The Flatness Factor in Lattice Network Coding:
Design Criterion and Decoding Algorithm

Jean-Claude Belfiore
Department of Communications and Electronics
Telecom ParisTech, LTCI UMR 5141
46, rue Barrault, 75013 Paris, France
Email: belfiore@enst.fr

Cong Ling
Department of Electrical and Electronic Engineering
Imperial College London
London SW7 2AZ, United Kingdom
Email: cling@ieee.org

Abstract—In a recent work, Nazer and Gastpar proposed the compute-and-forward strategy as a physical-layer network coding scheme. They described a code structure based on nested lattices whose algebraic structure makes the scheme reliable and efficient. In a more recent paper, Niesen and Whiting revealed a fundamental limitation of the decoder used by Nazer and Gastpar. In this work, we consider maximum-likelihood decoding of compute-and-forward, aiming to overcome its limitation. By examining the decoding metric from the viewpoint of Gaussian measures over lattices, we present a design criterion of the lattice code based on the flatness factor, and propose a new decoding algorithm based on inhomogeneous Diophantine approximation.

I. INTRODUCTION

In [1], Zhang et al. introduced the physical-layer network coding concept (PNC) in order to turn the broadcast property of the wireless channel into a capacity boosting advantage. Instead of considering the interference as a nuisance, each relay converts an interfering signal into a combination of simultaneously transmitted codewords. PNC concept has received a particular interest in the last years because it provides means of embracing interference and improving network capacity.

In a recent work [2], Nazer and Gastpar proposed a new physical-layer network coding scheme. The proposed strategy, called compute-and-forward (CF), exploits interference to obtain higher end-to-end transmission rates between users in a network. The relays are required to decode noiseless linear equations of the transmitted messages using the noisy linear combination provided by the channel. The destination, given enough linear combinations, can solve the linear system for its desired messages. This strategy is based on the use of structured codes, particularly nested lattice codes to ensure that integer combinations of codewords are themselves codewords. The authors demonstrated its asymptotic gain using information-theoretic tools. Standard minimum Euclidean distance decoding was assumed.

The authors in [3] followed and generalized the framework of Nazer and Gastpar by introducing the Lattice Network Coding (LNC). They related the Nazer-Gastpar’s approach to the theorem of finitely generated modules over a principle ideal domain (PID). They gave sufficient conditions for lattice partitions to have a vector space structure which is a desirable property to make them well suited for PNC. Then, they generalized the lattice code construction and developed encoding and decoding methods. Standard minimum Euclidean distance decoding was still assumed.

In a more recent work [4], Niesen and Whiting revealed a fundamental limitation of standard minimum Euclidean distance decoding, namely, it achieves no more than 2 degrees of freedom. This is due to the quantization of channel coefficients, which leads to a tradeoff between channel coefficient approximation and noise amplification. This tradeoff was associated with a problem of Diophantine approximation in [4]. They further proposed a scheme achieving higher degrees of freedom based on real interference alignment. However, this scheme is not robust, among many of its shortcomings.

In [5], the first author essentially proposed an analysis of the compute-and-forward strategy when maximum-likelihood (ML) decoding is used. It should be emphasized that ML decoding does not subscribe to the limitation shown in [4]. A new quantity, the Flatness Factor, was introduced, which measures the quality of ML decoding. After changing the definition of the flatness factor in order to be consistent with [8], [9], this paper studies more deeply the properties of it and gives some new insights into lattice network coding.

II. COMPUTE AND FORWARD

In our model, we consider one relay receiving messages from $k$ sources $S_1,\ldots,S_k$ and transmitting a linear combination of these $k$ messages. The relay observes a noisy linear combination of the transmitted signals through the channel. Received signal at the relay is expressed as,

$$y = \sum_{j=1}^{k} h_j x_j + w$$

(1)

where $h_j$ is the channel coefficient between source $S_j$ and the relay and $x_j$ is the vector transmitted by source $S_j$.

The relay searches to transmit a noiseless linear combination of the received signals with integer coefficients given by vector $a = [a_1 \ a_2 \ \cdots \ a_k]^T$. To achieve that goal, it decodes a noiseless linear combination of the transmitted vectors,

$$x_R = \sum_{j=1}^{k} a_j x_j$$

(2)
and retransmits it to the destination or another relay. We consider a complex-valued channel model with complex inputs and outputs. The channel coefficients $h_i$ are complex, circular, i.i.d. Gaussian, $h_i \sim \mathcal{N}(0, 1)$. $z$ is Gaussian, zero mean, with variance $\sigma^2 (z \sim \mathcal{N}(0, \sigma))$. Let $h = [h_1 \ h_2 \ \cdots \ h_k]^T$ denote the vector of channel coefficients. Source vectors $x_j$ are carved from a lattice code. The sources have no channel side information (CSI). CSI is only available at the relay.

III. THE ML DECODER

A. Solving the System of Diophantine Equations

The relay aims to decode a linear system of equations of the transmitted messages and passes it towards the destination. After calculating the vector $a$ chosen following some given criterion, the relay recovers a linear combination of the transmitted signals. We rewrite the received (scaled) signal at the relay in the following form,

$$y = \lambda + \sum_{j=1}^{k} \xi_j x_j + w$$

where $\lambda$ is a point of a lattice $\Lambda$, $\xi_j = \frac{h_j}{a_j}$ and $w$ is the additive i.i.d. Gaussian noise. The recovered linear system of equations $\lambda = \sum_{j=1}^{k} a_j x_j$ is a linear system of Diophantine equations. This system admits the following solutions.

Suppose that the transmitted vectors $x_j \in \Lambda_j$ where $\Lambda_j$ are full rank lattices. Then, since

$$\lambda = \sum_{j=1}^{k} a_j x_j,$$

the lattice in which $\lambda$ lives is

$$\Lambda = a_1 \Lambda_1 + a_2 \Lambda_2 + \cdots + a_k \Lambda_k.$$

Our aim, here, is to express the messages $x_j$ as a function of $\lambda$, for a given $\lambda \in \Lambda$. But the system of Diophantine equations admits an infinite number of solutions. The Hermite Normal Form (HNF) allows to solve this system [7]. We show here how to proceed.

From Equation (4), we get

$$\lambda = \sum_{j=1}^{k} \frac{a_j}{\lambda} \frac{M_j z_j}{x_j},$$

where matrices $V_j$ are square $n \times n$ matrices. Then the solution to the system of Diophantine equations is,

$$x_j = s_j + v_j$$

where $v_j = M_j V_j B^{-1} \lambda$ and $s_j$ is any vector in the lattice $L_j \subset \Lambda_j$ of generator matrix $M_j U_j$.

B. ML Decoding Metric

The ML decoder maximizes $p(y/\lambda)$ over all possible values of $\lambda$. The conditional probability $p(y/\lambda)$ can be expressed as,

$$p(y/\lambda) = \sum_{\sum_{j=1}^{k} \frac{a_j}{\lambda} \frac{M_j z_j}{x_j}} p(x_1, \ldots, x_k)$$

where

$$p(y/x_1, \ldots, x_k) \propto e^{-\frac{\|y-(\sum_{j=1}^{k} a_j h_j x_j)\|^2}{2\sigma^2}}$$

and $x_1, \ldots, x_k$ are (a priori) supposed equiprobable and given by (6). The decoding rule is now to find,

$$\hat{\lambda} = \arg \max_{\lambda \in \Lambda} \varrho(\lambda),$$

with

$$\varrho(\lambda) = \sum_{q \in \mathcal{L}} e^{-\frac{\|w-\sum_{j=1}^{k} h_j x_j\|^2}{2\sigma^2}}.$$
flatness factor in terms of the theta series (the proof is given in [9]).

**Proposition 2.** [Expression of $\epsilon_L(\sigma)$]

$$\epsilon_L(\sigma) = \mu^n \Theta_L \left( \frac{1}{2\pi \sigma^2} \right) - 1 \quad (11)$$

where $\mu = \frac{V(L)\pi^2}{2\pi \sigma^2}$ is the generalized signal-to-noise ratio, and $\Theta_L(z) = \sum_{\lambda \in \mathbb{L}} e^{-\pi z \|\lambda\|^2}$ is the theta series of $L$.

The flatness factor is closely related to the smoothing parameter studied in [8]. The advantage of the flatness factor is two-fold:

- It gives a precise characterization $\epsilon_L(\sigma)$ by the theta series, so it is more precise than the bounds available in [8].
- The smoothing parameter is mostly concerned with small values of $\epsilon_L(\sigma)$, while the flatness factor can handle both small and large values. The latter is of interest in coding applications.

**B. Design Criterion**

We need that the flatness factor of $L$ be as large as possible to ensure that the maximum likelihood metric will be as different as possible from the likelihood metrics of the other points of the lattice $L$. Formally, we have the following design criterion of the lattice $L$:

**Proposition 3.** [Goodness for network coding] In order to have good decoding performance in compute-and-forward, the theta series $\Theta_L(z)$ should be large.

This requires from the lattice $L$ to be as ‘bad’ as possible in the standard sense of coding (i.e., not dense at all). The generator matrix of $L$ is $\sum_{i=1}^{k} a_i M_i U_j$. But, since $\sum_{j=1}^{k} a_i M_i U_j = 0$, from the HNF, we deduce that we have to align vector $a$ with vector $h$ as much as possible.

As an illustration, Figure 2 shows the values of some flatness factors as a function of the generalized signal to noise ratio $\mu$. For our purpose, the Leech lattice is worse than the $Z^2$ lattice.

**V. DECODING ALGORITHM**

We are now interested in an algorithm which must maximize $\vartheta(\lambda)$ in an efficient way. To do this, we need the Fourier transform and Jacobi theta functions. In fact, we will not attempt to compute $\vartheta(\lambda)$ itself; instead, we will propose inhomogeneous Diophantine approximation as a solution to ML decoding.

**A. Fourier transform and Jacobi theta function**

Since $f_{\sigma,L}(y)$ is obviously periodic on $L$, its Fourier transform is defined on the dual lattice $L^*$. The Fourier coefficients are given by

$$f_{\sigma,L}(q^*) = \frac{1}{V(L)} e^{-2\pi \sigma^2 |q|^2}$$

where $q^* \in L^*$. (12)

The Fourier expansion of $f_{\sigma,L}(y)$ is then

$$f_{\sigma,L}(y) = \frac{1}{V(L)} \sum_{q^* \in L^*} e^{-2\pi \sigma^2 |q|^2} e^{2\pi i \langle q^*, y \rangle}. \quad (13)$$

Now we express the Gaussian measure as the Jacobi theta function (sometime referred to as the Riemann theta function in the multi-dimensional case), via the Fourier transform (13). Let $\mathbb{H}_n$ be set of symmetric square matrices whose imaginary part is positive definite. For an $n \times n$ matrix $T \in \mathbb{H}_n$ and an $n$-dimensional complex vector $z$, the multi-dimensional theta function is defined as

$$\theta(z; T) = \sum_{q \in \mathbb{Z}^n} e^{\pi i q^T T q + 2\pi i q^T z}. \quad (14)$$

Comparing with (13), we recognize that

$$f_{\sigma,L}(y) = \frac{1}{V(L)} \theta(z; T) \quad (15)$$
for $z = C^{-1}y$ and $T = 2\pi i\sigma^2(CTC)^{-1}$. Known results of the Jacobi theta function may be applied to analyze the Gaussian measure over lattices.

**B. The 1-D Real Case**

Here,

$$\varrho(\lambda) = \sum_{k \in \mathbb{Z}} e^{-\frac{(\lambda - \alpha - \beta k)^2}{2\pi^2}}$$

for some given values of $\alpha$ and $\beta$. So, we have to study the function $f_{\sigma, z}(y)$ since, obviously, we have

$$\varrho(\lambda) \propto f_{\sigma, z}(y - \alpha \lambda).$$

We will show now that ML decoding is equivalent to Diophantine approximation

$$\arg\max_{\lambda \in \Lambda} \varrho(\lambda) = \arg\min_{\lambda, k \in \mathbb{Z}} |y - \alpha \lambda - \beta k|.$$  \hspace{1cm} (16)

To do this, we specialize (15) to the 1-D case:

$$f_{\sigma, z}(y) = \frac{1}{\sqrt{2\pi\sigma}} \sum_{k \in \mathbb{Z}} e^{-\frac{(y - \alpha - \beta k)^2}{2\pi^2}} = \sum_{k \in \mathbb{Z}} e^{-2\sigma^2 \sigma^2 k^2 + 2\pi i k y}.$$ \hspace{1cm} (17)

In the 1-D case, the Jacobi theta function is a function defined for two complex variables $z$ and $\tau$:

$$\theta(z; \tau) = \sum_{k = -\infty}^{\infty} e^{\pi i k^2 + 2\pi i k z} = 1 + 2 \sum_{k=0}^{\infty} e^{\pi i k r} \cos(2\pi k z)$$ \hspace{1cm} (18)

where $z$ can be any complex number and $\tau$ is confined to the upper half-plane. Comparing (17) and (18), we recognize that

$$f_{\sigma, z}(y) = \theta(z; \tau), \quad \text{for} \quad z = y, \ \tau = 2\pi i\sigma^2.$$ \hspace{1cm} (19)

By using the Jacobi theta function, we have,

**Proposition 4.** $f_{\sigma, z}(y)$ is monotonically decreasing for $y \in (0, 1/2)$.

**Proof:** Let $r = e^{\pi i r}$ and $z = y$. We fix $r$ so that $\theta(y; \tau) = \theta(y | r)$ is a function of $y$ for $r = e^{-2\pi i r^2}$. Using the triple product of the Jacobi theta function [10]

$$\theta(y; \tau) = \prod_{m=1}^{\infty} (1 - r^{2m})(1 + e^{2\pi y r^{2m-1}})(1 + e^{-2\pi y r^{2m-1}}),$$

we obtain an alternative expression of the Gaussian measure

$$f_{\sigma, z}(y) = \prod_{m=1}^{\infty} (1 - r^{2m})(1 + 2 \cos(2\pi y)r^{2m-1} + r^{4m-2}).$$ \hspace{1cm} (20)

Obviously, $f_{\sigma, z}(y)$ is periodic in $y$ with period 1, and its monotonicity is the same as that of $\cos(2\pi y)$.

**Corollary 5.** The Diophantine-approximation decoder (16), intuitively conjectured in [5], is in fact optimum in 1-D.

**Proof:** Follows directly from proposition 4. More precisely, $f_{\sigma, z}(y)$ is monotonically decreasing as $y$ gets away from an integer $a$, until it reaches the minimum $a \pm 0.5$.

**C. The Multidimensional Case**

The multidimensional case requires to be able to derive product formulas from Jacobi theta series and show that the function $f_{\sigma, L}(y)$ has a regular behavior (decreases when the distance between $y$ and a lattice point increases) inside a Voronoi cell, or inside a certain region centered at a lattice point. If it is true (and we conjecture it is), then we have

**Conjecture 6.** Maximizing the ML metric is equivalent or close to solving a multidimensional inhomogeneous Diophantine approximation problem. More precisely,

$$\arg\max_{\lambda \in \Lambda} \varrho(\lambda) \simeq \arg\min_{\lambda, q \in \mathcal{E}} \|u(\lambda) - q\|^2.$$ \hspace{1cm} (22)

Even if we are unable to prove the conjecture for now, there are evidences supporting a decoder like (22). Since $f_{\sigma, L}(y)$ is the Fourier transform of a positive measure, we have

**Proposition 7.** $f_{\sigma, L}(y)$ is a positive-definite function. In particular, $f_{\sigma, L}(y) \leq f_{\sigma, L}(0)$.

Moreover, it is easy to see

**Proposition 8.** The first derivative $f'_{\sigma, L}(y) = 0$, while the second derivative $f''_{\sigma, L}(y) < 0$, when $y \in \mathcal{E}$.

Therefore, $f_{\sigma, L}(y)$ is bell-shaped in the vicinity of a lattice point, which is a local (and also global) maximum. The Diophantine-approximation decoder is a good approximation with respect to this monotonic decoding metric (at least locally).

We close this investigation with a remark on the different roles played by Diophantine approximation in this paper and in [2]. Diophantine approximation was a detrimental effect in [2], while it plays a constructive role in this paper. We expect it will achieve a better performance in compute-and-forward.

**References**


