Multi-user communication systems : from interference management to network coding

Asma Mejri

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2013-ENST-0086

EDITE - ED 130

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

Télécom-ParisTech

Spécialité « Communications et Électronique »

présentée et soutenue publiquement par

Asma MEJRI

le 13 Décembre 2013

Systèmes de Communications Multi-utilisateurs : de la Gestion d'interférence au Codage de Réseaux

Directeur de thèse : **Ghaya REKAYA-BEN OTHMAN**

M. Cong LING, Maître de Conférences, Imperial College	Rapporteur
M. Ramesh PYNDIAH, Professeur, Télécom Bretagne	Rapporteur
M. Jean-Claude BELFIORE, Professeur, Télécom-ParisTech	Examinateur
M. Hichem BESBES, Professeur, SUP'COM	Examinateur
M. Sheng YANG, Maître de Conférences, Supélec	Examinateur
Mme. Ghaya REKAYA-BEN OTHMAN, Professeur, Télécom-ParisTech	Directeur de thèse

T H È S E

Télécom-ParisTech
Grande école de l'Institut Mines-Télécom - membre fondateur de ParisTech
46 rue Barrault 75013 Paris - (+33) 1 45 81 77 77 - www.telecom-paristech.fr

♣ ♣ ♣

To my father ***Tahar*** *and my mother* ***Arbia***

To my soul and lovely twin sister ***Emna***

To my brother ***Wajdi*** *and my sister* ***Ameni***

To my grandfather ***Abd-El-Aziz*** *and my nephew* ***Youssef***

♣ ♣ ♣

Acknowledgments

If I have seen further it is by standing on the shoulders of Giants.

-Isaac Newton.

I would like to take advantage of this opportunity to thank all those who supported me during this experience.

First, I would like to thank my Ph.D advisor, Professor Ghaya Rekaya for giving me the opportunity to do a Ph.D under her supervision.

I am very grateful to the jury members for their interest in my work. I thank Professor Jean-Claude Belfiore for acting as the chairman and Professor Ramesh Pyndiah and Dr. Cong ling for accepting to review and evaluate my thesis. I was honored that Professor Hichem Besbes participated in the jury as examiner. In addition, I thank Dr. Sheng Yang for his valuable comments.

This thesis is the result of three years of work spent at Télécom-ParisTech. I address my gratitude first to all the members of the ComElec department especially our team leader Professor Philippe Ciblat, our head of the department Professor Bruno Thedrez, Michèle Wigger, Olivier Rioul and the administrative staff, Zouina, Chantal, Yvonne and Nazha for their assistance. Many thanks go to Florence Bernard for her support and help. I thank also my collegues at Télécom-ParisTech who contributed to a good atmosphere. Special thanks to Selma, Fanny, Mohamed, Arwa, Julia, Youlong, Milad, Hamed, Mariem, Karim, Rupesh, Wiem, Nassar, Ehsen, Sarah and all those I forgot to mention.

Special thanks to my office mate Elie for his endless support, appreciable help and technical and non-technical discussions. Thank you Elie for being a source of re-motivation, optimism and positive energy. Without you my Ph.D journey would not be the same. I mention also a good friend I met during this experience, David. Thank you for all the moments and discussions we shared and for your endless support in particular during the last months of my work.

A thought goes also to my friends outside TélécomParisTech, Yosra, Ahlem, and Zakia and to my friend Houssem who passed away in 2012.

Last but not least, I want to express my deep gratitude to my parents, brother, sisters, Rim, Sonia and Kalthoum for their love and support. I owe them the success of my studies, and this thesis is also theirs.

Abstract

Wireless communication systems are taking an ever growing place in our daily life. Driven by the developments of digital technologies and the emergence of new multimedia applications, different communication networks are available today. The most popular examples are the cellular and wireless sensor networks.

Practical wireless communication systems are inherently multiuser networks where several transmitters and receivers share the available wireless resources to exchange their data. An important issue in such multiuser networks is the multiple access interference resulting from the superposition and broadcast properties of the wireless medium. This interference is commonly treated as nuisance. However, a new technique termed *Physical-Layer Network Coding* (PLNC) revealed the advantages of interference in enabling more efficient and reliable transmissions. Using PLNC, intermediate nodes in a wireless multihop relay network including multiple access channels treat interference as useful information to decode and forward functions of the original source signals. This new management technique is shown to essentially provide higher transmission rates among other significant benefits.

Motivated by the promising potential of Physical-Layer Network Coding, we are interested in this work in the analysis, design and performance evaluation of PLNC-based communication strategies in practical multiuser network configurations. Studied strategies include a very promising linear PLNC protocol termed the *Compute-and-Forward* (CF), as well as the *Analog Network Coding* (ANC). Three network topologies are investigated: the *Two-Way Relay Channel* (TWRC), the *Multi-Source Multi-Relay* (MSMR) *Channel* and the *distributed Multiple-Input Multiple-Output* (MIMO) *Channel.*

The first part of this work is devoted to study the Compute-and-Forward protocol in the basic multiple access channel. For this strategy, we propose an optimal solution to design efficient network codes based on solving a lattice shortest vector problem. Moreover, we derive novel bounds on the ergodic rate and the outage probability for the CF operating in fast and slow fading channels respectively. Besides, we develop novel decoding algorithms proved, numerically, to outperform the traditional decoding scheme for the CF.

The second part of this work is dedicated to the design and end-to-end performance evaluation of network codes for the CF and the ANC in the TWRC and the MSMR channel. For each network model we study the decoding at the relay nodes and the end destination, propose search algorithms for optimal network codes for the CF based on a modified Fincke-Pohst algorithm, and evaluate, theoretically and numerically, the end-to-end error rate and achievable transmission rate.

The third and last part of this work is devoted to the distributed MIMO channel. For this network model, we are concerned with the design of MIMO decoders. In particular, we study a new architecture of linear decoders termed *Integer Forcing* (IF) linear receivers. Inspired by the CF protocol, the IF receivers take advantage of the interference provided by the wireless medium to decode integer linear combinations of the original codewords from which the source messages are easily recovered through a matrix inversion. Motivated by the promising theoretical gains of the IF architecture, we move in this work a step further towards its practical implementation by developing efficient algorithms to select optimal IF receivers parameters, and providing a numerical analysis of their error rate performance.

Contents

List of Figures

List of Tables

List of abbreviations

The abbreviations used in this work are summarized in the following.

LTE	Long Term Evolution
SHM	Structural Health Monitoring
P2P	Peer-to-Peer
QPSK	Quadrature Phase-Shift Keying
PLNC	Physical-Layer Networ Coding
CF	Compute-and-Forward
ANC	Analog Network Coding
DoF	Denoise-and-Forward
AF	Amplify-and-Forward
DF	Decode-and-Forward
TWRC	Two-Way Relay Channel
MSMR	Multi-Source Multi-Relay
MIMO	Multiple Input Multiple Output
MARC	Multiple Access Relay Channel
MAC	Multiple Access Channel
AWGN	Additive White Gaussian Noise
MAP	Maximum A Posteriori
ML	Maximum Likelilhood
ZF	Zero Forcing
MMSE	Minimum Mean Square Error
MMSE-GDFE	Minimum Mean Square Error-Generalized Decision Feedback Equalizer
IF	Integer Forcing
DMT	Diversity Multiplexing Tradeoff

LLL	Lenstra Lenstra Lovàsz
HNF	Hermite Normal Form
IDA	Inhomogeneous Diophantine Approximation
CSI	Channel State Information
SNR	Signal-to-Noise Ratio
i.i.d	independent and identically distributed
bits/c.u	bits per channel use

List of notations

We consider in this work the following notations. Vectors and matrices are written in boldface, in lowercase and uppercase respectively.

$\mathbf{0}_n$	Zero vector of dimension n
$\mathbf{M}^{n \times m}$	Matrix of n rows and m columns
$\mathbf{I}_n$	Identity matrix of dimension n
$\mathbb{F}_p$	Finite Field of prime size p
$\mathbb{R}$	The real field
$\mathbb{Z}$	The integer field
$\mathbb{C}$	The complex field
$\mathbb{R}^n$	The real field of dimension n
$(:)^t$	Regular transpose operation
$(:)^*$	Hermitian transpose operation
$\mathrm{Re}(:)$	Real part of a complex number
$\mathrm{Im}(:)$	Imaginary part of a complex number
$\|\mathbf{x}\|$	Eucliean norm of a vector $\mathbf{x}$
$\mathbb{E}$	Mathematical expectation
log	The logarithm operation to the base 2
ln	The natural logarithm
$\lfloor \mathbf{x} \rfloor$	Largest integer not greater than $\mathbf{x}$
$\lceil \mathbf{x} \rceil$	Smallest integer not less than $\mathbf{x}$

$\oplus$	Addition over the finite field F_p
$\ominus$	Substraction over the finite field F_p
$\bigoplus$	Summation over the finite field F_p

Resume Detaille de la These

Cette thèse est dédiée à l'analyse, la construction et l'étude des performances de schémas de codage de réseaux au niveau physique (PLNC) appropriés à trois principales configurations de systèmes de communications multi-terminaux: le canal à relais bidirectionnel (Two-Way Relay Channel, TWRC), le canal à sources et relais multiples (Multi-Source Multi-Relay, MSMR) et le canal MIMO distribué. La motivation derrière le choix de ces configurations est leur application potentielle dans les systèmes de communications réels. En effet, le canal TWRC peut par exemple modéliser les communications satellitaires. Le canal MSMR modélise parfaitement la communication dans un réseau de capteurs sans fil et le canal MIMO distribué est approprié au réseau cellulaire en présence de station de base à antennes multiples.

Le premier réseau étudié, le TWRC présenté en Figure.1, est constitué de deux nœuds N_1 et N_2 communiquant à l'aide du relais R. Tous les nœuds de ce réseau sont équipés d'une seule antenne. Pour cette configuration, nous proposons de nouveaux algorithmes de construction de schémas de codages de réseaux pour le protocole Compute-and-Forward, et nous analysons les performances, en termes de taux d'erreurs et de débit de transmission, au niveau des nœuds N_1 et N_2, du CF, et des stratégies Analog Network Coding (ANC) et Denoise-and-Forward (DoF).

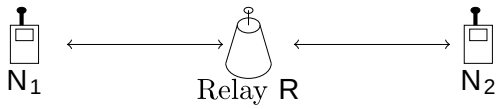


Figure 1: Le canal à relais bidirectionnel.

La deuxième configuration étudiée dans cette thèse est le canal MSMR présenté en Figure.2 et constitué de N sources indépendantes, N relais et une destination commune D. Tous les nœuds de ce réseau sont équipés d'une seule antenne. Pour ce scénario, nous proposons des algorithmes de construction de schémas de codage PLNC pour le CF et le ANC respectivement. Une analyse numérique des performances des algorithmes proposés est aussi fournie.

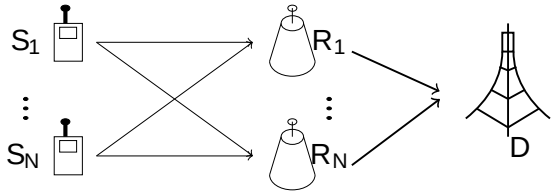


Figure 2: Le canal à sources et relais multiples.

Finallement, nous nous intéressons au canal MIMO distribué (présenté en Figure.3) composé de N sources indépendantes équipées chacune d'elles d'une seule antenne, et d'une destination commune D équipée de $\mathsf{M} \geq \mathsf{N}$ antennes. Pour cette dernière configuration, nous étudions une nouvelle classe de décodeurs MIMO nommés *Integer Forcing linear receivers* (IF). Nous établissons de nouveaux algorithmes de décodeurs IF prouvés théoriquement et par simulations numériques, plus performants que les décodeurs MIMO linéaires existants.

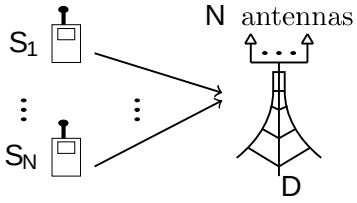


Figure 3: Le canal MIMO distribué.

Pour ces trois réseaux de communications, nous supposons que les nœuds sont parfaitement synchronisés et fonctionnent en mode half-duplex. Dans le cas du TWRC, les nœuds N_1 et N_2 ne sont pas en vue directe. La destination sait toujours si les relais implémentent du PLNC ou non. En plus, nous supposons une connaissance parfaite du canal seulement en réception, c'est à dire au niveau des nœuds relais ou à la destination finale. Finalement, les métriques d'évaluation de performances considérées dans cette thèse sont le taux d'erreurs par message et le débit de transmission moyen à la destination finale.

Le premier chapitre de cette thèse détaillée est une introduction au codage de réseaux (Network Coding) en multicast dans les réseaux de communications à sources et destinations multiples. Nous introduisons aussi dans ce chapitre le codage de réseaux à la couche physique et présentons les principaux travaux existants en littérature.

Le deuxième chapitre est dédié à l'étude du protocole CF dans le canal à accès multiples (MAC). Nous commençons par la présentation du protocole ainsi que les principaux résultats théoriques existants. Ensuite, nous présentons nos principales contributions de ce chapitre. D'abord, nous proposons un critère de construction de codes PLNC en se basant sur la maximisation du débit du calcul pour le CF. En utilisant des tech-

niques de réseaux de points, nous montrons que la solution optimale de ce problème de maximisation correspond à la solution d'un problème du vecteur le plus court dans un réseau de points donné (shortest vector problem). Ensuite, nous proposons deux nouvelles bornes du débit du calcul ergodique et de la probabilité de coupure pour le protocol CF dans le canal à évanouissement ergodique et quasi-statique respectivement. Nous clôturons ce chapitre avec le développement de nouveaux algorithmes de décodage efficaces pour le CF. Commençant par le canal MAC à Bruit Blanc Additif Gaussien (BBAG), nous établissons dans un premier lieu une nouvelle métrique de décodage à *maximum à postériori* (MAP), qui est le décodeur optimal dans ce cas. En utilisant cette nouvelle métrique, nous montrons que le problème de décodage MAP est équivalent à un problème de recherche de point le plus proche (closest vector problem) dans un réseau de points que nous résolvons en moyens du décodeur par sphères. Nos résultats de simulations montrent le gain de notre algorithme par rapport au décodeur classique du protocole CF. Pour le canal MAC à évanouissements, nous étudions le décodeur optimal à *maximum de vraissemblance* (ML). En analysant la métrique de décodage ML, nous développons un nouvel algorithme se basant sur l'approximation diophantienne de nombres réels par des entiers. Nos résultats de simulations montrent dans ce cas aussi que notre algorithme apporte un gain par rapport au décodeur existant du CF.

Dans le troisième chapitre, nous nous focalisons sur l'implémentation du protocole CF dans le canal à relais bidirectionnel. Nos principales contributions de ce chapitre concernent le développement de nouveaux algorithmes de construction de codes de réseaux pour le CF dans le canal à évanouissement se basant sur la méthode d'énumération Fincke-Pohst [9]. Nos résultats de simulations montrent l'efficacité de nos algorithmes et mettent en évidence la gain du protocole CF par rapport au protocoles ANC et DoF.

Dans le quatrième chapitre nous traitons le canal MSMR. Nous proposons une nouvelle formulation du problème de recherche de codes de réseaux optimaux pour le CF. En utilisant une modification de l'algorithme Fincke-Pohst, nous développons des méthodes pratiques de construction de ces codes optimaux. L'évaluation numérique de notre approche montre son efficacité et le gain en performances du protocole CF par rapport au protocole ANC.

Le dernier chapitre est dédié au canal MIMO distribué. Nous présentons dans un premier lieu les méthodes de décodage classiques, à savoir le décodeur optimal ML, les décodeurs sous-optimaux linéaires (ZF et MMSE) et les décodeurs linéaires précédés de prétraitement en utilisant une réduction de la matrice canal. Nous étudions en second lieu la nouvelle architecture de décodeurs IF. Nos principaux résultats à cet égard concernent le développement de nouveaux algorithmes de construction des paramètres optimaux de ces récepteurs permettant la maximisation du débit de transmission, ainsi que l'analyse numérique de leurs performances utilisant des schémas de codes imbriqués (nested lattice codes) de dimension finie et à faibles complexités de codage et décodage.

Chapitre 1: Introduction au Codage de Réseaux

Les techniques de routage actuellement utilisées dans les réseaux de communications sont basées sur la même stratégie: les flux de données envoyés par les nœuds sources, sont dupliqués au niveau des nœuds relais intermédiaires qui envoient par la suite une copie des données originales au nœud suivant dans la chaîne de transmission. En utilisant cette approche de relayage, le seul traitement autorisé aux relais est la duplication des flux entrants en maintenant les données indépendantes provenant de sources différentes du réseau séparées. Cette technique, bien qu'elle soit optimale dans le cas de réseaux point-à-point, elle ne l'est pas en présence de plusieurs paires d'émetteur-récepteur. Pour surmonter cette sous-optimalité, le codage de réseaux a été récemment proposé en littérature. L'idée consiste à autoriser les nœuds relais à combiner les flux de données indépendants et de transférer ces combinaisons linéaires à travers le réseau. Après la réception de plusieurs combinaisons émises par les relais, et sous certaines conditions, la destination finale peut récupérer les flux indépendants de données originales.

Dans ce contexte, nous décrivons le problème de multicast dans le réseau papillon, et nous présentons les principaux avantages du codage de réseaux comme l'augmentation des débits, l'optimisation des ressources dans les réseaux de communications sans fils et la sécurité des données. Nous exposons aussi quelques exemples des premières applications du codage de réseaux comme les réseaux de capteurs sans fils et le stockage distribué. En outre, le théorème de base du codage de réseaux est introduit. Ce théorème, prouvé par trois groupes de recherche dans [35–37], stipule l'existence d'un schéma de codage linéaire permettant, dans tout type de réseau, de communiquer les données d'informations sources aux destinations appropriées en atteignant la borne supérieure de l'information mutuelle pour chacune des paires source-destination. Une formulation algébrique équivalente à ce théorème est de même exposée.

Le codage de réseaux ainsi présenté se fait au niveau de la couche réseau: il s'agit de calculer des combinaisons des bits d'informations indépendants déjà décodés. Le codage de réseaux au niveau physique (PLNC) se base sur le même principe avec deux principales différences: le PLNC traite des combinaisons de signaux à la couche physique et sans décodage de ces derniers séparément. Nous expliquons cette différence à travers l'exemple du canal à relais bidirectionnel. La technique de PLNC a été développée en 2006 par deux principaux groupes de recherches: Zhang, Liew et Lam dans [4] et Popovski et Yomo dans [5, 6]. Dans [4] les auteurs montrent qu'en utilisant un simple schéma de modulation/démodulation, le PLNC permet, dans le canal à relais bidirectionnel, de doubler les débits de transmission atteignables en moyens des techniques de routage usuelles. Les premières stratégies de PLNC ont été par la suite proposées dans [4]. Inspirées par les techniques de relayage *Amplify-and-Forward* et *Decode-and-Forward*, les auteurs mettent en oeuvre respectivement les stratégies *Analog Network Coding* et *Denoise-and-Forward* toujours en considérant le canal à relais bidirectionnel. Ces premiers travaux ont suscité une intense activité de recherche tant sur le plan

théorique que pratique pour étendre ce nouveau concept dans divers contextes, en combinaison avec le codage source et le codage canal [7] et dans diverses configurations de réseaux multi-terminaux comme le canal à relais à accès multiples (Multiple Access Relay Channel) dans [47, 48], le canal à sources et relais multiples dans [8] et le canal MIMO [11, 63, 66, 72, 75]. Dans ce travail nous sommes intéressés par une nouvelle stratégie de PLNC récemment introduite en litérature, le *Compute-and-Forward*. Ce protocole se base sur la combinaison de codage canal et codage de réseaux au niveau physique utilisant les codes en réseaux de points imbriqués (nested lattice codes). Le concept fondamental du CF consiste à décoder, au niveau des nœuds relais, recevant la superposition des signaux provenant de différentes sources, une combinaison linéaire entière (à coefficients entiers) des mots de codes transmis par les sources. La structure linéaire des codes imbriquées garantit que la combinaison linéaire soit aussi un mot de code appartenant au même réseau de points utilisé par les sources. Depuis l'introduction de ce nouveau protocole par Nazer et Gastpar, diverses contributions ont été proposées traitant différents aspects relatifs au CF. Entre autres, les limites théoriques en terme de débits et de degrés de liberté ont été respectivement analysés dans [8, 56] et [58] et des algorithmes de décodage pour le CF ont été proposés récemment dans [59–61]. Le point commun à toutes les contributions citées ce-dessus est l'analyse du protocole CF d'un point de vue théorique. Nous proposons dans ce travail une implémentation pratique de cette stratégie dans des configurations de réseaux de communications multi-terminaux. La première partie de notre étude, faisant l'objet du chapitre suivant, est dédiée au développement d'algorithmes de décodage efficaces pour le CF considérant le canal à accès multiple.

Chapitre 2: Le protocole Compute-and-Forward

Le modèle canal

Nous étudions dans ce chapitre le protocole CF dans le canal à accès multiples de base composé de N sources indépendantes et un récepteur commun comme le montre la Figure.4.

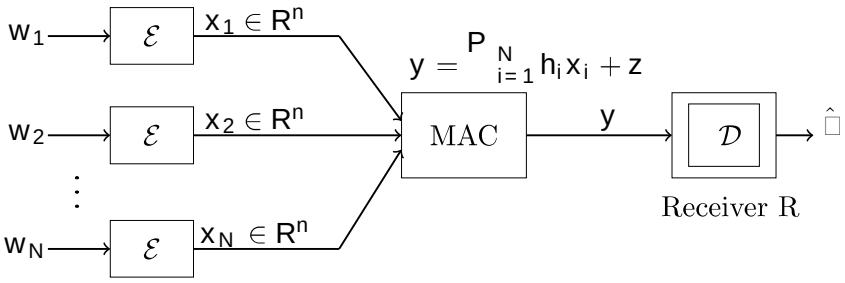


Figure 4: Canal à accès multiples réel.

Soit $\Lambda = \{\Lambda_F \cap \mathcal{V}_C\}$ le réseau de points (lattice) imbriqué généré à partir du réseau

de codage (Fine lattice) Λ_F et du réseau de mise en forme (Coarse lattice) Λ_C de région de Voronoi $\mathcal{V}_C$.

Le schéma de codage pour le CF est basé sur l'utilisation de codes imbriqués au niveau des sources. Dans ce contexte, chacune des sources génère un message $w_i \in F_p^k$ de dimension k du corps fini F_p de dimension p, p premier. Les messages sont ensuite codés pour construire les mots de code $x_i \in \Lambda$ appartenant au même réseau de points Λ. Les sources transmettent après leurs signaux au récepteur en respectant la contrainte de puissance définie par:

$$\frac{1}{n}E\left[\| x_i \|^2\right] \leq P \tag{1}$$

Où $P > 0$. Supposant une synchronisation parfaite entre les sources, le signal observé au niveau du récepteur est une superposition bruitée des mots de codes originaux qui peut s'écrire, pour un modèle de canal réel, sous la forme suivante:

$$y = \sum_{i=1}^{N} h_i x_i + z \tag{2}$$

où $h_i \in R$ représente le coefficient d'évanouissement entre la source S_i et le récepteur et $z \in R^n$ est un Bruit Blanc Additif Gaussien de moyenne nulle et variance σ^2. Soit $h = [h_1; :::; h_N]^t$ le vecteur composé des coefficients d'évanouissements correspondants à toutes les sources. Nous supposons une connaissance parfaite du canal au récepteur, c'est à dire le vecteur h est connu seulement à la réception. Soit $\rho = \frac{P}{\sigma^2}$ le rapport signal à bruit (Signal-to-Noise Ratio, SNR).

Schéma de décodage pour le Compute-and-Forward

Utilisant le protocole CF, l'objectif du récepteur est de décoder une combinaison linéaire entière v des mots de codes originaux sous la forme:

$$v = \left[\sum_{i=1}^{N} a_i x_i \mod \Lambda_C\right] \tag{3}$$

Où les coefficients $a_i \in Z; i = 1; :::; N$ sont choisis par le récepteur et forment le vecteur du code de réseau $a = [a_1; :::; a_N]^t \in Z^N$. En pratique, le récepteur est équipé d'un décodeur $\mathcal{D} : R^n \to \Lambda$ qui génère une estimation $\hat{v}$. Une erreur de décodage est déclarée lorsque $\hat{v} \neq v$. Pour avoir l'estimation de la combinaison désirée, le récepteur sélectionne un coefficient $\alpha \in R$ et un vecteur entier a et implémente les étapes suivantes:

1. Multiplication du signal reçu par α:

$$\tilde{y} = \alpha y = \sum_{i=1}^{N} \alpha h_i x_i + \alpha z = \underbrace{\sum_{i=1}^{N} a_i x_i}_{t} + \underbrace{\sum_{i=1}^{N} (\alpha h_i - a_i) x_i + \alpha z}_{\text{Bruit Effectif}} \tag{4}$$

   L'intérêt de cette étape consiste à réduire l'erreur d'approximation du signal reçu par la combinaison t à coefficients entiers.

2. Quantification au point le plus proche en termes de distance minimale dans le réseau de point Λ_F pour avoir $\hat{t} = Q_{\Lambda_F}(\tilde{y})$. Nous implémentons dans notre étude le décodeur par sphères pour résoudre ce problème.

3. Ramener le vecteur décodé au coarse lattice Λ_C en moyens de l'opération mod pour obtenir $\hat{\ } = \hat{t} \mod \Lambda_C$

Débit de calcul pour le Compute-and-Forward

La contribution fondamentale apporté avec le protocole CF consiste à offrir des débits de transmission plus élevés que ceux que nous pouvons atteindre avec les techniques de relayage et les stratégies de PLNC existantes. Nazer et Gastpar montrent dans [8] qu'en utilisant les réseaux de points imbriqués aux sources, le récepteur est capable de décoder une combinaison linéaire entière à condition que les débits des messages sources soient inférieurs à un débit de calcul (computation rate) R_{comp} donné par:

$$R_{comp} = \log^+ \left(\frac{}{^2 + \| h - a \|^2} \right) \tag{5}$$

avec $\in \mathbb{R}$ et $\log^+(x) = \max(\log(x); 0)$

Sélection des paramètres et a

Les deux paramètres fondamentaux du schéma du décodage du protocole CF sont le facteur de multiplication et le vecteur du code de réseaux a. Comme l'objectif de ce protocole est d'augmenter les débits de transmission, le choix optimal de ces paramètres se base sur la maximisation du débit du calcul et se ramène à résoudre le problème d'optimisation suivant [8]:

$$(; a)_{opt} = \underset{(\in \mathbb{R}^?; a \in \mathbb{Z}^N \setminus 0)}{\operatorname{argmax}} \log^+ \left(\frac{}{^2 + \| h - a \|^2} \right) \tag{6}$$

Selon ce problème de maximisation, la valeur optimale du facteur de multiplication a été trouvée par Nazer et Gastpar et est donné, pour un vecteur a fixé par [8]:

$$_{opt} = \frac{h^t a}{1 + \| h \|^2} \tag{7}$$

Le vecteur du code de réseaux optimal est donné par conséquent par le problème d'optimisation suivant:

$$a_{opt} = \underset{a \in \mathbb{Z}^N \setminus 0}{\operatorname{argmin}} \left(a^t G a \right) \tag{8}$$

où

$$G = I_N - \frac{}{1 + \| h \|^2} H \tag{9}$$

$H = [H_{ij}]; H_{ij} = h_i h_j; 1 \leq i; j \leq N$ et G est une matrice symmétrique définie positive de dimension N. Nous montrons que la résolution de ce problème de minimisation

est équivalent à chercher le vecteur le plus court dans le réseau de points Λ_G donné par la matrice de Gram G. Nous proposons deux approches pour l'implémentation en pratique de ce problème: une méthode optimale qui consiste à utiliser l'algorithme de Fincke-Pohst, et une deuxième sous-optimale se basant sur la réduction de réseaux de points (lattice reduction). Utilisant la réduction LLL, nous développons une borne inférieure du débit du calcul ergodique et une borne supérieure à la capacité de coupure pour le canal à évanouissement quasi-statique.

Décodeurs efficaces pour le CF: cas du canal Gaussien

En étudiant les étapes de décodage pour le protocole CF original, nous avons constaté des sous-optimalités dans l'étape de quantification. Dans cette partie nous étudions le cas particulier du canal MAC Gaussien où les coefficients $h_i = 1; \forall i = 1; :::; N$. Le signal reçu dans ce cas s'écrit sous la forme:

$$y = \sum_{i=1}^{N} x_i + z \tag{10}$$

Le récepteur désire dans ce cas décoder la combinaison donnée par

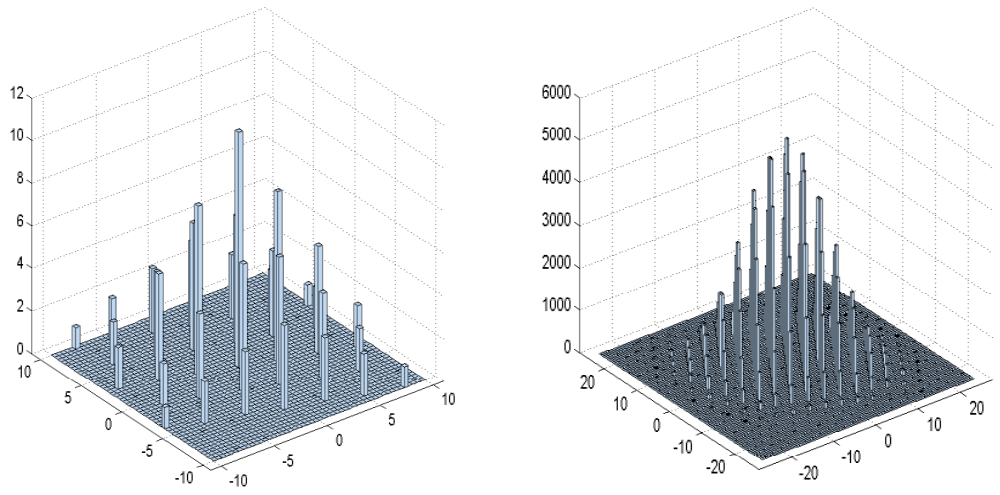
$$\square = \left[\sum_{i=1}^{N} x_i \right] \bmod \Lambda_C \tag{11}$$

Nous nous intéressons en premier lieu au décodage de la somme non bruitée des mots de code originaux $\square_s = \sum_{i=1}^{N} x_i$. Etant donné que l'opération mod n'a pas d'impact sur les erreurs de décodage, nous évaluons la probabilité d'erreurs en comptabilisant les erreurs de décodage de $\square_s$. La probabilité d'erreurs est donnée alors par:

$$P_e = \Pr\left[\hat{\square}_s \neq \square_s \right] \tag{12}$$

Soit Λ_s *l'alphabet somme* composé de toutes les sommes $\square_s = \sum_{i=1}^{N} x_i$. Grâce à la structure linéaire du réseau de codage Λ_F, Λ_s est un sous-ensemble fini de ce dernier défini par la région de mise en forme (shaping region) $\mathcal{S}_s$ traduisant la constrainte de puissance pour les mots de codes sommes $\square_s$.

En utilisant l'algorithme de décodage traditionnel du CF, l'étape de quantification au réseau de codage Λ_F permettant d'avoir une estimation de la somme $\square_s$ se base sur la minimisation de la distance euclidienne. Dans ce cadre, nous avons soulevé deux sous-optimalités fondamentales: le décodeur considère que les mots de codes sommes sont équiprobables alors que l'alphabet somme, étant obtenu par une superposition des mots de codes originaux, n'est pas uniforme comme illustré à travers la Figure.5. En plus, la recherche du point le proche est effectuée en négligeant la contrainte de puissance de l'alphabet somme. Nous étudions dans ce chapitre le décodeur *maximum à posteriori* (MAP) optimal tenant en compte ces deux sous-optimalités.



(a) Histogramme pour N= 2. (b) Histogramme pour N= 5.

Figure 5: Histogramme de l'alphabet somme.

Métrique de Décodage MAP

Nous commençons par la métrique de décodage MAP donnée par:

$$\begin{aligned}\hat{\square}_{\mathsf{map}} &= \underset{\square_s 2\,\square_s}{\operatorname{argmax}}\, \mathsf{p}(\square_s|\mathsf{y}) = \underset{\square_s 2\,\square_s}{\operatorname{argmax}}\, \mathsf{p}(\square_s)\mathsf{p}(\mathsf{y}|\square_s) \\ &= \underset{\square_s 2\,\square_s}{\operatorname{argmax}}\; \mathsf{p}(\square_s)\frac{1}{(\square\sqrt{2\square})^{\mathsf{n}}}\exp\left(-\frac{\|\,\mathsf{y}-\square_s\,\|^2}{2\square^2}\right) \\ &= \underset{\square_s 2\,\square_s}{\operatorname{argmin}}\; -\ln\left(\mathsf{p}(\square_s)\right)+\frac{\|\,\mathsf{y}-\square_s\,\|^2}{2\square^2}\end{aligned} \tag{13}$$

En utilisant cette métrique, nous développons une nouvelle expression pour la borne de l'union de la probabilité d'erreurs donnée par ce qui suit:

$$\mathrm{P_e} \le \frac{1}{2}\sum_{\square_s 2\,\square_s}\;\sum_{\hat{\square}_s 2\,\square_s n\square_s} \mathsf{p}(\square_s)\mathrm{erfc}\left(\sqrt{\mathsf{A}}+\frac{\mathsf{B}}{\sqrt{\mathsf{A}}}\right) \tag{14}$$

où $\mathsf{A}=\frac{\mathsf{d}^2_{\mathsf{min}}}{8\square^2}$, $\mathsf{B}=\frac{1}{4}\ln\left(\frac{\mathsf{p}(\square_s)}{\mathsf{p}(\hat{\square}_s)}\right)$ et $\mathsf{d}_{\mathsf{min}}$ représente la distance minimale du réseau de codage Λ_{F}.

Algorithme de décodage MAP pratique

Nous développons un algorithme de décodage MAP facile à implémenter en moyens d'une version modifiée du décodeur par sphères. Pour aboutir à cette fin, nous procédons par

deux étapes: d'abord nous caractérisons la distribution statistique des mots de codes sommes, ensuite nous développons la métrique MAP définie en (13). Nous modélisons les mots de codes sommes par des variables Gaussiennes discrètes de variance σ_s^2 et montrons que la métrique de décodage MAP est équivalente à:

$$\hat{s}_{map} = \underset{s \in \mathcal{A}_s^n}{\operatorname{argmin}} \left(\| y - s \|^2 + \sigma^2 \| s \|^2 \right) \tag{15}$$

où $\sigma = \frac{\sigma}{\sigma_s}$. En utilisant cette nouvelle métrique, nous montrons que le problème de décodage MAP revient à résoudre un problème du point le plus proche dans un nouveau réseau de points augmenté Λ_{aug} de matrice génératrice $M_{aug} = [M \ \sigma M]^t \in \mathbb{R}^{2n \times n}$ suivant notre nouvelle métrique donnée par:

$$\hat{s}_{map} = \underset{\substack{x_{aug} \in \Lambda_{aug} = \\ x_{aug} = M_{aug} s}}{\operatorname{argmin}} \| y_{aug} - x_{aug} \|^2 \tag{16}$$

où $y_{aug} = [y \ 0_n]^t$. Nous montrons de même que le décodage MAP est équivalent à effectuer un pré-traitement MMSE-GDFE suivi d'un décodage à minimisation de la distance euclidienne suivant notre métrique suivante:

$$\hat{s}_{map} = \underset{s \in \mathcal{A}_s^n}{\operatorname{argmin}} \| Fy - Bs \|^2 \tag{17}$$

où $F \in \mathbb{R}^{n \times n}$ et $B \in \mathbb{R}^{n \times n}$ présentent les matrices du prétraitement MMSE-GDFE correspondant au système $y = s + z$ tel que $B^t B = \left(1 + \sigma^2\right) I_n$ et $F^t B = I_n$.

Résultats de simulations

Nous évaluons la probabilité d'erreurs du décodeur existant du protocole CF basé sur la minimisation de la distance euclidienne et la comparons à celle de notre nouveau décodeur MAP que nous implémentons utilisant l'algorithme de décodage par sphères. Nous incluons le décodage MAP par recherche exhaustive à titre comparatif. Nous considérons trois configurations différentes de schémas de codage, de dimensions n du réseau Λ et de nombre de sources N. La Figure.6 correspond au cas où $n = 2$ et $N = 2$. La contrainte de puissance dans ce cas est égale à $P = 21$. Nos résultats de simulations montrent que notre algorithme MAP a les mêmes performances que la recherche exhaustive ce qui valide, même pour un nombre faible de sources N, la distribution Gaussienne discrète des mots de codes sommes sur laquelle se base notre algorithme MAP. Nous soulignons aussi que le gain du décodeur MAP par rapport au décodeur standard du protocole CF est limité à 0.5dB pour une probabilité d'erreurs de 10^{-1}. Les résultats de simulations tracés dans la Figure.7 correspondant au cas $N = 5$ confirment aussi la validité de notre modélisation Gaussienne. La dernière configuration que nous considérons correspond au cas du réseau entier de dimension $n = 4$ et de matrice génératrice la matrice identité I_4. Nos résultats de simulations tracés dans la Figure.8 pour $N = 2$ montrent d'une part que notre algorithme atteint les mêmes performances que la recherche MAP exhaustive,

et d'autre part mettent en évidence le gain de notre approche par rapport au décodeur standard évalué à 1dB pour une probabilité d'erreurs de 10^{-3}. Ces résultats confirment l'importance d'utiliser le décodeur MAP pour cette configuration ayant des gains non négligeables par rapport à l'approche existante.

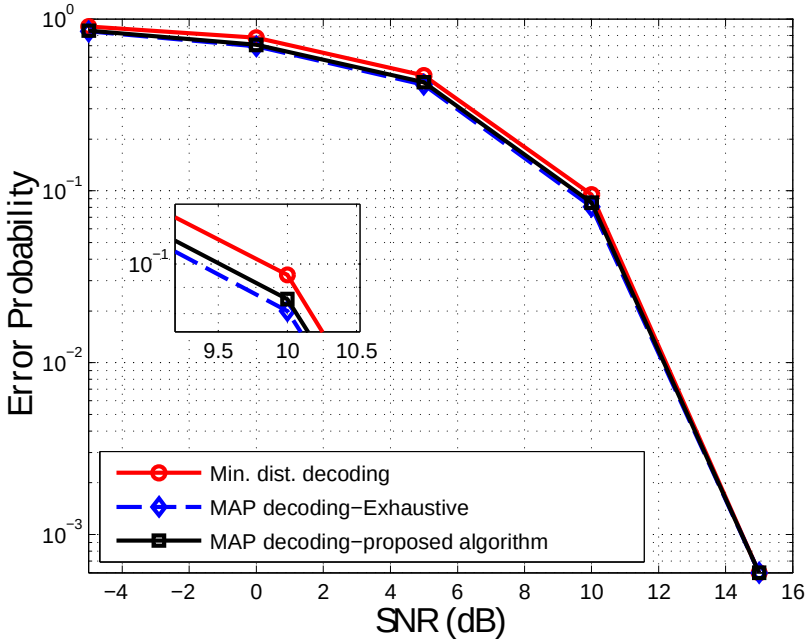


Figure 6: Probabilité d'erreurs pour $\mathsf{n} = 2; \mathsf{N} = 2; \mathsf{P} = 21$.

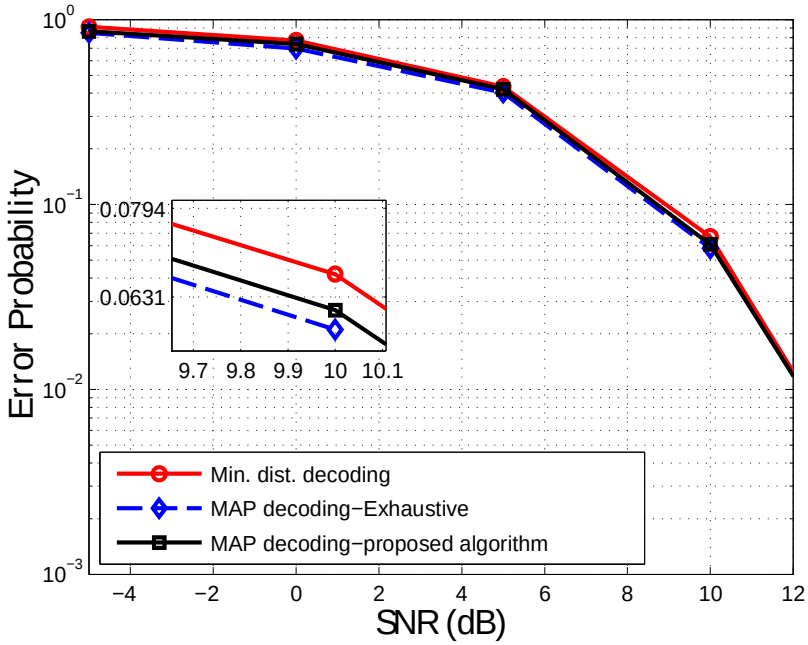


Figure 7: Probabilité d'erreurs pour $\mathsf{n} = 2; \mathsf{N} = 5; \mathsf{P} = 6{:}5$.

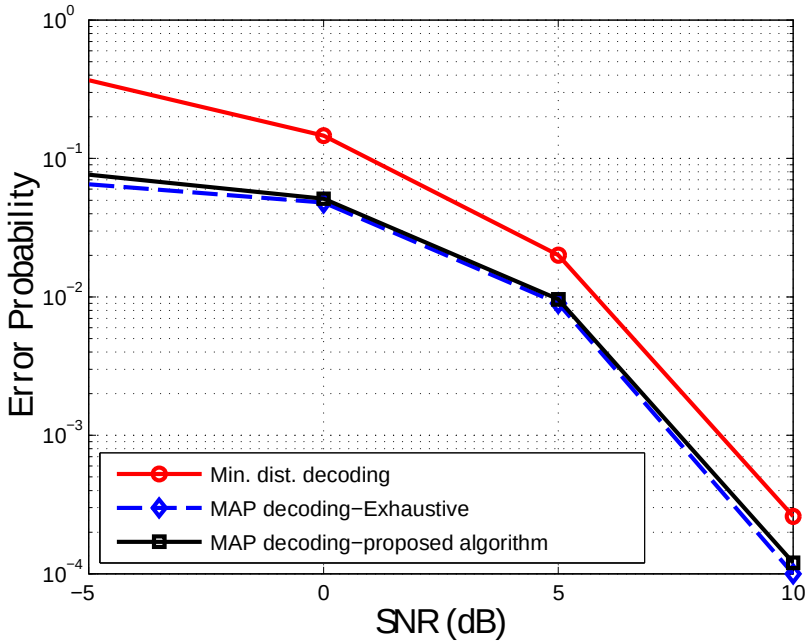


Figure 8: Probabilité d'erreurs pour $\mathsf{n} = 4; \mathsf{N} = 2; \mathsf{P} = 1$.

Décodeurs efficaces pour le CF: cas du canal à évanouissement

Dans cette partie nous étudions le cas du canal à évanouissements. Nous analysons le décodeur à *Maximum à Vraisemblance* (ML), qui est le décodeur optimal pour ce modèle canal. Nous considérons seulement le cas des réseaux de points entiers pour des raisons de simplification et nous nous focalisons sur le décodage de la combinaison entière $t = \sum_{i=1}^{N} a_i x_i \in \Lambda_f$. Nous évaluons la probabilité d'erreurs en comptabilisant les erreurs sur le décodage de cette combinaison.

Métrique de décodage ML

La métrique de décodage ML est donnée par:

$$\hat{t} = \underset{t \in \Lambda_f}{\operatorname{argmax}}\, p(\tilde{y}|t) \tag{18}$$

Nous montrons que ce problème de maximisation peut s'écrire sous la form suivante:

$$\hat{t} = \underset{t \in \Lambda_f}{\operatorname{argmax}} \sum_{(x_1,\dots,x_N) \in \mathbb{Z}^N = \sum_{i=1}^{N} a_i x_i = t} \exp\left(\frac{-1}{2\sigma^2} \| \tilde{y} - \sum_{i=1}^{N} \tilde{h}_i x_i \|^2\right) \tag{19}$$

Soit la fonction ML suivante

$$\varphi(\Lambda) = \sum_{(x_1,\dots,x_N) \in \mathbb{Z}^N = \sum_{i=1}^{N} a_i x_i = t} \exp\left(\frac{-1}{2\sigma^2} \| \tilde{y} - \sum_{i=1}^{N} \tilde{h}_i x_i \|^2\right) \tag{20}$$

Pour trouver la solution ML, nous devons maximiser la fonction ML φ. Dans notre étude, nous traitons d'abord le cas multi-dimensionnels puis le cas de $n = 1$. Pour le cas général, nous montrons que le problème de décodage ML est équivalent à résoudre une *Approximation Diophantienne* donnée par:

$$\hat{t} = \underset{t \in \Lambda_f\,;\, q \in \mathcal{A}_L}{\operatorname{argmax}} \| \psi(\Lambda) - q \|^2 \tag{21}$$

où $\mathcal{A}_L$ est un sous-ensemble fini du réseau de points $\mathcal{L}$ défini par une matrice génératrice $\sum_{i=1}^{N} \tilde{h}_i M U_i$.

En ce qui concerne le cas uni-dimensionnel, nous analysons en détails la fonction ML. Cette fonction est périodique, dépend du SNR, des coefficients d'évanouissements, du vecteur du code de réseaux a ainsi que de la contrainte de puissance P. Nous étudions aussi l'impact de ces paramètres sur le comportement de la fonction ML et explorons le problème de platitude: pour certaines valeurs des paramètres dont dépend φ, le maximum de cette fonction peut être atteint pour différentes valeurs de t, ce qui résulte en des erreurs de décodage. Un exemple de ce comportement est présenté

à travers la Figure.9. Comme nous pouvons le constater, la fonction ML atteint son maximum pour $t = 5$ et $t = 6$. Le récepteur dans ce cas ne peut pas distinguer la valeur de t pour laquelle la fonction ' est maximisée ce qui génère des erreurs de détection.

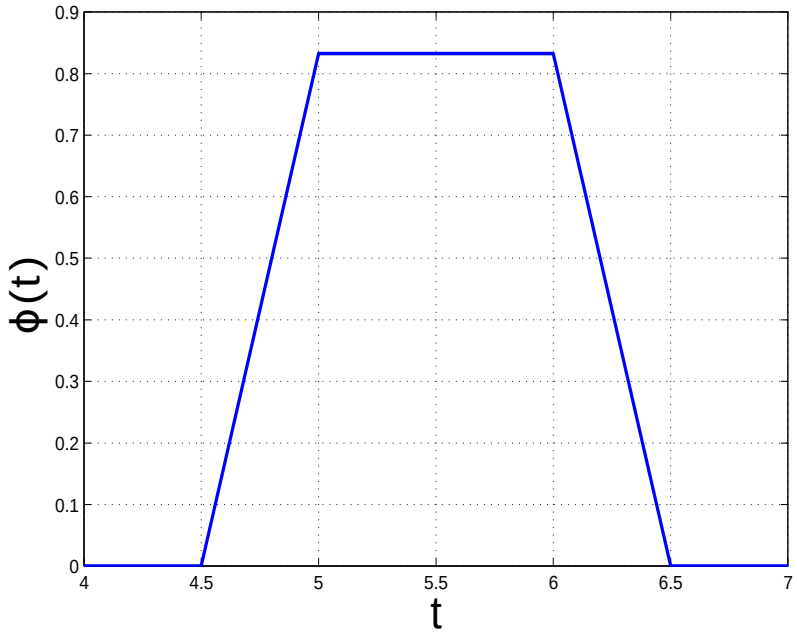


Figure 9: Platitude de la fonction ML.

Pour surmonter le problème de platitute de la fonction ML, nous proposons une approximation du décodeur ML qui consiste à résoudre le problème suivant:

$$\hat{t} = \underset{k2Z;t2A_t}{\operatorname{argmin}} \mid \square^{0}k - t - y^{0} \mid \tag{22}$$

où $k \in Z$, $\square^{0} = \frac{\square}{\square}$ et $y^{0} = -\frac{\not{\square}}{\square}$, avec $\square = \square h_1 u_1 + \square h_2 u_2$; $\square = a_1 \square h_2 - a_2 \square h_1$ et $(u_1; u_2)$ vérifient $u_1 a_1 + u_2 a_2 = \mathrm{pgcd}(a_1; a_2)$. Ce problème de minimisation est équivalent à la résolution d'une approximation diophantienne inhomogène (IDA). Dans notre implémentation de ce problème, nous utilisons une version modifiée de l'algorithme de Cassel.

Résultats de simulations

Nous évaluons les performances de notre algorithme d'approximation diophantienne et du décodeur standard du protocole CF en termes de probabilité d'erreurs. Nous considérons le cas scalaire où $n = 1$ et des constellations entières définies par l'alphabet $[-S_m\ S_m]$. Nos résultats présentés par la Figure.10 pour $S_m = 5$ montrent que notre algorithme atteint les mêmes performances que le décodeur à minimisation de la distance

euclidienne à faible et moyen SNR. Notre approche apporte un gain seulement à fort SNR où le décodeur standard du CF présente une platitude.

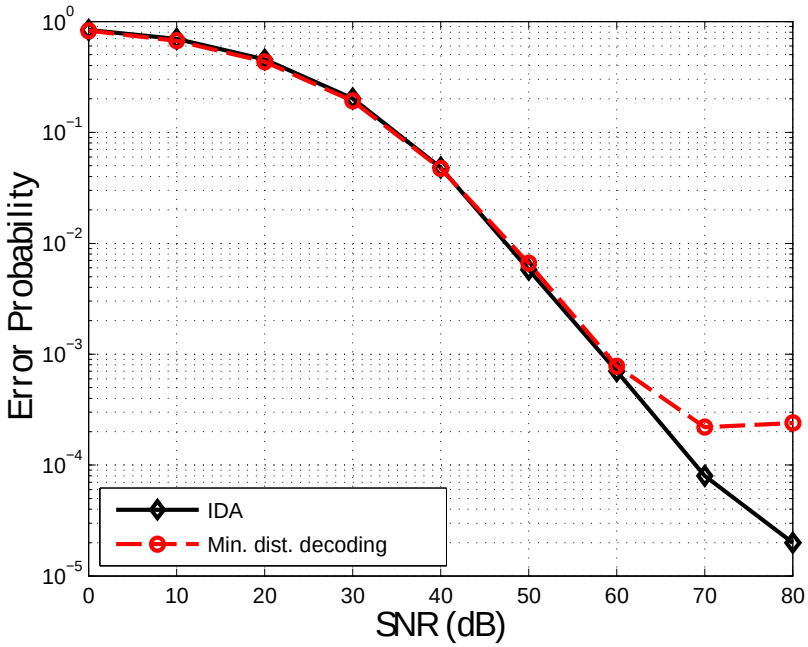


Figure 10: Probabilité d'erreurs pour $S_m = 5$.

Chapitre 3: Le canal à relais bidirectionnel

Dans ce chapitre nous adressons la première application des stratégies de codage de réseaux dans le canal à relais bidirectionnel présenté par la Figure.11. Les nœuds N_1 et N_2 désirent échanger leurs messages $w_1 \in F_p$ et $w_2 \in F_p$ respectivement. Cet échange se déroule dans deux phases différentes (orthogonales). Pendant la première phase, le nœud N_1 (respectivement N_2) code son message w_1 (respectivement w_2) en $x_1 \in \Lambda$ (respectivement $x_2 \in \Lambda$) utilisant le même réseau de codage Λ_F et respectant la même contrainte de puissance définie par le réseau de mise en forme Λ_C tel que

$$\frac{1}{n}E\left[\| x_i \|^2\right] \leq P; \quad i = 1; 2 \tag{23}$$

Les mots de codes sont ensuite transmis simultanément au relais R. Durant la deuxième phase, le relais implémente le codage de réseaux et renvoie aux nœuds N_1 et N_2 un signal x_R qui est une fonction des mots de codes originaux. Chacun de ces nœuds se sert de cette fonction et de la connaissance à priori de son message original pour déduire une estimation du message désiré, $\hat{w}_2$ pour N_1 et $\hat{w}_1$ pour N_2.

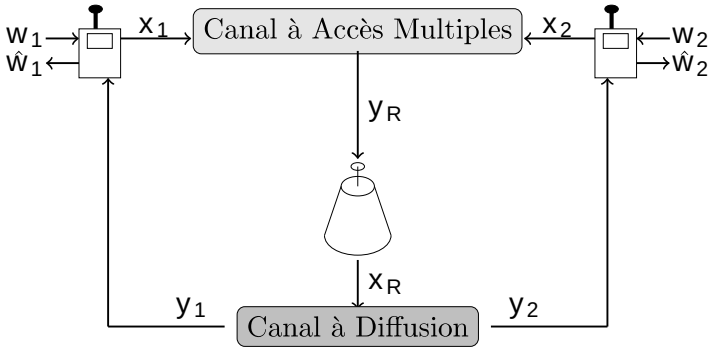


Figure 11: Canal à relais bidirectionnel implémentant le PLNC.

Nous traitons dans une première partie le canal Gaussien et étudions les protocoles Analog Network Coding, le Compute-and-Forward et le Denoise-and-Forward. Nous analysons ensuite le canal à évanouissements et étudions les protocoles Analog Network Coding et le Compute-and-Forward. Nous évaluons pour les deux canaux le taux d'erreurs total défini par la probabilité d'erreurs $P_{e;sum}$ donnée par

$$P_{e;sum} \stackrel{4}{=} \Pr(\hat{w}_1 \neq w_1) + \Pr(\hat{w}_2 \neq w_2) \tag{24}$$

Et le débit d'échange défini par:

$$\mathcal{R}_{ex} = \mathcal{R}_{N_1!\ N_2} = \mathcal{R}_{N_2!\ N_1} = \min(\mathcal{R}_{N_1!\ R}; \mathcal{R}_{R!\ N_2}) \tag{25}$$

Cas du Canal Gaussien

Pour ce premier cas, le signal reçu au relais s'écrit sous la forme:

$$y_R = x_1 + x_2 + z_R \tag{26}$$

où $z_R \in \mathbb{R}^n$ est un BBAG de variance σ_R^2. A partir de cette superposition, le relais calcule et diffuse un signal $x_R = f(x_1; x_2)$ à N_1 et N_2. Ce signal dépend de la stratégie de PLNC adoptée. Nous analysons dans la suite le traitement effectué au niveaux du relais et des nœuds sources pour chacun des protocoles ANC, CF et DoF.

Schéma Analog Network Coding

Le relais dans ce cas multiplie le signal reçu par un facteur d'amplification $\alpha = \sqrt{\frac{P}{1+2P}}$ et diffuse la fonction $x_R = \alpha y_R$. Le nœud N_i $(i = 1; 2)$ observe le signal

$$y_i = x_R + z_i = \alpha x_1 + \alpha x_2 + \alpha z_R + z_i \tag{27}$$

Le traitement effectué au niveau du nœud N_i $(i = 1; 2)$ pour obtenir une estimation du message désiré w_j $(j = 2; 1)$ est le suivant:

1. Soustraction du mot de code émis: $\tilde{y}_i = y_i - \square x_i = \square x_j + \square z_R + z_i$.
2. Décodage ML de x_j : $\hat{x}_j = \text{argmin}_{\square 2 \square} \parallel \tilde{y}_i - \square\square \parallel^2$.
3. Application de la fonction $\square^{\square 1}$: $\hat{w}_j = \square^{\square 1}(\hat{x}_j)$

Nous montrons que le débit d'échange utilisant le protocole ANC est donné par:

$$\mathcal{R}_{ex;ANC} = \frac{1}{2}\log(1+\square_{eq}) = \frac{1}{2}\log\left(1+\frac{\square^2}{1+3\square}\right) \tag{28}$$

Schéma Compute-and-Forward

Avec le protocole CF, le relais calcule et diffuse la fonction $x_R = [x_1 + x_2] \bmod \Lambda_C$ suivant les étapes du calcul décrites en détails dans le chapitre précédent. A la réception de ce signal, le nœud N_i $(i = 1; 2)$ effectue les traitements suivants:

1. Décodage ML: $\hat{x}_{R;j} = \text{argmin}_{\square 2 \square} \parallel y_i - \square \parallel^2 \; ; \; j = 2; 1$.
2. Application de la fonction $\square^{\square 1}$: $u_j = \square^{\square 1}(\hat{x}_{R;j}) = w_1 \oplus w_2$.
3. Soustraction du message connu: $\hat{w}_j = u_j \ominus w_i$ $(j = 2; 1)$.

Le débit d'échange pour le protocole CF a été prouvé dans [60, 67] et est donné par:

$$\mathcal{R}_{ex;CF} = \frac{1}{2}\log\left(\frac{1}{2}+\frac{P}{\square^2}\right) \tag{29}$$

Schéma Denoise-and-Forward

L'objectif de décodage au niveau du relais implémentant le protocole DoF est le même qu'utilisant le protocole CF. La seule différence est que le relais n'effectue pas l'étape de multiplication à son signal reçu y_R. Pendant la deuxième phase de communication, les nœuds N_1 et N_2 implémentent les mêmes traitements que dans le cas du CF. Le débit d'échange pour le protocole DoF est donné par:

$$\mathcal{R}_{ex;DoF} = \frac{1}{2}\log\left(\frac{P}{\square^2}\right) \tag{30}$$

Résultats de simulations

Nous évaluons le taux d'erreurs total et le débit d'échange pour les tratégies ANC, CF et DoF. Commençant par le débit d'échange, nos résultats de simulations présentés en Figure.12 montrent que le protocole CF est optimal à fort SNR et offre de performances meilleurs que les protocoles ANC, DoF, le codage de réseaux couche paquets (3-TS Network Coding) et la stratégie de relayage se basant sur le simple routage.

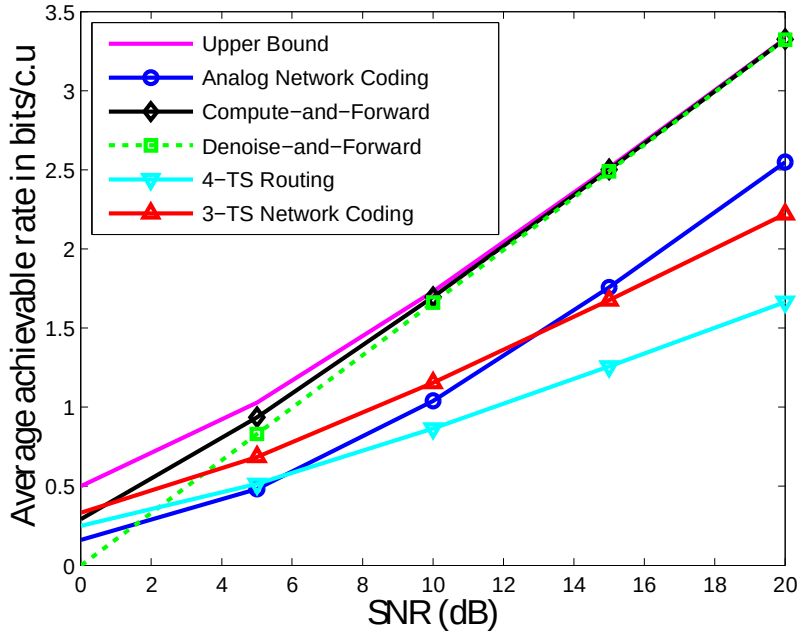


Figure 12: Débit d'échange moyen par utilisation canal pour le canal Gaussien.

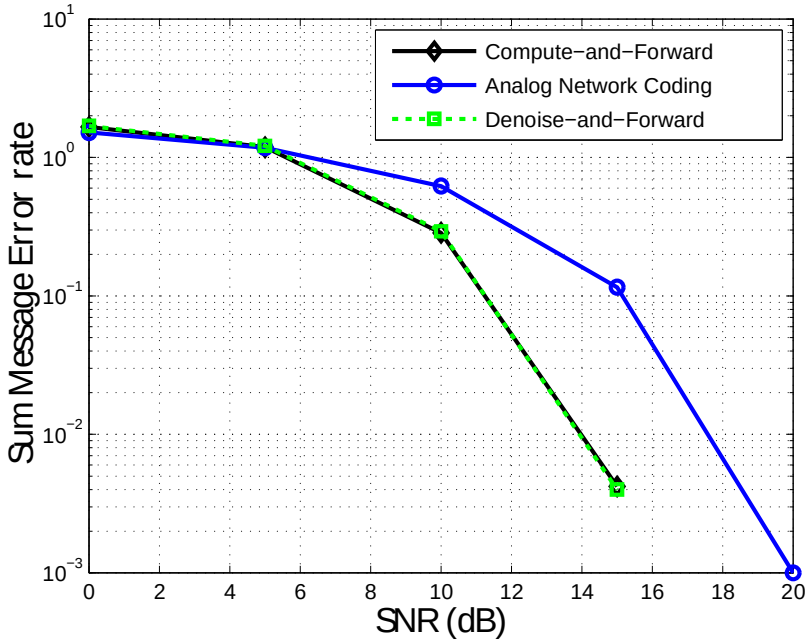


Figure 13: Taux d'erreurs total pour le canal Gaussien.

Le sous-optimalité du protocole DoF par rapport au CF est due à l'étape de multiplication du signal reçu au niveau du relais, qui permet d'obtenir des débits de calculs plus élevés. Dans le cas du ANC, sa sous-optimalité provient de l'amplification du bruit au niveau du relais. En ce qui concerne le taux d'erreurs total, nos résultats de simulations tracés en Figure.13 confirment que les protocoles CF et DoF ont le même taux d'erreurs. Le gain de ces deux derniers par rapport à la stratégie ANC s'évalue à 3.75dB à un taux d'erreurs total de 10^{-2}.

Cas du Canal à évanouissements

Pour ce deuxième cas de figure, le signal reçu au niveau du relais s'écrit sous la forme:

$$y_R = h_1 x_1 + h_2 x_2 + z_R \tag{31}$$

où $h_1; h_2 \in R$ représentent les coefficients d'évanouissements correspondant au canal entre N_1 et R et N_2 et R respectivement.

Schéma Analog Network Coding

Le relais dans ce cas amplifie le signal reçu par le facteur $\alpha = \sqrt{\frac{P}{1+\sigma^2 |h|^2}}$ et le diffuse aux nœuds sources. Ces derniers observent les signaux suivants:

$$y_1 = h_1 x_R + z_1 = \alpha h_1^2 x_1 + \alpha h_1 h_2 x_2 + \alpha h_1 z_R + z_1 \tag{32}$$

$$y_2 = h_2 x_R + z_2 = \alpha h_2^2 x_2 + \alpha h_1 h_2 x_1 + \alpha h_2 z_R + z_2 \tag{33}$$

Le traitement au niveaux de N_1 et N_2 consiste aux étapes suivantes:

1. Soustraction du mot de code connu:
   N_1 obtient $\tilde{y}_1 = y_1 - \alpha h_1^2 x_1 = \alpha h_1 h_2 x_2 + \alpha h_1 z_R + z_1$
   N_2 obtient $\tilde{y}_2 = y_2 - \alpha h_2^2 x_2 = \alpha h_1 h_2 x_1 + \alpha h_2 z_R + z_2$

2. Décodage ML:

$$\hat{x}_2 = \underset{x_2 \in \mathcal{A}}{\operatorname{argmin}} \| \tilde{y}_1 - \alpha h_1 h_2 x \|^2 \;\; ; \;\; \hat{x}_1 = \underset{x_2 \in \mathcal{A}}{\operatorname{argmin}} \| \tilde{y}_2 - \alpha x \|^2 \tag{34}$$

3. Mapping au corps fini pour obtenir: $\hat{w}_2 = \phi^{-1}(\hat{x}_2) \;\; ; \;\; \hat{w}_1 = \phi^{-1}(\hat{x}_1)$

Le débit d'échange pour le protocole ANC est donné dans ce cas par:

$$\mathcal{R}_{ex;ANC} = \min_{m=1;2} \frac{1}{2} \log \left(1 + \frac{h_m^2 P^2}{1 + \sigma^2 (1 + \| h \|^2)} \right) \tag{35}$$

Schéma Compute-and-Forward

Le relais dans ce cas décode la combinaison donnée par:

$$x_R = [a_1 x_1 + a_2 x_2] \mod \Lambda_C \tag{36}$$

Ce signal est ensuite diffusé aux nœuds finaux qui effectuent le traitement suivant:

1. Décodage ML: $\hat{x}_{R;i} = \text{argmin}_{\square 2 \square} \| y_i - h_i \square \|^2$; $i = 2;1$
2. Mapping au corps fini: $u_i = \square^{\square 1}(\hat{x}_{R;i}) = q_1 w_1 \oplus q_2 w_2$; $i = 1;2$.
3. Soustraction des messages connus: $n_1 = u_1 \ominus q_1 w_1 = q_2 w_2; n_2 = u_2 \ominus q_2 w_2 = q_1 w_1$.
4. Division par les messages q_i: $\hat{w}_2 = \frac{n_1}{q_2}$; $\hat{w}_1 = \frac{n_2}{q_1}$

Une condition nécessaire de décodabilité aux nœuds finaux consiste à avoir $q_2 \neq 0$ au niveau de N_1 et $q_1 \neq 0$ au niveau de N_2. Cette condition est équivalente à avoir $[a_1] \mod p \neq 0$ et $[a_2] \mod p \neq 0$. Nous établissons dans ce chapitre un nouveau lemme de construction de codes de réseaux pour le CF dans le canal à relais bidirectionnel tenant en compte cette condition de décodabilité et développons un algorithme pratique de son implémentation se basant sur la méthode d'énumération Fincke-Pohst [9].

Résultats de simulations

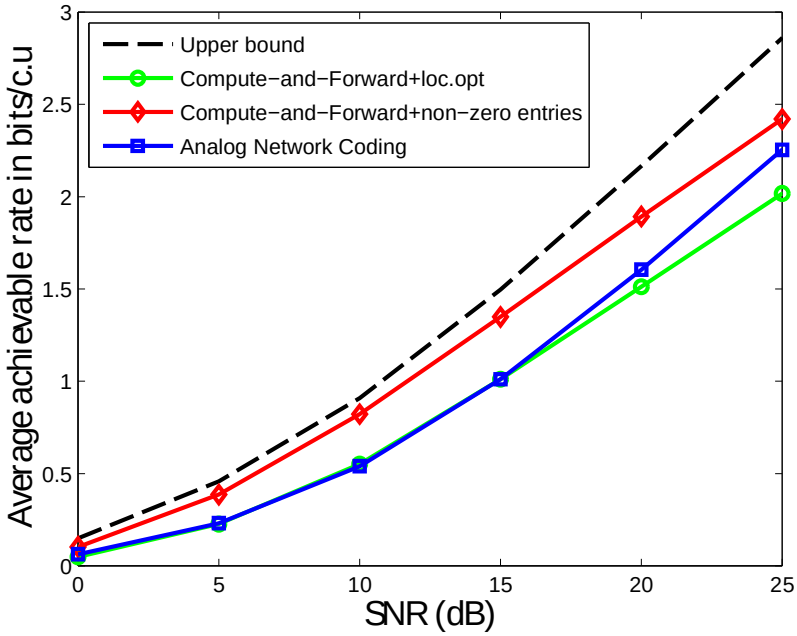


Figure 14: Taux d'échange pour le canal à évanouissements.

Nous évaluons les performances des stratégies CF et ANC en termes de débit d'échange et de taux d'erreurs total. Pour le protocole CF, nous étudions notre algorithme mettant en oeuvre la condition de décodabilité ainsi que le schéma de codage standard où le vecteur du code de réseaux a est construit en maximisant le débit de calcul au niveau du relais sans considération de la contrainte de décodabilité.

Commençant par le débit d'échange, nos résultats de simulations présentés en Figure.14 montrent la perte en performances due au non respect de la contrainte de décodabilité. Notre algorithme apporte un gain considérable par rapport à l'approche existante et à la stratégie ANC.

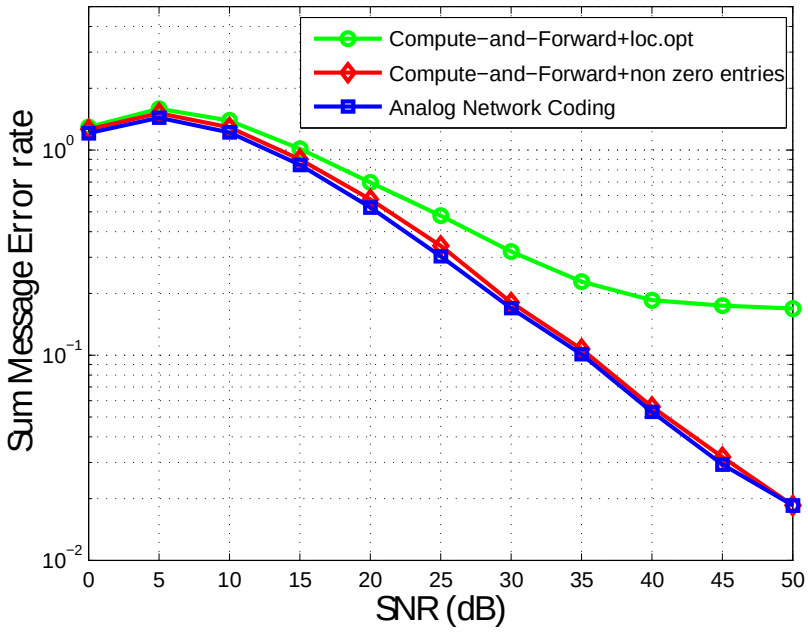


Figure 15: Taux d'erreurs total pour le canal à évanouissements.

En ce qui concerne le taux d'erreurs total dont les résultats de simulations sont présentés à travers la Figure.15, nous soulignons tout d'abord la perte significative en performances à cause de la négligence de la contrainte de décodabilité. Notre algorithme apporte en effet un gain considérable par rapport au CF standard dépassant 15dB à fort SNR. Nos résultats numériques mettent en évidence aussi que notre algorithme offre les mêmes performances que la stratégie ANC contrairement au cas du canal Gaussien. Ce comportement est dû à l'erreur de quantification ou d'approximation des coefficients d'évanouissements réels par les les coefficients entiers formant le vecteur du code de réseaux.

Chapitre 4: Le canal à sources et relais multiples

Dans ce chapitre nous étudions l'implémentation des stratégies ANC et CF dans le canal à sources et relais multiples présenté en Figure.16.

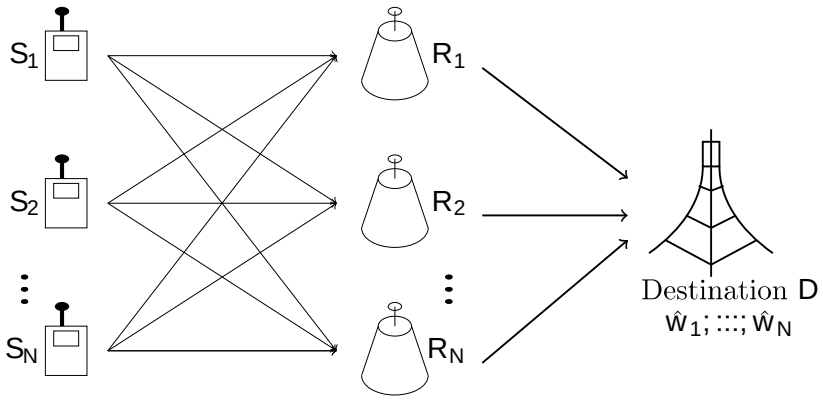


Figure 16: Canal à sources et relais multiples.

Les sources $S_i; i = 1; :::; N$ désirent communiquer leurs messages w_i à la destination D. La transmission se déroule en deux phases orthogonales. Dans un premier lieu, les sources encodent leurs messages en vecteurs $x_i \in \Lambda$ et les envoient simultanément aux relais. Le signal reçu au relais R_m s'écrit sous la forme:

$$y_m = \sum_{i=1}^{N} h_{im} x_i + z_m \tag{37}$$

où $h_{im} \in R$ représente le coefficient d'évanouissement entre la source S_i et le relais R_m, supposé constant durant la transmission des mots de codes x_i. $z_m \in R^n$ est un BBAG de variance σ^2. Nous supposons une connaissance parfaite du canal au récepteur. Dans ce contexte, le relais R_m connait uniquement le vecteur canal $h_m = [h_{1m} ::: h_{Nm}]^t$. De plus, nous supposons que la destination a une connaissance parfaite des vecteurs $h_1; :::; h_N$. Pendant la deuxième phase de transmission, chacun des relais implémente un codage de réseaux au niveau physique pour calculer le signal $\Delta_m; m = 1; :::; N$ en fonction des mots de codes originaux. Chacun des relais transmet par la suite sa fonction à la destination. Les liens relais-destination sont supposés parfaits et orthogonaux. La destination utilise toutes les fonctions $\Delta_1; :::; \Delta_N$ pour avoir des estimations des messages originaux $\hat{w}_1; :::; \hat{w}_N$. La probabilité d'erreurs à la destination est définie par:

$$P_D = \Pr\left[\bigcup_{i=1}^{N} \hat{w}_i \neq w_i\right] \tag{38}$$

Schéma Analog Network Coding

Le rôle des relais utilisant la stratégie ANC consiste à amplifier le signal reçu. La fonction calculée au relais R_m est alors donnée par:

$$\square_m = \square_m y_m = \square_m \left(\sum_{i=1}^{N} h_{im} x_i + z_m \right) \tag{39}$$

Le facteur d'amplification relatif au relais R_m est égal à:

$$\square_m = \sqrt{\frac{\square}{1 + \square \| h_m \|^2}} \tag{40}$$

L'avantage de la stratégie ANC est la facilité d'implémentation. Cependant, un des inconvénients majeurs est l'amplification du bruit qui résulte en une dégradation des performances.

Schéma Compute-and-Forward

Dans le cas du protocole CF, le relais R_m décode et transmet la fonction

$$\square_m = \left[\sum_{i=1}^{N} a_{mi} x_i \right] \mod \Lambda_C \tag{41}$$

Les coefficients $a_{m1}; :::; a_{mN} \in Z$ forment le vecteur du code de réseaux $a_m = [a_{m1} ::: a_{mN}]^t$ correspondant au relais R_m. Nous analysons le système d'équations reçu à la destination et montrons que ce dernier s'écrit sous la forme:

$$L = \begin{pmatrix} \hat{\square}_1^t \\ \vdots \\ \hat{\square}_N^t \end{pmatrix} A = [A X] \mod \Lambda_C \tag{42}$$

où les lignes de la matrice $A \in Z^{N \square N}$ correspondent aux vecteurs $a_1^t; :::; a_N^t$ tel que:

$$A = \begin{pmatrix} a_1^t \\ \vdots \\ a_N^t \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{pmatrix}$$

En étudiant les étapes de décodage à la destination, nous proposons un nouveau lemme établissant un critère de construction des vecteurs entiers $a_1; :::; a_N$ maximisant le débit de transmission total telle que la matrice A satisfait $\det(A) \neq [0] \mod p$. Nous développons aussi des algorithmes pratiques de construction d'une telle matrice en se basant sur l'algorithme de Fincke-Pohst.

Résultats de simulations

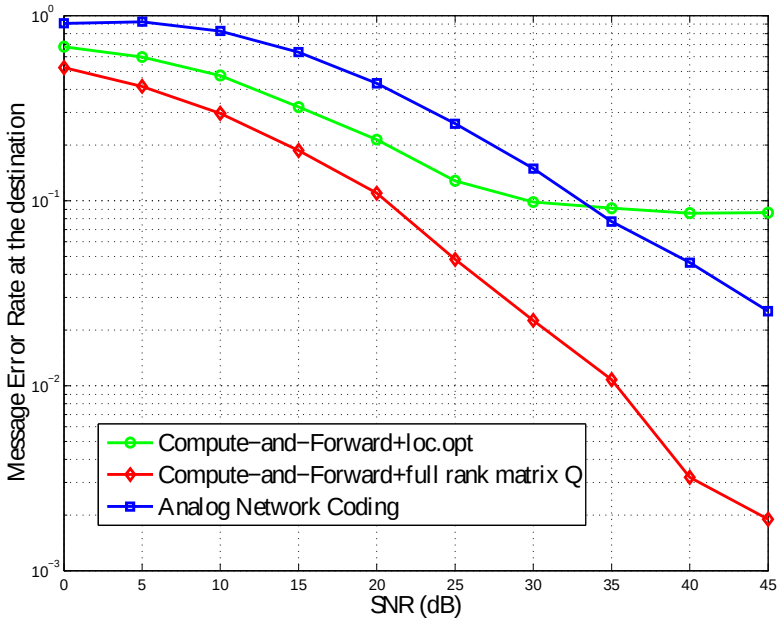


Figure 17: Taux d'erreurs à la destination pour le canal MSMR.

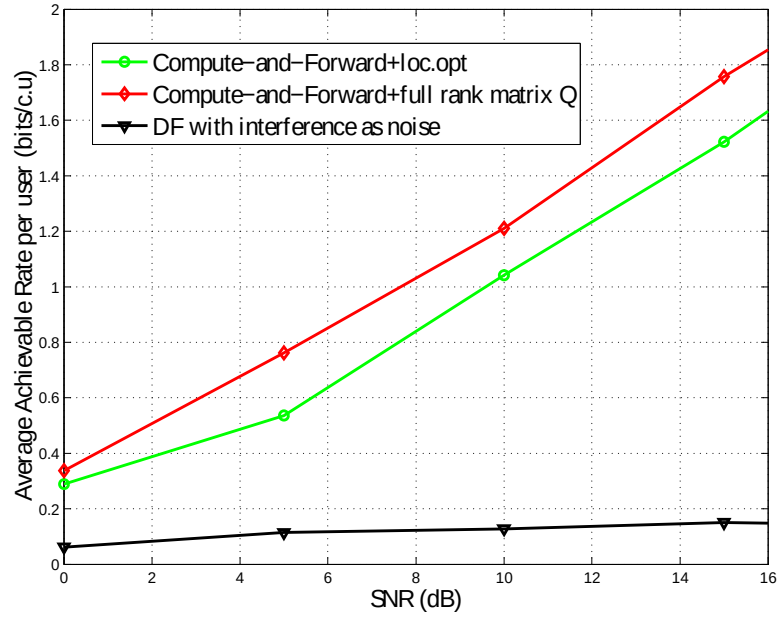


Figure 18: Débit de transmission moyen pour le canal MSMR.

Nous évaluons la probabilité d'erreurs et le débit de transmission total à la destination. Nos résultats de simulations présentés à travers la Figure.17 et la Figure.18 mettent en évidence l'importance de notre algorithme tenant en compte la contrainte sur la matrice A et son gain par rapport à la stratégie ANC et au schéma existant du protocole CF basé sur la recherche de la matrice A qui permet de maximiser les débits de calculs aux relais d'une façons indépendante.

Chapitre 5: Le canal MIMO distribué

Nous traitons dans ce dernier chapitre le canal MIMO distribué composé de M sources équipée chacune d'elle d'une seule antenne, et d'une destination commune équipée de $N \geq M$ antennes.

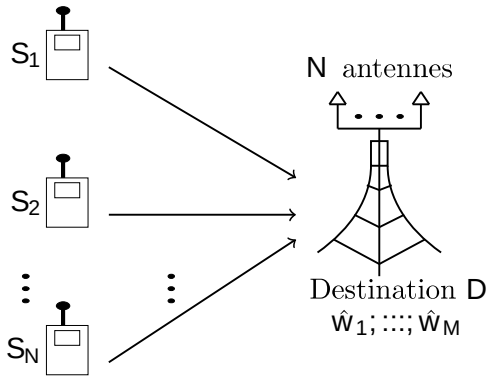


Figure 19: Canal MIMO distribué.

Les messages $w_1;:::;w_M$ des sources sont encodés et transmis à travers le canal. Le signal reçu à la destination s'écrit sous la forme

$$Y = HX + Z \tag{43}$$

où les matrices

$$X = \begin{bmatrix} x_1^t \\ \vdots \\ x_M^t \end{bmatrix} \in R^{M \times n} \; ; \; H = \begin{bmatrix} h_1^t \\ \vdots \\ h_N^t \end{bmatrix} \in R^{N \times M} \; ; \; Z = \begin{bmatrix} z_1^t \\ \vdots \\ z_N^t \end{bmatrix} \in R^{N \times n} \tag{44}$$

représentent respectivement la matrice des mots de codes sources, la matrice des coefficients d'évanouissements et la matrice du BBAG. Les vecteurs z_m pour $m = 1;:::;N$ sont générés selon la loi normale $\mathcal{N}(0; \sigma^2 I_n)$. Nous considérons le cas du canal à évanouissement quasi-statique et supposons une connaissance parfaite du canal au récepteur. Dans une première partie nous présentons les décodeurs MIMO classiques, commençant par le décodeur ML optimal ensuite les décodeurs linéraires ZF et MMSE et les récepteurs linéaires précédés d'un prétraitement à travers une réduction de la matrice canal. Dans

une seconde partie, nous exposons la nouvelle architecture des décodeurs *Integer Forcing*. Le principe de ces derniers consiste à exploiter la structure linéaire des codes correcteurs d'erreurs afin de simplifier l'architecture du récepteur: au lieu de décoder les mots de codes sources séparément, il suffit de décoder des combinaisons linéaires linéairement indépendantes de ces derniers dont les coefficients sont donnés par une matrice A entière et de rang plein. Un critère de sélection de cette matrice a été proposé en littérature et consiste à maximiser le débit total. En se basant sur ce critère, nous développons de nouveaux algorithmes efficaces pour la sélection de la meilleure matrice A qui soit de rang plein.

Résultats de simulations

Nous évaluons les performances en termes de probabilité d'erreurs et de débit de transmission total. Nous analysons le décodeur ML optimal, les récepteurs linéaires ZF et MMSE, les décodeurs LLL+ZF et LLL+MMSE implémentant la réduction LLL, et les décodeurs IF utilisant nos algorithmes proposés. Nos résultats de simulations présentés par la Figure.20 et la Figure.21 mettent en évidence le gain apporté par la nouvelle architecture des décodeurs IF par rapport aux récepteurs linéaires existants.

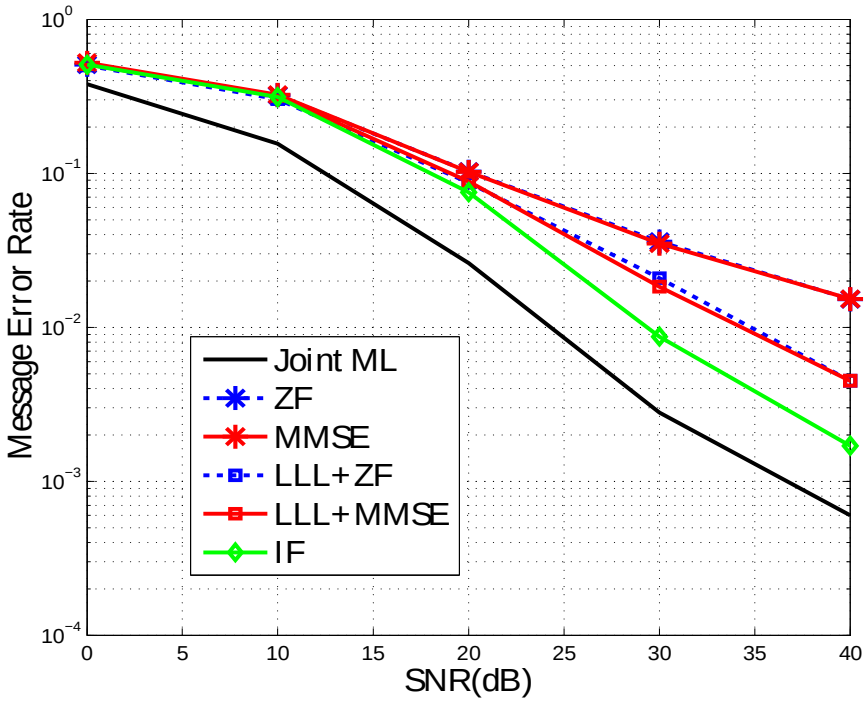


Figure 20: Taux d'erreurs pour le canal MIMO distribué.

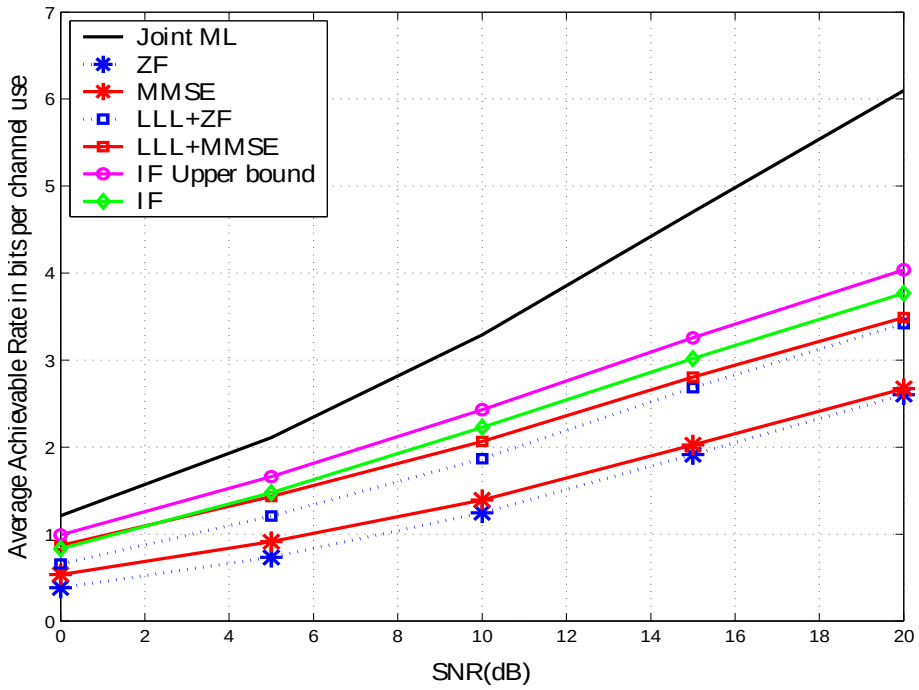


Figure 21: Débit total de transmission pour le canal MIMO distribué.

Perspectives

Comme perspectives pour les travaux futurs, nous proposons les directions suivantes:

- **Décodeurs Integer Forcing combinés avec le codage Espace-temps**: notre étude de l'architecture des décodeurs IF élaborée dans cette thèse a révélé l'importance de ces récepteurs et leurs gains significatifs par rapport aux techniques de décodage sous-optimales existantes. Nous visons dans le futur à étudier les gains possibles de cette nouvelle architecture dans un système MIMO codé, où un code espace-temps est implémenté à l'émission.

- **Codage de réseaux pour les communications optiques**: pour cette direction, nous visons à étudier l'application des technique de codage de réseaux dans les systèmes de communications optiques.

- **Codage de réseaux pour le stockage distribué**: l'une des premières applications du codage de réseaux est le stockage distribué. Nous visons à travers cette piste de recherche à explorer la construction de codes de réseaux au niveau physique afin de concevoir des systèmes de stockage efficaces et sécurisés.

Introduction

Last years have witnessed spectacular developments of wireless networks that have widely transformed all aspects of our daily life. Driven by the emergence of new real-time high-throughput multimedia applications and the success of digital technologies, several network solutions are available today and are thoroughly used in all modes of communications. Main examples include cellular networks, wireless ad-hoc networks and wireless sensor networks.

Practical wireless communication systems are inherently multiuser systems accomodating multiple transmitters and receivers that share the same, often limited, resources such as bandwidth. This is the case for example of cellular mobile networks where the task of a base station is to serve many subscribers in the same geographical location at the same time. The main distinguishing features of such multiuser networks are the *broadcast* and *superposition*. Indeed, as signals of different users, sharing the same physical resources, travel through the same interface, a signal sent from a transmitter is broadcast to all nearby users, consequently it reaches both the desired and unintended receivers. On the other hand, instantaneous transmissions by different users result in a superposition of signals at the receivers covered by the same transmission range. These two intrinsic properties of the wireless medium create a *multiuser interference* or *multiple access interference*. The design of a reliable wireless system is conditioned on a good understanding and management of this interference problem which can be detrimental to the system performance.

Multiple access interference is a widely investigated topic particularly in the realm of Information Theory. There are essentially two ways to resolve this problem: a *single-user* approach and a *multiuser* technique. The first method aims to provide an *orthogonal access* to the channel by allocating and maintaining separate channel resources to each user, either in time (e.g., Time Division Multiple Access), in frequency (e.g., Frequency Division Multiple Access) or in signal code (e.g., Code Division Multiple Access). Despite the fact that this single-user approach guarantees interference-free transmissions, there remain drawbacks, essentially a reduced spectral efficiency. Lessons learned from multiuser Information Theory [1] show that orthogonal multiple access is suboptimal. The best way to optimally share the spectral resources in a multiuser system is to harness

the interference and instead of avoiding it, we should consider it as a useful information to serve the decoding process of the desired signal. This is the philosophy of the second multiuser detection [2] approach which deals with the design of multiple access codes and interference cancellation schemes. From an information-theoretic perspective, these techniques allow to increase the spectral efficiency [3], however, their high design complexity make their implementation in practical settings a challenging task.

In this work, we are interested in a new approach to mitigate the multiple access interference in wireless networks termed *Physical-layer network coding* (PLNC). This framework came recently into light with the pioneering works of Zhang *et al.* in [4] and Popovski and Yomo in [5, 6]. It has been proposed as a valuable solution to improve the way to manage interference in wireless networks including multiple access channels. The philosophy of this new approach is to enable intermediate nodes in a given wireless network, observing a signal resulting from multiple access interference, to decode and forward functions of the interfering signals. Treating interference as useful information under PLNC is proved to offer higher transmission rates and several noteworthy advantages.

Physical-Layer Network Coding can operate in conjunction to physical layer techniques such as source coding and channel coding [7]. Joint source-network coding arises particularly in networks where the sources are correlated such as sensor networks. In general settings where the sources are uncorrelated, integrating channel coding and network coding has attracted a particular research attention and several works have been developed in this context. In this scope, a very promising linear Physical-Layer Network Coding protocol termed the *Compute-and-Forward* (CF) has emerged in the last few years. Introduced by Nazer and Gastpar in [8], the CF scheme allows to harness the multiple access interference through the use of lattice-based channel coding. This new framework is applicable to any network configuration accomodating source nodes, relays and destinations that communicate through linear additive white Gaussian noise channels. Main primary works on the CF are information theoretic and show its promising potential particularly in terms of transmission rates that go highly beyond those permitted by existing relaying strategies based on interference avoidance. However, several relevant issues related to the implementation of the CF in practical communication scenarios have been overlooked.

Objectives, Assumptions and Considered Scenarios

Motivated by the promising gains of PLNC, this work is dedicated to the analysis, design and performance evaluation of Physical-Layer Network Coding strategies in multiuser wireless communication systems including multiple access channels. We focus on PLNC joint to lattice-based channel coding and study the end-to-end implementation and performance of the CF, the Analog Network Coding (ANC) and the Denoise-and-Forward (DoF) strategies. For practical implementation reasons, we study for the CF protocol missing issues related to the network codes design and optimal decoding algorithms at

the level of the relay nodes and end destinations. We study the three following network configurations:

1. The Two-Way Relay Channel (TWRC, depicted in Figure 22) with two communicating nodes N_1, N_2 and a relay node R. All nodes are equipped with a single antenna. For this setting, we aim to analyze the design and end-to-end error performance of the ANC, the DoF and the CF strategies.

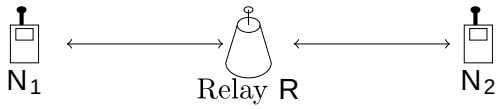


Figure 22: Two-Way Relay Channel.

2. The Multi-Source Multi-Relay Channel (MSMR, depicted in Figure 23) with N independent sources, N relays and a common destination D. All nodes in this network are equipped with a single antenna. For this setting we aim to study the design and end-to-end performance of network codes for the CF and the ANC.

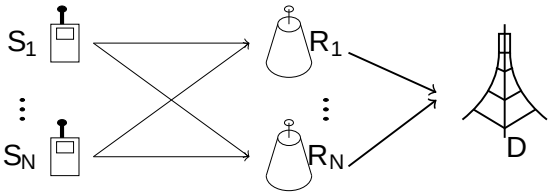


Figure 23: The Multi-Source Multi-Relay Channel.

3. The Distributed Multiple Input Multiple Output (MIMO) Channel (depicted in Figure 24) with N independent single antenna sources and a common destination D equipped with $\mathsf{M} \geq \mathsf{N}$ antennas. For this setting, we aim to study a new architecture of MIMO decoders inspired by the CF protocol termed *Integer Forcing linear receivers* (IF) and compare its performance to the traditional MIMO decoders.

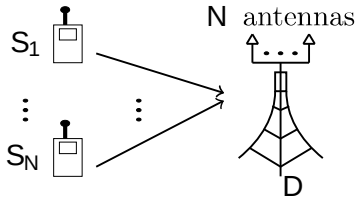


Figure 24: The Distributed MIMO Channel.

For these three network models, we assume that all nodes operate in a half-duplex mode and are perfectly synchronized. The sources and the destination for the TWRC and MSMR channel are not in line of sight. The destination for these two scenarios is always aware whether the relays use PLNC or not. In addition, we assume perfect channel state information (CSI) at the receiver: relays, when they receive signals from the sources, and the destination have perfect CSI. Finally, the performance metrics considered in this thesis are the message error rate and the average achievable rate at the destination.

The choice of the above described network topologies is driven by their potential application in practical communication systems. The TWRC, for example, can model sattelite communications. The MSMR channel can model a communication over a wireless sensor network and the distributed MIMO channel fits cellular uplink networks with multiple antenna base stations. Although we use similar tools in our analysis that make some results redundant, we found that the three networks should be separately studied since they represent distinct network codes design constraints and decodability conditions at the end destinations. Moreover, it is important to point out that some of the addressed topics in this thesis were simultaneously (and independently) studied by other research groups. Our novel contributions are clearly stated in the following.

Thesis Outline and Contributions

This dissertation is composed of five main chapters. The contents and the contributions of each one of them are summarized in the following.

Chapter 1: Network Coding This chapter is devoted to address the fundamentals of Network Coding and to give some insights into its applications, advantages and challenges. In section 1.1 we illustrate the basic concept of Network Coding and outline its most acknowledged benefits and challenges. Section 1.2 is dedicated to layout some applications of Network Coding. The main Network Coding theorem is provided in section 1.3. It establishes the necessary and sufficient condition on the design of maximum information achieving network codes in multicast networks. In the last section 1.4 we delve into the principle of Physical-Layer Network Coding and present a literature overview on this topic.

Chapter 2: The Compute-and-Forward Protocol This chapter is dedicated to analyze the CF protocol in the basic multiple access channel. As a starting point, we describe in section 2.1 nested lattice coding which is the key ingredient of the CF encoding and decoding schemes. In section 2.2 we outline the decoding steps in the case of real-valued channels. This channel model will be used as a building block for complex-valued channels addressed in section 2.3. The main information-theoretic results regarding the achievable rate will be presented in section 2.4. Our novel results in this chapter include

- A Proposition, in section 2.5, of an optimal solution to design network codes for the CF. By maximizing the achievable rate at the receiver, we show that this solution

is related to a shortest vector problem that can be solved using lattice reduction and decoding techniques.

- A Derivation, in section 2.6, of a novel lower bound on the *ergodic rate* for the CF operating in fast fading channels.

- A Derivation, in section 2.7, of a novel upper bound on the outage probability for the CF in the case of slow fading channels.

- A Derivation, in section 2.8, of a novel *maximum a posteriori* (MAP) decoding metric for the CF operating in Gaussian channels and development of practical decoding algorithms shown to outperform the traditional decoding scheme for the CF.

- An analysis, in section 2.9, of optimal decoders for the CF operating in slow fading multiple access channels and development of a practical decoding algorithm based on Diophantine Approximation.

Chapter 3: The Two-Way Relay Channel This chapter is devoted to analyze the end-to-end performance of the most aknowledged Physical-Layer Network Coding strategies, mainly, the Denoise-and-Forward, the Analog Network Coding and the Compute-and-Forward. Section 3.1 will be devoted to the Gaussian channels case. First, we will describe the system model and assumptions as well as the performance tools. Processings related to the ANC, DoF and CF will be detailed and the corresponding end-to-end error rate performance and achievable rate using a nested lattice code scheme will be addressed. The fading channels case will be the subject of section 3.2. We will start with introducing the system model and assumptions. Then, we will describe the end-to-end processing related to the ANC and the CF schemes. Our novel results in this chapter include:

- A lemma stating a novel design criterion for optimal network codes search for the CF in the fading TWRC.

- A proposition of a search algorithm for efficient network codes based on a modified version of the Fincke-Pohst algorithm [9]. Numerical results evaluating the performance of the proposed approach are provided and show the effectiveness of our method.

- An analysis of the end-to-end performance of the ANC and the CF. We show that for the Gaussian channels case, the CF outerperforms the ANC, however, for the fading channel case, due to channel approximation errors, both strategies achieve almost same error performance. The gain of the CF over the ANC is only reported in terms of the average achievable rate.

Chapter 4: The Multi-Source Multi-Relay Channel We aim in this chapter to study the network codes design and the end-to-end performance of the ANC and CF in the real-valued Multi-Source Multi-Relay channel. In section 4.1 we describe the system model and assumptions. Sections 4.2 and 4.3 are dedicated respectively to the ANC and the CF schemes. Our novel results in this chapter include:

- A study of the end-to-end communication based on ANC and analysis of the conditions for successful decoding at the destination.
- A formulation of the optimization problem to search for the optimal network codes for the CF that allow to maximize the overall message rate at the destination.
- A proposition, in section 4.4, of algorithms to design efficient network codes for the CF based on a modified version of the Ficke-Pohst algorithm. Numerical results evaluating the performance of our approach are provided in section 4.5 and demonstrate the effectiveness of our method.
- A comparison of the end-to-end performance for the CF and the ANC. We show that the former achieves better performance than the latter.

Chapter 5: The Distributed MIMO Channel Inspired by the CF protocol, a new architecture of decoders in MIMO systems termed *Integer Forcing linear receivers* has been recently introduced in literature by Zhan *et al.* in [10–12]. The promising potential of this new architecture over traditional linear receivers such as the Zero-Forcing (ZF) and the Minimum Mean Square Error (MMSE) detector has been proved under a theoretical capacity achieving perspective. Motivated by the theoretical promising gains of the IF linear receivers, we aim in this chapter to go one step further towards practice by developing practical and efficient algorithms to design the IF receivers parameters and providing an evaluation of their error rate performance using finite length nested lattice coding schemes. As a starting point, we describe in section 5.1 the system model and assumptions. Section 5.2 is dedicated to review the basic optimal and suboptimal MIMO decoders studied in literature, namely the Maximum Likelihood (ML) decoder, linear receivers through the ZF and the MMSE and lattice reduction-aided linear receivers. Following, we study the Integer Forcing architecture. An overview on this new design is provided in section 5.3 and the main information theoretic results concerning their the achievable rate and Diversity Multiplexing Tradeoff (DMT) are overviewed. Our novel results for this chapter include:

- A development, in section 5.4, of novel algorithms to find the optimal IF receivers parameters based on the sum rate maximization criterion.
- A performance evaluation of our methods and comparison to the traditional MIMO decoders in section 5.5 using a finite length nested lattice coding scheme. Our numerical results demonstrate the effectiveness of our algorithms and confirm the outerpformance of the new IF architecture over the existing MIMO linear receivers.

Finally, the results of this work and some future research perspectives are summarized in a general conclusion.

Chapter 1

Network Coding

Networks are taking an ever-growing place in our day-to-day life. Different network systems exist today and are thoroughly used in all modes of communications. For example, beyond computer networks and the world wide web, wireless networks such as cellular networks, wireless ad-hoc networks (e.g., IEEE 802.11) and sensor networks have become ubiquitous. Routing mechanisms currently used in these network systems share mostly the same philosophy: data replication and forwarding. In such networks, data delivered by a *source* node is independently transmitted to the intended *destination* through a chain of *relay* nodes using a *store-and-forward* architecture. The role of an intermediate node is to clone the information flow it receives via an input link, and to forward a copy to the next node in the chain for subsequent transmission. Using this approach, independent data streams are processed in a separate way and apart from data replication, no additional processing is allowed at intermediate nodes.

In a communication scenario involving a single source-destination pair, the store-and-forward architecture is adequate to achieve the network capacity. Nevertheless, there is evidence that in a communication network accomodating multiple users and dealing with many source-destination pairs this strategy can be detrimental to the system performance. Indeed, the store-and-forward implies in this case to dedicate the whole network resources to process a single source packet at a time unit which evidently comes at the cost of more latency, more power consumption at the relay nodes and results in a data rate loss. Recently, a new coding perspective termed *Network Coding* has been introduced to enhance the network throughput and improve the system performance. This approach breaks from the traditional routing paradigm by observing that intermediate nodes in a communication network can be allowed to not only forward but also perform some coding operations and processing on the content of the incoming independent data flows. For example, at the network layer, this consists in executing binary operations on the independent bit streams (e.g., bitwise exclusive-OR), while at the physical layer, Network Coding is made at the signal space level and more general linear or non linear combinations can be made on the independent incoming electromagnetic waves.

Although Network Coding capitalizes on a very simple idea of mixing independent information flows, its generality and vast application potential have motivated an intensive research in several communities, most notably in the realm of Information and Coding Theory, Computer Science, wireless communications, cryptography and matrix theory. Several areas started to benefit from Network Coding and numerous applications continue to emerge ranging from distributed storage, cooperative communications, to network monitoring, management and security. Network Coding is expected to greatly deal with the future design of Information Technology systems and networking protocols.

This chapter is devoted to address the fundamentals of Network Coding and to give some insights into its applications, advantages and challenges. In section 1.1 we illustrate the basic concept of Network Coding and outline its most acknowledged benefits and challenges. Section 1.2 is dedicated to layout some applications of Network Coding. The main Network Coding theorem is provided in section 1.3. It establishes the necessary and sufficient condition on the design of maximum information achieving network codes in multicast networks. In the last section 1.4 we delve into the principle of Physical-Layer Network Coding (PLNC) and present a literature overview on this topic.

1.1 Network Coding: bene□ts and challenges

Network Coding is a new research field brought up in the turn of the millenium. Research works on this area date back to the paper of Yeung *et al.* [13] where the basic concept of Network Coding was first proposed for satellite communication networks. Later on, in 2000, Ahleswede *et al.* in [14] have completely developed the idea of Network Coding and showed its first potential gains over the traditional routing approach in a single source multicast transmission over a noiseless wireline network. Since this pioneering work, a vast portion of the literature [15–19] has been devoted to investigate the possible gains of this new concept as well as its applications [20] and limits [21].

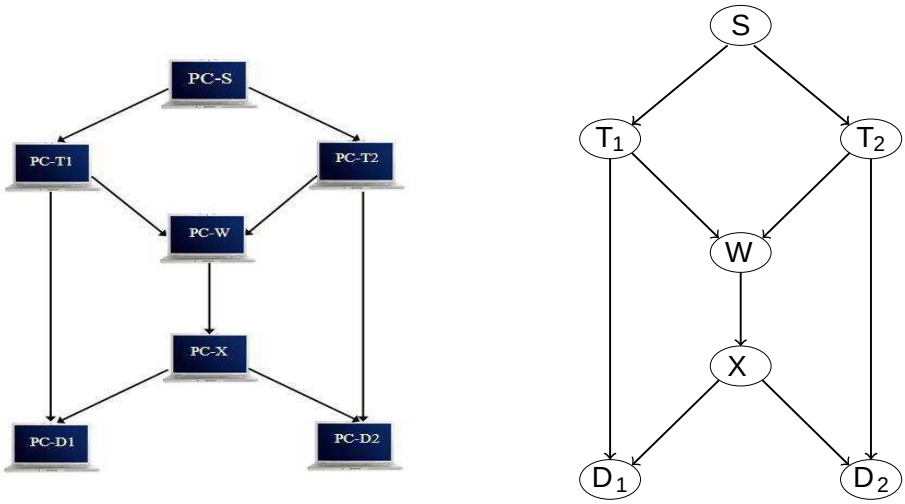
We will in the following depart from the multicast scenario in wireline networks to explain the concept of Network Coding, and through simple examples we will exhibit its most recognized benefits, mainly throughput increase, significant savings of wireless resources, and security. Then we proceed to discuss the main challenges that arise when dealing with the applicability of Network Coding in real systems, such as integration in present infrastructures and complexity. But before we embark in our illustration, we provide the following definitions for convenience.

De□nition 1.1. A *communication network* is represented by a finite directed graph G, where several edges from one node (vertice) to another can be assigned. A node without any incoming edges is termed a *source* node, while any other node is called a *sink* node. A directed edge from a node i to a node j is denoted as $(i;j)$ and is called a *channel*. The *capacity* of a direct communication from a node i to another node j is given by the multiplicity of independent channels between them. In practice, this graph model may represent a physical network, typically wireline networks (such as computer networks).

Definition 1.2. A communication network is said to be *cyclic* if it contains a directed cycle, otherwise, it is called *acyclic*.

Definition 1.3. A *multicast* transmission refers to the communication of a message or an information from a source node to a group of independent destinations simultaneously. In practice, the multicast scenario can correspond to a particular application such as a video-conference call.

Example 1.1. Consider the example of the network illustrated in Figure 1.1(a) composed of computers that are interconnected via several wires. The communication objective here is to transmit data from the computer PC-S to the computers PC-D1 and PC-D2. To this network we associate the directed acyclic graph depicted in Figure 1.1(b) in which vertices correspond to nodes and edges to channels. The node S is the source of the graph, nodes D1 and D2 are the final sink nodes (or destinations). All the direct transmissions in this network are of unit capacity.



(a) A wireline computers network. (b) Graph model.

Figure 1.1: Example of the butterfly communication network.

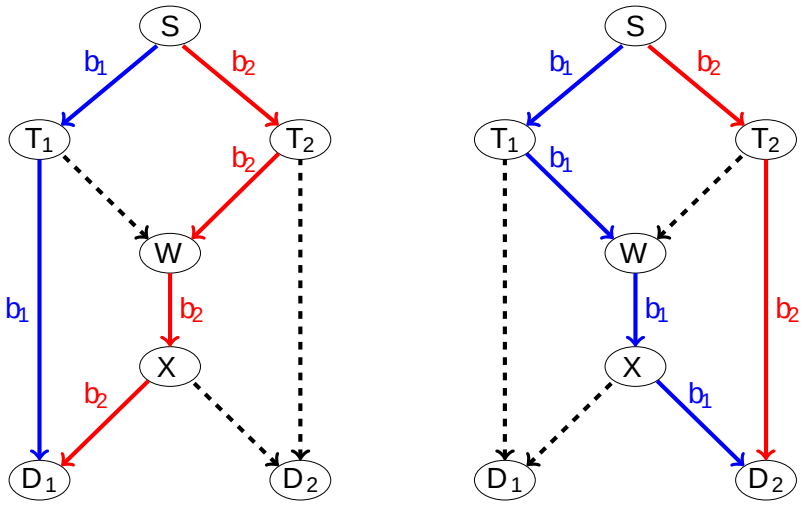
This network is a very famous example in the Network Coding literature known as the *butterfly network*.

1.1.1 Throughput increase

The first gain of Network Coding manifests in terms of throughput increase in a multicast transmission involving a single source [14] or multiple sources [16].

To demonstrate this benefit we consider a multicast scenario in the butterfly network described in Example 1.1. Assume that the source S emits two different information bits b_1 and b_2 and desires to send them simultaneously to the destination nodes D_1 and D_2.

If the network resources were allocated to the destination node D_1 only, it could receive the desired bits b_1 and b_2 from the paths $\{ST_1D_1\}$ and $\{ST_2WXD_1\}$ respectively as illustrated in Figure 1.2(a). The same scenario happens if the destination D_2 uses the network resources alone, it could get the bit b_1 via the path $\{ST_1WXD_2\}$ and b_2 through $\{ST_2D_2\}$ as shown in Figure 1.2(b).



(a) Routing to D_1. (b) Routing to D_2.

Figure 1.2: Multicast in the Butterfly network using traditional routing.

Now consider the case where the network resources are shared by both destinations D_1 and D_2. A first way to multicast the desired bits is to use the traditional store-and-forward routing approach. According to this strategy, the independent bit streams are kept separate in the network, and having in mind that every channel in the network can carry a single bit per time unit, the node W, receiving both bits at a same time slot, needs to make a decision to forward either b_1 or b_2. If the decision is taken in favor of the bit b_1, the destination D_1 receives b_1 and D_2 gets b_1 and b_2. Alternating the decision in favor of the bit b_2 during a second time unit allows to achieve the multicast objective and results in a multicast rate of 1:5 bits per time unit. This rate is the maximum possible under the store-and-forward strategy based on bit replication and forwarding.

A different way to perform the multicast over the butterfly network is based on Network Coding as illustrated in Figure 1.3. The basic idea is to enable the node W to mix the bits b_1 and b_2 and forward the resulting combination to the node X. Under this perspective, the node W performs the exclusive-OR bit $b_1 \oplus b_2$ and sends it over the channel $\{WX\}$. The node X replicates thus $b_1 \oplus b_2$ to reach both destinations. This way, destination D_1 receives the bit b_1 and $b_1 \oplus b_2$ from which it can decode the bit b_2. In like manner, destination D_2 can decode for the bit b_1 from the received bits b_2 and $b_1 \oplus b_2$. This Network Coding-based approach results in a multicast rate of 2 bits per time unit. It performs strictly better than the simple replication-based strategy by

permitting higher multicast rate, lower latency and improved network resources share between the destination nodes D_1 and D_2.

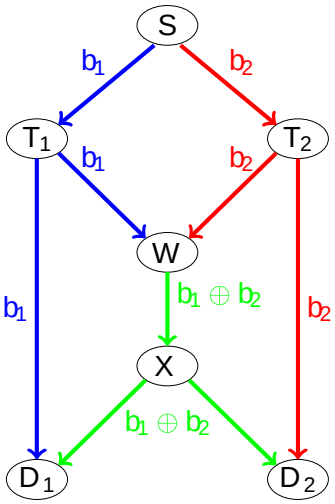


Figure 1.3: Network Coding in the butterfly network.

The exclusive-OR bit operation considered previously is a very basic and simple form of coding which can be generalized. For instance, linear Network Coding [15] in which output packets are linear combinations of the received independent packets, provides a linear framework that facilitates the coding and decoding operations and allows to achieve the optimal throughput when multicasting using polynomial time algorithms compared to the NP-hard conventional routing techniques.

The butterfly network example illustrates a fundamental result: *Network Coding allows to achieve the optimal data rate when multicasting over lossless wired networks.* This main finding was proved by Ahlswede *et al.* in [14] using information theoretic tools. This result opened the way to investigate throughput advantages of Network coding in other network types and traffic patterns. It was then proved that Network Coding offers a throughput benefit also in the case of unicast (transmission from a single source to a single destination node) in lossless wired networks [19] and in the case of broadcast [22] and multicast [23] in wireless networks.

1.1.2 Wireless Resources

Wireless networks face several problems that do not exist in their wireline counterparts. A first challenge is the resources allocation. Indeed, such networks are inherently multiuser environments. A difficult task is then to efficiently share the available resources in order to satisfy the users' different demands under the constraints of the wireless network. In addition, with the evolution of wireless applications and services, the number of connected users is continuously increasing. On the other hand, spectral resources are being scarce and are not sufficient to satisfy all the demands. Moreover, a relevant re-

quirement and crucial design parameter in wireless networks is energy efficiency. Indeed, compared to the wired case, wireless devices are power-limited and have to operate in an energy efficient way to maximize the network lifetime. For example, sensor nodes in a wireless sensor networks or user equipments in cellular networks are battery operated. Then, it is of fundamental importance to efficiently and reliably design communication protocols that require as low as possible processing and transmission powers.

All these problems result in performance loss and require more efficient routing mechanisms. We show through Example 1.2 that Network Coding can be a solution to the above listed drawbacks leading to improvements in the system performance.

Example 1.2. Consider the wireless communication network composed of two source nodes S_1 and S_2 and an intermediate node R, known as the Two-Way Relay Channel (TWRC). In this network, S_1 and S_2 send respectively the bits b_1 and b_2 and desire to exchange them. In absence of a direct link between the source nodes, the intermediate node R acts as a router (or relay).

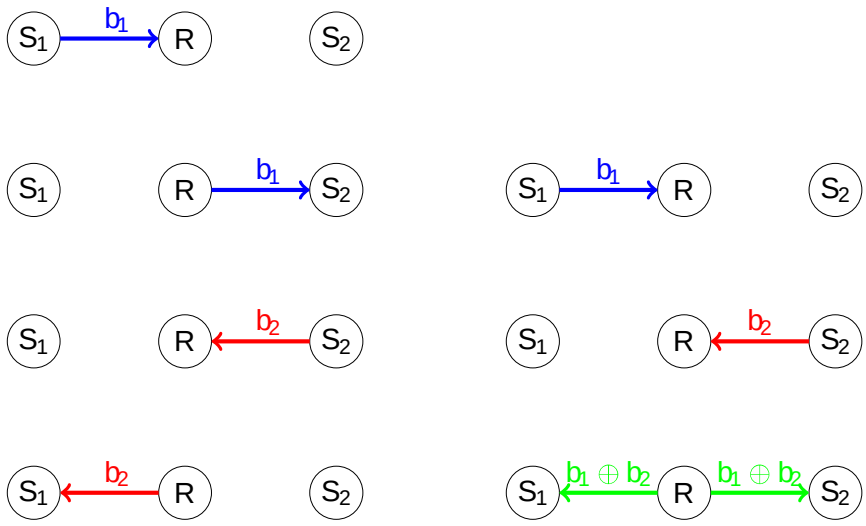


Figure 1.4: Bits exchange in the Two-Way Relay Channel.

Using the traditional store-and-forward method, the sources are able to exchange their bits within 4 time slots as illustrated in Figure 1.4(a): the relay node simply replicates the information bit it receives then sends a copy to the intended destination.

Now, consider a Network Coding-based relaying using the simple exclusive-OR bit coding depicted through Figure 1.4(b). We refer to this scheme as *straightforward Network Coding* [24]. In this scope, the relay node decodes each bit separately during the two first time slots, then computes the bit $b_1 \oplus b_2$ and brodcasts it to S_1 and S_2. Afterwards, based on the side information available at the sources, the latters decode the

received combination to recover the desired bit. For example, given that S_1 has a copy of the bit b_1, it can decode from $b_1 \oplus b_2$ the bit b_2. This way, only 3 time slots are necessary to perform the bits exchange.

The example of the Two-Way Relay Channel shows that Network Coding allows to perform a reliable transmission while realizing significant savings on the network resources: energy consumption is reduced (the relay R operates once rather than twice), batteries of wireless terminals are saved which results in a network lifetime enhancement, latency is reduced (bits exchange takes three time slots instead of four) and bandwidth is more efficiently used (the wireless medium is busy for shorter period).

1.1.3 Security

From a security point of view, Network Coding has both pros and bottelnecks depending on the application and the network scenario.

Looking at the security benefits, coding at intermediate nodes can offer a considerable protection against eavesdroppers. As an example, consider the butterfly network studied previously and assume that an eavesdropper manages to wiretap the channel $\{WX\}$. If the node W implements the traditional routing, the adversary can obtain either the bit b_1 or the bit b_2. However, when applying Network Coding, the eavesdropper, obtaining only the coded bit $b_1 \oplus b_2$, is unable to decode any of the source bits. Then it is clear that Network Coding allows a secure communication. More discussions about the impact of Network Coding on the security in wireline and wireless networks are addressed respectively in [19] and [25].

1.1.4 Complexity

It has been shown in various scenarios that Network Coding offers a complexity advantage over the conventional routing mechanism. This is the case of applications like gossip-based data dissemination [19] in wireless sensor networks, where low-complexity suboptimal solutions are required for practical reasons.

1.1.5 Challenges

The implementation of Network Coding in real systems requires to solve a plethora of practical challenges related to the network architecture and physical resources.

From a system design standpoint, the integration of Network Coding in already present infrastructures comes with the challenge to adapt the network architecture without radically changing the existing software and equipments. In the case of wireless networks for example, this necessitates to rethink of the protocol stack design to set up coding-aware layers, for instance the *medium access control* and *routing* layers.

From a physical resources perspective, the main challenge concerns the complexity cost. Indeed, in order to warranty the deployment of Network Coding particularly

for real-time and high throughput applications such as audio and video, the coding operations and decoding algorithms need to have linear complexity, consume low-power, meet the memory requirements imposed by the system devices and support the quality of service specifications.

1.2 Applications of Network Coding

We give in this section some insights into the most acknowledged applications of Network Coding in wireless networks, ad-hoc sensor networks and distributed storage systems.

1.2.1 Wireless Networks

Wireless networks such as cellular networks present a natural ground for Network Coding application due to the broadcast nature of the wireless medium that makes independent information flows naturally mix.

Motivated by the throughput benefits in the wireline networks, several works investigated the opportunities that Network Coding may offer in wireless networks and showed that this mechanism is beneficial in several ways. First of all, it allows to increase the network throughput by redundancy reduction and data compression [26]. The COPE architecture, the first practical deployment of Network Coding-based opportunistic algorithms, shows that Network Coding performs better than the traditional IEEE 802.11 routing mechanisms [27] and improves the network throughput. Moreover, Network Coding is an efficient error-control tool used to reduce the retransmission time. Its advantages over traditional Automatic-Repeat reQuest schemes are proved in terms of bandwidth efficiency [28].

The gains that can be offered using Network Coding in this particular type of networks depend on several practical issues such that packet arrival asynchronization, unbalanced traffic and channel fading and changing conditions. A reliable design of Network Coding-based wireless systems is conditioned by the careful consideration of these practical issues.

1.2.2 Ad-hoc Sensor Networks

With the declining costs of electronics and the emergence of computing technologies, ad-hoc sensor networks are being essential components of wireless monitoring systems used for example to supervise a civil engineering structure, or to ensure a remote medical assistance.

Network Coding can be used in several applications for ad-hoc sensor networks. A first addressed application is to use it as a routing mechanism to cope with the unreliability of the wireless medium and take advantage of the throughput increase and energy consumption reduction [29]. In addition, Network Coding can be used in ad-hoc sensor networks to enhance the efficiency of data collection [21]. Among the most

interesting encoding functions on the data measurements, the mean, mode, max and min functions were studied in [30]. Additionally, Network Coding can be used to improve the performance of sensor networks with untuned radios (where each sensor in the network transmits at a randomly selected frequency) [20].

In this Ph.D thesis, we were involved in the european project *Smart Management for Sustainable Human Environement* (SmartEN) [31] which aims to develop smart wireless sensor technologies for structural health monitoring (SHM). Our focus was related to the communication limitations in wireless sensor networks used for the SHM of bridges. In this application, a network of wireless sensor nodes is deployed to ensure a continuous bridge inspection in order to understand the performance of the bridge, detect its weaknesses and predict its remaining life time. Sensors gather physical properties under interest (e.g., the operating vibration of the bridge, wind power, humidity) and transmit their measurements to a remote control center via a gateway node in a multihop relay fashion. In this scope, we addressed the use of Network Coding to mitigate the interference problem occuring when the sensors broadcast their measurements. For more discussions about this specific appplication, we refer readers to our work [32] in which we provide an overview on SHM of bridges from civil and communication engineering perspectives and survey the main design challenges and communication requirements.

1.2.3 Distributed Storage

Due to their scalability, availability and performance, distributed storage mechanisms are revolutionizing the data storage and management techniques. Peer-to-Peer (P2P) distributed storage systems rely on a client-server architecture in which data files are splitted into several blocks and replicated through the network to create a redundancy that guarantees a reliable access to different blocks even if several nodes in the network are unavailable. Despite the fact that this data replication-based strategy is reliable, it is not efficient in terms of the required storage and maintenance bandwidth.

The first novel experience with a P2P system based on Network Coding was brought by Microsoft and is known as *Avalanche* [33]. It is shown that Network Coding copes with the above listed drawbacks by allowing the server to distribute a randomly coded version of the original information blocks. Similarly, peer nodes produce and send out linear combinations of the fragments they already hold. Network coding in this case allows to reduce the bandwidth use and offers more efficient and reliable access to data. More recent line of research combining replication and coding for distributed storage applications is proposed by Dimakis in [34].

1.3 The Main Network Coding Theorem

The main Network Coding theorem is about the existence of network codes that allow to achieve the maximum data flow in a multicast network.

In optimization theory, the maximum information that can be transported through

a given network is fundamentally characterized by the *max-flow min-cut Theorem*. In the following, we will first state this theorem, then we will expose the network multicast problem and the main Network Coding theorem.

1.3.1 The Max-Flow Min-Cut Theorem

Consider the network represented by the directed acyclic graph $G = (V; E)$ where V refers to the set of vertices (nodes) and $E \subseteq V \times V$ is the set of edges (channels).

Let $S \in V$ be a source node delivering information to a sink node $D \in V$ through different edges where the *capacity* of an edge $(i; j) \in E$ is represented by a non-negative real number R_{ij}. We provide the following definitions for convenience.

Definition 1.4. A *cut* between S and D is a set of vertices B such that $S \in B$ and $D \notin B$, i.e. if the cut B is removed, S and D become disconnected.

Definition 1.5. The *value* of a cut v is the sum of the capacities of the edges in the cut. Let $E_B = \{(i; j) \in E : i \in B; j \notin B\}$ be the set of edges in the cut. Then the value of a cut is given by $v = \sum_{(i;j)\in E_B} R_{ij}$. A *min-cut* is a cut with the minimal value.

The maximum information flow that the source can transmit to the intended destination in a given network is known as the *max-flow* and is given by the min-cut value according to the Max-Flow Min-Cut theorem stated in the following.

Theorem 1.1. *Consider a graph $G = (V; E)$ and a source node $S \in V$ sending information to a destination D. If B is a cut between S and D and E_B is the set of edges in the cut, then*

$$\textit{max-flow}(S \to D) = \min_{B} \sum_{(i;j)\in E_B} R_{ij} \tag{1.1}$$

If the cut value is equal to $\mathcal{R}$, then the source S can send information to D at a maximum rate $\mathcal{R}$. In the graph model, this is equivalent to the existence of exactly $\mathcal{R}$ edge-disjoint routes from S to D.

The Max-Flow Min-Cut theorem was proved in independent works, initially by Menger in [35] and later by Fulkerson [36] and Elias *et al.* in [37].

1.3.2 The Main Network Coding Theorem

Let S be the source node and $D = \{d_i; 1 \leq i \leq N\}$ be a set of N destination nodes. The node S is associated to an information source U that delivers $\mathcal{R}$ bits per unit time, i.e., the source sends out symbols $s_1; :::; s_R; s_i \in F_q$, of size q over the finite field F_q.

Consider now a multicast scenario where S transmits information simultaneously to the N destinations. The value of the min-cut between the source node and each one of the destinations is $\mathcal{R}$. We assume in addition that the transmissions over the network are synchronous, i.e. during every time unit, all nodes receive their inputs and send out their outputs simultaneously.

The multicast problem is to conceive a coding scheme which allows to send the source information bits to all destinations at the same rate $\mathcal{R}$.

Using information-theoretic tools, the main Network Coding theorem states that the max-flow rate for multicast is achievable provided that intermediate nodes perform linear processing on the received independent information flows using suitable linear network codes. By linear operations, we mean additions and multiplications over the finite field $\mathbb{F}_q$. This theorem is stated in the following.

Theorem 1.2. *Consider a directed graph $G = (V; E)$, a source node S producing $\mathcal{R}$ bits per unit time, and N destinations. Assume that the min-cut value from the source to each one of the destinations is $\mathcal{R}$. Then, with an appropriate selection of linear network code coefficients, there exists a multicast transmission scheme over a large enough finite field $\mathbb{F}_q$ that supports all destinations simultaneously at a rate equal to $\mathcal{R}$.*

Given that the value of the min-cut from the source to each destination is $\mathcal{R}$, if the network resources were allocated to a single destination, the latter can receive the original information at the rate $\mathcal{R}$. Nevertheless, in a multiuser environment, the network resources should be shared between the different destinations which leads to a rate loss. The Network Coding theorem states that if intermediate nodes operate a linear processing on their incoming information flows, each destination can receive the maximum rate as if it was using the network resources only by itself.

1.3.3 An Algebraic Statement of the Network Coding Theorem

The main Network Coding theorem states that linear network codes are sufficient to achieve the max-flow for multicast and shows the existence of such codes over finite field $\mathbb{F}_q$ of large enough dimension. We aim in the following to provide the equivalent algebraic formulation of this theorem.

Assume that P intermediate nodes in the network are engaged in moving the symbols $s_1; \ldots; s_R$ delivered by the source S to the N destinations.

In linear Network Coding, each node produces a new packet which is a linear combination of its input symbols. Each edge e in the network transports thus a linear function of the source symbols with finite field coefficients given by the vector $c(e) = [c_1(e) \ldots c_R(e)] \in \mathbb{F}_q^{1 \times R}$, called the *coding vector*. The information flow carried by edge e can be writen as:

$$p(e) = \sum_{i=1}^{R} c_i(e) s_i = [c_1(e)\ c_2(e) \ldots c_R(e)] \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_R \end{bmatrix}$$

Given that the linear combinations are operated in the finite field, the encoded packets belong to the same field and have the same size as the original source symbols.

After computing the linear combination, each node forwards the calculated packet along with the coding vector to the next hops. A similar output is produced at each node. At a destination node, this yields a system of linear equations from which the destination can decode the original source symbols. For example, consider a destination node D_j with $\mathcal{R}$ input edges and let p_i^j denote the packet flow carried by the i^{th} input edge. In addition, let A_j be the matrix whose rows correspond to the coding vectors associated with the input edges of the destination D_j. Then, in order to recover the original symbols, the destination D_j needs to solve the linear system given by:

$$\begin{bmatrix} p_1^j \\ p_2^j \\ \vdots \\ p_R^j \end{bmatrix} = A_j \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_R \end{bmatrix}$$

which imposes that the matrix A_j should be full rank. In order to enable all destination nodes to successfully decode the desired symbols, the network code vectors should be selected such that all the matrices A_j, $1 \leq j \leq N$ are full rank.

As an example, consider the network depicted in Figure 1.5 where the received equations at the destinations D_1 and D_2 are defined by the matrices A_1 and A_2 given by:

$$A_1 = \begin{bmatrix} 1 & 0 \\ \alpha_4 + \alpha_1\alpha_3 & \alpha_2\alpha_4 \end{bmatrix}; A_2 = \begin{bmatrix} \alpha_3 + \alpha_1\alpha_4 & \alpha_2\alpha_4 \\ 0 & 1 \end{bmatrix}$$

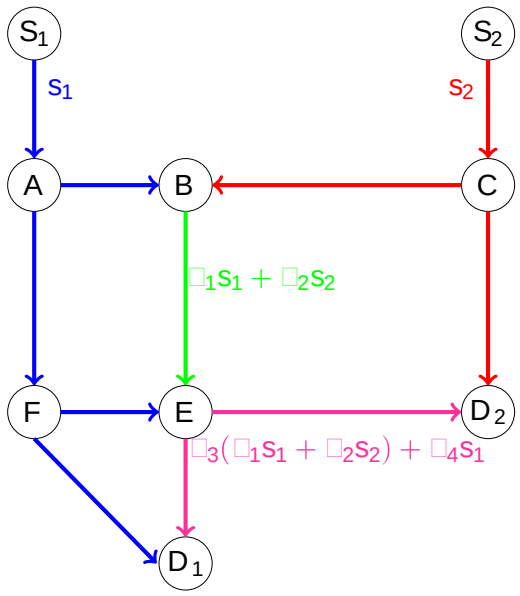


Figure 1.5: Example of linear Network Coding.

The multicast requirements imply for this scenario to select the coefficients $\square_k; 1 \leq k \leq 4$ such that the matrices A_1 and A_2 are full rank. For a general setting, this network coding design problem is expressed by the following theorem.

Theorem 1.3. *In linear Network Coding, there exists an enough large finite field* F_q *and values of the coding vectors coefficients* $\{\square_k\}$*, such that all the coefficients matrices* $A_j; 1 \leq j \leq N$ *at the destination nodes are full rank.*

This main Network Coding theorem was proved by Ahlswede *et al.* in [14] and Li *et al.* in [15]. It states the existence of linear network codes that allow to achieve the maximum multicast flow that we can transport over a given network. In particular, it specifies the necessary and sufficient conditions to multicast at a certain rate in this network. The challenging task that arises from this theorem is to design low-complexity encoding and decoding schemes combined with good performance and applicability in various network types (wireline, wireless, lossless and lossy) and traffic patterns (multicast, unicast and broadcast).

These design issues have been the subject of several research works. For example, the construction of algebraic network codes was investigated independently by Koetter and Medard in [38] and Jaggi *et al.* in [39]. The main limitation of such deterministic codes is the requirement of a complete knowledge of the network, which is not avilable in general. To remedy to this impediment, several contributions have been particularly interested in random linear Network Coding, where random coding operations are performed independently by each node with no global network-knowledge need. The asymptotic optimality of random coding is proved in [40] where authors show that random linear codes can achieve the max-flow min-cut capacity using large code lengths. Additionally, the effectiveness of random distributed linear coding is demonstrated in both lossless [27, 41] and lossy [42] networks, especially in wireless networks with correlated sources (typically sensor networks).

More discussions and an update on the literature on these issues are available on the *Network Coding Homepage* [43].

1.4 Physical-Layer Network Coding

1.4.1 Motivation

In practical wireless communication systems, multiple transmitters and receivers in the same geographical location share the same spectrum. This is essentially because the system designs are constrained by the physical resources, often limited and finite such as bandwidth, and the most economical system is the one that permits several users to efficiently share these available resources. This is the case for example of cellular mobile networks where the task of a base station is to serve many subscribers at the same time.

The main distinguishing features of such *multiuser* networks are the *broadcast* and *superposition*. Indeed, as signals of different users travel through the same air interface,

a signal sent from a transmitter is broadcast to all nearby users, consequently it reaches both the desired and unintended receivers. On the other hand, instantaneous transmissions by different users result in a superposition of signals at the receivers covered by the same transmission range. These two intrinsic properties of the wireless medium create a *multiuser interference* or *multiple access interference*. The design of a reliable wireless system is conditioned on a good understanding and management of this interference problem which can be detrimental to the system performance.

Multiple access interference is a widely investigated topic particularly in the realm of Information Theory. There are essentially two ways to resolve this problem. The first is a *single-user* approach and aims to provide an *orthogonal access* to the channel by allocating and maintaining separate channel resources to each user, either in time (e.g., Time Division Multiple Access), in frequency (e.g., Frequency Division Multiple Access) or in signal code (e.g., Code Division Multiple Access). Despite the fact that this single-user approach guarantees interference-free transmissions, there remain drawbacks, essentially a reduced spectral efficiency.

Lessons learned from multiuser Information Theory [1] show that orthogonal multiple access is suboptimal. The best way to optimally share the spectral resources in a multiuser system is to harness the interference and instead of avoiding it, we should consider it as a useful information to serve the decoding process of the desired signal. This is the philosophy of the second *multiuser detection* [2] approach which deals with the design of multiple access codes and interference cancellation schemes. From an information-theoretic perspective, these techniques allow to increase the spectral efficiency [3], however, their design complexity make their implementation in practical settings a challenging task.

Recently, *Physical-Layer Network Coding* (PLNC) has been introduced as a valuable solution to improve the way of interference management in wireless networks including multiple access channels. PLNC turns the broadcast and superposition properties of the wireless media into boosting characteristics to achieve higher end-to-end transmission rates. The aim of this new framework is to allow simultaneous transmissions from distinct wireless agents in the network and enable intermediate nodes to decode and forward functions of the interfering signals. PLNC ressembles to the straightforward Network Coding with two main differences: *i)* PLNC is performed at the physical layer of the protocol stack, i.e. decoded functions at a given node are performed at the signal space, while Network Coding as described in the previous schemes is executed at the network layer and applies on the bit space, *ii)* using PLNC, intermediate nodes decode and forward a function of the original signals without decoding each one of them separately in contrast to straightforward Network Coding which mixes the already decoded bits.

PLNC is a new tool to cope with the interference problem always considered tough. It has grabbed particular attention in multi-hop relay-based networks, where relay nodes do not need to decode original signals separately. PLNC in this case can bring promising performance improvement provided that the following conditions are satisfied [4]:

1. A relay node must be able to appropriately transform the superimposed interfering signals into intrepretable output functions to be forwarded to the intended destinations.

2. A destination must be able to decode the desired information from the network coded functions it receives from the relays.

In order to better explain how does PLNC work, we provide in the following an illustrative example.

1.4.2 Illustrative example

Consider the Two-Way Relay Channel described in Example 1.2 where two source nodes S_1 and S_2 exchange their bits with the assistance of an intermediate relay node.

Common to the store-and-forward and the straightforward Network Coding strategies studied previously is the interference avoidance. Indeed superposition of the source bits at the relay was prevented by time scheduling: S_1 and S_2 had to transmit their data in two different time slots. The best throughput performance was obtained with straightforward Network Coding which makes the bits exchange last three time slots, while it lasts four time slots using the traditional routing approach.

Now, equipped with the basics of PLNC, we will investigate a simple relaying scheme in which the source nodes are authorized to send their data to the relay at the same time slot as illustrated in Figure 1.6. We assume that the sources modulate their bits using a Quadrature Phase-Shift Keying (QPSK) modulation such that the source S_i sends at a given time symbol $s_i(t)$ such that

$$s_i(t) = \mathrm{Re}[(\square_i + j\,\square_i)\exp(j\,!\,t)] = \square_i \cos(!\,t) - \square_i \sin(!\,t) \tag{1.2}$$

where $\square_i \in \{-1;1\}$ and $\square_i \in \{-1;1\}$ represent the corresponding modulated QPSK bits with the mapping that associates $\square_i = 1$ to the bit "0" and $\square_i = -1$ to the bit "1"; similar mapping is assumed in the quadrature phase where $\square_i$ is used. In addition we assume that the source signals arrive at the relay with a symbol and carrier phase synchronization and with the same amplitude and phase. Noise-free links from the sources to the relay are also assumed for ease of presentation.

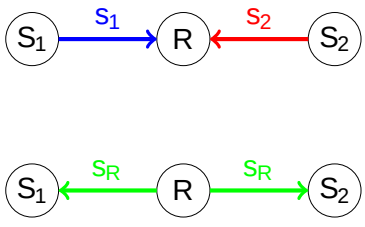


Figure 1.6: Physical-Layer Network Coding in the TWRC.

Looking at the physical layer, when the sources transmit their signals, the relay observes during one symbol period the addition of the original bandpass signals as:

$$\begin{aligned} y_R(t) &= s_1(t) + s_2(t) \\ &= [\square_1 \cos(! t) - \square_1 \sin(! t)] + [\square_2 \cos(! t) - \square_2 \sin(! t)] \\ &= (\square_1 + \square_2) \cos(! t) - (\square_1 + \square_2) \sin(! t) \end{aligned} \tag{1.3}$$

where $y_R^{(I)} = \square_1 + \square_2$ and $y_R^{(Q)} = \square_1 + \square_2$ are respectively the corresponding base-band in-phase (I) and quadrature (Q) components.

Due to the superposition of the original signals, the relay is not able to separate out each of them. Alternatively, the relay will help the data relaying by performing Network Coding at the source signals already combined. The key ingredient of this scheme is to *map* the received signal $y_R(t)$ into an interpretable signal $s_R(t)$ that will be broadcast to S_1 and S_2 during a second phase of the communication scheme. The mapping presented here was proposed by Zhang *et al.* in [4]. Accordingly, the relay produces the following signal:

$$s_R(t) = \square_1 \oplus \square_2 + j\ (\square_1 \oplus \square_2) = \square_R + j\ \square_R \tag{1.4}$$

where $\square_R = \square_1 \oplus \square_2$ and $\square_R = \square_1 \oplus \square_2$ are obtained respectively from $y_R^{(I)}$ and $y_R^{(Q)}$ according to the modulation/demodulation mapping defined in the Table. 1.1 and applicable to both in-phase and quadrature components.

Table 1.1: PLNC mapping for the in-phase signal components

Symbol from S_1: $\square_1$	Symbol from S_2: $\square_2$	Received combination at the relay $y_R^{(I)} = \square_1 + \square_2$	Mapping to the symbol at the relay $\square_R$
1	1	2	1
1	-1	0	-1
-1	1	0	-1
-1	-1	-2	1

In other words, this PLNC mapping consists in the following demodulation scheme:

$$\square_R = \begin{cases} -1 & \text{if } y_R^{(I)} = 0 \\ 1 & \text{if } y_R^{(I)} = -2 \text{ or } 2 \end{cases}; \quad \square_R = \begin{cases} -1 & \text{if } y_R^{(Q)} = 0 \\ 1 & \text{if } y_R^{(Q)} = -2 \text{ or } 2 \end{cases} \tag{1.5}$$

After deriving the correspoding values of $\square_R$ and $\square_R$, the relay broadcasts the signal s_R to the nodes S_1 and S_2, which given the side information, can recover the desired information bits.

Although the described PLNC scheme here is based on a very simple modulation/demodulation mapping, it demonstrates how, thanks to Physical-Layer Network Coding, it is possible to convey the same amount of information in the TWRC within only two time slots.

1.4.3 Literature Overview

Works on Physical-Layer Network Coding were first developed in 2006 by different research groups: Zhang, Liew and Lam in [4], Popovski and Yomo in [5, 6].

In [4], authors show that Network Coding at the physical layer allows to increase the throughput over the TWRC with Additive White Gaussian Noise (AWGN) links by 100%. Authors use the scheme described in the previous paragraph and provide extended mappings suitable to more general linear network topologies. First discussions on the implications of Physical-Layer Network Coding on the processing and tasks of the upper layers like the medium access control and routing were proposed also in this work.

Popovski and Yomo introduced in [5, 6] new PLNC strategies for the TWRC inspired by the very known Amplify-and-Forward (AF) and Decode-and-Forward (DF) relaying techniques. In the AF-based approach, the relay node amplifies and broadcasts the received combination of the source signals. This strategy was later studied by Katti *et al.* in [44] and implemented in software defined radios under the name of *Analog Network Coding* (ANC). This technique is advantegeous in the sense that it is easy to implement, however, particularly in noisy networks, its main drawback is the noise accumulation given that the relay node amplifies in this case the received combination without cleaning up the noise. The DF-based strategy is known as *Denoise-and-Forward* (DoF) and in contrast to the ANC, it is a noiseless PLNC technique. The idea behind DoF is to find the optimal mapping that transforms the received noisy signal to a noise-free combination of the source signals. This strategy was investigated for both the AWGN and Rayleigh fading TWRC, and subsequent works were developed in this topic in [45, 46] with a particular focus on the design of optimized modulation and mapping schemes.

Since these works, PLNC has been developed in different directions and applied in various commmunication network scenarios ranging from the Multiple Access Relay Channel (MARC) [47, 48], the Multi-Sources Relay Channel (MSRC) [8] to the TWRC [49–51] with a particular focus on the last topology.

From a physical layer point of view, Network Coding can operate in conjunction to physical layer techniques essentially source coding and channel coding [7]. The need to design a joint source-network coding scheme arises particularly in networks where the sources are correlated such as sensor networks. In general settings where the sources are uncorrelated, integrating channel coding and Network Coding has attracted a particular research attention and several works have been developed in this context. We distinguish in literature two main frameworks that deal with channel coding joint to Physical-Layer Network Coding: a lattice coding-based framework where channel coding is done using lattice codes, and a linear-coding framework with channel coding schemes that do not result in lattice structures.

The first framework dates back to the works of Nazer and Gastpar [52–55] which were further developed in [8, 56, 57] with the introduction of a new PLNC strategy termed the

Compute-and-Forward (CF). In this scheme, source nodes encode their messages into lattice codewords. The role of a relay node observing the output of a multiple access channel is to decode and forward an integer linear combination of the original codewords. The lattice structure guarantees that this combination is also a codeword from the same coding lattice used at the sources. Due to its promising potential, the CF has received a significant attention and has been extensively studied in the last few years. Among many other issues, the analysis of the achievable degrees of freedom [58] and the construction of efficient decoding algorithms [59] have been addressed. Later, the original work on the CF was followed by several contributions based on lattice coding and distinct decoding approaches. Among the important works, Narayanan *et al.* in [60, 61] developed a PLNC scheme based on spherical lattice coding and minimum angle decoding, and Feng *et al.* in [62] proposed an algebraic approach as an extention of the primary work of Nazer and Gastpar and provided a codes design based on lattice partitions and module theory .

For what concerns the second framework, it includes a variety of contributions based on linear coding schemes that do not result in a lattice structure. The most acknowledged contributions are brought by [63] with *Repeat Accumulate* coding scheme, by [64] with a *multilevel coding* scheme, by [65] with a *low density parity check codes* and [66] with *convolutional codes.*

Most of the above cited contributions are in the form of information-theoretic results. In particular, a vast portion of works focused on the information exchange rate over the TWRC with AWGN channels and demonstrated that PLNC mappings such that the CF outperform the traditional relaying strategies and can achieve rates within 1=2 bit of the cut-set upper bound which is asymptotically optimal [60, 67–69]. In order to make real wireless systems take advantage of these exciting findings and promising gains, several research works are currently focused on the implementation challenges of PLNC strategies which consist mainly in the synchronization and channel estimation issues. To the best of our knowledge, these practical constraints were first addressed in [70] where a PLNC-based prototype for bi-directional relaying in the TWRC is successfully implemented in a software defined radio platform.

Common to the previously mentioned works is that the network nodes are equipped with a single antenna. However, it is worth mentioning that PLNC has been also developed for networks with multiple antennas. In this case, PLNC can provide two favors: enhance the system throughput or/and turn down the processing complexity. A variety of PLNC schemes have been developed to combine these advantages with the diversity gain brought by the MIMO channel. Among the proposed solutions are [71] with a linear detection-based scheme, [72] with ML decoding-based XOR mapping, and [73] with Analog Network Coding. Besides, PLNC has been used in conjuction to Space-Time codes such as the Alamouti code in [74] and structured codes using lattices in [75].

1.5 Conclusion

This chapter was devoted to introduce the concept of Network Coding. Through simple examples, we gave insights into its benefits, challenges and most famous applications. In addition, we outlined the main Network Coding theorem and its equivalent algebraic formulation. The last part of the chapter was dedicated to explain the principle of Physical-Layer Network Coding and expose the most notable research works achieved in this context.

In this work, we are interested in PLNC joint to lattice-based channel coding. In particular, we aim to design and analyze the performance of the CF, the ANC and the DoF strategies in different multiuser network configurations. As a starting point, we dedicate the next chapter to study the Compute-and-Forward protocol. After reviewing the original work of Nazer and Gastpar, we provide criteria to design optimal network code functions for the CF and propose novel decoding algorithms which outperform the standard decoding scheme for the CF. Following chapters are devoted to the end-to-end implementation and performance analysis of the above mentioned PLNC strategies in the TWRC, the Multi-Source Multi-Relay Channel and the Multiple Input Multiple Output (MIMO) channel.

Chapter 2

The Compute-and-Forward protocol

The last few years have witnessed the emergence of a very promising linear Physical-Layer Network Coding protocol termed *Compute-and-Forward*. Introduced by Nazer and Gastpar in [8], this scheme allows to harness the multiple access interference resulting from the broadcast and superposition properties of the wireless channel to achieve higher transmission rates. This new framework is applicable to any network configuration accomodating source nodes, relays and destinations that communicate through linear additive white Gaussian noise channels. In a nutshell, source nodes deliver messages from a finite field, map them onto codewords from a lattice and transmit them accross the network. The role of a relay node observing the output of a multiple access channel is to take advantage of the noisy supersposition of these lattice points to decode a *linear noiseless integer* combination of them. The computed function is then forwarded to the next relays for subsequent transmissions. Upon receiving enough linear combinations, the end destination in the network can ideally recover the original source messages. The CF protocol owes its success to the potential algebraic and structural properties of lattice codes as well as to their capacity achieving capabilities.

Since the pioneering work of Nazer and Gastpar and thanks to the promised merit of this protocol, the CF has emerged as an essential tool in several of the most relevant and challenging issues in Network Information Theory, including interference alignment [76–78], secrecy [79] and relay-based communications for which various network scenarios have been treated such as the TWRC [76], the Multi-Way Relay Channel [80], the Multiple Access Relay Channel [81, 82], and distributed MIMO channels [10, 11].

Our objective in this chapter is twofold: review the CF protocol as proposed in the original work of Nazer and Gastpar and expose our novel results related to the design of network codes and practical decoding algorithms. For this purpose, we will consider the basic multiple access channel model composed of N sources and a receiver. As

a starting point, we describe in section 2.1 the nested lattice coding which is the key ingredient of the CF encoding and decoding schemes. In section 2.2 we outline the decoding steps in the case of real-valued channels. This channel model will be used as a building block for complex-valued channels addressed in section 2.3. The main information-theoretic results regarding the achievable rate will be presented in section 2.4. After these overviewing sections, our results are organized as follows: in section 2.5, we investigate an optimal solution to design network codes for the CF. By maximizing the achievable rate at the receiver, we show that this solution is related to a shortest vector problem. In section 2.6 we introduce the *ergodic rate* for the CF operating in fast fading channels and derive a novel lower bound using the complex LLL reduction. The same tool is used in section 2.7 to derive a novel upper bound on the outage probability in the case of slow fading channels. Besides, in sections 2.8 and section 2.9 we develop practical decoding algorithms for the CF in the case of Gaussian and fading channels respectively. Numerical results evaluating the performance of the proposed algorithms are also provided. A concluding section summarizes the outcomes of the present chapter.

2.1 Nested Lattice codes

2.1.1 Motivation

The problem of multicasting over the Gaussian butterfly network including both point-to-point and multiple access channels is behind the Compute-and-Forward protocol [55]. The challenge was to find good linear error correcting codes that allow to take advantage of the interference provided by the multiple access channels to reproduce functions of original sources and therefore generate higher transmission rates.

Inspired by the lattice construction developed by Erez, Litsyn and Zamir in [83], nested lattice codes have been adopted by Nazer and Gastpar who showed that this lattice design allows to increase the multicast rate in the studied network. These codes satisfy the linear structure requirement, allow to achieve the AWGN channel capacity, and more interestingly, they have salient structural properties well suited to the natural function performed by multiple access channels. The added value of these codes is twofold: allow to take advantage of the interference to design more efficient network codes and protect against the channel noise (see Appendix 5.A for the basic definitions in lattices).

The considered nested lattice design $\Lambda = (\Lambda_F; \Lambda_C)$ involves a fine lattice Λ_F and a coarse lattice Λ_C of fundamental voronoi region $\mathcal{V}_C$. The nested lattice codebook is $\mathcal{C}_\square = \{\mathcal{V}_C \cap \Lambda_F\}$ composed of the Fine lattice points that fall within the fundamental voronoi region of the coarse lattice. These codes are constructed using linear codes over finite fields F_p of prime size p. The idea behind this design is to conserve linearity while mapping from the finite field to the real field. This means that messages from the finite field can be mapped onto the codebook and back without losing linearity. Mathematically, this is expressed by the existence of a bijective mapping $\square$ from the

finite field F_p to the nested lattice code $\mathcal{C}_\square = \{\mathcal{V}_C \cap \Lambda_F\}$ such that:

$$\begin{aligned}
&\square : F_p \to \mathcal{C}_\square = \{\mathcal{V}_C \cap \Lambda_F\} \\
&\text{Encoding} : \square(w_i) = x_i \\
&\text{Decoding} : \square^{-1}([a_1 x_1 + \cdots + a_M x_M] \bmod \Lambda_C) = q_1 w_1 \oplus \cdots \oplus q_M x_M \\
&\qquad \text{for} \quad a_i \in Z; q_i \in F_p; i = 1; \ldots; M :
\end{aligned}$$

where the finite field coefficients q_i are related to the integer coefficients a_i by:

$$q_i = g^{-1}([a_i] \bmod p)\,; \; i = 1; \ldots; M \tag{2.1}$$

and $g : F_p \to \{0; \ldots; p-1\}$ denotes the one-to-one mapping that associates each element in the finite field to an integer in Z_+.

The existence of asymptotically-good high-dimensional nested lattice codes and the corresponding bijective mapping $\square$ was proved in [8].

2.1.2 Construction of nested lattice codes

Several lattice constructions are studied in literature particularly for lattice dimensions up to 29 [84]. The most known are Construction A for dimensions up to 15, Construction B for dimensions 8 to 24, and Construction C for lattice dimensions that are power of 2. For what concerns the CF, the fine lattice is generated by shifting a linear code using Construction A. Consider a linear code C over F_p and let $L \in F_p^{k \times n}$ be its generator matrix. Construction A consists of the following steps [83]:

1. Construct the discrete codebook $\mathcal{C} = \{uL; u \in F_p^k\}$ from the code C.
2. Construct the lattice $\Lambda^\square$ by projecting the codebook into reals using the embedding function $g(:)$, dividing by p and copying over Z^n: $\Lambda^\square = p^{-1} g(\mathcal{C}) + Z^n$
3. Construct the Fine lattice by rotating $\Lambda^\square$ by the generator matrix of the coarse lattice M_C, $\Lambda_F = M_C \Lambda^\square$

Any lattice generated using Construction A is of full rank [85].

In practical settings, the field Z/pZ also noted Z_p (which is a ring and for p prime, a field) can be used to generate low-complexity (in the encoding and decoding senses) fine lattice codes. This field represents the set of integers from 0 to $p-1$ with integer addition and multiplication modulo p. The corresponding mapping g is equal to the identity function.

A coarse lattice with low-complexity encoding and decoding operations can be just a scaled version of Z^n by the size of the field p, i.e., $\Lambda_C = pZ^n$.

Example 2.1. We give here an example of a nested lattice code. We consider the field Z_{11} with addition and multiplication modulo 11. Additionally, we consider $k = 1$ and

$n = 2$. In order to build the fine lattice, we consider the linear code C over Z_{11}^2 of a generator matrix $G = [2\ 3]$. The codebook corresponding to step 1. in Construction A is then $\mathcal{C} = \{u{:}[2\ 3] \bmod(11); u \in Z_{11}^2\}$. Given that $g = id$ in this case, the fine lattice is the set of points in $\Lambda_F = \mathcal{C} + 11Z_{11}^2$. For the coarse lattice we choose $\Lambda_C = 11Z^2$. The nested lattice code is then given by $\Lambda = \{\mathcal{V}_C \cap \Lambda_F\}$. We illustrate in Figure 2.1 a portion of the fine and coarse lattices as well as the nested lattice code points. In this graph, green bold points correspond to the code $\mathcal{C}$, small blue points are the fine lattice points, the coarse lattice points are the red crosses. Voronoi regions of the coarse lattice are drawn in dashed red lines. Elements of the nested lattice code are the points of the fine lattice inside the fundamental voronoi region of the coarse lattice.

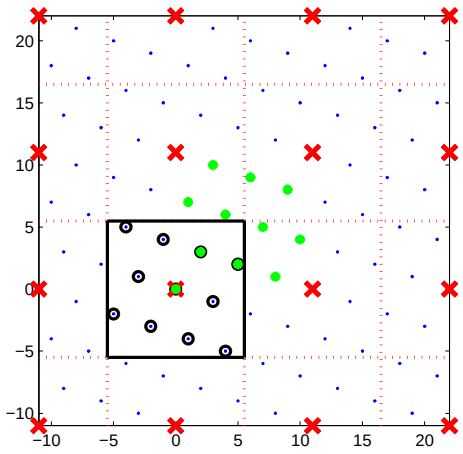


Figure 2.1: Example of a nested lattice codebook in Z^2.

Equipped with the nested lattice coding scheme, we describe in the next section the CF protocol. We will consider a nested lattice design $\Lambda = (\Lambda_F; \Lambda_C)$ involving a fine lattice Λ_F and coarse lattice Λ_C.

2.2 Compute-and-Forward in real-valued Channels

As a starting point, we consider the case of a real-valued fading Multiple Access Channel (MAC) composed of N sources $S_1; :::; S_N$ and a receiver R as depicted in Figure 2.2.

Each source delivers a message that can be represented as a string of bits. The information vector produced by each source $S_i; i = 1; :::; N$ is represented by a length-k finite field message $w_i \in F_p^k$ drawn independently and uniformally from the set of possible values.

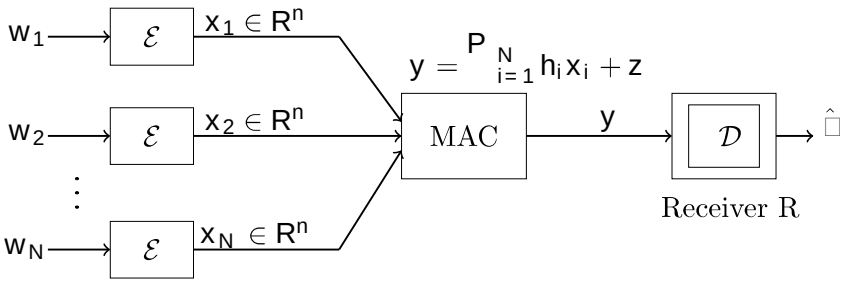


Figure 2.2: Generic Gaussian real-valued MAC.

2.2.1 Encoding scheme

Each source is equipped with a same encoder $\mathcal{E}$ that maps the finite field message w_i to a real-valued $n-$dimensional lattice codeword x_i:

$$\begin{aligned} \mathcal{E} : \mathbb{F}_p^k &\longrightarrow \mathbb{R}^n \\ w_i &\longmapsto x_i \end{aligned} \tag{2.2}$$

More precisely, the encoders implement the same mapping □ defined previously to map the messages onto codewords from the same nested lattice Λ. The lattice codewords are subject to a symmetric power constraint given by:

$$\frac{1}{n}\mathbb{E}\left[\| x_i \|^2\right] \leq P \tag{2.3}$$

for $P > 0$. The fine lattice corresponds to the coding lattice from which are carved the codewords while the coarse lattice acts to satisfy the power constraint P. The codewords are assumed to be independent and uniformally distributed over Λ.

The message rate r, defined as the length of the message in bits normalized by the number of the channel uses, is the same for all sources and is equal to:

$$r = \frac{1}{n}\log|\Lambda_F \cap \mathcal{V}_C| = \frac{1}{n}\log p^k = \frac{k}{n}\log p \tag{2.4}$$

2.2.2 Decoding scheme

After encoding their messages, the sources transmit the codewords $x_1, \ldots, x_N$ simultaneously across the channel. The receiver observes therefore a noisy linear combination of the sent codewords as the ouput of a multiple access channel in the form:

$$y = \sum_{i=1}^{N} h_i x_i + z \tag{2.5}$$

where $h_i \in \mathbb{R}$ denotes the fading channel from the source S_i to the receiver and $z \in \mathbb{R}^n$ denotes the additive white Gaussian noise of zero-mean and variance □², $z \sim \mathcal{N}(0, \square^2 I_n)$.

Let $h = [h_1; :::; h_N]^t$ denote the vector of the channel coefficients to the receiver. In this section we assume fixed channel vector, fast fading and slow fading channels will be addressed in sections 2.6 and 2.7 respectively. We assume also that channel state information (CSI), i.e., the knowledge of h, is available only at the receiver, sources need only to know their target message rates. Additionally, let $\square = \frac{P}{\square^2}$ denote the Signal-to-Noise Ratio (SNR).

When receiving the noisy superposition of the original codewords, the receiver attempts to decode a noiseless integer linear combination $\square$ in the form:

$$\square = \left[\sum_{i=1}^{N} a_i x_i \right] \mod \Lambda_C \tag{2.6}$$

where the coefficients $a_i \in Z; i = 1; :::; N$ are chosen by the receiver and form the network code vector $a = [a_1; :::; a_N]^t \in Z^N$.

Using Physical-Layer Network Coding, the receiver does not need to perform a joint Maximum Likelihood (ML) decoding to decode each codeword separately $\hat{x}_1; :::; \hat{x}_N$. Instead, it attempts to decode $\square$ as a regular codeword from the same nested lattice Λ. This is because the linear structure of the lattice guarantees that any integer combination of lattice codewords is also a lattice codeword.

By mapping the desired combination $\square$ to the finite field using $\square^{\square 1}$, the decoding objective is equivalent to recover a linear combination u of the finite field source messages in the form:

$$u = \square^{\square 1}(\square) = \sum_{i=1}^{N} q_i w_i \tag{2.7}$$

where the coefficients $q_i \in F_p$ are given by $q_i = g^{\square 1}([a_i] \bmod p)$.

The relay is equipped with a decoder $\mathcal{D} : R^n \to \Lambda$, that recovers an estimate $\hat{\square}$ of $\square$. A decoding error occurs if $\hat{\square} \neq \square$ and the desired equation with a coefficient vector a is decoded with an average probability of error $\square$if

$$\begin{aligned} \hat{\square} &\overset{4}{=} \mathcal{D}(y) \\ \Pr\left[\hat{\square} \neq \square\right] &< \square \end{aligned} \tag{2.8}$$

A computation rate $\mathcal{R}(h; a)$ is said to be achievable if for any $\square > 0$ and n large enough, there exist an encoder $\mathcal{E}$ and a decoder $\mathcal{D}$, such that for any channel fading vector $h \in R^N$ and network code vector $a \in Z^N$, the receiver can recover the desired equation with an average probability of error $\square$as long as the source message rate r satisfies:

$$r < \mathcal{R}(h; a) \tag{2.9}$$

Remark 2.2. Step 2 in the decoding process is based on minimum distance decoding through the lattice quantizer Q_{Λ_F}. The input of this quantizer can be seen as a single user additive noise channel with desired vector t and noise $z_{eq} = \sum_{i=1}^{N} (\alpha h_i - a_i) x_i + \alpha z$. The problem here is that the effective noise z_{eq} includes a non-Gaussian part, resulting from the channel quantization, that makes minimum distance decoding in this case suboptimal compared to ML decoding, and for the Gaussian channel case, suboptimal compared to *maximum a posteriori* (MAP) decoding. In order to make the effective noise independent of the original signals, Nazer and Gastpar propose in [67] to add to the encoded codewords some randomness using dither vectors that are known at both the sources and the receiver. The sources transmit dithered version of their mapped vectors. Using this tool, authors show in [67] that the density of the effective noise can be upper bounded by the density of an i.i.d Gaussian vector given by:

$$\sigma_{e\alpha}^2 = \alpha^2 \sigma^2 + P \parallel \alpha h - a \parallel^2 \tag{2.11}$$

Although this theoretical tool solves the dependence between the effective noise and the desired signal, it does not give practical insights particularly into the performance gap between the minimum distance decoder and the optimal decoders (ML decoding for the fading channels and MAP decoding for the Gaussian channels). In this chapter, we dedicate sections 2.8 and 2.9 to study the optimal decoders for the CF in the Gaussian and fading channels respectively. We develop novel practical decoding algorithms for the MAP and ML criteria and provide numerical results evaluating and comparing the performance of our algorithms to the conventional minimum distance decoder.

Remark 2.3. As most of the Physical-Layer Network Coding strategies, the CF capitalizes on the assumption that the transmitted codewords arrive at the receiver at the same time. In this work, we make this synchronism assumption and refer readers to a recent line of research [89] where the impact of symbol-asynchronism on the CF is investigated.

2.3 Compute-and-forward in Complex-valued channels

In narrowband communications, the wireless channel is uniquely complex-valued. Then, in order to warranty the deployment in practical wireless networks, it is of fundamental importance to extend the CF to the case of complex-valued channels. This is the goal of this section.

As far as the encoding part is concerned, each source in this case generates two finite field messages of identical lengths k: $w_i^{(Re)}$ and $w_i^{(Im)}$. Equipped with the encoder $\mathcal{E}$ and the mapping α, the sources encode each one of the resulting messages onto $n-$dimensional codewords from the same nested lattice code Λ such that:

$$x_i^{(Re)} = \alpha \left[w_i^{(Re)} \right] \quad ; \quad x_i^{(Im)} = \alpha \left[w_i^{(Im)} \right] \tag{2.12}$$

The channel input from the source s_i is then the codeword $x_i \in \mathbb{C}^n$ given by:

$$x_i = x_i^{(Re)} + j\, x_i^{(Im)} \tag{2.13}$$

And the message rate in this case is $r = \frac{2k}{n} \log p$.

The baseband representation of the multiple access channel output is:

$$y = \sum_{i=1}^{N} h_i x_i + z \tag{2.14}$$

where in this case the channel fading vector $h \in \mathbb{C}^N$ and $z \in \mathbb{C}^n$ is drawn i.i.d according to $\mathcal{CN}\left(0; \sigma^2 I_n\right)$.

The decoder in this case treats the real and imaginary parts of the channel output separately. These two components are given by:

$$y^{(Re)} = \sum_{i=1}^{N} \left[h_i^{(Re)} x_i^{(Re)} - h_i^{(Im)} x_i^{(Im)} \right] + z^{(Re)} \tag{2.15}$$

$$y^{(Im)} = \sum_{i=1}^{N} \left[h_i^{(Im)} x_i^{(Re)} + h_i^{(Re)} x_i^{(Im)} \right] + z^{(Im)} \tag{2.16}$$

where $h_i^{(Re)}; h_i^{(Im)}; z^{(Re)}; z^{(Im)}$ correspond to the real and imaginary parts of the channel vector and the noise vector respectively.

Looking at the real and imaginary parts separately, they can be seen as the outputs of real-valued multiple access channels with $2N$ sources. Given these two real signals independently, the receiver selects a scaling parameter α and a coefficient vector $a \in \{Z + j\, Z\}^N$ and implements separately the steps described previously for the real-valued channel case. From $y^{(Re)}$ the receiver decodes the combination

$$\left[\alpha^{(Re)}\right] = \left[a_i^{(Re)} x_i^{(Re)} - a_i^{(Im)} x_i^{(Im)} \right] \bmod \Lambda_C \tag{2.17}$$

and from $y^{(Im)}$ the decoder attempts to decode

$$\left[\alpha^{(Im)}\right] = \left[a_i^{(Im)} x_i^{(Re)} + a_i^{(Re)} x_i^{(Im)} \right] \bmod \Lambda_C \tag{2.18}$$

Finally, by mapping these equations back to the finite field using φ^{-1}, the receiver can recover the real and imaginary parts of a linear combination u of the source messages as:

$$u^{(Re)} = \left[\sum_{i=1}^{N} \left[q_i^{(Re)} w_i^{(Re)} \oplus \left[-q_i^{(Im)} \right] w_i^{(Im)} \right] \right] \tag{2.19}$$

$$u^{(Im)} = \left[\sum_{i=1}^{N} \left[q_i^{(Im)} w_i^{(Re)} \oplus q_i^{(Re)} w_i^{(Im)} \right] \right] \tag{2.20}$$

where for $i = 1;:::;N$ the finite field coefficients satisfy

$$q_i^{(Re)} = g^{-1}\left[\sum_{i=1}^{N} a_i^{(Re)} h_i\right] \bmod p \tag{2.21}$$

$$q_i^{(Im)} = g^{-1}\left[\sum_{i=1}^{N} a_i^{(Im)} h_i\right] \bmod p \tag{2.22}$$

We summarize in Figure 2.4 the decoding steps for the complex-valued channel case.

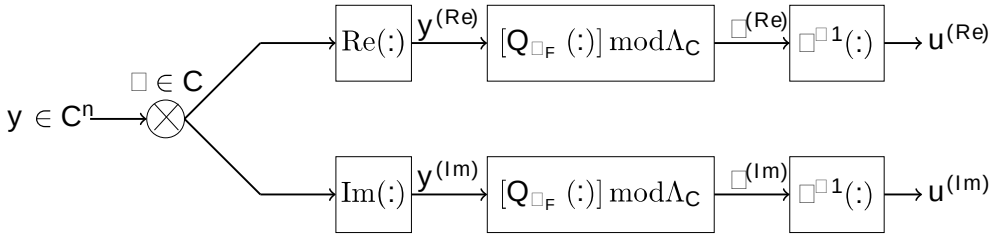


Figure 2.4: Block diagram of the Compute-and-Forward in complex-valued MACs.

2.4 Computation Rate

The fundamental contribution brought by the CF framework is information theoretic and amounts to enabling higher transmission rates that go beyond those permitted by earlier relaying strategies existing in literature. Nazer and Gastpar showed in [8] that a successful computation of a desired lattice equation is possible as soon as the message rates are less than a computation rate R_{comp} defined in Theorem 2.1.

Theorem 2.1. *The computation rate is defined as the number of bits of the linear function that are reliably computed per channel use. A receiver observing an ouput of a complex-valued multiple access channel given by the channel vector $h \in \mathbb{C}^N$, can recover any set of non-zero equations with coefficients vector $a \in \{\mathbb{Z} + j\mathbb{Z}\}^N$ if the message rates are less than the computation rate R_{comp} given by:*

$$R_{comp} = \log^+\left(\frac{P}{\alpha^2 e_\alpha}\right) = \log^+\left(\frac{1}{|\alpha|^2 + \alpha\|\alpha h - a\|^2}\right) \tag{2.23}$$

for $\alpha \in \mathbb{C}$ *and* $\log^+(x) = \max(\log(x); 0)$

For complex-valued channels, the vectors $a; ja$ and $a^?$ lead to the same computation rate. For real valued channels, the computation rate is multiplied by a factor $\frac{1}{2}$.

The computation rate is different from the usual sense of rates. Once achieved, it means that the desired lattice equation can be reliably decoded. However, this single equation does not allow to decode the original messages separately. This task requires a full rank set of equations which can be originated from a successive Compute-and-Forward performed at a single receiver as long as the message rates are satisfied, or from

a distributed computation at different receivers (different relays in a general network configuration) that have access to the same original messages.

Besides, it is worth to mention that the rate expression is the result of an asymptotic optimization problem based on the premise of the existence of high dimensional nested lattices that have good properties in terms of coding and shaping gains. For instance, the fine lattice is assumed to be AWGN good and the coarse lattice is required to be good for covering, quantization and AWGN. Although this construction promises high transmission rates, the complexity of such good lattice codes makes these theoretical gains hard to achieve in practical settings.

Remark 2.4. The computation rate is derived by approximating the effective noise term by an i.i.d Gaussian random vector of variance σ^2_{e} as mentioned in Remark.2.2. If the components of the effective noise term were white Gaussian and independent, the minimum distance decoding would be equivalent to ML decoding and the achievable rate would be equal to $R_{comp;ML}$:

$$R_{comp;ML} = \log \left(1 + \frac{P}{|a|^2 + \alpha \|\alpha h - a\|^2} \right) \tag{2.24}$$

Remark 2.5. The computation rate depends on the scaling factor used to reduce the approximation gap of the real (complex) channel vector by integer vector. The highest the value of this parameter, the lowest the approximation error and thus the highest the achievable rates. On the other hand, the scaling introduces an additional penalty by amplifying the noise, which results in performance degradation. There is a tradeoff then between noise enhancement and integer approximation of reals. This tradeoff is known as the *Diophantine Approximation Tradeoff*.

2.5 Selection of receiver parameters

The two fundamental parameters of the decoding process are the scaling factor and the network code vector a. The receiver is free to choose them, however the choice needs to be carefully made since it greatly impacts the performance.

In literature, there are essentially two optimization criteria to find the optimal values of the receiver parameters. The first criterion, proposed by Nazer and Gastpar in [67], is based on the maximization of the computation rate according to:

$$(\alpha; a)_{opt} = \underset{(\alpha \in \mathbb{C}^?; a \in \mathbb{Z}[i]^N \setminus 0)}{\operatorname{argmax}} \log^+ \left(\frac{P}{|\alpha|^2 + \alpha \|\alpha h - a\|^2} \right) \tag{2.25}$$

The second criterion, proposed by Feng *et al.* in [62], assumes hypercube shaping lattice designs and asks for the minimization of the probability of decoding error under minimum

distance decoding according to:

$$(\square;\mathsf{a})_{\mathsf{opt}} = \underset{(\square 2\,\mathsf{C}^{?};\mathsf{a}2\,\mathsf{Z}[\mathsf{i}]^{\mathsf{N}}\ \mathsf{n}0)}{\operatorname{argmin}} \mathsf{K}\,\exp\left[-\frac{\mathsf{d}^2}{4\square^2\,(|\ \square\ |^2+\square\|\ \square\mathsf{h}-\mathsf{a}\ \|^2)}\right] \tag{2.26}$$

where d stands for the minimum inter-coset distance of the nested lattice design, and K denotes the number of shortest vectors in the set $\Lambda_{\mathsf{F}} - \Lambda_{\mathsf{C}}$.

According to these two optimization criteria, the optimal value of $\square$ corresponds to the Minimum Mean Square Error (MMSE) factor expressed by (Proof in Appendix 5.B.1):

$$\square_{\mathsf{opt}} = \frac{\square\mathsf{h}^{?}\mathsf{a}}{1+\square\|\ \mathsf{h}\ \|^2} \tag{2.27}$$

By replacing in the rate expression the scaling factor by the optimal MMSE parameter we get (see Appendix 5.B.2):

$$\mathsf{R}_{\mathsf{comp}}(\mathsf{h};\mathsf{a}) = \log^{+}\left[\|\mathsf{a}\|^2 - \frac{\square|\ \mathsf{h}^{?}\mathsf{a}\ |^2}{1+\square\|\ \mathsf{h}\ \|^2}\right]^{\square_{\square 1}!} \tag{2.28}$$

Then the optimal network code vector satisfies:

$$\mathsf{a}_{\mathsf{opt}} = \underset{\mathsf{a}2\,\mathsf{Z}[\mathsf{i}]^{\mathsf{N}}\ \mathsf{n}0}{\operatorname{argmax}} \log^{+}\left[\|\mathsf{a}\|^2 - \frac{\square|\ \mathsf{h}^{?}\mathsf{a}\ |^2}{1+\square\|\ \mathsf{h}\ \|^2}\right]^{\square_{\square 1}!} \tag{2.29}$$

Remark 2.6. The computation rate can be equivalently written as

$$\mathsf{R}_{\mathsf{comp}} = \log\left[1+\square\|\ \mathsf{h}\ \|^2\right]^{\square} - \log\left[\|\ \mathsf{a}\ \|^2+\square\{\|\ \mathsf{h}\ \|^2\|\ \mathsf{a}\ \|^2-|\ \mathsf{h}^{?}\mathsf{a}\ |^2\}\right]^{\square} \tag{2.30}$$

The first part represents the rate of a MAC with channel vector h and the second term is the loss in rate due to the channel quantization [58]. The maximization of the computation rate imposes a minimization of the loss in rate term. To do that, we should align a to h which corresponds to increase $\|\ \mathsf{a}\ \|^2$. Authors in [58] show that this diophantine approximation problem and the loss in rate term are behind the limited achievable degrees of freedom for the CF which are lower than 2 for any network configuration involving N sources and N receivers (relays).

According to the optimization problem in (2.29), the optimal network code vector that allows simultaneously to maximize the computation rate and minimize the error probability is a solution of the integer optimization problem stated in the following theorem.

Theorem 2.2. *For a given channel coefficient vector* $\mathsf{h} \in \mathsf{C}^{\mathsf{N}}$*, the optimal non-zero network code vector* $\mathsf{a} \in \{\mathsf{Z}+\mathsf{j}\,\mathsf{Z}\}^{\mathsf{N}}$ *is solution of the integer minimization problem as:*

$$\mathsf{a}_{\mathsf{opt}} = \underset{\mathsf{a}\neq 0}{\operatorname{argmin}}\,\{\mathsf{a}^{?}\mathsf{G}\,\mathsf{a}\} \tag{2.31}$$

where

$$G = I_N - \frac{\square}{1 + \square \| h \|^2} H \tag{2.32}$$

$H = [H_{ij}]; H_{ij} = h_i h_j^?; 1 \leq i; j \leq N$ *and* G *is a Hermitian definite positive matrix of dimension* N.

Proof. The minimization problem in (2.31) follows from the fact that maximizing the computation rate (and minimizing the decoding error probability) are equivalent to minimize $Q(a)$ given by:

$$\begin{aligned} Q(a) &= \|a\|^2 - \frac{\square | h^? a |^2}{1 + \square \| h \|^2} \\ &= a^? a - \frac{\square}{1 + \square \| h \|^2} \sum_{i;j} h_i^? h_j a_i^? a_j \\ &= a^? a - \frac{\square}{1 + \square \| h \|^2} \left(\sum_{i=1}^{N} h_i^? a_i \right) \left(\sum_{j=1}^{N} h_j a_j^? \right) \\ &= a^? a - \frac{\square}{1 + \square \| h \|^2} a^? h h^? a \\ &= a^? \left(I - \frac{\square}{1 + \square \| h \|^2} H \right) a = a^? G a \end{aligned} \tag{2.33}$$

Now, in order to prove that the matrix G is definite positive, we look at its eigenvalues. According to the expression of this matrix, for $\square_i; i = 1; \ldots; N$ eigenvalues of H, the eigenvalues of G are equal to $\square_i = 1 - \frac{\square}{1 + \square k h k^2} \square_i$. Given that H admits $\square_1 = \| h \|^2; \square_i = 0; i = 2; \ldots; N$, G has N strictly positive eigenvalues: $\square_1 = 1 - \frac{\square k h k^2}{1 + \square k h k^2}; \square_i = 1; i = 2; \ldots; N$. Then it is definite positive. □

The optimization problem in Theorem 2.2 has no closed-form. Nevertheless, using lattice theory tools, we show in Proposition 2.1 that solving for the optimal network code vector reduces to solve a shortest vector problem in a lattice. This result was also independently proved by Feng *et al.* in [62] and Osmane in his PhD dissertation [90].

Proposition 2.1. *The optimal network code vector* a *corresponds to the coordinates of the shortest vector in the lattice* Λ_G *of Gram matrix* G.

Proof. Given that G is definite positive, it can be considered as a Gram matrix of a lattice Λ_G. Let the full rank matrix M denote a generator matrix of the underlying lattice, then we can write: $G = M^? M$. The quadratic form Q can then equivalently be written as:

$$Q(a) = a^? M^? M a = \| M a \|^2 \tag{2.34}$$

The minimization of Q requires then to find the lattice vector with the shortest length. The coordinates of this shortest vector correspond to the non-zero vector a in $\{Z + j Z\}^N$ (in Z^N for the real-valued channel case). □

In practice, there are essentially two ways to solve this shortest vector problem. The first approach is suboptimal and relies on lattice reduction techniques [91] such as the complex LLL (C-LLL) reduction [92] (or LLL reduction [93] for real lattices). Given a generator matrix M of the lattice Λ_{G}, the C-LLL reduction computes a reduced matrix $\mathsf{M}_{\mathsf{red}} = \mathsf{M}\,\mathsf{U}$ where U is a unimodular matrix. The first column of the reduced matrix corresponds to the shortest vector u of the underlying lattice and satisfies:

$$\| \mathsf{u} \| \leq 2^{\frac{N-1}{4}} \left(\mathsf{vol}\left(\Lambda_{\mathsf{G}}\right)\right)^{\frac{1}{N}} \tag{2.35}$$

where $\mathsf{vol}\left(\Lambda_{\mathsf{G}}\right) = \sqrt{\det\left(\mathsf{G}\right)} = \sqrt{\prod_{i=1}^{N} \lambda_i} = \sqrt{1+\alpha \| \mathsf{h} \|^2}^{N-1=2}$ is the volume of the lattice Λ_{G}.

The second approach is optimal and is based on using the Fincke-Pohst algorithm [9] to search for the integer vector that minimizes the quadratic form Q. In order to reduce the computation complexity, the search space can be limited to the coefficients vector that satisfies:

$$\| \mathsf{a} \|^2 \leq 1 + \alpha \| \mathsf{h} \|^2 \tag{2.36}$$

since the computation rate is equal to zero otherwise [67].

Remark 2.7. The optimal MMSE scaling parameter as well as the network code vector require the knowledge of the channel state information at the receiver which is a commonly considered assumption. Readers can find in [94] a recent work where authors propose a blind CF without the CSI requirement. Additionally, it is of fundamental importance to stress that the considered criteria to find the optimal network code vector are based on optimization problems at the receiver. However, the receiver in practice is a relay node taking part of a communication scenario within a global network configuration. Consequently, these local optimization criteria need to be adapted to take into account the network level constraints.

2.6 Fast fading channels: Ergodic Rate

So far, we considered that the channel gains are fixed during the whole transmission period. In this section we draw our attention to the case of fast fading channels. We define for this channel model the ergodic rate for the CF and derive a novel lower bound by the means of the complex LLL reduction.

2.6.1 Definition

In fast fading channels, transmission is achieved through a number of independently faded channel realizations. The rate in this case is obtained by averaging over all channel realizations.

Let $R(h;a)$ be the maximum computation rate achievable for fixed network code vector a using the optimal MMSE scaling:

$$R(h;a) \stackrel{4}{=} \max_{a \in Z[i]^N \setminus 0} \log^+ \left(\|a\|^2 - \frac{|h^* a|^2}{1+\|h\|^2} \right)^{-1} \tag{2.37}$$

We define then the *ergodic rate* [95] as:

Definition 2.1. The ergodic rate R_e for the Compute-and-Forward is defined as:

$$R_e \stackrel{4}{=} E_h\{R(h;a)\} \tag{2.38}$$

where the mathematical expectation averages over the realizations of the channel vector.

2.6.2 Lower Bound

When the complex LLL reduction is used to find the optimal network code vector a, we obtain a lower bound on the ergodic rate as stated in Theorem 2.3.

Theorem 2.3. *The ergodic rate of the Compute-and-Forward is lower bounded by:*

$$R_e \geq \frac{1}{N} E_h(C_h) - c \tag{2.39}$$

when the complex LLL reduction is used to find the optimal network code vector a. $C_h = \log\left(1+\|h\|^2\right)$ *is the instantenous capacity of the multiple access channel (MISO) with fading channel vector* h, *and* $c = \frac{N-1}{2}$. *An upper bound on the ergodic capacity for* $h \sim \mathcal{CN}(0; I_N)$ *is given by [95]:*

$$E(C_h) \stackrel{4}{=} \int_0^1 \log(1+t) e^{-t} \frac{t^N}{N!} dt \tag{2.40}$$

Proof. By definition, the ergodic rate is given by

$$\begin{aligned} R_e &= E_h(R(h;a)) \\ &= E_h\left[\max_{a \in Z[i]^N \setminus 0} \log^+ \left(\|a\|^2 - \frac{|h^* a|^2}{1+\|h\|^2} \right)^{-1} \right] \\ &= E_h\left[\max_{a \in Z[i]^N \setminus 0} \log^+ \left(a^* G a \right)^{-1} \right] \\ &= E_h\left[\log^+ \left(\min_{a \in Z[i]^N \setminus 0} (a^* G a) \right)^{-1} \right] \end{aligned} \tag{2.41}$$

Let a_{opt} denote the optimal network code vector that allows to maximize $R(h;a)$ in (2.37), then we have:

$$\min_{a \in Z[i]^N \setminus 0} a^* G a = \|M a_{opt}\|^2 \tag{2.42}$$

When $\mathbf{a}_{opt}$ is obtained using the complex LLL reduction, the upper bound on the shortest vector provided in (2.35) allows to write:

$$\| \mathbf{M}\,\mathbf{a}_{opt} \|^2 \leq 2^{\frac{N-1}{2}} \left(\frac{1}{1+|\mathbf{h}|^2} \right)^{\frac{1}{N}} \tag{2.43}$$

Then we get

$$\begin{aligned} R_e &\geq E_{\mathbf{h}} \left[\log^+ \left(\frac{\left(1+|\mathbf{h}|^2\right)^{1/N}}{2^{\frac{N-1}{2}}} \right) \right] \\ &\geq E_{\mathbf{h}} \left[\frac{1}{N} \log^+ \left(1+|\mathbf{h}|^2\right) - \frac{N-1}{2} \right] \\ &= \frac{1}{N} E_{\mathbf{h}} \left[\log^+ \left(1+|\mathbf{h}|^2\right) \right] - \frac{N-1}{2} \end{aligned} \tag{2.44}$$

The proof follows by considering $c = \frac{N-1}{2}$ and $C_{\mathbf{h}} = \log\left(1+|\mathbf{h}|^2\right)$. □

2.7 Slow fading channels: Outage Probability Analysis

The Compute-and-Forward protocol is also applicable to slow fading channels. In this case, the channel vector $\mathbf{h}$ is generated according to some probability distribution and then remains constant during the whole transmission time. For this channel model, we define the rate outage probability and derive a novel upper bound using the complex LLL reduction.

2.7.1 Definition

Consider a multiple access channel where N sources operate with a computation rate R^0. We define the *rate outage probability* as,

Definition 2.2. A rate outage event occurs if the maximum achievable rate R_{comp} is lower than the fixed rate R^0. The *rate outage probability* is then given by

$$P_{out}\left(R^0\right) = \Pr\left[R_{comp}(\mathbf{h};\mathbf{a}) < R^0 \right] \tag{2.45}$$

2.7.2 Upper Bound

When the complex LLL reduction is used to find the optimal network code vector, the outage probability of the Compute-and-Forward is upper bounded as stated Theorem 2.4.

Theorem 2.4. *For a system operating with a computation rate R^0, the rate outage probability of the Compute-and-Forward is upper bounded by,*

$$P_{out}\left(R^0\right) \leq \Pr\left[1+|\mathbf{h}|^2 < 2^{N\left(R^0+c\right)} \right] \tag{2.46}$$

when the complex LLL reduction is used to solve for the optimal network code vector. The upper bound is similar to the outage probability of a multiple access channel under a target rate $N\ R^0 + c$.

Proof. The maximum achievable rate $R(h;a)$ given in (2.37) is equivalent to:

$$\begin{aligned} R(h;a) &= \log^+ \left(\min_{a \in Z[i]^N \setminus 0} (a^? G a) \right)^{-1} \\ &= \log^+ \left(d_{min}^2 \right) \end{aligned}$$

where d_{min} stands for the minimal distance of the lattice Λ_G and corresponds to the length of the shortest vector in this lattice. The rate outage probability is equivalent to:

$$\begin{aligned} P_{out}(R^0) &= \Pr\left[\log^+ \left(d_{min}^2 \right) < R^0 \right] \\ &= \Pr\left[d_{min} > 2^{-R^0/2} \right] \end{aligned} \tag{2.47}$$

When the complex-LLL reduction is used to solve for the shortest vector problem, the minimal distance is upper bounded according to (2.43). Then we get:

$$\begin{aligned} P_{out}(R^0) &\leq \Pr\left[2^{\frac{N-1}{4}} \left(1 + \|h\|^2 \right)^{-1/2N} > 2^{-R^0/2} \right] \\ &= \Pr\left[\left(1 + \|h\|^2 \right)^{-1/2N} < 2^{R^0/2 + \frac{N-1}{4}} \right] \\ &= \Pr\left[1 + \|h\|^2 < 2^{N(R^0 + c)} \right] \end{aligned} \tag{2.48}$$

this ends the proof.

□

2.8 Optimal Decoders for the CF: Gaussian channels

The conventional decoding scheme for the CF consists of two main parts: decoding a point from the fine lattice through the scaling operation and minimum distance decoding described in steps 1 and 2 in section 2.2.2, and a modulo operation with respect to the coarse lattice (step 3 in the decoding scheme). The problem is that in presence of the non-Gaussian effective noise as indicated in Remark.2.2, minimum distance decoding is suboptimal. Optimal decoders for the CF are the MAP decoder in the case of Gaussian channels, and the ML decoder in the case of fading channels.

Although the conventional decoder is proved to be optimal in asymptotic regime and for high dimensional lattices, its performance gap to the optimal decoders is not known particularly in practical settings using finite-dimensional lattices. We aim in this section to study the optimal MAP decoding in the Gaussian MAC. We dedicate the next section to the analysis of the ML decoding in the fading MAC. For ease of presentation, we will consider the case of real-valued channels. Extension to the complex-valued channels case follows using the same techniques at the real and imaginary parts of the channel output separately.

2.8.1 System Model

Consider a real $n-$dimensional nested lattice design $\Lambda = (\Lambda_F; \Lambda_C)$ and let M denote a generator matrix of the fine lattice Λ_F.

The system we are interested in within this section is the Gaussian multiple access channel composed of N sources and a receiver. Transmitted vectors are $n-$dimensional nested lattice codewords $x_1; :::; x_N$ carved from Λ according to the power constraint $\frac{1}{n}E[\| x_i \|^2] \leq P; i = 1; :::; N$. The channel output is given by:

$$y = \sum_{i=1}^{N} x_i + z \tag{2.49}$$

where $z \in \mathbb{R}^n$ stands for the AWGN generated i.i.d according to a normal distribution $\mathcal{N}(0; \sigma^2 I_n)$. From this observed vector, the receiver attempts to decode a noiseless sum of the original codewords in the form:

$$\square = \left[\sum_{i=1}^{N} x_i \right] \mod \Lambda_C \tag{2.50}$$

We are interested in the following in decoding $\square_s = \sum_{i=1}^{N} x_i$. Given that modulo-lattice operation is done separately, it does not impact the decoding error. We define then the error probability at the receiver as

$$P_e = \Pr[\hat{\square}_s \neq \square_s] \tag{2.51}$$

Let Λ_s denote the *sum codebook* which is the set of all $\square_s = \sum_{i=1}^{N} x_i$. Given the linear structure of the coding lattice, Λ_s will be a subset of the fine lattice Λ_F restricted to a *sum shaping region* $\mathcal{S}_s$ such that all sum codewords $\square_s$ fall within this region. In addition, given that Λ_s is obtained through a superposition of the originally transmitted codewords, its distribution is no more uniform.

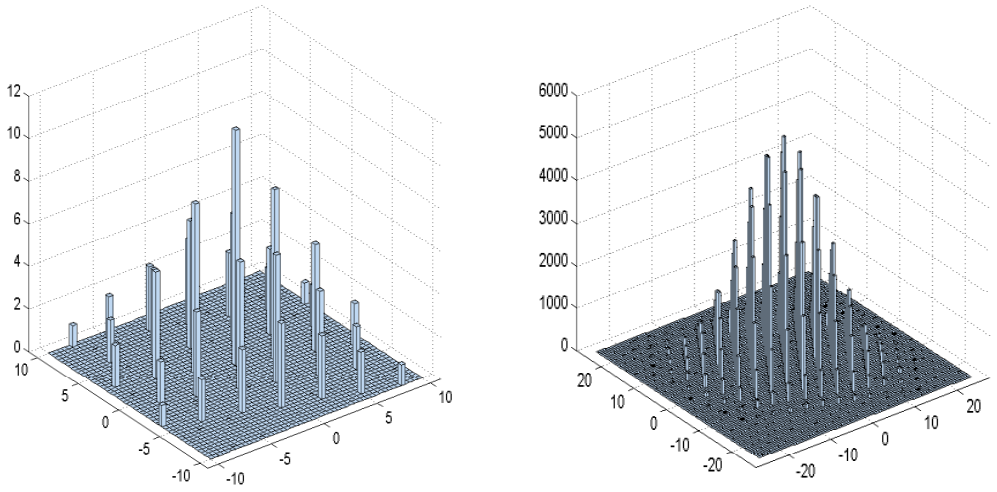
Using the conventional CF decoder, the receiver decodes $\square_s = \sum_{i=1}^{N} x_i$ using an MMSE scaling followed by minimum distance decoding to the nearest point in the fine lattice. This method has two fundamental limitations: it ignores the shaping region of the sum codewords $\mathcal{S}_s$, and does not take into account the non-uniform distribution of the sum codebook Λ_s. Our goal in this section is to analyze the optimal decoding approach that takes into account these two constraints and develop practical decoding algorithms.

2.8.2 Discrete Gaussian Distribution of the Sum Codebook

The original codewords are drawn uniformally and independently from the nested lattice code, they are modeled by uniform random variables of zero-mean ($\square_x = 0$) and variance $\square_x^2 = \frac{1}{n}E[\| x_i \|^2] \leq P$ for $i = 1; :::; N$.

Consider now the sum codewords $\square_s = \sum_{i=1}^{N} x_i$ obtained through the superposition of the vectors sent by the sources. Given the uniform distribution of the original codewords, The *Central Limit Theorem* states that $\square_s$ is a random variable of mean $\square_s = N\,\square_x = 0$ and variance $\square_s^2 = N\,\square_x^2$. Particularly, for increasing number of sources N, the sum codewords converge to a normal distribution $\mathcal{N}(\square_s; \square_s^2 I_n)$.

In order to be able to use this result to approximate the vectors $\square_s$ by random Gaussian variables, we need in addition to take into consideration the fact that the sum codewords are discrete and correspond to lattice points. For this purpose we introduce the lattice Gaussian distributions. This tool arises in several problems in coding theory [96], mathematics [97] and cryptography [98].



(a) Histogram for N = 2. (b) Histogram for N = 5.

Figure 2.5: Histogram of the codebook induced by the sum of codewords.

Let $f_{\square_s}(x)$ denote the Gaussian distribution of variance $\square_s^2$ centered at the zero vector such that for $\square_s > 0$ and all $x \in \mathbb{R}^n$:

$$f_{\square_s}(x) = \frac{1}{\sqrt{2\square\square_s}\,\square_n} e^{\square \frac{kxk^2}{2\square_s^2}} \tag{2.52}$$

Consider also the Λ_F-periodic function $f_{\square_s}(\Lambda_F)$ defined by:

$$f_{\square_s}(\Lambda_F) = \sum_{\square_s 2\,\square_F} f_{\square_s}(\square_s) = \frac{1}{\sqrt{2\square\square_s}\,\square_n} \sum_{\square_s 2\,\square_F} e^{\square \frac{k\square_s k^2}{2\square_s^2}} \tag{2.53}$$

Then the sum codewords can be modeled by the discrete Gaussian distributions over Λ_F

centered at the zero vector according to:

$$p(\square_s) = \frac{f_{\square_s}(\square_s)}{f_{\square_s}(\Lambda_F)} \tag{2.54}$$

We illustrate in Figure 2.5 two examples of the statistical distribution of the sum codebook resulting from the superposition of $N = 2$ and $N = 5$ codewords carved from the nested lattice code described in Example 2.1. These examples show that the discrete Gaussian distribution fits our settings. As a proof of concept, we will show by numerical results that this Gaussian model is well justified in the context of lattice network coding even for low number of sources.

2.8.3 MAP decoder: Error Probability and Design Criterion

Under the non-uniform distribution of the sum codebook, the optimal decoder that minimizes the probability of decoding error at the receiver is the *maximum a posteriori* decoder given according to the following:

$$\begin{aligned}
\hat{\square}_{map} &= \underset{\square_s 2 \square_s}{\operatorname{argmax}}\, p(\square_s|y) \\
&= \underset{\square_s 2 \square_s}{\operatorname{argmax}}\, p(\square_s) p(y|\square_s) \\
&= \underset{\square_s 2 \square_s}{\operatorname{argmax}}\, p(\square_s) \frac{1}{(\square\sqrt{2\square})^n} \exp\left[-\frac{\| y - \square_s \|^2}{2\square^2}\right] \\
&= \underset{\square_s 2 \square_s}{\operatorname{argmin}}\, -\ln(p(\square_s)) + \frac{\| y - \square_s \|^2}{2\square^2}
\end{aligned} \tag{2.55}$$

Notice that the MAP decoder does not involve a scaling step as the case of the conventional decoder.

Using this optimal MAP decoder, we derive in the following theorem a union bound estimate on the decoding error probability.

Theorem 2.5. *Consider a nested lattice design $\Lambda = (\Lambda_F; \Lambda_C)$ and a receiver computing a noiseless sum of N source codewords in a Gaussian multiple access channel using the optimal maximum a posteriori decoder. Then the union bound estimate of the probability of decoding error is*

$$P_e \leq \frac{1}{2} \sum_{\square_s 2 \square_s} \sum_{\hat{\square}_s 2 \square_s n \square_s} p(\square_s) \operatorname{erfc}\left[\sqrt{A} + \frac{B}{\sqrt{A}}\right] \tag{2.56}$$

where $A = \frac{d_{min}^2}{8\square^2}$, $B = \frac{1}{4} \ln \frac{p(\square_s)}{p(\hat{\square}_s)}$ and d_{min} denotes the minimum distance of the fine lattice Λ_F.

Proof. The proof of our theorem is based on the pairwise error probability defined as the probability that the sum codeword $\square_s$ has a larger MAP decoding metric in (2.55) than $\hat{\square}_s$ given that $\square_s$ is transmitted. Its expression is formulated as follows

$$\begin{aligned}
\Pr(\square \longrightarrow \hat{\square}_s) &= \Pr\left[-\ln \frac{\square}{p(\hat{\square}_s)}^{\square} + \frac{\| y - \hat{\square}_s \|^2}{2\square^2} < -\ln(p(\square_s)) + \frac{\| y - \square_s \|^2}{2\square^2} \right] \\
&= \Pr\left[\ln \frac{p(\square_s)}{p(\hat{\square}_s)} + \frac{\| y - \hat{\square}_s \|^2}{2\square^2} - \frac{\| y - \square_s \|^2}{2\square^2} < 0 \right] \\
&= \Pr\left[2\square^2 \ln \frac{p(\square_s)}{p(\hat{\square}_s)} + \| \square_s - \hat{\square}_s \|^2 + 2 \underset{D}{\square_s - \hat{\square}_s; z} \underset{E}{} < 0 \right] \\
&= \Pr(G < 0) = Q\left(\frac{\square_G}{\square_G} \right) \\
&= Q\left(\frac{\| \square_s - \hat{\square}_s \|}{2\square} + \frac{\square}{\| \square_s - \hat{\square}_s \|} \ln \frac{p(\square_s)}{p(\hat{\square}_s)} \right)
\end{aligned}$$

Where Q(:) denotes the Q function and it is easy to prove that

$$G = 2\square^2 \ln \frac{p(\square_s)}{p(\hat{\square}_s)} + \| \square_s - \hat{\square}_s \|^2 + 2 < \square_s - \hat{\square}_s; z >$$

is a random Gaussian variable of mean $\square_G$ and variance $\square_G^2$ given by:

$$\square_G = \| \square_s - \hat{\square}_s \|^2 + 4\square^2 \ln \frac{p(\square_s)}{p(\hat{\square}_s)} \tag{2.57}$$

$$\square_G^2 = 4\square^2 \| \square_s - \hat{\square}_s \|^2 \tag{2.58}$$

Using the union bound, we get,

$$\begin{aligned}
P_e &\leq \sum_{\square_s 2 \square_s} p(\square_s) \sum_{\hat{\square}_s 2 \square_s n \square_s} \Pr(\square_s \longrightarrow \hat{\square}_s) \\
&\leq \sum_{\square_s 2 \square_s} \sum_{\hat{\square}_s 2 \square_s n \square_s} p(\square_s) Q\left(\frac{\| \square_s - \hat{\square}_s \|}{2\square} + \frac{\square}{\| \square_s - \hat{\square}_s \|} \ln \frac{p(\square_s)}{p(\hat{\square}_s)} \right)
\end{aligned}$$

We can therefore, using the relation $Q(x) = \frac{1}{2}\mathrm{erfc}(\frac{x}{\sqrt{2}})$, write:

$$P_e \leq \frac{1}{2} \sum_{\square_s 2 \square_s} \sum_{\hat{\square}_s 2 \square_s n \square_s} p(\square_s) \mathrm{erfc}\left(\frac{\| \square_s - \hat{\square}_s \|}{2\sqrt{2}\square} + \frac{\square}{\sqrt{2} \| \square_s - \hat{\square}_s \|} \ln \frac{p(\square_s)}{p(\hat{\square}_s)} \right)$$

The last step to prove our theorem is based on two facts:

- $\| \square_s - \hat{\square}_s \| \geq d_{min}$, for all $\square_s; \hat{\square}_s \in \Lambda_s$. This inequality results from the linear structure and the geometrical symmetric properties of the fine lattice Λ_F.

- the function $\mathrm{erfc}(x + \frac{\alpha}{x})$; $\alpha \in \mathbb{R}$ is a decreasing function with respect to x [99].

The proof follows then by considering A and B as defined above. □

Given the derived upper bound, we propose a lattice design criterion as follows.

Proposition 2.2. *Minimization of the error probability under MAP decoding requires to design nested lattices $\Lambda = (\Lambda_F; \Lambda_C)$ such that the minimum distance of the Fine lattice is maximized.*

Proof. The upper bound on the error probability is a strictly decreasing function of A [99], thus a decreasing function of the minimum distance of the lattice Λ_F. Then in order to make the error probability small, the coding lattice Λ_F has to have a large minimum distance d_{min}. □

The construction of such good codes is out of the scope of this work. Even though, we point out that for lattices built using Construction A over linear codes, this criterion requires to design linear codes with minimum euclidean weights.

2.8.4 Practical MAP decoding Algorithms

We aim in this section to develop practical decoding algorithms that allow to reliably find the optimal MAP estimate of the optimization problem in (2.55). For this purpose we use the Gaussian distribution of the sum codewords. Accordingly, the MAP decoding rule in (2.55) is equivalent to:

$$\hat{\alpha}_{map} = \underset{\alpha_s \in 2\,\alpha_s}{\operatorname{argmin}} \ln\left(f_{\alpha_s}(\Lambda_F)\right) + n \ln\left(\alpha_s\sqrt{2\alpha}\right) + \frac{1}{2\alpha_s^2} \| \alpha_s \|^2 + \frac{1}{2\alpha^2} \| y - \alpha_s \|^2$$

The first and second terms in this optimization problem are independent of the variable α_s, they can be disregarded in the optimization over α_s. Then we define a new MAP decoding metric given by:

$$\hat{\alpha}_{map} = \underset{\alpha_s \in 2\,\alpha_s}{\operatorname{argmin}} \| y - \alpha_s \|^2 + \beta^2 \| \alpha_s \|^2 \tag{2.59}$$

where $\beta = \frac{\alpha}{\alpha_s}$. Using this new metric, we show in Proposition.2.3 that MAP decoding reduces to solve for a closest vector problem.

Proposition 2.3. *The MAP decoding metric in (2.59) is equivalent to find the closest vector in the lattice Λ_{aug} of generator matrix $M_{aug} = [M \ \ \beta M]^t \in \mathbb{R}^{2n \times n}$ to the vector $y_{aug} = [y \ 0_n]^t$ according to the following metric:*

$$\hat{\alpha}_{map} = \underset{\substack{x_{aug} \in \Lambda_{aug} = \\ x_{aug} = M_{aug}\alpha_s}}{\operatorname{argmin}} \| y_{aug} - x_{aug} \|^2 \tag{2.60}$$

Proof. The decoding metric in (2.59) can be written as:

$$\hat{\square}_{\text{map}} = \underset{\square_s 2 \square_s}{\text{argmin}} \left(\begin{array}{c} \square \\ \square \\ \square \end{array} \begin{array}{c} \square \\ y \\ 0_n \end{array} \begin{array}{c} \square \\ \square \\ \square \end{array} \begin{array}{c} \square \\ \square_s \\ \square\square_s \end{array} \begin{array}{c} \square \\ \square \\ \square \end{array} \right)^{\square_2}$$

$$= \underset{\square_s 2 \square_s}{\text{argmin}} \| y_{\text{aug}} - I_{\text{aug}} \square_s \|^2 \tag{2.61}$$

where $I_{\text{aug}} = [I_n \ \square I_n]^t \in R^{2n \square n}$ is a full rank matrix. On the other hand, given that the sum codewords belong to the fine lattice according to the shaping region $\mathcal{S}_s$, any codeword $\square_s$ can be written in the form $\square_s = M u$ where $u \in \mathcal{A}_s \subset Z^n$ and $\mathcal{A}_s$ translates the shaping constraint imposed by $\mathcal{S}_s$ and can be deduced from the shaping boundaries limited by the transmission power constraint P. Consequently the optimization problem in (2.61) is equivalent to solving

$$\begin{aligned} \hat{\square}_{\text{map}} &= \underset{u 2 A_s = \square_s = M u}{\text{argmin}} \| y_{\text{aug}} - I_{\text{aug}} M u \|^2 \\ &= \underset{u 2 A_s = \square_s = M u}{\text{argmin}} \| y_{\text{aug}} - M_{\text{aug}} u \|^2 \end{aligned} \tag{2.62}$$

M_{aug} is a full rank matrix and u is an integer vector, then solving (2.62) consists in finding the closest vector $x_{\text{aug}} = M_{\text{aug}} u$ to y_{aug} in the $n-$dimensional lattice Λ_{aug} of a generated matrix M_{aug}. After finding the optimal integer vector u_{opt} that minimizes the metric in (2.62), the optimal MAP estimate is deduced by $\hat{\square}_{\text{map}} = M u_{\text{opt}}$. □

In practice, the Sphere Decoder can be used to solve the closest vector problem. We propose in this work a modified version of this algorithm to take into account the shaping constraint as described in Appendix 5.B.3.

Remark 2.8. The MAP decoding metric in (2.59) involves two terms each one of them is given by an euclidean distance. When the first term is dominant, which is the case when $\square^2 = \frac{\square^2}{\square_s^2} = \frac{\square^2}{N \square_x^2} \ll 1$, the MAP decoding rule reduces to ML decoding (which is equivalent to minimum distance decoding in this case since we don't perform a scaling step). Given that $\square_x^2$ depends on the power constraint P, we deduce that this case of figure is likely to happen either at high Signal-to-Noise Ratio or when $N \square_x^2$ is sufficiently higher than the noise variance $\square^2$. We expect then that the MAP decoding and the conventional decoder achieve similar performance at high SNR range. Adversely, at the low and moderate SNR regime and when the product $N \square_x^2$ is small, the second term in the decoding metric applies an incremental constraint that considers the non-uniform distribution of the sum codewords in Λ_s which is not taken into account under the conventional decoder. In this case, we expect that the MAP decoder outperforms the minimum distance decoding-based one.

We provide in the following proposition an equivalent formulation of the MAP decoding metric related to perform MMSE-GDFE preprocessing followed by minimum euclidean distance decoding.

Proposition 2.4. *[Equivalence between MAP decoding and MMSE-GDFE preprocessed lattice decoding] The MAP decoding metric in (2.59) is equivalent to MMSE-GDFE preprocessed minimum euclidean distance decoding according to the metric:*

$$\hat{\mathbf{s}}_{\text{map}} = \underset{\mathbf{s} \in \mathbb{Z}[i]^n}{\operatorname{argmin}} \| \mathbf{F}\mathbf{y} - \mathbf{B}\mathbf{s} \|^2 \tag{2.63}$$

where $\mathbf{F} \in \mathbb{R}^{n \times n}$ *and* $\mathbf{B} \in \mathbb{R}^{n \times n}$ *denote respectively the forward and backward filters of the MMSE-GDFE preprocessing for the channel* $\mathbf{y} = \mathbf{s} + \mathbf{z}$ *given in (2.49) such that* $\mathbf{B}^t\mathbf{B} = \left(1 + \sigma^2\right)\mathbf{I}_n$ *and* $\mathbf{F}^t\mathbf{B} = \mathbf{I}_n$.

Proof. Let $\mathbf{N}(\mathbf{s})$ denote the metric we aim to minimize in (2.59), we have the following:

$$\begin{aligned}
\mathbf{N}(\mathbf{s}) &= \| \mathbf{y} - \mathbf{s} \|^2 + \sigma^2 \| \mathbf{s} \|^2 \\
&= \mathbf{y}^t\mathbf{y} - 2\mathbf{y}^t\mathbf{s} + \mathbf{s}^t\mathbf{s} + \sigma^2\mathbf{s}^t\mathbf{s} \\
&= \left(1 + \sigma^2\right)\mathbf{s}^t\mathbf{s} + \mathbf{y}^t\mathbf{y} - 2\mathbf{y}^t\mathbf{s} \\
&= \mathbf{s}^t\mathbf{B}^t\mathbf{B}\,\mathbf{s} + \mathbf{y}^t\mathbf{y} - 2\mathbf{y}^t\mathbf{F}^t\mathbf{B}\,\mathbf{s} \\
&= \underbrace{\mathbf{s}^t\mathbf{B}^t\mathbf{B}\,\mathbf{s} + \mathbf{y}^t\mathbf{F}^t\mathbf{F}\mathbf{y} - 2\mathbf{y}^t\mathbf{F}^t\mathbf{B}\,\mathbf{s}}_{\|\mathbf{F}\mathbf{y} - \mathbf{B}\mathbf{s}\|^2} + \underbrace{\mathbf{y}^t\left(\mathbf{I}_n - \mathbf{F}^t\mathbf{F}\right)\mathbf{y}}_{\Gamma(\mathbf{y})}
\end{aligned} \tag{2.64}$$

where $\mathbf{F} \in \mathbb{R}^{n \times n}$ and $\mathbf{B} \in \mathbb{R}^{n \times n}$ are chosen such that: $\mathbf{B}^t\mathbf{B} = \left(1 + \sigma^2\right)\mathbf{I}_n$ and $\mathbf{F}^t\mathbf{B} = \mathbf{I}_n$. Given that $\Gamma(\mathbf{y}) > 0$ and independent of $\mathbf{s}$, minimization of $\mathbf{N}(\mathbf{s})$ is equivalent to minimize $\| \mathbf{F}\mathbf{y} - \mathbf{B}\mathbf{s} \|^2$. The last piece to our proof is to show that the matrices $\mathbf{F}$ and $\mathbf{B}$ correspond to the filters of the MMSE-GDFE preprocessing in the system $\mathbf{y} = \mathbf{s} + \mathbf{z}$ of input $\mathbf{s}$ and AWGN $\mathbf{z}$. This proof is provided in Appendix 5.C. □

In order to find the MAP estimate according to the decoding metric in (2.63), the receiver, given the channel output, first performs MMSE-GDFE preprocessing, then performs minimum euclidean distance decoding to find the nearest point to $\mathbf{F}\mathbf{y}$ in the lattice of generator matrix $\mathbf{B}\mathbf{M}$ according to the shaping constraint imposed by the subset Λ_s.

The first step of this method requires to derive the expressions of the matrices $\mathbf{F}$ and $\mathbf{B}$. For this purpose consider the augmented matrix $\mathbf{I}_{\text{aug}} = \begin{pmatrix} \mathbf{I}_n \\ \sigma\mathbf{I}_n \end{pmatrix}$. Let its QR decomposition as:

$$\mathbf{I}_{\text{aug}} = \mathbf{Q}\mathbf{R} = \begin{pmatrix} \mathbf{Q}_1 \\ \mathbf{Q}_2 \end{pmatrix} \mathbf{R}$$

where $\mathbf{Q} \in \mathbb{R}^{2n \times n}$ is an orthogonal matrix and $\mathbf{R} \in \mathbb{R}^{n \times n}$ is upper triangular. The expressions of the desired filters are given by [100–102]:

$$\mathbf{F} = \mathbf{Q}_1^t \quad ; \quad \mathbf{B} = \mathbf{R} \tag{2.65}$$

With the QR decomposition of the augmented matrix we have

$$\mathbf{I}_{\text{aug}}^t\mathbf{I}_{\text{aug}} = \left(1 + \sigma^2\right)\mathbf{I}_n = \mathbf{R}^t\mathbf{R} = \mathbf{B}^t\mathbf{B} \tag{2.66}$$

And we can write $I_n = Q_1 R$ which leads to the relation between the two filters as

$$F^t B = I_n \tag{2.67}$$

2.8.5 Numerical results

In this section we evaluate the performance of the conventional decoder (based on MMSE scaling and minimum distance decoding) and the proposed MAP decoding algorithm implementing a modified Sphere Decoder. In addition, in order to validate the Gaussianity law assumption we considered to derive our MAP decoding metric, we include a naive exhaustive search to solve (2.55). Using this approach, no assumptions on the sum codebook distribution is considered. The receiver, given the number of sources and the original codebook associated to the nested lattice Λ, derives the statistics of the sum codebook to compute the corresponding values of $p(\square_s)$ for all codewords $\square_s \in \Lambda_s$, then, it exhaustively seeks the codeword which maximizes the decoding metric in (2.55). We studied in our analysis two lattice examples as described below.

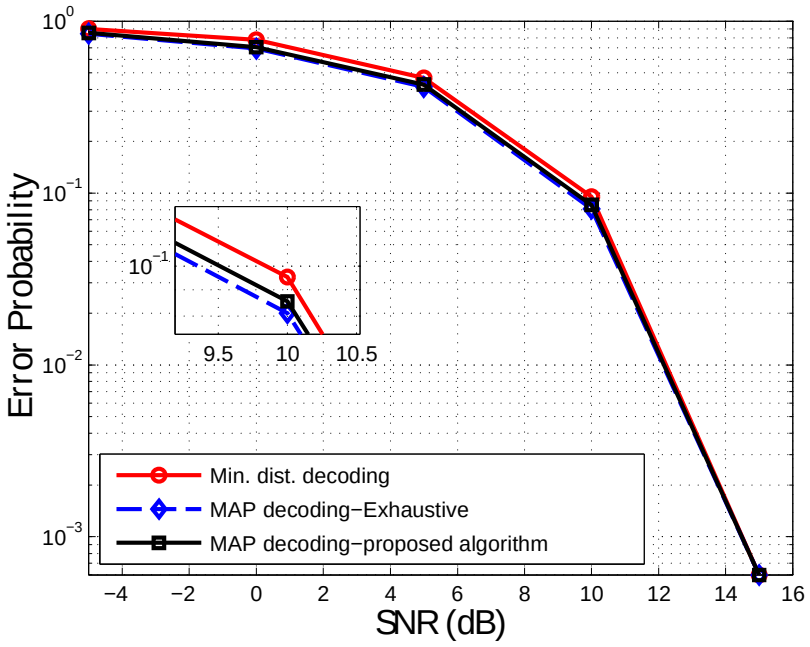


Figure 2.6: Error performance for the case $n = 2; N = 2; P = 21$.

Example 1: 2-Dimensional lattice ($n = 2$) for this first example we have chosen the 2-dimensional lattice Λ described in Example 2.1 and considered the cases of $N = 2$ and $N = 5$ which correspond to the statistical distribution in Figure 2.5. The shaping constraint in this case is given by $P = \square_x^2 = 6{:}5$. Given the number of sources and the

power constraint imposed by the coarse lattice, we calculated for each case the bounds requirements to be considered in the decoding process.

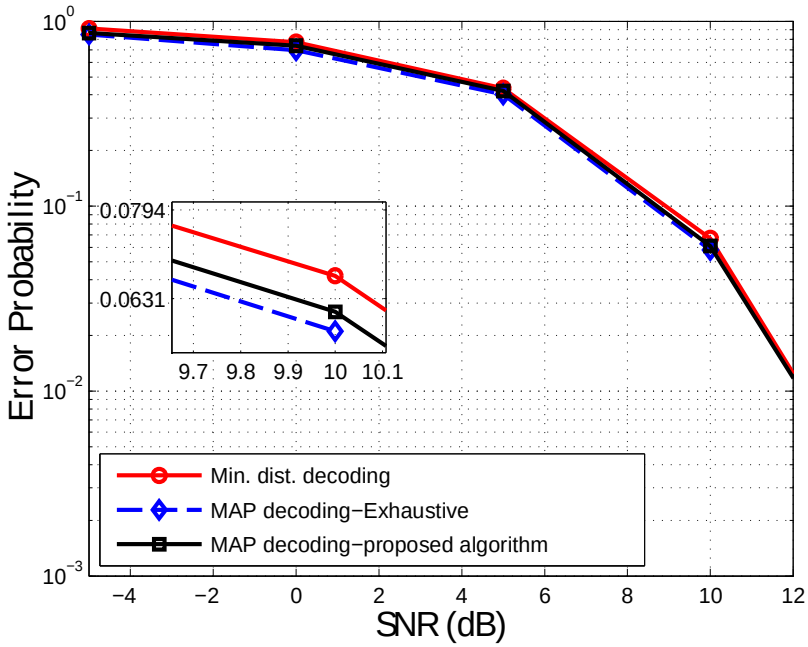


Figure 2.7: Error performance for $n = 2; N = 5; P = 6{:}5$.

Numerical results concerning the first case, depicted in Figure 2.6, show that our proposed algorithm achieves almost identical performance as the exhaustive search, which confirms the effectiveness of our metric as well as the validity of the Gaussianity law assumption considered to model the sum-codewords even for the case of low number of sources N. Moreover, plotted curves show that the MAP decoder outperforms the conventional minimum distance decoding (Min. dist. decoding). The gain for this 2-dimensional lattice case is not huge, and is limited to 0:5dB for an probability equal to 10^{-1}. Results for the case of $N = 5$ plotted in Figure 2.7 confirm the previous findings and show that the performance gap between the MAP and the Minimum distance decoder is not also high. Common to these two settings is the high value of $N\sigma_x^2$, which joins our analysis in Remark. 2.8.

Example 2: 4-Dimensional lattice ($n = 4$) In this second example we have chosen the 4-dimensional integer lattice Λ of a generator matrix the identity I_4 together with a cubic shaping region according to $P = 1$. The aim of considering this example is to analyze the performance of the MAP decoder when the lattice dimension increases. Simulation results depicted in Figure 2.8 show that our proposed MAP algorithm allows to achieve a gain of 1dB at a codeword error rate of 10^{-3} over the minimum distance decoder while keeping a small gap to the exhaustive search. This case shows the merit of

applying the MAP decoding in settings where the product $N\sigma_x^2$ is small. In addition, we notice that the gap between the MAP decoder and the conventional one is independent of the lattice dimension, it rather increases in settings involving small $N\sigma_x^2$.

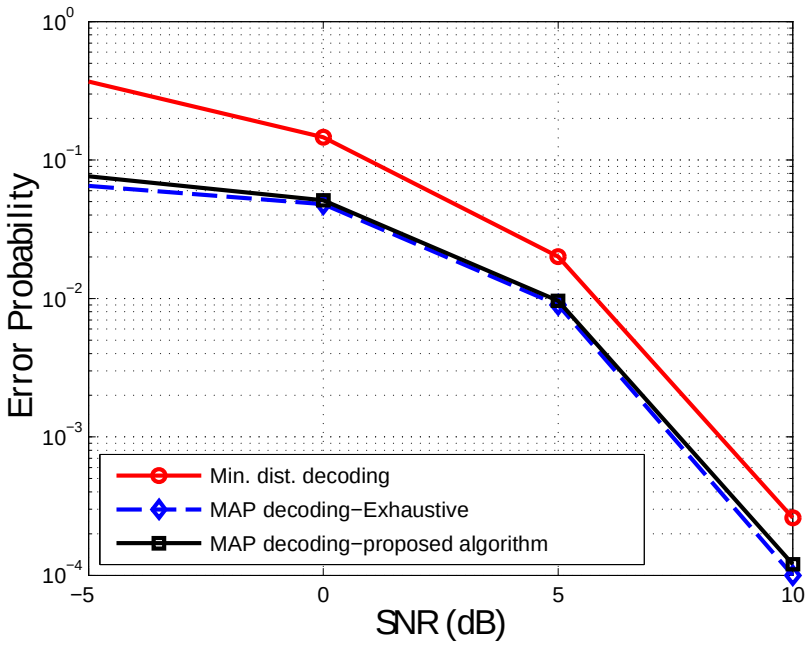


Figure 2.8: Error performance for $n = 4; N = 2; P = 1$.

2.9 Optimal Decoders for the CF: fading channels

We study in this section the case of fading channels. The tools we will use in our analysis are valid only in the case of integer lattices, thus we will consider an $n-$dimensional nested lattice code $\Lambda \subset \mathbb{Z}^n$ involving a fine lattice $\Lambda_F \subset \mathbb{Z}^n$ of a generator matrix M and a coarse lattice $\Lambda_C \subset \mathbb{Z}^n$. For this case, M is an integer full rank matrix. We will start with the multi-dimensional case then we provide more in depth analysis regarding the one-dimensional case.

2.9.1 System Model

The real-valued multiple access channel output is written as,

$$y = \sum_{i=1}^{N} h_i x_i + z \tag{2.68}$$

where $x_i \in \Lambda \subset \mathbb{Z}^n$ are the lattice codewords sent by the sources according to the power constraint in (2.3), $h_i \in \mathbb{R}$ denote the fixed channel gains and $z \in \mathbb{R}^n$ stands for the

AWGN. Recall that the decoding objective is to recover an estimate of

$$\Box = \left[\sum_{i=1}^{N} a_i x_i \right] \bmod \Lambda_C \tag{2.69}$$

where $a = [a_1; \ldots; a_N]^t \in Z^N$ is the network code vector. We are concerned with the optimal ML decoding for recovering the integer combination: $t = \sum_{i=1}^{N} a_i x_i$, the modulo-lattice operation is performed in a second stage separately. The decoding error probability is defined then as:

$$P_e = \Pr\left[\hat{t} \neq t \right] \tag{2.70}$$

In order to decode an estimate of t, the receiver first selects the parameters $\Box \in R$ and $a \in Z^N$. Given the vector a and the shaping boundaries for the original codewords, it is known that the searched vector t belongs to a subset Λ_f in the fine lattice Λ_F. However, in contrast to the Gaussian channels case, it is difficult in this setting to characterize the distribution of the combinations t in Λ_f since it depends on the channel vector h, the network code vector a and the Signal-to-Noise Ratio. We will assume then a uniform distribution and analyze its corresponding decoding rule based on Maximum Likelihoood criterion. To the best of our knowledge, this decoding approach was also independenly investigated by Belfiore and Ling in [103].

Accordingly, the optimal receiver parameters $\Box$ and a are selected under ML decoding-based criterion by maximizing the rate $R_{comp;ML}$ defined in (2.24). Nevertheless, one can easily observe that the maximization of this rate is equivalent to the optimization problem in (2.25) and (2.26) for which the optimal scaling parameter is the MMSE factor and the optimal network code vector corresponds to the shortest vector in the lattice Λ_G defined in Theorem.2.2.

After selecting $\Box$ and a, the receiver scales the channel output to get:

$$\tilde{y} = \sum_{i=1}^{N} a_i x_i + \sum_{i=1}^{N} \left(\Box \tilde{h}_i - a_i \right) x_i + \tilde{z} \tag{2.71}$$

where $\tilde{h}_i = \Box h_i; i = 1; \ldots; N$ and $\tilde{z} = \Box z$, and attempts to decoder $t = \sum_{i=1}^{N} a_i x_i$.

2.9.2 ML Decoding Metric

The decoding metric of the ML criterion is based on maximizing the conditional probability $p(\tilde{y}|t)$ over all possible values of $t \in \Lambda_f$ according to

$$\hat{t} = \underset{t \in \Box_f}{\operatorname{argmax}}\, p(\tilde{y}|t) \tag{2.72}$$

Given that $t = \sum_{i=1}^{N} a_i x_i$, we can equivalently write (2.72) as:

$$\hat{t} = \underset{t \in \Box_f}{\operatorname{argmax}} \sum_{(x_1; \ldots; x_N) \in \Box^N : \sum_{i=1}^{N} a_i x_i = t} p(\tilde{y} | (x_1; \ldots; x_N))\, p(x_1; \ldots; x_N) \tag{2.73}$$

The transmitted codewords are assumed to be uniformally distributed over the nested lattice code Λ, i.e., $x_1, \ldots, x_N$ are equiprobable. On the other hand, we have,

$$p(\tilde{y}|x_1, \ldots, x_N) \propto \exp\left(\frac{-1}{2\tilde{\sigma}^2} \| \tilde{y} - \sum_{i=1}^{N} \tilde{h}_i x_i \|^2\right) \tag{2.74}$$

where $\tilde{\sigma}^2 = \sigma^2\sigma_e^2$. Combining (2.74) and (2.73), we get:

$$\hat{t} = \underset{t \in \mathcal{A}_f}{\operatorname{argmax}} \sum_{(x_1, \ldots, x_N) \in \mathbb{Z}^N : \sum_{i=1}^{N} a_i x_i = t} \exp\left(\frac{-1}{2\tilde{\sigma}^2} \| \tilde{y} - \sum_{i=1}^{N} \tilde{h}_i x_i \|^2\right) \tag{2.75}$$

Let

$$\Psi(\lambda) = \sum_{(x_1, \ldots, x_N) \in \mathbb{Z}^N : \sum_{i=1}^{N} a_i x_i = t} \exp\left(\frac{-1}{2\tilde{\sigma}^2} \| \tilde{y} - \sum_{i=1}^{N} \tilde{h}_i x_i \|^2\right) \tag{2.76}$$

Our objective in the following is to express Ψ as a function of the desired equation t. To this end, we need to express the codewords $x_i; i = 1, \ldots, N$ as functions of t. Given the integer nature of the vector a and the codewords x_i, this task requires to solve the system of diophantine equations $t = \sum_{i=1}^{N} a_i x_i$. For $n-$dimensional vectors ($x_i; i = 1, \ldots, N$ and t), this can be done using the Hermite Normal Form (HNF) of integral matrices [104, 105] as explained in the following.

2.9.3 Diophantine Equations: Hermite Normal Form

Define the integer-valued matrix $\tilde{M} \in \mathbb{Z}^{n \times nN}$ as,

$$\tilde{M} = [a_1 M \;\; a_2 M \;\; \ldots \;\; a_N M]$$

The Hermite Normal Form of $\tilde{M}$ is such that:

$$\tilde{M} U = \left[0^{n \times (N-1)n} | B\right] \tag{2.77}$$

where $U \in \mathbb{Z}^{nN \times nN}$ is a unimodular matrix, and $B \in \mathbb{Z}^{n \times n}$ is an invertible matrix.

Futhermore, we decompose the matrix U in the form:

$$U = \begin{bmatrix} U_1 & V_1 \\ U_2 & V_2 \\ \vdots & \vdots \\ U_N & V_N \end{bmatrix} \tag{2.78}$$

where $V_i \in \mathbb{Z}^{n \times n}$ and $U_i \in \mathbb{Z}^{n \times n(N-1)}$. Then, the solution of the system of diophantine equations is,

$$x_i = d_i + v_i \tag{2.79}$$

where $v_i = M V_i B^{-1} t$ and d_i belong to the lattice of a generator matrix $M U_i$ for $i = 1, \ldots, N$.

2.9.4 Likelihood Function

We go back now to the ML decoding rule defined in (2.75) and replace the vectors x_i by the solution of the diophantine equations given in (2.79), we obtain

$$\hat{t} = \underset{t \in \square_f}{\operatorname{argmax}} \sum_{q \in L} \exp\left[\frac{-1}{2\square^2} \| ! (t) - q \|^2\right] \tag{2.80}$$

where $q = \sum_{i=1}^{N} \tilde{h}_i d_i$ belongs to the lattice $\mathcal{L}$ of a generator matrix $\sum_{i=1}^{N} \tilde{h}_i M U_i$ and $! (t) = \tilde{y} - \sum_{i=1}^{N} h_i M V_i B^{\square 1} t$.

Then, in order to find the ML solution, we need to find the maximum of the likelihood function:

$$' (t) = \sum_{q \in L} \exp\left[\frac{-1}{2\square^2} \| ! (t) - q \|^2\right] \tag{2.81}$$

This function is a sum of Gaussian measures, it is periodic and depends on the Signal-to-Noise Ratio. Additionally, its most important characteristic is that it can be flat, which means that for some values of the channel coefficients, the network code vector and the Signal-to-Noise Ratio, the maximum of $'$ can be achieved by several values of t, which makes the ML decision rule ambiguous and results in decoding errors. This flatness behavior is characterized by Belfiore and Ling in [103] by the so called the *Flatness Factor* defined below.

Definition 2.3. Let $\mathcal{L}$ be a $n-$dimensional full rank lattice and define the function:

$$' (y; \square) = \sum_{q \in L} \exp\left[\frac{-1}{2\square^2} \| y - q \|^2\right]$$

The *flatness factor* of the lattice $\mathcal{L}$ is defined by:

$$\square_L (\square) \triangleq \frac{E_y (' (y; \square))}{\max_{y \in R^n} ' (y; \square)} \tag{2.82}$$

and satisfies: $0 \leq \square_L (\square) \leq 1$. The mathematical expectation $E_y (' (y; \square))$ is given by,

$$E_y (' (y; \square)) = \frac{1}{\mathrm{vol}(\mathcal{L})} \int_{V(L)} ' (y; \square) dy$$

where $\mathcal{V}(\mathcal{L})$ corresponds to the Voronoi region of the lattice $\mathcal{L}$.

For the ML decoding rule, we should minimize the flatness factor of the lattice $\mathcal{L}$ over which is performed the sum of the Gaussian measures in order to be able to distinguish the maximum values of the likelihood function and perform a correct decoding decision.

Beyond this implication on the lattice design, solving the ML decoding metric requires more reseach on the sum of Gaussian measures. Alternatively, authors in [90, 103]

propose an approximation of ML decoding based on *Diophantine Approximation* and consists in the optimization problem given by:

$$\hat{t} = \underset{t2\square_f\ ;\ q2A_L}{\operatorname{argmax}} \| ! (\square) - q \|^2 \tag{2.83}$$

Where $\mathcal{A}_L$ is a finite subset of the lattice $\mathcal{L}$ fixed by the boundaries of the original codewords according to the transmission power constraint. For one-dimensional lattices, there are several algorithms pertaining to the resolution of the diophantine approximations of reals. However, solving the multi-dimensional case, requires additionally to develop efficient algorithms to handle simultaneous diophantine approximations.

2.9.5 Case study: 1-dimensional lattices

In order to better explain the previous results, we analyze in this subsection the case of one-dimensional lattices in Z. Additionally, we consider the case of two sources. In this scheme, transmitted codewords x_1 and x_2 are just integer scalars drawn i.i.d from the integer constellation over Z defined by $\mathcal{A} = [-S_m\ S_m] = [-S_m; -S_m + 1; :::; S_m]$ for $S_m \in Z^+$. This integer codebook can be seen as a nested lattice code in Z involving the fine lattice $\Lambda_F = Z$ and the coarse lattice $\Lambda_C = 2S_m Z$.

The channel output in this scenario is given by:

$$y = h_1 x_1 + h_2 x_2 + z \tag{2.84}$$

with $h_i \in R$ and $z \sim \mathcal{N}(0; \square^2)$. Given the channel state information, the receiver selects the optimal scaling parameter and the optimal network code vector $a = [a_1\ a_2]^t$ and attempts to decode the integer combination $t = a_1 x_1 + a_2 x_2$ from the integer set $\mathcal{A}_t$ determined by S_m and the values of the coefficients a_1 and a_2. The scaled channel output is given by:

$$\tilde{y} = a_1 x_1 + a_2 x_2 + \square\tilde{h}_1 - a_1\square x_1 + \square\tilde{h}_2 - a_2\square x_2 + \tilde{z} \tag{2.85}$$

where $\tilde{h}_i = \square h_i\,; i = 1; 2$ and $\tilde{z} = \square z$.

Under these settings, the ML solution is given by:

$$\hat{t} = \underset{t2A_t}{\operatorname{argmax}} \sum_{\substack{(x_1;x_2)2A^2= \\ a_1x_1+a_2x_2=t}} \exp\square\frac{-1}{2\square^2} \| \tilde{y} - \tilde{h}_1 x_1 - \tilde{h}_2 x_2 \|^2\square \tag{2.86}$$

And the likelihood function is given by:

$$' (t) = \sum_{\substack{(x_1;x_2)2A^2= \\ a_1x_1+a_2x_2=t}} \exp\square\frac{-1}{2\square^2} \| \tilde{y} - \tilde{h}_1 x_1 - \tilde{h}_2 x_2 \|^2\square \tag{2.87}$$

Our aim now is to express $'$ as a function of t only. Therefore, we need to solve the *Diophantine Equation* $t = a_1x_1 + a_2x_2$. Let $g = a_1 \wedge a_2$ denote the greatest common divisor (gcd) of a_1 and a_2.

If the desired scalar t is a multiple of the greatest common divisor of the coefficients a_1 and a_2, the diophantine equation admits an infinite number of solutions in the form:

$$\begin{cases} x_1 = \frac{u_1}{g}t + \frac{a_2}{g}k \\ x_2 = \frac{u_2}{g}t - \frac{a_1}{g}k \end{cases} \tag{2.88}$$

where $k \in Z$ and $(u_1; u_2)$ is a particular solution of the equation $a_1x_1 + a_2x_2 = g$ that can be derived using the *Extended Euclid Algorithm* [106].

If t is not a multiple of g, then the diophantine equation has no solutions. For what concerns our case, the network code vector a corresponds to the coordinates of a lattice shortest vector, then the coefficients a_1 and a_2 are coprime. Thus, the diophantine equation under question has always infinite solutions given by the system in (2.88) with $g = 1$. This result is also applicable to the general case of $N > 2$ sources.

Accordingly, we can write the ML solution in (2.86) as

$$\hat{t} = \underset{t2A_t}{\operatorname{argmax}} \overbrace{\sum_{k=-1}^{1} \exp\left[\frac{-1}{2\sigma^2} \| \tilde{y} - t + k \|^2\right]}^{'(t)} \tag{2.89}$$

where $= \tilde{h}_1u_1 + \tilde{h}_2u_2$, $= a_1\tilde{h}_2 - a_2\tilde{h}_1$ and $k \in Z$.

2.9.5.1 Properties of the likelihood function

$'$ is a sum of gaussian functions, it is periodic and has the following properties:

- *mean* $m = \tilde{y}$
- *period* $p = \frac{}{2\sigma^2}$
- *width* $w = \frac{}{2\sigma^2}$

In addition, $'$ depends on the SNR, the channel coefficients, the coefficient vector a and obviously on the constellation bounds defined by S_m. We illustrate in Figure 2.9 an example of the likelihood function obtained for $S_m = 5$, $x_1 = 3$, $x_2 = 4$ at SNR = 10dB and $h = [-1{:}191\ 1{:}189]^t$. The optimal network code vector for this case is equal to $a = [-1\ 1]^t$. Accordingly, the desired combination should be equal to $t = 1$. The corresponding likelihood function depicted in Figure 2.9 is well maximized at $\hat{t} = 1$. In this case, it is easy to decode the maximum of $'(t)$ since we can distinguish a peak corresponding to the unique $\hat{t}$ for which this function is maximized.

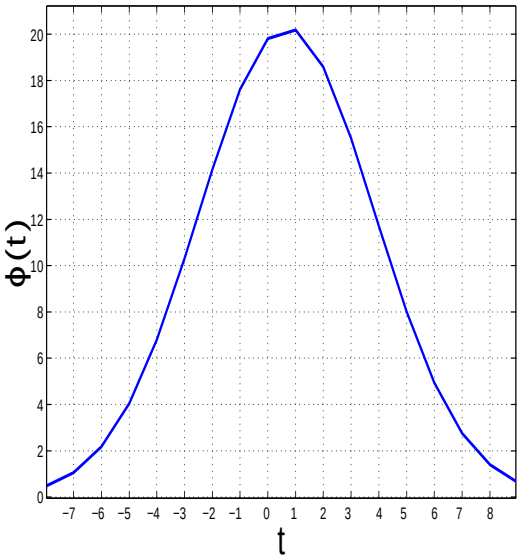
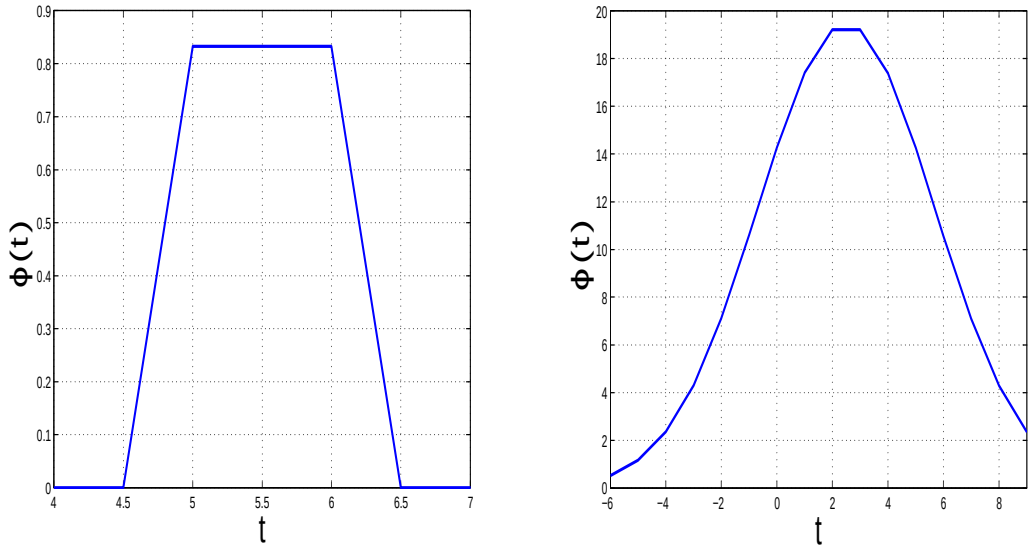


Figure 2.9: Example of the Likelihood function.

- Impact of h and a: The choice of the network code vector a can greatly impact the behavior of the likelihood function. Particularly, when this integer vector is aligned to the channel vector h (they become colinear), the period $p = \frac{a_1 h_1 \square a_2 h_2}{2 \simeq^2}$ of the likelihood function becomes small and results in a flatness of ' and impossibility of decoding the right $\hat{t}$ since the maximum can be obtained for different values. This result is demonstrated through Figure 2.10(a) obtained at SNR = 60dB $S_m = 5; x_1 = -5; x_2 = -4; h = [1{:}3681 - 0{:}2359]^t; a = [-1\ 0]^t$. The maximum of the likelihood function is obtained for two integer values $t_1 = 5$ and $t_2 = 6$ while the correct decodable value must be $\hat{t} = 5$ for the corresponding values of x_1 and x_2. This case is likely to happen at high SNR range for which the maximization of the computation rate $R_{comp;ML}$ requires to align a to h.

- Impact of the constellation size: The likelihood function depends of the constellation size and the values of S_m. When the size of the codebook increases, the set $\mathcal{A}_t$ over which the desired combination t should be searched becomes large. Consequently, the width of ' becomes large and the likelihood function is made flat. Thus, decoding the maximal value of t becomes ambiguous. An example of this scenario is illustrated in Figure 2.10(b) obtained for $S_m = 10; \text{SNR} = 10\text{dB}; x_1 = -2; x_2 = -4; h = [1{:}4741\ \ -0{:}2839]^t; a = [-1\ 0]^t$. We can see that the likelihood function attains its maximum for $t = 2$ and $t = 3$ while the correctly decoded value is $\hat{t} = 2$. This ambiguity leads to decoding errors.



(a) $S_m = 5; SNR = 60dB$ (b) $S_m = 10; SNR = 10dB$

Figure 2.10: Flatness of the likelihood function.

2.9.5.2 Diophantine Approximation

The sum of Gaussian functions in the likelihood function makes the ML decoding hard to handle in practice. Our aim in the following is to find a quasi-ML solution easy-to-implement. For this purpose, we study the possible values of t that allow to maximize the likelihood function:

- For $t \in R$: $'$ is maximized for t satisfying $\tilde{y} - \square t + \square k = 0$, which is equivalent to:

$$\hat{t} = \frac{\tilde{y}}{\square} + \frac{\square}{\square} k \Rightarrow \hat{t} \in \frac{\tilde{y}}{\square} + \frac{\square}{\square} Z \tag{2.90}$$

- For $t \in Z$: $'$ is maximized for t which minimizes $| \tilde{y} - \square t + \square k |$.

Since we are interested in integer-valued combinations, the solution corresponds to the minimization of $| \tilde{y} - \square t + \square k |$. Given this observation, we define a new optimization problem equivalent to (2.89) by:

$$\hat{t} = \underset{k \in Z; t \in A_t}{\operatorname{argmin}} | \tilde{y} - \square t + \square k | \tag{2.91}$$

Let $\square^0 = \frac{\square}{\square}$ and $y^0 = -\frac{\not{y}}{\square}$, then the minimization problem is equivalent to:

$$\hat{t} = \underset{k \in Z; t \in A_t}{\operatorname{argmin}} | \square^0 k - t - y^0 | \tag{2.92}$$

This problem corresponds to solving the *Inhomogeneous Diophantine Approximation in the absolute sens* (IDA) [107], $F(t;k)$, defined as,

$$F(t;k) = | \square^{0}k - t - y^{0} | \tag{2.93}$$

It consists in finding the best rational approximation $\frac{t}{k}; k \in Z$ of the real number $\square^{0}$ assumed an additional real shift y^{0}. In the general settings for such problems, the error approximation function $F(t;k)$ is considered and it is stated that a rational number $t=k$ is the best Diophantine Approximation if, for all other rational numbers $t^{0}=k^{0}$

$$k^{0} \leq k \Rightarrow F(k^{0},t^{0}) \geq F(k;t)$$

and

$$F(k^{0},t^{0}) \leq F(k;t) \Rightarrow k^{0} \geq k$$

For what concerns our settings, in addition to the error approximation function, the set of the diophantine approximations is determined by the limits imposed by the shaping boundaries $\mathcal{A}_t$.

In literature, there exist simple and easy-to-implement algorithms to solve Diophantine Approximations of reals. The best known one is the *Cassel's Algorithm* [108]. In this work we adopt a modified version of this algorithm to take into consideration the shaping constraint and ensure that the resulting solution $(t;k)$ satisfies $t \in \mathcal{A}_t$. The proposed algorithm is given in Appendix 5.D.

2.9.5.3 Simulation results

In this section we address the performance of the conventional decoder (based on MMSE preprocessed minimum distance decoding) and the proposed Inhomogenous Diophantine Approximation (IDA). We consider the same settings analyzed previously involving two sources transmitting integer symbols x_1 and x_2 drawn i.i.d from the constellation set $\mathcal{A} = [-S_m \; S_m]$ to a common receiver interested in recovering an integer combination $t = a_1x_1 + a_2x_2$. We analyze the error probability as a function of the SNR, for which a decoding error counts if $\hat{t} \neq t$.

For what concerns the conventional decoder, given the channel state information, the receiver solves for the best network code vector a solution of the shortest vector problem, scales the channel output, then decodes to the nearest integer value. For the IDA, given the vector a, the receiver first implements the *Extended Euclid* algorithm to solve the Diophantine equation $a_1x_1 + a_2x_2 = g$, then uses the modified Cassel's algorithm to find the best inhomogeneous Diophantine approximation.

In Figure 2.11 minimum distance decoding and IDA decoding are compared. We plot the decoding error probability as a function of the SNR for the case of $S_m = 5$. This figure shows that both decoding methods achieve same performance in low and moderate SNR values. The importance of the IDA method rises asymptotically, since for this case, the conventional decoder presents a floor in the error probability.

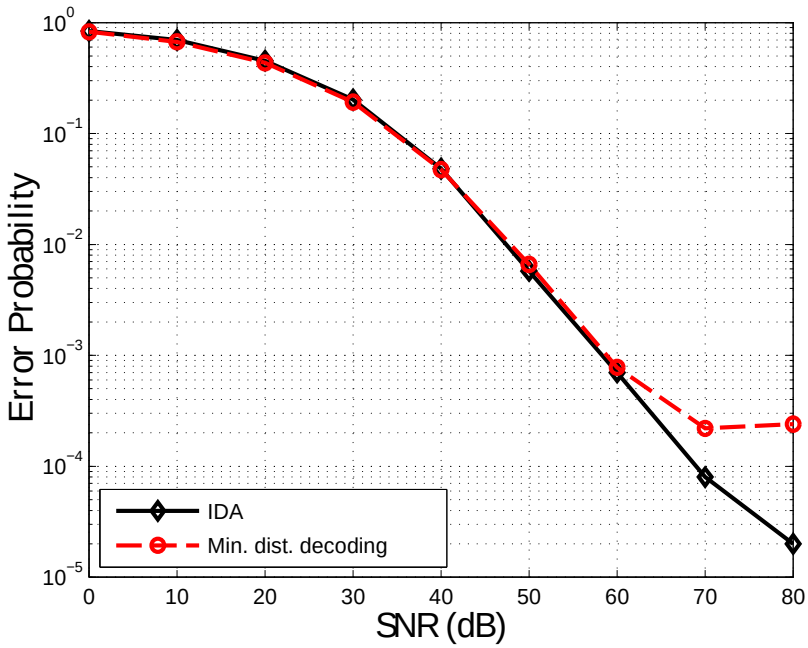


Figure 2.11: Error Probability for $S_m = 5$.

In Figure 2.12, we analyze the performance of the proposed IDA decoding for three values of the constellation interval, defined by $S_m = 5; 7; 10$. This is to understand the impact of the constellation size on the diversity order. Figure 2.12 illustrates that for $S_m = 5$ or less, the system has a diversity order equal to 1 for real symbols (which would correspond to a diversity order equal to 2 with complex-valued symbols). However, for higher constellation size, e.g., for $S_m = 7$ and $S_m = 10$, the diversity order is limited to 1=2. This is because when the constellation range increases, the likelihood function becomes flat, which makes the error function $F(t; k)$ subject to the diophantine approximation flat. This result confirms our previous analysis on the impact of the constellation on the likelihood function.

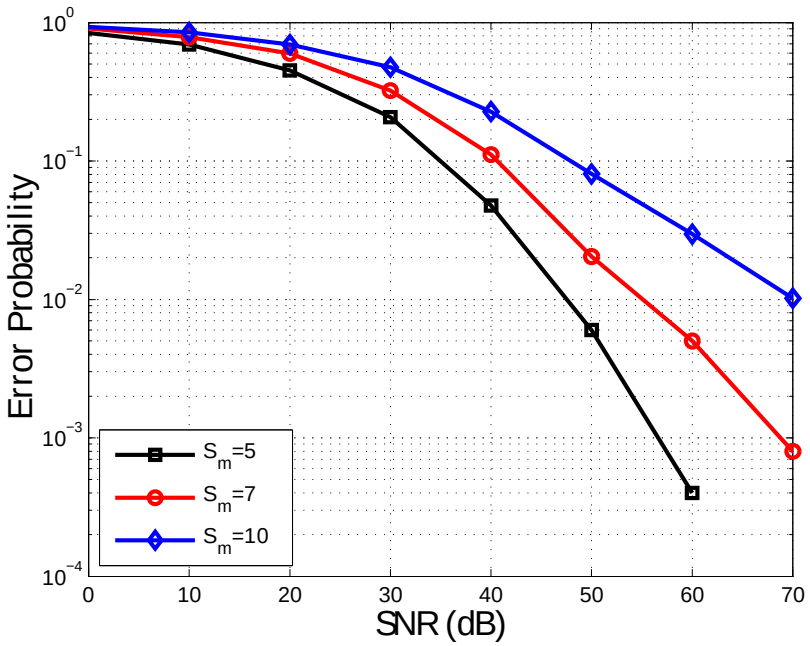


Figure 2.12: Error Probability using the Inhomogeneous Diophantine approximation.

2.10 Conclusion

In this chapter we were interested in the Compute-and-Forward protocol. After an overview on the basic encoding and decoding scheme for this stragey, we provided deeper insights into the practical aspects covering the design of network codes and more importantly optimal decoding approaches. We showed that the design of the optimal network code vector reduces to solve a shortest vector problem. We proposed the complex LLL reduction to solve this problem which allowed as to derive novel bounds on the ergodic rate for the CF and the outage probability. Besides, we focused on the optimal decoding approaches. For the Gaussian channels case we proposed a novel MAP decoding metric using Gaussian lattice distributions and proposed a practical algorithm based on a modified Sphere Decoder. Our numerical results show the effectiveness of the proposed methods and its outperformance compared to the conventional decoder of the CF. For the fading channels, we analyzed the case of multi-dimensional lattices and gave a detailed analysis of the one-dimensional case for which a quasi-ML decoding algorithm based on diophantine approximation was developed and showed to outperform the traditional decoding scheme for the CF.

In this chapter we dealt with the main information-theoretic and communication aspects for the CF scheme considering a basic multiple access channel. The next chapter will be devoted to the implementation of this protocol in a first network scenario which

is the Two-Way Relay Channel. We will be interested in the design of efficient network codes for the CF in this particular network as well as to its end-to-end performance in addition to the Analog Network Coding and Denoise-and-Forward strategies.

Chapter 3

The Two-way Relay channel

In this chapter, we delve into the first network topology we aim to explore in this work, the *Two-Way Relay Channel*. In this network, as shown in Figure 3.1, two nodes N_1 and N_2 desire to exchange their messages via a relay node R. This network model is considered as a basic building block of general wireless networks. It has been extensively studied in literature due to its simple structure, and helped to widen the investigation of the benefits of Network Coding in more general network configurations. In practice, this network can model the communication between two mobile users via an access point or the information exchange between two earth stations via a satellite.

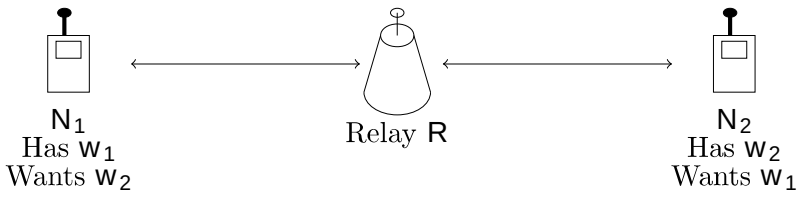


Figure 3.1: Two-Way Relay Channel.

Works on two-way communication between two nodes without a relay node date back to the work of Shannon [109]. In this setting, the two nodes act as transmitters and receivers at the same time to exchange their messages. Main results concerning this setup are information theoretic and provide only inner and outer bounds on the capacity region which is not known in general. Later on, the two-way communication in presence of a relay node without direct links between the nodes has been introduced by Wu *et al.* in [24]. Two-way relaying with direct links has been investigated subsequently in several contributions [110–113]. In this work we are interested in the bidirectional relaying in absence of direct links between the communicating nodes. In this setting, a relay node *in the middle*, that can receive from and transmit to both nodes, intervene to support the end-to-end communication. Transmission from the nodes to the relay is refered to

as the *uplink*, while transmission from the relay to the nodes is refered to as *downlink*.

The traditional routing and relaying protocols require four time slots to achieve the data exchange. The uplink phase lasts two times slots during which each node sends its data to the relay separately. Similarly, the downlink phase lasts two time slots to convey the original data to the nodes. With the introduction of Network Coding, savings in the downlink phase have been allowed. The relay in this case takes only one time slot to broadcast a combination of the original data to both nodes. More interestingly, using Physical-Layer Network Coding, savings at both phases are possible and enable a two-time slots data exchange. In such settings, during the uplink phase, the nodes transmit their data *simultaneously* to the relay and the latter computes and broadcasts, during the downlink phase, a combination of the original messages. Due to the concurrent transmission from the nodes to the relay, the uplink phase is modeled by a *multiple access channel*. Conversely, the downlink phase is modeled by a *broadcast channel with receiver side information* as depicted in Figure 3.2

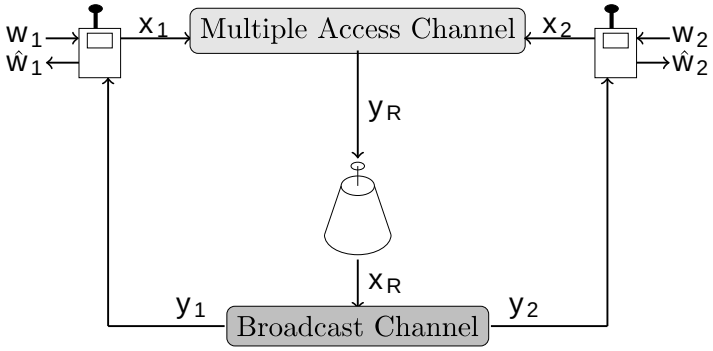


Figure 3.2: Two-phase bidirectional Relaying.

These two channel models have been widely studied over the last few decades. Major contributions are information theoretic and concern the capacity region for conveying messages over a MAC which has been completely characterized in [114, 115] and the capacity region of the broadcast channel identifyied in [116] in the case of stochastically degraded channels. These results have been combined to Physical-Layer Network Coding techniques to derive the achievable rate regions in two-phase bidirectional relaying considering different relaying strategies (Amplify-and-Forward, Denoise-and-Forward, Compute-and-Forward) in the premise of full-duplex nodes [68, 69, 117–120] and half duplex-nodes considering uncoded modulations in [110, 121–123], linear codes in [63, 64, 66, 124, 125] and lattice-based coded schemes in [60, 67]. These contributions provide an upper bound on the capacity of the two-way relay channel and demonstrate that the use of the above cited strategies allow only to approach this bound at high Signal-to-Noise Ratio. The exact capacity of this network is still an open problem.

Motivated by the promising theoretical gains of the lattice based-schemes, we focus on this chapter in the two-phase bidirectional relaying using an $n-$dimensional nested

lattice design $\Lambda = (\Lambda_F; \Lambda_C)$ involving a fine lattice $\Lambda_F \subset R^n$ and a coarse lattice $\Lambda_C \subset R^n$ and consider half-duplex nodes and real-valued channels. Our objective is to analyze the end-to-end performance of the most aknowledged PLNC strategies, mainly, the Denoise-and-Forward (DoF), the Analog Network Coding (ANC) and the Compute-and-Forward. These strategies have been studied previously in literature. However, previous works looked only at the related issues from an information theoretic perspective. We aim in this work to analyze in addition the error performance and to design efficient network codes for the CF strategy. For a complete analysis, we consider the Gaussian and fading two-way relay channels.

The chapter will be organized as follows: section 3.1 is devoted to the Gaussian channels case. First, we will describe the system model and assumptions as well as the performance tools. Processings related to the ANC, DoF and CF will be detailed and the corresponding end-to-end error rate performance and achievable rate using a nested lattice code scheme will be addressed. The fading channels case will be the subject of section 3.2. We will start with introducing the system model and assumptions. Then, we will describe the processing related to the ANC scheme. Afterwards, we focus on the CF scheme. For this protocol, we propose a novel design criterion for optimal network codes in the fading TWRC. Then, we propose a search algorithm based on a modified version of the Fincke-Pohst algorithm [9]. Numerical results evaluating the performance of the proposed approach are provided and show the effectiveness of our method. Finally, a concluding section is dedicated to summarize the results of the present chapter.

3.1 Gaussian Two-Way Relay Channels

3.1.1 System Model and Assumptions

All nodes in the TWRC are equipped with a single antenna and operate in half-duplex mode. The uplink and downlink phases are assumed orthogonal, then they do not interfere with each other.

Nodes N_1 and N_2 deliver respectively length$-k$ messages $w_1 \in F_p^k$ and $w_2 \in F_p^k$ drawn i.i.d from a finite field F_p of prime size p.

Each node is equipped with an encoder $\mathcal{E} : F_p \rightarrow \Lambda$ that implements the function $\square$ to map the finite field messages onto $n-$dimensional codewords $x_1 \in R^n$ and $x_2 \in R^n$ from the nested lattice Λ according to a symmetric power constraint given by:

$$\frac{1}{n} E \left[\| x_i \|^2 \right] \leq P; \quad i = 1; 2 \tag{3.1}$$

During the uplink phase, the nodes transmit their codewords simultaneously to the relay. Under the assumption of a perfect synchronization, the sent vectors arrive at the same time to the relay which observes the output of a MAC in the form:

$$y_R = x_1 + x_2 + z_R \tag{3.2}$$

where $z_R \in \mathbb{R}^n$ stands for the AWGN generated according to $\mathcal{N}\left(0; \sigma_R^2 I_n\right)$.

Due to the superposition of the original codewords, the relay is not able to detect each one of them separately. Rather, using Physical-Layer Network Coding, it will compute a function of them $x_R = f(x_1; x_2)$ satisfying the same power constraint P as the end nodes. This function is afterwards broadcast to N_1 and N_2 during the second phase. Received signal at node N_i for $i = 1; 2$ is given by:

$$y_i = x_R + z_i \tag{3.3}$$

where $z_i \in \mathbb{R}^n$ for $i = 1; 2$ denote the zero mean Gaussian noise of variance σ_i^2. We assume that the uplink and downlink channels are symmetric, then we have $\sigma_R^2 = \sigma_i^2 = \sigma^2$. In addition, we denote by $\gamma = \frac{P}{\sigma^2}$ the Signal-to-Noise Ratio.

From the channel output and given the available side information, node N_1 (respectively N_2) attempts to recover the desired message w_2 (repectively w_1). In practice, node N_i $(i = 1; 2)$ is equipped with a decoder $\mathcal{D}_i$ that outputs an estimate of $\hat{w}_j$ $(j = 2; 1)$ of the original messages w_j. A decoding error occurs if either $\hat{w}_1 \neq w_1$ or $\hat{w}_2 \neq w_2$. The end-to-end probability of error is given then by:

$$P_e \overset{4}{=} \Pr\left(\{\hat{w}_1 \neq w_1\} \cup \{\hat{w}_2 \neq w_2\}\right) \tag{3.4}$$

For coherence with existing works, we will consider the *Sum message error rate* to evaluate the performance of the studied strategies. This performance metric is defined in [126] as the sum of the message error rates at the two nodes and is obtained by the error probability:

$$P_{e;sum} \overset{4}{=} \Pr\left(\hat{w}_1 \neq w_1\right) + \Pr\left(\hat{w}_2 \neq w_2\right) \tag{3.5}$$

And is related to the end-to-end error probability by: $P_{e;sum} \geq P_e$.

From an information theoretic persective, the *exchange rate* characterizes the maximum information that can be reliably exchanged. For a given relaying scheme, the exchange rate $\mathcal{R}_{ex;scheme}$ is defined as the achievable rate per source node per channel use (a channel use signifies the use of the uplink and downlink phases). Assuming symmetric rates for both nodes N_1 and N_2, the exchange rate is equal to the minimum rate between the one achievable during the uplink $\mathcal{R}_{N_i!\ R}$ and that achievable during the downlink $\mathcal{R}_{R!\ N_i}$ according to:

$$\mathcal{R}_{ex;scheme} = \mathcal{R}_{N_1!\ N_2} = \mathcal{R}_{N_2!\ N_1} = \min\left(\mathcal{R}_{N_1!\ R}; \mathcal{R}_{R!\ N_2}\right) \tag{3.6}$$

The *exchange capacity* C_{ex} is the supremum of the exchange rates $\mathcal{R}_{ex;scheme}$ over all possible encoding and decoding schemes.

In literature, a vast portion of works has been devoted to find the exchange capacity of the two-way relay channel. However, research outcomes succeeded only in deriving an upper bound $C_{ex;UB}$ using the cut set bound given by [60]:

$$C_{ex;UB} = \frac{1}{2} \log\left(1 + \frac{P}{\sigma^2}\right) \tag{3.7}$$

In the following paragraph, we will describe in details three strategies used to compute, in the downlink phase, the function x_R. We will also analyze the recovery of desired messages at the end nodes and provide the corresponding exchange rates.

3.1.2 Analog Network Coding Scheme

The Analog Network Coding strategy was studied in several works [5, 6, 117, 121]. Its principle is similar to the amplify-and-forward protocol with the difference that, under Physical-Layer Network Coding, the relay amplifies the superposition of the original codewords. In this case, the relay selects a scalar $\alpha \in \mathbb{R}$ and computes the function:

$$x_R = \alpha y_R \tag{3.8}$$

α is chosen such that the network code vector x_R satisfies the power constraint P. Accordingly, its value is given by:

$$\alpha = \sqrt{\frac{\beta}{1+2\beta}} \tag{3.9}$$

After computing the function x_R, the relay broadcasts it together with the value of α to the end nodes. Node N_i $(i = 1; 2)$ receives, during the downlink phase, the signal:

$$y_i = x_R + z_i = \alpha x_1 + \alpha x_2 + \alpha z_R + z_i \tag{3.10}$$

Now, given this channel output and the receiver side information, each node will first substract each transmitted codeword (scaled by α). Node N_1 gets then:

$$\tilde{y}_1 = y_1 - \alpha x_1 = \alpha x_2 + \alpha z_R + z_1 \tag{3.11}$$

Similarly, N_2 obtains:

$$\tilde{y}_2 = y_2 - \alpha x_2 = \alpha x_1 + \alpha z_R + z_2 \tag{3.12}$$

Then, the decoders $\mathcal{D}_1$ and $\mathcal{D}_2$ implement ML decoding to estimate respectively $\hat{x}_1$ and $\hat{x}_2$ according to:

$$\hat{x}_2 = \underset{x_2 \in \mathcal{C}}{\operatorname{argmin}} \| \tilde{y}_1 - \alpha x \|^2 \;\; ; \;\; \hat{x}_1 = \underset{x_2 \in \mathcal{C}}{\operatorname{argmin}} \| \tilde{y}_2 - \alpha x \|^2 \tag{3.13}$$

Finally, the decoded codewords are mapped to the finite field to get:

$$\hat{w}_2 = \phi^{-1}(\hat{x}_2) \;\; ; \;\; \hat{w}_1 = \phi^{-1}(\hat{x}_1) \tag{3.14}$$

Now, in order to derive the exchange rate under Analog Network Coding strategy, consider the effective Signal-to-Noise Ratio γ_{eq} at end nodes after substraction of codeword side information. Dividing the power of the desired signal by the power of the effective noise in (3.11) and (3.12), we get:

$$\gamma_{eq} = \frac{\alpha^2 P}{\alpha^2 (1 + \alpha^2)} = \frac{\beta}{1+3\beta} \tag{3.15}$$

Then, the achievable exchange rate is given by:

$$\mathcal{R}_{ex;ANC} = \frac{1}{2}\log\left(1+\square_{eq}\right) = \frac{1}{2}\log\left(1+\frac{\square^2}{1+3\square}\right) \tag{3.16}$$

Remark 3.1. In order to derive the exchange rate for the Analog Network Coding, the capacity of a single user AWGN is used with effective Signal-to-Noise Ratio $\square_{eq}$. This is possible in this case for two reasons: first because the downlink channels after substraction of the codewords side information can be modeled by single users AWGN with Gaussian effective noises, second because we perform ML decoding in the downlink phase, which is equivalent to minimum distance decoding in this case.

The Analog Network Coding strategy is simple and easy-to-implement, nevertheless, due to the noise amplification, it may not be the best technique to use particularly in noisy networks. We move in the next paragraph to a noiseless Physical-Layer Network Coding strategy based on the Compute-and-Forward protocol.

3.1.3 Compute-and-Forward Scheme

In the case of the CF strategy, the network code function of the relay is a noiseless sum of the original codewords and consists of:

$$x_R = [x_1 + x_2] \mod \Lambda_C \tag{3.17}$$

Thanks to the modulo operation with respect to the coarse lattice, the decoded function in not only a codeword from the same lattice Λ, but also meets the transmit power requirement at the relay. As described in the previous chapter, in order to decode the desired sum, the relay selects the MMSE scaling factor $\square \in \mathbb{R}$ and performs the following steps:

1. Scale the channel output: $\tilde{y}_R = \square y_R$.
2. Decode to the nearest point in the fine lattice to get an estimate of the sum of the codewords $x_s = x_1 + x_2$: $x_s = Q_{\square_F}(\tilde{y}_R)$.
3. Perform modulo-operation with respect to the coarse lattice to get $x_R = [x_s] \mod \Lambda_C$.

In this Gaussian channel case, the MMSE parameter is given by:

$$\square = \frac{2\square}{1+2\square} \tag{3.18}$$

During the downlink phase, the relay broadcasts its decoded function x_R to the nodes N_1 and N_2. In this case, these nodes will first decode, from their channel outputs y_1 and y_2, the codeword x_R using ML decoding according to:

$$\hat{x}_{R;i} = \underset{\square 2\,\square}{\operatorname{argmin}} \| y_i - \square \|^2 \;\; ; \; i = 2;1 \tag{3.19}$$

Next, given that the decoded vectors belong to the nested lattice code, their mapping back to the finite field generates estimates of the addition of the original finite field messages as:

$$u_i = \varphi^{-1}(\hat{x}_{R;i}) = w_1 \oplus w_2 \; ; \; i = 2;1 \tag{3.20}$$

Finally, each node substracts its message to get the desired one according to:

$$\hat{w}_2 = u_2 \ominus w_1 \; ; \; \hat{w}_1 = u_1 \ominus w_2 \tag{3.21}$$

Now, for what concerns the exchange rate, it has been shown in [60, 67], that the CF strategy allows to achieve the following rate:

$$\mathcal{R}_{ex;CF} = \frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{\sigma^2}\right) \tag{3.22}$$

Although the exchange rate in this scenario allows to approach the upper bound of the exchange capacity at high Signal-to-Noise Ratio, it is still not understood why is the $\frac{1}{2}$ inside the log missing. Two hypotheses were proposed in [60] to explain the origin of this suboptimality: this is due either to the structure of the nested lattice code or to the decoding approach at the relay based on minimum distance decoding which is suboptimal compared to the optimal MAP decoding as discussed in the previous chapter. The first hypothesis was rejected in [60] where authors analyzed the exchange rate of a spherical-shaping lattice design using minimum angle decoding at the relay and Slepian-Wolf coding at the downlink phase and proved that also using this lattice coding scheme, the exchange rate is equal to $\frac{1}{2}\log\left(\frac{1}{2} + \frac{P}{\sigma^2}\right)$. The second hypothesis has not been investigated so far due to the difficuly of the MAP decoder. In our ongoing research we are investigating this research avenue and believe that the tools developed in the previous chapter related to the novel MAP decoding metric, could open the way towards new results and answers to this rate issue.

Remark 3.2. End-to-end decoding errors for the CF scheme depend both on the correctness of the decoding of the sum of codewords at the relay, and the decoding of $\hat{x}_{R;i}$ in the downlink phase at end nodes. The first error type may result from the suboptimality of the minimum distance decoding compared to the MAP decoding as discussed in the previous chapter. The second case is likely to happen since the two downlink channels are perturbed by different noises z_1 and z_2. Then, although end nodes use optimal ML decoding, they may not decode the same combination estimated at the relay's level.

Remark 3.3. The side information at end nodes is used at the messages' level. However, it can be also made at the codewords' level. In this case, after decoding $\hat{x}_{R;i}$ in (3.42), node $N_i (i = 1;2)$ substracts its transmitted codewords x_i from $\hat{x}_{R;i}$ to get $\hat{x}_j = [\hat{x}_{R;i} - x_i] \bmod \Lambda_C$; $(j = 2;1)$, then it maps to the finite field to get $\hat{w}_j = \varphi^{-1}(\hat{x}_j)$. Given that the mapping to the finite field does not impact the decoding correctness, this way to recover the original messages achieves similar performance as the method based on the messages side information.

3.1.4 Denoise-and-Forward Scheme

Similar to the CF, the Denoise-and-Forward strategy is a noiseless Physical-Layer Network Coding technique. It consists of finding the mapping that transforms the received signal at the relay to a noise-free combination of the source signals. Considering the nested lattice coding scheme, the aim is to compute the noiseless addition of the original codewords as:

$$x_R = [x_1 + x_2] \mod \Lambda_C \tag{3.23}$$

Notice that this decoding objective is similar to the CF relaying scheme. Nevertheless, the decoding at the relay is different. In this case, the relay does not scale the channel output by the MMSE factor. Rather, it just performs the following steps:

1. Decode to the nearest point in the fine lattice to get an estimate of the sum of the codewords $x_s = x_1 + x_2$: $x_s = Q_{\square_F}(y_R)$.

2. Perform modulo-operation with respect to the coarse lattice to get $x_R = [x_s] \mod \Lambda_C$.

The processing in the downlink phase is similar to the case of the CF strategy.

The reason to introduce this scheme is to show the impact of the MMSE scaling step distinguishing the DoF from the CF. Indeed, the scaling step allows to achieve higher exchange rate. This can be seen from the exchange rate using the DoF equal to:

$$\mathcal{R}_{ex;DoF} = \frac{1}{2} \log \left(\frac{P}{\square^2} \right) \tag{3.24}$$

From an information theoretic point of view, the DoF is expected to perform like the CF in the asymptotic regime and represent suboptimal performance at low Signal-to-Noise Ratio. From an error rate perspective, the DoF may achieve better performance since in this case, given that the relay does not perform the MMSE scaling, decoding to the nearest point in the fine lattice through step 1 is equivalent to ML decoding, while in the case of the CF, due to the non-Gaussian effective noise resulting from the scaling of the channel ouput, this decoding step is done using minimum distance decoding which is suboptimal compared to the ML decoder. Nevertheless, according to the obtained results in the previous chapter using finite dimensional nested lattice codes, the gain is not expected to be very significant.

3.1.5 Simulation Results

In this section we delve into the numerical results obtained through Monte-Carlo simulations and evaluating the exchange rate and the sum message error rate of the described schemes as functions of the Signal-to-Noise Ratio. We consider the nested lattice coding scheme described in Example 2.1 in the previous chapter. For comparison reasons, we include the exchange rates for the traditional routing that requires 4 time slots refered

to as $\mathcal{R}_{\text{ex;routing}}$ and the one corresponding to the straightforward Network Coding based on 3 times slots transmission refered to as $\mathcal{R}_{\text{ex;netcod}}$ given respectively by:

$$\mathcal{R}_{\text{ex;routing}} = \frac{1}{4}\log\left(1+\frac{P}{\sigma^2}\right) \; ; \; \mathcal{R}_{\text{ex;netcod}} = \frac{1}{3}\log\left(1+\frac{P}{\sigma^2}\right) \tag{3.25}$$

Notice that the $\frac{1}{4}$ and $\frac{1}{3}$ factors result respectively from the use of four and three time slots to perform the messages exchange.

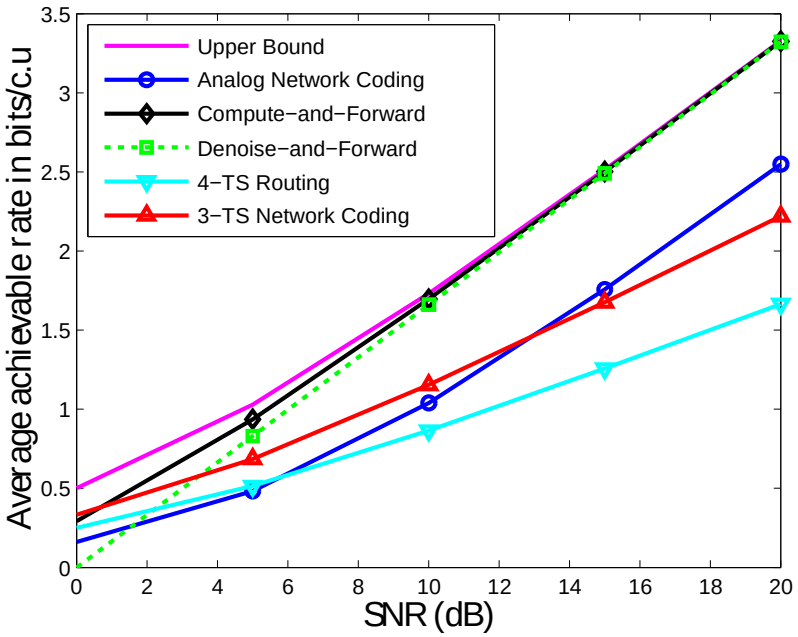


Figure 3.3: Average achievable rate in bits per channel use for the Gaussian TWRC.

Starting with the rate performance depicted in Figure.3.3, numerical results show that the CF allows to approach the upper bound at high Signal-to-Noise Ratio. The ANC however, represents a constant gap to the upper bound. This suboptimality is explained by the noise amplification at the relay's level. In addition, comparing the CF to the DoF, we observe that the former outperforms the latter at low and moderate SNR range. This shows the role played by the MMSE scaling considered in the CF scheme. These numerical results demonstrate also the suboptimality of the traditional routing and the 3-TS Network Coding. This shows the importance of using Physical-Layer Network Coding techniques beyong the standard ways of relaying.

For what concerns the error rate performance, we compare in Figure 3.4 the sum message error rate of the CF, DoF and ANC. Our results show that the CF and the DoF achieve almost the same performance. This result shows that for this setting, the minimum distance decoding and ML decoding are almost similar. Numerical results

show also that the CF outperforms the ANC. The former presents a gap of 3:75dB over the latter at a sum message error rate equal to 10^{-2}. This result confirms again the promised potential of the CF and its outperformance compared to the ANC scheme.

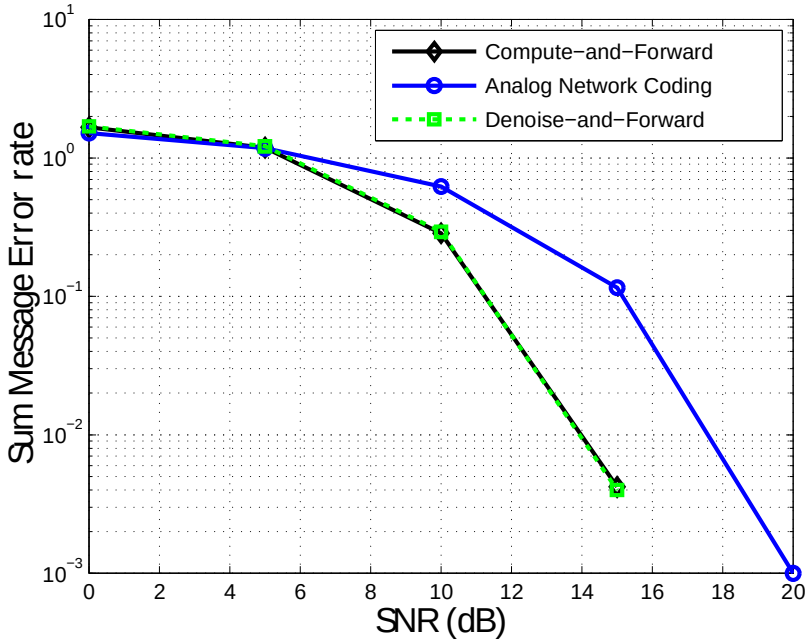


Figure 3.4: Sum Message Error Rate as a function of the SNR for the Gaussian TWRC.

3.2 Fading Two-Way Relay Channels

For what concerns the fading Two-Way Relay Channel, we will study the Analog Network Coding and the CF strategies. Single antenna half-duplex nodes assumptions are also considered in this channel model.

3.2.1 System Model and Assumptions

After encoding their finite field messages w_1 and w_2 onto nested lattice codewords x_1 and x_2 according to the transmit power defined in (3.1), these vectors are transmitted simulateneously to the relay. The channel output at the relay is written as:

$$y_R = h_1 x_1 + h_2 x_2 + z_R \tag{3.26}$$

where $h_1; h_2 \in R$ denote the real-valued fixed channel gains from the node N_1 and N_2 to the relay R respectively and $z_R \in R^n$ according to $\mathcal{N}(0; \sigma_R^2 I_n)$. Let $h = [h_1\ h_2]^t$ be the channel vector. We assume that channel state information is only available at the receiver, i.e. during the uplink phase, the relay knows the channel vector h.

During the downlink phase, the relay computes a network code function $x_R = f(x_1; x_2)$ according to the same transmit power and broadcasts it to the nodes N_1 and N_2. Received signal at node N_i $(i = 1; 2)$ is written as:

$$y_i = h_i x_R + z_i \tag{3.27}$$

where $z_i \in R^n$ denotes a zero mean AWGN of variance σ_i^2. The uplink and downlink channels are assumed symmetric, i.e., the nodes are subject to the same transmit power requirements, the channel fading coefficients are identical and the noises have the same variances $\sigma_R^2 = \sigma_i^2 = \sigma^2$. Given the channel state information at the receiver, during the downlink phase, node N_1 (respectively N_2) is assumed to know h_1 (respectively h_2). In addition, we define the Signal-to-Noise Ratio as $= \frac{P}{\sigma^2}$.

End nodes use their side information to estimate from their channel outputs the desired messages. Performance tools to be used in this channel model are the same we considered in the previous section for the Gaussian channel case. For what concerns the exchange capacity, it is also unkown for the fading channel case. Only an upper bound is provided using the cut set bound as:

$$\mathcal{R}_{ex;UB} = \min_{m=1;2} \log \left(1 + h_m^2 \frac{P}{\sigma^2}\right) \tag{3.28}$$

We will in the following describe the schemes based on the ANC and the CF.

3.2.2 Analog Network Coding Scheme

Under the ANC scheme, the computed network code at the relay is a scaled version of its channel input $x_R = y_R$ where is chosen according to the transmit power constraint P. For the fading channel case, its value is equal to:

$$= \sqrt{\frac{}{1 + \| h \|^2}} \tag{3.29}$$

After computation of x_R, the relay broadcasts during the donwlink phase both this function and the factor to the end nodes. Channel outputs at node N_1 and N_2 are given as:

$$y_1 = h_1 x_R + z_1 = h_1^2 x_1 + h_1 h_2 x_2 + h_1 z_R + z_1 \tag{3.30}$$

$$y_2 = h_2 x_R + z_2 = h_2^2 x_2 + h_1 h_2 x_1 + h_2 z_R + z_2 \tag{3.31}$$

Given these channel outputs, the codeword side information, the knowledge of the channel gains h_1 at the node N_1 and h_2 at N_2 and the knowledge of , end nodes will first substract their transmitted codewords (weighted by the values of and the corresponding channel coefficients). N_1 gets then:

$$\tilde{y}_1 = y_1 - h_1^2 x_1 = h_1 h_2 x_2 + h_1 z_R + z_1 \tag{3.32}$$

Similarly, N_2 obtains:

$$\tilde{y}_2 = y_2 - \square h_2^2 x_2 = \square h_1 h_2 x_1 + \square h_2 z_R + z_2 \tag{3.33}$$

Next, decoders $\mathcal{D}_1$ and $\mathcal{D}_2$ available at the nodes N_1 and N_2 respectively, implement ML decoding to recover estimates of the original codewords according to:

$$\hat{x}_2 = \underset{\square 2 \square}{\operatorname{argmin}} \parallel \tilde{y}_1 - \square h_1 h_2 \square \parallel^2 \;\; ; \;\; \hat{x}_1 = \underset{\square 2 \square}{\operatorname{argmin}} \parallel \tilde{y}_2 - \square\square \parallel^2 \tag{3.34}$$

Finally, the decoded codewords are mapped to the finite field to get:

$$\hat{w}_2 = \square^{\square 1}(\hat{x}_2) \;\; ; \;\; \hat{w}_1 = \square^{\square 1}(\hat{x}_1) \tag{3.35}$$

By computing the effective Signal-to-Noise Ratio in the downlink phase after substraction of the codewords side information, it is easy to show that the exchange rate under the ANC scheme is equal to:

$$\mathcal{R}_{ex;ANC} = \min_{m=1;2} \frac{1}{2} \log \square 1 + \frac{h_m^2 \square^2}{1 + \square(1 + \parallel h \parallel^2)} \square \tag{3.36}$$

3.2.3 Compute-and-Forward Scheme

3.2.3.1 Processing at the relay

Under the CF strategy, the relay exploits the linear structure of the lattice design and computes x_R as an integer linear combination of the original codewords in the form:

$$x_R = [a_1 x_1 + a_2 x_2] \mod \Lambda_C \tag{3.37}$$

where the coefficients $a_1; a_2 \in Z$ form the network code vector $a = [a_1 \; a_2]^t$. Given the integer nature of these coefficients, the combination $a_1 x_1 + a_2 x_2 \in \Lambda_F$ belongs to the fine lattice, and with the modulo-lattice operation, it is ensured that the vector x_R satisfies the transmit power requirement imposed by the coarse lattice. In the finite field, this combination is associated to the sum u of the original messages such that:

$$u = \square^{\square 1}(x_R) = q_1 x_1 \oplus q_2 x_2 \tag{3.38}$$

where the finite field coefficients are related to the integer network code coefficients by: $q_i = g^{\square 1}([a_i] \mod p) \;\; ; \;\; i = 1; 2$. In order to compute the function x_R, the relay selects a scaling factor $\square$ and a network code vector a and performs the following steps:

1. Scale the channel output: $\tilde{y}_R = \square y_R$.
2. Decode to the nearest point in the fine lattice to get an estimate of the integer combination $x_c = a_1 x_1 + a_2 x_2 : x_c = Q_{\square_F}(\tilde{y}_R)$.
3. Perform modulo-operation with respect to the coarse lattice: $x_R = [x_c] \mod \Lambda_C$.

As discussed in the previous chapter, the optimal relay's parameters are chosen such that the computation rate at the relay is maximized. The optimal scaling parameter is the MMSE factor equal to:

$$\alpha = \frac{< h^t; a >}{1 + \| h \|^2} \tag{3.39}$$

This value results in a computation rate in the uplink phase $\mathcal{R}_{N_i \to R}$ equal to:

$$\mathcal{R}_{N_i \to R} = \frac{1}{2} \log^+ \left(\|a\|^2 - \frac{| h^t a |^2}{1 + \| h \|^2} \right)^{-1} \tag{3.40}$$

Accordingly, the optimal network code vector that allows to maximize the computation rate at the relay is a solution of the minimization problem given by:

$$a_{opt} = \underset{a \neq 0}{\operatorname{argmin}} \, a^t G a \tag{3.41}$$

where $G = I_2 - \frac{\alpha}{1+\alpha \|h\|^2} h h^t$ is a definite positive matrix in $R^{2 \times 2}$ studied in previous chapter in Theorem 2.2. The optimal network code vector corresponds to the coordinates of the shortest vector in the lattice Λ_G of Gram matrix G.

3.2.3.2 Processing at end nodes and decodability condition

During the downlink phase, the relay broadcasts both the network code vector a and the computed function x_R to the end nodes. Upon receiving the channel output, N_1 and N_2 first decode the codeword x_R using ML decoding according to:

$$\hat{x}_{R;i} = \underset{\lambda \in \Lambda_i}{\operatorname{argmin}} \, \| y_i - h_i \lambda \|^2 \;\; ; \; i = 2; 1 \tag{3.42}$$

Then, given that the estimated codewords belong to the nested lattice, N_1 and N_2 use the mapping φ^{-1} to map them back to the finite field in order to get estimates on the finite field combinations such that:

$$u_i = \varphi^{-1}(\hat{x}_{R;i}) = q_1 w_1 \oplus q_2 w_2 \; ; \; i = 1; 2 \tag{3.43}$$

where $q_1 = g^{-1}([a_1] \mod p) \, ; q_2 = g^{-1}([a_2] \mod p)$ are known at both nodes from the values of the network code vector a broadcast during the downlink phase. Next, each node substracts its message side information weighted by finite field coefficient. N_1 gets:

$$n_1 = u_1 \ominus q_1 w_1 = q_2 w_2 \tag{3.44}$$

Similarly, N_2 deduces:

$$n_2 = u_2 \ominus q_2 w_2 = q_1 w_1 \tag{3.45}$$

Finally, nodes recover estimates of their desired messages by inverting (divisions are performed over the finite field F_p.) by the opposite finite field coefficient such that:

$$\hat{w}_2 = \frac{n_1}{q_2} \; ; \; \hat{w}_1 = \frac{n_2}{q_1} \tag{3.46}$$

It is clear that in order to enable both nodes N_1 and N_2 recover the desired messages, the finite field coefficients q_1 and q_2 should be non-zero, meaning that the network code vector a should satisfy: $[a_1] \mod p \neq 0$ and $[a_2] \mod p \neq 0$ at the same time. However, the optimization problem in (3.41) rejects only the values in the form $[a_1\ 0]^t$ or $[0\ a_2]^t$ which are not sufficient to guarantee recovering both messages at the two nodes. In order to adapt this local optimization problem to the Two-Way Relay network, we propose in Lemma 3.1 a new optimization problem for finding the optimal network code vector for the CF taking into account the non-zero condition over the finite field.

Lemma 3.1. *For the real-valued fading Two-Way Relay Channel using the Compute-and-Forward strategy, the optimal network code coefficient vector is a solution to the minimization problem:*

$$a_{opt} = \underset{\substack{[a_1] \mod p \neq 0 \\ [a_2] \mod p \neq 0}}{\operatorname{argmin}} a^t G a \tag{3.47}$$

It corresponds to a shortest vector in the lattice Λ_G of Gram matrix G having non-zero entries modulo the field size p.

If the network code vector satisfies this non-zero entries condition, the exchange rate for the CF is equal to:

$$\mathcal{R}_{ex;CF} = \frac{1}{2}\log^+\left(\|a\|^2 - \frac{|h^t a|^2}{1+\|h\|^2}\right) \tag{3.48}$$

Otherwise, it is equal to 0. In addition, we know from (2.36) that the exchange rate is equal to zero for integer vectors satisfying:

$$\|a\|^2 \geq 1 + \|h\|^2 \tag{3.49}$$

In the previous chapter, we suggested two tools to solve for the shortest vector problem: lattice reduction techniques and the Fincke-Pohst algorithm. Under the Two-Way Relay Channel settings, lattice reduction techniques are not well suited since they do not guarantee the additional non-zero constraint. We propose then in the following to use the Fincke-Pohst algorithm.

Solving the optimization problem in (3.47) consists in finding the integer vector $a \in Z^2$ having non-zero coordinates modulo p such that the metric $a^t G a$ is minimized. Let $G = R^t R$ be the Cholesky decomposition of the definite positive matrix G where R is an upper triangular real matrix. Minimization problem in (3.47) is equivalent to:

$$a_{opt} = \underset{\substack{[a_1] \mod p \neq 0 \\ [a_2] \mod p \neq 0}}{\operatorname{argmin}} \|Ra\|^2 \tag{3.50}$$

Given that the exchange rate is equal to zero for the condition mentioned in (3.49), the search space can be limited to the set $\Gamma_a = \{a \in Z^2; \|a\|^2 \leq 1 + \square\|h\|^2\}$.

The obvious method to solve the minimization problem in (3.50) is to perform an exhaustive search over Γ_a and seek the integer vector that minimizes $\|Ra\|^2$ under the non-zero condition. However, this search method leads to an increasing complexity specially at high SNR values. The idea is to reduce the search space to the sphere of radius $C > 0$ such that $\|Ra\|^2 \leq C$. This is the philosophy of the Fincke-Pohst algorithm. In our settings, we will include to the standard Fincke-Pohst approach the non-zero constraint and the search space condition taking into consideration only the integer vectors in Γ_a. Our proposed algorithm is developed in the next paragraph.

3.2.4 Modi□ed Fincke-Pohst for Optimal Network Codes Search

Let $R_{ij}; i; j = 1; 2$ denote the entries of the matrix R, then we can write:

$$\begin{aligned} a^t G a &= \|Ra\|^2 \\ &= (R_{11}a_1 + R_{12}a_2)^2 + (R_{22}a_2)^2 \\ &= u_{11}(a_1 + u_{12}a_2)^2 + u_{22}a_2^2 \end{aligned} \tag{3.51}$$

where $u_{ii} = R_{ii}; i = 1; 2$ and $u_{12} = \frac{R_{12}}{R_{11}}$. Accordingly, to satisfy $\|Ra\|^2 \leq C$ is equivalent to consider the following inequalities:

$$\begin{cases} u_{22}a_2^2 \leq C \\ u_{11}(a_1 + u_{12}a_2)^2 + u_{22}a_2^2 \leq C \end{cases} \tag{3.52}$$

These conditions lead to the following boundaries requirements on the coefficients a_1 and a_2:

$$-\sqrt{\frac{C}{u_{22}}} \leq a_2 \leq \sqrt{\frac{C}{u_{22}}} \tag{3.53}$$

$$-\sqrt{\frac{C - u_{22}a_2^2}{u_{11}}} - u_{12}a_2 \leq a_1 \leq -\sqrt{\frac{C - u_{22}a_2^2}{u_{11}}} - u_{12}a_2 \tag{3.54}$$

After choosing the sphere radius C, we start with searching the coefficient a_2. Refering to (3.53) and given the integer nature of a_2 we get:

$$LB_2 \leq a_2 \leq UB_2 \tag{3.55}$$

with

$$LB_2 = \left\lceil -\sqrt{\frac{C}{u_{22}}} \right\rceil ; \; UB_2 = \left\lfloor \sqrt{\frac{C}{u_{22}}} \right\rfloor \tag{3.56}$$

Then, the value of a_2 is chosen such that the bound requirements in (3.55)-(3.56) are satisfied and that $[a_2] \bmod p \neq 0$.

Once the values of a_2 is found, we proceed by seeking the value of the coefficient a_1. From (3.54) we get:

$$LB_1 \leq a_1 \leq UB_1 \tag{3.57}$$

with

$$LB_1 = \left\lceil -\sqrt{\frac{C - u_{22}a_2^2}{u_{11}}} - u_{12}a_2 \right\rceil \; ; \; UB_1 = \left\lfloor -\sqrt{\frac{C - u_{22}a_2^2}{u_{11}}} - u_{12}a_2 \right\rfloor \tag{3.58}$$

Accordingly, the coefficient a_1 is chosen such that the bounds requirements in (3.57)-(3.58) are satisfied and $[a_1] \bmod p \neq 0$.

The coefficients a_1 and a_2 are then selected as follows: first we choose the coefficient a_2 satisfying the bounds requirements in (3.55)-(3.56) and $[a_2] \bmod p \neq 0$. For this value, we choose the coefficient a_1 that meets the bounds in (3.57)-(3.58) and $[a_1] \bmod p \neq 0$. If such coefficient does not exist, we repeat the previous step and select another coefficient a_2. The process is repeated until we find a coefficient a_1 fulfilling the required conditions. When both coefficients are found, we check if the resulting vector a belongs to the set Γ_a. If this condition is satisfied, a candidate to our optimization problem is found. Afterwards, we select among the obtained candidates the one that results in the smallest value of the quadratic form $a^t G a$. We summarize our proposed algorithm to find the optimal network code vector for the two-way relay channel in Appendix 5.E.

Remark 3.4. An importance parameter in our proposed approach is the initial sphere radius C. In order to guarantee the existence of at least a lattice point inside the sphere over which is searched the integer vector a, we consider C according to [127] such that:

$$C = \min\left(\mathrm{diag}\left(G\right)\right) \tag{3.59}$$

3.2.5 Simulation Results

We move now to the numerical results to evaluate the performance of the ANC strategy and the proposed algorithm to find the optimal network code vector for the CF strategy. First of all, in order to demonstrate the importance of our Lemma 3.1 and the necessity to take the non-zero contraint into account while looking for the optimal network code vector for the CF, we studied, through averaging over 10000 random channel realizations, the probability of having zero entries. Obtained results depicted in Figure 3.5 show indeed that the non-zero constraint is not negligeable. For example, for SNR $\leq$ 15dB, the probability of zero-entries is always higher than 0:4.

Besides, we evaluated the *exchange rate* and the *sum message error rate* for the ANC, the CF with network code vector found according to the local optimization problem in (3.41) and the CF based on our proposed algorithm to find the optimal network code vector such that non-zero entries contraints are satisfied. For the coding scheme, we considered the nested lattice code described in Example 2.1. Numerical results plotted

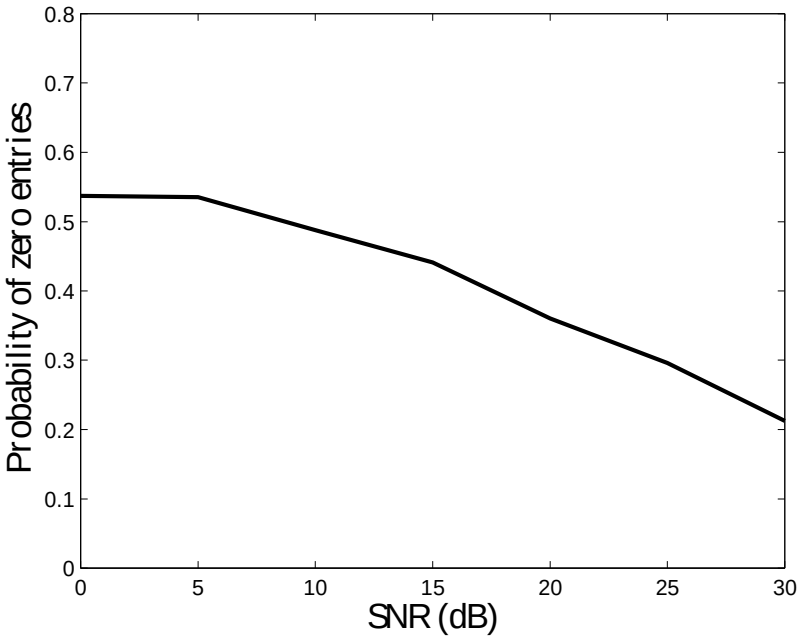


Figure 3.5: Probability of non-zero entries.

in Figure 3.6 and Figure 3.7 confirm the performance degradation when the non-zero condition is not respected. The efficiency of our proposed algorithm is also demonstrated. Our method brings a rate gain of about 0:5 bits/c.u and a gain of more than 15dB at high SNR values over the CF based on the local optimization criterion at the relay's level. Besides, our method allows to approach the upper bound on the exchange rate. For what concerns the ANC, our results confirm the outperformance of the CF over this strategy as far as the exchange rate is concerned. Nevertheless, we note that both protocols achieve almost same error performance unlike the Gaussian channel case. This difference in the perfromance gap is due to the main issue regarding the CF in fading channels: the channel quantization or approximation. Indeed, the approximation errors impact the performance of this strategy. This issue was studied in recent works [86, 87] where the sensitivity of the CF to channel quantization errors have been studied and an alternative solution based on precoding at the transmitters assuming a global channel state information has been proposed to remedy to the impact of approximation errors.

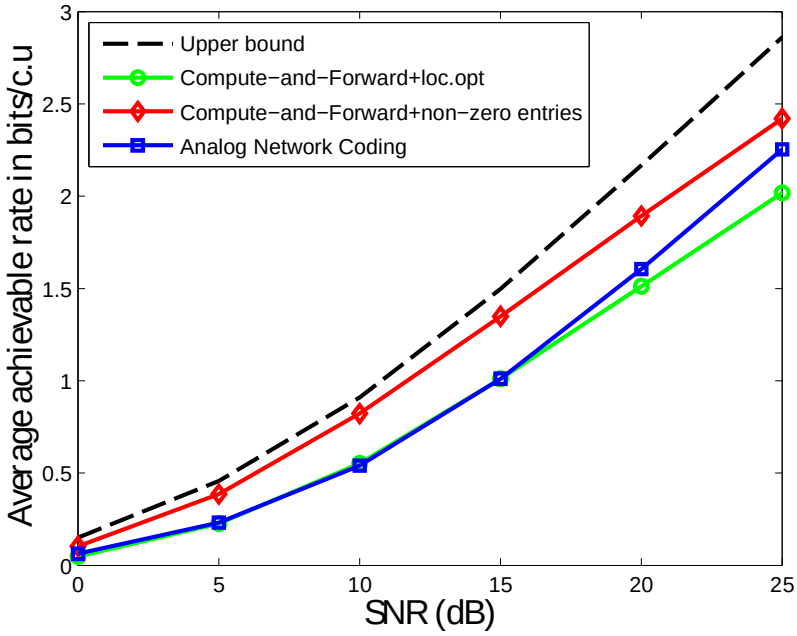


Figure 3.6: Average achievable rate in bits per channel use for the fading TWRC.

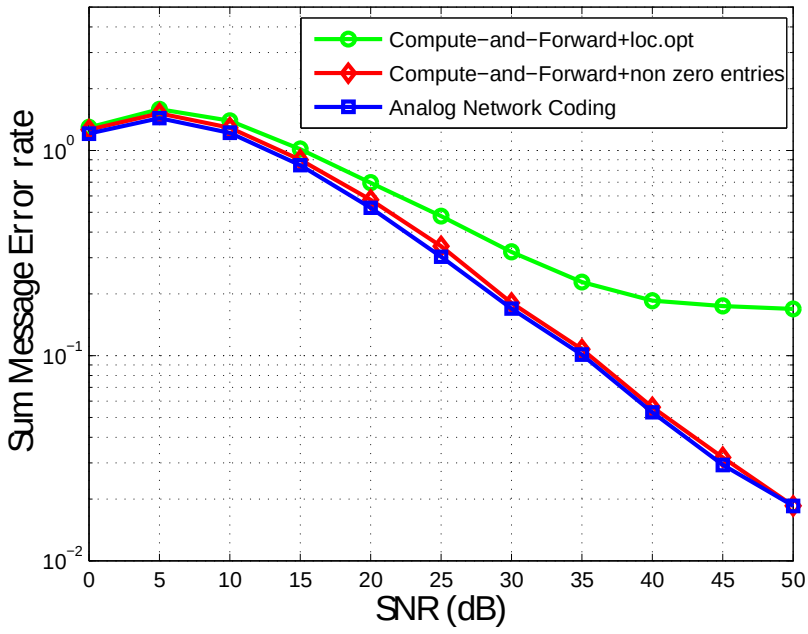


Figure 3.7: Sum Message Error Rate for the fading TWRC.

3.3 Conclusion

This chapter was dedicated to study Physical-Layer Network Coding strategies in the Two-Way Relay Channel. For what concerns the Gaussian channels case, we analyzed the end-to-end performance of the ANC, DoF and CF. Our numerical results show the outperformance of the CF over other strategies and demonstrate the potential of PLNC techniques over the traditional routing strategies. For what concerns the fading channel case, we provided a new lemma to design efficient network codes for the CF and developed a search algorithm based on a modified Fincke-Pohst version. Effectiveness of the proposed method is confirmed by numerical results.

The two-way relay channel has been widely studied in literature. Further research effort should be put to extend the Physical-Layer Network Coding techniques, that have been mainly studied in the case of the TWRC, to other network topologies. This is the objective of the next chapter through the investigation of the Multi-Source Multi-Relay channels configuration.

Chapter 4

The Multi-Source Multi-Relay channel

In this chapter we aim to explore Physical-Layer Network Coding strategies in a second network topology, the *Multi-Source Multi-Relay channel* (MSMR). In this network, as shown in Figure 4.1, N source nodes $S_1; ...; S_N$ desire to communicate their messages to a common destination D via N intermediate relay nodes $R_1; ...; R_N$.

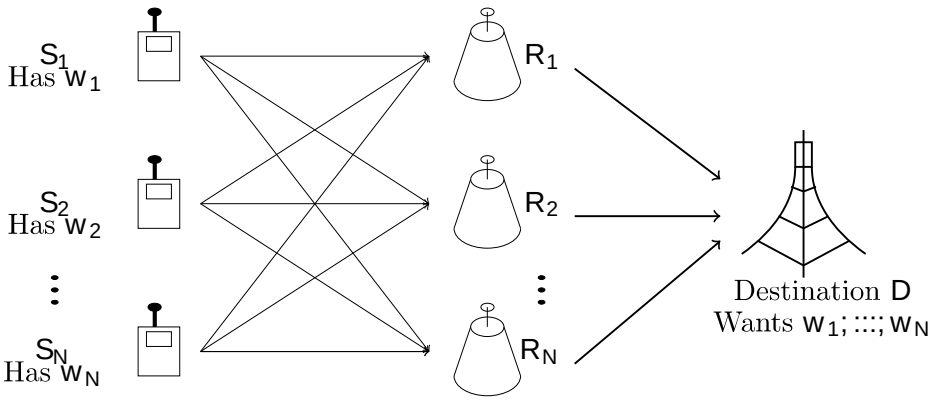


Figure 4.1: Multi-Source Multi-Relay Channel.

This network model arises in several practical communication systems such as cellular networks (e.g., LTE advanced and 802.16j standards) and wireless sensor networks (WSNs). In the first example, relay stations help to forward information from mobile stations (User Equipments) to a common eNode-B (Base station) allowing effective extension of the service coverage and enhancement of the system throughput. In the second example, and particularly for long distance transmissions in WSNs, several intermediate sensors are configured to act as relays to communicate the data measured by source sensors to a common remote central processor in an energy efficient way allowing to prolong the network lifetime.

In contrast to the two-way relay channel, the MSMR channel has not been widely investigated in literature. We aim in this chapter to study the network codes design and the end-to-end performance of the ANC and CF in the real-valued fading Multi-Source Multi-Relay channel considering lattice-based coding schemes. In section 4.1 we describe the system model and assumptions. Then, in section 4.2 we analyze the end-to-end communication based on ANC. We proceed in section 4.3 with the CF scheme. For this protocol, we propose a novel optimization problem to search for the optimal network codes that allow to maximize the overall message rate at the destination and propose in section 4.4 search algorithms based on a modified version of the Ficke-Pohst algorithm. Numerical results evaluating the performance of our approach are provided in section 4.5 and demonstrate the effectiveness of our method. Finally, a concluding section will be dedicated to summarize the present chapter.

4.1 System Model and Assumptions

All nodes in the network are equipped with a single antenna and operate in half duplex mode. In absence of direct links from the sources to the destination, messages transmission is performed in two phases: a *multiple access phase* and an *orthogonal access phase*. The first phase concerns the transmissions from the sources to the relays. Interested in PLNC techniques, we enable the sources $S_1;:::;S_N$ to transmit at the same time, this phase lasts then one time slot. Each relay, observing the superposition of source signals, computes a network code function and transmits it during a separate time slot to the destination assuming perfect point-to-point link from each relay to the destination, i.e., the destination obtains exactly the computed functions at the relays. The second phase lasts then N time slots.

During the first phase, each source S_i delivers a length-k message w_i drawn i.i.d from a prime size field F_p according to a uniform distribution. Each source is equipped with an encoder $\mathcal{E}$ that implements the one-to-one function $\square$ to map the message w_i to an $n-$dimensional lattice codeword x_i from the nested lattice $\Lambda = (\Lambda_F;\Lambda_C)$ involving a fine lattice $\Lambda_F \in R^n$ and a coarse lattice $\Lambda_C \in R^n$. Λ_F is the coding lattice from which are carved the codewords, and Λ_C acts to satisfy the shaping region imposed by the power constraint given by:

$$\frac{1}{n}E\left[\| x_i \|^2\right] \leq P \tag{4.1}$$

for $P > 0$ and $i = 1;:::;N$. The message rate is equal to $r = \frac{k}{n}\log p$.

After encoding their messages, the sources transmit simultaneously their codewords through the channel. This concurrent transmission together with the broadcast nature of the wireless medium makes the codeword of each source reach all the relay nodes. Each relay R_m receives thus a superposition of the original codewords modeled as an

output of a multiple access channel in the form

$$y_m = \sum_{i=1}^{N} h_{im} x_i + z_m \tag{4.2}$$

where $h_{im} \in \mathbb{R}$ denotes the real channel coefficient between the source S_i and the relay R_m assumed fixed during the transmission of entire codewords, $z_m \in \mathbb{R}^n$ is a zero-mean Additive White Gaussian Noise of variance generated i.i.d according to $\mathcal{N}(0; \sigma^2 I_n)$. We assume that channel state information is available only at the receiver, i.e. each relay R_m knows only its corresponding channel vector $h_m = [h_{1m} \dots h_{Nm}]^t$. In addition, we assume that the destination knows all the channel vectors $h_1, \dots, h_N$. Furthermore, we denote by γ the Signal-to-Noise Ratio equal to $\gamma = \frac{P}{\sigma^2}$.

The second phase concerns the transmissions from the relays to the destination. Using Physical-Layer Network Coding, each relay decodes, from its channel output y_m, a linear network code as a function of the original codewords $u_m = f(x_1, \dots, x_N)$ such that the transmit power at the relays P is satisfied. Assuming an orthogonal access to the destination, after computation, each relay forwards its function to the destination during a separate time slot. Given an enough set of equations $(u_1, \dots, u_N)$ with appropriate conditions, the destination D can recover the original messages.

The destination is equipped with a decoder $\mathcal{D} : \mathbb{R}^n \to \mathbb{F}_p$ that outputs estimates $\hat{w}_1, \dots, \hat{w}_N$ of the desired messages. A decoding error occurs if $\hat{w}_i \neq w_i, \forall i = 1, \dots, N$. We say that a message w_i can be recovered at rate r_i if for any $\varepsilon > 0$ and n large enough, there exist a decoder $\mathcal{D}$ such that:

$$\begin{aligned} \hat{w}_i &\overset{4}{=} \mathcal{D}(u_1, \dots, u_N) \\ &\Pr(\hat{w}_i \neq w_i) < \varepsilon \end{aligned} \tag{4.3}$$

The message error probability at the destination is defined as:

$$P_D = \Pr\left[\bigcup_{i=1}^{N} \hat{w}_i \neq w_i\right] \tag{4.4}$$

We are interested in this work in two PLNC schemes not studied previously in the Multi-Source Multi-Relay channel model: the Analog Network Coding and the Compute-and-Forward. We will analyze in the following the processing at the relays and the destination for each scheme.

4.2 Analog Network Coding Scheme

4.2.1 Processing at the relays

The role of a relay node under the ANC strategy is to amplify and forward its received signal. The network code function in this case is a scaled version of the superposition

of the original codewords. For this purpose, each relay R_m selects a parameter β_m and computes the function α_m as:

$$\alpha_m = \beta_m y_m = \beta_m \left(\sum_{i=1}^{N} h_{im} x_i + z_m \right) \tag{4.5}$$

The value of the scaling factor is chosen such that the resulting function α_m satisfies the power constraint P. Accodingly, the scaling parameter for relay R_m is given by:

$$\beta_m = \sqrt{\frac{\square}{1 + \square \| h_m \|^2}} \; ; \; m = 1; \ldots; N \tag{4.6}$$

After computation, each relay transmits both its decoded function and the amplification parameter to the destination in a separate time unit.

4.2.2 Processing at the destination and decodability condition

Assuming perfect links from the relays to the destination, the latter receives at the end of the second transmission phase all functions $\alpha_1; \ldots; \alpha_N$ and parameters $\beta_1; \ldots; \beta_N$. Given the expressions of the network code functions, we can write the following system at the destination:

$$\underbrace{\begin{pmatrix} \square_1^t \\ \square_2^t \\ \vdots \\ \square_N^t \end{pmatrix}}_{L} = \underbrace{\begin{pmatrix} \square_1 h_{11} & \square_1 h_{21} & \cdots & \square_1 h_{N1} \\ \square_2 h_{12} & \square_2 h_{22} & \cdots & \square_2 h_{N2} \\ \vdots & \vdots & \vdots & \vdots \\ \square_N h_{1N} & \square_N h_{2N} & \cdots & \square_N h_{NN} \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} x_1^t \\ x_2^t \\ \vdots \\ x_N^t \end{pmatrix}}_{X} + \underbrace{\begin{pmatrix} \square_1 z_1^t \\ \square_2 z_2^t \\ \vdots \\ \square_N z_N^t \end{pmatrix}}_{Z} \tag{4.7}$$

where the rows of the matrix $L \in \mathbb{R}^{N \times n}$ are the functions (transposed) computed at the different relays, the matrix $X \in \mathbb{R}^{N \times n}$ is composed of the codewords sent by the source nodes, $Z \in \mathbb{R}^{N \times n}$ is the real matrix whose rows correspond to the scaled noise vectors at the relays and the matrix $B \in \mathbb{R}^{N \times N}$. Given these definitions, system (4.7) can be written in a matrix form as:

$$L = BX + Z \tag{4.8}$$

Assuming that the noise vectors at the different relays $z_1; \ldots; z_N$ are independent, it is easy to show that the noise Z is Gaussian of covariance matrix Σ equal to:

$$\Sigma = \begin{pmatrix} \square_1^2 \square^2 I_n & 0_n & \cdots & 0_n \\ 0_n & \square_2^2 \square^2 I_n & \cdots & 0_n \\ \vdots & \vdots & \ddots & \vdots \\ 0_n & \cdots & \cdots & \square_N^2 \square^2 I_n \end{pmatrix} \tag{4.9}$$

Additionally, given the availibility of the coefficients $\beta_m; m = 1; \ldots; N$ and the vectors $h_1; \ldots; h_N$, the matrix B is known at the destination. Based on that, recovery of original messages is performed in two steps as follows:

1. Solve for the codewords matrix $\hat{X}$ in the system (4.8) and get estimates of the original codewords $\hat{x}_1; \ldots; \hat{x}_N$.

2. Map the obtained vectors to the finite field using the mapping $\square^{-1}$ to get estimates on the desired messages as: $\hat{w}_i = \square^{-1}(\hat{x}_i)$, for $i = 1; \ldots; N$.

For the first step, the destination performs a simple inversion by the matrix B to get:

$$\hat{X} = B^{-1} L \tag{4.10}$$

This operation requires that the matrix B be of full rank (invertible). This is possible if its determinant is non-zero over R. Let $B_{i;j}; (i; j = 1; \ldots; N)$ denote the elements of the matrix B. Then we have :

$$\det(B) = \sum_{s \in S_n} \varepsilon(s) \prod_{i=1}^{N} B_{s(i);i} \tag{4.11}$$

where S_n denotes the set of all permutations in $\{1; \ldots; N\}$ and $\varepsilon(s)$ is the signature of the permutation s which is equal to 1 if it is an even permutation and -1 if it is an odd permutation. According to the expression of B, we have $B_{i;j} = \square_i h_{j;i}; i; j = 1; \ldots; N$, then (4.11) is equivalent to:

$$\begin{aligned}
\det(B) &= \sum_{s \in S_n} \varepsilon(s) \prod_{i=1}^{N} \square_i h_{s(i);i} \\
&= \sum_{s \in S_n} \varepsilon(s) \left(\prod_{i=1}^{N} \square_i \right) \left(\prod_{i=1}^{N} h_{s(i);i} \right) \\
&= \left(\prod_{i=1}^{N} \square_i \right) \sum_{s \in S_n} \varepsilon(s) \prod_{i=1}^{N} h_{s(i);i} \\
&= \left(\prod_{i=1}^{N} \square_i \right) \det(H)
\end{aligned} \tag{4.12}$$

where the rows of the matrix $H \in R^{N \times N}$ are the vectors h_i^t that correspond to the channel gains between the sources and relay R_i for $i = 1; \ldots; N$. Given that these vectors are independent, the matrix H is full rank with high probability (close to one). And since $\square_i \neq 0; \forall i = 1; \ldots; N$, we deduce that the full rank condition on the matrix B is satisfied.

This way to estimate the original codewords is advantageous in the sense that it is easy to implement, however, as we can observe, the inversion by the matrix B results in amplification of the noise Z which is already an amplified version of the noise accumulated at each relay node. We expect that this noise enhancement lead to poor performance at the destination. Additionally, compared to the case of the Two-Way Relay Channel where the processing at the destination under the ANC strategy is based

on ML decoding, we expect that the performance gap between the ANC and the CF will be more significant in the Multi-Source Multi-Relay channel case based on a suboptimal decoding approach at the destination.

4.3 Compute-and-Forward Scheme

4.3.1 Processing at the relays

Using the CF strategy, each relay R_m attempts to compute, from the channel output y_m, a linear integer combination of the original codewords in the form:

$$\lambda_m = \left[\sum_{i=1}^{N} a_{mi} x_i\right] \mod \Lambda_C \tag{4.13}$$

where the coefficients $a_{m1}, \ldots, a_{mN} \in Z$ form the network code vector $a_m = [a_{m1} \ldots a_{mN}]^t$ for relay R_m. Given the integer nature of these coefficients and the linear structure of the lattice coding scheme, the combination $\lambda_{m;F} = \sum_{i=1}^{N} a_{mi} x_i$ belongs to the fine lattice Λ_F. The modulo-lattice operation guarantees that the computed functions meet the transmit power constraint P at the relays. In the finite field, λ_m is associated to the finite field combination u_m of the original messages in the form:

$$u_m = \varphi^{-1}(\lambda_m) = \sum_{i=1}^{N} q_{mi} w_i \tag{4.14}$$

where the coefficients $q_{mi} \in F_p$ are given by: $q_{mi} = g^{-1}([a_{mi}] \mod p)$.

Each relay R_m is equipped with a decoder $\mathcal{D}_m$ that decodes an estimate $\hat{\lambda}_m$ of the desired combination. After selection of a scaling factor α_m and a network code vector $a_m \in Z^N$, the decoder performs the following steps:

1. Scale the channel output: $\tilde{y}_m = \alpha_m y_m$.
2. Quantize to the fine lattice to get an estimate on $\lambda_{m;F}$: $\hat{\lambda}_{m;F} = Q_{\Lambda_F}(\tilde{y}_m)$.
3. Take modulo-operation with respect to the coarse lattice to get: $\hat{\lambda}_m = [\hat{\lambda}_{m;F}] \mod \Lambda_C$.

A decoding error occurs at the relay R_m if $\hat{\lambda}_m \neq \lambda_m$. The probability of error at the relay R_m is then equal to:

$$P_{R_m} = \Pr\left[\hat{\lambda}_m \neq \lambda_m\right] \tag{4.15}$$

Given the network coding vector a_m, the following computation rate $\mathcal{R}_m$ is achievable at the relay R_m:

$$\mathcal{R}_m = \frac{1}{2} \log^+ \left[\frac{\alpha_m}{\alpha_m^2 + \alpha_m \|\alpha_m h_m - a_m\|^2}\right] \tag{4.16}$$

For what concerns the selection of the scaling factor and the network code vector, since the objective of the CF is to reliably decode an integer combination with the highest possible rate, each relay R_m selects its parameters α_m and a_m such that its computation rate $\mathcal{R}_m$ is maximized. As discussed in chapter 2, according to this local optimization criterion, the optimal scaling parameter chosen locally at the level of each relay R_m is given by:

$$\alpha_m = \frac{P < h_m^t ; a >}{1 + P\|h_m\|^2} \tag{4.17}$$

Which results in a computation rate $\mathcal{R}_m$ given by:

$$\mathcal{R}_m (a_m) = \frac{1}{2} \log^+ \left(\|a_m\|^2 - \frac{P | h_m^t a_m |^2}{1 + P \| h_m \|^2} \right)^{-1} \tag{4.18}$$

Under the same local rate maximization criterion, the optimal network code vector for each relay R_m for $m = 1; \ldots; N$ is found according to the integer optimization problem given by:

$$a_m \underset{a_m \in \mathbb{Z}^N ; a_m \neq 0_N}{\operatorname{argmin}} a_m^t G_m a_m \tag{4.19}$$

where

$$G_m = I_N - \frac{P}{1 + P\|h_m\|^2} H_m \ ; \ H_m = h_m h_m^t \tag{4.20}$$

After the computation of the desired combinations, each relay transmits its decoded function $\hat{\alpha}_m$ and network code vector a_m to the destination.

4.3.2 Processing at the destination and decodability condition

At the end of the second transmission's phase, the destination collects the combinations $\hat{\alpha}_1; \ldots; \hat{\alpha}_N$ and the integer vectors $a_1; \ldots; a_N$. With this input, the destination forms the following system:

$$L = \begin{pmatrix} \hat{\alpha}_1^t \\ \vdots \\ \hat{\alpha}_N^t \end{pmatrix} A = [A \, X] \mod \Lambda_C \tag{4.21}$$

where the rows of the network code coefficients matrix $A \in \mathbb{Z}^{N \times N}$ are the vectors $a_1^t; \ldots; a_N^t$ such that:

$$A = \begin{pmatrix} a_1^t \\ \vdots \\ a_N^t \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{pmatrix}$$

Based on the knowledge of the matrix L and the network code matrix A, recovery of the original messages at the destination is performed in two steps as follows:

1. Map the system (4.21) to the finite field using φ^{-1} to get:

$$U = QW \tag{4.22}$$

where $U = \varphi^{-1}(L) \in \mathbb{F}_p^{N \times n}$, $Q \in \mathbb{F}_p^{N \times N}$ such that its finite field elements are given by $q_{ij} = g^{-1}([a_{ij}] \bmod p)$ for $i, j = 1, \ldots, N$, and $W = \varphi^{-1}(X) \in \mathbb{F}_p^{N \times n}$ such that its rows correspond to the transpose of the original finite field messages $w_1^t, \ldots, w_N^t$.

2. Invert the matrix Q in system (4.22) and get estimates of the original messages: $\left[\hat{w}_1^t \ldots \hat{w}_N^t\right]^t = \hat{W} = Q^{-1}U$, where Q^{-1} denotes the inverse of Q over the finite field $\mathbb{F}_p$ and can be implemented in practice using the Gaussian elimination.

Detailing the processing at the destination as described in the above steps allowed as to establish an important decodability condition at the destination that has been overlooked in previous works: the destination is able to reliably recover the original messages if and only if the finite field coefficients matrix Q is full rank over $\mathbb{F}_p$. Given the relation between Q and A, this condition is equivalent to require that the determinant of the network code coefficients matrix A over R be non-zero modulo p.

If the full rank condition at the destination is satisfied, the destination is able to recover the original messages with a rate $\mathcal{R}_D$ limited by the minimum achievable rate at the relays $R_1, \ldots, R_N$ such that:

$$\mathcal{R}_D = \min\{\mathcal{R}_1, \ldots, \mathcal{R}_N\} \tag{4.23}$$

Otherwise, the rate $\mathcal{R}_D$ is equal to 0.

However, the local optimization problem in (4.19) based on which are selected the network code vectors that constitute the matrix A does not take into consideration the network level full rank condition. Indeed, each relay in the network selects locally and independently its network code vector under a local optimization criterion to maximize its computation rate. Consequently, there is no guarantee that the full rank constraint at the destination is satisfied. In order to combine the full rank requirement and the computation rate maximization at the relays, the network code vectors $a_1, \ldots, a_N$ should be selected according to the following criterion:

$$(a_1, \ldots, a_N) = \underset{\substack{a_1, \ldots, a_N \in Z^N \\ [\det(A)] \bmod p \neq 0}}{\operatorname{argmax}} \mathcal{R}_D \tag{4.24}$$

$$= \underset{\substack{a_1, \ldots, a_N \in Z^N \\ [\det(A)] \bmod p \neq 0}}{\operatorname{argmax}} \min\{\mathcal{R}_1, \ldots, \mathcal{R}_N\} \tag{4.25}$$

With this design criterion, it is ensured that the full rank condition is met jointly to a maximization of the computation rate at the level of each relay node which leads to the maximization of the rate at the destination. Given the expressions of the computation

rates $\mathcal{R}_1;:::;\mathcal{R}_N$, we propose in Lemma 4.1 a new optimization problem for finding the optimal network code vectors for the CF taking into account the full rank condition over the finite field while maximizing the computation rate at each relay.

Lemma 4.1. *For the real-valued fading Multi-Source Multi-Relay channel using the Compute-and-Forward strategy, the optimal network code vectors that allow simultanously to maximize the computation rate at each relay and guarantee full rank condition at the destination are solutions of the minimization problem:*

$$(a_1;:::;a_N) = \underset{\substack{a_1;:::;a_N \in Z^N \\ [\det(A)] \mod p \neq 0}}{\operatorname{argmax}} \min_{m=1;:::;N} a_m^t G_m a_m \tag{4.26}$$

where G_m is defined in (4.20).

Before we embark in the description of the algorithms we propose to solve this optimization problem, we provide in the following paragraph an analytical analysis on the impact of the full rank condition on the end-to-end performance by deriving an upper bound on the error probability at the destination operating with the CF.

4.3.3 Error Probability Analysis at the Destination

Recall from equation (4.4) that the probability of decoding error at the destination P_D counts the errors on the original messages such that $P_D = \Pr\left[\bigcup_{i=1}^{N} \hat{w}_i \neq w_i\right]$. However, under the CF scheme, errors on the detection of the original messages at the destination depend both on the correctness of decoding the linear combinations $\hat{\lambda}_1;:::;\hat{\lambda}_N$ at the relays and the probability that the matrix Q is full rank. Then, the probability of error P_D depends on the probabilities of errors $P_{R_m}; m = 1;:::;N$ and the probability P_{fr} of Q to have a rank failure over F_p according to:

$$P_D = \Pr\left[(\det(Q) = 0) \cup \left[\bigcup_{m=1}^{N} \hat{\lambda}_m \neq \lambda_m\right]\right] \tag{4.27}$$

$$\leq \Pr(\det(Q) = 0) + \Pr\left[\bigcup_{m=1}^{N} \hat{\lambda}_m \neq \lambda_m\right] \tag{4.28}$$

$$\leq \Pr(\det(Q) = 0) + \sum_{m=1}^{N} \Pr\left[\hat{\lambda}_m \neq \lambda_m\right] \tag{4.29}$$

$$= P_{fr} + \sum_{m=1}^{N} P_{R_m} \tag{4.30}$$

In addition, we know from [128] that the probability that the $N \times N$ matrix Q over a finite field of size p is not full rank is given by:

$$\Pr(\det(Q) = 0) = 1 - \prod_{i=1}^{N} \left(1 - \frac{1}{p^i}\right) \tag{4.31}$$

Therefore, assuming additionally equal error probabilities at the relays $P_{R_m} = P_R; m = 1;:::;N$ which holds since the transmissions from the sources to the relays are made independently, we obtain an upper bound on the error probability at the destination as:

$$P_D \leq 1 - \prod_{i=1}^{N} \left(1 - \frac{1}{p^i}\right) + N P_R \tag{4.32}$$

The error probability at the destination depends then on the finite field size p, the number of relays N as well as the error probability at the relays P_R. Whereas, it does not depend on the Signal-to-Noise Ratio. This observation will be confirmed later by numerical results.

The obtained upper bound on the error probability shows again that the full rank condition plays a key role in the determination of the end-to-end error performance of the CF strategy. For this purpose, we propose in the following efficient algorithms to search for network code vectors taking into account the full rank constraint according to (4.26). Then, we will analyze numerically the impact of the full rank failure both on the achievable rate and the message error probability at the destination.

4.4 Efficient Network Codes Search for the CF

Solving the optimization problem in (4.26) consists in finding the integer vectors $a_m \in Z^n$ such that the metrics $a_m^t G_m a_m$ are minimized for all $m = 1;:::;N$ and the vectors $a_1;:::;a_N$ form a matrix $A = \left[a_1^t ::: a_N^t\right]^t$ of determinant non-zero modulo the field size p. Looking at the first minimization problem separately, we know that the optimal vector that allows to minimize the metric $a_m^t G_m a_m$ corresponds to the coordinates of the shortest vector in the lattice of Gram matrix G_m. Combining this minimization problem to the full rank condition, our idea is based on a cooperation between the relay nodes and consists of two steps as follows:

Step 1 : in the first step, instead of searching at each relay R_m the optimal integer vector a_m that minimizes its own metric $a_m^t G_m a_m$ and maximizes the computation rate $\mathcal{R}_m$, we attempt to find a candidate set

$$\mathcal{T}_m^{N_{max}} = \{a_m^{(1)}; a_m^{(2)}; :::; a_m^{(N_{max})}\} \tag{4.33}$$

of size N_{max} composed of the best integer vectors $a_m^{(1)}; :::; a_m^{(N_{max})}$ coordinates of the lattice points in Λ_{G_m} with shortest lengths which correspond to the maximum computation rates achievable for the underlying relay R_m. The length N_{max} is initialized to N and modified according to numerical results obtained by simulations. We propose in (4.4) a Fincke-Pohst based algorithm to the search of the sets $\mathcal{T}_m^{N_{max}}$ for $m = 1;:::;N$.

Step 2 : in the second step, given the candidate sets $\mathcal{T}_1^{N_{max}}; \mathcal{T}_2^{N_{max}}; :::; \mathcal{T}_N^{N_{max}}$, we pick up the best integer vectors $a_1 \in \mathcal{T}_1^{N_{max}}$, $a_2 \in \mathcal{T}_2^{N_{max}}$,...,$a_N \in \mathcal{T}_N^{N_{max}}$ to construct

the matrix $A = \left[a_1^t ::: a_N^t\right]^t$ such that $[\det(A)] \mod p \neq 0$ and the minimum of the corresponding rates $\mathcal{R}_1; \mathcal{R}_2; :::; \mathcal{R}_N$ is maximized. This way, the minimum achievable rate at the destination gets maximized while the full rank requirement is satisfied.

We detail in the following paragraph the processing corresponding to the first step of our proposed strategy.

Searching Candidate Set for each relay

We aim to find for a given relay R_m the candidate set $\mathcal{T}_m^{N_{max}} = \{a_m^{(1)}; a_m^{(2)}; :::; a_m^{(N_{max})}\}$ of fixed length N_{max} with minimum values of the metric $a_m^t G_m a_m$ corresponding to maximum values of the computation rate $\mathcal{R}_m$. In order to find the desired set $\mathcal{T}_m^{N_{max}}$, we proceed with the following steps:

Step 1 : First, we enumerate all non-zero integer vectors t such that $t^t G_m t$ is minimized. In order to reduce the complexity of this enumeration step, we consider the Fincke-Pohst algorithm to limit the search space to the sphere of radius C such that only integer vectors that satisfy $t^t G_m t \leq C$ are considered. With the obtained vectors we form the set:

$$\mathcal{T}_m = \{t \in Z^N ; t \neq 0_N ; t^t G_m t \leq C\} \tag{4.34}$$

We adjust the radius C defining the search space to get at least N_{max} vectors in $\mathcal{T}_{max}$, i.e., to guarantee that $|\mathcal{T}_m| \geq N_{max}$.

Step 2 : Sort the vectors $t_1; t_2; :::; t_{j\mathcal{T}_m j}$ in a descending order corresponding to their achievable rate values $\mathcal{R}_m(t_i)$ in (4.18) for $i = 1; :::; |\mathcal{T}_m|$ such that:

$$\mathcal{R}_m(t_1) \geq \mathcal{R}_m(t_2) \geq ::: \geq \mathcal{R}_m\left[t_{j\mathcal{T}_m j}\right] \tag{4.35}$$

Step 3 : Select the first N_{max} vectors of $\mathcal{T}_m$ to form the desired set $\mathcal{T}_m^{N_{max}}$.

The first enumeration step aiming to find the integer vectors $t \in Z^N \setminus 0_n$ is based on the Fincke-Pohst algorithm as follows.

Let $G_m = R^t R$ be the Cholesky decomposition of the definite positive matrix G_m where $R \in R^{N \times N}$ is an upper triangular matrix. Let $R_{ij}; i; j = 1; :::; N$ denote the elements of the matrix R and $t = [t_1\ t_2\ ::: t_N]^t$. Then the metric $t^t G_m t$ is equivalent to:

$$\begin{aligned} t^t G_m t = \|Rt\|^2 &= \sum_{i=1}^{N} \left(\sum_{j=i+1}^{N} R_{ij} t_j + R_{ii} t_i \right)^2 \\ &= \sum_{i=1}^{N} \left(p_{ii} t_i + \sum_{j=i+1}^{N} p_{ij} t_j \right)^2 \end{aligned} \tag{4.36}$$

where $p_{ii} = R_{ii}^2; i = 1;:::;N$, $p_{ij} = \frac{R_{ij}}{R_{ii}}; j = i+1;:::;N$. Then, solving for $t^t G_m t \leq C$ for $C > 0$ is equivalently to solve for:

$$\sum_{i=1}^{N} \left(p_{ii} @t_i + \sum_{j=i+1}^{N} p_{ij} t_j A \right)^2 \leq C \tag{4.37}$$

Using (4.37), we derive bounds for each component $t_i; i = 1;:::;N$ for the searched vector t. We start our search with the N^{th} component. Refering to (4.37) and given the integer nature of the searched vector we have the following bounds:

$$LB_N \leq t_N \leq UB_N \tag{4.38}$$

with

$$LB_N = \left\lceil -\sqrt{\frac{C}{p_{NN}}} \right\rceil \tag{4.39}$$

$$UB_N = \left\lfloor \sqrt{\frac{C}{p_{NN}}} \right\rfloor \tag{4.40}$$

Once the value of t_N is chosen, we proceed with evaluating the $(N-1)^{th}$ component t_{N-1}. Refering to (4.37) we can write:

$$p_{NN} t_N^2 + p_{N-1;N-1} (t_{N-1} + p_{N-1;N} t_N)^2 \leq C \tag{4.41}$$

which leads to the following bounds:

$$LB_{N-1} \leq t_{N-1} \leq UB_{N-1} \tag{4.42}$$

with

$$LB_{N-1} = \left\lceil -\sqrt{\frac{C - p_{NN} t_N^2}{p_{N-1;N-1}}} - p_{N-1;N} t_N \right\rceil \tag{4.43}$$

$$UB_{N-1} = \left\lfloor \sqrt{\frac{C - p_{NN} t_N^2}{p_{N-1;N-1}}} - p_{N-1;N} t_N \right\rfloor \tag{4.44}$$

Note that the bounds for the component t_{N-1} depend only on the sphere radius C and the values of the previously evaluated component t_N. Then, we proceed with the evaluation of the remaining components for $i = N-2;:::;1$ in a similar fashion. Based on (4.37) we derive similar computation to the following bounds for any element t_i for $i = N-2;:::1$:

$$\left\lceil \sqrt{\frac{1}{p_{ii}} @C - \sum_{l=i+1}^{N} \left(p_{ll} @t_l + \sum_{j=l+1}^{N} p_{lj} t_j A \right)^2 A} - \sum_{j=i+1}^{N} p_{ij} t_j \right\rceil \leq t_i$$

$$\left\lfloor \sqrt{\frac{1}{p_{ii}} @C - \sum_{l=i+1}^{N} \left(p_{ll} @t_l + \sum_{j=l+1}^{N} p_{lj} t_j A \right)^2 A} - \sum_{j=i+1}^{N} p_{ij} t_j \right\rfloor \geq t_i$$

Let

$$S_i = \sum_{j=i+1}^{N} p_{ij} t_j$$

$$T_i = C - \sum_{l=i+1}^{N} p_{ll} \left(t_l + \sum_{j=l+1}^{N} p_{lj} t_j \right)^2 = T_{i+1} + p_{ii} (S_i + t_i)^2$$

then the bounds are equivalent to

$$LB_i \leq t_i \leq UB_i \tag{4.45}$$

with

$$LB_i = \left\lceil -\sqrt{\frac{T_i}{p_{ii}}} + S_i \right\rceil \tag{4.46}$$

$$UB_i = \left\lfloor \sqrt{\frac{T_i}{p_{ii}}} + S_i \right\rfloor \tag{4.47}$$

The components $t_N, t_{N-1}, \ldots, t_1$ of the searched vector $\mathbf{t}$ are then selected as follows: first we choose the coefficient t_N satisfying the bounds requirements in (4.38)-(4.39). For this value, we choose a coefficient t_{N-1} according to the bounds requirements in (4.42)-(4.43). If such coefficient does not exist, we repeat the previous step and select another coefficient t_N. The process is repeated until we find the two coefficients t_N and t_{N-1} fulfilling the required conditions. When both coefficients are found, we proceed with the same fashion to search the coefficient t_{N-2} according to the bounds (4.45)-(4.46) and so on until we find the N components $t_N, t_{N-1}, \ldots, t_1$ meeting the desired conditions on the bounds. A candidate vector $\mathbf{t} = [t_N \; t_{N-1} \ldots t_1]^t$ that satisfies $\mathbf{t}^t \mathbf{G}_m \mathbf{t} \leq C$ is then obtained. The value of the sphere radius C is then updated and the search process is repeated to record all the non-zero vectors in $\mathcal{T}_m$.

A fundamental parameter to the Fincke-Pohst-based enumeration step is the initial value of the sphere radius C. As we proceeded in chapter 3, we fix this parameter to:

$$C = \min \left(\text{diag} \left(\mathbf{G}_m \right) \right) \tag{4.48}$$

By setting the value of C this way, it is big enough to have at least one candidate vector $\mathbf{t}$ within, and small enough not to have many vectors inside.

We summarize in the following the steps of our proposed method to search the candidate set $\mathcal{T}_m^{N_{max}}$ for a relay R_m.

Algorithm 1 Candidate set search algorithm

Input: radius C, matrix G_m, $N_{mathrmmmax}$, fixed parameter g.
Output: The set of integer vectors $\mathcal{T}_m^{N_{max}}$ and their corresponding rates set $\Upsilon_m^{N_{max}}$
Step 1 : Perform Cholesky decomposition of $G_m = R^t R$, and set $p_{ii} = R_{ii}^2$ for $i = 1;:::;N$ and $p_{ij} = \frac{R_{ij}}{R_{ii}}$ for $j = i+1;:::;N$.
Step 2 : Search the set $\mathcal{T}_m = \{t \in Z^N ; t \neq 0_N ; t^t G_m t \leq C\}$ according to the procedure:

1. (*Initialization*) Set $i = N; d = C; T_i = C; S_i = 0$, $\mathcal{T}_m = \emptyset$.
2. (*Compute bounds for* t_i) Set $Z = \sqrt{\frac{T_i}{p_{ii}}}; UB_i = \lfloor Z - S_i \rfloor; LB_i = \lceil -Z - S_i \rceil$ and set $t_i = LB_i - 1$.
3. (*Increase* t_i) Set $t_i = t_i + 1$, if $t_i \leq UB_i$ go to, else go to.
4. if $i = N$ terminate and output the searched set $\mathcal{T}_m$, else set $i = i + 1$ and go to.
5. (*Decrease* i) For $i = 1$ go to 6), else set $i = i - 1; S_i = \sum_{j=i+1}^{N} p_{ij} t_j ; T_i = T_{i+1} + p_{ii} (t_i + S_i)^2$ and go to step 2).
6. If $t = 0_N$ terminate, else record the vector t as candidate and update the set $\mathcal{T}_m = \{\mathcal{T}_m ; t\}$.

Step 3 : Adjust the sphere radius: if $|\mathcal{T}_m| < N_{max}$, set $C = gC$ and repeat Step 2.
Step 4 : Sort the vectors $t_1; t_2; :::; t_{jT_m j}$ in a descending order corresponding to their achievable rate values $\mathcal{R}_m (t_i)$ in (4.18) for $i = 1;:::;|\mathcal{T}_m|$ such that:

$$\mathcal{R}_m (t_1) \geq \mathcal{R}_m (t_2) \geq ::: \geq \mathcal{R}_m \left(t_{jT_m j} \right) \tag{4.49}$$

Step 5 : Select the first N_{max} vectors of $\mathcal{T}_m$ to form the desired set $\mathcal{T}_m^{N_{max}}$ and the corresponding rates set $\Upsilon_m^{N_{max}}$ such that:

$$\mathcal{T}_m^{N_{max}} = \{t_1; t_2; :::; t_{N_{max}}\} \tag{4.50}$$

$$\Upsilon_m^{N_{max}} = \{\mathcal{R}_m (t_1) ; \mathcal{R}_m (t_2; :::; \mathcal{R}_m (t_{N_{max}}))\} \tag{4.51}$$

4.5 Simulation Results

We address in this section the performance evaluation and analysis of the two studied PLNC schemes. We consider the case of $N = 2$ where there are two sources, two relays and a destination. Monte-Carlo simulations have been carried out to evaluate two performance metrics at the destination: the message error rate given by the error probability P_D, and the average achievable rate per user given by $\mathcal{R}_D = \min(\mathcal{R}_1; \mathcal{R}_2)$. Numerical results are related to the nested lattice coding scheme described in chapter 2 in Example 2.1. In addition, for the average achievable rate, we included a Decode-and-Forward strategy for comparison. In this scenario, relay R_1 receives $y_1 = h_{11}x_1 + h_{21}x_2 + z_1$ from which it decodes the codeword x_1 and considers the interfering signal x_2 as noise. Then R_1 forwards its decoded signal to the destination. Similarly, relay R_2 decodes x_2 from its channel output $y_2 = h_{12}x_1 + h_{22}x_2 + z_2$ and treats x_1 as noise. The corresponding rates $\mathcal{R}_1$ and $\mathcal{R}_2$ are given by:

$$\mathcal{R}_1 = \frac{1}{2}\log\left(1 + \frac{h_{11}^2}{1 + h_{21}^2}\right) \; ; \; \mathcal{R}_2 = \frac{1}{2}\log\left(1 + \frac{h_{22}^2}{1 + h_{12}^2}\right) \tag{4.52}$$

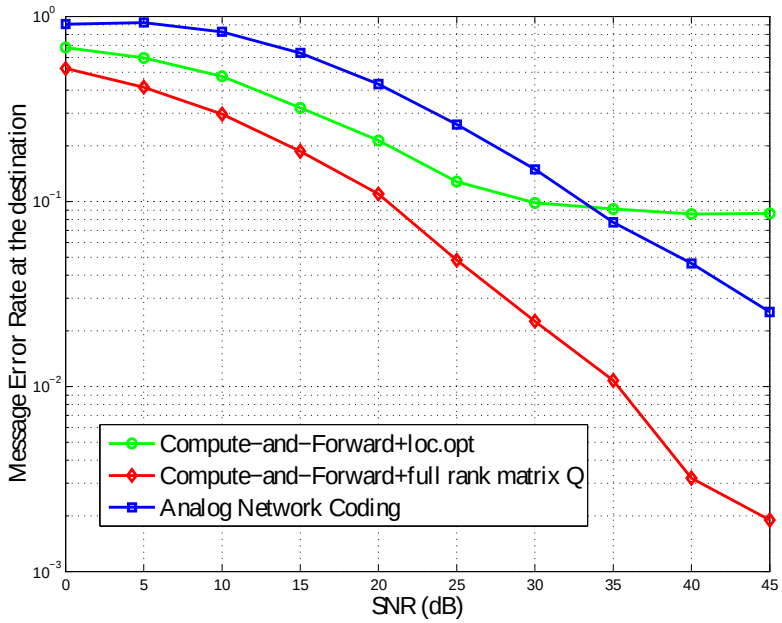


Figure 4.2: Message Error Rate for the MSMR channel.

Starting with the message error rate, we compare in Figure 4.2 the performance of the Analog Network Coding scheme, the Compute-and-Forward scheme with local optimization in which the network code vectors are selected without taking into consideration the full rank condition of the finite field coefficients matrix Q over the finite field F_p, and the

compute-and-forward scheme using our proposed algorithms to solve for the optimization problem in (4.26) under the system level full rank constraint. First result to report in the light of Figure 4.2 is the impact of the full rank failure on the error probability at the destination under the CF strategy. Our analytical analysis we made previously in section shows that the overall error probability at the destination depends on N, the error probability at the relays and the probability of full rank failure of the matrix Q which is independent of the SNR. This explains the obtained performance concerning the CF scheme based on local optimization criterion which does not guarantee the full rank condition. Indeed, the probability of error for this scheme decreases as function of the SNR until a certain point when it becomes flat, i.e., independent of the SNR. In the decreasing part of the curve, the error probability at the destination is comparable to the error probability at the relays $2\mathrm{P}_{\mathsf{R}}$. Starting from the point where the curve becomes flat, the error probabilities at the relays become insignificant compared to the probability of full rank failure, therefore, the overall errror probability at the destination is dominated by the full rank failure probability P_{fr} which is a constant for fixed N and size field p.

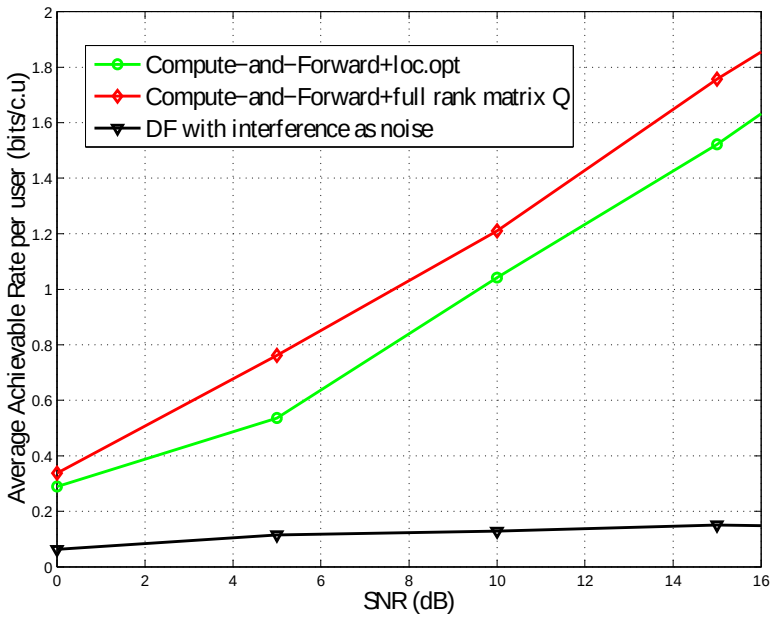


Figure 4.3: Average achievable rate per user for the MSMR channel.

In addition, numerical results depicted in Figure 4.2 show the effectiveness of our proposed algorithms to find efficient network code vectors for the CF strategy under the full rank requirement. Our method brings a gain of more than 10dB over the CF with local optimization-based network codes design at a message error rate equal to 10^{-1} and a gain of more than 15dB over the Analog Network Coding strategy at a message error

rate of $210^{\square 2}$.

Now, moving to the average achievable rate performance, results depicted in Figure 4.3 join the previous findings. The penalty of the full rank failure on the average achievable rate is also significant. Satisfying this system level condition using our proposed algorithms brings for example a gain of 2dB for a target rate of 1bits/c.u. In addition, Figure 4.3 demonstrates the outperformance of the CF over the Decode-and-Forward scheme, again this proves the importance of such PLNC techniques and their potential to make the interference resulting from the superposition of different users' signals a boosting characteristic to achieve higher transmission rates.

4.6 Conclusion

This chapter was dedicated to study the ANC and the CF strategies in the Multi-Source Multi-Relay channel. We analyzed the processing at the relay nodes and the destination for each scheme. In addition, for the CF, we pointed out the full rank condition for possible decoding at the destination, analyzed its impact on the end-to-end performance and proposed a new lemma to design efficient network codes for the CF taking this decodability condition into account. Further, we developed practical search algorithms based on the Fincke-Pohst approach. Effectiveness of the proposed method as well as the outperformance of the CF over the ANC are confrmed by numerical results considering a nested lattice coding scheme.

Common to the previously studied networks, namely the TWRC and the MSMR channel, is that the relays are equipped with a single antenna. In the next chapter we aim to explore the multiple antennas case. We will consider the distributed MIMO channel and study the novel class of receivers termed *Integer-Forcing Linear Receivers* inspired from the Compute-and-Forward strategy.

Chapter 5

Distributed MIMO channel

Multiple antenna technologies play a fundamental role in the design of most of the successful wireless communication systems due to their potential to increase the spectral efficiency and the transmission data rates. Several wireless standards such as the LTE and the WiMAX (IEEE 802.16) have incorporated MIMO communications to enhance the network performance and take advantage of the diversity brought by multiple antennas. In this context, we introduce the last network topology we aim to investigate in this work, the *Distributed MIMO channel*. In this network, as shown in Figure 5.1, M *single antenna* source nodes $S_1; :::; S_M$ desire to communicate their messages to a common destination D equipped with $N \geq M$ antennas. Data streams are independently encoded at the sources and sent concurrently to the destination which implements a MIMO decoder to recover all the original information messages.

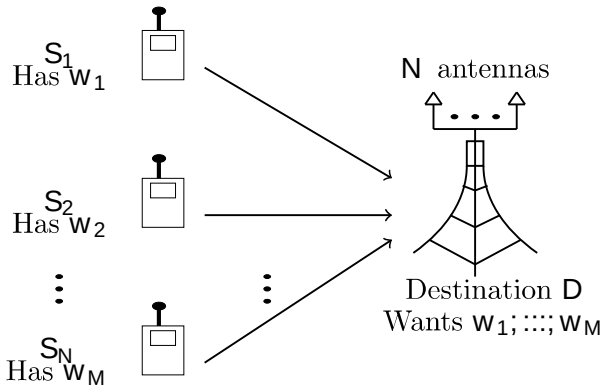


Figure 5.1: Distributed MIMO Channel.

In practice, this network can be used to model any $M \times N$ MIMO system with independent encoding at the transmit antennas (e.g., V-BLAST setting) or a communication from different single antenna wireless devices to a common multiple antenna receiver, a

scenario we encouter in cellular uplink networks with multiple antenna base stations.

What concerns us in this network topology is the design of the MIMO decoders. Particularly, we aim to investigate a new architecture of linear receivers termed *Integer Forcing Linear Receivers* (IF). Inspired by the Compute-and-Forward protocol, this architecture has been recently proposed by Zhan *et al.* in [10–12] and is based on its essence of the use of structured codes for channel coding. Briefly, source nodes use independently a same lattice code to encode their messages. At the receiver, instead of creating interference-free independent data streams as is the case of the traditional linear receivers (Zero-Forcing (ZF) and Minimum Mean Square Error (MMSE) detector), both interference and code's linearity are exploited to decode *integer linear combinations* of the original codewords. Upon decoding a full rank set of such combinations according to an integer full rank coefficient matrix, original messages can be recovered by a simple matrix inversion with rates that go highly beyond those attainable using the traditional linear receivers.

Based on the Compute-and-Forward original framework, the potential of the new IF architecture has been proved under a theoretical capacity achieving perspective and its benefits have been also demonstrated in the case of inter-symbol interference channels [129, 130] and multiuser MIMO channels [131]. Motivated by the theoretical promising gains of the IF linear receivers, we aim in this work to go one step further towards practice by developing practical and efficient algorithms to design the IF receivers parameters and providing an evaluation of their error rate performance using finite length nested lattice coding schemes. As a starting point, we describe in section 5.1 the system model and assumptions. For ease of presentation, we will consider the real-valued MIMO channel case. Extension of the results follow easily using the complex-to-real transformation described in chapter 2. Following, in section 5.2 we review the basic optimal and suboptimal MIMO decoders studied in literature, namely the ML decoder, linear receivers through the ZF and the MMSE and lattice reduction-aided linear receivers. The integer forcing architecture is introduced in section 5.3. For this decoders, we will review the main information theoretic results concerning the achievable rate and Diversity-Multiplexing Tradeoff (DMT). Based on the sum rate maximization criterion, we develop in section 5.4 novel algorithms to find the optimal IF receivers parameters. Performance of our methods are numerically evaluated and compared to the traditional MIMO decoders in section 5.5 using a finite length nested lattice coding scheme. Finally, the results of this chapter are summarized in a concluding section.

5.1 System Model and Assumptions

Each source S_i in the network delivers a data stream that can be represented as a length$-\mathsf{k}$ message w_i drawn i.i.d from a prime size field F_p according to a uniform distribution. In order to be able to use an Integer Forcing linear receiver, two key requirements need to be satisfied: *a same nested lattice code* is used for channel coding at the sources and *encoding of the data streams is done independently.* Accordingly,

each source S_i is equipped with a separate encoder $\mathcal{E}_i : F_p \to \Lambda$ that implements the one-to-one mapping to map the message w_i to an $n-$dimensional lattice codeword x_i from the nested lattice $\Lambda = (\Lambda_F; \Lambda_C)$ involving a fine lattice $\Lambda_F \subset R^n$ and a coarse lattice $\Lambda_C \subset R^n$. Encoded vectors satisfy a symmetric power constraint given by:

$$\frac{1}{n} E \left[\|x_i\|^2 \right] \leq P \tag{5.1}$$

for $P > 0$ and $i = 1; ...; M$. Each of the sources transmit at the same message rate

$$r = \frac{k}{n} \log p \tag{5.2}$$

And the *total rate* of the studied network is given by:

$$\mathcal{R}_{tot} = M r \tag{5.3}$$

After encoding their messages, the sources transmit their codewords simultaneously to the destination. Assuming a perfect synchronization between the transmitters, the MIMO channel ouput at the destination can be expressed as:

$$Y = HX + Z \tag{5.4}$$

where the matrices

$$X = \begin{bmatrix} x_1^t \\ \vdots \\ x_M^t \end{bmatrix} \in R^{M \times n} \; ; \; H = \begin{bmatrix} h_1^t \\ \vdots \\ h_N^t \end{bmatrix} \in R^{N \times M} \; ; \; Z = \begin{bmatrix} z_1^t \\ \vdots \\ z_N^t \end{bmatrix} \in R^{N \times n} \tag{5.5}$$

denote respectively the matrix of the transmitted codewords, the MIMO channel matrix, and the additive Gaussian noise matrix. The vectors $h_m^t = [h_{m1} \; h_{m2} \; ... \; h_{mN}]$ for $m = 1; ...; N$ represent the fading coefficients from the sources to the receive antenna m and have entries generated i.i.d according to a normal distribution $\mathcal{N}(0; 1)$. The vectors z_m for $m = 1; ...; N$ are generated i.i.d according to the normal distribution $\mathcal{N}(0; \sigma^2 I_n)$. In addition, we consider a *slow fading* channel model for which the channel realizations remain constant during the entire transmission of a codeword and we assume that channel state information is available only at the receiver. Additionally, we denote by $\rho = \frac{P}{\sigma^2}$ the Signal-to-Noise Ratio.

According to the matrix notation in (5.4), received signal at the m^{th} antenna can be expressed by:

$$y_m^t = h_m^t X + z_m^t \tag{5.6}$$

The destination is equipped with a decoder $\mathcal{D}$ that generates estimates of the original messages such as,

$$\mathcal{D} : R^{N \times n} \to F_p^M \tag{5.7}$$

$$Y \mapsto \mathcal{D}(Y) = (\hat{w}_1; ...; \hat{w}_M) \tag{5.8}$$

A decoding error occurs if $\hat{w}_i \neq w_i; \forall i = 1;:::;M$. We say that the *sum rate* $\mathcal{R}_{Scheme}(H)$ is achievable using the decoding technique $^{0}Scheme^{0}$, if for any $" > 0$ and n large enough, there exist encoders $\mathcal{E}_1;:::;\mathcal{E}_M$ and a decoder $\mathcal{D}$ such that:

$$\begin{aligned}(\hat{w}_1;:::;\hat{w}_M) &\overset{4}{=} \mathcal{D}(Y) \\ \Pr((\hat{w}_1;:::;\hat{w}_M) \neq (w_1;:::;w_M)) &< \square\end{aligned} \tag{5.9}$$

and the total rate $\mathcal{R}_{tot}$ is lower than $\mathcal{R}_{Scheme}(H)$,

$$\mathcal{R}_{tot} \leq \mathcal{R}_{Scheme}(H) \tag{5.10}$$

The message error probability at the destination is defined as:

$$P_e = \Pr\left[\bigcup_{i=1}^{N} \hat{w}_i \neq w_i\right] \tag{5.11}$$

In addition to the rate and error probability performance, we will review the Diversity Multiplexing Tradeoff of the studied MIMO receivers including the new IF architecture. The DMT characterizes the asymptotic performance of a MIMO transmission scheme [132]. We say that a family of codes achieve a multiplexing gain r and diversity gain d if the total rate $\mathcal{R}$ and the average error probability P_e satisfy:

$$\lim_{SNR!\ 1} \frac{\mathcal{R}(SNR)}{\log(SNR)} \geq r \ ; \quad \lim_{SNR!\ 1} \frac{P_e(SNR)}{\log(SNR)} \leq -d \tag{5.12}$$

5.2 Traditional MIMO receivers

In this section we provide a brief overview of the most known decoding techniques, starting with the optimal ML decoder, then proceeding with suboptimal linear receivers and lattice-reduction aided linear receivers.

5.2.1 ML decoder

Traditional decoders for MIMO systems aim to decode original codewords separately. The optimal approach is the joint Maximum Likelihood decoding illustrated in Figure 5.2.

Implementing the ML criterion, the decoder $\mathcal{D}$ solves, jointly, for the most likely set of codewords $\hat{x}_1;:::;\hat{x}_M$ composing the matrix $\hat{X}$ according to the ML metric:

$$\hat{X} = \underset{\substack{(x_1;:::;x_M) \in \Lambda^M \\ X = x_1^t \ ::: \ x_M^t}}{\operatorname{argmin}} \|Y - HX\|^2 \tag{5.13}$$

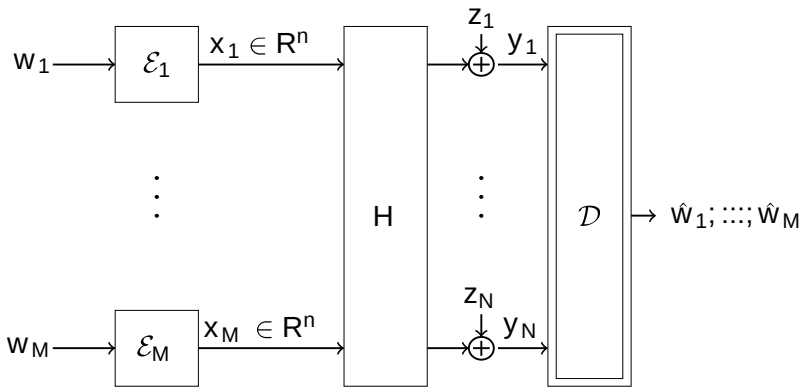


Figure 5.2: MIMO channel with linear independent encoding and ML joint decoding.

After solving for the original codewords, the estimated vectors are mapped back to the finite field to recover estimates on the original messages from:

$$\hat{w}_i = \square^{\square 1}(\hat{x}_i) \;\; ; \;\; i = 1; ...; M \tag{5.14}$$

The achievable sum rate under ML decoding is given by [133]:

$$\mathcal{R}_{ML}(H) = \min_{S \square \{1;2;...;M\}} \frac{M}{|\mathcal{S}|} \frac{1}{2} \log \det \square I_S + \square H_S H_S^t \square \tag{5.15}$$

Where H_S denotes the submatrix of H constructed from the columns of indices in $\mathcal{S} \subseteq \{1; 2; ...; M\}$. Notice that the achievable sum rate in this case is upper bounded by the channel *sum capacity* given by:

$$C = \frac{M}{2} \log \det \square I_N + \square H H^t \square \tag{5.16}$$

which is achievable with joint encoding at the transmit antennas.

For what concerns the DMT, we know from [132] that, for MIMO systems with independent encoding of data streams at the transmit antennas, the optimal DMT is obtained under ML decoding and is given by:

$$d_{ML}(r) = N \square 1 - \frac{r}{M} \square \tag{5.17}$$

where $r \in [0; M]$.

ML decoding offers optimal performance. However, its main drawnback is the high complexity which increases exponentially as the length of the transmitted codewords and the number of antennas increase. Several ML decoding algorithms are proposed in literature to reduce this complexity [88, 134–137]. The most known approaches use sequential decoding such as the Sphere Decoder we consider in our implementation.

5.2.2 Linear Receivers

Motivated by their low computational complexity, linear receivers such as the Zero-Forcing and the Minimum Mean Square Error detectors ar deployed in wireless systems limited by processing and computation capabilities. Based on such decoders, the receiver creates first interference-free data flows then decodes each information stream independently as depicted in Figure 5.3.

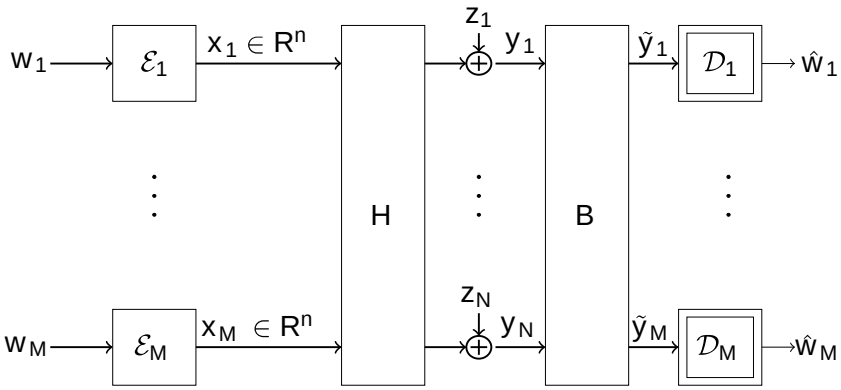


Figure 5.3: MIMO channel with linear independent encoding and Linear Receivers.

Interference elimination is made through a projection of the channel output Y with a preprocessing matrix $B \in R^{M \times N}$ such that:

$$\tilde{Y} = BY = BHX + BZ \tag{5.18}$$

The outputs $\tilde{y}_1; ...; \tilde{y}_M$ of the projection step are then treated separately by the independent decoders $\mathcal{D}_1; ...; \mathcal{D}_M$. Each input vector $\tilde{y}_m$ is treated as a noisy version of the codeword x_m from which an estimate $\hat{x}_m$ is decoded and mapped back to the finite field to get an estimate of the message w_m such that $\hat{w}_m = \mathcal{E}^{-1}(\hat{x}_m)$.

The objective of the processing step in this case is to eliminate the interference generated by the MIMO channel. In the case of the ZF receiver, the preprocessing matrix B_{ZF} is equal to the pseudo-inverse of the channel matrix given by:

$$B_{ZF} = (H^t H)^{-1} H^t \tag{5.19}$$

The noise amplification induced by the ZF preprocessing leads to performance degradation. In order to overcome this shortcoming at low SNR values, an MMSE receiver can be applied. In this case, the projection matrix is given by:

$$B_{MMSE} = H^t \left(HH^t + \frac{1}{\rho} I_N \right)^{-1} \tag{5.20}$$

Although simple, these linear receivers have poor performance in tems of both achievable sum rate and DMT [138]. Let b_m^t denote the m^{th} row vector of the preprocessing matrix

$\mathbf{B}$. Then, the achievable rate for the m^{th} data stream under linear receivers is given by:

$$R_{m;Lin}(\mathbf{H}) = \frac{1}{2}\log\left(1 + \frac{\|\mathbf{b}_m^t\mathbf{H}\|^2}{\|\mathbf{b}_m^t\|^2 + \sum_{i\neq m}\|\mathbf{b}_i^t\mathbf{H}\|^2}\right) \tag{5.21}$$

The achievable sum rate is dictated by the minimum achievable rate over the M streams and is given by,

$$\mathcal{R}_{Lin}(\mathbf{H}) = M \min_{m=1;\dots;M} R_{m;Lin}(\mathbf{H}) \tag{5.22}$$

For what concerns the DMT, it is showed in [132] that the ZF and MMSE linear receivers achieve the following diversity:

$$d_{Lin}(r) = \left(1 - \frac{r}{M}\right) \tag{5.23}$$

for $r \in [0; M]$.

5.2.3 Lattice Reduction-aided Linear Receivers

In order to enhance the performance of linear receivers, lattice reduction (LR) techniques can be used as a preprocessing step to improve the orthogonality of the channel matrix. A lattice reduction of $\mathbf{H}$ gives a near orthogonal matrix $\mathbf{H}_r \in \mathbb{R}^{N\times M}$ related to the former by: $\mathbf{H}_r = \mathbf{H}\mathbf{T}$ with $\mathbf{T} \in \mathbb{Z}^{M\times M}$ is a unimodular matrix, i.e., of integer entries and determinant equal to ± 1. Given this relation, the channel output can be written as:

$$\begin{aligned} \mathbf{Y} &= \mathbf{H}\mathbf{X} + \mathbf{Z} \\ &= (\mathbf{H}\mathbf{T})\mathbf{T}^{-1}\mathbf{X} + \mathbf{Z} \\ &= \mathbf{H}_r\left(\mathbf{T}^{-1}\mathbf{X}\right) + \mathbf{Z} \end{aligned} \tag{5.24}$$

Let $\mathbf{U} = \mathbf{T}^{-1}\mathbf{X}$, then we get

$$\mathbf{Y} = \mathbf{H}_r\mathbf{U} + \mathbf{Z} \tag{5.25}$$

Given the integer nature of the matrix $\mathbf{T}$, row vectors of the matrix $\mathbf{U}$ are also codewords from the original fine lattice Λ_F. Accordingly, solving for $\mathbf{X}$ in the system (5.24) is equivalent to solve for $\mathbf{U}$ in the system (5.25) with the near-orthogonal equivalent channel matrix $\mathbf{H}_r$. After decoding $\hat{\mathbf{U}}$, estimate on the codewords matrix is deduced by the relation $\hat{\mathbf{X}} = \mathbf{T}\hat{\mathbf{U}}$.

For LR-aided linear receivers, the decoding is similar to the detection performed using simply linear receivers with two main differences: the channel matrix is the new reduced matrix $\mathbf{H}_r$, and the decoding is made with respect to the codewords matrix $\mathbf{U}$ from which the original matrix $\mathbf{X}$ are deduced. Accordingly, for LR-aided ZF decoding, the projection matrix is given by:

$$\mathbf{B}_{LR\text{-}ZF} = \left(\mathbf{H}_r^t\mathbf{H}_r\right)^{-1}\mathbf{H}_r^t \tag{5.26}$$

In the case of LR-aided MMSE receiver, the processing matrix is expressed as:

$$B_{LR\text{-}MMSE} = \left(T^t T \right)^{-1} H_r^t \left(H_r \left(T^t T \right)^{-1} H_r^t + \frac{1}{\rho} I \right)^{-1} \tag{5.27}$$

The achievable rate for the m^{th} data stream for the case of LR-aided linear receivers is then given by:

$$R_{m;LR\text{-}Lin}(H) = \frac{1}{2} \log \left(1 + \frac{\| b_{r;m}^t H_r \|^2}{\| b_{r;m}^t \|^2 + \frac{1}{\rho} \sum_{i \neq m} \| b_{r;i}^t H_r \|^2} \right) \tag{5.28}$$

where $b_{r;m}^t$ denotes the m^{th} row vector of the projection matrix after lattice reduction. The achievable sum rate in this case is given by,

$$\mathcal{R}_{LR\text{-}Lin}(H) = M \min_{m=1;\dots;M} R_{m;LR\text{-}Lin}(H) \tag{5.29}$$

Several lattice reduction techniques exist in literature. For what concerns our study, we consider the low-complexity LLL reduction [93]. In our $M \times N$ MIMO channel settings, this technique allows to achieve the full receive diversity of [139]

$$d_{LR\text{-}Lin} = N \tag{5.30}$$

We provide in Appendix 5.F a detailed description of the LLL reduction algorithm.

5.3 Integer Forcing Linear Receivers

5.3.1 Architecture Overview

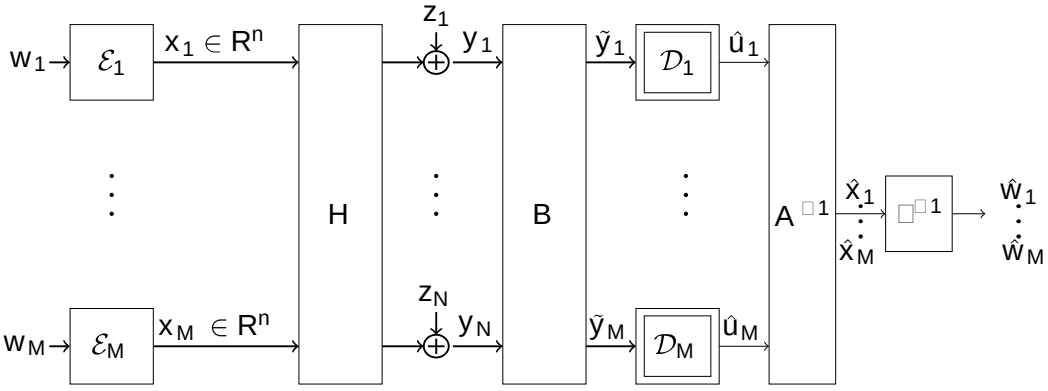


Figure 5.4: Block diagram of IF linear receivers.

In both linear receivers and LR-aided linear receivers, the interference provided by the channel is elimintated by creating and decoding interference-free independent data

streams at the receiver. But what if this interference was exploited? The philosophy of the new *Integer Forcing Linear Receivers* architecture is exactly to take advantage of the linear structure of the lattice codes to make the interference a boosting characteristic of the wireless MIMO channel. The idea is to decode at the destination *integer linear* combinations of the original codewords including both desired and interfering signals. Given the linear structure of the used lattice codes, these combinations are also codewords from the same lattice. After decoding a full rank set of linear combinations, original codewords are recovered by a simple matrix inversion and the original messages are estimated via a simple mapping of the decoded codewords to the finite field.

For this purpose, the receiver selects a real matrix $B \in R^{M \times N}$ and an *integer full rank* matrix $A \in Z^{M \times M}$ and performs the following steps:

1. ***Scaling of channel output***: the first processing step under the IF design is to scale the received signal the preprocessing matrix B such that

$$\tilde{Y} = BY = BHX + BZ = AX + (BH - A)X + BZ \tag{5.31}$$

   This step is necessary to move the channel output closer to the desired full rank set of integer linear combinations of the original codewords with coefficients matrix A. In the resulting scaled signal, the equivalent channel matrix is A and the effective noise term is composed of the scaled channel additive noise and the approximation error of the channel matrix by the integer coefficient matrix. The m^{th} output of the scaled signal can be written as,

$$\tilde{y}_m^t = \underbrace{a_m^t X}_{u_m^t} + \left(b_m^t H - a_m^t\right) X + b_m^t Z \tag{5.32}$$

   where a_m^t and b_m^t correspond respectively to the m^{th} row vectors of the IF coefficients matrix A and the preprocessing matrix B. At this level, given the integer nature of the vectors a_m, the combinations u_m for $m = 1, \ldots, M$ correspond to points from the fine lattice Λ_F.

2. ***Decoding of linear combinations***: the outputs $\tilde{y}_1, \ldots, \tilde{y}_M$ of the scaling step are afterwards passed through separate decoders $\mathcal{D}_1, \ldots, \mathcal{D}_M$. In this case, decoder $\mathcal{D}_m$ treats interfering signals as useful information and attempts to decode the combination $u_m^t = a_m^t X$. Given that these desired combinations correspond to points from the fine lattice, the decoders use the quantizer Q_{Λ_F} to get estimates of u_m such that:

$$\hat{u}_m = Q_{\Lambda_F}(\tilde{y}_m) \tag{5.33}$$

   Note that in this case, the original codewords are not decoded separately. The decoders recover only linear combinations of them.

3. ***Recovering original codewords***: the decoded combinations $\hat{u}_1, \hat{u}_2, \ldots, \hat{u}_M$ are then gathered to form the system $\hat{U} = AX$. Given the full rank matrix A, this

system is solved to decode the matrix of the original codewords as

$$\hat{X} = A^{-1}\hat{U} \tag{5.34}$$

The row vectors of the obtained matrix form estimated of the original codewords $\hat{x}_1^t; \dots; \hat{x}_M^t$.

4. ***Recovering original messages***: the decoded vectors are finally mapped back to the finite field to get estimates of the desired original messages as

$$\hat{w}_i = \mathcal{Q}^{-1}(\hat{x}_i) \;\; ; \;\; i = 1; \dots; M \tag{5.35}$$

These decoding steps are summarized in the block diagram in Figure 5.4.

Remark 5.1. The ZF receiver and the Lattice Reduction-aided ZF can be seen as particular cases of the Integer Forcing architecture. Given the projection matrices B_{ZF} and B_{LR-ZF}, it is easy to see that these decoders match the IF design with equivalent channel matrices giveny by $A_{ZF} = I_N$ and $A_{LR-ZF} = T^{-1}$ in the case of the ZF and the LR-aided ZF respectively. Through an example, authors in [11] show the suboptimality of restricting the equivalent channel matrix to be unimodular. As a proof of concept, we will implement in this work the LLL reduction and analyze its performance compared to the Integer Forcing receivers.

5.3.2 Achievable Rates

The fundamental contribution brought by the Integer Forcing Linear receivers is information theoretic and amounts to enabling higher rates that go highly beyond those permitted by the standard linear receivers. The acheivable sum rate under the IF architecture proved by Zhan *et al.* showed in [11] is stated in the following theorem.

Theorem 5.1. *Consider the MIMO channel with channel matrix* $H \in \mathbb{R}^{N \times M}$ *and a decoder operating with the Integer Forcing architecture. Then the following sum rate is achievable:*

$$\mathcal{R}_{IF}(H) = M \min_{m=1;\dots;M} R_{m;IF}(H; b_m; a_m) \tag{5.36}$$

with

$$R_{m;IF}(H; b_m; a_m) = \frac{1}{2}\log^+\left(\frac{1}{\|b_m^t\|^2 + \|b_m^t H - a_m^t\|^2}\right) \tag{5.37}$$

For any fixed preprocessing matrix $B \in \mathbb{R}^{M \times N}$ *of row vectors* $b_m^t; m = 1; \dots; M$ *and any full rank integer matrix* $A \in \mathbb{Z}^{M \times M}$ *of rows* $a_m^t; m = 1; \dots; M$.

An upper bound to the achievable sum rate using integer forcing linear receivers is found in [11] according to:

$$\mathcal{R}_{IF;UB} = \frac{M}{2}\log\left(1 + \mathrm{SNR}^2_{max}\right) \tag{5.38}$$

where σ_{max} denotes the maximal singular value of the channel matrix $\mathbf{H}$. In addition, we know from [11] that the achievable rate is equal to zero for coefficient vectors satisfying:

$$\|\mathbf{a}_m\|^2 \geq 1 + \sigma_{max}^2 \tag{5.39}$$

5.3.3 Diversity Multiplexing Tradeoff

In addition to the rate benefits offered by the new integer forcing architecture, the advantage of this design manifests in terms of the Diversity Multiplexing Tradeoff. Zhan *et al.* showed in [11] that integer forcing linear receivers allow to recover the optimal DMT as stated in the following theorem.

Theorem 5.2. *Consider the MIMO fading channel with* M *transmit antennas and* $N \geq M$ *receive antennas. The achievable Diversity Multiplexing Tradeoff under the IF architecture is given by:*

$$d_{IF}(r) = N\left(1 - \frac{r}{M}\right) \tag{5.40}$$

for $r \in [0; M]$.

5.3.4 Design criteria for Optimal IF parameters

The two fundamental parameters of the IF architecture are the preprocessing matrix $\mathbf{B}$ and the full rank integer matrix $\mathbf{A}$. The receiver has the freedom to select them, however, the choice needs to be carefully done since these parameters play a key role in the determination of the total achievable rate.

In order to build the IF architecture and find the best preprocessing matrix $\mathbf{B}$ and the IF coefficients matrix $\mathbf{A}$, authors in [12] propose a design criterion based on the maximization of the total sum rate $\mathcal{R}_{IF}(\mathbf{H})$ according to:

$$(\mathbf{B}; \mathbf{A})_{opt} = \underset{\substack{\mathbf{B} \in \mathbb{R}^{M \times N} \\ \mathbf{A} \in \mathbb{Z}^{M \times M};\, |\mathbf{A}| \neq 0}}{\operatorname{argmax}} \mathcal{R}_{IF}(\mathbf{H}) \tag{5.41}$$

Given the rate expression provided in (5.37), this optimization problem is equivalent to consider:

$$(\mathbf{b}_m; \mathbf{a}_m)_{opt} = \frac{M}{2} \underset{\mathbf{A} \neq 0}{\operatorname{argmax}} \min_{m=1,\ldots,M} \log^+ \left(\frac{1}{\|\mathbf{b}_m^t\|^2 + \sigma^2 \|\mathbf{b}_m^t \mathbf{H} - \mathbf{a}_m^t\|^2} \right) \tag{5.42}$$

Based on this, the optimal preprocessing vector $\mathbf{b}_m$ for a fixed integer coefficient vector $\mathbf{a}_m$, was found in [12] as (see Proof in Appendix 5.G.1):

$$\mathbf{b}_{m;opt}^t = \mathbf{a}_m^t \mathbf{H}^t \left(\mathbf{H}\mathbf{H}^t + \frac{1}{\sigma^2} \mathbf{I}_N \right)^{-1} \tag{5.43}$$

Accordingly, the optimal preprocessing matrix $\mathbf{B}$ is given, for a fixed integer full rank matrix $\mathbf{A}$ by,

$$\mathbf{B}_{opt} = \mathbf{A}\left(\mathbf{H}^t\left(\mathbf{H}\mathbf{H}^t + \frac{1}{\rho}\mathbf{I}_N\right)^{-1}\right) \tag{5.44}$$

By replacing in the expression of the rate $\mathbf{R}_{m;IF}(\mathbf{H}; \mathbf{b}_m; \mathbf{a}_m)$ in (5.37) the preprocessing vector by its optimal value, we obtain (see Proof in 5.G.2):

$$\mathbf{R}_{m;IF}(\mathbf{a}_m) = -\frac{1}{2}\log\left(\mathbf{a}_m^t \mathbf{V}\mathbf{D}\mathbf{V}^t\mathbf{a}_m\right) \tag{5.45}$$

where $\mathbf{V} \in \mathbb{R}^{N\times N}$ is the unitary matrix whose columns are the right singular vectors of $\mathbf{H}$ and $\mathbf{D} \in \mathbb{R}^{M\times M}$ is a diagonal matrix with elements

$$\mathbf{D}_{ii} = \begin{cases} \frac{1}{1+\rho\sigma_i^2} & \text{if } i \le \text{rank}(\mathbf{H}) \\ 1 & \text{if } i > \text{rank}(\mathbf{H}) \end{cases} \tag{5.46}$$

where σ_i is the i^{th} singular value of the channel matrix $\mathbf{H}$. The maximum achievable sum rate is then equal to:

$$\mathcal{R}_{IF} = \frac{M}{2}\max_{|A|\neq 0}\min_{m=1,\dots,M}\log\left(\frac{1}{\mathbf{a}_m^t \mathbf{V}\mathbf{D}\mathbf{V}^t\mathbf{a}_m}\right) \tag{5.47}$$

The optimal coefficient vectors are then selected such that the total achievable sum rate $\mathcal{R}_{IF}$ is maximized under the full rank condition of the integer coefficient matrix $\mathbf{A}$. Taking into account the conditions in (5.39) the optimal integer vectors $\mathbf{a}_1, \dots, \mathbf{a}_M$ are solution of the integer optimization problem stated in the following lemma.

Lemma 5.1. *The optimal coefficients vectors for the integer forcing linear receivers are found by the maximization of the achievable sum rate under the full rank condition such that*

$$(\mathbf{a}_1, \dots, \mathbf{a}_M)_{opt} = \underset{\substack{|\mathbf{A}|\neq 0 \\ \|\mathbf{a}_m\|^2 \le 1+\rho\sigma_{max}^2}}{\text{argmin}} \max_{m=1,\dots,N} \mathbf{a}_m^t \mathbf{G}\mathbf{a}_m \tag{5.48}$$

where

$$\mathbf{G} = \mathbf{V}\mathbf{D}\mathbf{V}^t \tag{5.49}$$

is symmetric definite matrix in $\mathbb{R}^{M\times M}$.

Proof. The proof follows from the fact that searching for the integer linearly independent vectors $\mathbf{a}_1, \dots, \mathbf{a}_M$ such that the sum rate in (5.47) is maximized is equivalent to find the vectors $\mathbf{a}_m (m = 1, \dots, M)$ for which the minimum of the function $\log\frac{1}{\mathbf{a}_m^t \mathbf{V}\mathbf{D}\mathbf{V}^t\mathbf{a}_m}$ is maximized, which is also equivalent to seek the integer linearly independe vectors such that the maximum of the function $\mathbf{a}_m^t \mathbf{V}\mathbf{D}\mathbf{V}^t\mathbf{a}_m$ is minimized. □

This optimization problem was only proposed in literature and no methods to solve it have been investigated so far. In the following section we aim to propose practical algorithms that allow to find the optimal linearly independent coefficient vectors such that the total sum rate is maximized. Performance evaluation of the developed algorithms is addressed afterwards.

5.4 Efficient IF Design Algorithms

Solving the optimization problem in (5.48) consists in finding the linearly independent integer vectors $a_m; m = 1;:::;M$ such that the maximum value of the quadratic form $Q(a_m) = a_m^t G a_m$ is minimized. Our proposed search method is based in two steps as follows:

Step 1 : the objective of this first step is to enumerate the top M_{max} integer vectors $t_1;:::;t_{M_{max}}$ that minimize the quadratic form Q in a set Ω ($| \Omega | = M_{max}$). This enumeration step is performed using the Fincke-Pohst algorithm as discussed later. Parameters of the Fincke-Pohst enumeration, for instance the sphere radius C defining the search space, are set up such that we have $M_{max} \geq M$.

Step 2 : Given the candidate set Ω, we pick up the M best linearly independent vectors $a_m \in \Omega$ for $m = 1;:::;M$ such that the corresponding maximum value of $Q(a_m)$ is minimized. For this purpose, we order first the set Ω into Ω_{ord} based on the lengths of the vectors $t_1;:::;t_{M_{max}}$ such that

$$Q(t_1) \leq ::: \leq Q(t_{M_{max}})$$

Then, given the ordered set Ω_{ord}, we select the top M linearly independent vectors $t_1;:::;t_M$ and form the searched vectors as $a_i = t_i; i = 1;:::;M$. In the meantime, the value of the sphere radius C of the Fincke-Pohst algorithm is adjusted to guarantee that $| \mathcal{S} | \geq M$ (repeat the search of the set Ω).

For what concerns the enumeration step, we adopt the Fincke-Pohst algorithm to limit the search space to the non-zero integer vectors t such that $t^t G t \leq C$ where $C > 0$ is a fixed parameter.

Let $G = R^t R$ be the Cholesky decomposition of the definite positive matrix G where $R \in R^{M \times M}$ is an upper triangular matrix. Let $R_{ij}; i; j = 1;:::;M$ denote the elements of the matrix R and $t = [t_1\ t_2\ :::\ t_M]^t$. Then the metric $t^t G t$ is equivalent to:

$$\begin{aligned} t^t G t = \|Rt\|^2 &= \sum_{i=1}^{M} \left(\sum_{j=i+1}^{M} R_{ij} t_j + R_{ii} t_i \right)^2 \\ &= \sum_{i=1}^{M} \left(p_{ii} t_i + \sum_{j=i+1}^{M} p_{ij} t_j \right)^2 \end{aligned} \tag{5.50}$$

where $p_{ii} = R_{ii}^2; i = 1;:::;M$, $p_{ij} = \frac{R_{ij}}{R_{ii}}; j = i+1;:::;M$. Then, solving for $t^t G t \leq C$ for $C > 0$ is equivalently to solve for:

$$\sum_{i=1}^{M} \left(p_{ii} \left(t_i + \sum_{j=i+1}^{M} p_{ij} t_j \right)^2 \right) \leq C \tag{5.51}$$

Using (5.51), we derive bounds for each component $t_i; i = 1;:::;M$ for the searched vector t. We start our search with the M^{th} component. Refering to (5.51) and given the integer nature of the searched vector we have the following bounds:

$$LB_M \leq t_M \leq UB_M \tag{5.52}$$

with

$$LB_M = \left\lceil -\sqrt{\frac{C}{p_{M\,M}}} \right\rceil \tag{5.53}$$

$$UB_M = \left\lfloor \sqrt{\frac{C}{p_{M\,M}}} \right\rfloor \tag{5.54}$$

Once the value of t_M is chosen, we proceed with evaluating the $(M-1)^{th}$ component t_{M-1}. Refering to (5.51) we can write:

$$p_{M\,M} t_M^2 + p_{M-1;M-1} (t_{M-1} + p_{M-1;M} t_M)^2 \leq C \tag{5.55}$$

which leads to the following bounds:

$$LB_{M-1} \leq t_{M-1} \leq UB_{M-1} \tag{5.56}$$

with

$$LB_{M-1} = \left\lceil -\sqrt{\frac{C - p_{M\,M} t_M^2}{p_{M-1;M-1}}} - p_{M-1;M} t_M \right\rceil \tag{5.57}$$

$$UB_{M-1} = \left\lfloor \sqrt{\frac{C - p_{M\,M} t_M^2}{p_{M-1;M-1}}} - p_{M-1;M} t_M \right\rfloor \tag{5.58}$$

Note that the bounds for the component t_{M-1} depend only on the sphere radius C and the values of the previously evaluated component t_M . Then, we proceed with the evaluation of the remaining components for $i = M-2;:::;1$ in a similar fashion. Based on (5.51) we derive similar computation to the following bounds for any element t_i for $i = M-2;:::1$:

$$\left\lceil \sqrt{\frac{1}{p_{ii}} \left(C - \sum_{l=i+1}^{M} p_{ll} \left(t_l + \sum_{j=l+1}^{M} p_{lj} t_j \right)^2 \right)} - \sum_{j=i+1}^{M} p_{ij} t_j \right\rceil \leq t_i$$

$$\left\lfloor \sqrt{\frac{1}{p_{ii}} \left(C - \sum_{l=i+1}^{M} p_{ll} \left(t_l + \sum_{j=l+1}^{M} p_{lj} t_j \right)^2 \right)} - \sum_{j=i+1}^{M} p_{ij} t_j \right\rfloor \geq t_i$$

Let

$$S_i = \sum_{j=i+1}^{M} p_{ij}\, t_j$$

$$T_i = C - \sum_{l=i+1}^{M} p_{ll} \left(t_l + \sum_{j=l+1}^{M} p_{lj}\, t_j \right)^2 = T_{i-1} + p_{ii}\,(S_i + t_i)^2$$

then the bounds are equivalent to

$$LB_i \leq t_i \leq UB_i \tag{5.59}$$

with

$$LB_i = \left\lceil -\sqrt{\frac{T_i}{p_{ii}}} + S_i \right\rceil \; ; \; UB_i = \left\lfloor \sqrt{\frac{T_i}{p_{ii}}} + S_i \right\rfloor \tag{5.60}$$

The components $t_M\,; t_{M-1}; \ldots; t_1$ of the searched vector $\mathbf{t}$ are then selected as follows: first we choose the coefficient t_M satisfying the bounds requirements in (5.52)-(5.53). For this value, we choose a coefficient t_{M-1} according to the bounds requirements in (5.56)-(5.57). If such coefficient does not exist, we repeat the previous step and select another coefficient t_M. The process is repeated until we find the two coefficients t_M and t_{M-1} fulfilling the required conditions. When both coefficients are found, we proceed with the same fashion to search the coefficient t_{M-2} according to the bounds (5.59)-(5.60) and so on until we find the M components $t_M\,; t_{M-1}; \ldots; t_1$ meeting the desired conditions on the bounds. A candidate vector $\mathbf{t} = [t_M \;\; t_{M-1} \ldots t_1]^t$ that satisfies $\mathbf{t}^t \mathbf{G} \mathbf{t} \leq C$ is then obtained. The value of the sphere radius C is then updated and the search process is repeated to record all the non-zero vectors in Ω. For what concerns the choice of the inital value of the sphere radius, we fix this parameter to:

$$C = \min\left(\mathrm{diag}\left(\mathbf{G}\right)\right) \tag{5.61}$$

5.5 Numerical Results

We address in this section performance evaluation of the studied MIMO decoders. We consider the case of $M = N = 2$ with two sources and a 2-antenna destination. Monte-carlo simulations have been carried out to evaluate both average achievable rates and the message error probability at the destination for the different studied receivers: the joint ML, the ZF and MMSE, the LLL-reduced ZF (LLL+ZF), LLL-reduced MMSE, and the integer forcing linear receivers using our proposed algorithms. Numerical results concern the nested lattice coding scheme described in chapter 2 in Example 2.1.

Starting with the achievable rates plotted in Figure 5.5, we first point out that LR-aided linear receivers perform better than the linear receivers. A gain of 5−dB of the

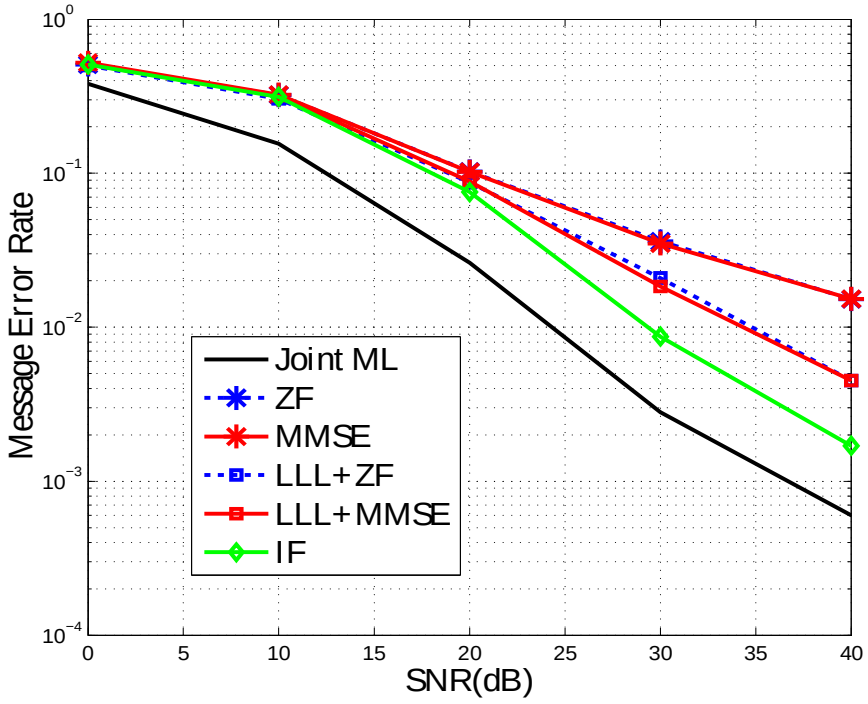


Figure 5.5: Message Error Rate for the Distributed MIMO channel.

LLL+ZF over the ZF is reported for a target rate of 2 bits/channel use. In addition, numerical results confirm that the Integer Forcing receiver outperforms the ZF and MMSE and even Lattice-Reduction aided linear receivers. The proposed algorithm allows to achieve a gain of 1:4dB over the LLL+MMSE and 2dB over the LLL+ZF for a target rate of 3 bits/channel use. This result confirms the suboptimality of restricting the equivalent channel matrix A in lattice reduction aided receivers to be unimodular. Furthermore, the proposed algorithm allows to approach the upper bound of the Integer Forcing receiver given by log 1 + 2max , and reduces the loss to 1:4dB. However, compared to the ML decoder the proposed architecture presents a considerable gap to the joint ML that overtakes 6dB for SNR values greater than 16dB.

Now as far as the error probability is concerned, same deduction can be made as illustrated in Figure 5.6: Integer Forcing Linear receivers outperform both linear receivers and LR-aided linear receivers. For a codeword error rate equal to 10 2 the gain of the IF over the LLL+ZF and LLL+MMSE is 5dB and about 17dB over the ZF. The gap between the proposed IF algorithm to the ML joint decoder counts 5dB. Numerical results demonstrate the effectiveness of our algorithms and confirm the theoretical findings regarding the potential of the new IF architecture.

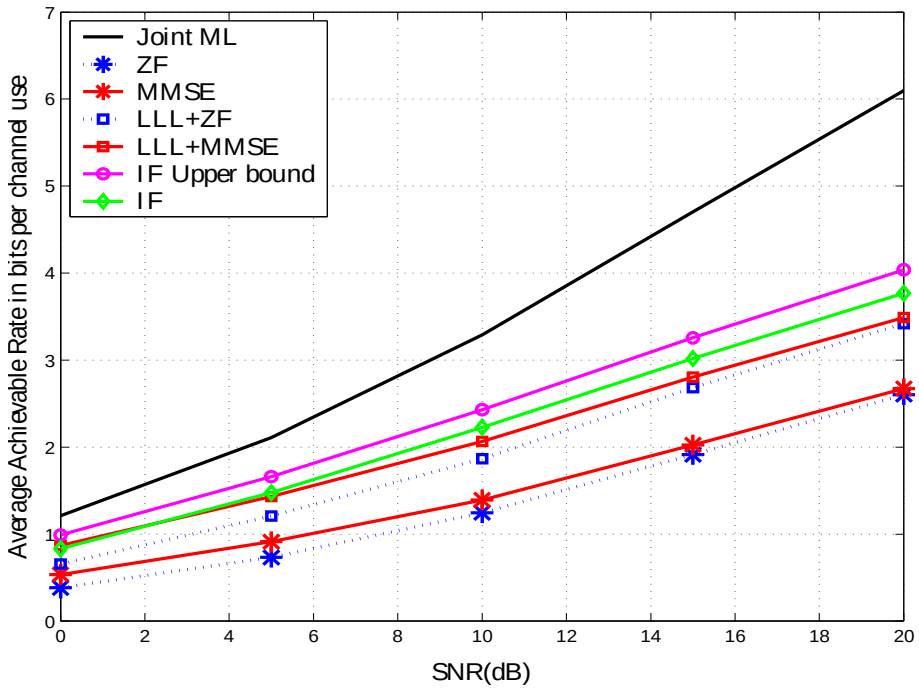


Figure 5.6: Average achievable rates for the distributed MIMO channel.

5.6 Conclusion

This chapter was devoted to study the distributed MIMO channel. In particular, we investigated a new architecture of MIMO receivers termed *Integer Forcing Linear Receivers*. This design is based on the premise of using structured codes at the transmit antennas in an independent fashion, i.e., without joint encoding at the sources. We reviewed the basic theoretical results regarding the IF receivers and developed novel algorithms to design the optimal parameters of the IF architecture. Numerical results are a proof of concept of the outperformance of the IF-based MIMO receivers over the existing linear receivers and lattice-reduction aided linear receivers.

Future research directions include the combination of the integer forcing receivers design with Space-Time Coding.

Conclusion and perspectives

Conclusion

Motivated by the emergence of Physical-Layer Network Coding as a new tool for multiple access interference management, this thesis was dedicated to the analysis, design and performance evaluation of physical-layer network coding-based communication strategies in multiuser wireless communication systems including multiple access channels.

A first part of the thesis was devoted to study the Compute-and-Forward protocol in the basic fading multiple access channel. We made an overview on the encoding scheme based on nested lattice codes, and the decoding scheme based on suboptimal minimum distance decoding. Then, we investigated the optimal solution to design network codes for the CF. By maximizing the achievable rate at the receiver, we showed that the optimal solution is related to a shortest vector problem that can be solved using the complex LLL reduction or the Fincke-Pohst algorithm. Further, we introduced the ergodic rate for the CF operating in fast fading channels and proposed a novel lower bound using the complex LLL reduction. The same tool was used to derive a novel upper bound on the outage probability for the CF operating in slow fading channels. Besides, we investigated optimal decoders for the CF protocol. Starting with the Gaussian multiple access channel where the optimal decoder is based on the maximum a posteriori (MAP) criterion, we developed first a new MAP decoding metric. Then, we showed that MAP decoding is equivalent to MMSE-GDFE preprocessed minimum euclidean distance decoding. Given the new metric, we developed a practical decoding algorithm and showed by numerical simulations its effectiveness and gains over the standard decoding scheme for the CF protocol. For what concerns the fading channel case, we studied the optimal maximum likelihood (ML) decoding. Starting with the multi-dimensional lattice case, we studied the ML decoding metric and showed that the optimal ML solution is related to solve a system of simultaneous diophantine equations. Then, we provided a deeper analysis for the one-dimensional integer-valued lattice case. We developed the decoding metric and studied theoretically and numerically its behavior as function of the channel fading coefficients, the network code vector coefficients and the signal-to-noise ratio. Moreover, we proposed an approximation of the ML decoder which reduces to solve an

Inhomogenous Diophantine Approximation of reals and proposed a practical algorithm based on the Cassel's algorithm. Numerical results evaluating the error performance of the proposed algorithm demonstrate its gain over the traditional decoding scheme for the CF particularly at high signal-to-noise ratio range.

A second part of the thesis was dedicated to study the implementation, design and performance evaluation of PLNC strategies, including the CF and the Analog Network Coding in practical multiuser communication network topologies including multiple access channels. The first network model we studied is the two-way relay channel considering both Gaussian and fading channels. This network is the most known and most studied in the Network Coding literature. Starting with the Gaussian model, we investigated the end-to-end communication considering a relay node operating with the ANC, the Denoise-and-Forward and the CF. We analyzed the error rate and achievable rate performance of these PLNC strategies. Our results showed that these techniques achieve better performance than the traditional relaying strategies that avoid multiuser interference by transmission time scheduling. In addition, among the three studied techniques, the CF is the best one. For what concerns the fading channels case, we proposed a new lemma stating a novel design criterion for the CF operating in the TWRC, then we proposed a practical search algorithm to design efficient network codes based on the Fincke-Pohst enumeration. Our numerical results demonstrated the effectiveness of our approach and show the outerpformance of the CF over the ANC. The second network topology we have been interested in is the Multi-Source Multi-Relay channel. In constract to the TWRC, physical-layer network coding strategies have not been studied in this network model. In this thesis we studied the end-to-end communication in this topology where the relay nodes operate with PLNC. In particular, we analyzed the cases of the ANC and the CF. For the first strategy, we analyzed the processing at the relays and the decodability condition et the end destination. Similarly, for the CF we studied the condition on the network code vectors for successful decoding at the destination, based on which we derived a novel lemma on the optimization problem for the selection of the optimal network codes for the CF. For practical reasons, we proposed Fincke-Pohst-based algorithms to solve for the optimization problem. Our numerical results evaluating the error rate and the achievable transmission rate at the destination demonstrate the effectiveness of our algorithms and show that the CF outperforms the ANC strategy.

The third and last part of the thesis was dedicated to the distributed MIMO channel. In this setting, we were concerned with the design of MIMO decoders. In particular, we studied a new architecture of linear receivers termed Integer Forcing (IF) linear receivers. This new design has been proposed recently in literature. Inspired by the Compute-and-Forward framework, the IF receivers aim to take advantage of the interference provided by the wireless medium to first decode a full rank set of integer linear combinations of the original codewords assumed to be carved from the same lattice (i.e., users sharing the same wireless channel use the same channel coding scheme). Then, given such combinations according to an integer full rank matrix, original source messages can be

recovered by a simple matrix inversion. Motivated by the theoretical potential of these decoders, we were interested in this work in the practical implementation of the IF receivers. We developed practical and efficient algorithms to design the IF parameters and provided a numerical evaluation of their error rate performance using practical finite length lattice coding schemes. Our simulation results confirm the outperformance of this new architecture over the traditional MIMO systems linear receivers and show the reliability of our developed approach.

Perspectives

For future, we propose the following research directions:

Integer Forcing architecture combined to Space-Time Coding IF linear receivers are proved to offer significant gains in terms of DMT and error probability and to outperform existing linear receivers provided that independent linear encoding is performed at the transmit antennas. For this line of research we aim to explore the combination of the IF architecture with lattice-based Space-Time Coding and investigate the possible benefits in terms of decoding complexity and diversity gains.

PLNC in Optical Communications PLNC is proved to significantly improve the end-to-end performance in wireless communication networks. In this line of research, we aim to explore the possible gains of this new coding strategy in optical networks that become popular and rapidely developed to provide to the end users high data rates with the best quality of service.

PLNC for Distributed Storage Distributed storage and cloud computing solutions are among the main applications that started to benefit from Network Coding. With the increasing demand for cloud services, it is of fundamental importance to develop robust, efficient and secure storage techniques. In this line of research, we aim to explore reliable distributed storage approaches based on Network Coding at the physical layer using structured codes.

Appendices

5.A Lattice Definitions

We provide in this appendix the basic definitions in lattice theory. For more details and deeper analysis in this topic, we refer readers to [83, 84].

Definition 5.1 (*Lattice*). An n-dimensional ***lattice*** Λ is a discrete group of rank p, $p \leq n$ of the euclidean space R^n. It is the set spanned by the p linearly independent vectors $v_1; :::; v_p$ of R^n. Explicitly, Λ is given by the set of integer linear combinations as:

$$\Lambda = \left(x = \sum_{i=1}^{p} a_i v_i;\ a_i \in Z \right)$$

p is called the lattice dimension and the vectors $v_1; :::; v_p$ represent a non-unique basis of the lattice Λ. Any vector $x \in \Lambda$ can be written in the form:

$$x = M s; s \in Z^n$$

where M is called a ***generator matrix*** of the lattice. The main characteristic of Λ is *linearity*, i.e. for any $a; b \in Z$ and $x; y \in \Lambda$, $ax + by \in \Lambda$. The matrix given by $G = M\,{}^tM$ is called the ***Gram matrix*** of the lattice.

Definition 5.2 (*Fundamental Volume*). The parallelotope consisting of the points:

$$\alpha_1 v_1 + ::: + \alpha_p v_p; \quad 0 \leq \alpha_i < 1$$

is called the fundamental parallelotope or fundamental region for the lattice Λ. The fundamental volume $\mathrm{vol}(\Lambda)$ of the lattice Λ is the volume of the fundamental parallelotope and is given by: $\mathrm{vol}(\Lambda) = |\det(M)| = \sqrt{\det(G)}$.

Definition 5.3 (*Lattice Quantizer*). A ***lattice quantizer*** Q_α is the mapping that takes a real vector x to the nearest point in Λ in Euclidean distance as

$$Q_\alpha(x) = \underset{\alpha \in \Lambda}{\operatorname{argmin}} \| x - \alpha \|_2$$

The set of points that quantize to a given lattice point is called the ***Voronoi Region***. The ***fundamental Voronoi Region*** $\mathcal{V}_{\square}$ of a lattice Λ corresponds to the voronoi region of the zero vector.

Definition 5.4 (*Modulus operation*). The $\mathsf{mod} - \square$ operation returns the quantization error with respect to Λ. For $x \in R^n$: $[x] \bmod \Lambda = x - Q_{\square}(x)$.

Definition 5.5 (*Nested Lattice Codes*). A ***nested lattice code*** Λ is the set of all points of a lattice Λ_F (termed the *Fine* lattice) that fall within the fundamental Voronoi Region of a lattice Λ_C (termed the *Coarse* lattice) as:

$$\Lambda = \{\square = [\square_F] \bmod \Lambda_C ; \square_F \in \Lambda_F\}$$

The rate of a nested lattice code is given by:

$$r = \frac{1}{n} \log |\Lambda_F \cap \mathcal{V}_C| = \frac{1}{n} \log \frac{\mathrm{vol}(\mathcal{V}_{\square_F})}{\mathrm{vol}(\mathcal{V}_{\square_C})}$$

Definition 5.6 (*Minimum Distance*). The minimum distance d_{min} of a lattice Λ is the minimum distance between any two distinct lattice points from Λ. It is equal to the length of the shortest non-zero lattice vector as:

$$d_{min} = \min\{\|x - y\| : x \neq y \in \Lambda\} = \min\{\|x\| : x \in \Lambda \setminus \{0\}\}$$

Definition 5.7 (*Moments*). The second moment of a lattice Λ is defined as the second moment per dimension of a uniform distribution over the fundamental Voronoi region $\mathcal{V}$ as:

$$\square^2_{\square} = \frac{1}{n\mathrm{vol}(\mathcal{V})} \int_{\mathcal{V}} \|x\|^2 dx$$

The *normalized second moment* of the lattice Λ is given by:

$$G(\Lambda) = \frac{\square^2_{\square}}{(\mathrm{vol}(\mathcal{V}))^{2=n}}$$

Definition 5.8 (*Quantization goodness*). A sequence of lattices $\Lambda^{(n)} \subset R^n$ is good for mean-squared error quantization if:

$$\lim_{n \to \infty} G\left(\Lambda^{(n)}\right) = \frac{1}{2\square e}$$

Definition 5.9 (*AWGN goodness*). Let z denote an $n-$dimensional random vector generated according to the Gaussian distribution $\mathcal{N}(0; \square^2 I_n)$. The *volume-to-noise ratio* of the a lattice Λ is given by:

$$\square(\Lambda; P_e) = \frac{(\mathrm{vol}(\mathcal{V}))^{2=n}}{\square^2}$$

The variance $\square^2$ is selected such that $\Pr(z \in \mathcal{V}) = P_e$. A sequence of lattices $\Lambda^{(n)}$ is AWGN good if:

$$\lim_{n \to \infty} \square\left(\Lambda^{(n)}; P_e\right) = 2\square e, \quad \forall P_e \in (0; 1)$$

and the probability of error decreases exponentially in n for fixed volume-to-noise ratio greater than $2\square e$.

5.B Compute-and-Forward

5.B.1 Optimal scaling factor for the CF

In this appendix we will show that the computation rate in (2.23) is uniquely maximized by the MMSE scaling factor

$$\alpha_{\text{opt}} = \frac{\beta \mathbf{h}^{\mathsf{T}}\mathbf{a}}{1+\beta^2\|\mathbf{h}\|^2} \tag{5.62}$$

For this purpose, define $f(\beta)$ as

$$f(\beta) = \left(\frac{\beta^2+\beta^2\|\beta\mathbf{h}-\mathbf{a}\|^2}{\beta}\right)^{-1} = \|\beta\mathbf{h}-\mathbf{a}\|^2 + \frac{\beta^2}{\beta^2} \tag{5.63}$$

then the computation rate in (2.23) is equal to $R_{\text{comp}} = \log^+(1/f(\beta))$. Maximizing the computation rate is equivalent then to minimize f with respect to β for a fixed vector $\mathbf{a}$. We have the following:

$$f(\beta) = \frac{1}{\beta^2}\beta^{\mathsf{T}}\beta + (\beta\mathbf{h}-\mathbf{a})^{\mathsf{T}}(\beta\mathbf{h}-\mathbf{a})$$

To find the argument which minimizes f we compute the derivative of this function with respect to β:

$$\begin{aligned}\frac{\partial f(\beta)}{\partial \beta} &= \frac{2\beta}{\beta^2} + \mathbf{h}^{\mathsf{T}}(\beta\mathbf{h}-\mathbf{a}) + (\beta\mathbf{h}-\mathbf{a})^{\mathsf{T}}\mathbf{h} \\ &= \frac{2\beta}{\beta^2} + \beta\mathbf{h}^{\mathsf{T}}\mathbf{h} - \mathbf{h}^{\mathsf{T}}\mathbf{a} - \beta\mathbf{h}^{\mathsf{T}}\mathbf{h} - \mathbf{a}^{\mathsf{T}}\mathbf{h} \\ &= 2\left(\frac{\beta}{\beta^2} + \beta\mathbf{h}^{\mathsf{T}}\mathbf{h} - \mathbf{h}^{\mathsf{T}}\mathbf{a}\right)\end{aligned}$$

The optimal scaling parameter satisfies $\frac{\partial f(\beta_{\text{opt}})}{\partial \beta_{\text{opt}}} = 0$ which is equivalent to:

$$\beta_{\text{opt}} = \frac{\mathbf{h}^{\mathsf{T}}\mathbf{a}}{\frac{1}{\beta^2}+\mathbf{h}^{\mathsf{T}}\mathbf{h}} \Rightarrow \beta_{\text{opt}} = \frac{\beta\mathbf{h}^{\mathsf{T}}\mathbf{a}}{1+\beta^2\|\mathbf{h}\|^2}$$

This ends the proof.

5.B.2 Maximum Computation Rate

In this appendix we will show that the optimal computation rate corresponding to the optimal MMSE scaling factor is equal to:

$$R_{\text{comp}}(\mathbf{h};\mathbf{a}) = \log^+\left(\frac{\beta^2}{\|\mathbf{a}\|^2 - \frac{\beta^2|\mathbf{h}^{\mathsf{T}}\mathbf{a}|^2}{1+\beta^2\|\mathbf{h}\|^2}}\right)^{-1} \tag{5.64}$$

With the definition of the function f in Appendix 1, we know that the maximum computation rate is equal to: $R_{comp}(h;a) = \log^{+}(1/f(\rho_{opt}))$. Let us compute $f(\rho_{opt})$:

$$\begin{aligned} f(\rho_{opt}) &= \frac{1}{\rho}\left(\frac{\rho^2 |h^{?}a|^2}{1+\rho\|h\|^2}\right)^{\rho} + \left(\frac{\rho h^{?}a}{1+\rho\|h\|^2}h - a\right)^{2} \\ &= \frac{\rho|h^{?}a|^2}{1+\rho\|h\|^2} + \frac{\rho^2|h^{?}a|^2}{(1+\rho\|h\|^2)^2}\|h\|^2 + \|a\|^2 - 2\frac{\rho|h^{?}a|^2}{1+\rho\|h\|^2} \\ &= \frac{\rho|h^{?}a|^2 + \rho^2|h^{?}a|^2\|h\|^2 - 2\rho\left(1+\rho\|h\|^2\right)|h^{?}a|^2}{(1+\rho\|h\|^2)^2} + \|a\|^2 \\ &= \|a\|^2 - \frac{\rho|h^{?}a|^2}{1+\rho\|h\|^2} \end{aligned}$$

The proof follows by setting $R_{comp}(h;a) = \log^{+}(1/f(\rho_{opt}))$.

5.B.3 Modified Sphere Decoder for MAP Decoding

In this appendix we provide a modified version of the sphere decoder to find the optimal MAP estimate solution of the optimization problem given in (2.62). Recall that the objective is to find the integer vector u_{opt} in $\mathcal{A}_s$ such that $\|y_{aug} - M_{aug}u\|^2$ is minimized. The idea behind the sphere decoder is to reduce the search space to the sphere of radius C centered in y_{aug}. Then the optimal integer vector satisfies

$$\|y_{aug} - M_{aug}u\|^2 \leq C^2 \tag{5.65}$$

We include the shaping constraint in the search process such that only points corresponding to the integer vectors that belong to the region $\mathcal{A}_s$ are visited inside the sphere.

Let $M_{aug} = QR$, be the QR decomposition of M_{aug} where R is upper triangular of coefficients $r_{ij}; i,j = 1,\ldots,n$, and let $\%= M_{aug}^{-1}y_{aug}$ be the zero-forcing vector and $\rho = \%- u$. Inequality (5.65) can then be written as

$$\begin{aligned} &\|R\rho\|_2^2 \leq C^2 \\ &\sum_{i=1}^{n} p_{ii}\left(\rho_i + \sum_{j=i+1}^{n} p_{ij}\rho_j\right)^2 \leq C^2 \end{aligned} \tag{5.66}$$

where $p_{ii} = r_{ii}^2; i = 1,\ldots,n$; $p_{ij} = \frac{r_{ij}}{r_{ii}}; j = i+1,\ldots,n$. Using (5.66), we derive bounds for every component u_i of the desired vector u. Starting with the the n^{th} component we get the following bounds,

$$-\frac{C}{\sqrt{p_{nn}}} \leq \rho_n \leq \frac{C}{\sqrt{p_{nn}}} \tag{5.67}$$

and given that $\rho = \%- u$, we obtain

$$\%_n - \frac{C}{\sqrt{p_{nn}}} \leq u_n \leq \%_n + \frac{C}{\sqrt{p_{nn}}} \tag{5.68}$$

For the remaining components for $i = n-1;:::;1$, we derive similar computation using (5.66) to get the following bounds:

$$-\sqrt{\frac{1}{p_{ii}}\left(C^2 - \sum_{l=i+1}^{n} p_{ll}\left(u_l + \sum_{j=l+1}^{n} p_{lj}u_j\right)^2\right)} + \sum_{j=i+1}^{n} p_{ij}u_j \le u_i$$

$$\sqrt{\frac{1}{p_{ii}}\left(C^2 - \sum_{l=i+1}^{n} p_{ll}\left(u_l + \sum_{j=l+1}^{n} p_{lj}u_j\right)^2\right)} + \sum_{j=i+1}^{n} p_{ij}u_j \ge u_i$$

Let

$$S_i = \sum_{j=i+1}^{n} p_{ij}u_j$$

$$T_i = C^2 - \sum_{l=i+1}^{n} p_{ll}\left(u_l + \sum_{j=l+1}^{n} p_{lj}u_j\right)^2 = T_{i+1} + p_{ii}(S_i - u_i)^2$$

then the bounds are equivalent to

$$-\sqrt{\frac{T_i}{p_{ii}}} + S_i \le u_i \le \sqrt{\frac{T_i}{p_{ii}}} + S_i \tag{5.69}$$

Due to the integer nature of the vector u, we define the upper and lower bounds for the searched components as follows

$$b_{inf;i} = \left\lceil -\sqrt{\frac{T_i}{p_{ii}}} + S_i \right\rceil \tag{5.70}$$

$$b_{sup;i} = \left\lfloor \sqrt{\frac{T_i}{p_{ii}}} + S_i \right\rfloor \tag{5.71}$$

which leads to

$$b_{inf;i} \le u_i \le b_{sup;i};\ i = 1;:::;n \tag{5.72}$$

In addition to these bounds requirements obtained from the metric minimization, we add the shaping constraint. Given that the vector $u \in \mathcal{A}_s$, we define for each component u_i, the bounds c^i_{min} and c^i_{max} such that: $c^i_{min} \le u_i \le c^i_{max}$. Thus we get a new interval I_i for each element u_i including both bound and shaping requirements such that:

$$I_i = \left[\max(b_{inf;i}; c^i_{min}); \min(b_{sup;i}; c^i_{max})\right] \tag{5.73}$$

Given these intervals, the search of the n components is done as follows: we first choose the component s_n in the interval I_n, then we search for the candidate s_{n-1} satisfying

requirements of (5.72) inside I_{n-1}. If no value for u_{n-1} exists, we go back to select another candidate for u_n. The same process is repeated until obtaining the set of n components $u_n; u_{n-1}; \ldots; u_1$ for which all bounds and shaping requirements are satisfyied. Once a corresponding point is found, the intervals I_i and the radius of the searching sphere are updated and the process continues until finding the nearest point to y_{aug}.
We summarize below the different steps of our algorithm.

Algorithm 2 Sphere decoder-based MAP Decoding algorithm

Input: $y_{aug}; M_{aug}; C; c^i_{min}; c^i_{max}; i = 1; \ldots; n$
Output: s_{opt}
Step 1: Precoding phase: perform QR decomposition $M_{aug} = QR$, calculate $\rho = M^{-1}_{aug} y_{aug}$ and set $d = C; T_n = C^2; S_k = \rho_k; k = 1; \ldots; n$
Step 2: Search phase:

1. (*Index initialization*) Set $i = n$.
2. (*Computing bounds for* s_i) Calculate $b_{inf;i}; b_{sup;i}$, set $LB(u_i) = max(b_{inf;i}; c^i_{min})$, $UB(u_i) = min(b_{sup;i}; c^i_{max})$ and set $u_i = LB(s_i) - 1$.
3. Set $u_i = u_i + 1$. If $u_i \leq UB(u_i)$ go to v), else go to iv).
4. If $i = n$, terminate and output $u_{opt} = \hat{u}$, else set $i = i + 1$ and go to iii).
5. For $i = 1$ go to v), else set $i = i - 1$ and $\gamma_{i-1} = \rho_{i-1} - S_i$, $T_{i-1} = T_i - p_{ii}(S_i - u_i)^2$, $S_{i-1} = \rho_{i-1} + \sum_{j=i}^{n} p_{i-1;j}\gamma_j$ then go to ii).
6. Set $\hat{d}^2 = T_n - T_1 + p_{11}(S_1 - u_1)^2$. If $\hat{d} \leq d$, then set $\hat{u}_i = u_i; i = 1; \ldots; n; d = \hat{d}; T_n = d$ and go to ii), else go to iii).

5.C MMSE-GDFE preprocessing filters

In this appendix we aim to show that the matrices F and B in the equivalent MAP decoding metric given in (2.63) by the relations

$$B^t B = \frac{1}{\sigma^2} + \sigma^2 I_n \; ; \; F^t B = I_n \tag{5.74}$$

correspond respectively to the forward and backward filters of the MMSE-GDFE preprocessing in the channel $y = \gamma_s + z$ with input γ_s such that $\frac{1}{n}E\left[\|\gamma_s\|^2\right] = \gamma_s^2$. For this purpose, let F_m and B_m be the filters of the MMSE-GDFE preprocessing such that:

$$\begin{aligned} F_m y &= F_m \gamma_s + F_m z \\ &= B_m \gamma_s + (F_m - B_m)\gamma_s + F_m z \end{aligned} \tag{5.75}$$

Let the effective noise $\mathbf{w} = (\mathbf{F}_m - \mathbf{B}_m)\,\boldsymbol{\rho}_s + \mathbf{F}_m \mathbf{z}$. The MMSE-GDFE filters correspond to the minimization of the variance of the effective noise ε given by:

$$\begin{aligned}
\varepsilon &= \frac{1}{n}\mathcal{E}\left\{\mathbf{w}^t\mathbf{w}\right\} = \frac{1}{n}\mathcal{E}\left\{\mathrm{tr}\left\{\mathbf{w}\mathbf{w}^t\right\}\right\} \\
&= \frac{1}{n}\mathrm{tr}\left\{\mathcal{E}\left\{(\mathbf{F}_m - \mathbf{B}_m)\,\boldsymbol{\rho}_s\boldsymbol{\rho}_s^t(\mathbf{F}_m - \mathbf{B}_m)^t\right\} + \mathcal{E}\left\{\mathbf{F}_m \mathbf{z}\mathbf{z}^t\mathbf{F}_m^t\right\}\right\} \\
&= \frac{1}{n}\mathrm{tr}\left\{(\mathbf{F}_m - \mathbf{B}_m)\,\underbrace{\mathcal{E}\left\{\boldsymbol{\rho}_s\boldsymbol{\rho}_s^t\right\}}_{\sigma_s^2\mathbf{I}_n}(\mathbf{F}_m - \mathbf{B}_m)^t + \mathbf{F}_m\,\underbrace{\mathcal{E}\left\{\mathbf{z}\mathbf{z}^t\right\}}_{\sigma^2\mathbf{I}_n}\mathbf{F}_m^t\right\} \\
&= \frac{\sigma_s^2}{n}\mathrm{tr}\left\{(\mathbf{F}_m - \mathbf{B}_m)\,(\mathbf{F}_m - \mathbf{B}_m)^t + \sigma^2\mathbf{F}_m\mathbf{F}_m^t\right\} \\
&= \frac{\sigma_s^2}{n}\mathrm{tr}\left\{\mathbf{F}_m\mathbf{F}_m^t - \mathbf{F}_m\mathbf{B}_m^t - \mathbf{B}_m\mathbf{F}_m^t + \mathbf{B}_m\mathbf{B}_m^t + \sigma^2\mathbf{F}_m\mathbf{F}_m^t\right\} \\
&= \frac{\sigma_s^2}{n}\mathrm{tr}\left\{\mathbf{F}_m\left(\mathbf{I}_n + \sigma^2\mathbf{I}_n\right)\mathbf{F}_m^t\mathbf{F}_m\mathbf{B}_m^t - \mathbf{B}_m\mathbf{F}_m^t + \mathbf{B}_m\mathbf{B}_m^t\right\}
\end{aligned}$$

Let the matrix $\mathbf{T}$ such that $\mathbf{T}\mathbf{T}^t = (1+\sigma^2)\mathbf{I}_n$ and $\mathbf{G}$ such that $\mathbf{G} = \mathbf{F}_m\mathbf{T}$, then ε is equal to:

$$\begin{aligned}
\varepsilon &= \frac{\sigma_s^2}{n}\mathrm{tr}\left\{\mathbf{G}\left(\mathbf{G} - \mathbf{B}_m\mathbf{T}^{-t}\right)^t - \mathbf{T}^{-1}\mathbf{B}_m^t + \mathbf{B}_m\left(\mathbf{I}_n - \mathbf{T}\mathbf{T}^t\right)^{-1}\mathbf{B}_m^t\right\} \\
&= \frac{\sigma_s^2}{n}\mathrm{tr}\left\{\mathbf{G}\left(\mathbf{G} - \mathbf{B}_m\mathbf{T}^{-t}\right)^t - \mathbf{T}^{-1}\mathbf{B}_m^t + \frac{\sigma^2}{1+\sigma^2}\mathbf{B}_m\mathbf{B}_m^t\right\}
\end{aligned} \tag{5.76}$$

For fixed backward filter $\mathbf{B}_m$ we seek first the optimal forward matrix $\mathbf{F}_m$ which minimizes ε. This minimization requires to have $\mathbf{G} = \mathbf{B}\mathbf{T}^{-t}$ which results in:

$$\mathbf{F}_m = \frac{1}{1+\sigma^2}\mathbf{B}_m \tag{5.77}$$

The corresponding minimum effective noise variance is equal to:

$$\varepsilon_{\min} = \frac{\sigma_s^2}{n}\frac{\sigma^2}{1+\sigma^2}\mathrm{tr}\left\{\mathbf{B}_m\mathbf{B}_m^t\right\} = \frac{\sigma_s^2}{n}\frac{\sigma^2}{1+\sigma^2}\mathrm{tr}\left\{\mathbf{B}_m^t\mathbf{B}_m\right\} \tag{5.78}$$

According to (2.67), the backward filter satisfies $\mathbf{B}_m^t\mathbf{B}_m = \left(1+\sigma^2\right)\mathbf{I}_n$ wich leads to the minimum variance:

$$\varepsilon_{\min} = \sigma_s^2\sigma^2 \tag{5.79}$$

Now, we will show that $\mathbf{F} = \mathbf{F}_m$ and $\mathbf{B} = \mathbf{B}_m$. First, notice from (5.74) that the relations satisfied by the processing matrices $\mathbf{F}$ and $\mathbf{B}$ are similar to the ones satisfied by the MMSE-GDFE filters. The missing piece to prove the equivalence then is to prove

that F and B allow to minimize the variance of the effective noise w. We compute then the corresponding variance refered to as ε_{eq} as:

$$\begin{aligned}
\varepsilon_{eq} &= \frac{\sigma_s^2}{n}\mathrm{tr}\left((F-B)(F-B)^t + \rho^2 FF^t\right) \\
&= \frac{\sigma_s^2}{n}\mathrm{tr}\left(1 + \rho^2 FF^t - FB^t - BF^t + BB^t\right) \\
&\overset{(a)}{=} \frac{\sigma_s^2}{n}\left((1+\rho^2)\mathrm{tr}\left(FF^t\right) - \mathrm{tr}\left(FB^t\right) - \mathrm{tr}\left(BF^t\right) + \mathrm{tr}\left(BB^t\right)\right) \\
&\overset{(b)}{=} \frac{\sigma_s^2}{n}\left((1+\rho^2)\mathrm{tr}\left(F^tF\right) - \mathrm{tr}\left(B^tF\right) - \mathrm{tr}\left(F^tB\right) + \mathrm{tr}\left(B^tB\right)\right) \\
&\overset{(c)}{=} \frac{\sigma_s^2}{n}\Big((1+\rho^2)\mathrm{tr}\left(F^tF\right) - \underbrace{2\,\mathrm{tr}\left(F^tB\right)}_{n} + \underbrace{\mathrm{tr}\left(B^tB\right)}_{(1+\rho^2)n}\Big) \\
&= \frac{\sigma_s^2}{n}\left((1+\rho^2)\mathrm{tr}\left(F^tF\right) + (\rho^2-1)n\right)
\end{aligned}$$

where (a) follows from linearity of trace, (b) follows from commutativity of trace of matrices ($\mathrm{tr}(AB) = \mathrm{tr}(BA)$), (c) follows using $\mathrm{tr}(A) = \mathrm{tr}(A^t)$. Finally, we use the relation $F^tB = I_n$ to deduce that $F^tF = \left(B^tB\right)^{-1}$ which gives $\mathrm{tr}\left(F^tF\right) = \frac{n}{1+\rho^2}$. Consequently we get:

$$\varepsilon_{eq} = \sigma_s^2\rho^2 = \varepsilon_{min} \tag{5.80}$$

This ends the proof.

5.D Modified Cassel's Algorithm

In this appendix we provide a modified Cassels's algorithm to solve the Inhomogenoues Diophantine Approximation in (2.92). The algorithm requires as inputs: the real values $y^0 = -\frac{\gamma}{\alpha}$, $\rho^0 = \frac{\beta}{\alpha}$ and the shaping limit $\mathcal{A}_t$. The algorithm outputs the pair $(\hat{t};\hat{k}) \in (\mathcal{A}_t;\mathbb{N})$ as the best approximation of the real ρ^0given the additive shift y^0. The constraint in line (5) allows to restrict the search in the finite set $\mathcal{A}_t$.

1: $\theta_{-1} = -1; \theta_0 = \rho^0; \theta_{-1} = -y^0;$
2: $t_0 = 0; t_1 = 1; T_1 = 0;$
3: $k_0 = 1; k_1 = 0; K_1 = 0;$
4: $n = 2$
5: while $\theta_{n-1} \neq 0 \wedge \theta_{n-1} \neq 0 \wedge T_{n-1} \in \mathcal{A}_t$ do
6: $\quad a_n = \lfloor \frac{\theta_{n-2}}{\theta_{n-1}} \rfloor;$
7: $\quad t_n = t_{n-2} + a_n t_{n-1}; k_n = k_{n-2} + a_n k_{n-1};$
8: $\quad \theta_n = \theta_{n-2} + a_n \theta_{n-1};$
9: $\quad$ if $K_{n-1} \leq k_{n-1}$ then
10: $\quad\quad b_n = \lfloor \frac{\theta\theta_{n-1} - \theta_{n-2}}{\theta_{n-1}} \rfloor;$

$T_n = T_{n-1} + t_{n-2} + b_n t_{n-1}; K_n = K_{n-1} + k_{n-2} + b_n k_{n-1};$
$\square_n = \square_{n-1} + \square_{n-2} + b_n \square_{n-1};$
else
$T_n = T_{n-1} - t_{n-1}; K_n = K_{n-1} - k_{n-1};$
$\square_n = \square_{n-1} - \square_{n-1};$
end if
$n = n + 1;$
end while
$\hat{t} = T_n;$
$\hat{k} = K_n;$

5.E Optimal Network Code Search Algorithm for the CF in the TWRC

Algorithm 3 Optimal Network Codes Search algorithm for the CF in the TWRC

Input: radius C, matrix G.

Output: the optimal network code vector a_{opt} for real-valued fading TWRC

Step 1 Perform Cholesky decomposition of $G = R^t R$, and set $u_{ii} = R_{ii}^2$ for $i = 1; 2$ and $u_{12} = \frac{R_{12}}{R_{11}}$.

Step 2: Search the candidate vector a minimizing $a^t G a$ according to the procedure:

1. (*Initialization*) Set $i = 2; T_i = C; S_i = 0$.
2. (*Compute bounds for* a_i) Set $Z = \sqrt{\frac{T_i}{u_{ii}}}; UB(a_i) = \lfloor Z - S_i \rfloor; LB(a_i) = \lceil -Z - S_i \rceil$ and set $a_i = LB(a_i) - 1$.
3. (*Increase* a_i) Set $a_i = a_i + 1$, if $[a_i] \bmod p = 0$, go to $a_i = 1$. For $a_i \leq UB(a_i)$ go to 5), else go to 4).
4. if $i = 2$ terminate and output the searched vector $a_{opt} = [a_1\ a_2]^t$, else set $i = i + 1$ and go to 3).
5. (*Decrease* i) For $i = 1$ go to 6), else set $i = i - 1; S_1 = u_{12} a_2; T_1 = C - u_{22} a_2^2$ and go to step 2).
6. Test for $a \in \Gamma_a$. If condition satisfied update $a_{opt} = a$ and if $a^t G a \leq C$ update the radius $C = a^t G a$ and go to 3).

5.F LLL Reduction

Lenstra, Lenstra and Lovàsz introduced in 1982 a new reduction approach called LLL reduction [93]. This algorithm was applied in different fields, from integer polynomial factorization [93], resolution of linear and non-linear programming problems [91], diophantian equation resolution, to cryptography problems. From an application to another, the original algorithm LLL has been modified and led to many algorithm variantes. The most known example is the *LLL with Deep insertions* [104] whose complexity is not polynomial [140]. Let $B = (b_1; :::; b_n)$ denotes a basis of a lattice Λ. In order to reduce this basis, three main steps are considered: orthogonolization, size reduction and vector swap as follows.

- **Orthogonalization**

The principle methods which can be applied to achieve orthogonolization are: Gram Schmidt process, Givens' rotations, Householder reflections and Cholesky decomposition. In our study we use often the Gram Schmidt orthogonolization which is the simplest one. This iterative process, constructs from a basis $B = (b_1; :::; b_n)$, the basis $B^? = (b_1^?; :::; b_n^?)$ defined as:

$$\begin{aligned} b_1^? &= b_1 \\ b_i^? &= b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^? \;\; ; \;\; \forall i = 2; :::; n \\ \mu_{ij} &= \frac{\langle b_i \;\; ; b_j^? \rangle}{\langle b_j^? \;\; ; b_j^? \rangle} \end{aligned} \tag{5.81}$$

Where $\langle :; : \rangle$ denotes the scalar product. Thus, the basis $B^?$ is an orthogonal basis [104].

- **Size reduction**

This step consists on reducing the size of a given basis vectors in order to make them as short as possible and the most orthogonal between them. The used parameters in this step are the Gram Schmidt coefficients μ_{ij}. A basis $B = (b_1; :::; b_n)$ is said size-reduced if these coefficients satisfy the following inequality:

$$| \mu_{ij} | \leq \frac{1}{2}; \;\; 1 \leq i < j \leq n$$

A single basis element is called size-reduced if $| \mu_{ij} | \leq \frac{1}{2}$. The choice of the upper bound $\frac{1}{2}$ comes from the fact that only unimodular transformations bring an equivalent basis of the same lattice. Each coefficient μ_{ij} is quantized by its floor value and is then decremented by this value. The obtained vector b_i is reduced by this quantity multiplied by the vectors b_j ; $j = i - 1; :::; 1$. We detail in the following algorithm the steps of the size-reduction phase.

1: if $| \mu_{k;l} | > \frac{1}{2}$ then

2: $q \leftarrow \lfloor 0{:}5 + \mu_{k;l} \rfloor$
3: $b_k \leftarrow b_k - q b_l$
4: $\mu_{k;l} \leftarrow \mu_{k;l} - q$
5: for $i = 1$ to $l - 1$ do
6: $\mu_{k;i} \leftarrow \mu_{k;i} - q\mu_{k-1;i}$
7: end for
8: end if

- Swap

This unimodular transformation is generally applied in reduction algorithms since it allows a better size-reduction. The most used operation consists of swapping two vectors b_i and b_j when the vector b_i has bigger euclidean norm.
Here we have the Swap procedure algorithm.

1: $b_k \leftrightarrow b_{k-1}$ (Swap b_k an b_{k-1})
2: if $(k \geq 2)$ then
3: for $j = 1$ to $k - 2$ do
4: $\mu_{k;j} \leftrightarrow \mu_{k-1;j}$ (Swap $\mu_{k;j}$ and $\mu_{k-1;j}$)
5: end for
6: end if
7: $\mu \leftarrow \mu_{k;k-1}$
8: $B \leftarrow B_k + \mu^2 B_{k-1}$
9: $\mu_{k;k-1} \leftarrow \mu \frac{B_{k-1}}{B}$
10: $B_k \leftarrow B_{k-1} \frac{B_k}{B}$
11: $B_{k-1} \leftarrow B$

The LLL-algorithm considers the vectors of the basis by pair. Indeed, for $2-$dimensional lattice, the basis $(b_1; b_2)$ is LLL-reduced (Gaussian-Reduced), where $b_1 = b_1^?$ and $b_2 = \mu_{21} b_1^? + b_2^?$, if we have:

$$\frac{\langle b_1 \ ; b_2 \rangle}{\| b_1 \|^2} \leq \frac{1}{2} \| b_1 \|^2 \leq \| b_2 \|^2 \tag{5.82}$$

To guarantee polynomial time termination, the second constraint of (5.82) is released and replaced by:

$$\| b_1 \|^2 \leq \frac{4}{3} \| b_2 \|^2 \tag{5.83}$$

To generalize to a basis $b_1; :::; b_n$, we should recall the Gram-Schmidt Orthogonolization and then proceed as below. The lattice defined by a pair of vectors b_i and b_{i+1} projected orthogonally to $b_1; :::; b_{i-1}$ has basis:

$$b_i(i) = b_i^? \tag{5.84}$$

$$b_{i+1}(i) = b_{i+1}^? + \mu_{i+1;i} b_i^? \tag{5.85}$$

the LLL basis reduction conditions are the following:

$$\begin{aligned} |\ \mu_{ij}\ | &\leq \frac{1}{2};\ 1 \leq i < j \leq n \\ \delta |\ b_i^*\ |^2 &\leq |\ b_{i+1}^* + \mu_{i+1,i} b_i^*\ |^2 \end{aligned} \tag{5.86}$$

The second condition is equivalent to the following one:

$$|\ b_{i+1}^*\ |^2 \geq \left(\delta - \mu_{i+1,i}^2\right) |\ b_i^*\ |^2$$

If the first condition is satisfied, the basis is called size-reduced. The second condition is called Lovàsz condition, and as we can notice, it concerns only adjacent pairs of the basis $b_i; b_{i+1}$. In practice, the used value is $\delta = \frac{4}{3}$. The different steps of the LLL-reduction algorithm are summarized in the following.

Require: basis $B = (b_1; :::; b_n)$ of $n-$dimensional real lattice.

I. Computation of the Gram Schmidt coefficients of the basis vectors $b_i; i = 1; :::; n$
$b_1^* \leftarrow b_1$
$B_1 \leftarrow \langle b_1^*; b_1^* \rangle$
for $i = 2$ to n **do**
    $b_i^* \leftarrow b_i$
    for $j = 1$ to $i - 1$ **do**
        $\mu_{ij} \leftarrow \langle b_i; b_j^* \rangle$
        $b_i^* \leftarrow b_i^* - \mu_{ij} b_j^*$
    end for
    $B_i \leftarrow \langle b_i^*; b_i^* \rangle$
end for
II. Verification of conditions i) et ii)
$k \leftarrow 2$
while $k \leq n$ **do**
    $RED(k; k-1)$
    if $B_k \geq (\frac{3}{4} - \mu_{k;k-1}^2) B_{k-1}$ **then**
        for $l = k - 2$ to 1 **do**
            $RED(k; l)$
        end for
        $k \leftarrow k + 1$
    else
        $SWAP(k)$
        $k \leftarrow \max(2; k - 1)$
    end if
end while

5.G Integer Forcing Linear Receivers

5.G.1 Optimal Preprocessing IF matrix

In this appendix we will show that the sum total achievable rate in (5.42) is uniquely maximized by the preprocessing vector

$$b_m^t = a_m^t H^t \left(H H^t + \frac{1}{\text{SNR}} I_N \right)^{-1} \tag{5.87}$$

For this purpose, define $f(b_m)$ as:

$$f(b_m) = \frac{1}{\text{SNR}} \|b_m\|^2 + \|b_m^t H - a_m^t\|^2 \tag{5.88}$$

Then we have $R_{m;IF}(H; b_m; a_m) = \frac{1}{2} \log^+ \left(\frac{1}{f(b_m)} \right)$. Maximizing the achievable rate with respect to b_m is equivalent then to minimize f with respect to the same vector for fixed a_m. Then we have the following:

$$f(b_m) = \frac{1}{\text{SNR}} b_m^t b_m + \left(b_m^t H - a_m^t \right) \left(H^t b_m - a_m \right) \tag{5.89}$$

$$= \frac{1}{\text{SNR}} b_m^t b_m + b_m^t H H^t b_m - 2 b_m^t H a_m + a_m^t a_m \tag{5.90}$$

$$= b_m^t \left(H H^t + \frac{1}{\text{SNR}} I_N \right) b_m - 2 b_m^t H a_m + a_m^t a_m \tag{5.91}$$

Then, to find the argument which minimizes f, we compute the first derivative with respect to the variable b_m, we get:

$$\frac{\partial f(b_m)}{\partial b_m} = 2 \left(H H^t + \frac{1}{\text{SNR}} I_N \right) b_m - 2 H a_m \tag{5.92}$$

The optimal preprocessing vector satisfies $\frac{\partial f(b_{m;opt})}{\partial b_{m;opt}} = 0$, which is equivalent to have:

$$b_{m;opt}^t = a_m^t H^t \left(H H^t + \frac{1}{\text{SNR}} I_N \right)^{-1} \tag{5.93}$$

5.G.2 Optimal IF Coefficient Matrix

In this appendix we will show that the rate maximum rate $R_{m;IF}(a_m)$ corresponding to the optimal preprocessing vector b_m is given by:

$$R_{m;IF}(a_m) = -\frac{1}{2} \log a_m^t V D V^t a_m \tag{5.94}$$

We have the following:

$$R_{m;IF}(a_m) = \frac{1}{2} \log^+ \left(\frac{1}{f(b_{m;opt})} \right) \tag{5.95}$$

Let us then start with computing $f(b_{m;opt})$:

$$\begin{aligned} f(b_{m;opt}) &= \frac{1}{\rho} b_{m;opt}^t b_{m;opt} + b_{m;opt}^t H H^t b_{m;opt} - b_{m;opt}^t H a_m - a_m^t H^t b_{m;opt} + a_m^t a_m \\ &= b_{m;opt}^t \left(\frac{1}{\rho} I_N + H H^t \right) b_{m;opt} - b_{m;opt}^t H a_m - a_m^t H^t b_{m;opt} + a_m^t a_m \end{aligned} \quad (5.96)$$

Combining (5.93) and (5.96) we get:

$$f(b_{m;opt}) = a_m^t a_m - a_m^t H^t \left(\frac{1}{\rho} I_N + H H^t \right)^{-1} H a_m \quad (5.97)$$

Let $H = U \Sigma V^t$ be the singular value decomposition of H where $U \in R^{N \times N}$ is orthonormal, i.e., $U^{-1} = U^t$, $\Sigma \in R^{N \times M}$ is composed of elements $\Sigma_{ii} = \sigma_i^2$ with σ_i is the i^{th} singular value of the matrix H, and $\Sigma_{ij} = 0$ for $i \neq j$. The matrix $V \in R^{M \times M}$ is unitary and composed of the eigenvectors of the matrix $H^t H$. Accordingly, (5.97) is equivalent to:

$$\begin{aligned} f(b_{m;opt}) &= a_m^t a_m - a_m^t V \Sigma^t U^t \left(\frac{1}{\rho} I_N + U \Sigma \Sigma^t U^t \right)^{-1} U \Sigma V^t a_m \\ &= a_m^t a_m - a_m^t V \Sigma^t U^t \left(U \left(\frac{1}{\rho} I_N + \Sigma \Sigma^t \right) U^t \right)^{-1} U \Sigma V^t a_m \\ &= a_m^t a_m - a_m^t V \Sigma^t U^t U^{t-1} \left(\frac{1}{\rho} I_N + \Sigma \Sigma^t \right)^{-1} U^{-1} U \Sigma V^t a_m \\ &= a_m^t I_M a_m - a_m^t V \Sigma^t \left(\frac{1}{\rho} I_N + \Sigma \Sigma^t \right)^{-1} \Sigma V^t a_m \\ &= a_m^t V V^t a_m - a_m^t V \Sigma^t \left(\frac{1}{\rho} I_N + \Sigma \Sigma^t \right)^{-1} \Sigma V^t a_m \\ &= a_m^t \left[V V^t - V \Sigma^t \left(\frac{1}{\rho} I_N + \Sigma \Sigma^t \right)^{-1} \Sigma V^t \right] a_m \\ &= a_m^t V \left[I_M - \Sigma^t \left(\frac{1}{\rho} I_N + \Sigma \Sigma^t \right)^{-1} \Sigma \right] V^t a_m \end{aligned} \quad (5.98)$$

Let

$$D = I_M - \Sigma^t \left(\frac{1}{\rho} I_N + \Sigma \Sigma^t \right)^{-1} \Sigma \quad (5.99)$$

Given the values of the elements of Σ, it is easy to show that the matrix $D \in R^{M \times M}$ is diagonal such that its components satisfy:

$$D_{ii} = \begin{cases} \frac{1}{1+\rho\sigma_i^2} & \text{if } i \leq \text{rank}(H) \\ 1 & \text{if } i > \text{rank}(H) \end{cases} \quad (5.100)$$

Finally we get:

$$\mathsf{f}\ (\mathsf{b}_{\mathsf{m};\mathsf{opt}}) = \mathsf{a}_{\mathsf{m}}^{\mathsf{t}} \mathsf{V}\, \mathsf{D} \mathsf{V}^{\mathsf{t}} \mathsf{a}_{\mathsf{m}} \tag{5.101}$$

And the desired result follows then by setting $\mathsf{R}_{\mathsf{m};\mathsf{IF}}\,(\mathsf{a}_{\mathsf{m}}) = \frac{1}{2} \log^{+} \left(\frac{1}{\mathsf{f}\,(\mathsf{b}_{\mathsf{m};\mathsf{opt}})} \right)$.

Bibliography

[1] T. Cover and J.A. Thomas. *Elements of Information Theory.* John Wiley & Sons, 1991.

[2] S. Verdú. *Multiuder Detection.* Cambridge University Press, 1998.

[3] A-J. Grant. *Multiple User Information Theory and Coding.* Ph.D dissertation, 1996.

[4] S. Zhang, S-C. Liew, and P-P. Lam. Hot topic: physical-layer network coding. In *Proceedings of the 12th annual international conference on Mobile computing and networking*, MobiCom '06, pages 358–365, New York, NY, USA, 2006. ACM.

[5] P. Popovski and H. Yomo. The anti-packets can increse the achievable throughput of a wireless multi-hop network. In *Proceedings of the International Conference on Communications*, pages 3885–3890, 2006.

[6] P. Popovski and H. Yomo. Bi-directional amplification of throughput in a wireless multi-hop network. In *IEEE 63rd Vehicular Technology Conference*, volume 2, pages 588–593, 2006.

[7] M. Effros, M. Medard, T. Ho, D. Karger S. Ray, R. Koetter, and B. Hassibi. Linear network codes: A unified framework for source, channel, and network coding. 2003.

[8] B. Nazer and M. Gastpar. Compute-and-forward: Harnessing interference with structured codes. In *IEEE International Symposium onInformation Theory*, pages 772–776, 2008.

[9] U. Fincke and M. Pohst. *Improved Methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis*, volume 44. Mathematics of Computation, 1985.

[10] J. Zhan, B. Nazer, M. Gastpar, and U. Erez. Mimo compute-and-forward. In *IEEE International Symposium on Information Theory*, pages 2848–2852, 2009.

[11] J. Zhan, B. Nazer, M. Gastpar, and U. Erez. Integer-forcing linear receivers. In *IEEE International Symposium on Information Theory Proceedings*, pages 1022–1026, 2010.

[12] J. Zhan, B. Nazer, U. Erez, and M. Gastpar. Integer-forcing linear receivers: A new low-complexity mimo architecture. In *In the proceedings of the 72nd IEEE Vehicular Technology Conference Fall*, pages 1–5, 2010.

[13] R.W. Yeung and Z. Zhang. Distributed source coding for satellite communications. *IEEE Transactions on Information Theory*, 45(4):1111–1120, 1999.

[14] R. Ahleswede, N. Cai, S.-Y.R. Li, and R.W. Yeung. Network information flow. *IEEE Transactions on Information Theory*, 46(4):1204–1216, 2000.

[15] S-Y. R. Li, R. W. Yeung, and N. Cai. Linear network coding. *IEEE Transactions on Information Theory*, 49(2):371 – 381, 2003.

[16] R. Koetter and M. Medard. An algebraic approach to network coding. *IEEE/ACM Transactions on Networking*, 11(5):782–795, 2003.

[17] R.W. Yeung, S-Y.R. Li, N.Cai, and Z. Zhang. Network coding theory. *Foundations and Trends in Communications and Information Theory*, 2(4):241–329, 2005.

[18] C. Fragouli and E. Soljanin. Network coding fundamentals. *Foundations and Trends in Networking*, 2(1):1–133, 2007.

[19] T. Ho and L. Desmond. *Network Coding: An Introduction.* Cambridge University Press, New York, NY, USA, 2008.

[20] C. Fragouli and E. Soljanin. Network coding applications. *Foundations and Trends in Networking*, 2(2):135–269, 2007.

[21] C. Fragouli, J-Y. Le Boudec, and J. Widmer. Network coding: An instant primer. *SIGCOMM Comput. Commun. Rev.*, 36(1):63–68, 2006.

[22] C. Fragouli, J. Widmer, and J.-Y. Le Boudec. A network coding approach to energy efficient broadcasting: From theory to practice. In *25th IEEE International Conference on Computer Communications*, pages 1–11, 2006.

[23] Y. Xi and E.M. Yeh. Distributed algorithms for minimum cost multicast with network coding in wireless networks. In *4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, pages 1–9, 2006.

[24] Y. Wu, P.A. Chou, and S.Y. Kung. Information exchange in wireless networks with network coding and physical layer broadcast. *Proceedings of the* 39^{th} Annual Conference on Information Science and Systems, 2005.

[25] J. Dong, R. Curtmola, and R. Sethi et al. Toward secure network coding in wireless networks: Threats and challenges. In *4th Workshop on Secure Network Protocols*, pages 33–38, 2008.

[26] C. Fragouli, D. Katabi, A. Markopoulou, M. Medard, and H. Rahul. Wireless network coding: Opportunities and challenges. In *IEEE Military Communications Conference*, pages 1–8, 2007.

[27] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft. Xors in the air: Practical wireless network coding. *Networking, IEEE/ACM Transactions on*, 16(3):497–510, 2008.

[28] D. Nguyen, T. Tran, T. Nguyen, and B. Bose. Wireless broadcast using network coding. *IEEE Transactions on Vehicular Technology*, 58(2):914–925, 2009.

[29] L. Wang, G. Zhang, C. Ma, and X. Fan. Application research on network coding in wsn. In *Fifth International Conference on Internet Computing for Science and Engineering*, pages 162–166, 2010.

[30] A. Giridhar and P.R. Kumar. Computing and communicating functions over sensor networks. *IEEE Journal on Selected Areas in Communications*, 23(4):755–764, 2005.

[31] http://smarten-itn.eu/.

[32] A. Mejri, G. Rekaya-Ben Othman, and J. C. Belfiore. *Physical Layer Network Coding for Bridge Wireless Monitoring.* Taylor and Frands Group, Biondini and Frangopol editions, London, 2012.

[33] C. Gkantsidis and P. R. Rodriguez. Network coding for large scale content distribution. In *24th Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 4, pages 2235–2245, 2005.

[34] A.G. Dimakis, P.B.Godfrey, Y. Wu, M.J. Wainwright, and K. Ramchandran. Network coding for distributed storage systems. *IEEE Transactions on Information Theory,*, 56(9):4539–4551, 2010.

[35] K. Menger. *Zur allgemeinne kurventheorie*, volume 10. Fundamenta Mathematicae, 1927.

[36] L. R. F. Jr and D.R. Fulkerson. Maximal flow through a network. *Canadian Journal of Mathematics*, 8:399–404, 1956.

[37] P. Elias, A. Feinstein, and C.E. Shannon. Note on maximum flow through a network. *IEEE Transactions on Information Theory*, 2:117–119, 1956.

[38] R. Koetter and M. Medard. An algebraic approach to network coding. *IEEE/ACM Transactions on Networking*, 11(5):782–795, 2003.

[39] S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen. Polynomial time algorithms for multicast network code construction. *IEEE Transactions on Information Theory*, 51(6):1973–1982, 2005.

[40] T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong. A random linear network coding approach to multicast. *IEEE Transactions on Information Theory*, 52(10):4413–4430, 2006.

[41] S. Katti, D. Katabi, W. Hu, H. Rahul, and M. Medard. The importance of being opportunistic: Practical network coding for wireless environments. *Proceedings of the* 43rd *Allerton Conference*, 2005.

[42] Z. Guo, B. Wang, and J.-H. Cui. Efficient error recovery using network coding in underwater sensor networks. *in Proceedings of the* 6th *international IFIP-TC6 conference on Networking*, pages 227–238, 2007.

[43] http://www.ifp.illinois.edu/~koetter/NWC/.

[44] S. Katti, S. Gollakota, and D. Katabi. Embracing wireless interference: analog network coding. In *Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications*, SIGCOMM '07, pages 397–408, New York, NY, USA, 2007. ACM.

[45] T. Koike-Akino, P. Popovski, and V. Tarokh. Denoising maps and constellations for wireless network coding in two-way relaying systems. In *IEEE Global Telecommunications Conference*, pages 1–5, 2008.

[46] T. Koike-Akino, P. Popovski, and V. Tarokh. Optimized constellations for twoway wireless relaying with physical network coding. *IEEE Journal on Selected Areas on Communications*, 27(5):773–787, 2009.

[47] M. El Soussi, A. Zaidi, and L. Vandendorpe. Network coding for the multiple access relay channel using lattices. In *International Symposium on Applied Sciences in Biomedical and Communication Technologies*, pages 1–5, 2010.

[48] C. Hausl and P. Dupraz. Joint network-channel coding for the multiple access relay channel. In *3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, volume 3, pages 817–822, 2006.

[49] P. Popovski and T. Koike-Akino. Coded bidirectional relaying in wireless networks. In *New directions in Wireless Communications Research*, pages 817–822. Springer editions, 2009.

[50] S. Zhang S. Liew and L. Lu. Physical-layer network coding: Tutorial, survey, and beyond. *Elsevier Physical Communication Journal*, 2011.

[51] S. Fu, K. Lu, T. Zhang, Y. Qian, and H. Chen. Cooperative wireless networks based on physical layer network coding. *IEEE Wireless Communications*, 17(6):86–95, 2010.

[52] B. Nazer and M. Gastpar. Reliable computation over multiple-access channels. In *Proceedings of 43rd Annual Allerton Conference on Commununication, Control and Computation*, Monticello, September 2005.

[53] B. Nazer and M. Gastpar. Computing over multi-access channels with connections to wireless network coding. In *Proceedings of the International Symposium on Information Theory*, pages 1354–1358, 2006.

[54] B. Nazer and M. Gastpar. Computation over multiple-access channels. *IEEE Transactions on Information Theory*, 53(10):3498–3516, 2007.

[55] B. Nazer and M. Gastpar. Lattice coding increases multicast rates for gaussian multiple-access networks. In *Proceedings of 45th Annual Allerton Conference on Commununication, Control and Computation*, Monticello, IL, September 2007.

[56] B. Nazer and M. Gastpar. Compute-and-forward: Error-correcting codes for wireless network coding on the physical layer. In *5th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops*, pages 1–5, 2008.

[57] B. Nazer and M. Gastpar. Compute-and-forward: A novel strategy for cooperative networks. In *42nd Asilomar Conference on Signals, Systems and Computers*, pages 69–73, 2008.

[58] U. Niesen and P. Whiting. The degrees of freedom of compute-and-forward. *IEEE Transactions on Information Theory*, 58(8):5214–5232, 2012.

[59] J-C. Belfiore. Lattice codes for the compute-and-forward protocol: The flatness factor. In *IEEE Information Theory Workshop*, pages 1–4, 2011.

[60] M. P. Wilson, K. Narayanan, H. Pfister, and A. Sprintson. Joint physical layer coding and network coding for bi-directional relaying. In *IEEE Transactions on Information Theory*, volume 56, pages 5641–5654, 2010.

[61] K. Narayanan, M. P. Wilson, and A. Sprintson. Joint physical layer coding and network coding for bi-directional relaying. In *Proceedings of the Annual Allerton Conference*, 2007.

[62] C. Feng, D. Silva, and F. Kschischang. An algebraic approach to physical-layer network coding. *IEEE Transactions on Information Theory*, PP(99), 2013.

[63] Z. Zhang and S. Liew. Channel coding and decoding in a relay system operated with physical-layer network coding. *IEEE Jounral on Selected Areas on Communications*, 27(5):788–796, 2009.

[64] B. Hern and K. Narayanan. Multilevel coding schemes for compute-and-forward. In *Proceedings of the IEEE International Symposium on Information Theory*, pages 1713–1717, 2011.

[65] D. Wubben and Yidong Lang. Generalized sum-product algorithm for joint channel decoding and physical-layer network coding in two-way relay systems. In *IEEE Global Telecommunications Conference*, pages 1–5, 2010.

[66] D. To and J. Choi. Convolutional codes in two-way relay networks with physicallayer network coding. In *IEEE Transactions on Wireless Communications*, volume 9, pages 2724–2729, 2010.

[67] B. Nazer and M. Gastpar. Reliable physical layer network coding. *Proceedings of the IEEE transactions on Information Theory*, 99(3):438–460, 2011.

[68] W. Nam, S-Y. Chung, and Y-H. Lee. Capacity bounds for two-way relay channels. In *IEEE International Zurich Seminar on Communications*, pages 144–147, 2008.

[69] W. Nam, S. Chung, and Y. Lee. Capacity of the gaussian two-way relay channel to within 1=2 bit. In *IEEE Transactions on Information Theory*, volume 56, pages 5488–5495, 2010.

[70] L. Lu, T. Wang, S-C. Liew, and S. Zhang. Implementation of physical-layer network coding. In *IEEE International Conference on Communications*, pages 4734–4740, 2012.

[71] S. Zhang and S-C Liew. Physical layer network coding with multiple antennas. In *IEEE Wireless Communications and Networking Conference*, pages 1–6, 2010.

[72] Z. Zhou and B. Vucetic. An optimized network coding scheme in two-way relay channels with multiple relay antennas. In *IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1717–1721, 2009.

[73] R. Zhang, Y-C. Liang, C-C. Chai, and S. Cui. Optimal beamforming for two-way multi-antenna relay channel with analogue network coding. *IEEE Journal on Selected Areas in Communications*, 27(5):699–712, 2009.

[74] D. To, J. Choi, and I-M. Kim. Error probability analysis of bidirectional relay systems using alamouti scheme. *IEEE Communications Letters*, 14(8):758–760, 2010.

[75] A. Khina, Y. Kochman, and U. Erez. Physical-layer mimo relaying. In *IEEE International Symposium on Information Theory Proceedings*, pages 2437–2441, 2011.

[76] B. Nazer. Successive compute-and-forward. 2012.

[77] J. Goseling, J.H. Weber, and M. Gastpar. Compute-and-forward on wireless lattice networks with local interference. In *International Symposium on Wireless Communication Systems*, pages 281–285, 2012.

[78] O. Ordentlich, U. Erez, and B. Nazer. The approximate sum capacity of the symmetric gaussian k-user interference channel. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 2072–2076, 2012.

[79] N. Kashyap, V. Shashank, and A. Thangaraj. Secure compute-and-forward in a bidirectional relay. 2013.

[80] J. Yuan T. Huang and Q-T. Sun. Opportunistic pair-wise compute-and-forward in multi-way relay channels. *to appear in the proceedings of the IEEE International Conference on Communications*, 2013.

[81] M. El Soussi, A. Zaidi, and L. Vandendorpe. Compute-and-forward on a multi-access relay channel: Coding and symmetric-rate optimization. *to appear in the proceedings of the IEEE Transactions on Wireless Communications*, 2013.

[82] M. El Soussi, A. Zaidi, and L. Vandendorpe. Resource allocation for multiple access relay channel with a compute-and-forward relay. In *8th International Symposium on Wireless Communication Systems*, pages 809–813, 2011.

[83] U. Erez, S. Litsyn, and R.Zamir. Lattices which are good for (almost) everything. *IEEE Transactions on Information Theory*, 51(10):3401–3416, 2005.

[84] J. H. Conway and N. J. A. Sloane. *Sphere-packings, lattices, and groups.* Springer-Verlag, New York, USA, 1987.

[85] B. Nazer. *Exploiting Interference through Algebraic Structure.* Ph.D dissertation, 2009.

[86] S. Gupta and M.A. Vazquez-Castro. Physical-layer network coding based on integer-forcing precoded compute and forward. In *IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications*, pages 600–605, 2012.

[87] K.N. Pappi, G. K. Karagiannidis, and R. Schober. How sensitive is compute-and-forward to channel estimation errors. In *To appear in the proceedings of ISIT*, 2013.

[88] E. Viterbo and J. Boutros. A universal lattice code decoder for fading channels. *IEEE Transactions on Information Theory*, 45(5):1639–1642, 1999.

[89] H. Najafi, M.-O. Damen, and A. Hjorungnes. Symbol-asynchronous compute-and-forward. In *IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications*, pages 1830–1834, 2011.

[90] A. Osmane. *Réseaux Spontanés et Auto-Organisants: du codage Spatio-Temporel au Codage de Réseaux.* Ph.D dissertation, 2011.

[91] C. P. Schnorr and M. Euchner. *Lattice Basis Reduction : Improved Practical Algorithms and Solving Subset Sum Problems*, volume 66. Mathematical Programming, 1994.

[92] Y.H. Gan, C. Ling, and W. H. Mow. Complex lattice reduction algorithm for low-complexity full-diversity mimo detection. *IEEE Transactions on Signal Processing*, 57(7):2701–2710, 2009.

[93] A. K. Lenstra, H. W. Lenstra, and L. Lovàsz. Factoring polynomials with rational coefficients. *Matematische Annalen*, 261:515–534, 1982.

[94] C. Feng, D. Silva, and F.R. Kschischang. Blind compute-and-forward. In *IEEE International Symposium on Information Theory Proceedings*, pages 403–407, 2012.

[95] A. Sakzad, E. Viterbo, Y. Hong, and J. Boutros. On the ergodic rate for compute-and-forward. In *International Symposium on Network Coding*, pages 131–136, 2012.

[96] G.D. Forney, M.D. Trott, and S-Y. Chung. Sphere-bound-achieving coset codes and multilevel coset codes. *IEEE Transactions on Information Theory*, 46(3):820–850, 2000.

[97] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Math. Ann.*, 296:625–635, 1993.

[98] D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measure. In *Proceedings of the 45rd annual symposium on foundations of computer science*, pages 371–381, Italy, 2004.

[99] F. Behnamfar, F. Alajaji, and T. Linder. Performance analysis of map decoded space-time orthogonal block codes for non-uniform sources. In *Proceedings of the IEEE Information Theory Workshop*, pages 46–49, 2003.

[100] S.-J. Hwang and P. Schniter. On the optimality of mmse-gdfe pre- processed sphere decoding. In *IEEE Transactions On Information Theory*, volume 56, pages 2121–2129, 2010.

[101] H. El Gamal, G. Caire, and M-O. Damen. Lattice coding and decoding achieve the optimal diversity-multiplexing tradeoff of mimo channels. *IEEE Transactions on Information Theory*, 50(6):968–985, 2004.

[102] J. Jalden and P. Elia. Dmt optimality of lr-aided linear decoders for a general class of channels, lattice designs, and system models. 56(10), 2010.

[103] J-C. Belfiore and C. Ling. The flatness factor in lattice network coding: Design criterion and decoding algorithm. In *International Zurich Seminar on Communications*, 2012.

[104] H. Cohen. *A course in Computational Algebraic Number Theory.* Springer-Verlag, New York, USA, 1993.

[105] F. Lazebnik. *On Systems of Linear Diophantine Equations*, volume 69. Mathematics Magazine, 1996.

[106] T.H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms.* The MIT Press, 2009.

[107] I.V.L. Clarkson. *Approximation of Linear Forms by Lattice Points with Applications to Signal Processing.* Ph.D Thesis dissertation, 1997.

[108] J.W.S. Cassel. *An Introduction to Diophantine Approximation.* Cambridge University Press, 1957.

[109] C. Shannon. Two-way communication channels. *In 4th Berkeley Symposium on Mathematical Statistics and Probability*, 1:611–644, 1961.

[110] S. Kim, N. Devroye, P. Mitran, and V. Tarokh. Achievable rate regions and performance comparison of half duplex bi-directional relaying protocols. *IEEE Transactions on Information Theory*, 57(10):6405–6418, 2011.

[111] I. Ashar, V. Prathyusha, S. Bhashyam, and A. Thangaraj. Outer bounds for the capacity region of a gaussian two-way relay channel. *In the proceedings of the 50th Annual Allerton Conference*, 2012.

[112] Z. Peng and M. Vu. Partial decode-forward coding schemes for the gaussian two-way relay channel. In *In the proceedings of the International Conference in Communications*, pages 2451–2456, 2012.

[113] Y. Tian, D. Wu, C. Yang, and A.F. Molisch. Asymmetric two-way relay with doubly nested lattice codes. *IEEE Transactions on Wireless Communications*, 11(2):694–702, 2012.

[114] H. Liao. *Multiple access channels.* Ph.D dissertation, University of Hawaii, Honolulu, 1972.

[115] R. Ahlswede. Multi-way communication channels. *in Proceedings or the IEEE International Symposimum in Information Theory*, pages 23–52, 1961.

[116] T. Cover. Broadcast channels. *IEEE Transactions in Information Theory*, 18(1):2–14, 1972.

[117] B. Rankov and A. Wittneben. Achievable rate regions for the two-way relay channel. In *In the Proceedings of the IEEE International Symposium on Information Theory*, pages 1668–1672, 2006.

[118] L-L. Xie. Network coding and random binning for multi-user channels. In *10th Canadian Workshop on Information Theory*, pages 85–88, 2007.

[119] Y. Song and N. Devroye. List decoding for nested lattices and applications to relay channels. In *48th Annual Allerton Conference on Communication, Control, and Computing*, pages 1038–1045, 2010.

[120] A-S. Avestimehr, A. Sezgin, and D. Tse. Approximate capacity of the two-way relay channel: A deterministic approach. *In Proceedings of the 46th Annual Allerton Conference*, abs/0808.3145, 2008.

[121] B. Rankov and A. Wittneben. Spectral efficient protocols for half-duplex relay channels. *IEEE Journal in Selected Areas in Communications*, 25(2):379–389, 2007.

[122] T. Oechtering, C. Schnurr, I. Bjelakovic, and H. Boche. Achievable rate region of a two-phase bidirectional relay channel. *In Proceedings of the 41st Conference on Information Sciences and Systems*, 2007.

[123] C. Schnurr, T. J. Oechtering, and S. Stanczak. Achievable rates for the restricted half-duplex two-way relay channel. *In Proceedings of the 41st Asilomar Conference on Signals, Systems and Computers*, pages 1468–1472, 2007.

[124] P. Larsson, N. Johansson, and K.-E. Sunell. Coded bi-directional relaying. *In the proceedings of the IEEE Vehicular Technology Conference*, 2006.

[125] S-J. Kim, P. Mitran, and V. Tarokh. Performance bounds for bidirectional coded cooperation protocols. *IEEE Transactions on Information Theory*, 54(11):5235–5241, 2008.

[126] Y. Louie, Y. Li, and B. Vucetic. Practical physical layer network coding for two-way relay channels: performance analysis and comparison. *IEEE Transactions on Wireless Communications*, 9(2):764–777, 2010.

[127] G. Rekaya-Ben Othman. *Nouvelles constructions algébriques de codes spatio-temporel atteignant le compromis multiplexage-diversité*. Ph.D dissertation, 2009.

[128] W. C. Waterhouse. How often do determinants over finite fields vanish? *Discrete Mathematics*, 65(1):103–104, 1987.

[129] O. Ordentlich and U. Erez. Cyclic coded integer-forcing equalization. In *In the proceedings of the 48th Annual Allerton Conference on Communication, Control, and Computing*, pages 474–478, 2010.

[130] O. Ordentlich and U. Erez. Achieving the gains promised by integer-forcing equalization with binary codes. In *In the proceedings of the IEEE 26th Convention of Electrical and Electronics Engineers in Israel*, pages 000703–000707, 2010.

[131] J. Zhan, U. Erez, M. Gastpar, and B. Nazer. Mitigating interference with integer-forcing architectures. In *In the proceedings of the IEEE International Symposium on Information Theory Proceedings*, pages 1673–1677, 2011.

[132] L. Zheng and D. Tse. Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels. *IEEE Transactions on Information Theory*, 49(5):1073–1096, 2003.

[133] J. Zhan, B. Nazer, U. Erez, and M. Gastpar. Integer-forcing linear receivers. In *Revised for the IEEE Transactions on Information Theory*, pages 1–5, 2013.

[134] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger. Closest point search in lattices. *IEEE Transactions on Information Theory*, 48(8):2201–2214, 2002.

[135] M.-O. Damen, H. El-Gamal, and G. Caire. On maximum-likelihood detection and the search for the closest lattice point. *IEEE Transactions on Information Theory*, 49(10):2389–2402, 2003.

[136] B. Hassibi and H. Vikalo. On the sphere-decoding algorithm i. expected complexity. *IEEE Transactions on Signal Processing*, 53(8):2806–2818, 2005.

[137] J. Jalden and B. Ottersten. On the complexity of sphere decoding in digital communications. *IEEE Transactions on Signal Processing*, 53(4):1474–1484, 2005.

[138] K.R. Kumar, G. Caire, and A.L. Moustakas. Asymptotic performance of linear receivers in mimo fading channels. *IEEE Transactions on Information Theory*, 55(10):4398–4418, 2009.

[139] M. Taherzadeh, A. Mobasher, and A. Khandani. Lll reduction acheives the receive diversity in mimo decoding. *IEEE Trasactions on Information Theory*, 53:4801–4805, 2007.

[140] X. Chen, S. kim, Y. Li, and B. Zheng. Lll algorithm with deep insertions and its applications. *Citeseer*, 2007.

Curriculum Vitae

Asma Mejri
Institut Mines-Télécom, Télécom-ParisTech
46 rue Barrault, 75013, Paris, France
Email: asma.mejri@telecom-paristech.fr

Education

2010 – 2013	Ph.D in Communications and Electronics Télécom-ParisTech, France
2009 – 2010	Ms.c in Telecommunications Higher School of Communications of Tunis (Sup'Com), Tunisia
2007 – 2010	Engineering Dipl. in Telecommunications, Wireless Networks and Communications option Higher School of Communications of Tunis (Sup'Com), Tunisia

Professional Experience

2011 – 2013	Teaching assistant for ComElec Department Télécom-ParisTech, France
2010 – 2013	Early stage researcher for SmartEN Marie Curie ITN project

Awards and Honors

2012	Best paper award, International Conference in Communications and Networking
2010	Laureate for Wireless Networks and Communications option at Sup'Com
2009	Best Entrepreneurship Project Award, Challenge, Sup'Com, Tunisia
2003	Best Student Award in the Tunisian regional phase of the Mathematical Olympiades

Publications

Journal Papers

1. A. Mejri and G. Rekaya-Ben Othman, "The Compute-and-Forward Protocol: Overview and Beyond", in preparation for submission to the IEEE Transactions on Wireless Communications.

Conferences

1. A. Mejri and G. Rekaya-Ben Othman, "Practical Implementation of Integer Forcing Linear Receivers in MIMO Channels", *to appear in the Proceedings of the IEEE* 78^{th} *Vehicular Technology Conference Fall*, USA, September 2013.

2. A. Mejri and G. Rekaya-Ben Othman, "Bidirectional Relaying Via Network Coding: Design algorithm and Performance Evaluation", *to appear in the Proceedings of the International Conference on Telecommunications*, Morocco, May 2013.

3. A. Mejri and G. Rekaya-Ben Othman, "Practical Physical Layer Network Coding in Multi-Sources Relay Channels via the Compute-and-Forward", *to appear in the Proceedings of the Wireless Communications and Netowrking Conference*, China, April 2013.

4. A. Mejri, G. Rekaya-Ben Othman and J-C. Belfiore, "Physical Layer Network Coding for Bridge Wireless Monitoring", *In the Proceedings of the* 6^{th} *International Conference on Bridge Maintenance, Safety and Management*, Italy, July 2012.

5. A. Mejri, G. Rekaya-Ben Othman and J-C. Belfiore, "Lattice Decoding for the Compute-and-Forward Protocol", *In the Proceedings of the Third International Conference in Communications and Networking*, Tunisia, March 2012. **Best Paper Award**.

6. A. Mejri, L. Luzzi and G. Rekaya-Ben Othman, "On the Diversity of the Naive Lattice Decoder", *In the Proceedings of the* 7^{th} *International Workshop on Systems, Signals and Their Applications*, Algeria, May 2011.

Patents Filing

1. A. Mejri and G. Rekaya-Ben Othman, "Méthode de Décodage MAP par Réseau de points augmenté", Filed as a French Patent application by Institut Mines-Telecom, Telecom-ParisTech, October 2013.

Systèmes de Communications Multi-utilisateurs : de la Gestion d'Interférence au Codage de Réseaux

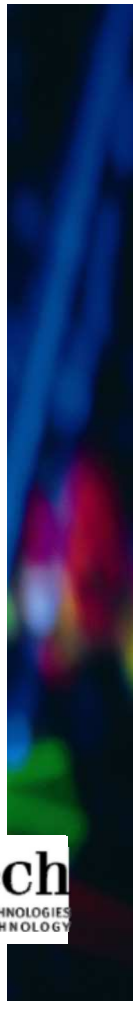
RESUME : Ce travail est dédié à l'analyse, la conception et l'évaluation des performances de schémas de codage de réseaux pour les systèmes de communications multi-termniaux. Nous étudions en premier lieu le protocole Compute-and-Forward dans le canal à accès multiples. Nous proposons un critère de construction de codes de réseaux efficaces pour cette stratégie basé sur la résolution d'un problème du vecteur le plus court d'un réseau de points. En addition, nous développons de nouveaux algorithmes de décodage prouvés numériquement plus performants que le décodeur existant du CF. La deuxième partie de ce travail concerne l'implémentation du protocole CF dans le canal à relais bidirectionnel et le canal à sources et relais multiples. Nous développons des algorithmes de construction de schémas de codage pour le CF et évaluons théoriquement et par simulations numériques leurs performances. La dernière partie concerne le canal MIMO distribué et en particulier une nouvelle architecture de décodeurs Integer Forcing inspirés par le CF. Nous proposons de nouveaux algorithmes de constructions des paramètres optimaux de ces décodeurs et montrons par simulations qu'ils apportent un gain significatif par rapport aux récepteurs linéaires existants.

Mots-Clés : Codage de réseaux au niveau physique, Compute-and-Forward, codage et décodage en réseaux de points.

Multi-user Communication Systems : From Interference Mitigation to Network Coding

ABSTRACT : This work is dedicated to analysis, design and performance evaluation of Physical-Layer Network Coding (PLNC) strategies in multiuser communication systems. The first part is devoted to study the Compute-and-Forward protocol in the basic multiple access channel. For this strategy, we propose an optimal solution to design efficient network codes based on solving a lattice shortest vector problem. Moreover, we derive novel bounds on the ergodic rate and the outage probability for the CF operating in fast and slow fading channels respectively. Besides, we develop novel decoding algorithms proved numerically to outperform the traditional decoding scheme for the CF. The second part is dedicated to the design and end-to-end performance evaluation of network codes for the CF and the Analog Network Coding in the Two-Way Relay Channel and the Multi-Source Multi-Relay channel. For each network model we study the decoding at the relay nodes and the end destination propose search algorithms for optimal network codes for the CF and evaluate, theoretically and numerically, the end-to-end error rate and achievable transmission rate. In the last part we study new decoders for the distributed MIMO channel termed Integer Forcing (IF). Inspired by the CF, IF receivers take advantage of the interference provided by the wireless medium to decode integer linear combinations of the original codewords. We develop in our work efficient algorithms to select optimal IF receivers parameters allowing to outperform existing suboptimal linear receivers.

Keywords : Physical-Layer Network Coding, Compute-and-Forward, lattice codes, lattice decoding.



TELECOM ParisTech

EDITE

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY