



HAL
open science

Lattice Decoding for the Compute-and-Forward Protocol

Asma Mejri, Ghaya Rekaya-Ben Othman, Jean-Claude Belfiore

► **To cite this version:**

Asma Mejri, Ghaya Rekaya-Ben Othman, Jean-Claude Belfiore. Lattice Decoding for the Compute-and-Forward Protocol. Third International Conference on Communications and Networking (ComNet), Mar 2012, Tunis, Tunisia. pp.1-8, 10.1109/ComNet.2012.6217737 . hal-00714518

HAL Id: hal-00714518

<https://hal.science/hal-00714518>

Submitted on 4 Jul 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Lattice Decoding for the Compute-and-Forward Protocol

Asma Mejri [†], Ghaya Rekaya-Ben Othman [†] and Jean Claude Belfiore [†]

[†] Dept. of Communications and Electronic

Telecom-ParisTech, 46 Rue Barrault, 75013 Paris, France

Email: {asma.mejri, rekaya, belfiore}@telecom-paristech.fr

Abstract—In this work we focus exclusively on the Compute-and-Forward (C&F) protocol as a channel coding-based approach for Physical Layer Network Coding. The Core principle of this relaying strategy is based on using Nested Lattice Codes. The source nodes in a relay network encode their messages into lattice codewords and transmit them to the relay. The latter receives a noisy mixing of these codewords and decodes an integer linear combination of them for sequential transmission.

To the best of our knowledge, all existent works related to the Compute-and-Forward protocol study only its theoretical limits and no experimental analysis has been proposed so far. Our contribution through this work concerns a plethora of practical aspects, related to lattice decoding for the C&F, that need to be solved to achieve the promising potential of this strategy. We propose practical decoding approaches and investigate the achieved diversity order and identify the relevant parameters that may influence it. We provide simulation results to compare the performance of the different proposed decoding approaches and to link theoretical results with practical aspects.

Index Terms—Network Coding, Physical Layer Network Coding, Lattice Coding and Decoding, Compute-and-forward

I. INTRODUCTION

Network Coding (NC) framework was first proposed in [1] for wired networks. To enhance the channel capacity, relay nodes operate some computation on the received packets after decoding them. Hence, the relay combines the received decoded packets and forwards them to the following nodes. NC can be considered as a new technique of performing routing, which allows to achieve higher capacity. For the case of Linear Network Coding, outgoing packets are linear combinations of the received packets taken over finite fields [2]-[3]. We illustrate this scheme in Fig.1.

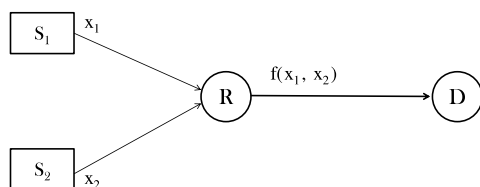


Fig. 1. Principle of Network Coding.

In [4] and [5], authors prove that NC achieves the optimal network capacity for multi-cast flows and provides gain in terms of throughput.

In wireless settings, several transmission problems, that don't

exist in the wired case, occur. First of all, resource allocation represents a big deal since many users share the same channel and then it becomes more difficult to equally enable different users, having different needs and constraints, to access the wireless medium. In addition, with the evolution of wireless applications and networks, the demand has been increasing, but in the same time, spectral resources are being scarce and are not sufficient to satisfy all the demands. Besides, compared to the wired networks, in wireless channels, energy efficiency represents an important constraint to consider, since wireless terminals use chargeable batteries and have to consume as less as possible power in order to be reliable enough. Finally, in wireless networks, the medium suffers from multi-path fading as well as interference due to the broadcast and superposition properties. All these problems result in loss in performance. From this raises the interest of Wireless Network Coding (WNC), based on exploiting the interference provided by the channel in order to improve the network performance. WNC turns the broadcast and superposition properties into boosting characteristics for achieving higher transmission rates and increasing the network throughput. Several works have been interested in NC in wireless frameworks [6]. In [7], authors exhibit the opportunities offered by WNC and the efficiency of this technique is proved for both uni-cast and multi-cast schemes. In [8], authors exhibit the advantages of WNC beyond traditional routing in both lossless and lossy wireless networks. Several practical systems were proposed to bridge theory with practice. In [9] and [10], authors investigate the factors that can affect the gains provided by WNC. They prove, experimentally, that the performance of WNC depend on the traffic, the number of flows, the topology of the network as well as the kind of the traffic. WNC can be implemented in the Network Layer, the MAC Layer or the Physical Layer. When applied in the physical layer, WNC is called Physical Layer Network Coding or PLNC [11], and can be performed joint to modulation-demodulation techniques [12] and channel coding. The first difference between such techniques and the WNC performed in upper layer is that the source nodes send their messages simultaneously not sequentially, the second difference is that the PLNC is a signal-space based NC. In fact, the relay mixes the received signals without decoding each one of them separately, in contrast to the case of NC, where the relay decodes the packets then combines the decoded bits for sequential transmission. In this work, we

focus exclusively on a channel coding-based PLNC strategy called 'Compute and Forward' (C&F). This protocol was first proposed by Gastpar and Nazer in [13] for Multiple Access Relay Channel where k users transmit n multidimensional information messages to one or more destinations helped by relay nodes. The latter, exploit the noisy linear combination of the original messages, provided by the channel, to decode noiseless linear integer equations of them and forward them to destination node. Receiving enough linear equations of the original transmitted messages, the destination decodes the desired messages. The proposed scheme is based on nested lattice codes since they have good statistical and algebraic structure properties that allow to achieve the capacity of the point-to-point AWGN channels and approach performance of standard random coding [14]-[15]. An interesting property of these codes is that they guarantee that integer combinations of transmitted codewords are themselves codewords. In [15] authors highlight the existence of such codes for which a relay node is able to decode lattice equations from the received lattice codewords' combination.

In this work we consider practical implementation of the C&F for the case of 2 users and investigate the case of one-dimensional source signal in which the source nodes transmit scalar real constellations. Then we address the case of two-dimensional source signal using a ST-coding design proposed in [30] for the Multiple Access Channel (MAC). For both schemes we study decoding techniques and focus on practical aspects that impact the diversity gain. Simulation results show that: first, the C&F relaying strategy meets its promised potential and provides better performance than the MAC decoding scheme. Then, the achieved diversity gain depends on the choice of the coefficients of the decoded function at the relay as well as on the constellation size for the one-dimensional scheme and on the lattice code for the multi-dimensional case.

The remainder of this paper is organized as follows: section II is dedicated to the system model and assumptions. The third section deals with the Compute-and-Forward protocol and the different steps necessary to perform it. We focus exclusively on the lattice decoding approaches and investigate the parameters that impact their performance. In the fourth section we are interested in the case of one-dimensional real constellations and we analyze the diversity order of the Compute-and-Forward and present some simulation results. Then we address an example of two-dimensional lattice coding design.

II. PROBLEM STATEMENT AND NOTATIONS

A. Notational Conventions

Through this paper we use the notations as follows: vectors and matrices are written in bold font, in lower and upper case, respectively. \mathbf{A}^\dagger and \mathbf{A}^t denote respectively the hermitian and the normal transpose of the matrix \mathbf{A} . For a vector \mathbf{a} , $\|\mathbf{a}\|$ denotes its euclidean norm.

B. System Model

We consider a Gaussian MAC composed of k sources S_1, \dots, S_k transmitting messages $\mathbf{x}_1, \dots, \mathbf{x}_k$ to one relay node R. The received signal \mathbf{y} at R is a linear combination of the messages $\mathbf{x}_i, i = 1 \dots k$ corrupted by noise. \mathbf{y} can be written as:

$$\mathbf{y} = \sum_{i=1}^k h_i \mathbf{x}_i + \mathbf{z} \quad (1)$$

where h_i denotes the channel coefficient between the source S_i and the relay, h_i are complex, circular, i.i.d Gaussian, $h_i \sim \mathcal{N}(0, 1)$. \mathbf{x}_i represents the transmitted information vector by source S_i and lives in an n -multidimensional lattice Λ_i assumed full rank, and \mathbf{z} stands for additive noise, zero-mean with variance σ^2 . Let $\mathbf{h} = [h_1, \dots, h_k]^t$ denote the vector of the channel coefficients unknown at the transmitters. We assume that Channel Side Information is only available at the relay node. Each transmitter only needs to know its target message rate. ρ stands for the Signal to Noise Ratio(SNR) at the relay node, $\rho = \frac{E_{av}}{\sigma^2}$. where E_{av} denotes the average energy per symbol. For the one-dimensional lattice case, the transmitted signals x_i are scalars that belong to real PAM constellations defined by $C = \{x_i \in [-S_m, S_m], S_m \in \mathbb{Z}\}$.

C. Problem Statement

When receiving the noisy linear combination of the original messages, the relay attempts to decode a noiseless integer combination λ of the messages \mathbf{x}_i in the following form:

$$\lambda = \sum_{i=1}^k a_i \mathbf{x}_i \quad (2)$$

where the coefficients $a_i \in \mathbb{Z}, i = 1, \dots, k$, are chosen by the relay as a function of an optimization scheme. λ lives in a lattice Λ such that

$$\Lambda = a_1 \Lambda_1 + \dots + a_k \Lambda_k \quad (3)$$

Gastpar and Nazer in [13] propose to choose the coefficient vector $\mathbf{a} = [a_1, \dots, a_k]^t$ that maximizes the Computation Rate defined in the next section. The relay recovers an estimate $\hat{\lambda}$ of the lattice point λ . A decoding error occurs if $\hat{\lambda} \neq \lambda$. Then, the error probability of C&F strategy is:

$$\mathbf{P}_e = \Pr(\hat{\lambda} \neq \lambda) \quad (4)$$

We highlight that decoding errors for the C&F don't consider the errors on individual vectors \mathbf{x}_i in contrast to the MAC decoding for which a decoding error occurs if at least one of the vectors \mathbf{x}_i is not correctly decoded, then, the MAC error probability \mathbf{P}_e can be expressed as

$$\mathbf{P}_e = \Pr(\cup_{i=1}^k \hat{\mathbf{x}}_i \neq \mathbf{x}_i) \quad (5)$$

III. COMPUTE-AND-FORWARD STRATEGY

The relay computes the lattice point $\lambda = \sum_{i=1}^k a_i \mathbf{x}_i$ by choosing the coefficient vector $\mathbf{a} = [a_1, \dots, a_k]^t$. In the following subsections we expose the three steps needed to perform the Compute-and-Forward.

A. Step 1: Scaling of the channel output

The transmitted vectors $\mathbf{x}_i, i = 1, \dots, k$, are carved from lattice codes which guarantee that any integer linear combination of the codewords is a codeword. However, in the considered model, the received linear combination of the transmitted codewords is no longer integer since the channel coefficients are complex (or real). Authors in [13] provide an elegant solution to this problem which consists in scaling the received signal by a factor α such that the obtained vector, $\tilde{\mathbf{y}} = \alpha\mathbf{y}$, is made as close as possible to an integer linear combination of the original codewords. Thus, the scaled channel output can be expressed as:

$$\begin{aligned}\tilde{\mathbf{y}} &= \alpha\mathbf{y} = \alpha \left(\sum_{i=1}^k h_i \mathbf{x}_i + \mathbf{z} \right) \\ &= \underbrace{\sum_{i=1}^k a_i \mathbf{x}_i}_{\lambda} + \underbrace{\sum_{i=1}^k (\alpha h_i - a_i) \mathbf{x}_i + \alpha \mathbf{z}}_{\text{Effective Noise}}\end{aligned}$$

The approximation of $\tilde{\mathbf{y}}$ by λ depends on the scaling factor α . Indeed, large values of α result in good approximations and yield the achievable rates [16]. However, large values of α amplify the noise and make the achievable rates low. This trade-off of approximation and noise enhancement was investigated in [13] where authors propose an approach to optimally choose the parameter α .

B. Step 2: Choice of the coefficient vector and the scaling factor

Gastpar and *Nazer* show in [13], Theorem 1, that for a given channel vector $\mathbf{h} = [h_1, \dots, h_k]^t$, a relay can recover any set of coefficient vector $\mathbf{a} = [a_1, \dots, a_k]^t$ while the message rates are less than the computation rate R_{comp} given by:

$$R_{\text{comp}}(\mathbf{h}, \mathbf{a}) = \log \left(\left(\|\mathbf{a}\|^2 - \frac{\rho \|\mathbf{h}^\dagger \mathbf{a}\|^2}{1 + \rho \|\mathbf{h}\|^2} \right)^{-1} \right) \quad (6)$$

Since the aim of the Compute-and-Forward strategy is to provide means to achieve higher data rates, the optimal values of the coefficient vector \mathbf{a} that look promising are those which maximize the computation rate R_{comp} , then:

$$\hat{\mathbf{a}} = \underset{\mathbf{a} \neq \mathbf{0}}{\operatorname{argmax}} \{R_{\text{comp}}(\mathbf{h}, \mathbf{a})\} \quad (7)$$

In [17], authors show that the maximization problem of equation (7) is equivalent to the minimization problem given by:

$$\hat{\mathbf{a}} = \underset{\mathbf{a} \neq \mathbf{0}}{\operatorname{argmin}} \{\mathbf{a}^t \mathbf{G} \mathbf{a}\} \quad (8)$$

where \mathbf{G} is a definite positive hermitian matrix given by:

$$\mathbf{G} = \mathbf{I} - \frac{\rho}{1 + \rho \|\mathbf{h}\|^2} \mathbf{H} \quad (9)$$

$\mathbf{H} = [H_{ij}]; H_{ij} = h_i h_j^\dagger; 1 \leq i, j \leq k$.

The minimization problem in equation (8) remains to the

minimization of the quadratic form given by the matrix \mathbf{G} . Solving equation (8) is equivalent to finding $\hat{\mathbf{a}}$ equal to the shortest vector in the lattice $\Lambda_{\mathbf{G}}$ whose Gram matrix is \mathbf{G} [17], and the coefficients $a_i, i = 1, \dots, k$, satisfy $\gcd(a_1, \dots, a_k) = 1$. In practical settings the Shortest Vector Problem can be solved using the Fincke-Pohst algorithm [18]-[19].

After finding $\hat{\mathbf{a}}$ maximizing the computation rate, the scaling factor α is computed. Its optimal value considering the same framework of *Nazer* and *Gastpar* corresponds to the MMSE coefficient proved to approach the capacity of linear Gaussian channels in lattice-based strategies. Its expression is given by [20]:

$$\alpha = \alpha_{\text{MMSE}} = \frac{\rho \mathbf{h}^\dagger \mathbf{a}}{(1 + \rho \|\mathbf{h}\|^2)} \quad (10)$$

C. Step 3: Decoding of Lattice Equation

The expression of the scaled channel output is given by:

$$\tilde{\mathbf{y}} = \lambda + \sum_{i=1}^k (\alpha h_i - a_i) \mathbf{x}_i + \alpha \mathbf{z}$$

which can be written as:

$$\tilde{\mathbf{y}} = \lambda + \sum_{i=1}^k \xi_i \mathbf{x}_i + \tilde{\mathbf{z}} \quad (11)$$

where $\xi_i = \tilde{h}_i - a_i, i = 1, \dots, k$, and $\tilde{h}_i = \alpha h_i$ is the i^{th} scaled channel coefficient. $\tilde{\mathbf{z}} = \alpha \mathbf{z}$ represents the scaled noise.

Now, the relay is required to decode λ from $\tilde{\mathbf{y}}$.

The decoding metric for the Maximum Likelihood (ML) criterion is based on maximizing the conditional probability $p(\tilde{\mathbf{y}}/\lambda)$ over all possible values of $\lambda \in \Lambda$, given by the expression,

$$\hat{\lambda} = \underset{\lambda \in \Lambda}{\operatorname{argmax}} \{p(\tilde{\mathbf{y}}/\lambda)\} \quad (12)$$

Since $\lambda = \sum_{i=1}^k a_i \mathbf{x}_i$, equation (12) is equivalent to

$$\hat{\lambda} = \underset{\lambda \in \Lambda}{\operatorname{argmax}} \sum_{\substack{(\mathbf{x}_1, \dots, \mathbf{x}_k) / \\ \sum_{i=1}^k a_i \mathbf{x}_i = \lambda}} p(\tilde{\mathbf{y}}/(\mathbf{x}_1, \dots, \mathbf{x}_k)) p(\mathbf{x}_1, \dots, \mathbf{x}_k) \quad (13)$$

We assume that $\mathbf{x}_1, \dots, \mathbf{x}_k$ are equiprobable, and since

$$p(\tilde{\mathbf{y}}/\mathbf{x}_1, \dots, \mathbf{x}_k) \propto \exp \left(\frac{-1}{2\sigma^2} \left\| \tilde{\mathbf{y}} - \sum_{i=1}^k \tilde{h}_i \mathbf{x}_i \right\|^2 \right)$$

the decoding rule in (13) is equivalent to,

$$\hat{\lambda} = \underset{\lambda \in \Lambda}{\operatorname{argmax}} \sum_{\substack{(\mathbf{x}_1, \dots, \mathbf{x}_k) / \\ \sum_{i=1}^k a_i \mathbf{x}_i = \lambda}} \exp \left(\frac{-1}{2\sigma^2} \left\| \tilde{\mathbf{y}} - \sum_{i=1}^k \tilde{h}_i \mathbf{x}_i \right\|^2 \right) \quad (14)$$

Let

$$\varphi(\lambda) = \sum_{\substack{(\mathbf{x}_1, \dots, \mathbf{x}_k) / \\ \sum_{i=1}^k a_i \mathbf{x}_i = \lambda}} \exp \left(\frac{-1}{2\sigma^2} \left\| \tilde{\mathbf{y}} - \sum_{i=1}^k \tilde{h}_i \mathbf{x}_i \right\|^2 \right)$$

This function is studied in details within the next paragraph for the one dimensional lattice case using finite constellations. It

will be shown that , under some assumptions, φ can be flat, i.e its maximum can be achieved for different values of λ , which impacts the system's diversity and makes the maximization problem in (12) hard to achieve. Belfiore in [21] introduces a so-called *Flatness Factor* describing the conditions to be satisfied to solve the ML decoding problem defined herein. The ML decoder is not the unique approach to perform lattice decoding for the Compute-and-Forward protocol. In what follows, we investigate some suboptimal decoders.

IV. SUBOPTIMAL LATTICE DECODING APPROACHES

A. Diophantine Approximation

This method is an approximation of the ML decoding. Its core principle is to express the decoding metric in equation (14) as a function of λ by replacing each one of $\mathbf{x}_i, i = 1, \dots, k$ by some function of the lattice equation λ . Since we have $\lambda = \sum_{i=1}^k a_i \mathbf{x}_i$, expressing \mathbf{x}_i as a function of λ remains to solve the system of Diophantine Equations defined by $\lambda = \sum_{i=1}^k a_i \mathbf{x}_i$. For the multidimensional case where k users transmit n -dimensional lattice codewords, this system can be solved using the *Hermite Normal Form* [21]-[18]. For simplification reasons, we explain, in what follows, this decoding technique for one-dimensional finite constellation case for 2 users introduced in [22]. In this case, the transmitted vectors \mathbf{x}_1 and \mathbf{x}_2 are integer scalars taken in a PAM constellation defined by $[-S_m, S_m], S_m \in \mathbb{Z}$. Then we get $\lambda = a_1 x_1 + a_2 x_2$, and the scaled received signal at the relay is $\tilde{y} = \lambda + \xi_1 x_1 + \xi_2 x_2 + \tilde{z}$. In this case, the ML solution $\hat{\lambda}$ satisfies

$$\begin{aligned} \hat{\lambda} &= \underset{\lambda \in \mathbb{Z}}{\operatorname{argmax}} \sum_{\substack{(x_1, x_2) / \\ a_1 x_1 + a_2 x_2 = \lambda}} \exp\left(\frac{-1}{2\sigma^2} \|\tilde{y} - \tilde{h}_1 x_1 - \tilde{h}_2 x_2\|^2\right) \\ &= \underset{\lambda \in \mathbb{Z}}{\operatorname{argmax}} \varphi(\lambda) \end{aligned} \quad (15)$$

where

$$\varphi(\lambda) = \sum_{\substack{(x_1, x_2) / \\ a_1 x_1 + a_2 x_2 = \lambda}} \exp\left(\frac{-1}{2\sigma^2} \|\tilde{y} - \tilde{h}_1 x_1 - \tilde{h}_2 x_2\|^2\right)$$

Our aim now is to express φ as a function of λ only. We need to solve the *Diophantine Equation* $\lambda = a_1 x_1 + a_2 x_2$. This equation admits solutions since $\gcd(a_1, a_2) = 1$ (\mathbf{a} is solution of a Shortest Vector Problem), then we start with solving $a_1 x_1 + a_2 x_2 = 1$. A particular solution (u_1, u_2) can be derived using the *Extended Euclid Algorithm* [23], and the set of all solutions is the following:

$$\begin{cases} x_1 = u_1 \lambda + a_2 k \\ x_2 = u_2 \lambda - a_1 k \end{cases} \quad (16)$$

where $k \in \mathbb{Z}$. Thus, we can write $\varphi(\lambda)$ as,

$$\hat{\lambda} = \underset{\lambda \in \mathbb{Z}}{\operatorname{argmax}} \underbrace{\sum_{k=-\infty}^{+\infty} \exp\left(\frac{-1}{2\sigma^2} \|\tilde{y} - \gamma \lambda + \beta k\|^2\right)}_{\varphi(\lambda)} \quad (17)$$

where $\gamma = \tilde{h}_1 u_1 + \tilde{h}_2 u_2$, $\beta = a_1 \tilde{h}_2 - a_2 \tilde{h}_1$ and $k \in \mathbb{Z}$.

1) *Properties of $\varphi(\lambda)$* : As we can easily see, φ is a sum of Gaussian functions, it is periodic and has the following properties:

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

$\varphi(\lambda)$ depends then on the Signal to Noise Ratio, the channel coefficients, the coefficient vector $\mathbf{a} = [a_1 \ a_2]^t$ and obviously on the constellation bounds defined by S_m . We illustrate an example of φ through Fig.2.

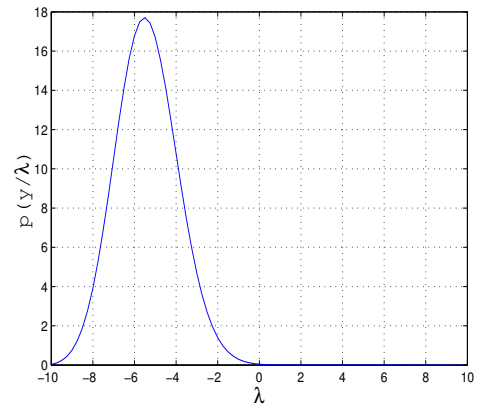


Fig. 2. SNR = 10dB, $S_m = 5$, $\mathbf{h} = [0.895, 0.731]^t$, $\mathbf{a} = [-1, -1]^t$.

2) *Diophantine Approximation*: We address here the possible values of $\hat{\lambda}$ which maximizes φ .

- $\lambda \in \mathbb{R}$: φ is maximized for λ satisfying $\tilde{y} - \gamma \lambda + \beta k = 0$. Then we get

$$\hat{\lambda} = \frac{\tilde{y}}{\gamma} + \frac{\beta}{\gamma} k \Rightarrow \hat{\lambda} \in \frac{\tilde{y}}{\gamma} + \frac{\beta}{\gamma} \mathbb{Z} \quad (18)$$

The obtained values must guarantee that $x_i, i = 1, 2$ belong to the finite constellation $[-S_m, S_m]$.

- $\lambda \in \mathbb{Z}$: φ is maximized for λ which minimizes $|\tilde{y} - \gamma \lambda + \beta k|$, hence,

$$\hat{\lambda} = \underset{\substack{(\lambda, k) / \\ (x_1, x_2) \in [-S_m, S_m]^2}}{\operatorname{argmin}} \{|\tilde{y} - \gamma \lambda + \beta k|\} \quad (19)$$

This minimization problem consists in solving the *Inhomogeneous Approximation in the absolute sens* [25], $F(\lambda, k)$, defined as,

$$F(\lambda, k) = |\tilde{y} - \gamma \lambda + \beta k| \quad (20)$$

which is equivalent to the minimization problem given by:

$$\hat{\lambda} = \underset{\substack{(\lambda, k) / \\ (x_1, x_2) \in [-S_m, S_m]^2}}{\operatorname{argmin}} \left\{ |\beta' k - \lambda + \tilde{y}'| \right\} \quad (21)$$

where $\beta' = \frac{\beta}{\gamma}$ and $\tilde{y}' = \frac{\tilde{y}}{\gamma}$. It corresponds to finding the approximations $\frac{\lambda}{k}$, $k \in \mathbb{Z}$ of the real number β' , assumed an additional real number \tilde{y}' .

In practice, the Diophantine Approximation can be solved using an Exhaustive Decoding which we use in our implementation. Another way to do consists in using the *Cassell's Algorithm* [26] which has to be modified in order to guarantee that the resulting solution (λ, k) ensures that $x_i, i = 1, 2$, belong to the constellation.

In the following, we propose a suboptimal approach for lattice equation decoding which is an approximation of the method based on the Diophantine Approximation.

B. MMSE-GDFE+SD

The proposed decoding rule is valid for the n -multidimensional case with k users.

1) *Decoding Rule*: An approximation of the minimization problem defined in equation (14) consists in finding $\hat{\lambda}$ satisfying,

$$\hat{\lambda} = \underset{\substack{(\mathbf{x}_1, \dots, \mathbf{x}_k) / \\ a_1 \mathbf{x}_1 + \dots + a_k \mathbf{x}_k = \lambda}}{\operatorname{argmax}} \exp \left(\frac{-1}{2\sigma^2} \left\| \tilde{\mathbf{y}} - \sum_{i=1}^k \tilde{h}_i \mathbf{x}_i \right\|^2 \right) \quad (22)$$

The maximization problem of (22) can be equivalently written as,

$$\hat{\lambda} = \underset{\substack{(\mathbf{x}_1, \dots, \mathbf{x}_k) / \\ a_1 \mathbf{x}_1 + \dots + a_k \mathbf{x}_k = \lambda}}{\operatorname{argmin}} \left\| \tilde{\mathbf{y}} - \tilde{\mathbf{h}}^t \mathbf{X} \right\|^2 \quad (23)$$

where $\tilde{\mathbf{h}} = [\tilde{h}_1, \dots, \tilde{h}_k]^t$ is the vector of the scaled channel coefficients and the matrix $\mathbf{X}^{k \times n}$ such that its i^{th} row corresponds to the message vector transmitted by the source S_i . This problem corresponds to solve the Closest Vector Problem (CVP) by finding the nearest lattice point $\hat{\mathbf{x}} = (\hat{x}_1, \dots, \hat{x}_k)$ to the received point representing the vector $\tilde{\mathbf{y}}$ in the lattice $\Lambda_{\tilde{\mathbf{h}}^t}$ of generator matrix $\mathbf{H} = \tilde{\mathbf{h}}^t$. Then, $\hat{\lambda}$ is computed by $\hat{\lambda} = \sum_{i=1}^k a_i \hat{x}_i$. The Sphere Decoder (SD) algorithm allows to solve the CVP problem [27]-[28].

One can notice that this system represents a rank deficiency. To overcome this problem, we perform an MMSE-GDFE preprocessing [29] before applying the SD. In the following paragraph we outline the principle of the MMSE-GDFE.

2) *MMSE-GDFE preprocessing*: The MMSE-GDFE pre-filtering is composed of two filters, a Forward filter \mathbf{F} and a Backward filter \mathbf{B} . In order to derive the expression of \mathbf{F} and \mathbf{B} , we proceed as follows. We define the augmented matrix $\mathbf{H}_{\text{aug}}^{(k+1) \times k}$ by,

$$\mathbf{H}_{\text{aug}} = \begin{pmatrix} \mathbf{H} \\ \frac{1}{\sqrt{\rho}} \mathbf{I}^{k \times k} \end{pmatrix}$$

then we consider its QR decomposition

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

where \mathbf{Q} is orthogonal matrix and \mathbf{R} is upper triangular. Then we can write $\mathbf{H} = \mathbf{Q}_1 \mathbf{R}$, and get the expressions of the filters

as: $\mathbf{F} = \mathbf{Q}_1^t$ and $\mathbf{B} = \mathbf{R}$.

The MMSE-GDFE transforms the system in (23) into the non equivalent problem given as

$$\hat{\mathbf{x}} = \underset{\mathbf{x}=(\mathbf{x}_1, \dots, \mathbf{x}_k)}{\operatorname{argmin}} \left\| \mathbf{F}\tilde{\mathbf{y}} - \mathbf{B}\mathbf{x} \right\|^2 \quad (24)$$

V. ONE-DIMENSIONAL FINITE CONSTELLATIONS: DIVERSITY ANALYSIS AND NUMERICAL RESULTS

Our examination of the diversity is based on an outage probability analysis. For the Multiple Access Channel decoding, the system is in outage if all the links from each source $S_i, i = 1, \dots, k$ to the relay node are in outage. Decoding error occurs if $\hat{\mathbf{x}}_i \neq \mathbf{x}_i, i = 1, \dots, k$. Thus for the MAC, the diversity order is $d_{\text{MAC}} = k$. However, for the Compute-and-Forward, the error events consider only errors on $\hat{\lambda}$. We address in the following the outage probability analysis in the case of the Compute-and-Forward for the case of two users, $k = 2$.

A. Case of two users ($k = 2$)

We define the error events $\varepsilon_1, \varepsilon_2$ and ε_3 as follows

- ε_1 : Only the link from S_1 to the relay is in outage
- ε_2 : Only the link from S_2 to the relay is in outage
- ε_3 : both links from the sources to the relay are in outage

thus, the total error probability is:

$$\mathbf{P}_e = \mathbb{P}(\varepsilon_1) + \mathbb{P}(\varepsilon_2) + \mathbb{P}(\varepsilon_3)$$

where $\mathbb{P}(\varepsilon_i)$ denotes the probability of the error event ε_i . Now let's analyze the error events. We focus our asymptotic analysis on the high SNR values regime.

As we saw within the first section, the basic parameter of the C&F is the coefficient vector $\mathbf{a} = [a_1, a_2]^t$ which maximizes the Computation Rate R_{comp} . From [13], we can write R_{comp} as follows,

$$R_{\text{comp}} = \underbrace{\log(1 + \rho \|\mathbf{h}\|^2)}_{\text{Capacity of MAC}} - \underbrace{\log(\|\mathbf{a}\|^2 + \rho(\|\mathbf{h}\mathbf{a}\|^2 - |\mathbf{h}^t \mathbf{a}|^2))}_{\text{Loss in Rate}}$$

We can easily observe that maximizing R is equivalent to minimizing the loss in Rate due to using the coefficient vector \mathbf{a} , which is equivalent to align \mathbf{a} to \mathbf{h} (they become colinear). Consequently, the period $p = \frac{a_1 \tilde{h}_2 - a_2 \tilde{h}_1}{2\sigma^2}$ of $\varphi(\lambda)$ becomes null. This results in a flatness of φ and impossibility to decode the right $\hat{\lambda}$ maximizing φ since the maximum can be obtained for different values of λ .

Now, for the error events, say that one of the links l_i from the source S_i to the relay is in outage, for example, the link from S_1 and the relay. Thus, for high SNR, \mathbf{a} becomes aligned to \mathbf{h} and we can write $a_i = ch_i, i = 1, 2; c$ is a constant, and the C&F decodes $\hat{\lambda} = c(h_1 x_1 + h_2 x_2)$. Since l_1 is in outage then $h_1 \simeq 0 \Rightarrow a_1 = 0$ and $a_2 = \pm 1$ (\mathbf{a} is solution of the shortest vector in \mathbf{Z}^2), hence $\hat{\lambda} \neq 0$, and a correctly decoded λ can be obtained. We deduce that the error events of ε_1 and ε_2 are not the dominant error events and the overall error probability is dominated by ε_3 . The diversity order of the C&F is $d_{\text{C&F}} = 2$, and for the general case, with k users, $d_{\text{C&F}} = k$. Notice that this is valid for the case of complex channel coefficients. In our

implementations, we consider the real channel case, thus the achieved diversity order of the Compute-and-Forward would be equal to 1.

B. Loss of diversity

As we have seen, the loss of diversity for the Compute-and-Forward is due to the flatness of the error probability $\varphi(\lambda)$.

- **Case of small Constellation size:** In this case, the diversity is equal to 1 and it is easy to decode the maximum of $\varphi(\lambda)$ since we can distinguish a peak corresponding to the unique $\hat{\lambda}$ for which φ is maximum. We illustrate an example of this case for SNR = 60dB and $S_m = 5$ in Fig.3. The values of h_i and a_i confirm that \mathbf{a} corresponds well to an aligned vector to \mathbf{h} and $\hat{\lambda} = 0$ is easily decodable.

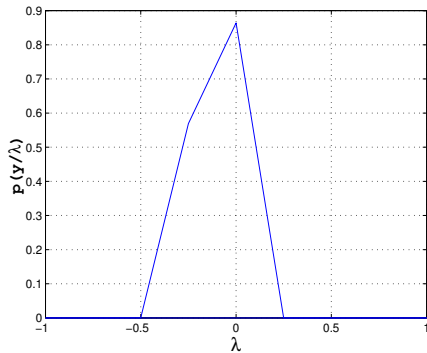


Fig. 3. SNR = 60dB, $S_m = 5$, $x_1 = 3, x_2 = 0, \mathbf{h} = [0.04, 0.6771]^t, \mathbf{a} = [0, -1]^t$.

For the same constellation size, $S_m = 5$ and for moderate SNR, it is relevant that the diversity is not achieved since it is an asymptotic parameter that must be observed at high SNR values. This confirms the behavior of φ in Fig.4 for SNR = 10dB. The maximum value is obtained for tow integer values $\lambda_1 = -7$ and $\lambda_2 = -6$ while the correctly decodable value must be $\hat{\lambda} = -6$ for the corresponding values of x_1 and x_2 .

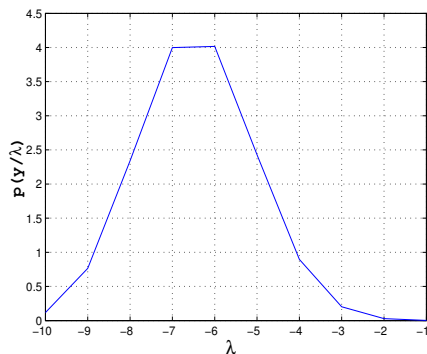


Fig. 4. SNR = 10dB, $S_m = 5$, $x_1 = 0, x_2 = -6, \mathbf{h} = [1.1909, 1.1892]^t, \mathbf{a} = [-1, 1]^t$.

- **Case of High Constellation size:** φ depends on the constellation S_m . For high range of S_m , a large set of the couple (x_1, x_2) has to be scanned, the width of φ becomes large and φ is made flat. Thus, decoding the maximal value of λ becomes ambiguous which results in a loss of diversity which becomes 1/2. We confirm this analysis by the results illustrated in Fig.5. We can see that the error probability attains its maximum for two values $\hat{\lambda} = -1$ and $\lambda = 0$, while the correctly decoded value is $\lambda = 0$. Thus, when the constellation size increases from $S_m = 5$ (Fig.3) to $S_m = 10$ (Fig.5), we loose the full diversity.

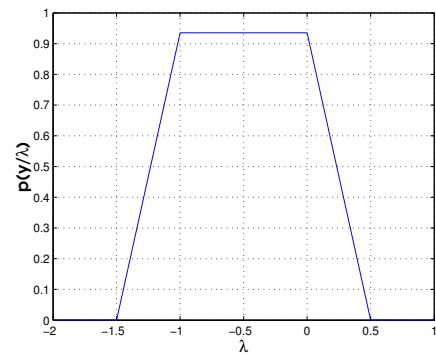


Fig. 5. SNR = 60dB, $S_m = 10, x_1 = 0, x_2 = -7, \mathbf{h} = [-0.8, 0.05]^t, \mathbf{a} = [-1, 0]^t$.

C. Simulation Results

In this subsection we address the results of the simulation of the different lattice decoding techniques we have seen so far, in particular the MMSE-GDFE+SD and the Diophantine Approximation (DA). We consider the case of two users transmitting symbols $x_i \in [-S_m, S_m], i = 1, 2$. And we analyze the Error probability as a function of the SNR at the relay for the Compute-and-Forward and for the MAC decoding, which consists in decoding both x_1 and x_2 separately. As plotted in Fig.6, the Compute-and-Forward meets its promised potential and provides elegant solutions to the interference problem that was traditionally considered difficult. The C&F provides a gain of 30dB at a SER = 10^{-3} over the MAC decoding. The Diophantine Approximation offers better performance than the MMSE-GDFE+SD, and achieves a gain of 7.5dB at SER = 10^{-3} , however it does not bring a diversity gain.

In Fig.7 we illustrate the performance of the C&F and MAC Decoding using the Diophantine Approximation. Through this figure, we make a numerical proof of our theoretical analysis as far as the diversity order of the C&F is considered. We show that for small constellation size, the achieved diversity order is 1, and for higher constellation size, e.g $S_m = 7$ and $S_m = 10$, the diversity order is limited to 1/2. In addition, increasing constellation range results in performance degradation.

So far, we investigated different lattice decoding approaches for the Compute-and-Forward protocol, and we made an analysis for the diversity order of this protocol. We defined a

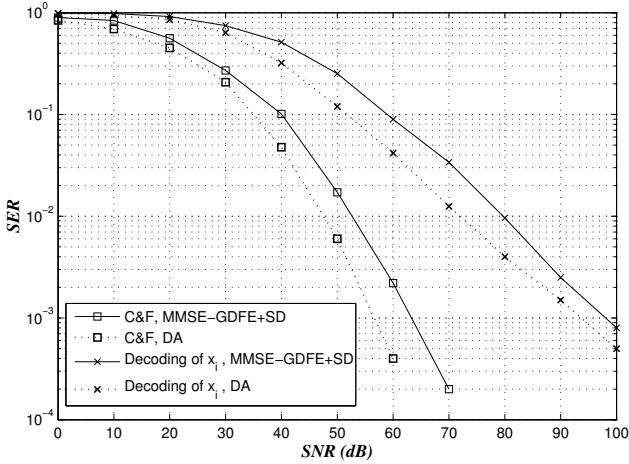


Fig. 6. Performance of the CF for 2 users scheme and temporal dimension $n=1$.

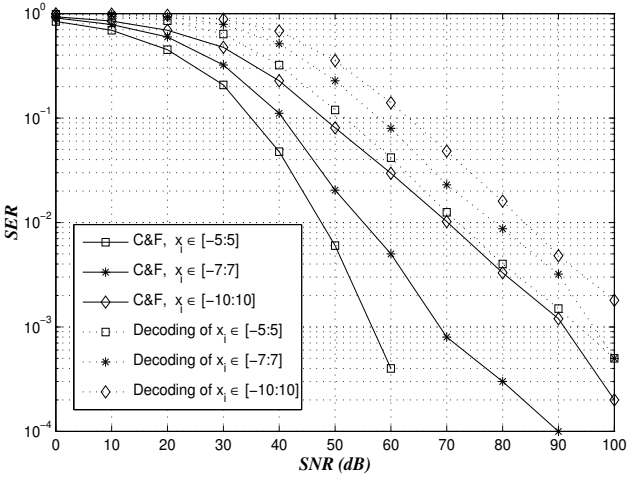


Fig. 7. Impact of the constellation bounds on the performance of the Compute-and-Forward.

probability function $\varphi(\lambda)$ of the lattice equation to be decoded, and we have seen through our analysis of the 2 users transmitting one-dimensional uncoded information message (without performing lattice coding), that the flatness of this function causes the loss of diversity and that the larger the constellation size is, the worst the performance are. So what would be the case of the multidimensional scheme in which each one of the k -sources transmits an n -dimensional codeword? the answer to this question is driven in the next section.

VI. MULTIDIMENSIONAL-LATTICES

A. Coding design for 2 users

1) *Motivation:* Our aim in this section consists in investigating the performance of the lattice decoding approaches we studied in section 2 for the coded scheme, where a source node S_i transmits a codeword $\mathbf{x}_i \in \Lambda$. We were inspired from the Space-Time Coding design considered for Multiple Access Channels in [30]. This coding approach offers a higher

diversity by making a joint coding of the individual codes of the source nodes. Since this scheme improves the performance and provides diversity gains for the MAC case, while decoding separate \mathbf{x}_i , we propose to use the same scheme in order to examine the performance of the C&F, and decoding of $\lambda = a_1\mathbf{x}_1 + \dots + a_k\mathbf{x}_k$ in coded case.

2) *Lattice Code Construction:* Let $\mathbf{s}_1 = [s_{11}, s_{12}]^t$ and $\mathbf{s}_2 = [s_{21}, s_{22}]^t$ be the information messages of the source S_1 and S_2 respectively, $s_{ij} \in \text{QAM}$ constellations represents the symbol transmitted by the source i during the time slot j . These messages are mapped to two codewords \mathbf{x}_1 and \mathbf{x}_2 respectively, given by:

$$\begin{aligned} \mathbf{x}_1 &= [\alpha(s_{11} + s_{12}\theta) \bar{\alpha}(s_{11} + s_{12}\bar{\theta})]^t \\ \mathbf{x}_2 &= [\gamma\alpha(s_{21} + s_{22}\theta) \bar{\alpha}(s_{21} + s_{22}\bar{\theta})]^t \end{aligned} \quad (25)$$

where $\alpha = 1 + i - i\theta$, $\theta = \frac{1+\sqrt{5}}{2}$, and $\gamma = i$.

3) *Decoding technique:* We use the MMSE-GDFE+SD decoding technique to estimate the codewords $\hat{\mathbf{x}}_1$ and $\hat{\mathbf{x}}_2$, then we construct the estimate lattice equation $\hat{\lambda} = a_1\hat{\mathbf{x}}_1 + a_2\hat{\mathbf{x}}_2$. A decoding Error is detected if $\hat{\lambda} \neq \lambda (= a_1\mathbf{x}_1 + a_2\mathbf{x}_2)$.

4) *Simulation results:* In Fig.8 we plot the performance of the proposed coding scheme for both the Compute-and-Forward protocol and the MAC decoding.

We deduce that the coding design, although solved the problem of poor diversity order for Multiple Access Channel in [30], it is not adequate for the Compute-and-Forward strategy, and does not provide any coding gain. Much more rigorous lattice code designs have to be adapted for physical Layer network coding based on the Compute-and-Forward protocol and a closer examination of the decoding metric using ML criterion has to be made in order to derive the necessary conditions for such code constructions.

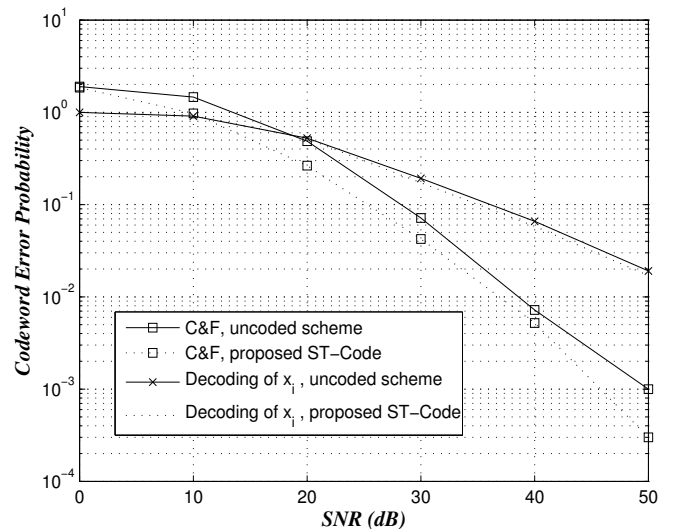


Fig. 8. Performance of the proposed coding scheme for 2 users.

B. Higher dimensions: The Flatness Factor

As we have seen for the one-dimensional case, the probability function $\varphi(\lambda)$ can be flat, and this flatness has to be avoided in order to get better performance and to achieve maximal diversity. For the general multidimensional lattice, Belfiore defines in [21] a parameter, called *The Flatness Factor* which describes the flatness of the function $\varphi(\lambda)$ and represents the ratio between the average and the maximal value of $\varphi(\lambda)$. This parameter is of a prime importance related to the lattice decoding for the Compute-and-Forward protocol.

VII. CONCLUSION AND PROSPECTIVES

In this work we proposed a review on the Compute-and-Forward relaying strategy and investigated promising lattice decoding approaches through both theoretical and experimental analysis. For the C&F, a relay node is required to decode a linear integer combination of the original transmitted codewords. We studied optimal lattice decoding approach based on the ML criterion and examined suboptimal decoding techniques using the Diophantine Approximation and the MMSE-GDFE preprocessing followed by the Sphere Decoder. Our analysis allowed to characterize the behavior of the error probability as a function of the lattice equation to be decoded, and point out the relevant parameters involved in the decoding stage.

We examined the limits for the case of one-dimensional finite real constellations and showed that a performance degradation and diversity order loss for the C&F are reported when the constellation size increases. This result was experimentally translated by the flatness of the error probability function.

This loss of diversity order inspired us to examine the performance of the C&F for 2-dimensional lattices using a joint coding design introduced in [30] as a solution to the decreasing diversity order in Multiple Access Channel. We have shown through simulations that these constructions are not sufficient to establish optimal performance for the C&F strategy. A tight study of the error probability function, and in particular the flatness factor, is imperative to fulfill lattice constructions for reliable C&F based PLNC.

ACKNOWLEDGMENTS

This work was supported by the project SmartEN which has received funding from the European Union People Program (FP7/2007-2013), under grant agreement n° 238726.

REFERENCES

- [1] R.Ahlsweide, N. Cai, S.-Y. R, and W. Yeung, "Network Information Flow", *IEEE Transactions On Information Theory*, Vol. 46, pp. 1204-1216, July 2000.
- [2] S.-Y. R. Li, R. W. Yeung and N.Cai, "Linear Network Coding", *IEEE Transactions On Information Theory*, Vol. 49, no. 2, pp. 781-381, Feb 2003.
- [3] R. Koetter and M. Medard, "An Algebraic Approach To Network Coding", *IEEE/ACM Transactions On Networks*, Vol. 11, pp. 782-795, October 2003.
- [4] C.Fragouli, J.Le Boudec and J.Widmer, "Network Coding: An Instant Primer", *Simulation*, 2005.
- [5] Fang-chun Kuo, "Exploiting Network Coding in Lossy Wireless Networks", *Thesis Dissertation*, June 2009.
- [6] S.Deb, M.Effros, T.Ho, D.Karger, R Koetter, Ralf Lun, and M. Muriel, "Network Coding For Wireless Applications: A Brief Tutorial", *International Workshop on Wireless Ad-hoc Networks*, May 2005.
- [7] C.Fragouli, D.Katabi, A.Markopoulou, M.Mdard and H.Rahul, "Wireless Network Coding: Opportunities and Challenges", *IEEE Military Communication Conference, MILCOM*, pp. 1-8, 2007.
- [8] Desmond.S Lun, M.Medard and R.Koetter, "Efficient Operation Of Wireless Packet Networks Using Network Coding", *International Workshop On Convergent Technologies*, 2005.
- [9] S.Katti, H.Rahul, d.Katabi et al, "XORs in the Air: Practical Wireless Network Coding", *IEEE/ACM Transactions on Networking*, Vol. 16, No. 3, June 2006.
- [10] I. Qazi, P. Gandhi, "Performance Evaluation Of Wireless Network Coding under Practical Setings", *Technical Report*, Department of Compter Science, University of Pittsburgh, May 2007.
- [11] S. Zhang, S.C. Liew and P.Lam, "Hot Topic: Physical Layer Network Coding", *Proceedings of the 12th Annual International Conference on Mobile Computing and Networking*.
- [12] S. Fu, K. Lu, T. Zhang, Y. Qian and H. H. chen, "Cooperative Wireless Networks Based On Physical Layer Network Coding", *IEEE Wireless Communications*, Vol. 17, pp. 86-95, December 2010.
- [13] B. Nazer and M.Gastpar, "Compute and Forward: Harnessing Interference through Structured Codes", *IEEE International Symposium On Information Theory, ISIT*, pp. 772-776, August 2008.
- [14] B. Nazer and M. Gastpar, "Lattice Coding increases Multicast Rates for Gaussian Multiple Access Networks", *Proceedings of 45th Annual Allerton Conference on Communication, Control and Computation*, Monticello, September 2007.
- [15] B. Nazer and M. Gastpar, "The Case for Structured Random Codes in Network Communication Theorems", *ITW*, Lake Tahoe, September 2007.
- [16] U. Niesen and P. Whiting, "The degrees of freedom of the Compute-and-Forward", *IEEE International Symposium on Information Theory*, pp. 1081-1085, July 2011.
- [17] Chen Feng, D. Silva and F.R. Kschischang, "An algebraic approach to physical Layer Network Coding", *IEEE International Symposium On Information Theory Proceedings (ISIT)*, pp. 1017-1021, 2010.
- [18] H. Cohen, "A Course in Computational Algebraic Number Theory", *Springer-Verlag*, 1993, pp. 103-105, Section 2.7.3: Finding Small Vectors in Lattices.
- [19] U. Fincke and M. Pohst, "Improved methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis", *Math. Comp.* 44, pp. 463-471.
- [20] G. David Forney Jr, "On The role of MMSE estimation in approaching the information-theoretic limits of linear Gaussian Channels: Shannon meets Wiener", *Proceeding, Allerton Conference*, pp. 430-439, October 2003.
- [21] J.-C.Belfiore, "Lattice Codes for the Compute-and-Forward Protocol: The Flatness Factor", *IEEE Information Theory Workshop*, October 2011.
- [22] A.Osmane and J.-C. Belfiore, "The Compute-and-Forward Protocol: Implementation and Practical Aspects", not published, available on arXiv, <http://arxiv.org/abs/1107.0300>.
- [23] T.H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, "Introduction to Algorithms", Third Edition. *The MIT Press*, 2009, pp. 933-939, Section 31.2: Greatest Common Divisor.
- [24] D. Micciancio and O. Regev, "Worst Case to average-case reductions based on Gaussian Measure", *SIAM J. On Computing*, pp. 276-302, May 2007.
- [25] I. V. L. Clarkson, "Approximation of Linear Forms by Lattice Points with Applications to Signal Processing", *Thesis Dissertation*, January 1997.
- [26] J. W. S. Cassel, "An Introduction to Diophantine Approximation", *Cambridge University Press*, 1957.
- [27] E. Agrell, T. Eriksson, A. Vardy and K. Zeger, "Closest Point Search in Lattices", *IEEE Transactions on Information Theory*, Vol. 48, pp. 2201-2214, August 2002.
- [28] J. Conway and N. Sloane, "Sphere Packings, Lattices and Graphs", *Springer-Verlag*, 1993.
- [29] S.-J. Hwang and P. Schniter, "On The Optimality of MMSE-GDFE Pre-processed Sphere Decoding", *IEEE Transactions on Information Theory*, Vol. 56, pp. 2121-2129, 2010.
- [30] M. Badr, "Space-Time Block Codes Constructions for MIMO Multiple-Access Channels", *Thesis Dissertation*, January 2010.