CODES DE CORRECTION D'ERREURS POUR LA TRANSMISSION DE LA TÉLÉVISION NUMÉRIQUE[†] – PHASE 1

RAPPORT FINAL

par

Jean-Yves Chouinard et Marc Trichard

Département de génie électrique

Université d'Ottawa

pour

Industrie Canada

Contrat 67CRC-4-0423

Approvisionnement et services

Gouvernement du Canada

Mars 1995

[†] Ce projet de recherche est financé en partie par le Programme des centres d'excellence de langue française
ıstrie Canada.

CODES DE CORRECTION D'ERREURS POUR LA TRANSMISSION DE LA TÉLÉVISION NUMÉRIQUE† – PHASE 1

RAPPORT FINAL

par

Jean-Yves Chouinard et Marc Trichard

Département de génie électrique

Université d'Ottawa

pour

Industrie Canada

Contrat 67CRC-4-0423

Approvisionnement et services

Gouvernement du Canada

Mars 1995

†Ce projet de recherche est financé en partie par le Programme des centres d'excellence de langue française d'Industrie Canada.

Table des matières

Liste des figures

Liste des symboles

a_i	symbole $(m+1)$-aire TCM à la sortie d'un codeur TCM à l'instant i
α	quotient des rapports $\left(\frac{d_{libre}}{\Delta_0}\right)^2$ et $2\frac{E_{sym}}{\Delta_0^2}$
$\alpha_{non-codé}$	quotient des rapports $\left(\frac{d_{min}}{\Delta_0}\right)^2$ et $2\frac{E_{sym(non-codé)}}{\Delta_0^2}$
	$\alpha_{non-codé} = \frac{1}{2\frac{E_{sym(non-codé)}}{\Delta_0^2}}$
d_{libre}	distance libre entre deux séquences complexes (treillis de Viterbi)
d_{min}	distance minimale euclidienne entre deux signaux complexes
Δ_0	distance euclidienne minimale pour une constellation donnée
$\Delta_l, l = 1, \ldots$	distance euclidienne minimale pour une sous-constellation au niveau de partitionnement l
E_{bit}	énergie d'un bit codé
$E_{bit(non-codé)}$	énergie d'un bit non-codé
E_{int}	énergie d'un symbole interférant QAM
E_{sym}	énergie d'un symbole codé
$E_{sym(non-codé)}$	énergie d'un symbole non-codé
γ	gain de codage asymptotique
γ_{dB}	gain de codage asymptotique (en décibels)
m	nombre de bits d'information à l'entrée d'un codeur TCM
I	degré d'entrelacement
$\tilde{m}$	nombre de bits d'information à l'entrée d'un codeur convolutionnel
N_{libre}	nombre moyen de chemins voisins à la distance libre d_{libre}
$N_{voisins}$	nombre moyen de signaux voisins sur la constellation, i.e. situés à la distance euclidienne minimale Δ_0
N_0	densité spectrale du bruit
ν	mémoire d'un codeur convolutionnel (le nombre d'états du treillis est égal à 2^ν)
$\mathcal{P}_{bit}$	probabilité d'erreur des bits d'information
$\mathcal{P}_{mot-code}$	probabilité de décodage erronné d'un mot-code Reed-Solomon

$\mathcal{P}_{sym}$	probabilité d'erreur des symboles
$\mathcal{P}_{sym(non-codé)}$	probabilité d'erreur des symboles pour la modulation QAM non-codée
R_{conv}	taux de code pour un codeur convolutionnel ($R_{conv} = \frac{\tilde{m}}{\tilde{m}+1}$)
$R_{concaténé}$	taux de code résultant pour un code concaténé
R_{TCM}	taux de code pour un codeur TCM ($R_{TCM} = \frac{m}{m+1}$)
ρ	rapport signal-à-bruit ($\rho = \frac{E_{sym}}{N_0}$)
ρ_{int}	rapport signal-à-interférence ($\rho_{int} = \frac{E_{sym}}{E_{int}}$)
$\rho_{non-codé}$	rapport signal-à-bruit non-codé ($\rho_{non-codé} = \frac{E_{sym(non-codé)}}{N_0}$)
S	symbole complexe (modulation TCM-64QAM à taux 2/3-2/3)
S_I	composante en phase du symbole complexe S pour la modulation codée TCM-64QAM 2/3-2/3
S_Q	composante en quadrature du symbole complexe S
$\mathbf{x}_i = (x_i^{(m)}, \ldots, x_i^{(1)})$	vecteur des bits d'information à l'entrée d'un codeur TCM à l'instant i
$\mathbf{y}_i = (y_i^{(m+1)}, \ldots, y_i^{(1)})$	mot-code à la sortie d'un codeur TCM (code d'Ungerboëck) à l'instant i

Liste des acronymes

MAP	code de correction récursif ("Maximum *a posteriori*")
NASA	"National Aeronautics and Space Administration"
NTSC	"National Television Systems Committee"
OFDM	multiplexage par répartition orthogonale de fréquences ("Orthogonal Frequency Division Multiplexing")
QAM	modulation d'amplitude en quadrature ("Quadrature Amplitude Modulation")
RS	code correcteur d'erreur Reed-Solomon
TCM	modulation codée (ou codulation) ("Trellis Coded Modulation")
TCM-QAM	modulation codée TCM utilisant la modulation d'amplitude en quadrature
TCM-32QAM	modulation codée TCM 32-aire conventionelle
TCM 64-QAM 2/3-2/3	modulation codée TCM 64-aire à taux 2/3 (en phase) et 2/3 (en quadrature)
TVHD	télévision à haute définition ("HDTV: high definition television")

Chapitre 1

Introduction

1.1 Description du projet de recherche

Ce projet de recherche consiste à étudier la performance des codes de correction d'erreurs appliqués à la télévision avancée numérique. Le système de télécommunications doit permettre la transmission d'un signal TVHD (i.e., télévision à haute définition ou "HDTV: high definition television" en anglais) numérique avec un début binaire allant de 15 $Mbits/s$ à 30 $Mbits/s$ dans une bande de fréquence de 6 MHz seulement (i.e. efficacité spectrale de 2.5 $bits/s/Hz$ à 5 $bits/s/Hz$ avant codage de canal) afin d'assurer une transition *aisée* du système NTSC ("National Television Systems Committee") existant au futur système TVHD. Ceci requiert donc une technique de modulation à niveaux multiples telle que la modulation QAM M-aire. De plus, la tolérance par rapport aux erreurs de transmission non corrigées est d'une erreur par minute [HLP93]. On doit ainsi ajouter de la redondance pour les codes de correction d'erreurs tout en maintenant la même efficacité spectrale.

1.2 Objectifs visés par le présent rapport

Les objectifs poursuivis dans le cadre de la phase 1 du projet de recherche se résument à une étude préliminaire comparative de la performance de certains codes de correction d'erreurs déjà proposés par les membres de la *Grand Alliance*[1] [WC94]. C'est l'objet du présent rapport. On y étudie plus spécifiquement la performance, en terme de probabilités d'erreurs, de la modulation codée (ou modulation TCM: de l'anglais "Trellis Coded Modulation") basée

[1]La *Grand Alliance* est constituée de compagnies manufacturière d'équipement de télévision supportant la mise en oeuvre d'un standard de télévision avancée de type numérique.

sur la modulation numérique d'amplitude QAM ("Quadrature Amplitude Modulation"). On étudie plus particulièrement les codes TCM-QAM à 32 niveaux (dénotés TCM-32QAM) ainsi que les codes TCM-64QAM à taux de code 2/3-2/3 (TCM-64QAM 2/3-2/3). Ce faisant, on exploite la redondance du code tout en maintenant l'efficacité spectrale.

Dans ce rapport, on représente le canal de transmission de télévision avancé par un canal affecté par du bruit gaussien blanc additif. Pour la modulation codée TCM-32QAM, on considère aussi une source d'interférence co-canal du même type que le signal désiré, c'est-à-dire un signal interférant QAM ayant le même débit et étant synchronisé avec le signal TCM-QAM.

Le code TCM-QAM (e.g. code TCM-32QAM et code TCM-64QAM 2/3-2/3) peut-être utilisé comme code *interne* afin de réduire le nombre d'erreurs aléatoires causées par le canal de transmission. En ajoutant au code interne TCM-QAM un second code correcteur d'erreurs, un code *externe* Reed-Solomon (code RS) par exemple, on peut éliminer la majorité des paquets d'erreurs ("error bursts") subsistant de la première étape de décodage. L'étude des codes concaténés Reed-Solomon avec la modulation codée TCM-QAM fait également l'objet du présent rapport final.

1.3 Plan du rapport

Ce rapport final est organisé de la manière suivante. Dans le présent chapitre, on a donné une brève description du projet de recherche et des objectifs poursuivis.

Les résultats préliminaires obtenus de simulations effectuées sur ordinateur sont présentés au chapitre 2. Après une brève description du système de télécommunications (section 2.2), on décrit le principe de la modulation codée TCM et on présente en détail la modulation codée TCM-32QAM basée sur la modulation d'amplitude en quadrature (section 2.3). On y indique comment se font les simulations; à savoir les paramètres du système de télécommunications (i.e. débit de transmission, type de codage de canal et technique de modulation), le canal de propagation simulé (bruit additif et interférence co-canal). Ensuite, on présente à la section 2.4 des courbes de probabilités d'erreurs, indiquant la dégradation du signal utile TVHD en fonction du rapport signal-à-bruit et du rapport signal-à-interférence. À la section 2.5, on explique la technique de modulation codée TCM-64QAM à taux 2/3-2/3. On y dérive l'expression de la probabilité d'erreur par symbole et par la suite, on présente les résultats des simulations obtenus avec la modulation codée TCM-64QAM 2/3-2/3 en les comparant avec la modulation codée TCM-32QAM.

Au chapitre 3, on s'intéresse aux codes correcteurs de groupements d'erreurs Reed-Solomon. Après avoir déterminé à la section 3.2.1 les paramètres des codes correcteurs Reed-Solomon choisis dans le cadre de ce travail, on présente à la section 3.2.2 l'algorithme

de décodage de Peterson-Gorenstein-Zierler que l'on a choisie et programmée pour effectuer les simulations sur ordinateur. À la section suivante (section 3.3), on présente les résultats des simulations relatifs à la performance des codes Reed-Solomon lorsque que ceux-ci sont concaténés à la modulation codée TCM-QAM.

Au chapitre 4, après un bref rappel des résultats de la phase 1 de cette étude (section 4.1), on indique l'état du travail de recherche présentement en cours. On indique, à la section 4.2, l'orientation envisagée pour la poursuite de ce projet de recherche. On y fait notamment référence à l'étude des codes dits récursifs: ces codes sont particulièrement prometteurs en ce qu'ils permettent de se rapprocher de la borne théorique de probabilité d'erreur de décodage par l'exploitation des *décisions a posteriori* des symboles décodés. Parmi les autres travaux de recherche suggérés, on mentionne l'étude de systèmes TVHD employant le multiplexage par répartition orthogonale de fréquences OFDM. On veut aussi étudier la dégradation sur les signaux TVHD causée par un signal interférant NTSC. Il y aurait également intérêt a étudier l'effet de la propagation multivoie à large bande.

Suit une bibliographie, répertoriant quelques références pertinentes portant sur la modulation codée, les codes de correction d'erreur Reed-Solomon ainsi que sur le sujet plus général de la télévision avancée.

La description des Corps Galois $GF(16)$, $GF(128)$ et $GF(256)$, requis pour effectuer la construction des codes correcteurs de groupements d'erreurs Reed-Solomon présentés au chapitre 3, est donnée à l'annexe A (aux pages 66 à 77).

Le listing des programmes en langage de programmation C utilisés pour ce rapport final sont présentés dans le document *Codes de correction d'erreurs pour la transmission de la télévision numérique (Phase 1): Listings des programmes.* La liste de ces programmes est donnée à l'annexe B (en page 78)

Chapitre 2

Modulation codée TCM

2.1 Introduction

On s'intéresse dans ce chapitre à la modulation codée TCM. On décrit à la section suivante (i.e. section 2.2) le système de télécommunication TVHD considéré. La section 2.3 présente la modulation codée TCM, et plus particulièrement la modulation codée TCM-QAM. On y indique les paramètres de codes TCM-QAM à 32 niveaux choisis pour les simulations. L'étude des performances de la modulation codée fait l'objet de la section 2.4. On présente en premier lieu des courbes théoriques asymptotiques de probabilité d'erreur des symboles en présence de bruit additif blanc gaussien. On considère ensuite la dégradation du signal en fonction du bruit additif blanc gaussien sur la base de simulations, puis on s'intéresse à la dégradation du signal causée par un signal interférant co-canal QAM. À la section 2.5, on décrit la modulation codée TCM-64QAM à taux 2/3-2/3. On y dérive l'expression de la probabilité d'erreur par symbole, puis on compare cette expression théorique avec les résultats de simulations pour le TCM-64QAM 2/3-2/3.

2.2 Système de télécommunications

La figure 2.1 montre les composantes du système de télécommunications utilisé pour les simulations. Au transmetteur, un générateur de séquences pseudo-aléatoires produit les bits d'information qui sont par la suite encodés avec un code Reed-Solomon. Les bits codés par le code Reed-Solomon sont par la suite entrelacés puis encodés à nouveau et modulés à l'aide d'un codeur/modulateur TCM employant une modulation d'amplitude QAM ("Quadrature Amplitude Modulation"). Le codeur TCM-QAM constitue un code de correction *interne* qui corrige la plupart des erreurs causées par le canal de transmission. Quant au code

Reed-Solomon, celui-ci est utilisé comme code de correction *externe* permettant de corriger la plupart des erreurs (ou groupements d'erreurs) subsistant du code de correction interne TCM-QAM. L'entrelaceur de bits permet de redistribuer plus uniformément dans le temps les erreurs devant être corrigées par le code externe et ainsi mieux exploiter sa capacité de correction. Les échantillons complexes du signal ainsi obtenus sont alors transmis dans le canal.

Le canal de transmission est caractérisé par une source de bruit gaussien blanc et additif. Les échantillons complexes du générateur de bruit blanc sont additionnés vectoriellement aux échantillons complexes du signal utile provenant du transmetteur. Une source d'interférence co-canal affecte aussi la transmission du signal dans le canal. Typiquement, cette source d'interférence devrait représenter un signal de télévision NTSC. Nous avons choisi, pour l'instant, un signal interférant du même type que le signal utilise, c'est-à-dire un signal QAM de même débit et synchronisé avec le signal désiré. On devrait obtenir ainsi une situation de pire cas, le démodulateur TCM-QAM ayant à reconstruire la séquence d'information originale en prenant des décisions à partir d'échantillons complexes corrompus, c'est-à-dire la somme vectorielle du signal désiré, de bruit (aléatoire) et du signal interférant co-canal QAM (ayant la même structure que le signal désiré).

On prévoit ajouter au canal de l'affaiblissement multivoie, de distribution de gaussienne complexe; permettant ainsi de générer des signaux dont l'amplitude suit une distribution de Rayleigh ou de Rice. On simule l'effet de la propagation multivoie en multipliant les échantillons complexes du signal avec un facteur complexe avec une fonction de densité de probabilité conjointe gaussienne complexe.

A la réception, les échantillons complexes affectés par le bruit additif gaussien et par l'interférence sont démodulés à l'aide de l'algorithme de Viterbi.

Une fois les bits décodés par le démodulateur TCM-QAM interne, ceux-ci sont remis dans leur ordre temporel original par le désentrelaceur de bits; ce qui a pour effet de mieux redistribuer les erreurs de décodage à l'entrée du codeur externe de groupements d'erreurs Reed-Solomon. La séquence de bits d'information décodés par le décodeur Reed-Solomon sont enfin comparés avec la séquence d'information originale générée au transmetteur afin de déterminer les symboles et les bits en erreur permettant ainsi de déterminer la performances des codes internes et externes en calculant les taux d'erreur par bit et par symbole résultants.

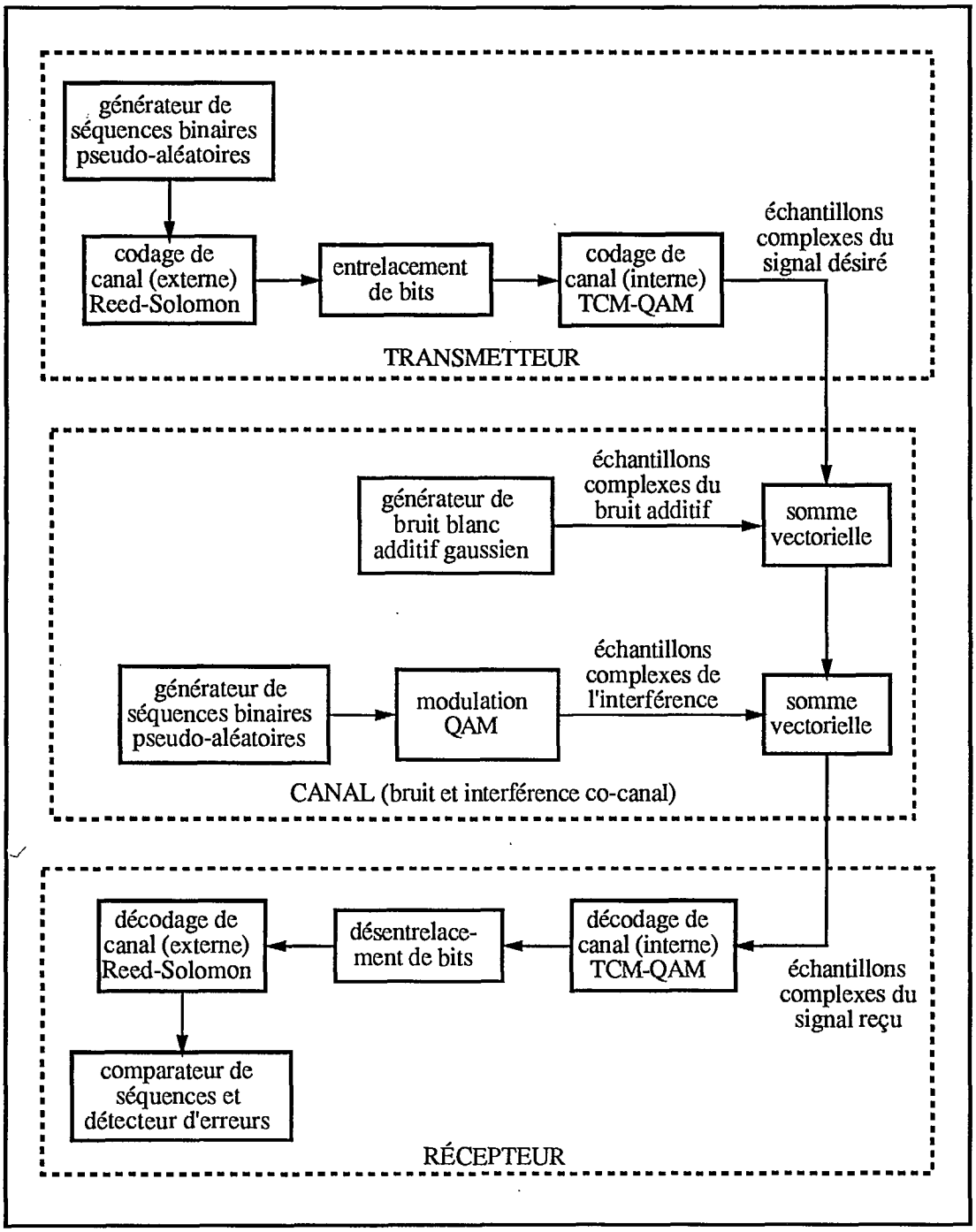

Figure 2.1: Schéma-bloc du système de télécommunications QAM avec bruit additif blanc gaussien et signal interférant du type QAM

2.3 Modulation codée TCM-QAM

2.3.1 Description de la modulation codée TCM-QAM

La modulation codée TCM combine le codage et la modulation permettant ainsi d'utiliser la distance euclidienne entre les échantillons complexes d'un signal reçu affecté par le canal de transmission et la position originale des signaux dans la constellation des signaux, pour calculer les métriques de branche dans le treillis de Viterbi. On obtient ainsi une performance meilleure que lorsque la démodulation et le décodage se font en cascade à partir de la distance de Hamming entre les mot-codes reçus et les mot-codes valides. Aussi, pour un taux de transmission, ou débit donné, on peut coder l'information sans pour autant accroître la largeur de bande requise pour transmettre le signal TCM.

Un encodeur TCM prends m bits d'information à la fois, soit $\mathbf{x}_i = (x_i^{(m)}, \ldots, x_i^{(1)})$ (à l'instant discret i), produit un mot-code $\mathbf{y}_i = (y_i^{(m+1)}, \ldots, y_i^{(1)})$, et forme un symbole $(m+1)$-aire de la manière suivante: $\tilde{m}$ de ces m bits d'information sont codés par un encodeur convolutionnel de taux $R_{conv} = \frac{\tilde{m}}{\tilde{m}+1}$ en $(\tilde{m}+1)$ bits codés. Ces $(\tilde{m}+1)$ bits: $\mathbf{y}_i = (y_i^{(\tilde{m}+1)}, \ldots, y_i^{(1)})$ sont en suite utilisés pour choisir l'une ou l'autre des $(\tilde{m}+1)$ *sous-constellations*, ou sous-ensembles de la constellation de $(m+1)$ signaux. Les $(m-\tilde{m})$ bits non-codés par l'encodeur convolutionnel, à savoir $(y_i^{(m+1)}, \ldots, y_i^{(\tilde{m}+2)})$, déterminent lequel des signaux $(m+1)$-aires de la sous-constellation choisie doit être transmis. Le nombre d'états du code convolutionnel est identifie par le paramètre ν et est égal à 2^{ν}.

Un paramètre important relatif à la performance des codes TCM est le gain de codage asymptotique γ. Celui-ci est défini comme étant le rapport:

$$\gamma = \frac{d_{libre}^2 / E_{sym}}{d_{min}^2 / E_{sym(non-codé)}}$$

où d_{libre} est la distance libre entre les chemins du treillis de Viterbi et E_{sym} l'énergie d'un bit codé, alors que d_{min} représente la distance euclidienne minimale et $E_{sym(non-codé)}$ l'énergie d'un bit non-codé.

Un autre paramètre important affectant la performance des codes TCM est le nombre moyen de chemins voisins N_{libre} à la distance libre d_{libre}.

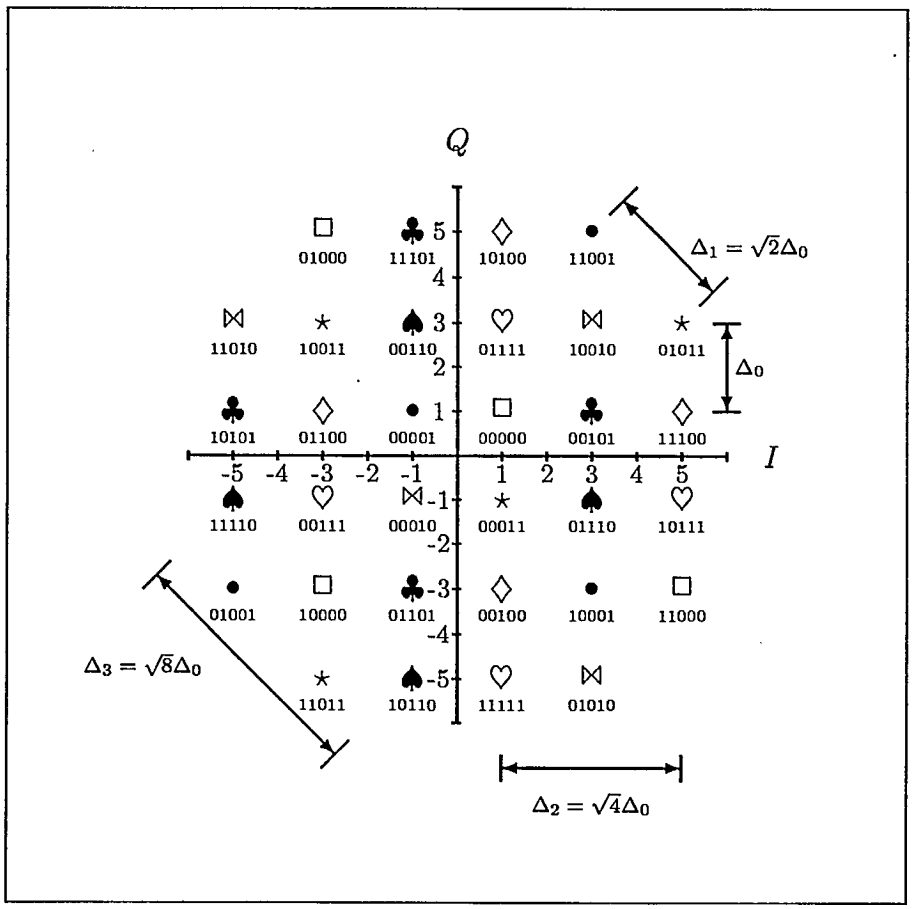

Figure 2.2: Constellation de signaux en modulation codée TCM-QAM à 32 niveaux: les bits $y_i^{(2)}$, $y_i^{(1)}$ et $y_i^{(0)}$ indiquent lequel des huit sous-ensembles de signaux (ou sous-constellation) est sélectionné alors que les bits $y_i^{(4)}$ et $y_i^{(3)}$ déterminent l'un des quatre signaux dans la sous-constellation.

La figure 2.2 représente la constellation de signaux en modulation codée TCM-QAM à 32 niveaux. Pour cette constellation, les bits $y_i^{(2)}$, $y_i^{(1)}$ et $y_i^{(0)}$ identifient l'un ou l'autre des huit sous-ensembles de signaux:

$$\begin{aligned}
y_i^{(2)}, y_i^{(1)}, y_i^{(0)} &= 000 \Longrightarrow \square \\
y_i^{(2)}, y_i^{(1)}, y_i^{(0)} &= 001 \Longrightarrow \bullet \\
y_i^{(2)}, y_i^{(1)}, y_i^{(0)} &= 010 \Longrightarrow \bowtie \\
y_i^{(2)}, y_i^{(1)}, y_i^{(0)} &= 011 \Longrightarrow \star \\
y_i^{(2)}, y_i^{(1)}, y_i^{(0)} &= 100 \Longrightarrow \diamondsuit \\
y_i^{(2)}, y_i^{(1)}, y_i^{(0)} &= 101 \Longrightarrow \clubsuit \\
y_i^{(2)}, y_i^{(1)}, y_i^{(0)} &= 110 \Longrightarrow \spadesuit \\
y_i^{(2)}, y_i^{(1)}, y_i^{(0)} &= 111 \Longrightarrow \heartsuit
\end{aligned}$$

Quant aux bits $y_i^{(4)}$ et $y_i^{(3)}$, ceux-ci indiquent lequel des quatre signaux est sélectionné dans un sous-ensemble donné [BDMS91].

Le partitionnement de la constellation 32-QAM en huit constellations (i.e., $\tilde{m} + 1 = 3$) est illustré à la figure 2.3.

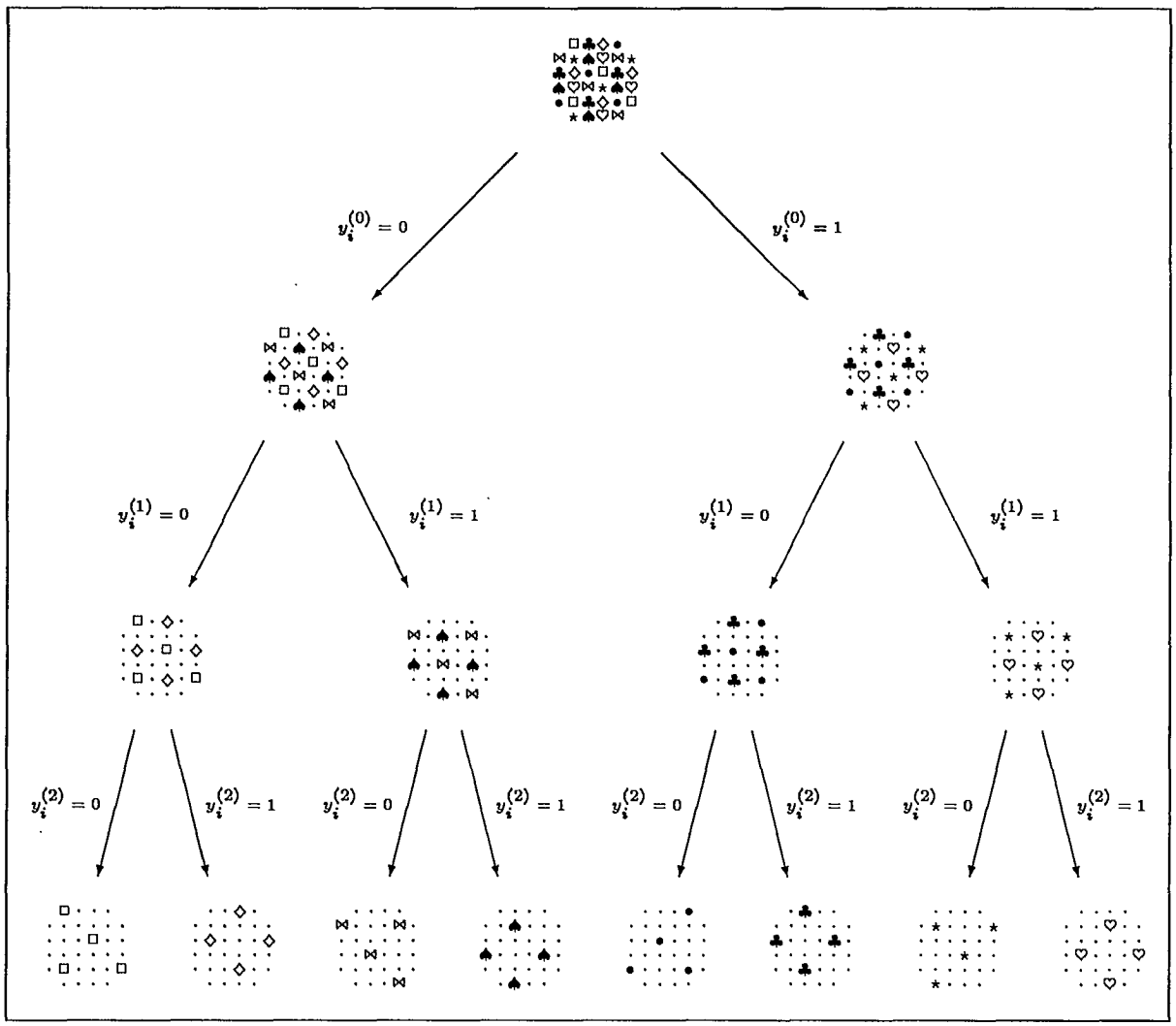

Figure 2.3: Partitionnement de la constellation de signaux en modulation codée TCM-QAM à 32 niveaux.

2.3.2 Paramètres de codes TCM-QAM à 32 niveaux

La liste des codes TCM-QAM à 32 niveaux, i.e. TCM-32-QAM, retenus pour les simulations est présenté aux pages suivantes. Ils s'agit de codes (bidimensionels) optimaux proposés par Ungerboëck [Ung87b, Ung82]. D'autres codes ont été évalués pour la télévision avancée par Heegard [HLP93] (et conduisant à des performances semblables) mais nous limitons ici notre étude aux codes d'Ungerboëck.

La structure des codes TCM est analysée en détail dans l'article de Forney [For70]. La figure 2.4 montre la structure spécifique d'un codeur TCM avec représentation d'Ungerboëck.

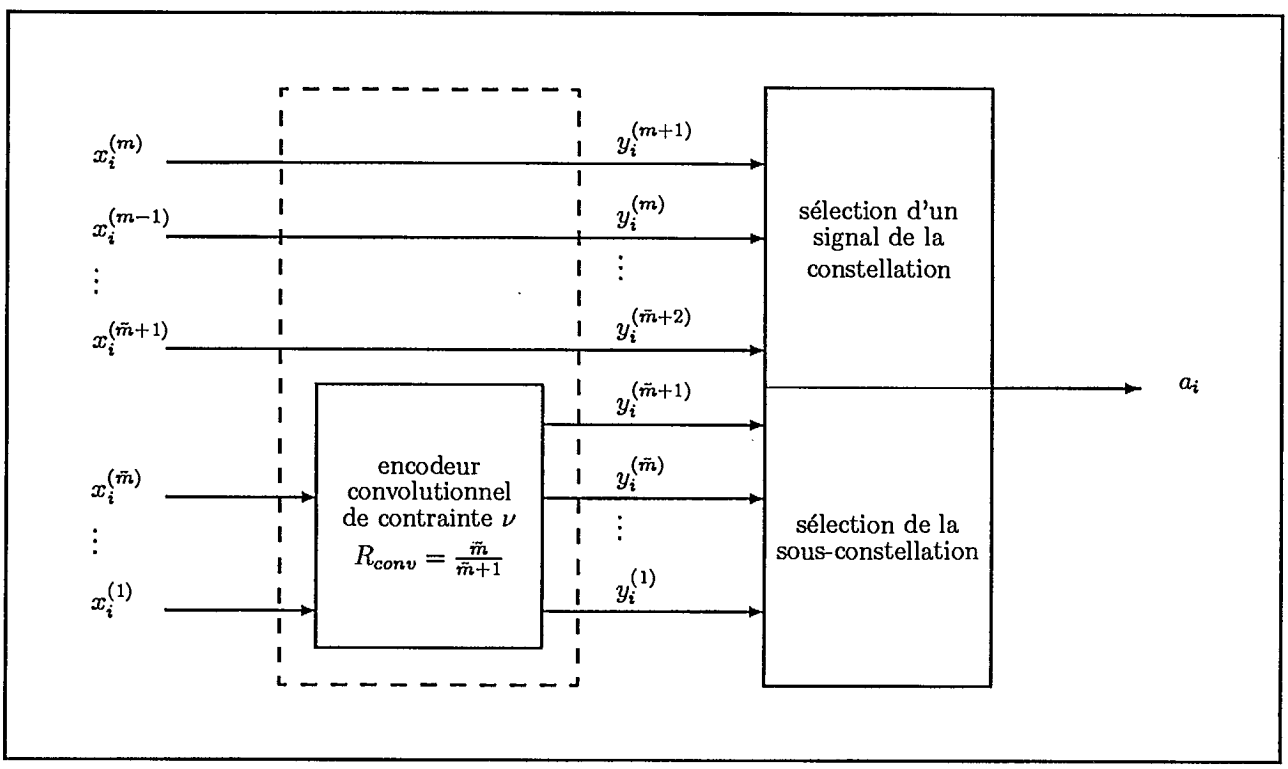

Figure 2.4: Schéma d'un codeur TCM utilisant la représentation d'Ungerboëck.

Ici, le taux de code R_{TCM} de chacun de ces codes est de $\frac{4}{5}$; on prends 4 bits à la fois, $\mathbf{x}_i = (x_i^{(4)}, x_i^{(3)}, x_i^{(2)}, x_i^{(1)})$, et on forme un symbole 32-aire QAM, c'est-à-dire a_i, à l'aide de la sortie $\mathbf{y}_i = (y_i^{(5)}, y_i^{(4)}, y_i^{(3)}, y_i^{(2)}, y_i^{(1)})$ d'un codeur convolutionnel de taux $R_{conv} = \frac{\tilde{m}}{\tilde{m}+1}$.

Code TCM-32QAM(2,1,2):

- Code TCM $(\tilde{m}+1, \tilde{m}, \nu)$: TCM-32QAM(2,1,2)
- Nombre d'états $2^{\nu} = 4$
- Rapport des carrés de la distance libre et de l'espacement minimal $d^2_{libre}/\Delta_0^2 = 4.0$
- Nombre moyen de chemins voisins à la distance libre $N_{libre} = 4$
- Gain de codage asymptotique $\gamma_{dB} = 3.01\ dB$

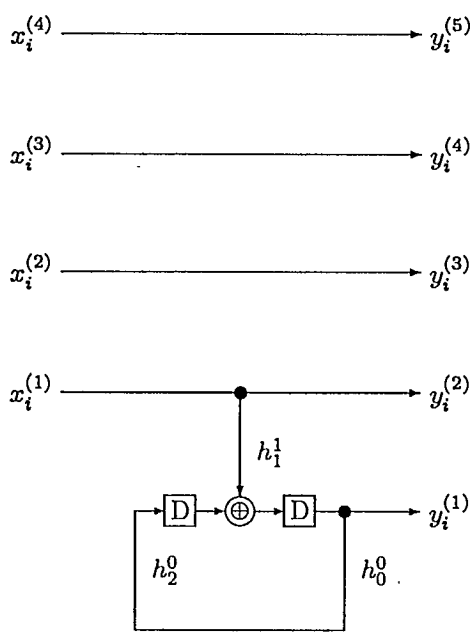

Figure 2.5: Structure de l'encodeur convolutionnel TCM-32QAM(2,1,2).

Code TCM-32QAM(3,2,3):

- Code TCM $(\tilde{m}+1, \tilde{m}, \nu)$: TCM-32QAM(3,2,3)
- Nombre d'états $2^{\nu} = 8$
- Rapport des carrés de la distance libre et de l'espacement minimal $d^2_{libre}/\Delta_0^2 = 5.0$
- Nombre moyen de chemins voisins à la distance libre $N_{libre} = 16$
- Gain de codage asymptotique $\gamma_{dB} = 3.98\ dB$

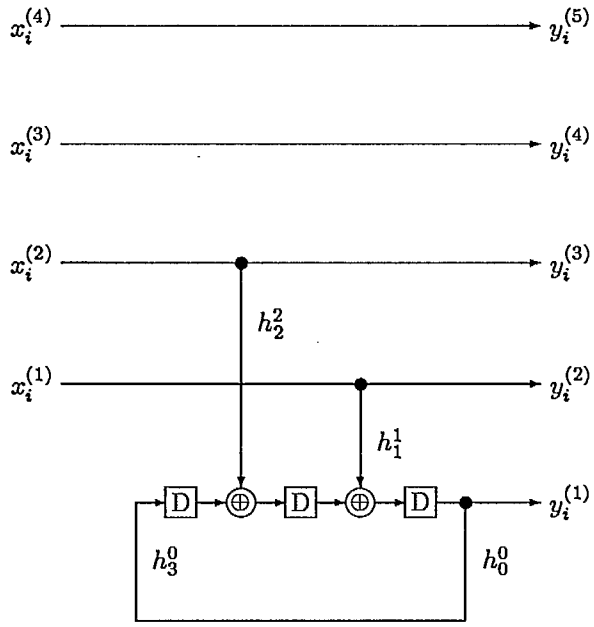

Figure 2.6: Structure de l'encodeur convolutionnel TCM-32QAM(3,2,3).

Code TCM-32QAM(3,2,4):

- Code TCM $(\tilde{m}+1, \tilde{m}, \nu)$: TCM-32QAM(3,2,4)
- Nombre d'états $2^{\nu} = 16$
- Rapport des carrés de la distance libre et de l'espacement minimal $d^2_{libre}/\Delta_0^2 = 6.0$
- Nombre moyen de chemins voisins à la distance libre $N_{libre} = 56$
- Gain de codage asymptotique $\gamma_{dB} = 4.77\ dB$

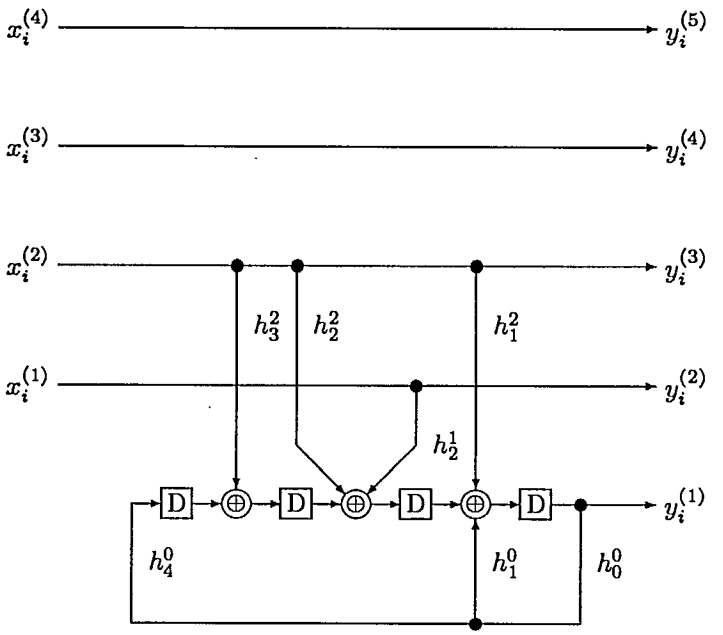

Figure 2.7: Structure de l'encodeur convolutionnel TCM-32QAM(3,2,4).

Code TCM-32QAM(3,2,5):

- Code TCM $(\tilde{m}+1, \tilde{m}, \nu)$: TCM-32QAM(3,2,5)
- Nombre d'états $2^{\nu} = 32$
- Rapport des carrés de la distance libre et de l'espacement minimal $d^2_{libre}/\Delta_0^2 = 6.0$
- Nombre moyen de chemins voisins à la distance libre $N_{libre} = 16$
- Gain de codage asymptotique $\gamma_{dB} = 4.77\ dB$

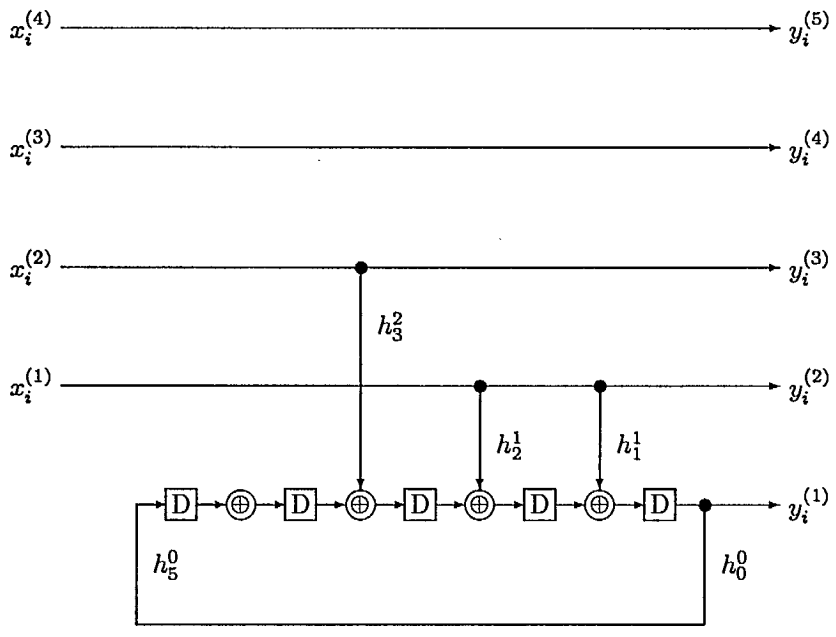

Figure 2.8: Structure de l'encodeur convolutionnel TCM-32QAM(3,2,5).

Code TCM-32QAM(3,2,6):

- Code TCM $(\tilde{m}+1, \tilde{m}, \nu)$: TCM-32QAM(3,2,6)
- Nombre d'états $2^{\nu} = 64$
- Rapport des carrés de la distance libre et de l'espacement minimal $d^2_{libre}/\Delta_0^2 = 7.0$
- Nombre moyen de chemins voisins à la distance libre $N_{libre} = 56$
- Gain de codage asymptotique $\gamma_{dB} = 5.44\ dB$

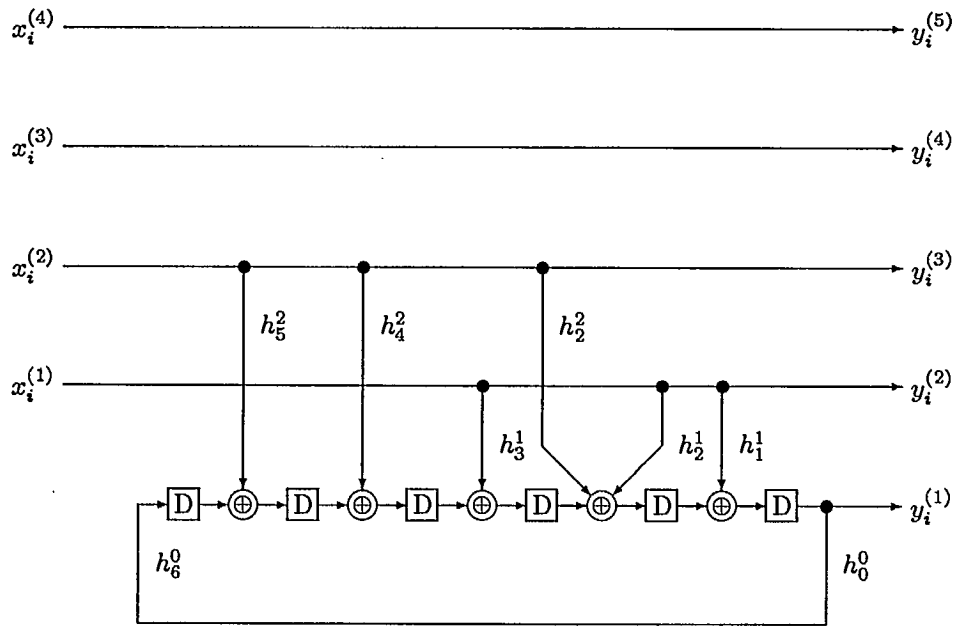

Figure 2.9: Structure de l'encodeur convolutionnel TCM-32QAM(3,2,6).

Code TCM-32QAM(3,2,7):

- Code TCM $(\tilde{m}+1, \tilde{m}, \nu)$: TCM-32QAM(3,2,7)
- Nombre d'états $2^{\nu} = 128$
- Rapport des carrés de la distance libre et de l'espacement minimal $d^2_{libre}/\Delta_0^2 = 8.0$
- Nombre moyen de chemins voisins à la distance libre $N_{libre} = 344$
- Gain de codage asymptotique $\gamma_{dB} = 6.02\ dB$

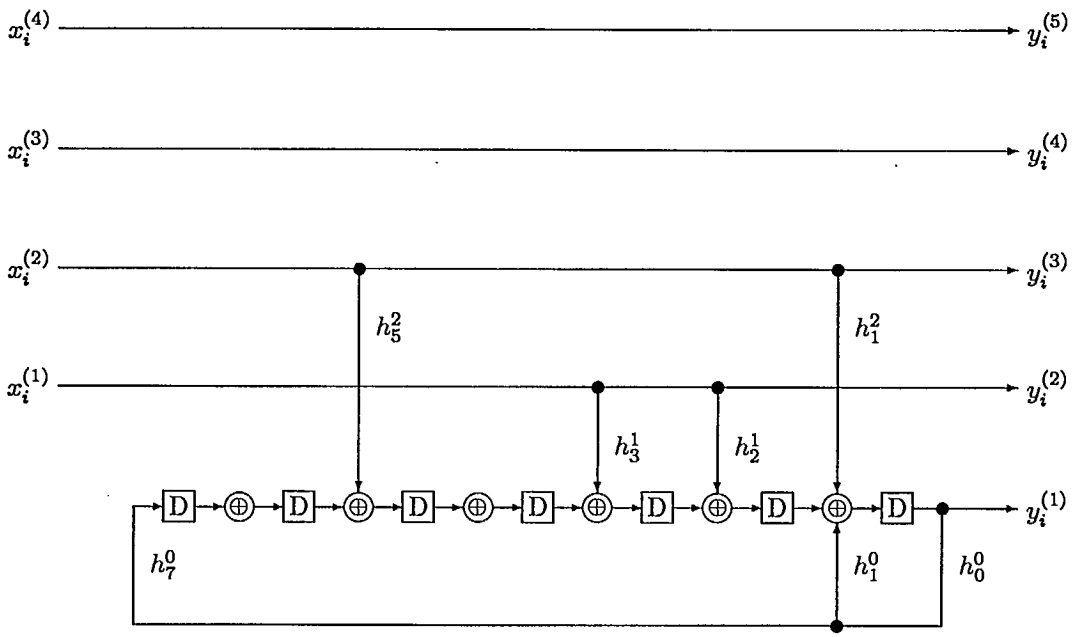

Figure 2.10: Structure de l'encodeur convolutionnel TCM-32QAM(3,2,7).

Code TCM-32QAM(3,2,8):

- Code TCM $(\tilde{m}+1, \tilde{m}, \nu)$: TCM-32QAM(3,2,8)
- Nombre d'états $2^{\nu} = 256$
- Rapport des carrés de la distance libre et de l'espacement minimal $d^2_{libre}/\Delta_0^2 = 8.0$
- Nombre moyen de chemins voisins à la distance libre $N_{libre} = 44$
- Gain de codage asymptotique $\gamma_{dB} = 6.02\ dB$

Code TCM-32QAM(3,2,9):

- Code TCM $(\tilde{m}+1, \tilde{m}, \nu)$: TCM-32QAM(3,2,9)
- Nombre d'états $2^{\nu} = 512$
- Rapport des carrés de la distance libre et de l'espacement minimal $d^2_{libre}/\Delta_0^2 = 8.0$
- Nombre moyen de chemins voisins à la distance libre $N_{libre} = 4$
- Gain de codage asymptotique $\gamma_{dB} = 6.02\ dB$

La figure 2.11 montre un exemple de codeur TCM-32QAM à quatre états: il s'agit du code TCM-32QAM(2,1,2).

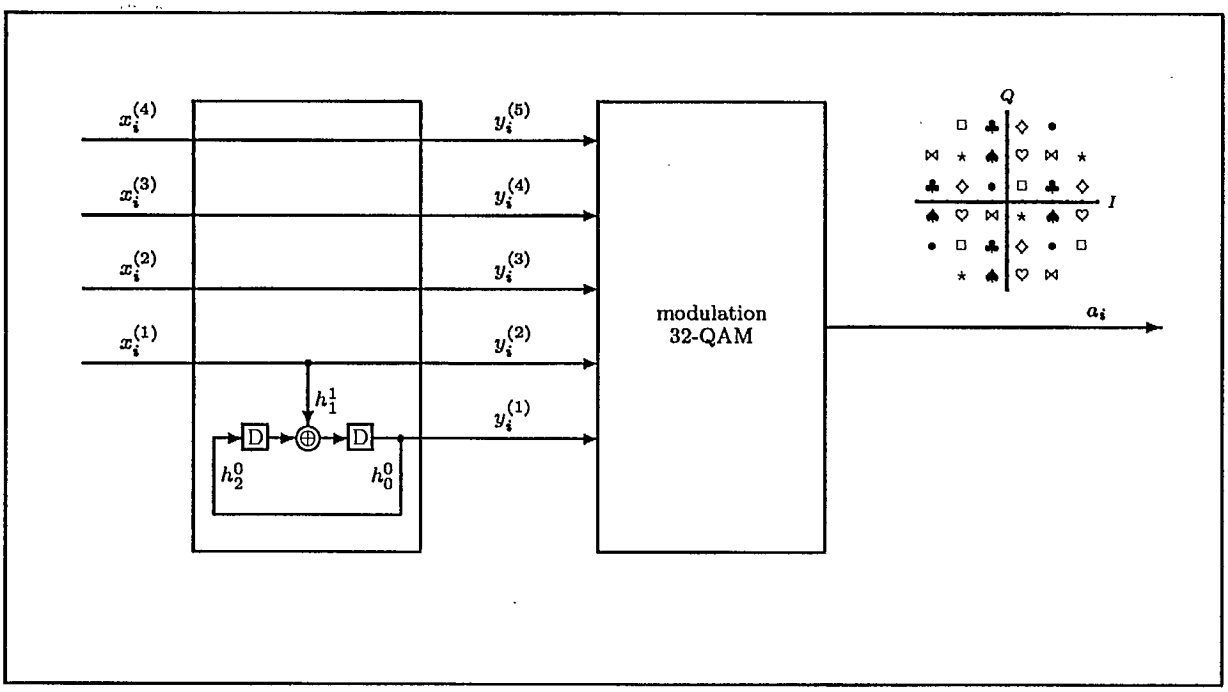

Figure 2.11: Exemple de codeur TCM-32QAM à quatre états (Code TCM-32QAM(2,1,2))

2.4 Performances de la modulation codée TCM-32QAM

2.4.1 Résultats théoriques asymptotiques en présence de bruit additif blanc gaussien

L'analyse des résultats théoriques asymptotiques donne lieu à plusieurs remarques importantes.

La probabilité d'erreur des symboles $\mathcal{P}_{sym}$ suit une loi asymptotique qui s'écrit, au premier ordre d'un développement limité de la fonction de transfert du code convolutionnel de la modulation TCM, comme indiquée par la formule de [Ung87a]:

$$\mathcal{P}_{sym} \approx N_{libre}\, Q\left(\frac{d_{libre}}{\sqrt{2\, N_0}}\right) \tag{2.1}$$

soit, en fonction du rapport signal-à-bruit $\rho = E_{sym}/N_0$:

$$\mathcal{P}_{sym} \approx N_{libre}\, Q\left(\sqrt{\alpha\, \rho}\right) \tag{2.2}$$

où $Q(x)$ est définie comme étant:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\left(-\frac{u^2}{2}\right)\, du$$

et α représente le quotient de la distance libre au carré d_{libre}^2 normalisée au carré de la distance euclidienne Δ_0^2 minimum séparant deux signaux de la constellation divisée par le double de l'énergie moyenne E_{sym}, normalisee à Δ_0^2, des signaux codés sur la constellation:

$$\alpha = \frac{\left(\frac{d_{libre}}{\Delta_0}\right)^2}{2\,\frac{E_{sym}}{\Delta_0^2}} \tag{2.3}$$

et N_{libre} désigne le nombre moyen de voisins proches sur le treillis du code, c'est-à-dire le nombre de chemins distincts distants de d_{libre} rejoignant deux états du codeur à des instants differents.

On peut comparer ce résultat (voir figure 2.12) à la probabilité d'erreur des symboles $\mathcal{P}_{sym(non-codé)}$ pour une modulation QAM non-codée à 16 niveaux, donnée par:

$$\mathcal{P}_{sym(non-codé)} \approx N_{voisins}\, Q\left(\sqrt{\alpha_{non-codé}\, \rho_{non-codé}}\right) \tag{2.4}$$

où $N_{voisins}$ désigne le nombre moyen de voisins proches sur la constellation, c'est-à-dire situés à la distance euclidienne minimale Δ_0. Cela correspond à un treillis dans lequel il n'y a qu'un

seul état avec un nombre de transitions parallèles égal au nombre de symboles possibles en sortie, lui-même égal au nombre de symboles possibles en entrée puisqu'il n'y a pas de bits codés rajoutés. Parmi l'ensemble des paires distinctes de transitions parallèles, il existe un sous-ensemble de paires distinctes de transitions pour lesquels, les points de la constellation associés aux symboles en sortie par une table de correspondance semblable à celles utilisées en modulation codée, sont à une distance minimale Δ_0 les uns des autres: cette distance serait la distance libre du trellis. Le nombre moyen, sur tous les chemins possibles, de chemins ainsi situés à la distance libre Δ_0 du trellis virtuel de la modulation QAM non-codée correspond alors au nombre moyen sur tous les points de la constellation des voisins proches, au sens les plus proches, soit à la distance minimale Δ_0^2 sur la constellation. Finalement, $\alpha_{non-codé}$ (respectivement $\rho_{non-codé}$) a la même expression que α (respectivement ρ), en substituant d_{libre} (respectivement E_{sym}) par $d_{min} = \Delta_0$ (respectivement $E_{sym(non-codé)}$), et N_{libre} par $N_{voisins}$:

$$\alpha_{non-codé} = \frac{\left(\frac{d_{min}}{\Delta_0}\right)^2}{2\,\frac{E_{sym(non-codé)}}{\Delta_0^2}} = \frac{1}{2\,\frac{E_{sym(non-codé)}}{\Delta_0^2}} \tag{2.5}$$

A partir des équations 2.2 et 2.4, Ungerboëck [Ung82] a défini le gain asymptotique de codage γ_{dB} (en décibels) par:

$$\gamma_{dB} = 10\ \log_{10}\left(\frac{(d_{libre}/\Delta_0)^2}{E_{sym}/E_{sym(non-codé)}}\right), \tag{2.6}$$

soit avec les notations de 2.3 et 2.5:

$$\gamma_{dB} = 10\ \log_{10}\left(\frac{\alpha}{\alpha_{non-codé}}\right). \tag{2.7}$$

On a alors tendance à donner d'avantage d'importance à ce gain asymptotique γ. En suivant le raisonnement de C. Heegard, A. Lery et H. Paik dans [HLP93], on remarque que d^2_{libre} contient un minimum:

$$d^2_{libre} = \min\{\Delta_0^2 \times d^2_{libre}(\nu, l),\ \Delta_l^2\}, \tag{2.8}$$

entre deux entités l'une, Δ_l^2 dépendant seulement du nombre l de bits en entrée du codeur, et l'autre, $d^2_{libre}(\nu, l)$, dépendant à la fois de l et du nombre d'états ν du codeur. Une fois fixé le nombre l de bits à coder, une augmentation de ν provoque une augmentation de la distance libre $d^2_{libre}(\nu, l)$ du code et de sa complexité alors que Δ_l^2 est la distance minimale entre deux transitions parallèles. Il en résulte qu'une augmentation illimitée de ν conduit à rendre la distance minimale du code atteinte sur deux transitions parallèles du code, et que le gain asymptotique sature. Les tables données par [Ung87b] pour $l = 3$ montrent ainsi que d^2_{libre} atteint la valeur $\Delta_3^2 = 8 \times \Delta_0^2$ lorsque $\nu = 7$. La figure 2.13 illustre la construction

des sous-constellations et donne les valeurs des distances Δ_l^2. Ainsi, pour des valeurs de ν supérieures à 7, il est possible que $d^2_{libre}(\nu, l)$ augmente, mais d^2_{libre} restera limité à Δ_3^2.

Les courbes théoriques asymptotiques tracées à très grande échelle et représentées sur la figure 2.13, permettent de mesurer le gain asymptotique γ_{dB} et de vérifier que pour $l = 3$, au-delà de $\nu = 7$ (pour le code TCM-QAM(3,2,7)), puisque $d^2_{libre} = \Delta_3^2$, le gain asymptotique sature. Cependant, ces considérations asymptotiques sont en partie faussées par la réalité, puisqu'en pratique, la loi asymptotique n'est pas complètement atteinte. Il est toutefois très vraisemblable qu'elles demeurent fondées et qu'il soit possible de les appliquer sans trop de discordance avec la réalité.

De manière plus significative, dans le domaine d'utilisation de la modulation TCM pour la TVHD, à savoir dans un intervalle de rapport $\rho = E_{sym}/N_0$ permettant une probabilité d'erreur des symboles de 10^{-3} à 10^{-5}, il apparait que les courbes ayant un gain asymptotique identique ne sont pas suffisamment voisines pour être considérées comme confondues. En d'autres termes, le facteur N_{libre} prend trop d'importance pour que l'on puisse le négliger raisonnablement. Ainsi, lorsque le gain asymptotique γ_{dB} sature avec une augmentation de ν, c'est-à-dire une augmentation de la complexité du code, on peut toutefois améliorer considérablement la probabilité d'erreur, grâce à ce coefficient multiplicateur N_{libre} qui dépend implicitement de ν: pour $l = 3$, entre un codeur de complexité donnée par $\nu = 7, 8$, ou 9, N_{libre} prend les valeurs 344, puis 44, puis 4, soit une amélioration pour la probabilité d'erreur des symboles d'environ 10^{-1} à 10^{-2}.

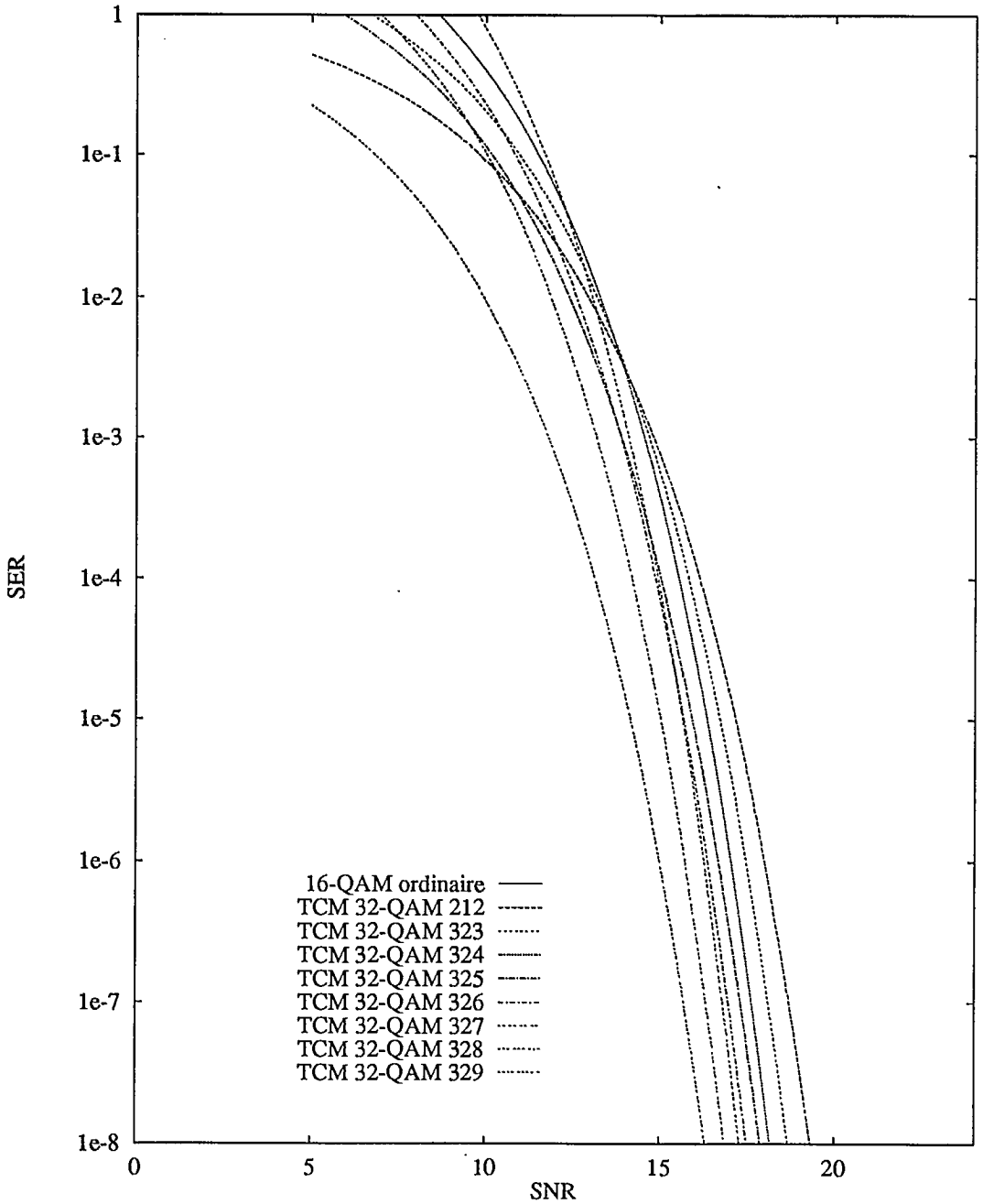

Figure 2.12: Courbes théoriques du taux d'erreur par symbole d'information (16-aire) $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour differents codes TCM-QAM.

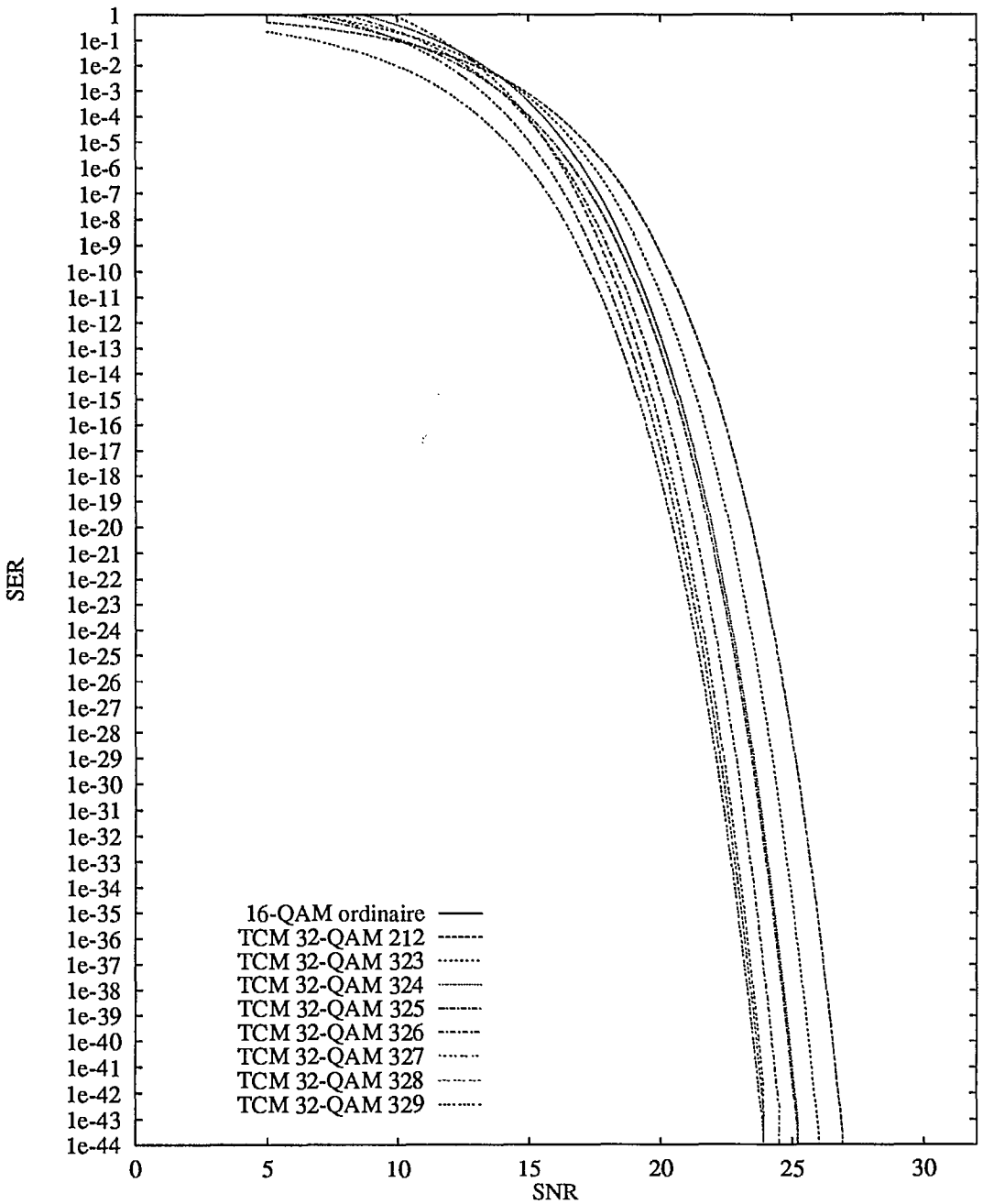

Figure 2.13: Courbes théoriques à grande échelle du taux d'erreur par symbole d'information (16-aire) $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour differents codes TCM-QAM.

2.4.2 Performance de la modulation codée TCM-32QAM en fonction du bruit additif blanc gaussien

Cependant, ces dernières considérations asymptotiques sont en partie faussées par la réalité, puisqu'en pratique, la loi asymptotique n'est pas complètement atteinte. Il est toutefois très vraisembable qu'elles demeurent fondées et qu'il soit possible de les appliquer sans trop de discordance avec la réalité.

Les courbes expérimentales donnent lieu à des écarts avec cette loi asymptotique, lesquels s'amoindrissent, heureusement lorsque le rapport $\rho = E_{sym}/N_0$ augmente. Il apparait que les résultats s'accordent assez justement avec les courbes asymptotiques. La figure 2.14 donne le taux d'erreur par symbole pour les codes TCM-32QAM(3,2,3) et TCM-32QAM(3,2,6) mentionnés à la section 2.3.2 (page 11).

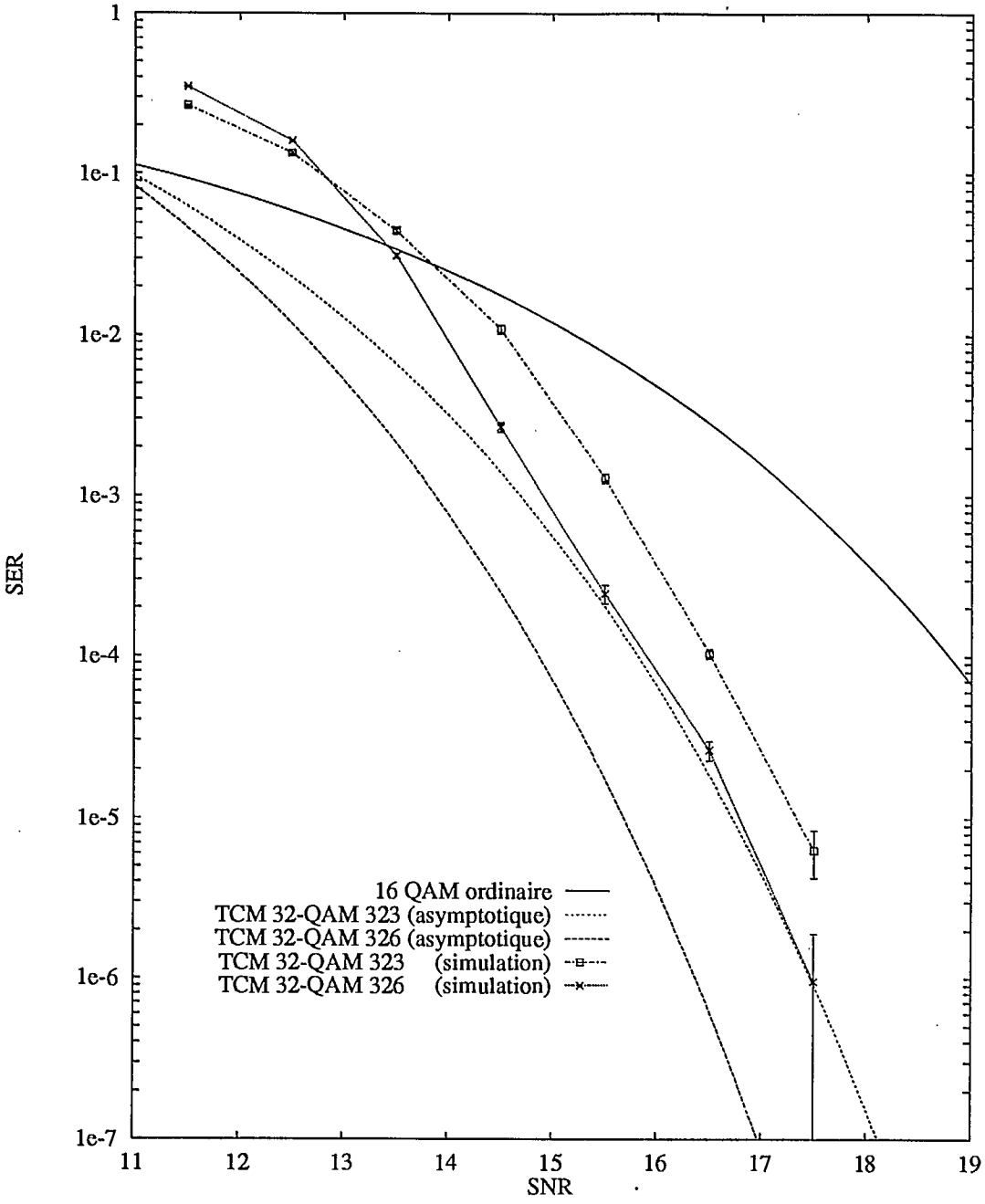

Figure 2.14: Courbes théoriques et expérimentales de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour la modulation TCM 32-QAM.

2.4.3 Performance de la modulation codée TCM-32QAM en présence d'un signal interférant QAM

Un autre phénomène important dans la pratique est celui des interférences entre canaux. On s'intéresse dans ce rapport préliminaire à une source d'interférence co-canal.Les courbes expérimentales données permettent de réaliser, à la vue des pertes considérables qu'il cause, combien il est fondamental de s'en affranchir. Un effort tout particulier sera donc fait pour éviter les pertes sévères induites par les interférences des signaux portées par des canaux voisins.

La figure 2.15 montre bien la dégradation du signal reçu et l'augmentation du taux d'erreur par symbole $\mathcal{P}_{sym}$ causés par un signal d'interférence co-canal QAM. Avec la modulation codée TCM-QAM, on obtient un taux d'erreur irréductible inacceptablement élevé lorsque le rapport signal-à-interférence ρ_{int} dépasse -15 dB. Ce rapport ρ_i est défini comme:

$$\rho_{int} = \frac{E_{sym}}{E_{int}} \tag{2.9}$$

où E_{int} représente l'énergie d'un symbole interférant QAM. La figure 2.16 montre le taux d'erreur par bit $\mathcal{P}_{bit}$ versus E_{bit}/N_0 en fonction du signal-à-interférence ρ_{int}.

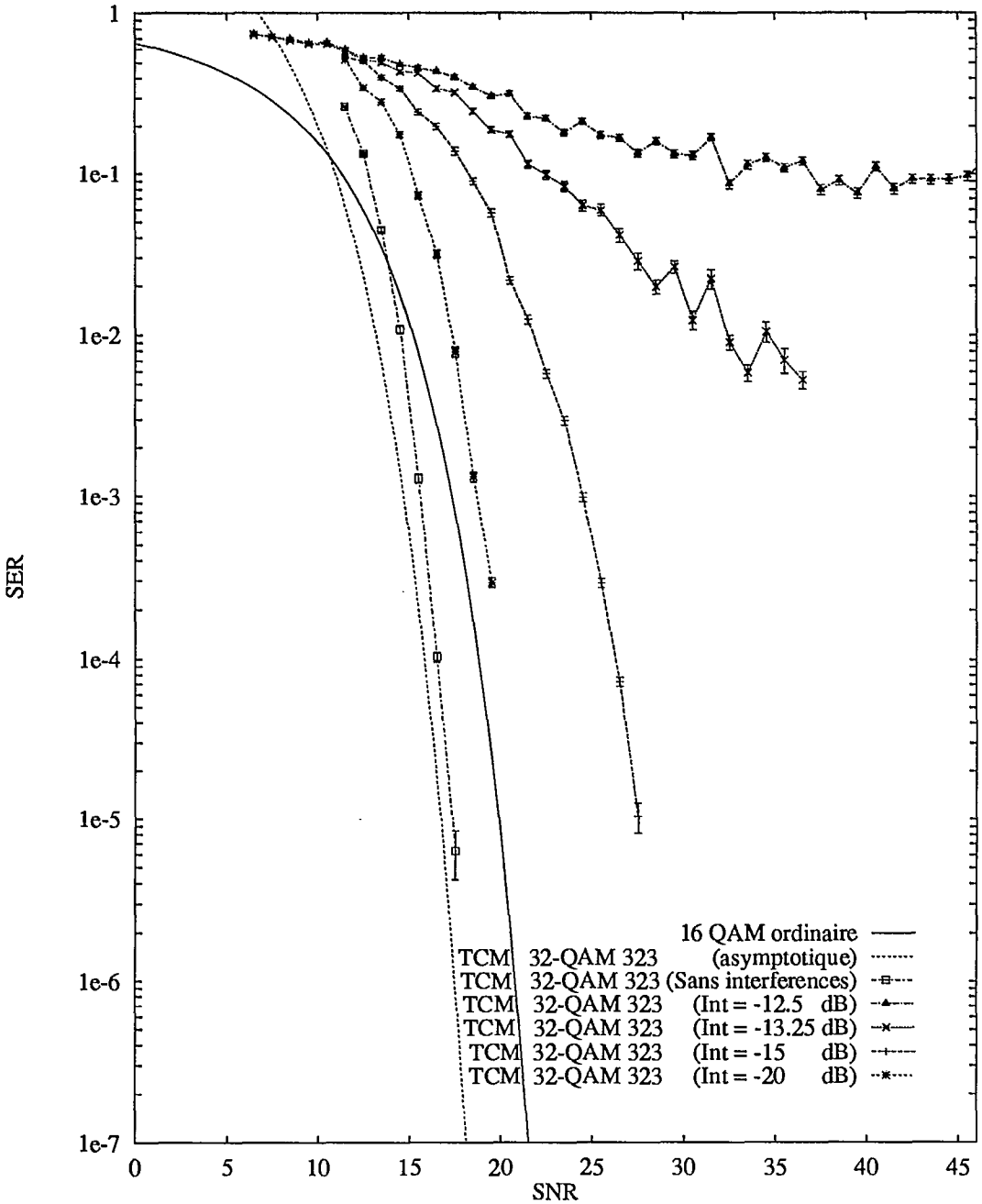

Figure 2.15: Taux d'erreur par symbole (16-aire) $\mathcal{P}_{sym}$ versus E_{sym}/N_0 en fonction du signal-à-interférence ρ_{int} pour le code TCM-QAM(3,2,3).

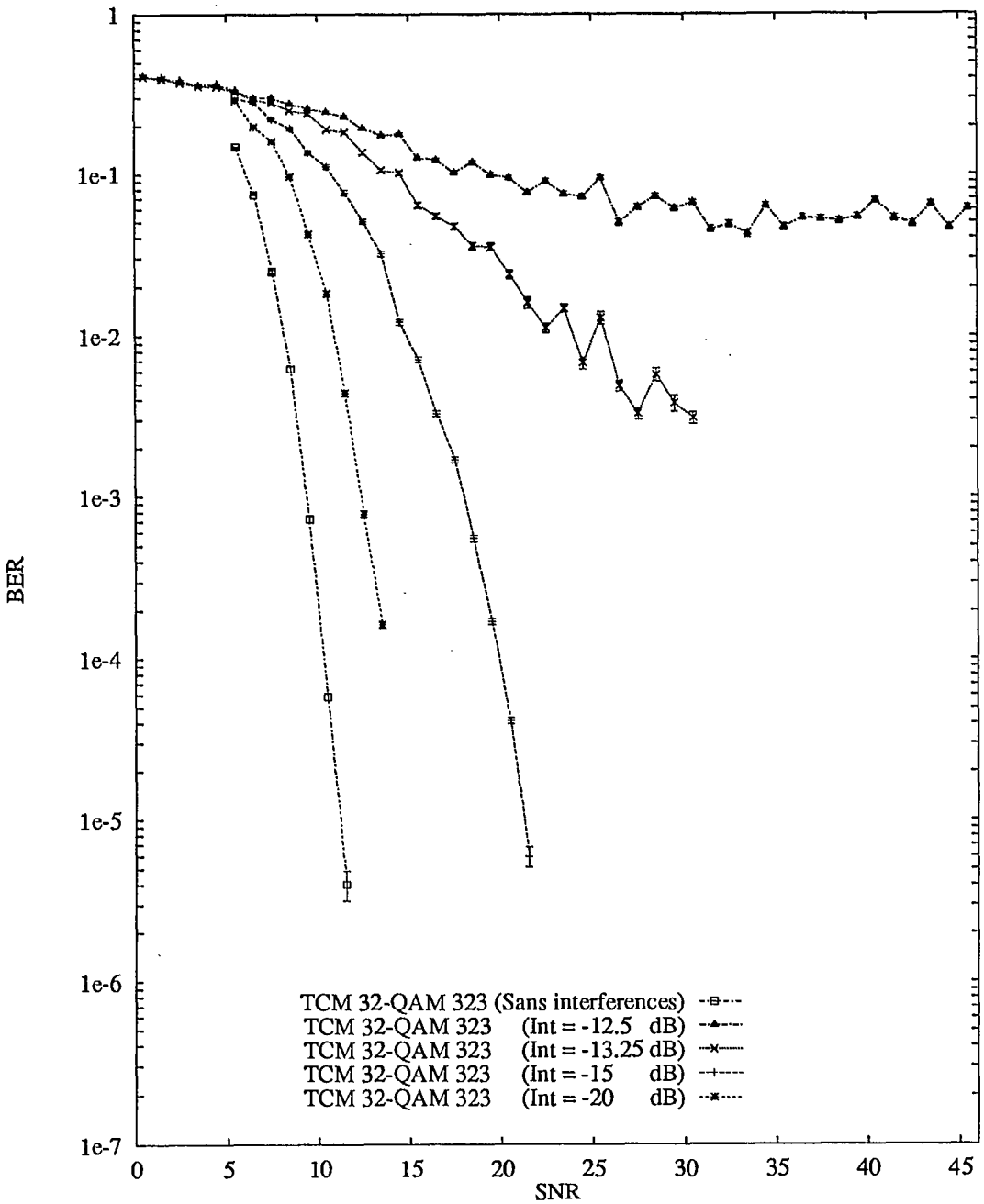

Figure 2.16: Taux d'erreur par bit $\mathcal{P}_{bit}$ versus E_{bit}/N_0 en fonction du signal-à-interférence ρ_{int} pour le code TCM-QAM(3,2,3).

2.5 Modulation codée TCM-64QAM à taux 2/3-2/3

2.5.1 Description de la modulation codée TCM-64QAM à taux 2/3-2/3

Un autre type de modulation étudiée et testée est la modulation codée TCM 64-QAM à taux 2/3-2/3. La modulation codée TCM-64QAM 2/3-2/3 est constituée d'un code TCM appliqué à une modulation en amplitude d'ordre 64 (TCM 64-QAM) pour lequel les quatres bits d'information sont codés séparément: chaque groupe de deux bits est codé avec un rapport 2/3 puis associé à un symbole dans un espace euclidien unidimensionnel, l'un porté par la composante en phase, l'autre par la composante en quadrature. Le shéma 2.17 ci-joint illustre la méthode de codage et montre que de la même façon, le décodage est effectué séparément pour les composantes en phase et en quadrature. Pour ce faire, l'algorithme de Viterbi est appliqué parallèlement deux fois pour les deux composantes du signal.

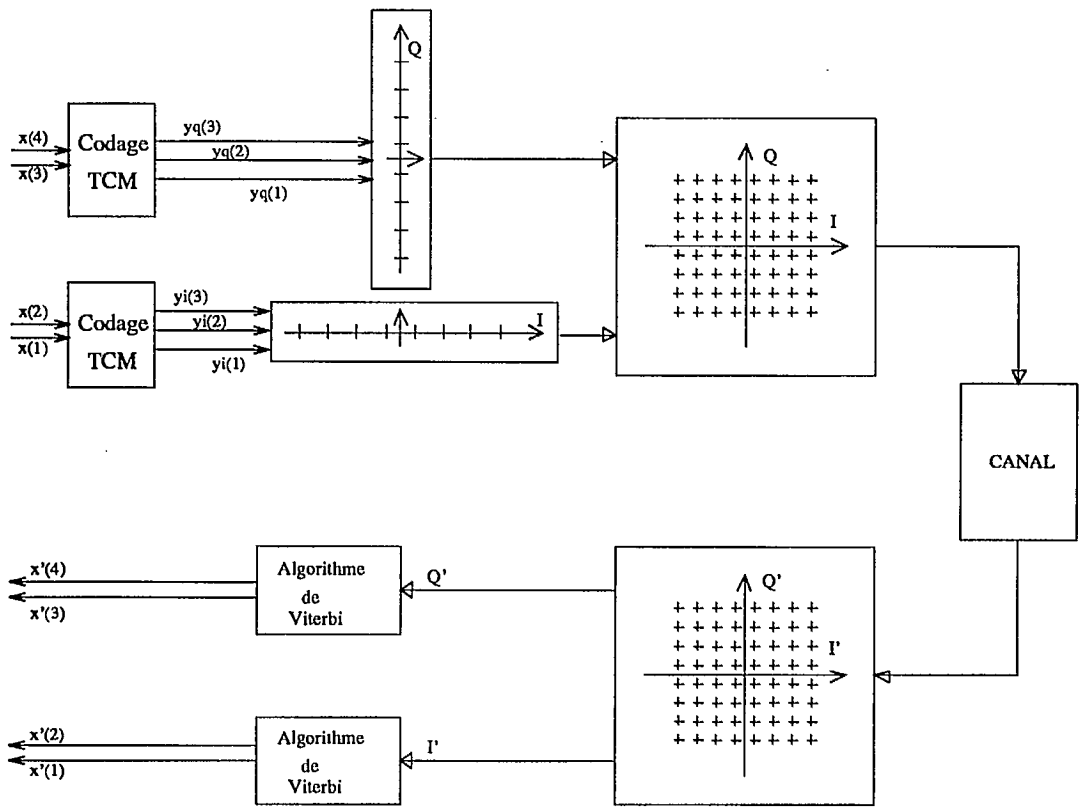

Figure 2.17: Schéma-bloc du système de télécommunications TCM 64-QAM à taux 2/3-2/3.

La figure 2.18 illustre la fonction de *"mapping"* unidimensionnel utilisé à cet effet. On peut remarquer que suivant le cas, selon que la longueur de mémoire du codeur convolutif soit égale à 2 ou qu'elle soit supérieure à 3, les sous-constellations ont respectivement deux éléments (les deux bits $y^{(1)}$ $y^{(2)}$ suffisent à les déterminer) ou un seul élément (les trois bits $y^{(1)}$ $y^{(2)}$ $y^{(3)}$ sont nécessaires pour les caractériser).

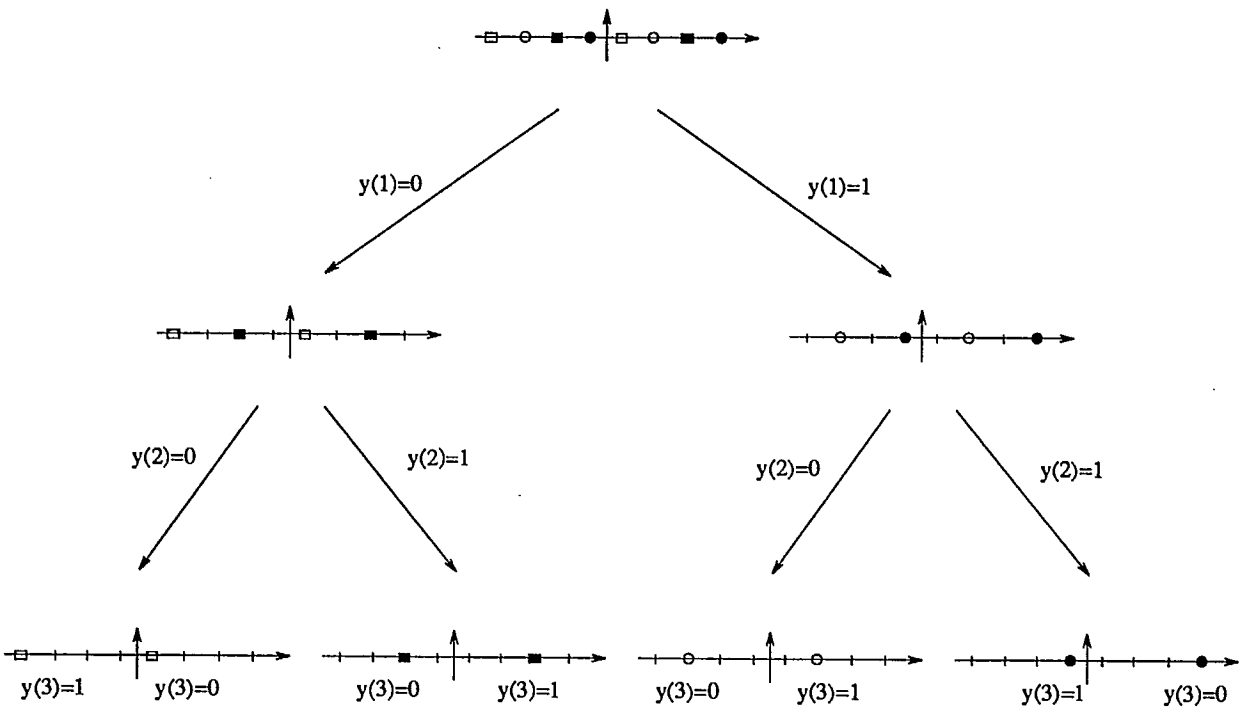

Figure 2.18: Fonction de *"mapping"* unidimensionnel utilisé pour le codage TCM-64QAM 2/3-2/3.

2.5.2 Expression de la probabilité d'erreur de la modulation codée TCM-64QAM à taux 2/3-2/3

Dans cette section, on dérive l'expression théorique asymptotique de la probabilité d'erreur par symbole pour la modulation TCM-64QAM 2/3-2/3. On note: $\mathcal{P}_{sym}^{(64_{2/3-2/3})}$ cette probabilité, et pour le cas d'une modulation TCM ordinaire: $\mathcal{P}_{sym}^{(N)}$, où N représente l'ordre de la modulation: 8 ou 32. Le symbole complexe S est constitué d'une composante en phase S_I et d'une composante en quadrature S_Q, i.e. $S = S_I + \jmath S_Q$, indédendantes l'une de l'autre. La probabilité d'erreur par symbole $\mathcal{P}_{sym}^{(N)}$ se calcule comme suit:

$$\begin{aligned}
\mathcal{P}_{sym}^{(64_{2/3-2/3})} &= \mathcal{P}\{S \text{ faux}\} \\
\mathcal{P}_{sym}^{(64_{2/3-2/3})} &= \mathcal{P}\{S_I \text{ faux } \vee S_Q \text{ faux}\} \qquad \text{car } S = S_I + \jmath S_Q \\
\mathcal{P}_{sym}^{(64_{2/3-2/3})} &= \mathcal{P}\{S_I \text{ faux}\} + \mathcal{P}\{S_Q \text{ faux}\} - \mathcal{P}\{S_I \text{ faux } \wedge S_Q \text{ faux}\} \\
\mathcal{P}_{sym}^{(64_{2/3-2/3})} &= \mathcal{P}\{S_I \text{ faux}\} + \mathcal{P}\{S_Q \text{ faux}\} - \mathcal{P}\{S_I \text{ faux}\}\,\mathcal{P}\{S_Q \text{ faux}\} \\
\mathcal{P}_{sym}^{(64_{2/3-2/3})} &= 2\mathcal{P}_{sym}^{(8)} - \left(\mathcal{P}_{sym}^{(8)}\right)^2 \qquad \text{car } S_I \text{ et } S_Q \text{ sont indépendants} \\
\mathcal{P}_{sym}^{(64_{2/3-2/3})} &\approx 2\mathcal{P}_{sym}^{(8)}
\end{aligned} \tag{2.10}$$

car pour des rapports signal-à-bruit élevés, et donc des valeurs de probabilité d'erreur par symbole unidimensionnel $\mathcal{P}_{sym}^{(8)}$ faibles, on a $\left(\mathcal{P}_{sym}^{(8)}\right)^2 \ll \mathcal{P}_{sym}^{(8)}$.

Avec les notations employées dans la section 2.5.3:

$$\mathcal{P}_{sym}^{(8)} = N_{libre} Q\left[\frac{d_{libre}}{\sqrt{2E_{sym}^{(8)}}}\sqrt{\rho}\right] \tag{2.11}$$

d'où l'expression finale de $\mathcal{P}_{sym}^{(64_{2/3-2/3})}$:

$$\mathcal{P}_{sym}^{(64_{2/3-2/3})} = 2N_{libre} Q\left[\frac{d_{libre}}{\sqrt{2E_{sym}^{(8)}}}\sqrt{\rho}\right] \tag{2.12}$$

à comparer avec:

$$\mathcal{P}_{sym}^{(32)} = N_{libre} Q\left[\frac{d_{libre}}{\sqrt{2E_{sym}^{(32)}}}\sqrt{\rho}\right] \tag{2.13}$$

Dans ces deux expressions, N_{libre} et d_{libre} dépendent du type de code TCM utilisé et ρ représente le rapport signal à bruit. La seule variable qui les differencie est l'énergie moyenne par symbole sur la constellation employée:

$$E_{sym}^{(8)} = \frac{21}{4}\Delta_0^2 \qquad \text{pour le TCM-64QAM 2/3-2/3}$$

$$E_{sym}^{(32)} = \frac{20}{4}\Delta_0^2 \qquad \text{pour le TCM 32-QAM}$$

et Δ_0 représente la distance euclidienne minimale entre symboles sur la constellation.

La théorie établit ainsi que les performances de la modulation TCM-64QAM 2/3-2/3 sont asymptotiquement légèrement inférieures à celles de la modulation TCM 32-QAM ordinaire. Cependant, elle apporte un gain en terme de complexité réduite du décodeur, puisque l'algorithme de Viterbi est appliqué à des signaux bruités modulés en amplitude d'ordre 3 au lieu de 5. Il est effectué deux fois sur les composantes en phase et en quadrature des signaux, mais ceci ne constitue pas une perte de temps: le décodage est réalisé parallèlement. Ce détail peut s'avérer d'une grande importance, notamment lors de l'implémentation réelle du système pour les signaux HDTV dont le très haut débit pourrait en pratique dépasser les capacités du démodulateur TCM 32-QAM ordinaire.

2.5.3 Résultats des simulations de la modulation codée TCM-64QAM à taux 2/3-2/3

Dans cette section, on présente les résultats des simulations de la modulation codée TCM-64QAM à taux 2/3-2/3. Les figures des pages suivantes donnent les courbes de probabilités d'erreur par symbole, i.e. $\mathcal{P}_{sym}$, calculées lors des simulations sur un même graphique que les courbes asymptotiques théoriques. On montre également les courbes de probabilités d'erreur par bit $\mathcal{P}_{bit}$ obtenues par simulation, les expressions analytiques de $\mathcal{P}_{bit}$ étant difficiles à obtenir même pour des treillis de Viterbi très simples.

Les simulations réalisées pour la modulation codée TCM-64QAM 2/3-2/3 donnent lieu à des marges d'erreurs plus ou moins significatives selon qu'il s'agisse de probabilité d'erreur par bit, $\mathcal{P}_{bit}$, ou par symbole, $\mathcal{P}_{sym}$. Les tests d'arrêt imposent un nombre d'erreurs par bit supérieur à 100 pour garantir une erreur relative de moins de 10% sur la probabilité d'erreur par bit. La probabilités d'erreur par symbole a une erreur relative beaucoup plus grande dans les hauts rapports signal-à-bruit, d'autant qu'un paquet d'erreur de 3, voire 4 bits, pourrait n'affecter qu'un seul symbole. Par exemple, sur une transition parallèle du treillis du codeur, il peut se produire un *événement erreur* sur un seul symbole, lequel affecte au moins 2 bits. C'est pourquoi, les courbes de probabilités d'erreur par bit sont représentées par des points avec leur intervalle de confiance qui est raisonable, alors que les courbes de probabilités d'erreur par symbole ont des marges d'erreurs plus grandes.

La figure 2.19 présente les courbes théoriques de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour trois types de modulation QAM M-aire: la modulation 16-QAM non-codée, la modulation codée TCM 32-QAM conventionnelle et la modulation codée TCM-64QAM à taux 2/3-2/3. Pour un rapport signal-à-bruit E_{sym}/N_0 suffisamment élevé, on note l'amélioration du taux d'erreur par symbole $\mathcal{P}_{sym}$ obtenue avec la modulation codée TCM comparativement à la modulation 16-QAM non-codée. La modulation codée TCM 32-QAM conventionnelle conduit à des résultats légèrement meilleurs que ceux obtenus avec la modulation codée TCM-64QAM 2/3-2/3 et ce, pour des treillis à 8 états (code TCM-QAM(3,2,3)) et à 64 états (code TCM-QAM(3,2,6)).

Les figures 2.14 et 2.20 montrent les courbes théoriques et expérimentales de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour les modulations TCM 32-QAM et TCM-64QAM 2/3-2/3 respectivement. Les résultats des simulations effectuées sur les deux mêmes types de code, i.e. TCM-QAM(3,2,3) et TCM-QAM(3,2,6), sont en accord avec les courbes asymptotiques théoriques. Notamment, les performances du système utilisant un codage TCM-64QAM 2/3-2/3 sont inférieures à celles du TCM 32-QAM ordinaire. La figure 2.21 donne une comparaison des courbes expérimentales de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction de E_{sym}/N_0 pour ces deux modulations codées TCM. On remarque toutefois que l'écart assez important dans le domaine des faibles rapports signal-à-bruit s'atténue sensiblement vers celui des hauts rapports. Il semble même,

en pratique, que dans le domaine d'utilisation du système, c'est-à-dire pour des probabilités d'erreur par bit proches de 10^{-5}, le codeur-décodeur TCM-64QAM 2/3-2/3 soit meilleur que l'autre.

Il est par contre moins intéressant de comparer les courbes de probabilités d'erreur des deux systèmes par symbole, puisque les symboles ont un format de bits different. Dans le cas de la modulation TCM-64QAM 2/3-2/3, les bits représentent deux symboles 8-aires au lieu d'un seul symbole 32-aire pour la modulation TCM 32-QAM conventionnelle. À la figure 2.22, on présente les courbes expérimentales de la probabilité d'erreur par bit $\mathcal{P}_{bit}$ en fonction du rapport signal-à-bruit E_{bit}/N_0 pour les modulations TCM 32-QAM et TCM-64QAM 2/3-2/3. On remarque encore une fois que la probabilité d'erreur décroît lorsque le nombre d'états du codeur TCM est plus grand. De plus, la modulation TCM 32-QAM donne, en général, des résultats meilleurs que le TCM-64QAM 2/3-2/3.

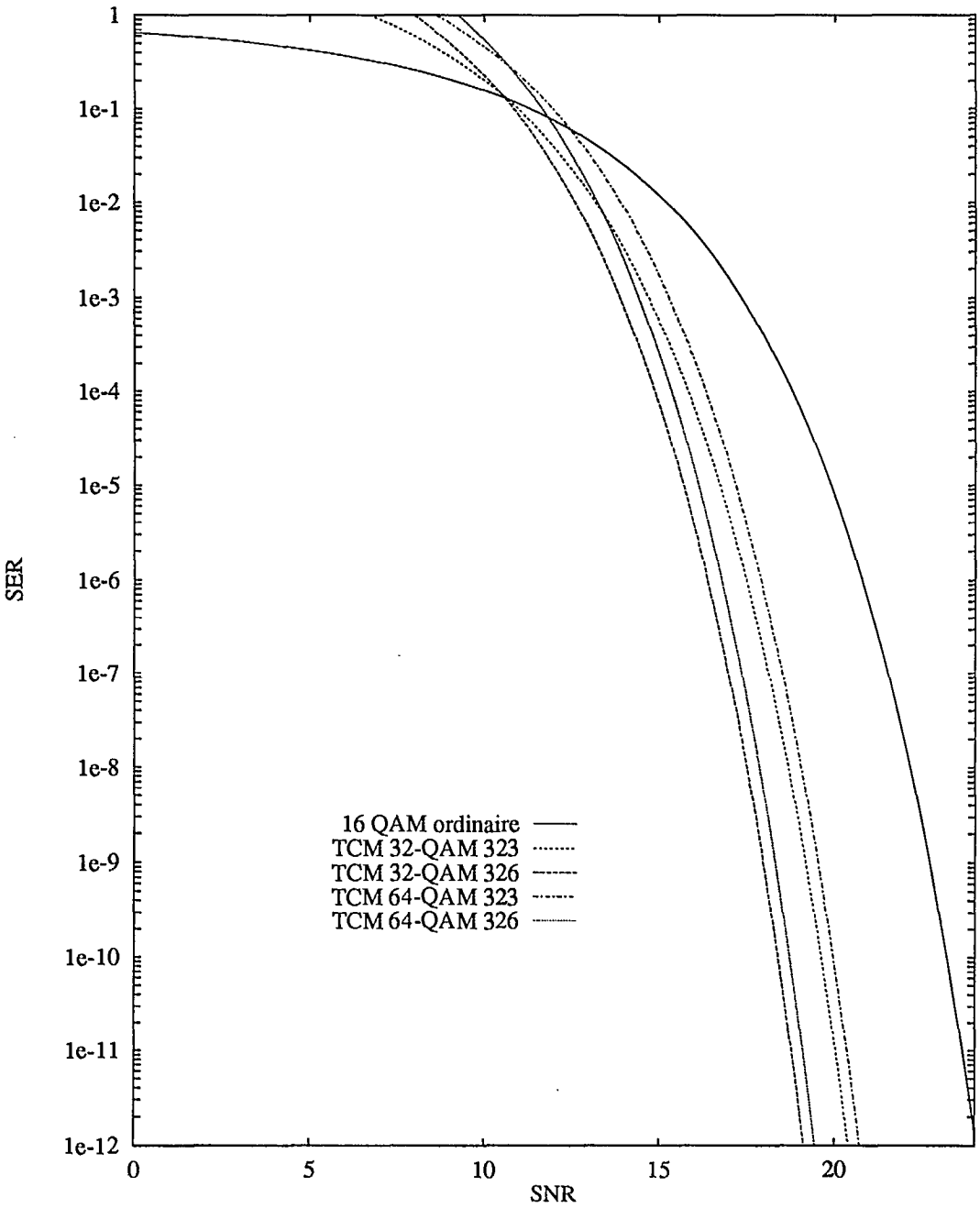

Figure 2.19: Courbes théoriques de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour les modulations 16-QAM, TCM 32-QAM et TCM-64QAM 2/3-2/3.

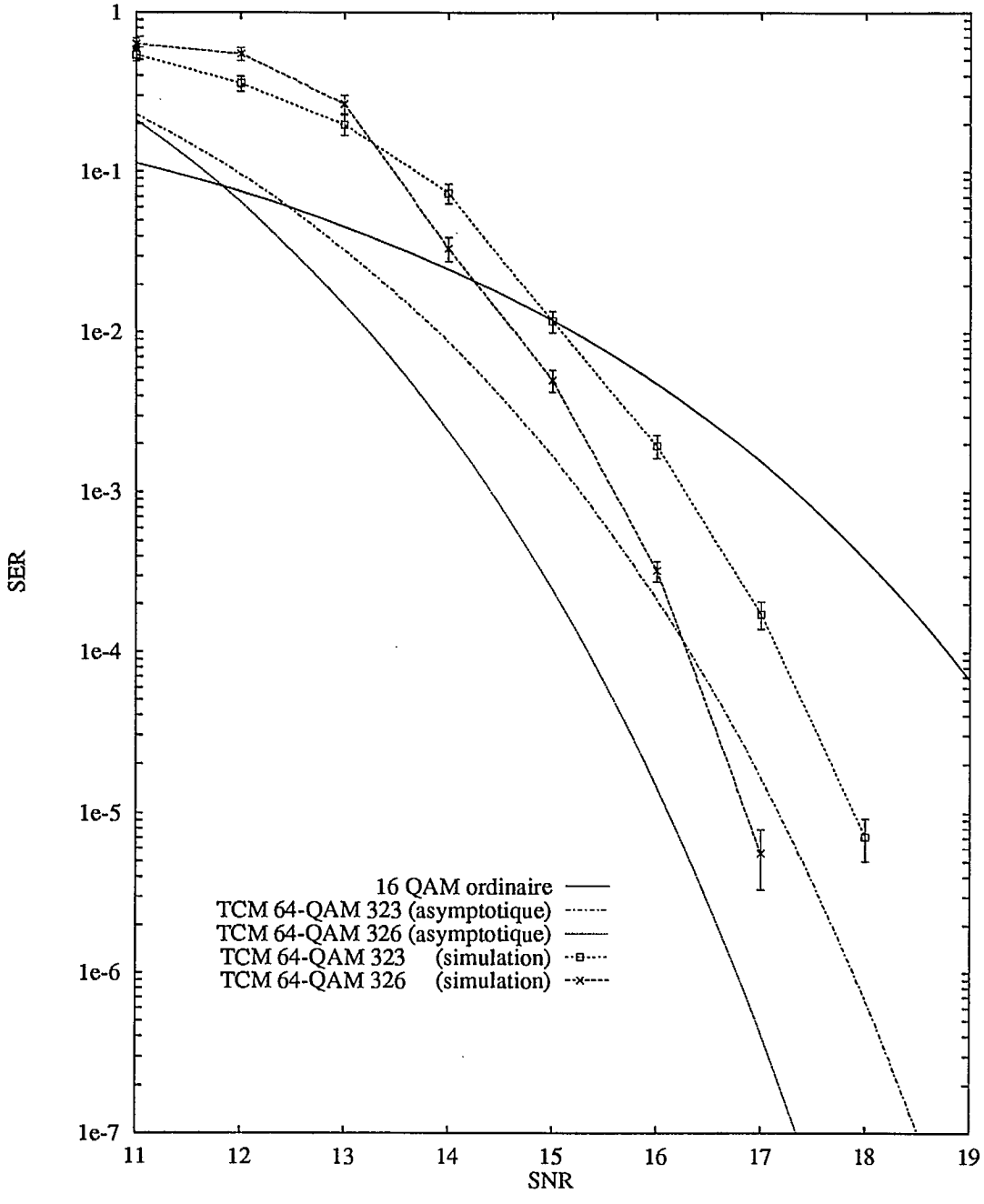

Figure 2.20: Courbes théoriques et expérimentales de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour la modulation TCM-64QAM 2/3-2/3.

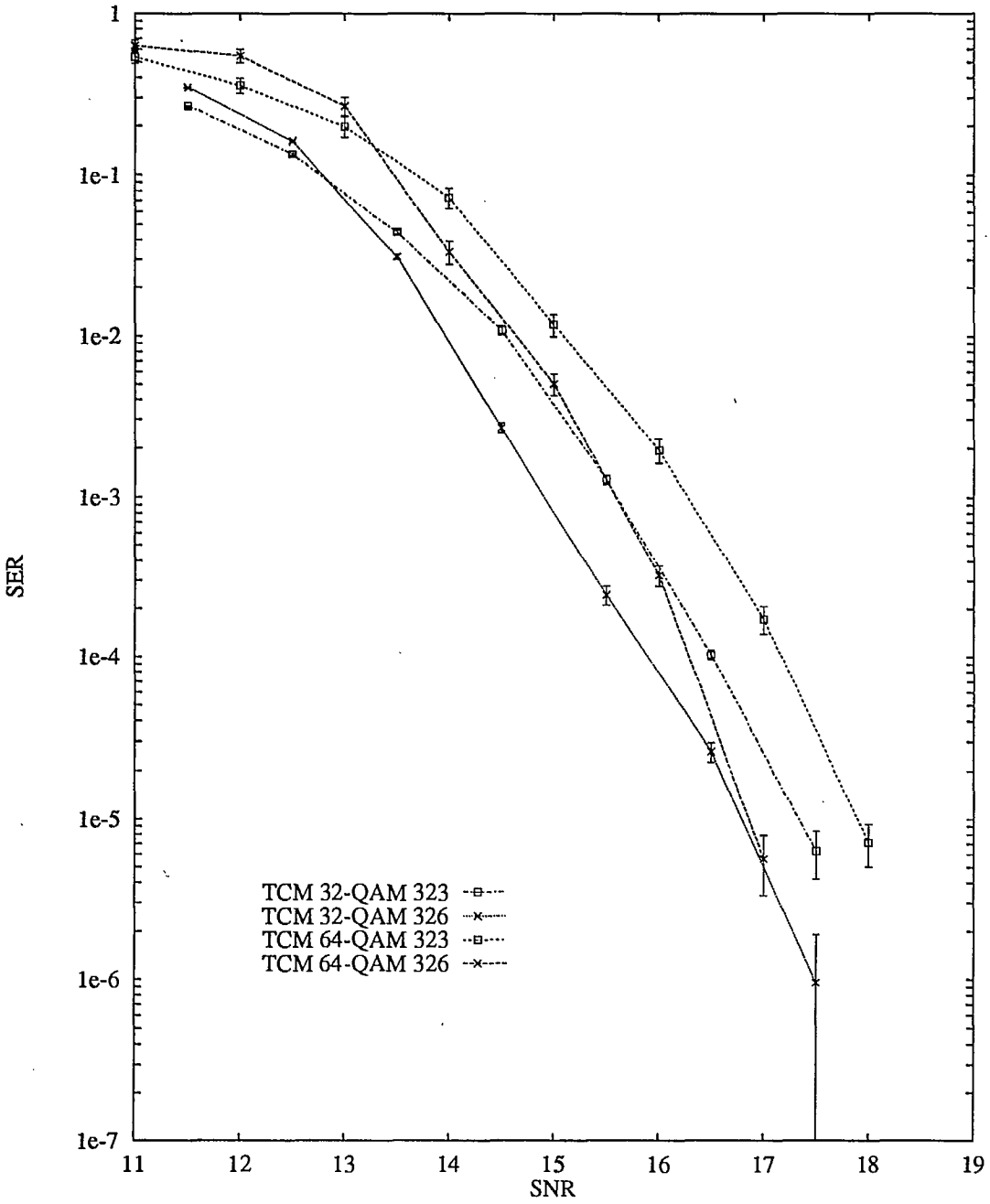

Figure 2.21: Comparaison des courbes expérimentales de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour les modulations TCM 32-QAM et TCM-64QAM 2/3-2/3.

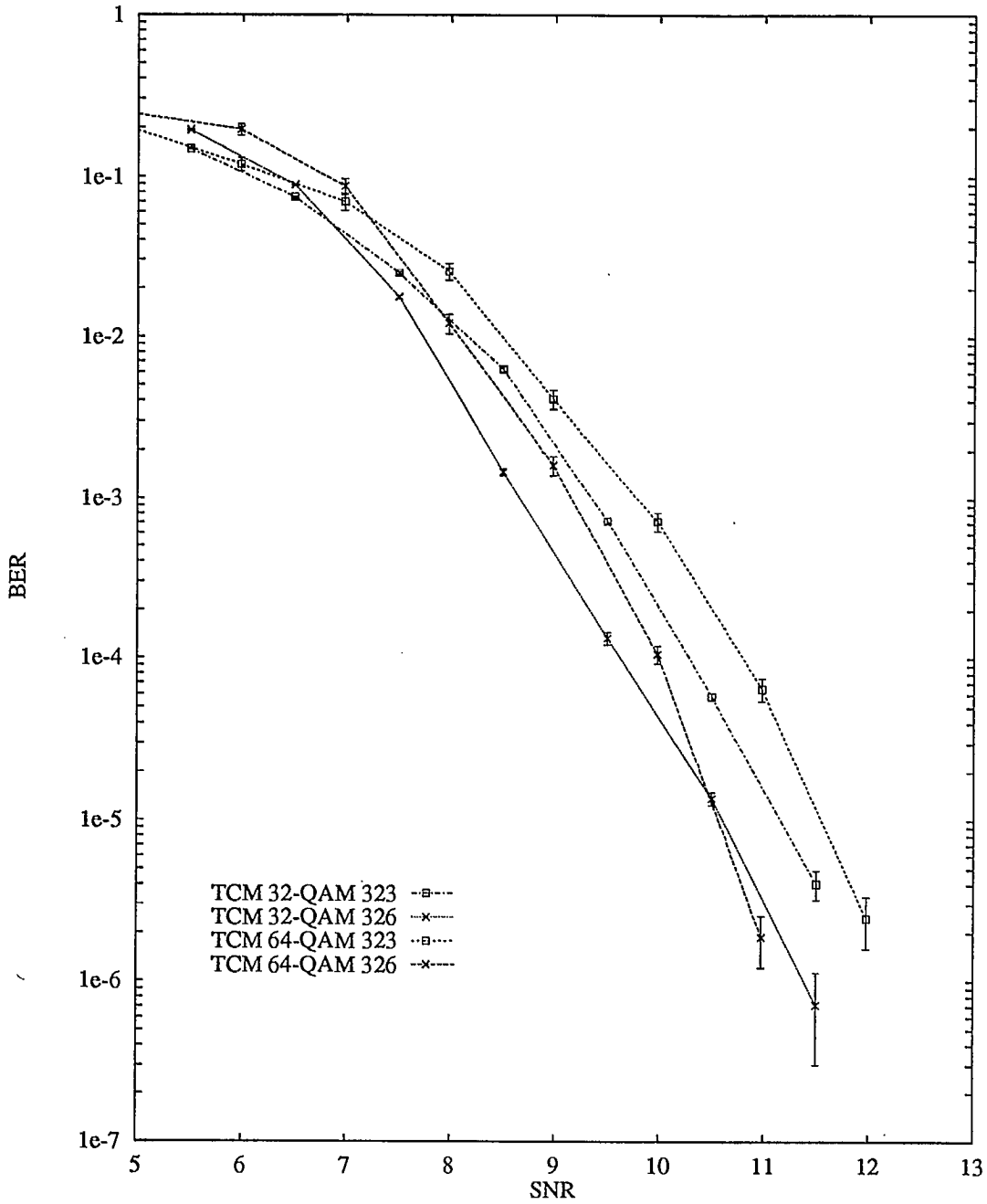

Figure 2.22: Courbes expérimentales de la probabilité d'erreur par bit $\mathcal{P}_{bit}$ en fonction du rapport signal-à-bruit par bit E_{bit}/N_0 pour les modulations TCM 32-QAM et TCM-64QAM 2/3-2/3.

2.6 Conclusion

Dans ce chapitre, on s'est intéressé essentiellement aux performances de la modulation TCM-QAM. Les paramètres réels de transmission ont permis de calculer l'efficacité spectrale des signaux de TVHD pouvant aller de 3 à 5 $bits/s/Hz$, ce que l'on rappelle dans le chapitre 1. Ici, nous nous sommes fixes à 4 $bits/s/Hz$, ce qui déterminait l'ordre de la modulation QAM à 32 niveaux. Le choix de la table de correspondance des symboles codés en sortie du codeur TCM a été guidé par la méthode systématique de partitionnement de la constellation proposée par Ungerboëck [Ung82]. Les figures 2.2 et 2.3 de la section 2.3.1 illustrent la construction et la position des signaux associés aux symboles et représentés en bande de base dans un plan complexe.

Le choix de bons codes a été lui aussi déterminé par les recherches de Ungerboëck, donnée par [Ung87b]. L'implémentation informatique des codes a été réalisée pour ces bons codes représentés dans la section 2.4. Les deux derniers, en raison de leur plus grande complexité, n'ont pas été utilisés dans les simulations, et ne sont précisés que sous la forme de leur définition par les polynômes de connection h_0 h_1, et h_2, et de leur performances théoriques asymptotiques, c'est-à-dire leur gain asymptotique γ, leur distance libre d_{libre}, et le nombre moyen N_libre de chemins situés à une distance d_{libre} l'un de l'autre.

Une discussion sur ces paramètres asymptotiques s'ensuit, et le tracé des courbes théoriques permet de les visualiser mieux. Les simulations ont été réalisées en bande de base, avec un débit normalisé à 1 bit/s, ce qui n'affecte nullement ni les performances du système, ni leur estimation. Une lecture détaillée des programmes permettrait de vérifier que la mesure des probabilités d'erreurs a été faite sans suréchantillonnage puisque la mise en forme du signal n'est pas nécessaire, en l'absence d'égalisateur et de système de synchronisation, supposée parfaite.

Les résultats de ces simulations, pour la modulation TCM-32QAM conventionnelle ainsi que pour la modulation TCM-64QAM à taux 2/3-2/3, donnent la satisfaction de se rapprocher sensiblement des courbes asymptotiques théoriques et de la possibilité, dans le cas du bruit additif gaussien, d'améliorer davantage les performances du système grâce à la concaténation de codes Reed-Solomon bien adaptés aux paquets d'erreurs générés par le décodage de Viterbi.

D'autres résultats avec une source d'interférence co-canal dans la même bande de fréquence que le signal TVHD, démontrent la nécessité de s'affranchir au maximum des dégradations catastrophiques qu'apportent cette source d'interférence.

Chapitre 3

Codes correcteurs concaténés Reed-Solomon et modulation codée TCM-QAM

3.1 Introduction

À la sortie du décodeur TCM, on retrouve soit des mot-codes sans erreur soit des mot-codes avec des erreurs regroupés selon que le symbole M-aire QAM est, ou non, décodé correctement. Afin d'éliminer la plupart des *paquets* d'erreurs résultant des décodages erronés des symboles QAM, on peut utiliser des codes de correction de paquets d'erreurs (en anglais: "error-bursts"), tels que les codes Fire ou les codes Reed-Solomon. Pour les simulations, on a choisi les codes Reed-Solomon en raison de leur capacité de correction, de leur flexibilité ainsi que de leur popularité.

3.2 Codes correcteurs de groupements d'erreurs Reed-Solomon

3.2.1 Paramètres de codes correcteurs Reed-Solomon

La liste qui suit donne les paramètres de codes correcteurs Reed-Solomon employés pour faire les simulations. Les premiers codes, i.e. les codes $RS(15, 9, 3)$, $RS(120, 108)$, $RS(160, 144, 8)$ et $RS(200, 180, 10)$, ne sont inclus dans la liste qu'à titre indicatif: le code $RS(15, 9, 3)$ a

servi à vérifier le bon fonctionnement de l'algorithme de décodage l'algorithme de Peterson-Gorenstein-Zierler.

Les Corps de Galois utilisés dans ce rapport pour déterminer les differents polynômes générateurs $g(x)_{RS(n,k,t)}$ des codes correcteurs Reed-Solomon $RS(n,k,t)$ sont décrits en détail à l'annexe A (voir page 64 et suivantes).

Code $RS(15,9,3)$:

- Corps de Galois $GF(q) = GF(2^m) = GF(2^4)$
- Longueur des mots-codes $n = 15$; $n' = 2^m - 1 = 2^4 - 1 = 15$ symboles hexadécimaux
- Nombre de symboles d'information $k = 9$; $k' = 9$ symboles hexadécimaux
- Capacité de correction $t = 3$ symboles hexadécimaux
- Taux du code $R_c = 60\%$ (redondance: $\frac{n-k}{n} = 40\%$)

Polynôme générateur $g(x)_{RS(15,9,3)}$ du code $RS(15,9,3)$:

$$\begin{aligned} g(x)_{RS(15,9,3)} &= (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6) \\ g(x)_{RS(15,9,3)} &= x^6 + \alpha^{10}\, x^5 + \alpha^{14}\, x^4 + \alpha^4\, x^3 + \alpha^6\, x^2 + \alpha^9\, x + \alpha^6 \end{aligned}$$

Code $RS(120, 108, 6)$:

- Corps de Galois $GF(q) = GF(2^m) = GF(2^7)$
- Longueur des mots-codes $n = 120$; $n' = 2^m - 1 = 2^7 - 1 = 127$ mots de 7 bits
- Nombre de symboles d'information $k = 108$; $k' = 115$ mots de 7 bits
- Capacité de correction $t = 6$ mots de 7 bits
- Taux du code $R_c = 90\%$ (redondance: $\frac{n-k}{n} = 10\%$)

Polynôme générateur $g(x)_{RS(120,108,6)}$ du code $RS(120, 108, 6)$:

$$\begin{aligned} g(x)_{RS(120,108,6)} &= \prod_{i=1}^{2t}(x - \alpha^i) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)\dots(x - \alpha^{11})(x - \alpha^{12}) \\ g(x)_{RS(120,108,6)} &= x^{12} + \alpha^{125}\, x^{11} + \alpha^{99}\, x^{10} + \alpha^{5}\, x^{9} + \alpha^{56}\, x^{8} + \alpha^{100}\, x^{7} + \alpha^{95}\, x^{6} + \\ &\quad \alpha^{113}\, x^{5} + \alpha^{82}\, x^{4} + \alpha^{44}\, x^{3} + \alpha^{24}\, x^{2} + \alpha^{63}\, x + \alpha^{78} \end{aligned}$$

Code $RS(160, 144, 8)$:

- Corps de Galois $GF(q) = GF(2^m) = GF(2^8)$
- Longueur des mots-codes $n = 160$; $n' = 2^m - 1 = 2^8 - 1 = 255$ octets
- Nombre de symboles d'information $k = 144$; $k' = 239$ octets
- Capacité de correction $t = 8$ octets
- Taux du code $R_c = 90\%$ (redondance: $\frac{n-k}{n} = 10\%$)

Polynôme générateur $g(x)_{RS(160,144,8)}$ du code $RS(160, 144, 8)$:

$$\begin{aligned} g(x)_{RS(160,144,8)} &= \prod_{i=1}^{2t}(x - \alpha^i) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)\dots(x - \alpha^{15})(x - \alpha^{16}) \\ g(x)_{RS(160,144,8)} &= x^{16} + \alpha^{121}\, x^{15} + \alpha^{106}\, x^{14} + \alpha^{110}\, x^{13} + \alpha^{113}\, x^{12} + \alpha^{107}\, x^{11} + \\ &\quad \alpha^{167}\, x^{10} + \alpha^{83}\, x^{9} + \alpha^{11}\, x^{8} + \alpha^{100}\, x^{7} + \alpha^{201}\, x^{6} + \alpha^{158}\, x^{5} + \\ &\quad \alpha^{181}\, x^{4} + \alpha^{195}\, x^{3} + \alpha^{208}\, x^{2} + \alpha^{240}\, x + \alpha^{136} \end{aligned}$$

Code $RS(200, 180, 10)$:

- Corps de Galois $GF(q) = GF(2^m) = GF(2^8)$
- Longueur des mots-codes $n = 200$; $n' = 2^m - 1 = 2^8 - 1 = 255$ octets
- Nombre de symboles d'information $k = 180$; $k' = 235$ octets
- Capacité de correction $t = 10$ octets
- Taux du code $R_c = 90\%$ (redondance: $\frac{n-k}{n} = 10\%$)

Polynôme générateur $g(x)_{RS(200,180,10)}$ du code $RS(200, 180, 10)$:

$$
\begin{aligned}
g(x)_{RS(200,180,10)} &= \prod_{i=1}^{2t}(x - \alpha^i) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)\dots(x - \alpha^{19})(x - \alpha^{20}) \\
g(x)_{RS(200,180,10)} &= x^{20} + \alpha^{18}\, x^{19} + \alpha^{62}\, x^{18} + \alpha^{82}\, x^{17} + \alpha^{54}\, x^{16} + \alpha^{66}\, x^{15} + \\
&\quad \alpha^{169}\, x^{14} + \alpha^{33}\, x^{13} + \alpha^{195}\, x^{12} + \alpha^{211}\, x^{11} + \alpha^{190}\, x^{10} + \alpha^{232}\, x^9 + \\
&\quad \alpha^{237}\, x^8 + \alpha^{96}\, x^7 + \alpha^{253}\, x^6 + \alpha^{171}\, x^5 + \alpha^{180}\, x^4 + \alpha^{229}\, x^3 + \\
&\quad \alpha^{230}\, x^2 + \alpha^{207}\, x + \alpha^{210}
\end{aligned}
$$

Code $RS(208, 188, 10)$:

- Corps de Galois $GF(q) = GF(2^m) = GF(2^8)$
- Longueur des mots-codes $n = 208$; $n' = 2^m - 1 = 2^8 - 1 = 255$ octets
- Nombre de symboles d'information $k = 188$; $k' = 235$ octets
- Capacité de correction $t = 10$ octets
- Taux du code $R_c = 90.385\% \approx 90\%$ (redondance: $\frac{n-k}{n} = 9.615\% \approx 10\%$)

Polynôme générateur $g(x)_{RS(208,188,10)}$ du code $RS(208, 188, 10)$:

$$
\begin{aligned}
g(x)_{RS(208,188,10)} &= \prod_{i=1}^{2t}(x - \alpha^i) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)\dots(x - \alpha^{19})(x - \alpha^{20}) \\
g(x)_{RS(208,188,10)} &= x^{20} + \alpha^{18}\, x^{19} + \alpha^{62}\, x^{18} + \alpha^{82}\, x^{17} + \alpha^{54}\, x^{16} + \alpha^{66}\, x^{15} + \\
&\quad \alpha^{169}\, x^{14} + \alpha^{33}\, x^{13} + \alpha^{195}\, x^{12} + \alpha^{211}\, x^{11} + \alpha^{190}\, x^{10} + \alpha^{232}\, x^9 + \\
&\quad \alpha^{237}\, x^8 + \alpha^{96}\, x^7 + \alpha^{253}\, x^6 + \alpha^{171}\, x^5 + \alpha^{180}\, x^4 + \alpha^{229}\, x^3 + \\
&\quad \alpha^{230}\, x^2 + \alpha^{207}\, x + \alpha^{210}
\end{aligned}
$$

Code $RS(255, 239, 8)$:

- Corps de Galois $GF(q) = GF(2^m) = GF(2^8)$
- Longueur des mots-codes $n = 255$; $n' = 2^m - 1 = 2^8 - 1 = 255$ octets
- Nombre de symboles d'information $k = 188$; $k' = 235$ octets
- Capacité de correction $t = 8$ octets
- Taux du code $R_c = 93.725\% \approx 94\%$ (redondance: $\frac{n-k}{n} = 6.275\% \approx 6\%$)

Polynôme générateur $g(x)_{RS(255,239,8)}$ du code $RS(255, 239, 8)$:

$$
\begin{aligned}
g(x)_{RS(255,239,8)} &= \prod_{i=1}^{2t}(x - \alpha^i) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)\dots(x - \alpha^{15})(x - \alpha^{16}) \\
g(x)_{RS(255,239,8)} &= x^{16} + \alpha^{121}\, x^{15} + \alpha^{106}\, x^{14} + \alpha^{110}\, x^{13} + \alpha^{113}\, x^{12} + \alpha^{107}\, x^{11} + \\
&\quad \alpha^{167}\, x^{10} + \alpha^{83}\, x^9 + \alpha^{11}\, x^8 + \alpha^{100}\, x^7 + \alpha^{201}\, x^6 + \alpha^{158}\, x^5 + \\
&\quad \alpha^{181}\, x^4 + \alpha^{195}\, x^3 + \alpha^{208}\, x^2 + \alpha^{240}\, x + \alpha^{136}
\end{aligned}
$$

3.2.2 Algorithme de décodage de Peterson-Gorenstein-Zierler

Il existe plusieurs manières de décoder les mot-codes Reed-Solomon corrompus par le canal de transmission. Parmi celles-ci on note l'algorithme de décodage de Berlekamp-Massey [LC83, CDG92] et l'algorithme de Peterson-Gorenstein-Zierler [Ple89, Bla84]. C'est cette dernière méthode, c'est-à-dire celle de Peterson-Gorenstein-Zierler décrite dans cette section, qui est utilisée pour effectuer les simulations par ordinateur du système de télécommunication numérique TVHD.

Algorithme de décodage de Peterson-Gorenstein-Zierler

1. Calculer les syndromes $S_i = \mathbf{v}(\alpha^i)$, for $i = 1, \ldots, 2t$

2. Déterminer le rang ν de la matrice des syndromes de sorte que la sous-matrice M soit non singulière:

$$M = \begin{pmatrix} S_1 & S_2 & \cdots & S_\nu \\ S_2 & S_3 & \cdots & S_{\nu+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_\nu & S_{\nu+1} & \cdots & S_{2\nu-1} \end{pmatrix}$$

   Débuter avec $\nu = t$, vérifier si le déterminant $\det(M) = 0$. Si $\det(M) \neq 0$, passer à l'étape suivante, sinon recommencer avec $\nu = \nu - 1$.

3. Calcul du polynôme de localisation d'erreurs $\Lambda(x)$ en utilisant l'inverse de la sous-matrice M:

$$\begin{pmatrix} \Lambda_\nu \\ \Lambda_{\nu-1} \\ \vdots \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} S_1 & S_2 & \cdots & S_\nu \\ S_2 & S_3 & \cdots & S_{\nu+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_\nu & S_{\nu+1} & \cdots & S_{2\nu-1} \end{pmatrix}^{-1} \begin{pmatrix} -S_{\nu+1} \\ -S_{\nu+2} \\ \vdots \\ -S_{2\nu} \end{pmatrix}$$

4. Trouver les racines en résolvant $\Lambda(x) = 0$ pour déterminer la position des erreurs, i.e. X_l pour $l = 1, \ldots, \nu$.

5. Calculer le poids des ν erreurs en solutionnant le système:

$$\begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_\nu \end{pmatrix} = \begin{pmatrix} X_1 & X_2 & \cdots & X_\nu \\ X_1^2 & X_2^2 & \cdots & X_\nu^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^\nu & X_2^\nu & \cdots & X_\nu^\nu \end{pmatrix}^{-1} \begin{pmatrix} S_1 \\ S_2 \\ \vdots \\ S_\nu \end{pmatrix}$$

6. Additionner au vecteur reçu $\mathbf{v}(x)$, la sous-séquence d'erreur calculée (i.e. position et poids des erreurs) $\hat{\mathbf{e}}(x)$ afin de corriger le mot-code:

$$\hat{\mathbf{c}}(x) = \mathbf{v}(x) + \hat{\mathbf{e}}(x)$$

3.3 Résultats des simulations pour les codes concaténés Reed-Solomon et la modulation codée TCM-QAM

Les courbes expérimentales (i.e., obtenues des simulations sur ordinateur) de probabilités d'erreur par symbole $\mathcal{P}_{sym}$, de probabilités d'erreur par bit $\mathcal{P}_{bit}$ en fonction du rapport signal-à-bruit, présentées dans cette section, indiquent les performances des codes Reed-Solomon concaténés avec la modulation codée TCM-QAM. On considère ici deux codes Reed-Solomon: les codes RS(208,188,10) et RS(255,239,8), corrigeant respectivement jusqu'à 10 et 8 octets inclusivement par mot-code. Ces codes Reed-Solomon sont utilisés conjointement avec la modulation codée: le TCM-32QAM bidimensionnel et TCM-64QAM 2/3-2/3 bi-unidimensionnel. Pour la modulation codée, deux profondeurs de treillis sont représentées: un treillis à 8 états pour le code TCM(3,2,3) alors que le treillis du code TCM(3,2,6) comporte 64 états. On s'intéresse aussi à l'effet de l'entrelacement des symboles entre la sortie de l'encodeur Reed-Solomon et l'entrée de l'encodeur TCM-QAM: la profondeur d'entrelacement est fixée à 8 mot-codes.

Les figures 3.1 et 3.2 donnent les courbes expérimentales de la probabilité d'erreur en fonction du rapport signal-à-bruit, par symbole $\mathcal{P}_{sym}$ versus E_{sym}/N_0 et par bit $\mathcal{P}_{bit}$ versus E_{bit}/N_0 respectivement, pour le code Reed-Solomon RS(208,188,10) avec les codes TCM(3,2,3) et TCM(3,2,6) pour la modulation TCM 32-QAM. On remarque une nette amélioration de la performance lorsque l'on passe d'une profondeur d'entrelacement de 1 (c'est-à-dire, sans entrelacement) à une profondeur d'entrelacement égale à 8, et ce pour les probabilités d'erreur par symbole $\mathcal{P}_{sym}$ et par bit $\mathcal{P}_{bit}$.

Les courbes expérimentales de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour les codes Reed-Solomon RS(208,188,10) et RS(255,239,8) avec la modulation TCM 32-QAM (codes TCM(3,2,3) et TCM(3,2,6)) avec entrelacement sont illustrées aux figures 3.3 et 3.5 respectivement. Que l'on choisisse la modulation codée TCM-32QAM ou le TCM-64QAM 2/3-2/3, on arrive à des performances comparables. Cependant, le nombre d'états du treillis de Viterbi influence la performance, et ce, pour les deux codes TCM: le code TCM(3,2,6) est toujours meilleur que le TCM(3,2,3). La probabilité d'erreur par bit $\mathcal{P}_{bit}$ en fonction du rapport signal-à-bruit E_{bit}/N_0 obtenue avec le code Reed-Solomon RS(255,239,8) concaténé avec la modulation TCM 32-QAM (figure 3.6) donne des résultats semblables lorsque l'on compare ce code Reed-Solomon avec le code plus performant RS(208,188,10) (figure 3.4).

Les figures 3.7 et 3.8, quant à elles montrent la probabilité de décodage erronné d'un mot-code Reed-Solomon en fonction du rapport signal-à-bruit E_{sym}/N_0 pour les codes Reed-Solomon RS(208,188,10) et RS(255,239,8) lorsque ceux-ci sont concaténés avec la modulation TCM 32-QAM. Ici encore, on a choisi les codes TCM(3,2,3) et TCM(3,2,6) pour la modulation codée TCM 32-QAM. L'entrelacement se fait encore sur 8 mot-codes Reed-Solomon.

Tel que prévu, le code Reed-Solomon RS(208,188,10) conduit à de meilleurs résultats que le code RS(255,239,8) en raison de sa plus grande capacité de correction, c'est-à-dire 10 octets pour le premier comparativement à seulement 8 pour le second. Le nombre d'états du code en treillis TCM-QAM affecte aussi le taux d'erreur de décodage des mots-codes: le code TCM-QAM(3,2,6) conduit invariablement à une probabilité d'erreur $\mathcal{P}_{mot-code}$ plus petite que le code TCM(3,2,3). Enfin, on remarque la faible difference entre les performances obtenues avec les deux méthodes de modulation codée: le TCM-32QAM et TCM-64QAM 2/3-2/3.

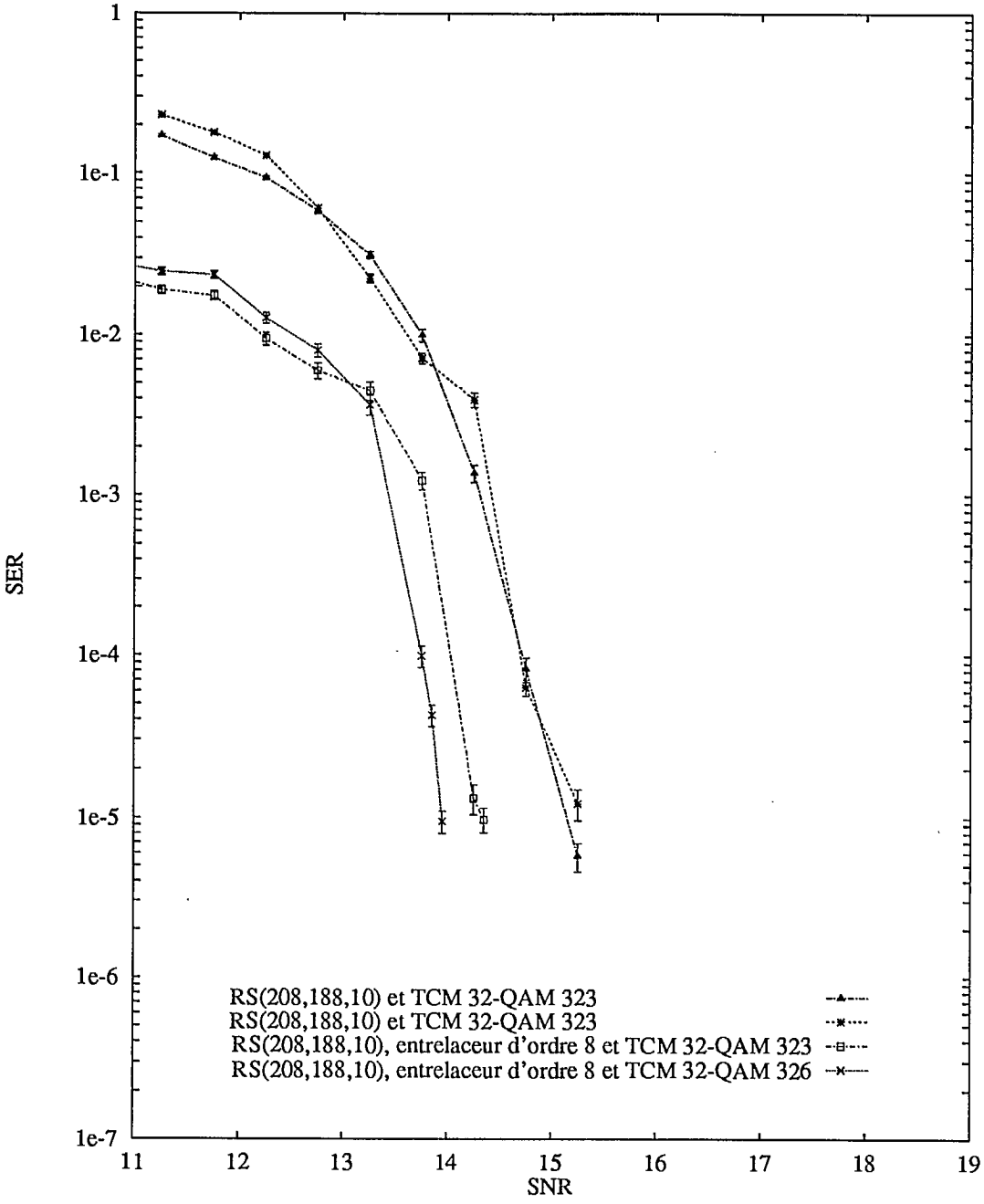

Figure 3.1: Courbes expérimentales de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour le code Reed-Solomon RS(208,188,10) avec la modulation TCM 32-QAM (codes TCM(3,2,3) et TCM(3,2,6)) avec et sans entrelacement.

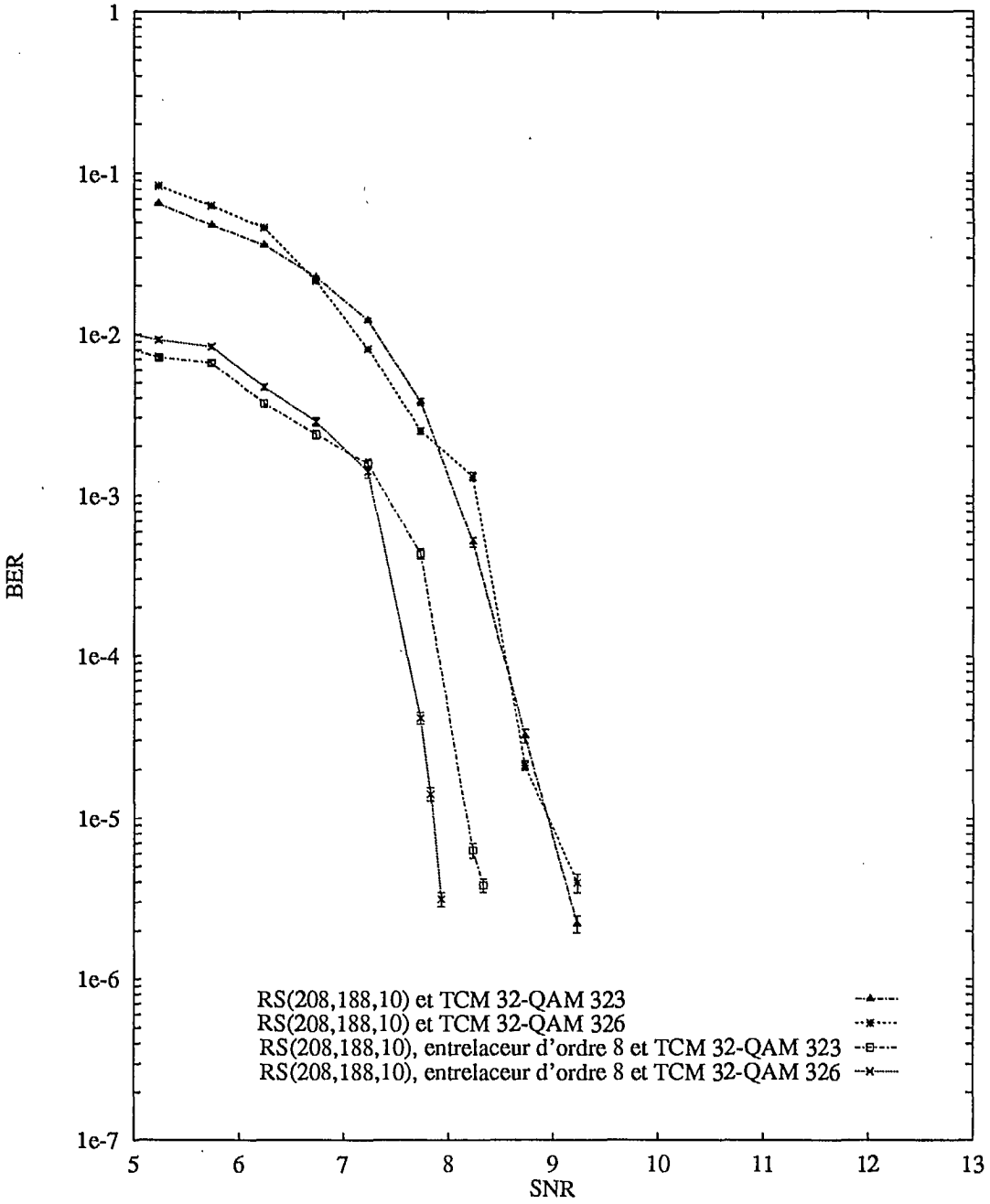

Figure 3.2: Courbes expérimentales de la probabilité d'erreur par bit $\mathcal{P}_{bit}$ en fonction du rapport signal-à-bruit E_{bit}/N_0 pour le code Reed-Solomon RS(208,188,10) avec la modulation TCM 32-QAM (codes TCM(3,2,3) et TCM(3,2,6)) avec et sans entrelacement.

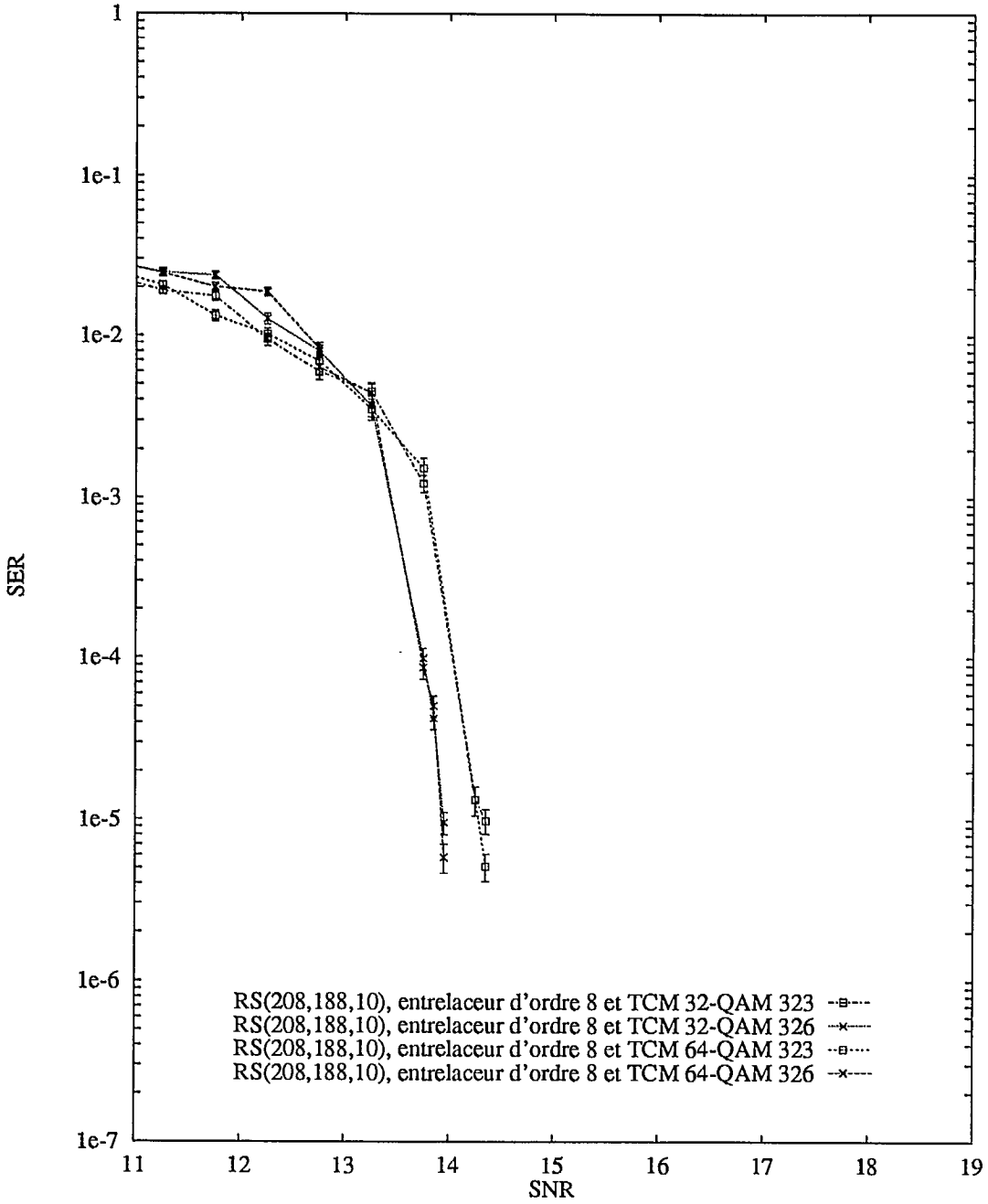

Figure 3.3: Courbes expérimentales de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour le code Reed-Solomon RS(208,188,10) avec les modulations TCM-32QAM et TCM-64QAM 2/3-2/3 (profondeur d'entrelacement: 8).

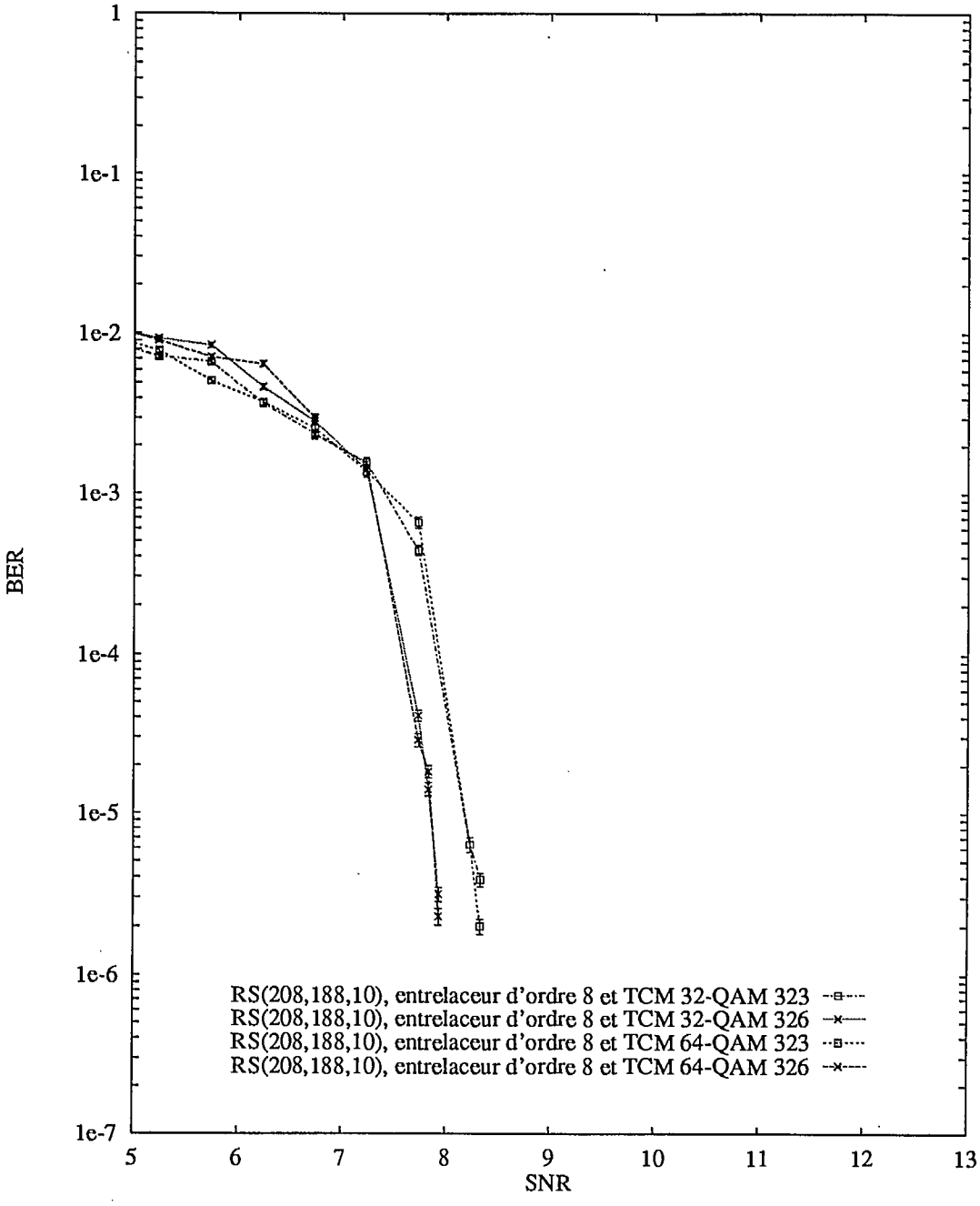

Figure 3.4: Courbes expérimentales de la probabilité d'erreur par bit $\mathcal{P}_{bit}$ en fonction du rapport signal-à-bruit E_{bit}/N_0 pour le code Reed-Solomon RS(208,188,10) avec les modulations TCM-32QAM et TCM-64QAM 2/3-2/3 (profondeur d'entrelacement: 8).

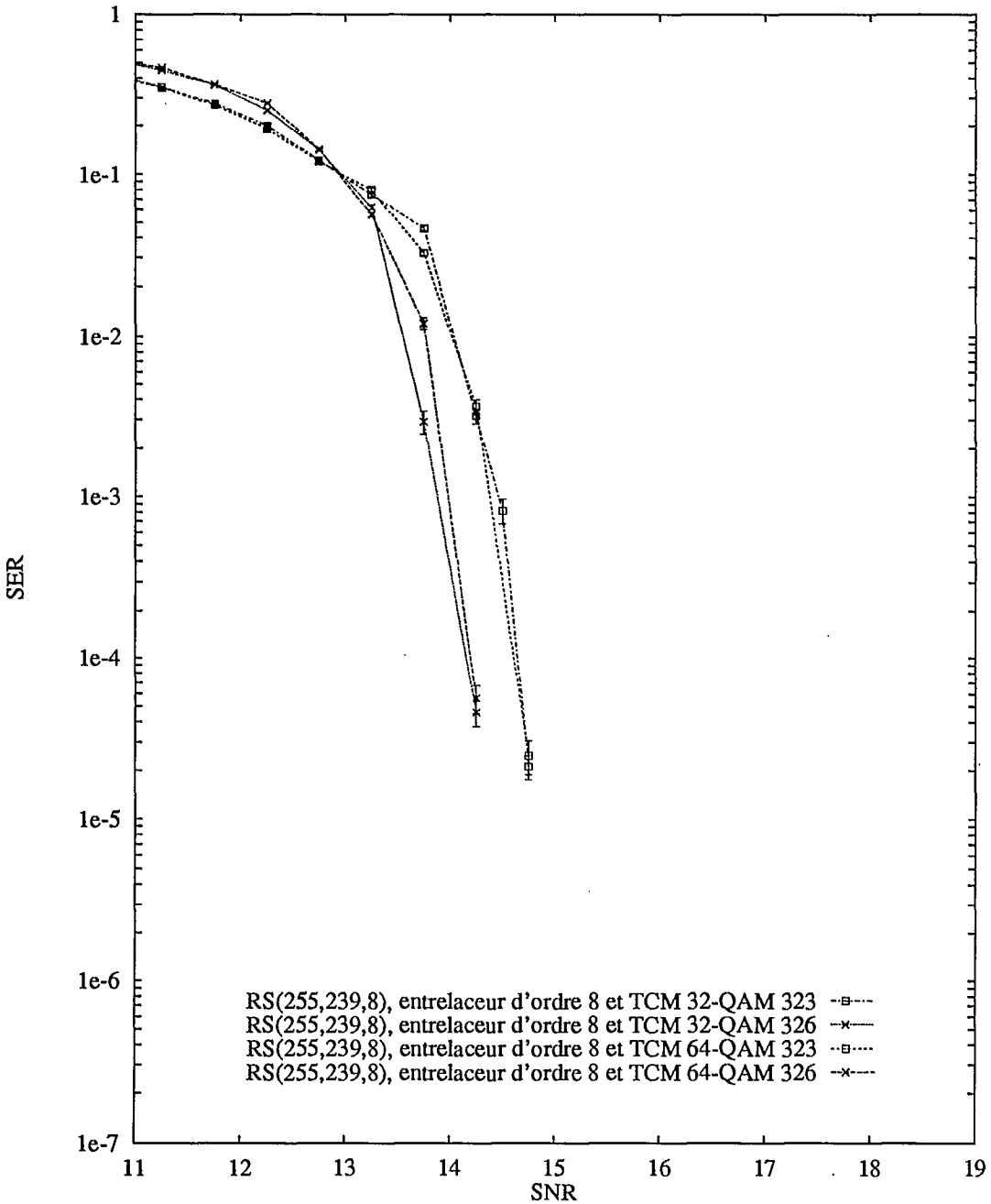

Figure 3.5: Courbes expérimentales de la probabilité d'erreur par symbole $\mathcal{P}_{sym}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour le code Reed-Solomon RS(255,239,8) avec les modulations TCM-32QAM et TCM-64QAM 2/3-2/3 (profondeur d'entrelacement: 8).

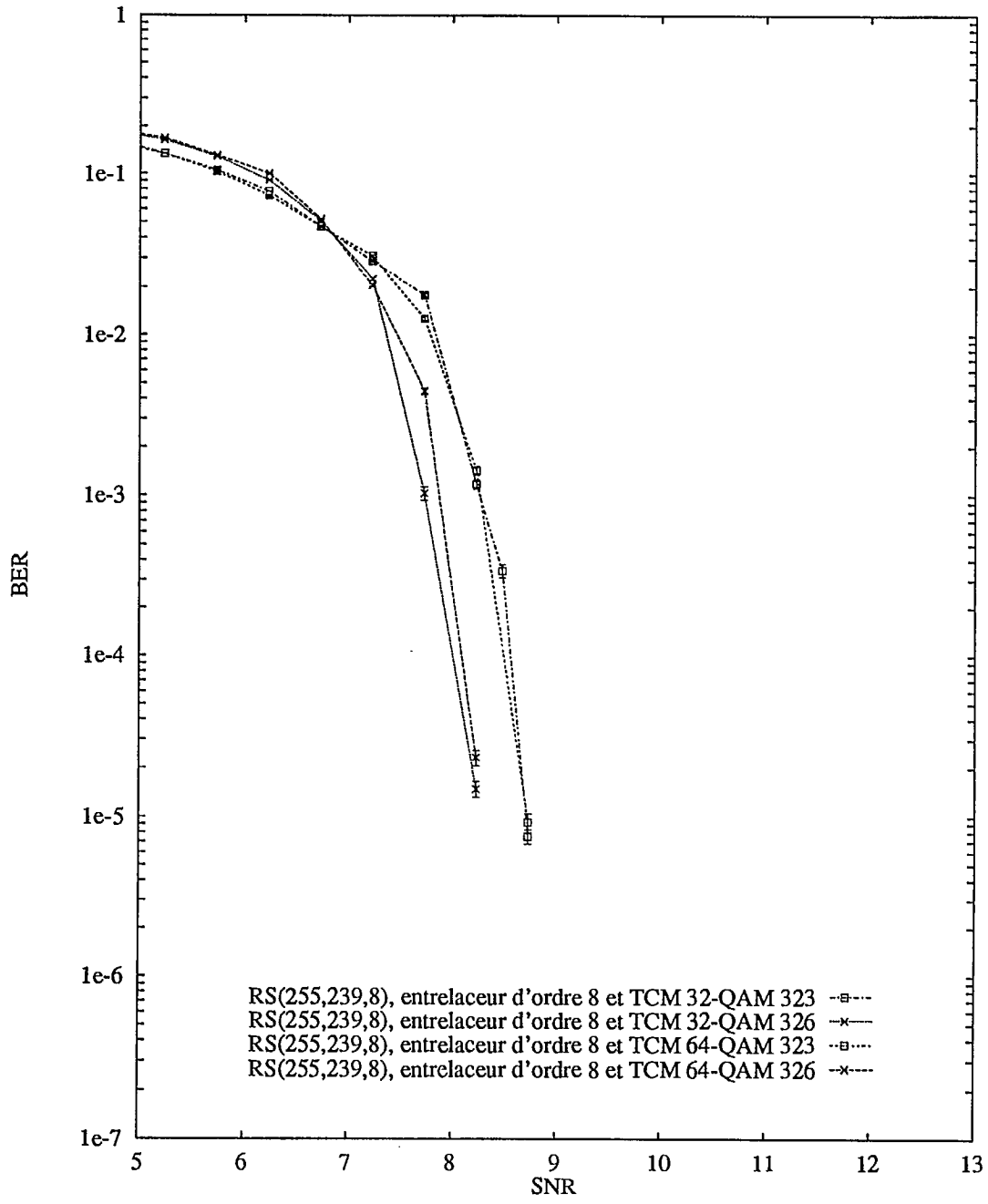

Figure 3.6: Courbes expérimentales de la probabilité d'erreur par bit $\mathcal{P}_{bit}$ en fonction du rapport signal-à-bruit E_{bit}/N_0 pour le code Reed-Solomon RS(255,239,8) avec les modulations TCM-32QAM et TCM-64QAM 2/3-2/3 (profondeur d'entrelacement: 8).

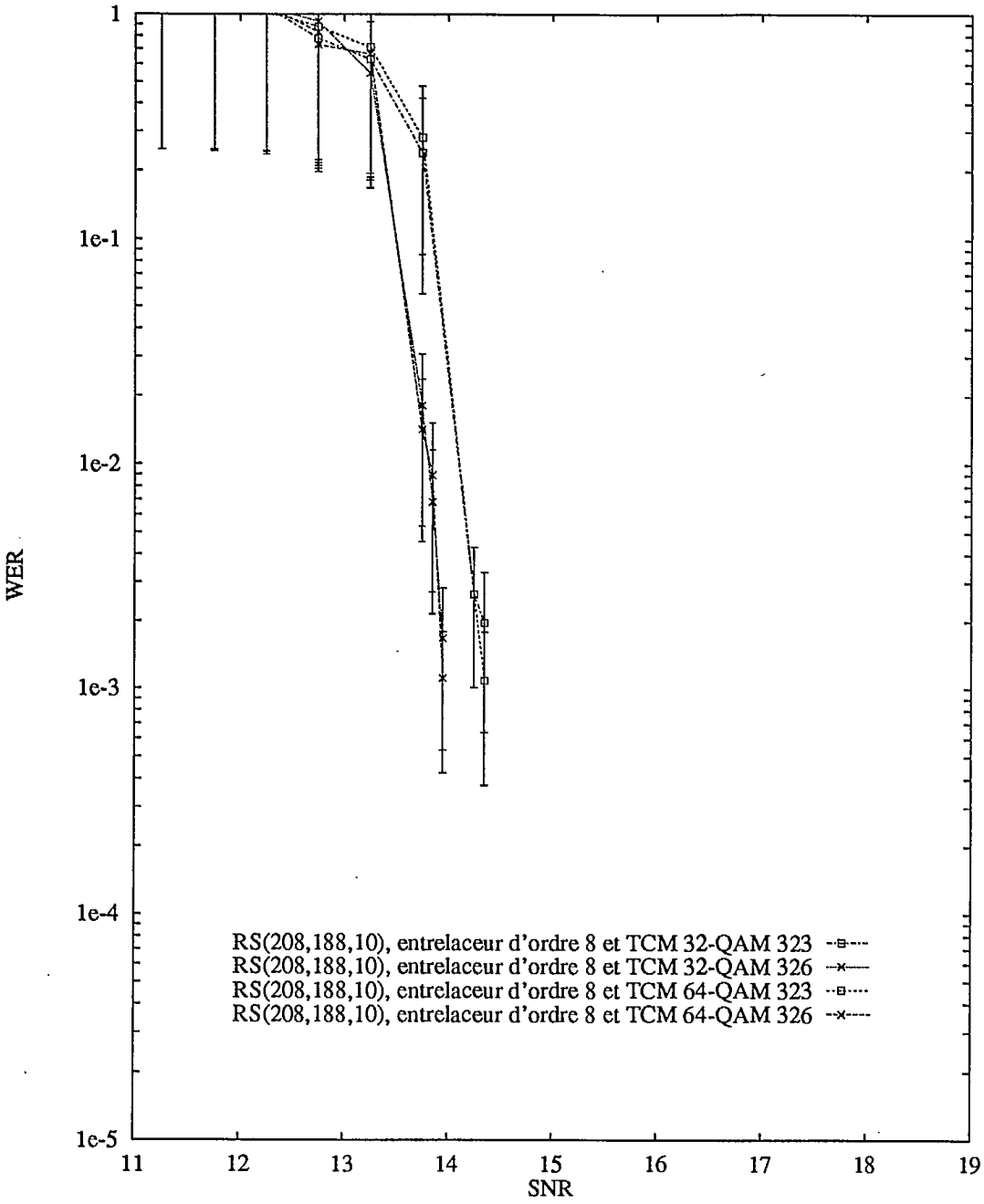

Figure 3.7: Probabilité de décodage erronné de mot-codes $\mathcal{P}_{mot-code}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour le code Reed-Solomon RS(208,188,10) avec les modulations TCM-32QAM et TCM-64QAM 2/3-2/3 (profondeur d'entrelacement: 8).

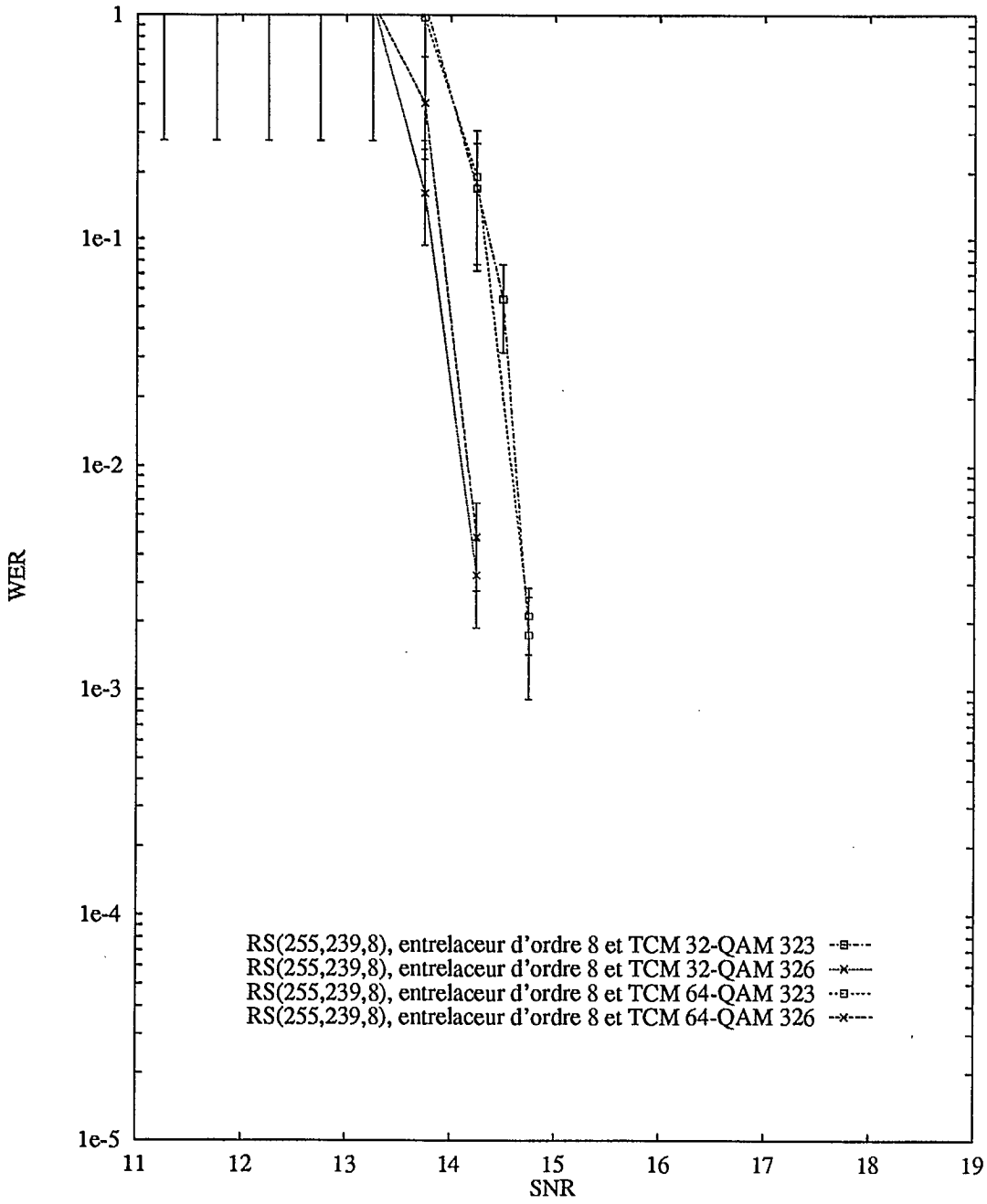

Figure 3.8: Probabilité de décodage erronné de mot-codes $\mathcal{P}_{mot-code}$ en fonction du rapport signal-à-bruit E_{sym}/N_0 pour le code Reed-Solomon RS(255,239,8) avec les modulations TCM-32QAM et TCM-64QAM 2/3-2/3 (profondeur d'entrelacement: 8).

3.4 Conclusion

Dans ce chapitre, on a présenté les codes correcteurs d'erreur Reed-Solomon qui seront utilisés comme codes externes afin de réduire davantage le taux d'erreur obtenu à la sortie du démodulateur TCM-QAM. Les paramètres des codes Reed-Solomon sont donnés dans ce chapitre (section 3.2.1) alors que les Corps de Galois requis pour former ces codes correcteurs d'erreurs se retrouvent à l'annexe A aux sections A.1 (page 65) pour le Corps de Galois $GF(16)$, A.2 (page 66) pour $GF(128)$ et A.3 (page 70) pour $GF(256)$. L'algorithme de décodage de Peterson-Gorenstein-Zierler est décrite à la section 3.2.2.

L'étude de la performance des codes de correction d'erreur Reed-Solomon concaténés avec la modulation codée TCM-QAM est présentée à la section 3.3 Les codes Reed-Solomon sont évalués en fonction de leur capacité de corriger les erreurs à la sortie du démodulateur TCM-QAM en présence de bruit additif blanc gaussien. On y indique entre autre que la performance est grandement améliorée par la concaténation des deux types de codes, à savoir Reed-Solomon et TCM-QAM. La performance des codes concaténés est affectée par le nombre d'états du codeur TCM ainsi que par la capacité de correction du code Reed-Solomon lui-même. Cependant, on ne remarque qu'une faible détérioration des performances lorsque l'on passe de la modulation codée bidimensionnelle TCM-32QAM à la modulation bi-unidimensionnelle TCM-64QAM 2/3-2/3.

Chapitre 4

Conclusion

4.1 Résumé du rapport

Dans ce rapport final, on a comparé les performances de la modulation TCM-32QAM à la modulation TCM-64QAM à taux 2/3-2/3. Une possibilité immédiate de la modulation TCM-64QAM 2/3-2/3 consiste à coder parallèlement les bits en phase et en quadrature avec des rapports égaux valant 2/3. Les bits codés en sortie sont concaténés entre eux pour former un symbole de 6 bits qu'une table de correspondance à 64 signaux permet de moduler de manière ordinaire. Cette étude est importante puisque c'est le choix de la modulation qui pèsera le plus en premier lieu dans le choix final des codes concaténés à y appliquer.

Les résultats théoriques garantissent l'utilisation efficace de bons codes TCM qui pourront être utilisés conjointement avec des codes Reed-Solomon. L'utilisation intermédiaire d'entrelaceur entre le codage RS et la modulation TCM, en parallèle avec un désentrelaceur en sortie du démodulateur TCM avant le décodage RS pourra encore améliorer les performances du système. Les résultats des simulations sont en accord avec les travaux plus larges de Heegard (voir [HLP93]). De nouveaux résultats concernant les performances en présence de signaux interférants dûs aux canaux voisins poussent à s'intéresser de très près à la question des interférences.

L'étude de la performance des codes de correction d'erreur Reed-Solomon concaténés avec la modulation codée TCM-QAM fait également l'objet du rapport final de la phase 1 du présent projet de recherche. Les codes Reed-Solomon sont évalués en fonction de leur capacité de corriger les erreurs subsistant à la sortie du démodulateur TCM-QAM en présence de bruit additif blanc gaussien. Les simulations réalisées sur ordinateur montrent bien l'importance d'entrelacer les symboles codés par l'encodeur Reed-Solomon avant de les soumettre au modulateur/codeur TCM-QAM.

4.2 Suggestions de travaux futurs

Dans cette section, on indique les travaux que l'on compte effectuer pour les phases 2 et 3 de ce projet.

1. Une des avenues les plus prometteuses en codage de canal est le décodage récursif (ou itératif) des symboles dans un système concaténé. Pour un système employant un code interne TCM-QAM, corrigeant les erreurs aléatoires du canal, et un code externe Reed-Solomon, qui lui corrige la plupart des groupements d'erreurs à la sortie du premier décodeur, il est possible d'exploiter la fiabilité des symboles détectés à la sortie de l'un des décodeurs pendant la détection de l'autre décodeur, et ce, de manière récursive, afin de réduire davantage le taux d'erreur des symboles d'information. Il a été démontré [Lee77] que cette stratégie de décodage permettait d'approcher la limite théorique de Shannon pour obtenir un taux d'erreur arbitrairement faible pour un rapport signal-à-bruit E_{bit}/N_0 et un taux de code concaténé $R_{concaténé}$ donnés. Il est possible de limiter la complexité des calculs en ne faisant de nouvelles *itérations* que si le mot-code décodé présente des erreurs[1]. Cette technique de décodage est d'autant plus intéressante pour la télévision avancée car l'information à protéger étant compressée typiquement dans un rapport de 1 à 60, chaque erreur de décodage affectera grandement la qualité de l'image une fois celle-ci décompressée. Un des aspects importants à considérer est la faisabilité d'implémentation de ces techniques de correction d'erreurs pour de la télévision avancée en fonction de la complexité requise des décodeurs et du gain additionnel de performance en terme de taux d'erreurs de transmission.

2. On veut étudier également la dégradation sur les signaux TVHD causée par un signal interférant NTSC (ou TVHD) lorsque l'on utilise la modulation codée TCM-QAM ainsi que les codes concaténés Reed-Solomon et TCM-QAM. On compte aussi étudier l'effet de la propagation multivoie ces signaux TVHD. Le signal TVHD couvrant une largeur de bande de fréquences de plusieurs MHz, on devra vraisemblablement considérer un modèle de canal à large bande, c'est-a-dire un modèle de canal avec affaiblissements sélectifs en fréquence.

3. Parmi les autres travaux de recherche envisagés, citons l'étude comparative de la performance de systèmes TVHD employant la technique de multiplexage par répartition orthogonale de fréquences OFDM (de l'anglais "Orthogonal Frequency Division Multiplexing") dont l'intérêt sur la modulation TCM-QAM est la facilité de gérer la

[1]Des simulations effectuées par Hagenauer, Offer et Papke [WB94] pour la sonde spatiale *Galileo* de la NASA démontrent que l'on peut réduire le taux d'erreur à environ 10^{-5} avec un rapport signal-à-bruit E_{bit}/N_0 de seulement 1.7 dB avec un code convolutionnel interne de taux $R_{concaténé} = \frac{1}{2}$, un entrelaceur de degré $I = 32$ et un code externe Reed-Solomon $RS(255, 223, 16)$ (code Reed-Solomon pouvant corriger jusqu'à 16 octets dans un mot-code de 255 octets).

présence de signaux interférants dûs aux canaux adjacents sans pour autant amoindrir de manière significative les performances du système en leur absence.

Bibliographie

[BDMS91] E. Biglieri, D. Divsalar, P.J. McLane, and M.K. Simon. *Introduction to Trellis-Coded Modulation with Applications.* Macmillan Publishing Company, New-York, 1991.

[BF91] K.B. Benson and D.G. Fink. *HDTV Avanced Television for the 1990s.* McGraw-Hill, New-York, 1991.

[Bla84] R.E. Blahut. *Theory and Practice of Error Control Codes.* Addison-Wesley, Reading, Mass., 1984.

[CDG92] G. Cohen, J.-L. Dornstetter, and P. Godlewski. *Codes correcteurs d'erreurs: une introduction au codage algébrique.* Masson, Paris, 1992. Collection Technique et Scientifique des Télécommunications *CNET-ENST.*

[Chi88] L. Chiariglione. *Signal Processing of HDTV.* North-Holland Publishing Company, Amsterdam, 1988. L. Chiariglione: éditeur.

[Eva95] B. Evans. *Understanding Digital Television: The Route to HDTV.* IEEE Press, Piscataway, 1995.

[For70] G.D. Forney. Convolutional Codes I: Algebraic Structure. *IEEE Transactions on Information Theory*, IT-16(6):720–738, novembre 1970.

[HLP93] C. Heegard, S.A. Lery, and W.H. Paik. Practical Coding for QAM Transmission of HDTV. *IEEE Journal on Selected Areas in Communications*, JSAC-11(1):111–118, janvier 1993.

[Ing93] A.F. Inglis. *Video Engineering.* McGraw-Hill, New-York, 1993.

[LC83] S. Lin and D. Costello. *Error Control Coding: Fundamentals and Applications.* Prentice-Hall, New-Jersey, 1983.

[Lee77] L.-N. Lee. Concatenated Coding Systems Employing a Unit-Memory Convolutional Code and a Byte-Oriented Decoding Algorithm. *IEEE Transactions on Communications*, COM-25(10):1064–1074, octobre 1977.

[Ple89] V. Pless. *Introduction to the Theory of Error-Correcting Codes.* Wiley-Interscience Series, New-York, 1989.

[RHG93] S.A. Raghavan, Y. Hebron, and I. Gurantz. On the Application of Appropraite APP Decoding to Digital Video Transmission. *IEEE Journal on Selected Areas in Communications*, JSAC-11(1):136–145, janvier 1993.

[Rze95] T.S. Rzeszewski. *Digital Video: Concepts and Applications Across Industries.* IEEE Press, Piscataway, 1995.

[Ung82] G. Ungerboeck. Channel Coding with Multilevel/Phase Signals. *IEEE Transactions on Information Theory*, IT-28(1):55–67, janvier 1982.

[Ung87a] G. Ungerboeck. Trellis-Coded Modulation with Redundant Signal Sets; Part I: Introduction. *IEEE Communications Magazine*, 25(2):5–11, février 1987.

[Ung87b] G. Ungerboeck. Trellis-Coded Modulation with Redundant Signal Sets; Part II: State of the Art. *IEEE Communications Magazine*, 25(2):12–21, février 1987.

[WB94] S.B. Wicker and V.K. Bhargava. *Reed-Solomon Codes and Their Applications*, chapter 11, pages 242–271. IEEE Press, Piscataway, 1994. Chapitre rédigé par J. Hagenauer, E. Offer et L. Papke et intitulé *Matching Viterbi Decoders and Reed-Solomon Decoders in a Concatenated System.*

[WC94] Y. Wu and B. Caron. Digital Television Terrestrial Broadcasting. *IEEE Communications Magazine*, 32(5):46–52, mai 1994.

[WLC94] Y. Wu, B. Ledoux, and B. Caron. Evaluation of Multi-Carrier Transmission Systems for Advanced Television in North America. In *NAB 1994 Broadcast Engineer Conference Proceedings*, mars 1994.

Annexe A

Description des Corps de Galois

Le Corps de Galois $GF(q) = GF(16)$ (voir annexe A.1 à la page 65) est en réalité une extension $GF(2^m) = GF(2^4)$ du Corps de Galois binaire $GF(2)$. De la même manière, les Corps de Galois $GF(q) = GF(128)$ et $GF(q) = GF(256)$, donnés aux annexes A.2 et A.3 respectivement (pages 66 et 70) sont des extensions $GF(2^m)$ (où $m = 7$ et 8) du Corps de Galois binaire $GF(2)$.

A.1 Corps de Galois $GF(q) = GF(16)$

Tableau A.1: Corps de Galois $GF(q) = GF(16)$

élément de $GF(16)$	polynôme	forme binaire	forme décimale
α^0	1	0 0 0 1	1
α^1	α	0 0 1 0	2
α^2	α^2	0 1 0 0	4
α^3	α^3	1 0 0 0	8
α^4	$\alpha + 1$	0 0 1 1	3
α^5	$\alpha^2 + \alpha$	0 1 1 0	6
α^6	$\alpha^3 + \alpha^2$	1 1 0 0	12
α^7	$\alpha^3 + \alpha + 1$	1 0 1 1	11
α^8	$\alpha^2 + 1$	0 1 0 1	5
α^9	$\alpha^3 + \alpha$	1 0 1 0	10
α^{10}	$\alpha^2 + \alpha + 1$	0 1 1 1	7
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1 1 1 0	14
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1 1 1 1	15
α^{13}	$\alpha^3 + \alpha^2 + 1$	1 1 0 1	13
α^{14}	$\alpha^3 + 1$	1 0 0 1	9

A.2 Corps de Galois $GF(q) = GF(128)$

Tableau A.2: Corps de Galois $GF(q) = GF(128)$ (partie 1)

élément de $GF(128)$	polynôme	forme binaire	forme décimale
α^0	1	0 0 0 0 0 0 1	1
α^1	α	0 0 0 0 0 1 0	2
α^2	α^2	0 0 0 0 1 0 0	4
α^3	α^3	0 0 0 1 0 0 0	8
α^4	α^4	0 0 1 0 0 0 0	16
α^5	α^5	0 1 0 0 0 0 0	32
α^6	α^6	1 0 0 0 0 0 0	64
α^7	$\alpha^3 + 1$	0 0 0 1 0 0 1	9
α^8	$\alpha^4 + \alpha$	0 0 1 0 0 1 0	18
α^9	$\alpha^5 + \alpha^2$	0 1 0 0 1 0 0	36
α^{10}	$\alpha^6 + \alpha^3$	1 0 0 1 0 0 0	72
α^{11}	$\alpha^4 + \alpha^3 + 1$	0 0 1 1 0 0 1	25
α^{12}	$\alpha^5 + \alpha^4 + \alpha$	0 1 1 0 0 1 0	50
α^{13}	$\alpha^6 + \alpha^5 + \alpha^2$	1 1 0 0 1 0 0	100
α^{14}	$\alpha^6 + 1$	1 0 0 0 0 0 1	65
α^{15}	$\alpha^3 + \alpha + 1$	0 0 0 1 0 1 1	11
α^{16}	$\alpha^4 + \alpha^2 + \alpha$	0 0 1 0 1 1 0	22
α^{17}	$\alpha^5 + \alpha^3 + \alpha^2$	0 1 0 1 1 0 0	44
α^{18}	$\alpha^6 + \alpha^4 + \alpha^3$	1 0 1 1 0 0 0	88
α^{19}	$\alpha^5 + \alpha^4 + \alpha^3 + 1$	0 1 1 1 0 0 1	57
α^{20}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha$	1 1 1 0 0 1 0	114
α^{21}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + 1$	1 1 0 1 1 0 1	109
α^{22}	$\alpha^6 + \alpha^4 + \alpha + 1$	1 0 1 0 0 1 1	83
α^{23}	$\alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$	0 1 0 1 1 1 1	47
α^{24}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	1 0 1 1 1 1 0	94
α^{25}	$\alpha^5 + \alpha^4 + \alpha^2 + 1$	0 1 1 0 1 0 1	53
α^{26}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha$	1 1 0 1 0 1 0	106
α^{27}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	1 0 1 1 1 0 1	93
α^{28}	$\alpha^5 + \alpha^4 + \alpha + 1$	0 1 1 0 0 1 1	51
α^{29}	$\alpha^6 + \alpha^5 + \alpha^2 + \alpha$	1 1 0 0 1 1 0	102
α^{30}	$\alpha^6 + \alpha^2 + 1$	1 0 0 0 1 0 1	69
α^{31}	$\alpha + 1$	0 0 0 0 0 1 1	3
α^{32}	$\alpha^2 + \alpha$	0 0 0 0 1 1 0	6

Tableau A.2: Corps de Galois $GF(q) = GF(128)$ (partie 2)

élément de $GF(128)$	polynôme	forme binaire	forme décimale
α^{33}	$+\alpha^3 +\alpha^2$	0 0 0 1 1 0 0	12
α^{34}	$+\alpha^4 +\alpha^3$	0 0 1 1 0 0 0	24
α^{35}	$\alpha^5 +\alpha^4$	0 1 1 0 0 0 0	48
α^{36}	$\alpha^6 +\alpha^5$	1 1 0 0 0 0 0	96
α^{37}	$\alpha^6 +\alpha^3 +1$	1 0 0 1 0 0 1	73
α^{38}	$\alpha^4 +\alpha^3 +\alpha +1$	0 0 1 1 0 1 1	27
α^{39}	$\alpha^5 +\alpha^4 +\alpha^2 +\alpha$	0 1 1 0 1 1 0	54
α^{40}	$\alpha^6 +\alpha^5 +\alpha^3 +\alpha^2$	1 1 0 1 1 0 0	108
α^{41}	$\alpha^6 +\alpha^4 +1$	1 0 1 0 0 0 1	81
α^{42}	$\alpha^5 +\alpha^3 +\alpha +1$	0 1 0 1 0 1 1	43
α^{43}	$\alpha^6 +\alpha^4 +\alpha^2 +\alpha$	1 0 1 0 1 1 0	86
α^{44}	$\alpha^5 +\alpha^2 +1$	0 1 0 0 1 0 1	37
α^{45}	$\alpha^6 +\alpha^3 +\alpha$	1 0 0 1 0 1 0	74
α^{46}	$\alpha^4 +\alpha^3 +\alpha^2 +1$	0 0 1 1 1 0 1	29
α^{47}	$\alpha^5 +\alpha^4 +\alpha^3 +\alpha$	0 1 1 1 0 1 0	58
α^{48}	$\alpha^6 +\alpha^5 +\alpha^4 +\alpha^2$	1 1 1 0 1 0 0	116
α^{49}	$\alpha^6 +\alpha^5 +1$	1 1 0 0 0 0 1	97
α^{50}	$\alpha^6 +\alpha^3 +\alpha +1$	1 0 0 1 0 1 1	75
α^{51}	$\alpha^4 +\alpha^3 +\alpha^2 +\alpha +1$	0 0 1 1 1 1 1	31
α^{52}	$\alpha^5 +\alpha^4 +\alpha^3 +\alpha^2 +\alpha$	0 1 1 1 1 1 0	62
α^{53}	$\alpha^6 +\alpha^5 +\alpha^4 +\alpha^3 +\alpha^2$	1 1 1 1 1 0 0	124
α^{54}	$\alpha^6 +\alpha^5 +\alpha^4 +1$	1 1 1 0 0 0 1	113
α^{55}	$\alpha^6 +\alpha^5 +\alpha^3 +\alpha +1$	1 1 0 1 0 1 1	107
α^{56}	$\alpha^6 +\alpha^4 +\alpha^3 +\alpha^2 +\alpha +1$	1 0 1 1 1 1 1	95
α^{57}	$\alpha^5 +\alpha^4 +\alpha^2 +\alpha +1$	0 1 1 0 1 1 1	55
α^{58}	$\alpha^6 +\alpha^5 +\alpha^3 +\alpha^2 +\alpha$	1 1 0 1 1 1 0	110
α^{59}	$\alpha^6 +\alpha^4 +\alpha^2 +1$	1 0 1 0 1 0 1	85
α^{60}	$\alpha^5 +\alpha +1$	0 1 0 0 0 1 1	35
α^{61}	$\alpha^6 +\alpha^2 +\alpha$	1 0 0 0 1 1 0	70
α^{62}	$\alpha^2 +1$	0 0 0 0 1 0 1	5
α^{63}	$\alpha^3 +\alpha$	0 0 0 1 0 1 0	10
α^{64}	$\alpha^4 +\alpha^2$	0 0 1 0 1 0 0	20
α^{65}	$\alpha^5 +\alpha^3$	0 1 0 1 0 0 0	40
α^{66}	$\alpha^6 +\alpha^4$	1 0 1 0 0 0 0	80
α^{67}	$\alpha^5 +\alpha^3 +1$	0 1 0 1 0 0 1	41
α^{68}	$\alpha^6 +\alpha^4 +\alpha$	1 0 1 0 0 1 0	82
α^{69}	$\alpha^5 +\alpha^3 +\alpha^2 +1$	0 1 0 1 1 0 1	45
α^{70}	$\alpha^6 +\alpha^4 +\alpha^3 +\alpha$	1 0 1 1 0 1 0	90

Tableau A.2: Corps de Galois $GF(q) = GF(128)$ (partie 3)

élément de $GF(128)$	polynôme	forme binaire	forme décimale
α^{71}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	0 1 1 1 1 0 1	61
α^{72}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha$	1 1 1 1 0 1 0	122
α^{73}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	1 1 1 1 1 0 1	125
α^{74}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha + 1$	1 1 1 0 0 1 1	115
α^{75}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$	1 1 0 1 1 1 1	111
α^{76}	$\alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1$	1 0 1 0 1 1 1	87
α^{77}	$\alpha^5 + \alpha^2 + \alpha + 1$	0 1 0 0 1 1 1	39
α^{78}	$\alpha^6 + \alpha^3 + \alpha^2 + \alpha$	1 0 0 1 1 1 0	78
α^{79}	$\alpha^4 + \alpha^2 + 1$	0 0 1 0 1 0 1	21
α^{80}	$\alpha^5 + \alpha^3 + \alpha$	0 1 0 1 0 1 0	42
α^{81}	$\alpha^6 + \alpha^4 + \alpha^2$	1 0 1 0 1 0 0	84
α^{82}	$\alpha^5 + 1$	0 1 0 0 0 0 1	33
α^{83}	$\alpha^6 + \alpha$	1 0 0 0 0 1 0	66
α^{84}	$\alpha^3 + \alpha^2 + 1$	0 0 0 1 1 0 1	13
α^{85}	$\alpha^4 + \alpha^3 + \alpha$	0 0 1 1 0 1 0	26
α^{86}	$\alpha^5 + \alpha^4 + \alpha^2$	0 1 1 0 1 0 0	52
α^{87}	$\alpha^6 + \alpha^5 + \alpha^3$	1 1 0 1 0 0 0	104
α^{88}	$\alpha^6 + \alpha^4 + \alpha^3 + 1$	1 0 1 1 0 0 1	89
α^{89}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$	0 1 1 1 0 1 1	59
α^{90}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha$	1 1 1 0 1 1 0	118
α^{91}	$\alpha^6 + \alpha^5 + \alpha^2 + 1$	1 1 0 0 1 0 1	101
α^{92}	$\alpha^6 + \alpha + 1$	1 0 0 0 0 1 1	67
α^{93}	$\alpha^3 + \alpha^2 + \alpha + 1$	0 0 0 1 1 1 1	15
α^{94}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha$	0 0 1 1 1 1 0	30
α^{95}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	0 1 1 1 1 0 0	60
α^{96}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3$	1 1 1 1 0 0 0	120
α^{97}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + 1$	1 1 1 1 0 0 1	121
α^{98}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$	1 1 1 1 0 1 1	123
α^{99}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	1 1 1 1 1 1 1	127
α^{100}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$	1 1 1 0 1 1 1	119
α^{101}	$\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$	1 1 0 0 1 1 1	103
α^{102}	$\alpha^6 + \alpha^2 + \alpha + 1$	1 0 0 0 1 1 1	71
α^{103}	$\alpha^2 + \alpha + 1$	0 0 0 0 1 1 1	7
α^{104}	$\alpha^3 + \alpha^2 + \alpha$	0 0 0 1 1 1 0	14
α^{105}	$\alpha^4 + \alpha^3 + \alpha^2$	0 0 1 1 1 0 0	28
α^{106}	$\alpha^5 + \alpha^4 + \alpha^3$	0 1 1 1 0 0 0	56
α^{107}	$\alpha^6 + \alpha^5 + \alpha^4$	1 1 1 0 0 0 0	112
α^{108}	$\alpha^6 + \alpha^5 + \alpha^3 + 1$	1 1 0 1 0 0 1	105

Tableau A.2: Corps de Galois $GF(q) = GF(128)$ (partie 4)

élément de $GF(128)$	polynôme	forme binaire	forme décimale
α^{109}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1$	1 0 1 1 0 1 1	91
α^{110}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	0 1 1 1 1 1 1	63
α^{111}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	1 1 1 1 1 1 0	126
α^{112}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1$	1 1 1 0 1 0 1	117
α^{113}	$\alpha^6 + \alpha^5 + \alpha + 1$	1 1 0 0 0 1 1	99
α^{114}	$\alpha^6 + \alpha^3 + \alpha^2 + \alpha + 1$	1 0 0 1 1 1 1	79
α^{115}	$\alpha^4 + \alpha^2 + \alpha + 1$	0 0 1 0 1 1 1	23
α^{116}	$\alpha^5 + \alpha^3 + \alpha^2 + \alpha$	0 1 0 1 1 1 0	46
α^{117}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2$	1 0 1 1 1 0 0	92
α^{118}	$\alpha^5 + \alpha^4 + 1$	0 1 1 0 0 0 1	49
α^{119}	$\alpha^6 + \alpha^5 + \alpha$	1 1 0 0 0 1 0	98
α^{120}	$\alpha^6 + \alpha^3 + \alpha^2 + 1$	1 0 0 1 1 0 1	77
α^{121}	$\alpha^4 + \alpha + 1$	0 0 1 0 0 1 1	19
α^{122}	$\alpha^5 + \alpha^2 + \alpha$	0 1 0 0 1 1 0	38
α^{123}	$\alpha^6 + \alpha^3 + \alpha^2$	1 0 0 1 1 0 0	76
α^{124}	$\alpha^4 + 1$	0 0 1 0 0 0 1	17
α^{125}	$\alpha^5 + \alpha$	0 1 0 0 0 1 0	34
α^{126}	$\alpha^6 + \alpha^2$	1 0 0 0 1 0 0	68

A.3 Corps de Galois $GF(q) = GF(256)$

Tableau A.3: Corps de Galois $GF(q) = GF(256)$ (partie 1)

élément de $GF(256)$	polynôme							forme binaire								forme décimale
α^0							1	0	0	0	0	0	0	0	1	1
α^1						α		0	0	0	0	0	0	1	0	2
α^2					α^2			0	0	0	0	0	1	0	0	4
α^3				α^3				0	0	0	0	1	0	0	0	8
α^4			α^4					0	0	0	1	0	0	0	0	16
α^5		α^5						0	0	1	0	0	0	0	0	32
α^6	α^6							0	1	0	0	0	0	0	0	64
α^7	α^7							1	0	0	0	0	0	0	0	128
α^8			α^4	$+\alpha^3$	$+\alpha^2$		$+1$	0	0	0	1	1	1	0	1	29
α^9		α^5	$+\alpha^4$	$+\alpha^3$		$+\alpha$		0	0	1	1	1	0	1	0	58
α^{10}	α^6	$+\alpha^5$	$+\alpha^4$		$+\alpha^2$			0	1	1	1	0	1	0	0	116
α^{11}	α^7	$+\alpha^6$	$+\alpha^5$		$+\alpha^3$			1	1	1	0	1	0	0	0	232
α^{12}	α^7	$+\alpha^6$			$+\alpha^3$	$+\alpha^2$	$+1$	1	1	0	0	1	1	0	1	205
α^{13}	α^7					$+\alpha^2$	$+\alpha$ $+1$	1	0	0	0	0	1	1	1	135
α^{14}			α^4			$+\alpha$	$+1$	0	0	0	1	0	0	1	1	19
α^{15}		α^5				$+\alpha^2$	$+\alpha$	0	0	1	0	0	1	1	0	38
α^{16}	α^6			$+\alpha^3$	$+\alpha^2$			0	1	0	0	1	1	0	0	76
α^{17}	α^7		$+\alpha^4$	$+\alpha^3$				1	0	0	1	1	0	0	0	152
α^{18}		α^5		$+\alpha^3$	$+\alpha^2$		$+1$	0	0	1	0	1	1	0	1	45
α^{19}	α^6		$+\alpha^4$	$+\alpha^3$		$+\alpha$		0	1	0	1	1	0	1	0	90
α^{20}	α^7	$+\alpha^5$	$+\alpha^4$		$+\alpha^2$			1	0	1	1	0	1	0	0	180
α^{21}	α^6	$+\alpha^5$	$+\alpha^4$		$+\alpha^2$		$+1$	0	1	1	1	0	1	0	1	117
α^{22}	α^7	$+\alpha^6$	$+\alpha^5$		$+\alpha^3$		$+\alpha$	1	1	1	0	1	0	1	0	234
α^{23}	α^7	$+\alpha^6$			$+\alpha^3$		$+1$	1	1	0	0	1	0	0	1	201
α^{24}	α^7				$+\alpha^3$	$+\alpha^2$	$+\alpha$ $+1$	1	0	0	0	1	1	1	1	143
α^{25}						α	$+1$	0	0	0	0	0	0	1	1	3
α^{26}					α^2	$+\alpha$		0	0	0	0	0	1	1	0	6
α^{27}				α^3	$+\alpha^2$			0	0	0	0	1	1	0	0	12
α^{28}			α^4	$+\alpha^3$				0	0	0	1	1	0	0	0	24
α^{29}		α^5	$+\alpha^4$					0	0	1	1	0	0	0	0	48
α^{30}	α^6	$+\alpha^5$						0	1	1	0	0	0	0	0	96
α^{31}	α^7	$+\alpha^6$						1	1	0	0	0	0	0	0	192
α^{32}	α^7		$+\alpha^4$	$+\alpha^3$	$+\alpha^2$		$+1$	1	0	0	1	1	1	0	1	157
α^{33}		α^5			$+\alpha^2$	$+\alpha$	$+1$	0	0	1	0	0	1	1	1	39
α^{34}	α^6			$+\alpha^3$	$+\alpha^2$	$+\alpha$		0	1	0	0	1	1	1	0	78
α^{35}	α^7		$+\alpha^4$	$+\alpha^3$	$+\alpha^2$			1	0	0	1	1	1	0	0	156
α^{36}		α^5			$+\alpha^2$		$+1$	0	0	1	0	0	1	0	1	37
α^{37}	α^6			$+\alpha^3$		$+\alpha$		0	1	0	0	1	0	1	0	74
α^{38}	α^7		$+\alpha^4$		$+\alpha^2$			1	0	0	1	0	1	0	0	148
α^{39}		α^5	$+\alpha^4$		$+\alpha^2$		$+1$	0	0	1	1	0	1	0	1	53
α^{40}	α^6	$+\alpha^5$		$+\alpha^3$		$+\alpha$		0	1	1	0	1	0	1	0	106
α^{41}	α^7	$+\alpha^6$		$+\alpha^4$		$+\alpha^2$		1	1	0	1	0	1	0	0	212
α^{42}	α^7		$+\alpha^5$	$+\alpha^4$		$+\alpha^2$	$+1$	1	0	1	1	0	1	0	1	181
α^{43}		α^6	$+\alpha^5$	$+\alpha^4$		$+\alpha^2$	$+\alpha$ $+1$	0	1	1	1	0	1	1	1	119
α^{44}	α^7	$+\alpha^6$	$+\alpha^5$		$+\alpha^3$	$+\alpha^2$	$+\alpha$	1	1	1	0	1	1	1	0	238

Tableau A.3: Corps de Galois $GF(q) = GF(256)$ (partie 2)

élément de $GF(256)$	polynôme								forme binaire								forme décimale
α^{45}	α^7	$+\alpha^6$						$+1$	1	1	0	0	0	0	0	1	193
α^{46}	α^7			$+\alpha^4$	$+\alpha^3$	$+\alpha^2$	$+\alpha$	$+1$	1	0	0	1	1	1	1	1	159
α^{47}			α^5				$+\alpha$	$+1$	0	0	1	0	0	0	1	1	35
α^{48}		α^6				$+\alpha^2$	$+\alpha$		0	1	0	0	0	1	1	0	70
α^{49}	α^7				$+\alpha^3$	$+\alpha^2$			1	0	0	0	1	1	0	0	140
α^{50}						α^2		$+1$	0	0	0	0	0	1	0	1	5
α^{51}					α^3		$+\alpha$		0	0	0	0	1	0	1	0	10
α^{52}				α^4		$+\alpha^2$			0	0	0	1	0	1	0	0	20
α^{53}			α^5		$+\alpha^3$				0	0	1	0	1	0	0	0	40
α^{54}		α^6		$+\alpha^4$					0	1	0	1	0	0	0	0	80
α^{55}	α^7		$+\alpha^5$						1	0	1	0	0	0	0	0	160
α^{56}		α^6		$+\alpha^4$	$+\alpha^3$	$+\alpha^2$		$+1$	0	1	0	1	1	1	0	1	93
α^{57}	α^7		$+\alpha^5$	$+\alpha^4$	$+\alpha^3$		$+\alpha$		1	0	1	1	1	0	1	0	186
α^{58}		α^6	$+\alpha^5$		$+\alpha^3$			$+1$	0	1	1	0	1	0	0	1	105
α^{59}	α^7	$+\alpha^6$		$+\alpha^4$			$+\alpha$		1	1	0	1	0	0	1	0	210
α^{60}	α^7		$+\alpha^5$	$+\alpha^4$	$+\alpha^3$			$+1$	1	0	1	1	1	0	0	1	185
α^{61}		α^6	$+\alpha^5$		$+\alpha^3$	$+\alpha^2$	$+\alpha$	$+1$	0	1	1	0	1	1	1	1	111
α^{62}	α^7	$+\alpha^6$		$+\alpha^4$	$+\alpha^3$	$+\alpha^2$	$+\alpha$		1	1	0	1	1	1	1	0	222
α^{63}	α^7		$+\alpha^5$					$+1$	1	0	1	0	0	0	0	1	161
α^{64}		α^6		$+\alpha^4$	$+\alpha^3$	$+\alpha^2$	$+\alpha$	$+1$	0	1	0	1	1	1	1	1	95
α^{65}	α^7		$+\alpha^5$	$+\alpha^4$	$+\alpha^3$	$+\alpha^2$	$+\alpha$		1	0	1	1	1	1	1	0	190
α^{66}		α^6	$+\alpha^5$					$+1$	0	1	1	0	0	0	0	1	97
α^{67}	α^7	$+\alpha^6$					$+\alpha$		1	1	0	0	0	0	1	0	194
α^{68}	α^7			$+\alpha^4$	$+\alpha^3$			$+1$	1	0	0	1	1	0	0	1	153
α^{69}			α^5		$+\alpha^3$	$+\alpha^2$	$+\alpha$	$+1$	0	0	1	0	1	1	1	1	47
α^{70}		α^6		$+\alpha^4$	$+\alpha^3$	$+\alpha^2$	$+\alpha$		0	1	0	1	1	1	1	0	94
α^{71}	α^7		$+\alpha^5$	$+\alpha^4$	$+\alpha^3$	$+\alpha^2$			1	0	1	1	1	1	0	0	188
α^{72}		α^6	$+\alpha^5$			$+\alpha^2$		$+1$	0	1	1	0	0	1	0	1	101
α^{73}	α^7	$+\alpha^6$			$+\alpha^3$		$+\alpha$		1	1	0	0	1	0	1	0	202
α^{74}	α^7				$+\alpha^3$			$+1$	1	0	0	0	1	0	0	1	137
α^{75}					α^3	$+\alpha^2$	$+\alpha$	$+1$	0	0	0	0	1	1	1	1	15
α^{76}				α^4	$+\alpha^3$	$+\alpha^2$	$+\alpha$		0	0	0	1	1	1	1	0	30
α^{77}			α^5	$+\alpha^4$	$+\alpha^3$	$+\alpha^2$			0	0	1	1	1	1	0	0	60
α^{78}		α^6	$+\alpha^5$	$+\alpha^4$	$+\alpha^3$				0	1	1	1	1	0	0	0	120
α^{79}	α^7	$+\alpha^6$	$+\alpha^5$	$+\alpha^4$					1	1	1	1	0	0	0	0	240
α^{80}	α^7	$+\alpha^6$	$+\alpha^5$	$+\alpha^4$	$+\alpha^3$	$+\alpha^2$		$+1$	1	1	1	1	1	1	0	1	253
α^{81}	α^7	$+\alpha^6$	$+\alpha^5$			$+\alpha^2$	$+\alpha$	$+1$	1	1	1	0	0	1	1	1	231
α^{82}	α^7	$+\alpha^6$		$+\alpha^4$			$+\alpha$	$+1$	1	1	0	1	0	0	1	1	211
α^{83}	α^7		$+\alpha^5$	$+\alpha^4$	$+\alpha^3$		$+\alpha$	$+1$	1	0	1	1	1	0	1	1	187
α^{84}		α^6	$+\alpha^5$		$+\alpha^3$		$+\alpha$	$+1$	0	1	1	0	1	0	1	1	107
α^{85}	α^7	$+\alpha^6$		$+\alpha^4$		$+\alpha^2$	$+\alpha$		1	1	0	1	0	1	1	0	214
α^{86}	α^7		$+\alpha^5$	$+\alpha^4$				$+1$	1	0	1	1	0	0	0	1	177
α^{87}		α^6	$+\alpha^5$	$+\alpha^4$	$+\alpha^3$	$+\alpha^2$	$+\alpha$	$+1$	0	1	1	1	1	1	1	1	127
α^{88}	α^7	$+\alpha^6$	$+\alpha^5$	$+\alpha^4$	$+\alpha^3$	$+\alpha^2$	$+\alpha$		1	1	1	1	1	1	1	0	254
α^{89}	α^7	$+\alpha^6$	$+\alpha^5$					$+1$	1	1	1	0	0	0	0	1	225
α^{90}	α^7	$+\alpha^6$		$+\alpha^4$	$+\alpha^3$	$+\alpha^2$	$+\alpha$	$+1$	1	1	0	1	1	1	1	1	223
α^{91}	α^7		$+\alpha^5$				$+\alpha$	$+1$	1	0	1	0	0	0	1	1	163
α^{92}		α^6		$+\alpha^4$	$+\alpha^3$		$+\alpha$	$+1$	0	1	0	1	1	0	1	1	91
α^{93}	α^7		$+\alpha^5$	$+\alpha^4$		$+\alpha^2$	$+\alpha$		1	0	1	1	0	1	1	0	182
α^{94}		α^6	$+\alpha^5$	$+\alpha^4$				$+1$	0	1	1	1	0	0	0	1	113

Tableau A.3: Corps de Galois $GF(q) = GF(256)$ (partie 3)

élément de $GF(256)$	polynôme	forme binaire	forme décimale
α^{95}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha$	1 1 1 0 0 0 1 0	226
α^{96}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + 1$	1 1 0 1 1 0 0 1	217
α^{97}	$\alpha^7 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$	1 0 1 0 1 1 1 1	175
α^{98}	$\alpha^6 + \alpha + 1$	0 1 0 0 0 0 1 1	67
α^{99}	$\alpha^7 + \alpha^2 + \alpha$	1 0 0 0 0 1 1 0	134
α^{100}	$\alpha^4 + 1$	0 0 0 1 0 0 0 1	17
α^{101}	$\alpha^5 + \alpha$	0 0 1 0 0 0 1 0	34
α^{102}	$\alpha^6 + \alpha^2$	0 1 0 0 0 1 0 0	68
α^{103}	$\alpha^7 + \alpha^3$	1 0 0 0 1 0 0 0	136
α^{104}	$\alpha^3 + \alpha^2 + 1$	0 0 0 0 1 1 0 1	13
α^{105}	$\alpha^4 + \alpha^3 + \alpha$	0 0 0 1 1 0 1 0	26
α^{106}	$\alpha^5 + \alpha^4 + \alpha^2$	0 0 1 1 0 1 0 0	52
α^{107}	$\alpha^6 + \alpha^5 + \alpha^3$	0 1 1 0 1 0 0 0	104
α^{108}	$\alpha^7 + \alpha^6 + \alpha^4$	1 1 0 1 0 0 0 0	208
α^{109}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	1 0 1 1 1 1 0 1	189
α^{110}	$\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$	0 1 1 0 0 1 1 1	103
α^{111}	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha^2 + \alpha$	1 1 0 0 1 1 1 0	206
α^{112}	$\alpha^7 + 1$	1 0 0 0 0 0 0 1	129
α^{113}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	0 0 0 1 1 1 1 1	31
α^{114}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	0 0 1 1 1 1 1 0	62
α^{115}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	0 1 1 1 1 1 0 0	124
α^{116}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3$	1 1 1 1 1 0 0 0	248
α^{117}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + 1$	1 1 1 0 1 1 0 1	237
α^{118}	$\alpha^7 + \alpha^6 + \alpha^2 + \alpha + 1$	1 1 0 0 0 1 1 1	199
α^{119}	$\alpha^7 + \alpha^4 + \alpha + 1$	1 0 0 1 0 0 1 1	147
α^{120}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$	0 0 1 1 1 0 1 1	59
α^{121}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha$	0 1 1 1 0 1 1 0	118
α^{122}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2$	1 1 1 0 1 1 0 0	236
α^{123}	$\alpha^7 + \alpha^6 + \alpha^2 + 1$	1 1 0 0 0 1 0 1	197
α^{124}	$\alpha^7 + \alpha^4 + \alpha^2 + \alpha + 1$	1 0 0 1 0 1 1 1	151
α^{125}	$\alpha^5 + \alpha^4 + \alpha + 1$	0 0 1 1 0 0 1 1	51
α^{126}	$\alpha^6 + \alpha^5 + \alpha^2 + \alpha$	0 1 1 0 0 1 1 0	102
α^{127}	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha^2$	1 1 0 0 1 1 0 0	204
α^{128}	$\alpha^7 + \alpha^2 + 1$	1 0 0 0 0 1 0 1	133
α^{129}	$\alpha^4 + \alpha^2 + \alpha + 1$	0 0 0 1 0 1 1 1	23
α^{130}	$\alpha^5 + \alpha^3 + \alpha^2 + \alpha$	0 0 1 0 1 1 1 0	46
α^{131}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2$	0 1 0 1 1 1 0 0	92
α^{132}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^3$	1 0 1 1 1 0 0 0	184
α^{133}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + 1$	0 1 1 0 1 1 0 1	109
α^{134}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha$	1 1 0 1 1 0 1 0	218
α^{135}	$\alpha^7 + \alpha^5 + \alpha^3 + 1$	1 0 1 0 1 0 0 1	169
α^{136}	$\alpha^6 + \alpha^3 + \alpha^2 + \alpha + 1$	0 1 0 0 1 1 1 1	79
α^{137}	$\alpha^7 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	1 0 0 1 1 1 1 0	158
α^{138}	$\alpha^5 + 1$	0 0 1 0 0 0 0 1	33
α^{139}	$\alpha^6 + \alpha$	0 1 0 0 0 0 1 0	66
α^{140}	$\alpha^7 + \alpha^2$	1 0 0 0 0 1 0 0	132
α^{141}	$\alpha^4 + \alpha^2 + 1$	0 0 0 1 0 1 0 1	21
α^{142}	$\alpha^5 + \alpha^3 + \alpha$	0 0 1 0 1 0 1 0	42
α^{143}	$\alpha^6 + \alpha^4 + \alpha^2$	0 1 0 1 0 1 0 0	84
α^{144}	$\alpha^7 + \alpha^5 + \alpha^3$	1 0 1 0 1 0 0 0	168

Tableau A.3: Corps de Galois $GF(q) = GF(256)$ (partie 4)

élément de $GF(256)$	polynôme	forme binaire	forme décimale
α^{145}	$\alpha^6 + \alpha^3 + \alpha^2 + 1$	0 1 0 0 1 1 0 1	77
α^{146}	$\alpha^7 + \alpha^4 + \alpha^3 + \alpha$	1 0 0 1 1 0 1 0	154
α^{147}	$\alpha^5 + \alpha^3 + 1$	0 0 1 0 1 0 0 1	41
α^{148}	$\alpha^6 + \alpha^4 + \alpha$	0 1 0 1 0 0 1 0	82
α^{149}	$\alpha^7 + \alpha^5 + \alpha^2$	1 0 1 0 0 1 0 0	164
α^{150}	$\alpha^6 + \alpha^4 + \alpha^2 + 1$	0 1 0 1 0 1 0 1	85
α^{151}	$\alpha^7 + \alpha^5 + \alpha^3 + \alpha$	1 0 1 0 1 0 1 0	170
α^{152}	$\alpha^6 + \alpha^3 + 1$	0 1 0 0 1 0 0 1	73
α^{153}	$\alpha^7 + \alpha^4 + \alpha$	1 0 0 1 0 0 1 0	146
α^{154}	$\alpha^5 + \alpha^4 + \alpha^3 + 1$	0 0 1 1 1 0 0 1	57
α^{155}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha$	0 1 1 1 0 0 1 0	114
α^{156}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^2$	1 1 1 0 0 1 0 0	228
α^{157}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + 1$	1 1 0 1 0 1 0 1	213
α^{158}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$	1 0 1 1 0 1 1 1	183
α^{159}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha + 1$	0 1 1 1 0 0 1 1	115
α^{160}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^2 + \alpha$	1 1 1 0 0 1 1 0	230
α^{161}	$\alpha^7 + \alpha^6 + \alpha^4 + 1$	1 1 0 1 0 0 0 1	209
α^{162}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	1 0 1 1 1 1 1 1	191
α^{163}	$\alpha^6 + \alpha^5 + \alpha + 1$	0 1 1 0 0 0 1 1	99
α^{164}	$\alpha^7 + \alpha^6 + \alpha^2 + \alpha$	1 1 0 0 0 1 1 0	198
α^{165}	$\alpha^7 + \alpha^4 + 1$	1 0 0 1 0 0 0 1	145
α^{166}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	0 0 1 1 1 1 1 1	63
α^{167}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	0 1 1 1 1 1 1 0	126
α^{168}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	1 1 1 1 1 1 0 0	252
α^{169}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^2 + 1$	1 1 1 0 0 1 0 1	229
α^{170}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1$	1 1 0 1 0 1 1 1	215
α^{171}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha + 1$	1 0 1 1 0 0 1 1	179
α^{172}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$	0 1 1 1 1 0 1 1	123
α^{173}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha$	1 1 1 1 0 1 1 0	246
α^{174}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + 1$	1 1 1 1 0 0 0 1	241
α^{175}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	1 1 1 1 1 1 1 1	255
α^{176}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha + 1$	1 1 1 0 0 0 1 1	227
α^{177}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1$	1 1 0 1 1 0 1 1	219
α^{178}	$\alpha^7 + \alpha^5 + \alpha^3 + \alpha + 1$	1 0 1 0 1 0 1 1	171
α^{179}	$\alpha^6 + \alpha^3 + \alpha + 1$	0 1 0 0 1 0 1 1	75
α^{180}	$\alpha^7 + \alpha^4 + \alpha^2 + \alpha$	1 0 0 1 0 1 1 0	150
α^{181}	$\alpha^5 + \alpha^4 + 1$	0 0 1 1 0 0 0 1	49
α^{182}	$\alpha^6 + \alpha^5 + \alpha$	0 1 1 0 0 0 1 0	98
α^{183}	$\alpha^7 + \alpha^6 + \alpha^2$	1 1 0 0 0 1 0 0	196
α^{184}	$\alpha^7 + \alpha^4 + \alpha^2 + 1$	1 0 0 1 0 1 0 1	149
α^{185}	$\alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$	0 0 1 1 0 1 1 1	55
α^{186}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha$	0 1 1 0 1 1 1 0	110
α^{187}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2$	1 1 0 1 1 1 0 0	220
α^{188}	$\alpha^7 + \alpha^5 + \alpha^2 + 1$	1 0 1 0 0 1 0 1	165
α^{189}	$\alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1$	0 1 0 1 0 1 1 1	87
α^{190}	$\alpha^7 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha$	1 0 1 0 1 1 1 0	174
α^{191}	$\alpha^6 + 1$	0 1 0 0 0 0 0 1	65
α^{192}	$\alpha^7 + \alpha$	1 0 0 0 0 0 1 0	130
α^{193}	$\alpha^4 + \alpha^3 + 1$	0 0 0 1 1 0 0 1	25
α^{194}	$\alpha^5 + \alpha^4 + \alpha$	0 0 1 1 0 0 1 0	50

Tableau A.3: Corps de Galois $GF(q) = GF(256)$ (partie 5)

élément de $GF(256)$	polynôme	forme binaire	forme décimale
α^{195}	$\alpha^6 + \alpha^5 + \alpha^2$	0 1 1 0 0 1 0 0	100
α^{196}	$\alpha^7 + \alpha^6 + \alpha^3$	1 1 0 0 1 0 0 0	200
α^{197}	$\alpha^7 + \alpha^3 + \alpha^2 + 1$	1 0 0 0 1 1 0 1	141
α^{198}	$\alpha^2 + \alpha + 1$	0 0 0 0 0 1 1 1	7
α^{199}	$\alpha^3 + \alpha^2 + \alpha$	0 0 0 0 1 1 1 0	14
α^{200}	$\alpha^4 + \alpha^3 + \alpha^2$	0 0 0 1 1 1 0 0	28
α^{201}	$\alpha^5 + \alpha^4 + \alpha^3$	0 0 1 1 1 0 0 0	56
α^{202}	$\alpha^6 + \alpha^5 + \alpha^4$	0 1 1 1 0 0 0 0	112
α^{203}	$\alpha^7 + \alpha^6 + \alpha^5$	1 1 1 0 0 0 0 0	224
α^{204}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	1 1 0 1 1 1 0 1	221
α^{205}	$\alpha^7 + \alpha^5 + \alpha^2 + \alpha + 1$	1 0 1 0 0 1 1 1	167
α^{206}	$\alpha^6 + \alpha^4 + \alpha + 1$	0 1 0 1 0 0 1 1	83
α^{207}	$\alpha^7 + \alpha^5 + \alpha^2 + \alpha$	1 0 1 0 0 1 1 0	166
α^{208}	$\alpha^6 + \alpha^4 + 1$	0 1 0 1 0 0 0 1	81
α^{209}	$\alpha^7 + \alpha^5 + \alpha$	1 0 1 0 0 0 1 0	162
α^{210}	$\alpha^6 + \alpha^4 + \alpha^3 + 1$	0 1 0 1 1 0 0 1	89
α^{211}	$\alpha^7 + \alpha^5 + \alpha^4 + \alpha$	1 0 1 1 0 0 1 0	178
α^{212}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + 1$	0 1 1 1 1 0 0 1	121
α^{213}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha$	1 1 1 1 0 0 1 0	242
α^{214}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + 1$	1 1 1 1 1 0 0 1	249
α^{215}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$	1 1 1 0 1 1 1 1	239
α^{216}	$\alpha^7 + \alpha^6 + \alpha + 1$	1 1 0 0 0 0 1 1	195
α^{217}	$\alpha^7 + \alpha^4 + \alpha^3 + \alpha + 1$	1 0 0 1 1 0 1 1	155
α^{218}	$\alpha^5 + \alpha^3 + \alpha + 1$	0 0 1 0 1 0 1 1	43
α^{219}	$\alpha^6 + \alpha^4 + \alpha^2 + \alpha$	0 1 0 1 0 1 1 0	86
α^{220}	$\alpha^7 + \alpha^5 + \alpha^3 + \alpha^2$	1 0 1 0 1 1 0 0	172
α^{221}	$\alpha^6 + \alpha^2 + 1$	0 1 0 0 0 1 0 1	69
α^{222}	$\alpha^7 + \alpha^3 + \alpha$	1 0 0 0 1 0 1 0	138
α^{223}	$\alpha^3 + 1$	0 0 0 0 1 0 0 1	9
α^{224}	$\alpha^4 + \alpha$	0 0 0 1 0 0 1 0	18
α^{225}	$\alpha^5 + \alpha^2$	0 0 1 0 0 1 0 0	36
α^{226}	$\alpha^6 + \alpha^3$	0 1 0 0 1 0 0 0	72
α^{227}	$\alpha^7 + \alpha^4$	1 0 0 1 0 0 0 0	144
α^{228}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	0 0 1 1 1 1 0 1	61
α^{229}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha$	0 1 1 1 1 0 1 0	122
α^{230}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2$	1 1 1 1 0 1 0 0	244
α^{231}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1$	1 1 1 1 0 1 0 1	245
α^{232}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$	1 1 1 1 0 1 1 1	247
α^{233}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha + 1$	1 1 1 1 0 0 1 1	243
α^{234}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$	1 1 1 1 1 0 1 1	251
α^{235}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha + 1$	1 1 1 0 1 0 1 1	235
α^{236}	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha + 1$	1 1 0 0 1 0 1 1	203
α^{237}	$\alpha^7 + \alpha^3 + \alpha + 1$	1 0 0 0 1 0 1 1	139
α^{238}	$\alpha^3 + \alpha + 1$	0 0 0 0 1 0 1 1	11
α^{239}	$\alpha^4 + \alpha^2 + \alpha$	0 0 0 1 0 1 1 0	22
α^{240}	$\alpha^5 + \alpha^3 + \alpha^2$	0 0 1 0 1 1 0 0	44
α^{241}	$\alpha^6 + \alpha^4 + \alpha^3$	0 1 0 1 1 0 0 0	88
α^{242}	$\alpha^7 + \alpha^5 + \alpha^4$	1 0 1 1 0 0 0 0	176
α^{243}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	0 1 1 1 1 1 0 1	125
α^{244}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha$	1 1 1 1 1 0 1 0	250

Tableau A.3: Corps de Galois $GF(q) = GF(256)$ (partie 6)

élément de $GF(256)$	polynôme	forme binaire	forme décimale
α^{245}	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + 1$	1 1 1 0 1 0 0 1	233
α^{246}	$\alpha^7 + \alpha^6 + \alpha^3 + \alpha^2 + \alpha + 1$	1 1 0 0 1 1 1 1	207
α^{247}	$\alpha^7 + \alpha + 1$	1 0 0 0 0 0 1 1	131
α^{248}	$\alpha^4 + \alpha^3 + \alpha + 1$	0 0 0 1 1 0 1 1	27
α^{249}	$\alpha^5 + \alpha^4 + \alpha^2 + \alpha$	0 0 1 1 0 1 1 0	54
α^{250}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2$	0 1 1 0 1 1 0 0	108
α^{251}	$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3$	1 1 0 1 1 0 0 0	216
α^{252}	$\alpha^7 + \alpha^5 + \alpha^3 + \alpha^2 + 1$	1 0 1 0 1 1 0 1	173
α^{253}	$\alpha^6 + \alpha^2 + \alpha + 1$	0 1 0 0 0 1 1 1	71
α^{254}	$\alpha^7 + \alpha^3 + \alpha^2 + \alpha$	1 0 0 0 1 1 1 0	142

Annexe B

Liste des programmes

- Programme *essai.c*
- Programme *essai2.c*
- Programme *essai3.c*
- Programme *TCM32_SNR_simul.c*
- Programme *TCM32_SNI_simul.c*
- Programme *TCM64_SNR_simul.c*
- Programme *TCM32_RS_SNR_simul.c*
- Programme *TCM32_RS_intrlv_SNR_simul.c*
- Programme *TCM64_RS_intrlv_SNR_simul.c*
- Programmes *TCM.c* et *TCM.h*
- Programmes *TCM2.c* et *TCM2.h*
- Programmes *TCM3.c* et *TCM3.h*
- Programmes *de_TCM.c* et *de_TCM.h*
- Programmes *de_TCM2.c* et *de_TCM2.h*
- Programmes *de_TCM3.c* et *de_TCM3.h*
- Programmes *RS_cdr.c* et *RS_cdr.h*

- Programmes *RS_dec.c* et *RS_dec.h*
- Programmes *intrlv.c* et *intrlv.h*
- Programmes *deintrlv.c* et *deintrlv.h*
- Programmes *integr.c* et *integr.h*
- Programmes *noise.c* et *noise.h*
- Programme *params.h*
- Programme *paths.h*
- Programmes *proba.c* et *proba.h*
- Programmes *reading.c* et *reading.h*
- Programmes *source.c* et *source.h*
- Programmes *theoric.c* et *theoric.h*
- Programmes *rapport.c* et *rapport.h*

DATE DUE
DATE DE RETOUR

CARR McLEAN 38-296