes logiques sont nécessaires. Cela est assez conséquent et hors d'atteinte pour une utilisation pratique car trop coûteux financièrement.

Ce code concaténé est très intéressant en terme de nombre maximum d'utilisateurs mais son utilisation a un inconvénient en terme de décodage. En effet, comme nous l'avons précisé précédemment, le décodage du code de Reed Solomon est un décodage dur ; or ce décodeur se trouve en aval, dans la chaîne de transmission, des décodeurs du bloc "décodage canal" et les performances de ces derniers en terme de TEB seront dégradées par cette sortie dure. C'est pour cela que nous proposons dans le chapitre suivant de regrouper les blocs "décodage canal" et "étalement de spectre" et d'utiliser un code concaténé similaire à celui que nous venons de décrire et qui jouera le rôle des codes correcteurs d'erreurs contenus dans ces deux blocs.

6.3 Synchronisation

Dans cette section, nous proposons un principe basé sur les codes correcteurs d'erreurs pour maintenir la synchronisation.

Pour cela, reprenons d'abord le principe de l'émetteur que nous avons décrit à la fin du chapitre 2, à la figure (2.7). Nous rappelons que le système fonctionne en modulation de phase. Avant que la porteuse du signal ne soit déphasée par la séquence d'étalement, nous pouvons considérer le signal comme un signal en modulation BPSK. Considérons désormais que nous n'avons plus une modulation BPSK mais une modulation QPSK définie de la manière suivante.
Sur la voie I, le bit d'information est émis, comme à l'accoutumée, avec une amplitude égale à A.
Sur la voie Q, le bit 0 est émis avec une amplitude égale à $\frac{A}{10}$; c'est le code à répétition de dimension 1 qui est utilisé .
Ainsi, le déphasage de la porteuse n'est plus de 0 ou π mais de θ ou $\pi - \theta$, avec $\theta = \arctan\left(\frac{1}{10}\right)$, suivant que le bit émis soit 0 ou 1. Après ce déphasage, vient le déphasage dû à la séquence d'étalement. Le code utilisé sur la voie I est un code de paramètre $[kN, k]$ où N est le facteur d'étalement du système. Tandis que le code utilisé sur la voie Q est le code à répétition de paramètres $[kN, 1, kN]$. Le code à répétition a un rendement de code plus faible que le code utilisé sur la voie I. Ainsi, il peut fonctionner dans un bruit ambiant plus important que l'autre code pour une même amplitude d'émission des deux codes. C'est pour cette raison que l'amplitude d'émission du code à répétition est moins forte que celle du code de paramètres $[kN, k]$. D'une part, le code de la voie I n'est que très peu perturbé par l'émission du code à répétition sur la voie Q. D'autre part, le fonctionnement de ce dernier n'est que très peu perturbé par le niveau de bruit dû à l'émission du code de la voie I.

A la réception, après multiplication par le conjugué de la séquence d'étalement correspondante, nous avons à décoder deux codes. L'un de ces codes se trouve sur la voie I, partie réelle : c'est le code qui correspond à nos données émises. L'autre code se trouve sur la voie Q, partie imaginaire : c'est le code qui va permettre la synchronisation. Ce dernier code est de longueur N, le facteur d'étalement. Dans le cas où la valeur issue du décodeur est le bit 0, cela signifie que l'émetteur et le récepteur sont synchronisés ou peu désynchronisés. Dans ce cas de figure, il n'y a pas de modifications à effectuer. Dans le cas où le bit décodé est le bit 1, cela signifie qu'il y a un risque de forte désynchronisation. Toutefois, il est nécessaire de regarder si ce phénomène est le même sur les 5 à 10 bits suivants. Si c'est bien le cas, un déphasage de quelques degrés s'impose. Si le cas est isolé, c'est qu'il est dû au bruit des autres utilisateurs plutôt qu'à une désynchronisation de l'émetteur et du récepteur, d'où l'utilité de regarder ce phénomène sur plusieurs bits avant de faire un déphasage de quelques degrés.

La figure (6.7) donne les TEB d'une liaison à spectre étalé en fonction

du maintien de la synchronisation. Nous constatons que cette méthode est appropriée, puisque les courbes représentant le taux d'erreur, dans le cas idéal et dans le cas de maintien de synchronisation, sont confondues.

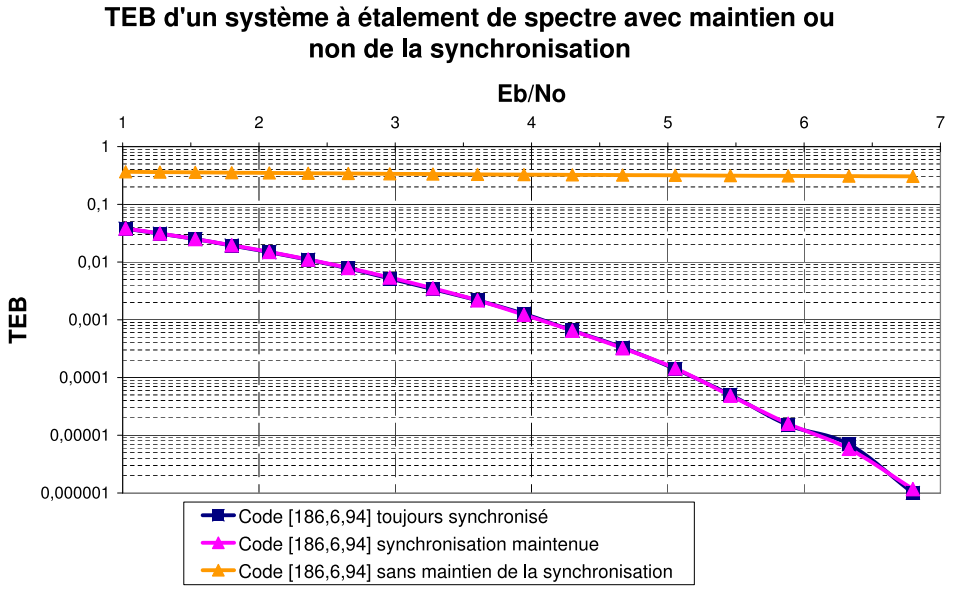


FIG. 6.7 – Taux d'erreur binaire en fonction de la synchronisation ou non entre l'émetteur et le récepteur.

Chapitre 7

Présentation et résultats du bloc "codage et étalement"

Dans ce chapitre, nous nous proposons de regrouper les blocs "codage canal" et "étalement de spectre" de la chaîne de transmission pour n'en faire qu'un seul, nommé "codage et étalement", et de le simuler. Nous avons remarqué que, dans le bloc "étalement de spectre", l'utilisation de codes correcteurs était nécessaire. Ces codes ont un rendement égal à l'inverse du facteur d'étalement N. De plus, des codes correcteurs sont utilisés dans le bloc "codage canal" ayant des rendements bien spécifiques. Ainsi, en regroupant les deux blocs, nous obtenons un code concaténé résultat des codes utilisés dans chacun des deux blocs. Ce code concaténé a pour rendement le produit des rendements des codes utilisés : dans notre étude, il est fixé à $\frac{1}{93}$. Nous allons donc simuler cette chaîne de transmission modifiée avec des codes ayant pour rendement total $\frac{1}{93}$. Le TEB maximum sera fixé à 10^{-6}, car c'est le TEB maximum souhaité en sortie du bloc "décodage canal" dans la littérature.

Dans une première section, nous donnerons la construction d'un code concaténé, ayant le rendement souhaité, se constituant d'un code de Reed Solomon concaténé avec un code convolutif et un code de petite dimension. Puis, dans une seconde section, nous utiliserons un code de Reed Muller d'ordre 1 ayant le rendement souhaité qui est le code $RM(1, 10)$ et nous ferons une comparaison de ces deux codes.

7.1 Code concaténé

Nous nous intéressons tout d'abord à la définition des codes convolutifs puis à la présentation du code concaténé utilisé dans le bloc "codage et étalement".

7.1.1 Les codes convolutifs

Les codes convolutifs constituent l'une des principales familles de codes correcteurs d'erreurs, une introduction à ces codes est donnée dans [47]. Dans un code convolutif, chaque bloc de n éléments en sortie du décodeur dépend non seulement du bloc composé des k éléments positionnés à l'entrée du décodeur mais aussi des m blocs précédents. Cette famille de codes fait appel à un effet de mémoire d'ordre m et la quantité $(m+1)$ s'appelle la longueur de contrainte K du code. De même que pour les codes en blocs, le rendement du code est défini par $R = \frac{k}{n}$. De plus, si les k éléments d'information présents à l'entrée du codeur sont effectivement transmis, le code est dit systématique.

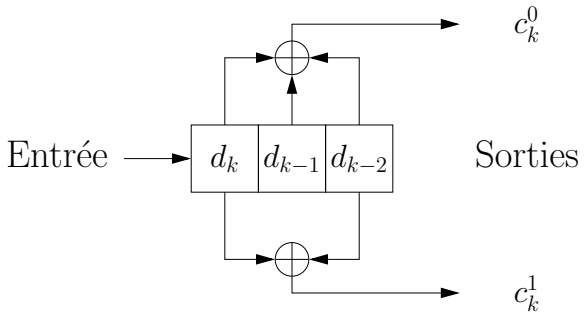


FIG. 7.1 – Exemple de codeur convolutif non systématique.

La figure (7.1) présente l'exemple d'un codeur convolutif de rendement $R = \frac{1}{2}$ et de longueur de contrainte $(m+1) = 3$. Ce codeur accepte en entrée des blocs de $k = 1$ bit et en sortie des blocs de $n = 2$ bits.

Chacune des sorties du codeur est égale au produit de convolution entre la suite binaire présente à l'entrée du codeur et la réponse de ce même codeur définie par ses séquences génératrices. Pour l'exemple de la figure (7.1), ces séquences sont données par :

$$\forall i \in \{0,1\},\ g_i = [g_{i0}, g_{i1}, g_{i2}]$$

avec

$$\forall i \in \{0,1\},\ c_k^i = \sum_{j=0}^{2} g_{ij} d_{k_j} \text{ et } g_{ij} \in \{0,1\}.$$

Les séquences génératrices sont fréquemment exprimées en octal, ce qui dans le cas de la figure (7.1), donne

$$\left\{ \begin{array}{lcll} g_0 & = & [1,1,1] & = & \langle 7 \rangle \\ g_1 & = & [1,0,1] & = & \langle 5 \rangle. \end{array} \right.$$

Remarquons que les sorties du codeur étant égales à des combinaisons linéaires des éléments d'information présents à l'entrée du codeur convolutif,

le code est nécessairement linéaire.

On peut également définir les codes convolutifs en considérant leurs polynômes générateurs qui s'expriment en fonction de la variable de retard usuel D. Toujours dans le cadre de notre exemple, les polynômes générateurs ont pour forme générale

$$\begin{cases} G_0 &= g_{00} + g_{01}D + g_{01}D^2 \\ G_1 &= g_{10} + g_{11}D + g_{11}D^2 \end{cases}$$

ou encore

$$\begin{cases} G_0 &= 1 + D + D^2 \\ G_1 &= 1 + D^2. \end{cases}$$

La représentation des codes convolutifs par des polynômes ou des matrices n'est pas réellement adaptée au décodage. Aussi pour réaliser les décodeurs, on utilise des représentations graphiques de ces codes, de type diagramme en arbre, diagramme d'état ou de treillis, voir [48]. La représentation en treillis est très efficace pour le décodage car elle est parfaitement adaptée aux algorithmes de décodage tel que l'algorithme de Viterbi [47, 48].

7.1.2 Code concaténé issu d'un code Reed Solomon avec un code convolutif et un code de petite dimension

Le principe de concaténation que nous proposons dans cette section est le même que celui que nous avons proposé dans la figure (6.5). Le code le plus externe est le code de Reed Solomon, le code le plus interne est le code de petite dimension, tandis que le code convolutif se situe au milieu.

Pour obtenir un code concaténé résultat ayant un rendement de $\frac{1}{93}$, nous avons pris les codes définis précédemment avec pour paramètres :

- $[63, 42, 9]$ pour le code de Reed Solomon sur $\mathbb{F}_{2^6}$,
- $G_0 = 1 + D + D^2 = \langle 7 \rangle$ et $G_1 = 1 + D^2 = \langle 5 \rangle$ pour le code convolutif binaire de rendement $\frac{1}{2}$,
- $[186, 6, 94]$ pour le code binaire de petite dimension.

Puis, n'ayant pas de contraintes sur les codes, si ce n'est le rendement du code concaténé, nous avons choisi d'étudier le comportement du code concaténé résultant des codes définis précédement et ayant pour paramètres :

- $[63, 55, 9]$ pour le code de Reed Solomon sur $\mathbb{F}_{2^6}$,

- $G_0 = 1 + D + D^2 = \langle 7 \rangle$ et $G_1 = 1 + D^2 = \langle 5 \rangle$ pour le code convolutif binaire de rendement $\frac{1}{2}$,
- $[240, 6, 120]$ pour le code binaire de petite dimension.

Les décodeurs utilisés sont :
- le décodeur souple présenté dans la thèse de S. Jacq [7], dont les principales propriétés sont rappelées dans le chapitre 1 section 3 "Décodage souple" pour le code de petite dimension,
- le décodeur de Viterbi sur les treillis avec sortie souple pour le code convolutif,
- le décodeur pour le code de Reed Solomon est le même que celui utilisé dans le chapitre précédent qui s'appuie sur la structure algébrique du code et utilise les polynômes localisateurs et évaluateurs ainsi que l'algorithme d'Euclide étendu qui est présenté dans la thèse de N. Sendrier [46].

Les résultats de simulations sont donnés en figure (7.2), nous commenterons ces résultats et les comparerons au code de Reed Muller dans la section suivante.

7.2 Codes de Reed Muller

Rappelons pour commencer, la définition des codes de Reed Muller avant de donner les résultats de notre étude avec le code $\mathcal{RM}(1, 10)$.
La construction et les propriétés des codes de Reed Muller sont données par Muller [49] en 1954. La même année, un algorithme de décodage à vote majoritaire est décrit par Reed [50]. Ces codes sont certains sous-espaces de l'espace binaire $\mathcal{B}_m$, où $\mathcal{B}_m = \{f | f : \mathbb{F}_2^m \to \mathbb{F}_2\}$. $\mathcal{B}_m$ est un espace vectoriel de dimension 2^m sur $\mathbb{F}_2$. Par conséquent, nous pouvons identifier $\mathcal{B}_m$ avec $\mathbb{F}_2^{2^m}$. En effet, chaque élément $(x_1, x_2, \ldots, x_m)$ de $\mathbb{F}_2^m$ peut être vu comme l'écriture binaire d'un nombre entre 0 et $2^m - 1$ en utilisant la correspondance suivante :

$$(x_1, x_2, \ldots, x_m) \leftrightarrow x_1 + 2x_2 + 2^2 x_3 + \cdots + 2^{m-1} x_m.$$

Cette correspondance nous donne la relation d'ordre naturelle sur le m-uplet. Et nous pouvons donc identifier la fonction $f \in \mathcal{B}_m$ avec le vecteur de $\mathbb{F}_2^{2^m}$:

$$(f(x_1, x_2, \ldots, x_m); (x_1, x_2, \ldots, x_m) \in \mathbb{F}_2^m).$$

Par la suite, $\mathbf{f}$ désignera la fonction f lorsque nous la regardons comme vecteur de $\mathbb{F}_2^{2^m}$. Les fonctions $f \in \mathcal{B}_m$ sont des fonctions polynomiales booléennes à m variables pouvant s'écrire sous la forme

$$f(x_1, x_2, \ldots, x_m) = \sum_{(a_1, \ldots, a_m) \in \mathbb{F}_2^m} c_{(a_1, \ldots, a_m)} x_1^{a_1} \ldots x_m^{a_m}$$

avec $c_{(a_1,\ldots,a_m)} \in \mathbb{F}_2$.

Exemple 1 *La fonction $f \in \mathcal{B}_2$ définie par $f(0,0) = 0$, $f(1,0) = 1$, $f(0,1) = 1$ et $f(1,1) = 0$ est identifiée par le vecteur $\mathbf{f} = (0,1,1,0)$ de $\mathbb{F}_2^4$.*

Le code de Reed Muller d'ordre r et de longueur $n = 2^m$, noté $\mathcal{RM}(r,m)$, est le code linéaire défini par :

$$\mathcal{RM}(r,m) = \{\mathbf{f} \in \mathcal{B}_m | deg(f) \leq r\},$$

ayant pour dimension $k = \sum_{i=0}^{r} \begin{pmatrix} m \\ i \end{pmatrix}$ et pour distance minimale $d = 2^{m-r}$. De par la définition des $\mathcal{RM}(r,m)$, les bits d'informations ne sont que les coefficients binaires de la fonction polynomiale booléenne. Ainsi, chaque coefficient binaire $c_{(a_1,\ldots,a_m)}$, ayant $s \leq r$ éléments a_i non nuls, donne $\begin{pmatrix} m \\ s \end{pmatrix}$ bits d'informations d'ordre s.

Dans le cadre de notre étude, nous nous sommes intéressés au $\mathcal{RM}(1,10)$. En effet, ce code a pour paramètres [1024,11,512] et un rendement d'environ 1/93. L'algorithme de décodage utilisé est l'algorithme utilisant la transformée de Hadamard rapide, présenté dans [51] et [52].

Les résultats obtenus lors de nos simulations sont donnés en figure (7.2). Dans le cas du code concaténé avec le code de petite dimension ayant pour paramètres $[240, 6, 120]$, nous avons, pour un TEB inférieur à 10^{-6}, au plus 31 utilisateurs qui peuvent cohabiter sur la même bande de fréquence. Tandis qu'avec le code concaténé, dont les paramètres du code de petite dimension sont $[186, 6, 94]$, nous n'obtenons que 30 utilisateurs.

Dans le cas du code $\mathcal{RM}(1,10)$, nous avons un maximum de 29 utilisateurs pouvant interagir ensemble. Ainsi, le code le plus intéressant pour notre étude est le code concaténé dont le code de petite dimension a pour paramètres $[240, 6, 120]$. Cependant, ce code n'est peut être pas le plus performant des codes concaténés issus de cette construction. En effet, nous n'avons testé que deux codes issus de cette construction. Il est nécessaire d'approfondir cette voie et de déterminer quels sont les paramètres des codes de Reed Solomon, du code convolutif et du code de petite dimension qui maximisent le nombre d'utilisateur pour un TEB fixé à 10^{-6}. Notons que pour un TEB de 10^{-5} le code qui conviendrait est le code $\mathcal{RM}(1,10)$. Les performances des deux codes concaténés se dégradent vite car à partir d'un certain niveau de bruit, trop de symboles du code de Reed Solomon sont erronés et l'algorithme de décodage du code de Reed Solomon ne corrige plus d'erreur. D'où une perte flagrante d'efficacité par rapport au code de Reed Muller.

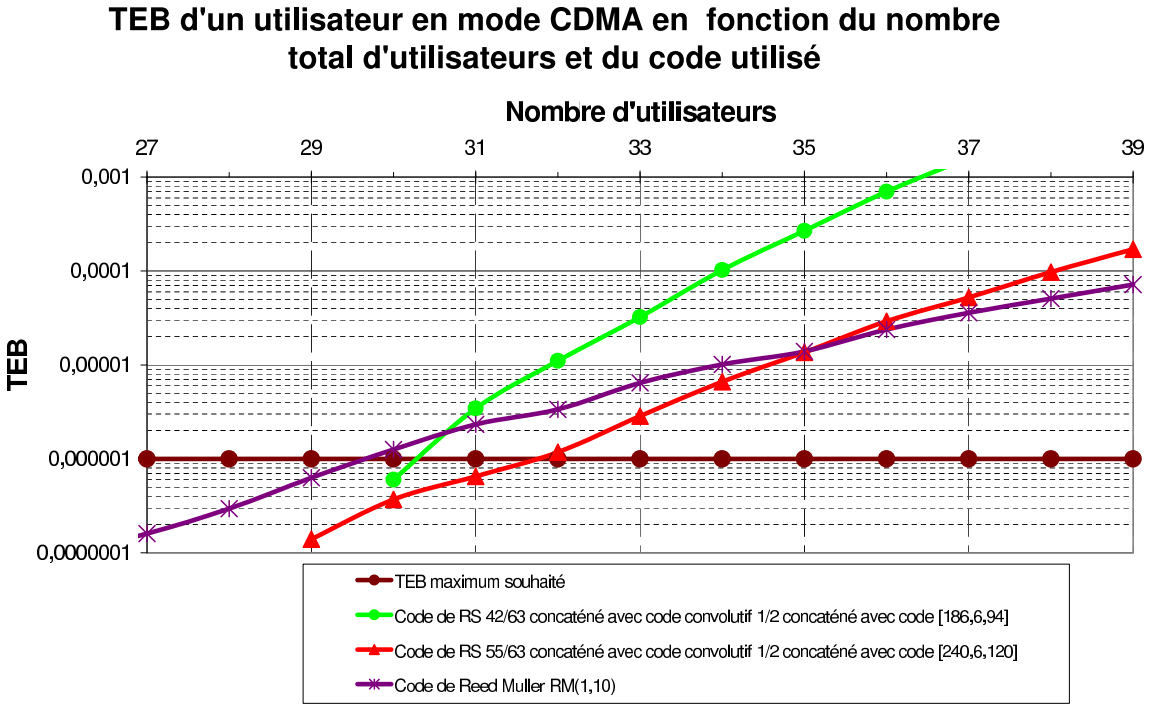


FIG. 7.2 – Courbes de simulation de la chaîne de transmission modifiée ayant les blocs “étalement de spectre” et “codage canal” regroupés.

Conclusion

Ce travail de thèse a permis de trouver plusieurs améliorations possibles de l'étalement de spectre grâce à l'utilisation de codes correcteurs d'erreurs.

Ce manuscrit montre que l'une de ces premières améliorations concernant l'étalement de spectre et le CDMA est l'utilisation de séquences d'étalement aléatoires à déphasage multiple. En effet, l'utilisation de ces séquences permet un gain de 4 utilisateurs sur les séquences aléatoires binaires et de 3 sur les séquences de Gold, sachant que le nombre maximum d'utilisateurs pouvant interagir en utilisant des séquences aléatoire à déphasage multiple, et dans les conditions que nous nous sommes fixés, est de 7 utilisateurs. Ces gains sont valables aussi bien pour le cas synchrone que pour le cas asynchrone.

La discrétisation du temps bit T_b en temps chip T_c, qui est le temps de base du système, a permis de montrer l'utilisation de manière implicite d'un code à répétition dans l'étalement de spectre. Les performances de cet étalement, en terme de TEB, peuvent être améliorées en choisissant des codes plus adaptés que le code à répétition tout en respectant les contraintes du système tel le débit d'information.

Ainsi, dans l'objectif d'une réalisation pratique, nous donnons dans ce mémoire des codes qui peuvent être utilisés à la place du code à répétition et qui satisfont aux contraintes du système. De plus, nous donnons les gains obtenus par rapport au code à répétition. Le décodage utilisé pour ces codes est un décodage exhaustif à maximum de vraisemblance qui fonctionne en temps réel grâce à la mise en parallèle des calculs. Cette mise en parallèle apporte un surcoût financier qui est minimisé par un choix convenable des codes.

Par ailleurs, nous proposons l'utilisation d'une méthode utilisant des codes correcteurs d'erreurs pour synchroniser l'émetteur et le récepteur.

Dans un souci d'efficacité et de simplicité de la chaîne de transmission, nous avons regroupé les deux blocs utilisant des codes correcteurs d'erreurs en un seul bloc. En effet, des codes correcteurs d'erreurs sont utilisés dans deux blocs successifs "codage canal" et "étalement de spectre" de la chaîne de transmission. Dans le cadre de ce regroupement, nous donnons des codes qui peuvent être utilisés pour ce bloc. Le code le plus performant parmi les trois que nous avons utilisé est un code concaténé dont le principe est défini dans ce manuscrit.

Toutefois, comme très peu de codes concaténés issus de cette consctuc-

tion ont été expérimentés, il est nécessaire de poursuivre cette étude pour déterminer les paramètres des trois codes constituant le code concaténé qui maximise le nombre d'utilisateurs. Ceci tout en respectant les contraintes que nous nous sommes fixées. De plus, il serait intéressant de déterminer si les constructions des codes présentés dans ce manuscrit sont les plus appropriées en terme de TEB pour des codes de très petit rendement. Ou si d'autres codes, comme les codes de Reed Muller qui se décodent rapidement, ne sont pas plus adaptés ?

Annexe A

Code CORTEX

Cette partie présente les codes CORTEX avec nos résultats de simulation. Nous pensions que ces codes seraient intéressants mais, à la vue des résultats de simulation, ce n'est pas le cas. Nous verrons pourquoi en fin de cette annexe.

Définissons tout d'abord les codes CORTEX, puis donnons les motivations qui nous ont amené à les utiliser. Enfin, présentons pour finir les résultats de nos simulations.

Les codes CORTEX furent introduits pour la première fois par J.C. Carlach et C. Vervoux [53] dans le cas binaire. A. Otmani [54, 55] en donne la définition sur un corps fini $\mathbb{F}$ quelconque ayant q éléments.

Définition 14 *Soit $\mathcal{B}$ un code linéaire de dimension k_b, de rendement 1/2 sur un corps $\mathbb{F}$ et ayant une matrice génératrice dont P_b est sa partie redondante. Soit e un entier $e \geq 1$; posons $k = ek_b$ et $P = I_e \otimes P_b$. Soit $\Pi = (\Pi_1, \ldots, \Pi_s)$ une suite de permutations de $\mathfrak{S}_k$. Le Code CORTEX $C_k(B, \Pi)$ construit à partir du code de base $\mathcal{B}$ suivant sa suite de permutations $\Pi_1, \ldots, \Pi_s$ est l'ensemble des mots $(m, R^{(s)}(m))$ lorsque m décrit l'espace $\mathbb{F}^{k_b}$.*

$\otimes$ désigne le produit de Kronecker de I_e par P_b.

Exemple 2 *Considérons le code binaire $\mathcal{H}_2$ ayant une matrice génératrice sous forme systématique telle que la partie redondante soit :*

$$\mathcal{R}_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Le code CORTEX construit à partir de ce code suivant la transposition (1,3) répétée deux fois, est le code de Hamming étendu de paramètres [8,4,4]. La figure (A.1) donne la représentation graphique associée à cette construction du code de Hamming sous forme de code CORTEX.

A. Otmani dans [54] propose un algorithme de décodage itératif, pour les codes CORTEX, sur un canal gaussien. En effet, de par leur structure, les

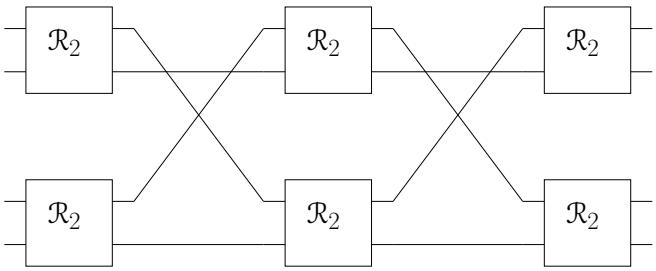


FIG. A.1 – Code de Hamming étendu de paramètres [8,4,4].

codes CORTEX binaires se prêtent très bien au décodage itératif car plusieurs codes de petites longueurs sont mis en relation pour permettre un échange de bits. Chaque boîte $\mathcal{B}$ peut communiquer avec les autres codes de base auxquels elle est liée pour leur donner l'information extrinsèque calculée au niveau du code $\mathcal{B}$. Les autres codes de base considèreront cette donnée comme de l'information "a priori" pour calculer à leur tour leur propre information extrinsèque pour chaque bit. Cet algorithme de décodage a besoin tout au long de son déroulement de données bruitées provenant du canal. Dans le cas des codes CORTEX à plus de trois niveaux, les codes de base qui ne sont pas sur la première ni la dernière couche ne voient aucun de ces bits transmis à travers le canal, tandis que pour ceux des couches externes seulement la moitié est transmise. Il est donc nécessaire de "simuler" pour ces bits une transmission à travers le canal gaussien en supposant que les données reçues à la sortie du canal sont nulles.

Cet algorithme ne donne malheureusement pas de très bons résultats. Cela est en partie dû au fait que les codes CORTEX considérés ont une très mauvaise distance minimale. Le nombre de permutations a un effet dégradant si celui-ci augmente. Ce phénomène est compréhensible car, lorsque le nombre de permutations est plus grand que deux, le nombre de symboles internes non-transmis, et donc initialisés à zéro, est supérieur au nombre de symboles reçus. Il est donc impossible de corriger autant de symboles inconnus uniquement à partir des symboles transmis, dont certains sont erronés. De plus, ce phénomène est prévisible d'après les travaux de G. Olocco et J.P. Tillich [56] qui montrent que les performances du décodage itératif sur un canal à effacement se dégradent de manière drastique au-delà de deux permutations.

Dans le cadre de notre étude, nous nous sommes intéressés à la construction d'un code CORTEX ayant 29 permutations. Sans modification de ce code ni du décodeur précédemment défini, nous savons d'après les travaux de A. Otmani, que le décodage ne sera pas performant du fait du nombre important de permutations et de bits internes inconnus. Toutefois, au lieu de ne transmettre sur le canal gaussien que les bits externes, nous nous sommes proposés de transmettre aussi les bits internes entrant dans chaque boîte $\mathcal{B}$. Ainsi, lors du décodage, les bits des blocs internes ne sont plus initialisés à zéro mais

à la valeur obtenue lorsque ceux-ci ont été transmis dans le canal. Dans ces conditions, le rendement du code considéré n'est plus de 1/2 mais de 1/31.

Exemple 3 *Considérons le code CORTEX défini dans l'exemple précédent et regardons sur la figure (A.2) les bits d'entrées et de sorties de tous les blocs* $\mathcal{B}$ *lorsque les bits d'information sont 1, 0, 1, 1.*

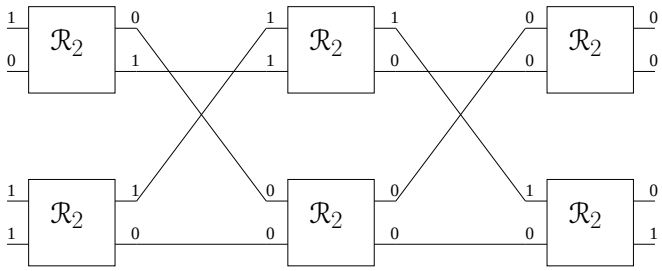


FIG. A.2 – Construction du mot du code CORTEX ayant pour bits d'information $(1, 0, 1, 1)$

Pour le code CORTEX considéré le mot émis sera $(1, 0, 1, 1, 0, 0, 0, 1)$ *qui est de rendement 1/2 tandis que, dans notre cas, ce sera le mot* $(1, 0, 1, 1, 1, 1, 0, 0, 0,\ 0, 1, 0, 0, 0, 0, 1)$ *qui est de rendement 1/4.*

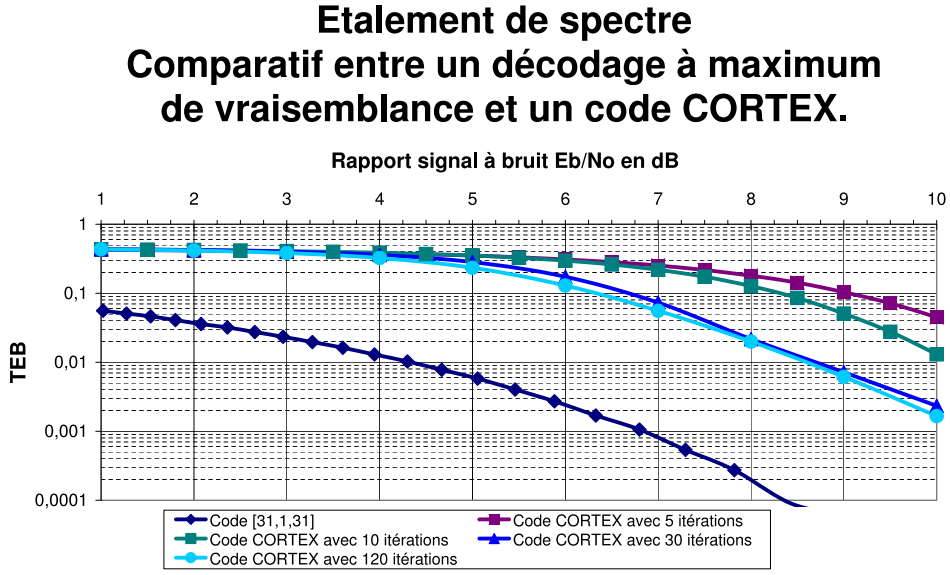


FIG. A.3 – Comparatif du TEB en mode étalement de spectre entre l'utilisation du code à répétition et un code CORTEX de même rendement.

Ces résultats ne sont en aucune manière concluants. En effet, la figure (A.3) présente les résultats de nos simulations ayant

pour code de base le code de Hamming étendu et la permutation $(0, 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15)$. Les courbes de TEB sont au-dessus du cas non codé et ceci, quelque soit le nombre d'itérations choisies. Ce qui est hors d'intérêt pour notre utilisation. Cela est dû en partie aux données reçues qui sont issues des bits internes et qui n'apportent aucune amélioration pour l'algorithme, voir même le dégrade.

Annexe B

Matrices génératrices des codes binaires utilisés

Dans cette annexe, sont référencées les matrices génératrices des codes de petite dimension donnés dans ce manuscrit. Ces matrices sont obtenues à l'aide du programme MAGMA [57], en utilisant la commande "BDLC" (Best Dimension Linear Code). Les entrées de cette commande sont au nombre de trois : la première correspond au corps sur lequel le code est défini ; la seconde est la longueur du code ; la troisième est la distance minimale du code. La sortie est la matrice génératrice d'un code en bloc sur $\mathbb{F}_q$ ayant la plus grande dimension et vérifiant les contraintes de longueur et de distance minimale.

Code [62,6,31]

$$M = \begin{pmatrix} 10010101011010010110101010010101011010101001011010010101011010 \\ 01011001101001011010011001011001101001100101101001011001101001 \\ 00111100001111000011110000111100001111000011110000111100001111 \\ 00000011111111000000001111111100000000111111110000000011111111 \\ 00000000000000111111111111111100000000000000001111111111111111 \\ 00000000000000000000000000000011111111111111111111111111111111 \end{pmatrix}$$

Code [62,8,28]

$$M = \begin{pmatrix}
10000000101100000100000101000011111110011010011100101001111011 \\
01000000101011101001011110100011101100000011101000011000011110 \\
00100000101000011111110011010011100101001111010010000000101101 \\
00010000010100001111111001101001110010100111101001000000010111 \\
00001000110111101100100000110110101010011101010010101100101000 \\
00000100011011110110010000011011010101001110101001010110010100 \\
00000010001101111011001000001101101010100111010100101011001010 \\
00000001111011010110111000000100100110011101001100011001000111
\end{pmatrix}$$

Code [186,6,94]

$$M = \begin{pmatrix}
10011001100110011001100110011001100110011001100110011001100110 \\
01100110011001100110011001100110011001100110011001100110011001 \\
10011001100110011001100110011001100110011001100110011001100111 \\
\\
01010010101010101010110101010010101101010101010101001010101001 \\
11100001111000011110000111100001111000011110000111100001111000 \\
01111000011110000111100001111000011110000111100001111000011111 \\
\\
00101010110100101101010100101011010101001011010010101011010000 \\
00011111111000000001111111100000000111111110000000011111111000 \\
00000111111110000000011111111000000001111111100000000111111111 \\
\\
00000111111110000000011111111000000111111110000000011111111000 \\
00000000000111111111111111100000000000000000111111111111111000 \\
00000000000001111111111111110000000000000000011111111111111110 \\
\\
00000000000001111111111111110000000000000000111111111111111000 \\
00000000000000000000000000111111111111111111111111111111111000 \\
00000000000000000000000000011111111111111111111111111111111110 \\
\\
00000000000000000000000000011111111111111111111111111111111000 \\
00000000000000000000000000000000000000000000000000000000000111 \\
11111111111111111111111111111111111111111111111111111111111110
\end{pmatrix}$$

Code [248,8,124]

$$M = \begin{pmatrix}
10010110011010010110100110010110011010011001011010010110011010 \\
01101001100101101001011001101001100101100110100101101001100101 \\
01101001100101101001011001101001100101100110100101101001100101 \\
10010110011010010110100110010110011010011001011010010110011010 \\
\\
01010101010101010101010101010101010101010101010101010101010101 \\
01010101010101010101010101010101010101010101010101010101010101 \\
01010101010101010101010101010101010101010101010101010101010101 \\
01010101010101010101010101010101010101010101010101010101010101 \\
\\
00110011001100110011001100110011100110011001100110011001100110011 \\
00110011001100110011001100110011100110011001100110011001100110011 \\
00110011001100110011001100110011100110011001100110011001100110011 \\
00110011001100110011001100110011100110011001100110011001100110011 \\
\\
00001111000011110000111100001111111100001111000011110000111100 \\
00001111000011110000111100001111111100001111000011110000111100 \\
00001111000011110000111100001111111100001111000011110000111100 \\
00001111000011110000111100001111111100001111000011110000111100 \\
\\
00000000111111110000000011111111111111110000000011111111000000 \\
00000000111111110000000011111111111111110000000011111111000000 \\
00000000111111110000000011111111111111110000000011111111000000 \\
00000000111111110000000011111111111111110000000011111111000000 \\
\\
00000000000000001111111111111111111111111111111100000000000000 \\
00000000000000001111111111111111111111111111111100000000000000 \\
00000000000000001111111111111111111111111111111100000000000000 \\
00000000000000001111111111111111111111111111111100000000000000 \\
\\
00000000000000000000000000000000000000000000000000000000000000 \\
11111111111111111111111111111111111111111111111111111111111111 \\
00000000000000000000000000000000000000000000000000000000000000 \\
11111111111111111111111111111111111111111111111111111111111111 \\
\\
00000000000000000000000000000000000000000000000000000000000000 \\
00000000000000000000000000000000000000000000000000000000000000 \\
11111111111111111111111111111111111111111111111111111111111111 \\
11111111111111111111111111111111111111111111111111111111111111
\end{pmatrix}$$

Code [240,6,120]

$$M = \left(\begin{array}{l}
100101100110100110010110011010011010011001011001101001100101 \\
011010011001011001101001100101100101100110100110010110011010 \\
011010011001011001101001100101100101100110100110010110011010 \\
100101100110100110010110011010011010011001011001101001100101 \\
\hline
010101010101010101010101010101010101010101010101010101010101 \\
010101010101010101010101010101010101010101010101010101010101 \\
010101010101010101010101010101010101010101010101010101010101 \\
010101010101010101010101010101010101010101010101010101010101 \\
\hline
001100110011001111001100110011001100110011001111001100110011 \\
001100110011001111001100110011001100110011001111001100110011 \\
001100110011001111001100110011001100110011001111001100110011 \\
001100110011001111001100110011001100110011001111001100110011 \\
\hline
000011110000111111110000111100000011110000111111110000111100 \\
000011110000111111110000111100000011110000111111110000111100 \\
000011110000111111110000111100000011110000111111110000111100 \\
000011110000111111110000111100000011110000111111110000111100 \\
\hline
000000001111111111111111000000000000000011111111111111111000000 \\
000000001111111111111111000000000000000011111111111111111000000 \\
000000001111111111111111000000000000000011111111111111111000000 \\
000000001111111111111111000000000000000011111111111111111000000 \\
\hline
000000000000000000000000000000011111111111111111111111111111111 \\
000000000000000000000000000000011111111111111111111111111111111 \\
000000000000000000000000000000011111111111111111111111111111111 \\
000000000000000000000000000000011111111111111111111111111111111
\end{array}\right)$$

Annexe C

Les programmes en C

Cette annexe donne, pour exemple, les deux types de programmes utilisés lors de cette étude.
Le premier programme nommé “Etalement de spectre” simule l'étalement de spectre avec ajout de bruit blanc gaussien et permet d'avoir un TEB en fonction du rapport signal à bruit $\frac{E_b}{N_0}$.
Le second programme nommé “CDMA” simule le CDMA avec un nombre d'utilisateurs donné en paramètre d'entrée, nous avons dans ce cas un TEB en fonction du nombre d'utilisateurs.
Quant au programme “Bruit Blanc Additif Gaussien”, il prend en entrée la moyenne “mean” et la variance “sigma” d'une distribution gaussienne, et donne en sortie un nombre aléatoire qui suit cette distribution, voir [58] et [59] pour le programme écrit en C.

Etalement de spectre

```
#include <math.h>
#include <stdlib.h>
#include <stdio.h>
#include "type.h"
#include "multipliecomplexe.h"
#include "conjugue.h"
#include "inversecomplexe.h"
#include "sommecomplexe.h"
#include "gngauss.h"
#define PI       3.1415926535897932385
int main (int argc, char *argv[])
{
  int i,j,l,m,M,N,k,n,res,mot;
  int dimechantillon,nberreur,indicereference;
  double distancereference,distance,moyenne,ecart;
  double *tableauvaleursuite;
  char * fichiersortie;
  char * fichierentree;
  complexe *cossin;
  complexe element,somme;
  int **tabmessage;
  complexe *BAM;
  complexe *valeursortie;
  FILE *fiche;
```

```
  FILE *fichs;
  if (argc != 9)
    {
      printf("\n ERREUR, le nombre de variable d'entrée est incorrect. Il faut :
\n- la taille de l'échantillon,\n- la longueur de l'étalement,\n- le nombre de phase,
\n- la moyenne,\n- l'écart type,\n- le nom du fichier d'entrée qui contient le code,
\n- le nom du fichier de sortie,\n- la graine de l'alea.\n");
      return(EXIT_FAILURE);
    }
  /*************************************************************************/
  /*************************** initialisation ******************************/
  /*************************************************************************/

  dimechantillon=atoi(argv[1]); /* taille de l'échantillon */
  k=atoi(argv[2]);              /* la longueur de l'étalement */
  n=atoi(argv[3]);              /* nombre de phases pour la séquence d'étalement */
  fichierentree=argv[6];        /* nom du fichier contenant le code formaté en -1,1 au lieu de 1, 0 */
  fichiersortie=argv[7];        /* nom du fichier de sortie */
  moyenne =atof(argv[4]);       /* valeur moyenne pour le bruit, généralement cette valeur est  0 */
  ecart=atof(argv[5]);          /* valeur de l'écart type */

  fiche=fopen(fichierentree,"r");
  fscanf(fiche,"%d %d",&M,&N);
  tabmessage=(int **) malloc (N * sizeof(int*));
  for (i=0;i<N;i++)
    {
      tabmessage[i]=(int *) malloc (M * sizeof(int));
      for (j=0;j<M;j++)
{
  fscanf(fiche,"%d",&res);
  tabmessage[i][j]=res;
}
    }
  fclose(fiche);
  if (fmod(k,M) != 0)
    {
      printf("\n ERREUR, il faut que le nombre de somme exponentielle soit multiple de M.\n");
      return(EXIT_FAILURE);
    }
  BAM=(complexe *)malloc (N*sizeof(complexe));

  nberreur =0;
  tableauvaleursuite=(double *)malloc(k*sizeof(double ));
  valeursortie=(complexe *)malloc(k*sizeof(complexe));
  cossin=(complexe *)malloc (n*sizeof(complexe ));
  for (i=0;i<n;i++)
    {
      cossin[i].reelle=cos(PI*2*i/n);
      cossin[i].imaginaire=sin(PI*2*i/n);
    }
  srandom(atoi(argv[8]));
  /*************************************************************************/
  /************************ programme principal  ***************************/
  /*************************************************************************/
  for(i=0;i<dimechantillon;i++)
    {
      /*********************************************************/
      /********** initialisation  séquence d'étalement **********/
      /*********************************************************/
      for(l=0;l <k;l++)
        tableauvaleursuite[l]=(random()>> 4) % n;
      /*************************************************************/
      /********************** fin initialisation ********************/
      /*************************************************************/
       mot =rand()%N; /* Choix aléatoire du mot à émettre */
       for (m=0;m<(k/M);m++)
{  /* émission du mot avec ajout de bruit */
```

```
  for (j=0;j<M;j++)
    {
      somme.reelle=tabmessage[mot][j]* cossin[(int)tableauvaleursuite[j+m*M]%n].reelle
                        +gngauss(moyenne,ecart);
      somme.imaginaire=tabmessage[mot][j]* cossin[(int)tableauvaleursuite[j+m*M]%n].imaginaire
                        +gngauss(moyenne,ecart);
      valeursortie[j+m*M]=somme;
    }
}
      /***********************************************/
      /***************** décision ********************/
      /***********************************************/
      for(l=0;l<N;l++)
{
  BAM[l].reelle=0;
  BAM[l].imaginaire=0;
}
      for(j=0;j<k;j++)
{
  element.reelle = -tabmessage[0][j%M];
  element.imaginaire = 0;
  element=sommecomplexe(multipliecomplexe(valeursortie[j],
                          conjugue(cossin[(int)tableauvaleursuite[j]])),element);
  BAM[0].reelle = element.reelle * element.reelle + BAM[0].reelle;
}
      distancereference=BAM[0].reelle;
      indicereference=0;
      for(l=1;l<N;l++)
{
  for(j=0;j<k;j++)
    {
      element.reelle = -tabmessage[l][j%M];
      element.imaginaire = 0;
      element=sommecomplexe(multipliecomplexe(valeursortie[j],
                          conjugue(cossin[(int)tableauvaleursuite[j]])),element);
      BAM[l].reelle = element.reelle * element.reelle + BAM[l].reelle;
      if (distancereference < BAM[l].reelle)
break;
    }
  if (distancereference > BAM[l].reelle)
    {
      distancereference=BAM[l].reelle;
      indicereference=l;
    }
}
      indicereference = indicereference ^ mot;
      if (indicereference != 0)
{
  l=0;
  while (indicereference != 0)
    {
      indicereference &= (indicereference-1);
      l++;
    }
  nberreur += l;
}
    }
  fichs=fopen(fichiersortie,"a");
  /* le TEB est inscrit dans un fichier avec les paramètres d'entrée du programme */
  fprintf(fichs,"%8d %3d %2d %4.2f %4.2f %8d %9.8f\n",dimechantillon,k,n,moyenne,ecart,nberreur,
                (double)nberreur/((log(N)/log(2))*dimechantillon));
  fclose(fichs);
  return(EXIT_SUCCESS);
}
```

CDMA

```
#include <math.h>
#include <stdlib.h>
#include <stdio.h>
#include "type.h"
#include "multipliecomplexe.h"
#include "conjugue.h"
#include "inversecomplexe.h"
#include "sommecomplexe.h"
#define PI       3.1415926535897932385
int main (int argc, char *argv[])
{
  int i,j,l,m,M,N,k,n,res,messageemis;
  int nbutilisateur,dimechantillon,nberreur,indicereference;
  double mult,distancereference;
  double **tableauvaleursuite;
  char * fichiersortie;
  char * fichierentree;
  complexe *cossin;
  complexe element,somme;
  int **tabmessage;
  complexe *BAM;
  complexe *valeursortie;
  complexe ** valeurcalculee;
  FILE *fiche;
  FILE *fichs;
  if (argc != 8)
    {
      printf("\n ERREUR, le nombre de variable d'entrée est incorrect. Il faut :
\n- la taille de l'échantillon,\n- le nombre de somme exponentielles,\n- le nombre de phase,
\n- le nombre d'utilisateur,\n- le nom du fichier d'entrée qui contient le code,
\n- le nom du fichier de sortie,\n- la graine de l'alea.\n");
      return(EXIT_FAILURE);
    }
  /*************************************************************************/
  /*************************** initialisation ******************************/
  /*************************************************************************/
  dimechantillon=atoi(argv[1]);  /* taille de l'échantillon */
  k=atoi(argv[2]);               /* la longueur de l'étalement */
  n=atoi(argv[3]);               /* nombre de phases pour la séquence d'étalement */
  nbutilisateur=atoi(argv[4]);   /* nombre total d'utilisateur */
  fichierentree=argv[5];         /* nom du fichier contenant le code formaté en -1,1 au lieu de 1, 0 */
  fichiersortie=argv[6];         /* nom du fichier de sortie */

  fiche=fopen(fichierentree,"r");
  fscanf(fiche,"%d %d",&M,&N);
  tabmessage=(int **) malloc (N * sizeof(int*));
  for (i=0;i<N;i++)
    {
      tabmessage[i]=(int *) malloc (M * sizeof(int));
      for (j=0;j<M;j++)
{
  fscanf(fiche,"%d",&res);
  tabmessage[i][j]=res;
}
    }
  fclose(fiche);
  if (fmod(k,M) != 0)
    {
      printf("\n ERREUR, il faut que le nombre de somme exponentielle soit multiple de M.\n");
      return(EXIT_FAILURE);
    }
  BAM=(complexe *)malloc (N*sizeof(complexe));
  nberreur =0;
  tableauvaleursuite=(double **)malloc(nbutilisateur*sizeof(double *));
  valeursortie=(complexe *)malloc(k*sizeof(complexe));
```

```
  valeurcalculee=(complexe **)malloc(2*sizeof(complexe));
  valeurcalculee[0]=(complexe *)malloc(k*sizeof(complexe));
  valeurcalculee[1]=(complexe *)malloc(k*sizeof(complexe));
  cossin=(complexe *)malloc (n*sizeof(complexe ));
  for (i=0;i<nbutilisateur;i++)
    tableauvaleursuite[i]=(double *)malloc(k*sizeof(double));
  for (i=0;i<n;i++)
    {
      cossin[i].reelle=cos(PI*2*i/n);
      cossin[i].imaginaire=sin(PI*2*i/n);
    }
  /*************************************************************************/
  /************************ programme principal ****************************/
  /*************************************************************************/
  srandom(atoi(argv[7]));
  mult= 2*PI/(1<<31 - 1 );
  for(i=0;i<dimechantillon;i++)
    {
      /*********************************************************/
      /**** initialisation des séquences et du mot à émettre  ***/
      /*********************************************************/
      for(l=0;l <k;l++)
tableauvaleursuite[0][l]=(random()>> 4) % n;
      for (j=1;j<nbutilisateur;j++)
for(l=0;l <k;l++)
  tableauvaleursuite[j][l]=random()*mult;
      messageemis=(random()>>5)%N;
      /*****************************************************************/
      /********************** fin initialisation ************************/
      /*****************************************************************/
      for (m=0;m<(k/M);m++)
{
  for (j=0;j<M;j++)
    {
      somme.reelle=tabmessage[messageemis][j]*
                                cossin[(int)tableauvaleursuite[0][j+m*M]%n].reelle;
      somme.imaginaire=tabmessage[messageemis][j]*
                                cossin[(int)tableauvaleursuite[0][j+m*M]%n].imaginaire;
              /*ajoute du BAM dû aux nbutilisateur-1 autres utilisateur  */
      for(l=1;l<nbutilisateur;l++)
{
  somme.reelle += cos(tableauvaleursuite[l][j+m*M]);
  somme.imaginaire += sin(tableauvaleursuite[l][j+m*M]);
}
      valeursortie[j+m*M]=somme; /* valeur reçu par le récepteur */
    }
}
      /***********************************************/
      /****************** décision *******************/
      /***********************************************/
      for(l=0;l<N;l++)
{
  BAM[l].reelle=0;
  BAM[l].imaginaire=0;
}
      for(j=0;j<k;j++)
{
  element.reelle = -1;
  element.imaginaire = 0;
  valeurcalculee[0][j]=sommecomplexe(multipliecomplexe(valeursortie[j],
                                      conjugue(cossin[(int)tableauvaleursuite[0][j]])),element);
  valeurcalculee[0][j].reelle =valeurcalculee[0][j].reelle*valeurcalculee[0][j].reelle;
  element.reelle = 1;
  element.imaginaire = 0;
  valeurcalculee[1][j]=sommecomplexe(multipliecomplexe(valeursortie[j],
                                      conjugue(cossin[(int)tableauvaleursuite[0][j]])),element);
  valeurcalculee[1][j].reelle =valeurcalculee[1][j].reelle*valeurcalculee[1][j].reelle;
```

```
}
      for(j=0;j<k;j++)
{
  if(tabmessage[0][j%M]==1)
    BAM[0].reelle += valeurcalculee[0][j].reelle;
  else
    BAM[0].reelle += valeurcalculee[1][j].reelle;
}
      distancereference=BAM[0].reelle;
      indicereference=0;
      for(l=1;l<N;l++)
{
  for(j=0;j<k;j++)
    {
      if(tabmessage[l][j%M]==1)
BAM[l].reelle += valeurcalculee[0][j].reelle;
      else
BAM[l].reelle += valeurcalculee[1][j].reelle;
      if (distancereference < BAM[l].reelle)
break;
    }
  if (distancereference > BAM[l].reelle)
    {
      distancereference=BAM[l].reelle;
      indicereference=l;
    }
}
      indicereference ^= messageemis;
      if (indicereference != 0)
{
  l=0;
  while (indicereference != 0)
    {
      indicereference &= (indicereference-1);
      l++;
    }
  nberreur += l;
}
    }
  /* le TEB est inscrit dans un fichier avec les paramètres d'entrée du programme */
  fichs=fopen(fichiersortie,"a");
  fprintf(fichs,"%8d %3d %2d %2d %8d %9.8f\n",dimechantillon,k,n,nbutilisateur,nberreur,
                                        (double)nberreur/((log(N)/log(2))*dimechantillon));
  fclose(fichs);
  return(EXIT_SUCCESS);
}
```

Bruit Blanc Additif Gaussien

```
#include <math.h>
#include <stdlib.h>
#include <stdio.h>
#include "gngauss.h"
#define PI       3.1415926535897932385
double gngauss(double mean, double sigma)
{

  double u, r;

  u = (double) rand() / RAND_MAX;
  if (u == 1.0) u = 0.999999999;
  r = sigma * sqrt( 2.0 * log( 1.0 / (1.0 - u) ) );

  u = (double) rand() / RAND_MAX;
  if (u == 1.0) u = 0.999999999;

  return( (double) ( mean + r * cos(2 * PI * u) ) );
}
```

Bibliographie

[1] J. G. Proakis. *Digital Communications.* McGraw-Hill International Editions.

[2] R. G. Gallager. *Information Theory and Reliable Communication.* John Wiley & Sons, 1968.

[3] G. Battail. *Théorie de l'information. Application aux techniques de communication.* Masson, 1997.

[4] C. Shannon. *A Mathematical Theory of Communication.* Bell System Technical Journal, 1948, pp. 379-423, 623-656.

[5] B. Char, K. Geddes, G. Gonnet, B. Leong, M. Monogan, S. Watt. *Maple V Library Reference Manuel.* Springer-Verlag, New York-Berlin-Heidelberg, 1991.

[6] M. Rybowicz, J.-P. Massias. *Maple V, release 4 : un système de calcul formel PC-Windows, UNIX, X-Window.* Eyrolles, 1997.

[7] S. Jacq. *Décodage itératif des codes produits : "turbo-codes en bloc", et évolution de leurs performances pour des modulations MDP et MAQ sur canal de Gauss et de Rayleigh.* Thèse de Doctorat de l'Université de Limoges, Mai 1996.

[8] A. Valembois. *Décodage, détection et reconnaissance des codes linéaires binaires.* Thèse de Doctorat de l'Université de Limoges, Octobre 2000.

[9] J.-P. Delmas. *Probabilité et télécommunication. Exercices et problèmes commentés.* Masson, 1987.

[10] D. V. Sarwate, M. B. Pursley. *Crosscorrelation Properties of Pseudorandom and Related Sequences.* Proceeding of the IEEE, Vol. 68, No. 5, May 1980, pp. 593-619.

[11] N.J.A. Sloane, F.J. McWilliams. *Pseudo-Random sequences and arrays.* Proceeding of IEEE,Vol. 64, No. 12, December 1976, pp. 1715-1729.

[12] N.J.A. Sloane, F.J. McWilliams. *The theory of error correcting codes.* North-Holland, 1977.

[13] E.R. Berlekamp. *Algebraic coding theory.* MacGraw-Hill, 1968.

[14] S.W. Golomb. *Shift register sequences.* Holden-Day, 1967.

[15] L.R. Welsh, R.A. Scholtz. *Group characters : sequences with good correlation properties.* IEEE Transaction on Information Theory, IT-24, No 5, September 1978, pp. 537-545.

[16] R.A. Gold. *Characteristic linear sequences and their coset function.* SIAM journal of applied mathematic, No. 14, Novenber 1966, pp. 980-985.

[17] R.A. Gold. *Maximal recursive sequence with 3-valued recursive cross-correlation function.* IEEE Transaction on Information Theory, No. 14, 1967, pp. 154-156.

[18] R.C. Dixon. *Spread Spectrum System with Commercial Application, third edition.* John Wiley & Sons, 1994.

[19] T. Kasami. *Weight Distribution Formula for some class of Cyclic Codes.* Coordinated Science Lab, Univ II, Urbana. Technical Report, R-285, Avril 1966.

[20] A. J. Viterbi. *CDMA : Principles of Spread Sprectrum Communication.* Addison Wesley, 1995.

[21] M. R. Karim, M. Sarraf. *W-CDMA and cdma2000 for 3G Mobile Networks.* McGrauw-Hill Telecom Professional, 2002.

[22] V. K. Garg. *IS-95 CDMA and cdma2000. Cellular/PCS Systems Implementation.* Prentice Hall, 2000.

[23] M. K. Simon, J. K. Omura, R. A. Scholtz, B. K. Levitt. *Spread Spectrum Communications Handbook.* McGraw-Hill International Editions, 2002.

[24] J. Meel. *Spread Spectrum : Introduction.*
http ://www.sss-mag.com/ss.html#tutorial, 1999.

[25] S. Leveque. *Conception et réalisation d'un système de transmission numérique CDMA autour de 60 GHz.* Thèse de Doctorat de l'Université de Marne-la-vallée, Décembre 1999.

[26] R. L. Peterson, R. E. Ziemer, D. E. Borth. *Introduction to spread spectrum communications.* Prentice Hall, 1995.

[27] B. Pearson. *A Condensed Review of Spread Spectrum Techniques for ISM Band Systems.* Application Note 9820 from Intersil Corporation, May 2000.
http ://www.nalanda.nitc.ac.in/industry/appnotes/Intersil/an9820.pdf

[28] Intersil Corporation. *Direct Sequence Spread Spectrum Baseband Processor.* July 1999.
http ://www.alldatasheet.com/datasheet-pdf/pdf/INTERSIL/HFA3860B.html

[29] B. Pearson. *Complementary Code Keying Made Simple.* Application Note 9850 form Intersil Corporation, May 2000.
http ://www.nalanda.nitc.ac.in/industry/appnotes/Intersil/an9850.pdf

[30] T. D. Chiueh, S. M. Li. *Trellis-Coded Complementary Code Keying for High-Rate Wireless LAN Systems.* IEEE Communications Letters, Vol. 5, No. 5, pp.191-193, May 2001.

[31] B. Ribov, G. Spasov. *Complementary Code Keying with PIC Based Microcontrollers For The Wireless Radio Communications.* Proceedings of

International Conference on Computer Systems and Technologies, 19-20 June 2003, Sofia (Bulgaria).

[32] Dr. K. Feher. *Wireless digital communication.* Prentice Hall, 1995.

[33] S. Penaud. *Etude des potentialités du chaos pour les systèmes de télécommunications, évaluation des performances de systèmes à accès multiples à répartition par les codes (CDMA) utilisant des séquences d'étalement chaotiques.* Thèse de Doctorat de l'Université de Limoges, Mars 2001.

[34] S. Penaud, Ph. Bouysse, J. Guittard, R. Quéré, A. Duverdier. *BER improvement of an asynchronous DS-CDMA system using chaotic spreading sequences.* Annal Télécommunication, 58, n°3-4 , 2003.

[35] T. P. Berger, L. Dubreuil. *Spread Spectrum, Cryptography and Information Hiding.* Proceedings of 9 th International Workshop on Algebraic and Combinatorial Coding Theory (ACCT) (Kranevo, Bulgaria), 19-25 June 2004, pp. 143-148.

[36] U. M. Maurer. *A Universal Statistical Test for Random Bits Generators.* Journal of Cryptology, Vol. 5, 1994.

[37] *A Statistical Test Suite for Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Application.* http ://csrc.nist.gov/rng/

[38] F. Arnault. *Théorie des Nombres et Cryptographie.* Cours de D.E.A de mathématiques de l'université de limoges, Mai 2002. http ://www.unilim.fr/pages_perso/francois.arnault/index.html

[39] S. Katzenbeisser, F. A. P. Petitcolas. *Information Hiding, techniques for steganography and digital watermarking.* Artech House, Computer Security Series, 2000.

[40] V. S. Pless, W. C. Huffman. *Handbook of coding theory, volume 1.* North Holland, 1998.

[41] V. S. Pless, W. C. Huffman. *Handbook of coding theory, volume 2.* North Holland, 1998.

[42] A. E. Brouwer. *Bounds on the minimum distance of linear codes.* http ://www.win.tue.nl/∼aeb/voorlincod.html

[43] V. Girardin, N. Limnios. *Probabilités. Cours et exercice en vue des applications.* Vuibert "les grands cours", Mai 2001.

[44] The Members of Thechnical Staff, Bell Labs. Edited by K. I. Kim. *Handbook of CDMA : System Design, Engineering and Optimization.* Prentice Hall Communication Engineering and Emerging Technologies Series, 2000.

[45] T. P. Berger, P Loidreau. *How to mask the structure of codes for a cryptographic use.* A paraître.

[46] N. Sendrier. *Codes correcteurs d'erreurs à haut pouvoir de correction.* Thèse de Doctorat de l'Université de Paris 6, Décembre 1991.

[47] L.H. Charles Lee. *Convolutional Coding, Fundamentals and Applications.* Artech House Publishers, 1997.

[48] E. Cadic. *Construction de Turbo Codes courts possédant de bonnes propriétés de distance minimale.* Thèse de Doctorat de l'Université de Limoges, Octobre 2003.

[49] D. E. Muller. *Application of Boolean algebra to switching circuit design and to error detection.* IEEE Trans. Comput. 3, 1954, pp. 6-12.

[50] I. S. Reed. *A class of multiple-error-correcting codes and the decoding scheme.* IEEE Trans. Inform. Theory IT-4 pp. 38-49, 1954.

[51] B. Sakkour. *Décodage des codes de Reed Muller au delà de la distance minimale.* Mémoire de DEA d'algorithmique, École Nationale Supérieure des Techniques Avancées, Juin 2003.

[52] A. E. Ashikhim, S. N. Litsyn. *Fast Decoding Algorithms for First Order Reed Muller and Related Codes.* Designs, Codes and Cryptography, vol. 7, pp. 187-214, 1996.

[53] J. C. Carlach, C. Vervoux. *A new family of block Turbo-Codes.* Proceedings of 13 th Applicable Algebra in Engineering Communication and Computing (AAECC)(Hawai, USA),14-19 November 1999, pp. 15-16.

[54] A. Otmani. *Codes cortex et construction de codes auto-duaux optimaux.* Thèse de Doctorat de l'Université de Limoges, Décembre 2002.

[55] A. Otmani. *Caractérisation des codes auto-duaux binaires de type II à partir du code de Hamming étendu [8, 4, 4].* Comptes Rendus Mathématique, Vol. 336, Issue 12, 15 June 2003, pp. 971-974.

[56] G. Olococ, J. P. Tillich. *Interactive Decoding of a New Family of Block Turbo-Codes.* 2nd International Symposium on Turbo Codes and related Topics (Brest, France) 4-7, 2000.

[57] *The Magma Computational Algebra System,for Algebra, Number Theory and Geometry.* http ://magma.maths.usyd.edu.au/magma/

[58] J. G. Proakis and M. Salehi. *Contemporary Communication Systems Using MATLAB.* Boston, PWS Publishing Company, 1998 pp. 49-50.

[59] C. Fleming. *Tutorial on Convolutional Coding with Viterbi Decoding.* http ://home.netcom.com/∼chip.f/viterbi/ccode/addnoise.html

Résumé : Dans cette thèse, nous étudions un système de communication nommé étalement de spectre. Le principe de ce système consiste à répartir l'énergie du signal à émettre sur une bande de fréquence plus large que celle réellement nécessaire à la transmission du signal utile. Le fonctionnement de l'étalement de spectre est basé sur l'utilisation de "séquences d'étalement" ayant de bonnes propriétés de corrélation. Dans cette thèse, nous introduisons des codes correcteurs d'erreurs pour améliorer l'efficacité de l'étalement du signal.
L'objectif de cette thèse est de déterminer l'efficacité de cette méthode et les critères de choix des codes correcteurs d'erreurs. Le nombre maximum d'utilisateurs dépend du choix du code correcteur d'erreur utilisé mais aussi de la séquence d'étalement utilisée. Une synthèse de l'étalement de spectre et du CDMA (Code Division Multiple Access) est présentée dans une première partie. Des limites théoriques sont données et des limites physiques sont posées. Puis deux systèmes à étalement de spectre utilisant des séquences d'étalement différentes sont présentés et comparés. Le système le plus performant, aussi bien théorique que pratique, est l'étalement de spectre "à déphasage multiple". La dernière partie présente divers codes correcteurs d'erreur et détermine celui qui maximise le nombre d'utilisateurs. Toutefois, pour un taux d'erreur binaire résiduel inférieur à 10^{-3} et un facteur d'étalement de 31, le nombre maximum d'utilisateurs obtenu en pratique est de 23 avec l'utilisation de code correcteurs d'erreur et de 7 sans, tandis que du point de vue théorique on en espère 45.

Mots-clés : Etalement de spectre, CDMA, codes correcteurs d'erreurs, limite de Shannon, séquence d'étalement, séquence de Gold.

Improvements of spread spectrum by using error-correcting codes

Abstract : In this thesis we study a communication system named spread spectrum. The principle of this system consists in distributing the energy of the signal to transmit on a frequency band broader than what is really necessary to the transmission of the useful signal. Spread spectrum is based on using "spreading sequences" having good properties of correlation. In this thesis we introduce error correcting codes to improve the efficiency of the spreading signal.
The aim of this thesis is to determine the efficiency of this method and the selection criteria of the error-correcting codes to use. The maximum number of users depends on the choice of the error-correcting code used but also on the spreading sequence used. A synthesis of the spread spectrum and CDMA (Code Division Multiple Access) are presented in a first part. Theoretical limits are given and physical limits are posed. Next two systems of spread spectrum using different spreading sequence are presented and compared. The most powerful system, theoretically as well as practically, is the spread spectrum "with multiple dephasing". The last part presents various error-correcting codes and determines which one maximizes the number of users. However, for a binary error rate residual lower than 10^{-3} and a spreading factor of 31 the maximum number of users obtained in practice is 23 with using error-correcting code and 7 without it, while from the theoretical point of view the expected number is 45.

Keywords : Spread spectrum, CDMA, error-correcting codes, Shannon limit, spreading sequence, Gold sequence.

Discipline : Mathématiques et ses applications

Laboratoire : LACO, Faculté des Sciences, 123 avenue Albert Thomas, 87060 Limoges Cedex, France.