Practical Physical Layer Network Coding in Multi-Sources Relay Channels via the Compute-and-Forward

Asma Mejri and Ghaya Rekaya-Ben Othman
Telecom ParisTech, 46 Rue Barrault, 75013 Paris, France, amejri,rekaya@telecom-paristech.fr

Abstract—**Recent years have witnessed the development of the Compute-and-Forward (CF) as a successful solution to perform noiseless linear Physical Layer Network Coding (PLNC). Research outcomes shed considerable light on the promising gain of this strategy from information-theoretic perspective. What misses is to design practical PLNC schemes based on the Compute-and-Forward and to evaluate their end-to-end performance in real communication scenarios. In this work we try to fill the gap between theory and practice: we investigate end-to-end communication over a Multi-Sources Relay Channel where the CF is used at intermediate nodes. We figure out practical constraints that deserve special attention in real end-to-end communication design and propose reliable solutions that enable to meet the promised potential of the CF. In order to confirm our theoretical analysis, we evaluate performance of the proposed schemes at the destination in terms of both average achievable rate and error rates under practical low complexity nested lattice encoding.**

Index Terms—**Physical Layer Network Coding, Compute-and-Forward, Lattice Coding and decoding.**

I. Introduction

Interference due to the broadcast and superposition properties of the wireless medium might seem disadvantegeous at first sight. Nevertheless, a new perspective called Physical Layer Network Coding revealed its advantage for more efficient and reliable transmission. The core principle of this framework is to allow intermediate nodes in wireless multi-hops relay networks including multiple access channels decode and forward *a function of originally transmitted signals* [1]. Our interest in this work goes to a recently developed class of PLNC termed the *Compute-and-Forward.* It is a promising solution to perform noiseless linear PLNC by exploiting interference provided by the channel through the use of structured lattice codes [2] constructed using linear codes over Finite Fields. Existing works on the Compute-and-Forward have shown its promising potential and shed considerable light on its merits. Several coding schemes as well as design algorithms for coefficients vectors have been proposed [3],[4]-[5]. However, these research findings either look at the related issues to the CF from an information theoretic perspective, or consider only local optimization at relays' level. What is missing is to understand, design and evaluate the end-to-end-performance of a practical Compute-and-Forward-based Physical Layer Network Coding schemes. In this work we try to fill this gap between theory and practice considering end-to-end communication over a Multi-Sources Relay Channel (MSRC) where source nodes want to communicate their messages drawn from a finite field to a common destination. We investigate two transmission schemes based on the CF: a first scheme termed *CCF* for Complete-CF in which relay nodes compute and forward a codeword from the same nested lattice as the sources'codewords. The second scheme termed *ICF* (I for Incomplete) for which intermediate relays compute and forward any integer linear combinations of original codewords which does not necessarily belong the nested lattice. This framework does not match exactly the original scheme of Gastpar and Nazer in [2], nevertheless, it is considered in several works [6]-[7]. For instance, in [6] the DEFID scheme is proposed as a practical low-complexity design for the CF. Our contributions in this regard are:

- We figure out for both schemes practical constraints related to the full rank of the network coefficients matrix over the finite field for the CCF and the full rank of the network coefficients matrix over the integers for ICF.
- We propose two algorithms to solve the derived full rank constraints for both schemes.
- We provide end-to-end performance evaluation and comparison of the two schemes at destination node in terms of both achievable rates and message error rates using a practical low-complexity nested lattice code over $\mathbb{Z}_p$ for p prime and considering the case of 2 sources, 2 relays and one common destination.

Remaining flow of this work is organized as follows: notational conventions are introduced in section II. In section III. the MSRC model and assumptions are addresed. In section VI. we review the encoding and decoding steps of the original framework of the CF. The considered practical nested lattice code is also described in this section. Following sections are dedicated to the CCF and ICF schemes respectively. For each transmission scheme, processing at both relays and destination are described, the decodability condition at the destination is highlighted and solved. End-to-end performance evaluation of the proposed algorithms is the focus of the section VIII. A concluding section ends the work.

II. Notational conventions

Through this work we use the notations as follows: vectors and matrices are written in bold font, in lower and upper case respectively. $\mathbb{R}$ denotes the field of reals. $\mathbb{F}_p$ denotes the size p finite field, where p is assumed always prime. $+$ and $\sum$ denote

978-1-4799-0110-4/13/$31.00 ©2013 IEEE

respectively the addition and summation operations over the real field. $\oplus$ and $\bigoplus$ represent the addition and summation operations over the finite field. $\mathbf{A}^{-1}$ represents the inverse of the matrix $\mathbf{A}$. Let $g : \mathbb{F}_p \to \{0, ..., p-1\}$ denote the one-to-one mapping function that associates each element in the finite field to an integer in $\mathbb{Z}_+$. g^{-1} denotes its inverse mapping. $\langle \mathbf{x}^t, \mathbf{y} \rangle$ represents the euclidean scalar product of $\mathbf{x}$ and $\mathbf{y}$. log operation is assumed with respect to base 2 and $\log^+(x) = max(\log(x), 0)$.

III. Multi-Sources Relay Channel: system model and assumptions

We consider the $K-$MSRC composed of K sources, K relays and one destination as illustrated in Fig.1. All nodes are equipped with a single antenna and operate in half duplex mode. For ease of presentation, only real-valued channels are considered in this work. Results can be easily extended to the complex-valued channels case using the complex-to-real transformations of [2].

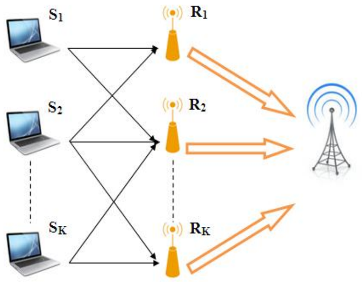

Fig. 1. Multi-Sources Relay Channel.

End-to-End Communication objective: each source node S_i in this network has a message $\mathbf{w}_i$ of length k drawn i.i.d from a prime size field $\mathbb{F}_p$ according to a uniform distribution . The sources desire to send their data to the common destination which is interested in recovering *all original messages* $\mathbf{w}_1, ..., \mathbf{w}_K$. In absence of direct links from the sources to the destination, intermediate nodes help the formers forward their messages in multi-hops relay fashion using the Compute-and-Forward. To achieve the communication objective, two transmission phases are needed:

1) ***Phase 1***: it lasts one time slot. The processing at each node in the network is as follows:
   - *Sources*: each source node maps its message $\mathbf{w}_i$ into an $n-$dimensional codeword $\mathbf{x}_i$ satisfying a symmetric power constraint given by: $\frac{1}{n}\mathrm{E}\| \mathbf{x}_i \|^2 \leq P$ for $P > 0$ and $i = 1, ..., K$. Then all sources transmit simultaneously their codewords through the channel. Due to the broadcast nature of the wireless medium, the codeword of each source reaches all the relay nodes.
   - *Relays*: The concurrent transmission by the source nodes makes each relay R_m receive a superposition of the codewords. Received signal at a relay R_m can be modeled as an output of a Multiple Access Channel (MAC) in the form
$$\mathbf{y}_m = \sum_{i=1}^{K} h_{im}\mathbf{x_i} + \mathbf{z}_m \qquad (1)$$
     where h_{im} denotes the real, i.i.d Gaussian channel coefficient between the source S_i and the relay R_m, $\mathbf{z}_m$ stands for a zero-mean Additive White Gaussian Noise of variance σ^2. Channel State Information is available only at the relays, i.e. each relay R_m knows only its corresponding channel vector $\mathbf{h}_m = [h_{1m} \ ... \ h_{Km}]$. We denote by ρ the Signal to Noise Ratio equal to $\rho = \frac{P}{\sigma^2}$. Each relay decodes a linear function $\lambda_m = f(\mathbf{x}_1, ..., \mathbf{x}_K)$. Coefficients of this function constitute the network code vector $\mathbf{a}_m$.
   - *Destination*: it remains idle in absence of direct links to the sources.
2) ***Phase 2***: it lasts K time slots and corresponds in the following:
   - *Sources*: during this phase source nodes are idle
   - *Relays*: each relay forwards its computed function and network code vector to the destination during one separate time slot. Links from the relays to the end destination are assumed perfects.
   - *Destination*: receives $\lambda_1, ..., \lambda_K$ and $\mathbf{a}_1, ..., \mathbf{a}_K$ from the relays and attempts to recover original messages $\mathbf{w}_1, ..., \mathbf{w}_K$.

Before formally describing the end-to-end transmission schemes, we provide in the following section an overview on the Compute-and-Forward.

IV. Compute-and-Forward: overview

The framework of the Compute-and-Forward proposed by Nazer and Gastpar in [2] consists in two parts: encoding part at sources using nested lattice codes, and decoding part at a receiver observing the output of a MAC based on minimum distance decoding. Before describing the encoding and decoding schemes we provide in the following few lattice definitions that are essential to understand the technical details. We refer interested readers to [8] for more information about lattice theory.

A. Lattice definitions

Definition IV.1 *An n-dimensional **lattice** Λ is a set of points of $\mathbb{R}^n$, $\Lambda = \{\mathbf{x} = \mathbf{M}\mathbf{s}, \mathbf{s} \in \mathbb{Z}^n\}$. $\mathbf{M}$ is called a generator matrix of the lattice. The points $\mathbf{x} \in \Lambda$ represent the lattice codewords and satisfy linearity, i.e. for any $a, b \in \mathbb{Z}$ and $\mathbf{x}, \mathbf{y} \in \Lambda$, $a\mathbf{x} + b\mathbf{y} \in \Lambda$.*

Definition IV.2 *A **lattice quantizer** Q_Λ is the mapping that takes real vector $\mathbf{x}$ to the nearest point in the lattice Λ in Euclidean distance: $Q_\Lambda(\mathbf{x}) = \mathrm{argmin}_{\lambda \in \Lambda} \| \mathbf{x} - \lambda \|$.*

Definition IV.3 *The **Voronoi Region** of a lattice point denotes the set of points that quantize to that point. The **fundamental***

Voronoi Region *$\mathcal{V}_\Lambda$ of a lattice Λ corresponds to the voronoi region of the zero vector.*

Definition IV.4 *The* $\mathbf{mod} - \boldsymbol{\Lambda}$ ***modulo operation*** *returns the quantization error with respect to Λ. For $\mathbf{x} \in \mathbb{R}^n$: $[\mathbf{x}] \,\text{mod}\Lambda = \mathbf{x} - Q_\Lambda(\mathbf{x})$.*

Definition IV.5 *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: $\Lambda = \{\lambda = [\lambda_{\text{F}}] \,\text{mod}\Lambda_{\text{C}}, \lambda_{\text{F}} \in \Lambda_{\text{F}}\}$*

B. Encoding scheme using Nested Lattice Codes

The encoding part of the original framework of the Compute-and-Froward is based in its essence on a high-dimensional capacity achieving Nested Lattice Codes. They are constructed based on linear codes over finite fields. The idea behind this design is to conserve linearity while mapping from finite field messages to codewords: messages of the sources are drawn i.i.d from a finite field $\mathbb{F}_p$ and mapped to codewords from a nested lattice code using a bijective mapping: $\phi : \mathbb{F}_p \longrightarrow \Lambda = \mathcal{V}_{\text{C}} \cap \Lambda_{\text{F}}$ such that $\mathbf{w}_i \longmapsto \mathbf{x}_i = \phi(\mathbf{w}_i)$. The Coarse lattice represents the shaping lattice which ensures that the power constraint P is met and the Fine lattice defines the coding lattice from which are selected the codewords. In practice, a nested lattice code can be constructed using linear codes or LDPC codes over finite fields. Consider a code C over $\mathbb{F}_p$ and let $\mathbf{G} \in \mathbb{F}_p^{k \times n}$ be its generator matrix. The coarse lattice can be just a scaled version of $\mathbb{Z}^n$ by the size of te field p, $\Lambda_{\text{C}} = p\mathbb{Z}^n$. As the coarse lattice defines the shaping region, the cost of this choice is the shaping gain. And the fine lattice is built by shifting the code C using Construction A as the following steps [9]:

1) Construct the discrete codebook, $\mathcal{C} = \left\{\mathbf{u}\mathbf{G}, \mathbf{u} \in \mathbb{F}_p^k\right\}$ from the code C
2) Construct the lattice Λ^* as: project the codebook into reals using the embedding function $g(.)$, divide by p and copy over $\mathbb{Z}^n$: $\Lambda^* = p^{-1} g(\mathcal{C}) + \mathbb{Z}^n$
3) Construct the Fine lattice by rotating Λ^* by the generator matrix of the coarse lattice $\mathbf{M}_{\text{C}}$, $\Lambda_{\text{F}} = \mathbf{M}_{\text{C}} \Lambda^*$

In the focus of this work, for performance evaluation and analysis, we consider the field $\mathbb{Z}/p\mathbb{Z}$ also noted $\mathbb{Z}_p$ to generate a low-complexity nested lattice code (it is a ring but for p prime it is a field). It 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. We consider the linear code C over $\mathbb{Z}_{11}^2$ $(k = 1, n = 2, p = 11)$ whose generator matrix is $\mathbf{G} = [2 \ 3]$. The codebook is then $\mathcal{C} = \left\{\mathbf{u}.[2 \ 3] \ \text{mod}(11), \mathbf{u} \in \mathbb{Z}_{11}^2\right\}$ and the Fine lattice is the set of points in $\Lambda_{\text{F}} = \mathcal{C} + 11\mathbb{Z}_{11}^2$. The coarse lattice is $\Lambda_{\text{C}} = 11\mathbb{Z}^2$. Codewords of the sources belong to the nested lattice code $\Lambda = \mathcal{V}_{\text{C}} \cap \Lambda_{\text{F}}$.

C. Decoding scheme

Attention is now drawn to the decoding part. According to the original framework of the CF [2], the aim of a relay node R_m observing a noisy real combination of transmitted codewords as modeled in Eq.(1), is to reliably decode, with the highest possible rate, a linear combination of the original messages in the form $\mathbf{u}_m = \bigoplus_{i=1}^{K} q_{mi} \mathbf{w}_i$ where coefficients $q_{mi} \in \mathbb{F}_p$. In practice, the relay is equipped with a separate decoder $\mathcal{D}_m$ that decodes an estimate $\hat{\mathbf{u}}_m$ of $\mathbf{u}_m$. Equations of all relays can be reliably decoded with average probability of error ϵ if: $\hat{\mathbf{u}}_m = \mathcal{D}_m(\mathbf{y}_m)$ and $\Pr\left(\cup_{m=1}^{K} (\hat{\mathbf{u}}_m \neq \mathbf{u}_m)\right) < \epsilon$. The decoding steps are the following:

i) Select a real parameter α_m and integer coefficients vector $\mathbf{a}_m = [a_{m1} \ ... \ a_{mK}] \in \mathbb{Z}^K$.
ii) Scale the received signal by α_m to approach the integer combination of lattice codewords with coefficients a_{mi}: $\tilde{\mathbf{y}}_m = \sum_{i=1}^{K} a_{mi} \mathbf{x}_{\text{i}} + \sum_{i=1}^{K} (\alpha_m h_{im} - a_{mi}) \mathbf{x}_{\text{i}} + \alpha_m \mathbf{z}_m$.
iii) Quantize to the Fine lattice: $\hat{\lambda}_{m,\text{F}} = Q_{\Lambda_{\text{F}}}(\tilde{\mathbf{y}}_m) = \sum_{i=1}^{K} a_{mi} \mathbf{x}_i$. In practice this is equivalent to search the closest lattice point in the Fine lattice and can be solved using Lattice Sphere Decoding. At this level, the decoded $\hat{\lambda}_{m,\text{F}}$ belongs to the Fine lattice since the coefficients $a_{mi} \in \mathbb{Z}$.
iv) Take the modulo operation with respect to the coarse lattice to guarantee that the resulting codeword belongs to the nested lattice code $\hat{\lambda}_m = \left[\sum_{i=1}^{K} a_{mi} \mathbf{x}_i\right] \text{mod}\Lambda_{\text{C}}$. With this operation, $\hat{\lambda}_m$ meets the power constraint P, as the original codewords, defined by the shaping region of the coarse lattice via the $\text{mod}\Lambda_{\text{C}}$ operation. For low complexity nested lattice coding scheme, where $\Lambda_{\text{C}} = p\mathbb{Z}^n$, this is equivalent to quantize to the nearest multiple of p over $\mathbb{Z}^n$.
v) Map $\hat{\lambda}_m$ back to the finite field. Since $\hat{\lambda}_m$ is a nested lattice codeword, this mapping gives the desired messages equation $\hat{\mathbf{u}}_m = \phi^{-1}(\hat{\lambda}_m) = \bigoplus_{i=1}^{K} q_{mi} \mathbf{w}_i$. The finite field coefficients q_{mi} are related to integer coefficients a_{mi} by $q_{mi} = g^{-1}\left([a_{mi}] \, \text{mod} p\right)$.

Notice that the decoding process includes two parts: decoding of a nested lattice codeword and mapping to finite field. Then a decoding error at the relay counts if the decoding of the lattice codeword is not correct, the mapping to finite field does not change the correctness of the decoding. The two fundamental parameters of the whole process are the scaling factor α_m and the coefficients vector $\mathbf{a}_m$. The relay is free to choose them, however the choice needs to be carefully made since it impacts greatly the performance. In literature, two basic criteria have been proposed to select optimal values of these parameters. Both of them are based on theoretical optimization problems at the relay's level. The first criterion proposed in [2] is based on the maximization of the computation rate assuming high-dimensional lattices given, for $\alpha_m \in \mathbb{R}, \mathbf{a}_m \in \mathbb{Z}^K$, by:

$$R_{\text{comp},m} = \frac{1}{2} \log^+ \left(\frac{\rho}{\alpha_m^2 + \rho \parallel \alpha_m \mathbf{h}_m - \mathbf{a}_m \parallel^2} \right) \quad (2)$$

The second criterion, proposed by Feng *et al.* in [4] is based on the minimization of the probability of decoding error assuming hypercube shaping lattices. According to these two optimization criteria, the optimal value of α_m corresponds to the Minimum Mean Square Error (MMSE) factor expressed as a function of $\mathbf{a}_m$ as: $\alpha_{opt,m} = \frac{\rho < \mathbf{h}_m^t , \mathbf{a}_m >}{1+\rho \|\mathbf{h}_m\|^2}$, and the optimal coefficients vector $\mathbf{a}_m$ corresponds to the shortest vector in the lattice $\Lambda_{\mathbf{G}_m}$ of Gram matrix $\mathbf{G}_m = \mathbf{I} - \frac{\rho}{1+\rho\|\mathbf{h}_m\|^2}\mathbf{H}_m$ where $\mathbf{H}_m = (H_{ij})_{i,j=1,...,K}, H_{ij} = \mathbf{h}_i \mathbf{h}_j^t$. This shortest vector problem can be solved in practice by the means of the Fincke-Pohst algorithm [8],[10].

Now, after reviewing the principle of the CF, we investigate the end-to-end constraints and performance of the CF-based schemes in the underlying MSRC.

V. Design 1: CCF

We present in this section a first CF-based scheme termed *Complete-CF* where the processing at intermediate relays follows exactly the original CF scheme. This scheme exploits both the linearity of the code and the linearity of the mapping from the real field to the finite field. Source nodes use the encoding scheme based on nested lattice codes and transmit their codewords during the first transmission's phase. The remaining communication processing steps at the relays and the destination are the following:

- *Relays*:
  - Receive $\mathbf{y}_m = \sum_{i=1}^K h_{im}\mathbf{x_i} + \mathbf{z}_m$.
  - Decode codewords $\hat{\lambda}_m = \left[\sum_{i=1}^K a_{mi}\mathbf{x}_i\right] \text{mod}\Lambda_\text{C}$ with the highest achievable rate as described in steps i)-iv) of the decoding process in section VI.C.
  - Forward both $\hat{\lambda}_m$ and the integer coefficients vector $\mathbf{a}_m = [a_{m1}...a_{mK}]$ to the destination.
- *Destination*:
  - Receives $\hat{\lambda}_1, ..., \hat{\lambda}_K$ and $\mathbf{a}_1, ..., \mathbf{a}_K$.
  - Maps codewords to finite field: $\hat{\mathbf{u}}_m = \phi^{-1}\left(\hat{\lambda}_m\right)$. Thanks to the linearity of the mapping ϕ from the nested lattice code to the finite field, $\hat{\mathbf{u}}_m = \bigoplus q_{mi}\mathbf{w}_i$ such that $q_{mi} = g^{-1}\left([a_{mi}] \,\text{mod} p\right)$.
  - Forms the linear system: $[\hat{\mathbf{u}}_1...\hat{\mathbf{u}}_K]^t = \mathbf{Q}\,[\mathbf{w}_1...\mathbf{w}_K]^t$ where $\mathbf{Q} = (q_{mi})_{m,i=1,...,K}$ represents the finite field coefficients matrix.
  - Inverts $\mathbf{Q}$ to solve for original messages: $\mathbf{Q}^{-1}[\hat{\mathbf{u}}_1...\hat{\mathbf{u}}_1]^t = [\hat{\mathbf{w}}_1...\hat{\mathbf{w}}_K]^t$ where $\mathbf{Q}^{-1}$ denotes the inverse of $\mathbf{Q}$ over $\mathbb{F}_p$.
- *Decodability condition*: *The destination can reliably recover original messages if and only if the finite field coefficients matrix* $\mathbf{Q}$ *is full rank over* $\mathbb{F}_p$.

This full rank condition for the CF in a large network design was first pointed out by Gastpar and Nazer in [2].

VI. Design 2: ICF

In this section we investigate a second CF-based scheme termed *Incomplete-CF*. In this scheme, encoding part of the protocol is kept at the sources. However the decoding part is incomplete: relay nodes compute and forward integer linear combinations of original codewords without mapping it to the nested lattice via the modulo operation. The resulting codeword coresponds therefore to a point from the Fine lattice. The missing step of mapping the integer combination to the nested lattice makes this scheme exploit only the linearity of the code and violate the power constraint. Its name ICF is due to this missing step. This decoding scheme, although does not match exactly the goal of the original framework of the CF, it has been considered in several works like [6], [11] and [7]. For instance, the DEFID coding-decoding scheme is proposed in [6] as a low complexity design for the CF. We detail in the following the processing at the relays as well as at the destination:

- *Relays*:
  - Receive $\mathbf{y}_m = \sum_{i=1}^K h_{im}\mathbf{x_i} + \mathbf{z}_m$.
  - Compute $\hat{\lambda}_{m,\text{F}} = \sum_{i=1}^K a_{mi}\mathbf{x}_i$ following steps i), ii) and iii) of the decoding process defined in section VI.C. - Forward both lattice equation $\hat{\lambda}_{m,\text{F}}$ and integer coefficients vector $\mathbf{a}_m$ to the destination.
- *Destination*:
  - Receives the K lattice equations and coefficients vectors.
  - Form the linear system: $\left[\hat{\lambda}_{1,\text{F}}...\hat{\lambda}_{K,\text{F}}\right]^t = \mathbf{A}\,[\mathbf{x}_1...\mathbf{x}_K]^t$ where $\mathbf{A}$ represents the integer coefficients matrix whose rows are the vectors $\mathbf{a}_m, m = 1, ..., K$.
  - Invert $\mathbf{A}$ over $\mathbb{Z}^n$ to solve for original codewords: $\mathbf{A}^{-1}\left[\hat{\lambda}_{1,\text{F}}...\hat{\lambda}_{K,\text{F}}\right]^t = [\hat{\mathbf{x}}_1...\hat{\mathbf{x}}_K]^t$.
  - Map estimated codewords back to the finite field to get estimates on the original messages: $\hat{\mathbf{w}}_i = \phi^{-1}(\hat{\mathbf{x}}_i)$.
- *Decodability condition*: *The destination can reliably recover original messages if and only if the integer network code coefficients matrix* $\mathbf{A}$ *is full rank over* $\mathbb{Z}^n$.

Since the selection of optimal coefficients vectors is performed independently at each relay node based on local optimization problems, there is no guarantee on the fulfillement of this decodability condition. This condition was pointed out in [6] for the DEFID scheme, however, no solution was proposed. A contribution of this work is to analyze the penalty of this constraint on the destination's performance and propose a reliable algorithm for selecting network code coefficients that satisfy a tradeoff between local and end-to-end-performance. The solution we propose is based on a cooperation between the relay nodes and consists in the following: since the optimal coefficients vector at each relay corresponds to the shortest vector of the lattice $\Lambda_{\mathbf{G}_m}$ defined previously, the idea is to select for each relay a set of potential candidates that correspond to the shortest vectors, meaning the highest achievable rates and lowest probability of decoding error at the relay, then select over all vectors delivered by all relay nodes those which allow to maximize the minimum achievable rate and that form a full rank set. The different steps of this method are summarized in the following:

i) Find for each relay node R_m the set $\mathcal{S}_{m,N}$ of the shortest vectors $\mathbf{u}_n,\ n = 1, ..., N$.
ii) Sort, for each relay node m the vectors $\mathbf{u}_n$ in a descending order corresponding to their achievable rates $\mathcal{R}_{\text{comp},m}^n$.
iii) Sort the overall set of achievable rates of all relay nodes in a descending order into the set $\{\mu_1, ..., \mu_{K\times N}\}$.

iv) Set $i = K$ and let $\mu_i = \mathcal{R}^n_{\text{comp},i}$ be the achievable rate at relay i corresponding to the vector $\mathbf{u}_n$. Find for all relays, $j \neq i$ the achievable rates higher than μ_i and find the combination of the corresponding vectors $\{\mathbf{u}_i, \mathbf{u}_j, j = 1, ..., K, j \neq i\}$ that are linearly independent. If the search does not result in a full rank set, set $i = i+1$ and go to step iii).

In our implementation we use the Fincke-Pohst algorithm for step i).

VII. CCF VS ICF

Given the above schemes and decodability conditions, it is worth answering to the following questions:

1) For the CCF: is having K linearly independent coefficient vectors (or integer coefficients matrix $\mathbf{A}$ full rank over the integer field) sufficient to allow recovery of original messages?
2) If the answer is no: how to guarantee that $\mathbf{Q}$ be full rank over the finite field?
3) What would be the difference between the CCF and the ICF schemes?

The answers are as follows:

1) No, having full rank of $\mathbf{A}$ is not enough to recover original messages: in fact, the recovery of original messages is obtained through the inversion of $\mathbf{Q}$ over $\mathbb{F}_p$. However, if $\mathbf{A}$ is full rank, it does not necessarily come with a full rank matrix $\mathbf{Q}$. A simple example is the following: consider the case of $K = 2$ and $\mathbb{F}_p = \mathbb{Z}_{11}$ with integer addition and multiplication modulo 11. Take the case of $\mathbf{A} = \begin{bmatrix} -1 & -3 \\ 3 & -2 \end{bmatrix}$ which is full rank (its determinant $d_{\mathbf{A}} = 11 \neq 0$). By mapping this matrix to $\mathbb{Z}_{11}$ we get $\mathbf{Q} = \begin{bmatrix} 10 & 8 \\ 3 & 9 \end{bmatrix}$. As one can easily observe, $\mathbf{Q}$ is not full rank over $\mathbb{Z}_{11}$ (its determinant equals to $d_{\mathbf{Q}} = 66 = [0] \operatorname{mod}(11)$).
2) Having in mind that the coefficients of the two matrices are related by $q_{ij} = g^{-1}\left([a_{ij}] \operatorname{mod} p\right)$, it is easy to see that the determinant of the matrix $\mathbf{Q}$ over $\mathbb{F}_p$ is equal to $d_{\mathbf{Q}} = g^{-1}\left([d_{\mathbf{A}}] \operatorname{mod} p\right)$. Therefore, to guarantee full rank of finite field coefficients matrix we need not only to have $d_{\mathbf{A}} \neq 0$ but also $[d_{\mathbf{A}}] \operatorname{mod} p \neq 0$. The reliable decodability condition is then to have either $\mathbf{Q}$ full rank over $\mathbb{F}_p$ or in terms of $\mathbf{A}$ to have a determinant different from a multiple of the size field p. One can see from the previous example, the full rank failure of $\mathbf{Q}$ arises from the fact of having $d_{\mathbf{A}} = 11$ a multiple of the field size $p = 11$. This observation was cited in Remark 9 in [2]. The question now is how to guarantee, from the selection of the integer matrix $\mathbf{A}$, to have $\mathbf{Q}$ full rank? In this regard, it is only showed in Theorem 11 of [2] that under some assumptions on the magnitude of the integer coefficients a_{ij} and for sufficiently large field size p and blocklength n, there exists a class of nested lattice codes for which $d_{\mathbf{A}} \neq 0 \Rightarrow [d_{\mathbf{A}}] \operatorname{mod} p \neq 0$. However, it is not completely understood how to solve this full rank constraint in practical settings, for moderate values of p and n and with no assumptions on the coefficients of the matrix $\mathbf{A}$. Main contributions of this work are to evaluate the impact of this condition on the destination's performance in terms of rate and error rate and to propose a search algorithm that guarantees successful message recovery at the destination. The method searches over network coefficients vectors that allow to achieve higher transmission rates taking into account the condition that $[d_{\mathbf{A}}] \operatorname{mod} p \neq 0$. It is also based on a cooperation between the relay nodes and consists on a slight modification of the algorithm proposed for the ICF as follows:
   i) Find for each relay node R_m the set $\mathcal{S}_{m,N}$ of the shortest vectors $\mathbf{u}_n$, $n = 1, ..., N$.
   ii) Sort, for each relay node m the vectors $\mathbf{u}_n$ in a descending order corresponding to their achievable rates $\mathcal{R}^n_{\text{comp},m}$.
   iii) Sort the overall set of achievable rates of all relay nodes in a descending order into the set $\{\mu_1, ..., \mu_{K\times N}\}$.
   iv) Set $i = K$ and let $\mu_i = \mathcal{R}^n_{\text{comp},i}$ be the achievable rate at relay i corresponding to the vector $\mathbf{u}_n$. Find for all relays, $j \neq i$ the achievable rates higher than μ_i.
   v) Form the matrix $\mathbf{U} = \left[\mathbf{u}_i \; \mathbf{u}_{j_{(j=1,..K)}}\right]$ of row vectors $\mathbf{u}_i$ and $\mathbf{u}_j, j = 1, ..., K$ found in the previous step, then find the combination of the corresponding vectors $\{\mathbf{u}_i, \mathbf{u}_j, j = 1, ..., K, j \neq i\}$ guaranteeing $[det(\mathbf{U})] \operatorname{mod} p \neq 0$. If the search condition is not satisfied, set $i = i + 1$ and go to step iii).
3) The differences between the two schemes are the following: first, the CCF takes the power constraint at the relay into account however the ICF does not. Second, the CCF exploits both the linearity of the code and the linearity of the mapping from the nested lattice code to the finite field, meanwhile, the second scheme harnesses only the linearity of the code. In addition, for the CCF, the destination first maps the lattice equations to the finite field then inverts the coefficients matrix over $\mathbb{F}_p$, meanwhile, under the ICF perspective, the destination inverts first the coefficients matrix over the integer field to estimate original codewords, afterwards maps each one of them individually to the finite field to recover source's messages. However, as we stressed earlier, the mapping to the finite field does not impact the correctness of the decoding objective. Therefore, we expect an equivalence of the end-to-end performance of two schemes when the decodability conditions are satisfied.

VIII. NUMERICAL RESULTS

We address in this section performance evaluation, analysis and comparison of the two studied transmission schemes at the destination node. We consider the case of $K = 2$. Monte-Carlo simulations have been carried out to evaluate the message error rate and the average achievable rate per user. The former is expressed as $\mathrm{P_e} = \Pr\left(\cup_{m=1}^{K}\left(\hat{\mathbf{w}}_m \neq \mathbf{w}_m\right)\right)$, and the latter is given by $R = \min_{m=1,\ldots,K}\{R_{\text{comp},m}\}$. Numerical results are related to the practical encoding scheme proposed in section III.B.

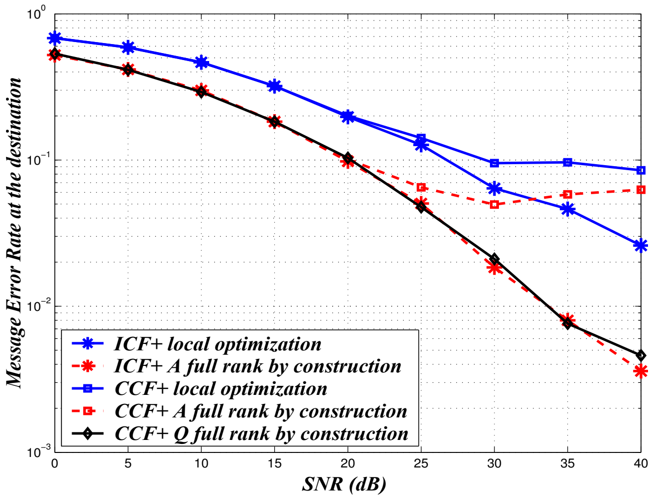

Fig. 2. Message Error rate at the destination node as a function of the SNR.

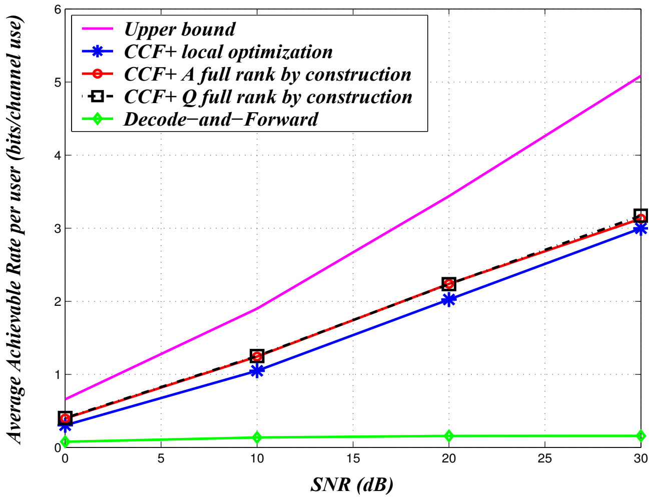

Fig. 3. Achievable Rates at the destination node as a function of the SNR.

Starting with the message error rate, in the light of Fig.2, we report for the ICF the suboptimality of the choice of $\mathbf{A}$ following the local optimization criteria as far as the end-to-end performance at the destination is concerned. Taking the decodability constraint into account while constructing the integer matrix as our proposed algorithm brings a gain of more than $10-$dB at high SNR ranges. Now, as far as the CCF is concerned, numerical results confirm that having $\mathbf{A}$ full rank over $\mathbb{Z}^n$ brings a performance gain but is not enough to achieve reliable decoding at the destination particularly at high SNR values. Our proposed algorithm that takes into consideration that $\mathbf{Q}$ be full rank improves greatly the end-to-end performance. Moreover, we report from the same figure that the two schemes achieve almost same end-to-end message error rate performance when the full rank constraints are solved. This result confirms our expectation in the previous section, that is the two schemes are equivalent if the corresponding decodability conditions are fulfilled. The only difference is that the ICF violates the power constraint at the relays' level. This scheme can therefore be used as a tool to validate theoretical results, but not as a real transmission scheme. Now moving to the average achievable rate performance. We restrict the evaluation to the CCF scheme since the impact of the full rank constraints on the two schemes is the same in terms of rate. As illustrated in Fig.3, penalty of the full rank constraint on the coefficients matrix $\mathbf{A}$ is considerable. We point out that satisfying full rank condition on $\mathbf{A}$ or $\mathbf{Q}$ brings the same gain of 2.5dB over the non full rank case in contrast to the error rate performance. This can be explained by the analytical rate expression evaluated over the real field. Moreover, we notice that although the CCF presents a noteworthy gap to the channel's capacity, it outperforms the Decode-and-Forward strategy. The former offers a significant gain over the latter that exceeds $1\text{bit per channel use}$ at moderate SNR values.

IX. Conclusion

Practical end-to-end communication over a MSRC using the CF as a PLNC strategy is considered. We explored and solved practical constraints that deserve a particular attention when dealing with the CF as a processing stage in a large network design. Numerical results evaluating the end-to-end performance at the destination in terms of achievable rate and error rate are a proof of the relevance of the addressed practical issues related to the CF as well as of the reliability of the proposed algorithms.

Acknowledgments

The authors would like to acknowledge the European Commission for funding SmartEN ITN (Grant No. 238726) under the Marie Curie ITN FP7 program.

References

[1] S Zhang. Hot topic: physical-layer network coding. In *in Proc. of ACM Mobicom*, pages 358–365, 2006.

[2] B. Nazer and M. Gastpar. Compute-and-forward: Harnessing interference with structured codes. In *ISIT*, pages 772 –776, july 2008.

[3] N.E. Tunali and K.R. Narayanan. Concatenated signal codes with applications to compute and forward. In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pages 1 –5, dec. 2011.

[4] C. Feng, D. Silva, and F.R. Kschischang. An algebraic approach to physical-layer network coding. In *ISIT*, pages 1017 –1021, june 2010.

[5] L. Wei and W. Chen. Compute-and-forward network coding design over multi-source multi-relay channels. *Wireless Communications, IEEE Transactions on*, 11(9):3348 –3357, september 2012.

[6] Or Ordentlich, Jiening Zhan, Uri Erez, Michael Gastpar, and Bobak Nazer. Practical code design for compute-and-forward. In *ISIT*, pages 1876–1880, 2011.

[7] J.-C. Belfiore. Lattice codes for the compute-and-forward protocol: The flatness factor. In *ITW*, pages 1 –4, oct. 2011.

[8] H. Cohen. *A course in computational algebraic number theory*. Springer-Verlag New York, Inc., New York, NY, USA, 1993.

[9] U. Erez, S. Litsyn, and R. Zamir. Lattices which are good for (almost) everything. In *ITW*, pages 271 – 274, march-4 april 2003.

[10] U. Fincke and M. Pohst. Improved Methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis. *Mathematics of Computation*, 44(170):463–471, 1985.

[11] Lili Wei and Wen Chen. Efficient compute-and-forward network codes search for two-way relay channel. *Communications Letters, IEEE*, 16(8):1204 –1207, august 2012.