# An Algebraic Approach to Physical-Layer Network Coding

Chen Feng, Danilo Silva, *Member, IEEE*, and Frank R. Kschischang, *Fellow, IEEE*



**Abstract**

The problem of designing physical-layer network coding (PNC) schemes via nested lattices is considered. Building on the compute-and-forward (C&F) relaying strategy of Nazer and Gastpar, who demonstrated its asymptotic gain using information-theoretic tools, an algebraic approach is taken to show its potential in practical, non-asymptotic, settings. A general framework is developed for studying nested-lattice-based PNC schemes—called lattice network coding (LNC) schemes for short—by making a direct connection between C&F and module theory. In particular, a generic LNC scheme is presented that makes no assumptions on the underlying nested lattice code. C&F is re-interpreted in this framework, and several generalized constructions of LNC schemes are given. The generic LNC scheme naturally leads to a linear network coding channel over modules, based on which non-coherent network coding can be achieved. Next, performance/complexity tradeoffs of LNC schemes are studied, with a particular focus on hypercube-shaped LNC schemes. The error probability of this class of LNC schemes is largely determined by the minimum inter-coset distances of the underlying nested lattice code. Several illustrative hypercube-shaped LNC schemes are designed based on Construction A and D, showing that nominal coding gains of $3$ to $7.5$ dB can be obtained with reasonable decoding complexity. Finally, the possibility of decoding multiple linear combinations is considered and related to the shortest independent vectors problem. A notion of dominant solutions is developed together with a suitable lattice-reduction-based algorithm.

**Index Terms**

Lattice network coding, nested lattice code, finite generated modules over principal ideal domains, Smith normal form.

Manuscript received July 21, 2011; revised Sep. 17, 2012 and July 3, 2013. The work of D. Silva was supported in part by the São Paulo Research Foundation (FAPESP-Brasil) and in part by the Brazilian National Research Council (CNPq) under Grant 482131/2010-1. This paper was presented in part at the IEEE International Symposium on Information Theory, Austin, TX, June 2010, and in part at the Annual Conference on Information Sciences and Systems, Baltimore, MD, March 2011.

C. Feng and F. R. Kschischang are with the Department of Electrical and Computer Engineering, University of Toronto, Canada (email: `cfeng@eecg.utoronto.ca`; `frank@comm.utoronto.ca`).

D. Silva is with the Department of Electrical Engineering, Federal University of Santa Catarina, Brazil (email: `danilo@eel.ufsc.br`).

## I. Introduction

Nested-lattice-based physical-layer network coding (LNC) is a type of compute-and-forward (C&F) relaying strategy [1] that is emerging as a compelling information transmission scheme in Gaussian relay networks. LNC exploits the property that integer linear combinations of lattice points are again lattice points. Based on this property, relays in LNC attempt to decode their received signals into integer linear combinations of codewords, which they then forward. This approach induces an end-to-end network coding channel from which the transmitted information can be recovered by solving a linear system.

In this paper, we develop a generic LNC scheme that makes no particular assumption on the structure of the underlying nested lattice code, thereby enabling a variety of code-design techniques. A key aspect of this approach is a so-called "linear labeling" of the points in a nested lattice code that gives rise to a beneficial compatibility between the $\mathbb{C}$-linear arithmetic operations performed by the wireless channel and the linear operations in the message space that are required for linear network coding. Similar to vector-space-based noncoherent network coding (e.g., [2]), the linear labelings of this paper induce a noncoherent end-to-end network coding channel with a message space having, in general, a module-theoretic algebraic structure, thereby providing a foundation for achieving noncoherent network coding over general Gaussian relay networks.

We study the error performance of a class of hypercube-shaped LNC schemes, and show that the error performance is largely determined by the minimum inter-coset distance of the underlying nested lattice code. By way of illustration, we adapt several known lattice constructions to give three exemplar LNC schemes that provide nominal coding gains of 3 to 7.5 dB while admitting reasonable decoding complexity.

We also study the possibility that a relay may attempt to decode more than one linearly independent combination of messages, and we relate this problem to the "shortest independent vectors problem" in lattices [3]. For this problem, a notion of dominant solutions is introduced together with a lattice-reduction-based algorithm, which may be of independent interest.

LNC can be seen as generalization of several previous physical layer network coding (PNC) schemes [4]–[6]. The earliest PNC schemes were applied to a two-way relay channel in which the relay attempts to decode the modulo-two sum (XOR) of the transmitted messages. It was observed in [7], [8] that the XOR can be replaced by a family of functions satisfying the so-called "exclusive law of network coding." Furthermore, the choice of function can potentially be adapted to the instantaneous channel realizations, although a complicated computer search may be needed [8] to choose the function optimally, even in the case of low-dimensional constellations such as 16-QAM. Because LNC considers only linear combinations, not general functions, it provides an efficient method, even in high-dimensional spaces, to perform such channel-adaptive decoding. Further PNC schemes presented in [9]–[12] aim to approach the capacities of various two-way relay channels. A survey of PNC for two-way relay channels can be found in [13].

The use of nested lattice codes (or Voronoi constellations) in PNC was first proposed in [6], [9], leading to the development of C&F relaying. A key feature of the C&F strategy is that no channel state information (CSI) is

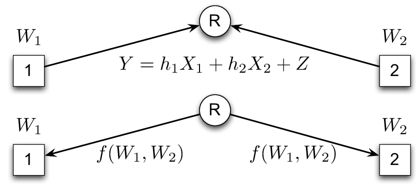



Fig. 1. Illustration of a two-round physical-layer network coding scheme.

required at the transmitters. In contrast to alternative advanced strategies such as noisy network coding [14] and quantize-map-and-forward strategy [15], [16], the C&F strategy does not require global channel-gain information at the destinations. All of these make C&F an appealing candidate for practical implementation.

The C&F strategy can be enhanced by assuming CSI at the transmitters [17] or by installing multiple antennas at the relays and destinations [18], [19]. Practical code constructions for C&F are presented (see, e.g., [20]–[23]). A recent survey of C&F can be found in [24].

After the conference publication of an earlier version of this work [25] (see also [26], [27]), several papers have appeared following our algebraic framework. For example, the work of [28] presents several design examples based on Eisenstein lattices, which can achieve a shaping gain of 0.167 dB compared to our examples based on Gaussian lattices. The work of [29] studies the existence of asymptotically-good nested lattices over Eisenstein integers, which can offer higher computation rates for certain channel realizations compared to the computation rates in [1] (which are based on Gaussian integers).

The remainder of this paper is organized as follows. Section II presents motivating examples to illustrate the role of algebra in PNC. Section III reviews some well-known mathematical preliminaries that will be useful in setting up our algebraic framework. Section IV presents a problem formulation of linear PNC and summarizes some of Nazer-Gastpar's main results in the context of our formulation. Section V studies the algebraic properties of LNC, presenting a generic LNC scheme that induces an end-to-end linear network coding channel over modules. Section VI turns to the geometric properties of LNC, presenting a union bound estimate as well as some design criteria. Section VII contains several illustrative design examples for practical LNC schemes, showing that a decent nominal coding gain is quite possible under practical constraints. Section VIII studies the problem of choosing multiple coefficient vectors, which is closely related to some known lattice problems. Section IX presents simulation results, while Section X concludes this paper.

## II. Motivating Examples

In this section, we illustrate the role of algebra in PNC with a particular focus on two-way relay channels, where two terminals attempt to exchange their messages $W_1, W_2$ through a central relay, as shown in Fig. 1. For this channel model, a PNC scheme consists of two rounds of communication. In the first round, the terminals simultaneously transmit their signals $X_1, X_2$ to the relay, and the relay tries to decode a function $f(W_1, W_2)$ of the messages from the received signal $Y$. In the second round, the relay broadcasts the decoded function $f(W_1, W_2)$

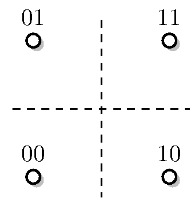



Fig. 2. Transmitted QPSK constellation.

to the terminals, based on which each terminal recovers the other message with its own message held as side information.

To illustrate how a PNC scheme works, we assume that the channels between terminals and the relay are complex-valued flat-fading channels with additive white Gaussian noise, that the messages $W_1, W_2$ take values in the set $\{00, 01, 10, 11\}$, and that (uncoded) Gray-labeled quaternary phase-shift-keying (QPSK) modulation is used, with the signal constellation given in Fig. 2. The channel gains between the terminals and the relay are denoted as $h_1$ and $h_2$. Furthermore, we assume that the relay aims to decode the XOR of the messages.

We first consider the ideal special case in which the channel gains are precisely unity, i.e., $h_1 = h_2 = 1$. The received constellation is depicted in Fig. 3(a), together with the decision region for XOR decoding. Although some received points are overlapping, say point $(W_1, W_2) = (01, 11)$ and point $(11, 01)$, the overlapping points have the same XOR value, resulting in no ambiguity.

Next, suppose that the channel gains are $h_1 = 1, h_2 = i$. In this scenario, unfortunately, overlapping points have different XOR values; see Fig. 3(b). For instance, point $(01, 10)$ has XOR value $01 \oplus 10 = 11$; whereas point $(11, 11)$ has XOR value $00$.

To solve this ambiguity, one natural attempt is to let the relay decode some linear function instead of the XOR. For example, if the relay interprets each message $W_\ell = [w_{\ell 1} \; w_{\ell 2}]$ ($\ell = 1, 2$) as an element in $\mathbb{F}_4$ by mapping it to $w_{\ell 1}\alpha + w_{\ell 2}$ (where $\alpha$ is a primitive element of $\mathbb{F}_4$) and tries to decode the function $f_1(W_1, W_2) = W_1 + \alpha W_2$, then both point $(01, 10)$ and point $(11, 11)$ give rise to the same value $10$. However, there are still some ambiguities that cannot be resolved by this function (the shaded dots in Fig. 3(b)).

In fact, no linear functions over $\mathbb{F}_4$ can resolve all the ambiguities in the received constellation, and the relay has to make use of the structure of a finite ring rather than that of a finite field. Specifically, let the relay interpret each message $W_\ell = [w_{\ell 1} \; w_{\ell 2}]$ as $w_{\ell 1} + w_{\ell 2} i \in \mathbb{Z}_2[i]$ with addition and multiplication defined as

$$a + bi + c + di = [a + c]_2 + [b + d]_2 i,$$

$$(a + bi)(c + di) = [ac - bd]_2 + [ad + bc]_2 i,$$

where $[\cdot]_2$ denotes the mod 2 operation. Then the function $f_2(W_1, W_2) = W_1 + iW_2$ is able to resolve all the ambiguities in Fig. 3(b). Moreover, the function $f_2$ works well even under other channel gains. In other words, the finite ring $\mathbb{Z}_2[i]$ seems to be a "good match" for QPSK constellation. This is not a coincidence. As we will see

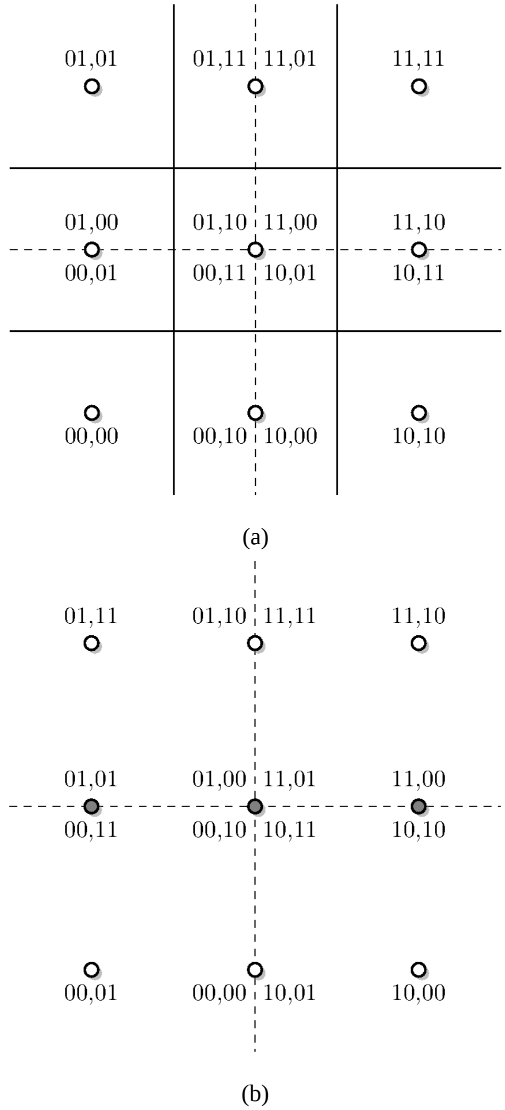



Fig. 3. Received constellations with QPSK when (a) $h_1 = h_2 = 1$, and (b) $h_1 = 1$, $h_2 = i$.

later, every nested-lattice-based constellation has such a good match.

## III. Algebraic Preliminaries

In this section we recall some essential facts about principal ideal domains, modules, and the Smith normal form, all of which will be useful for our study of the algebraic properties of complex nested lattices. All of this material is standard; see, e.g., [30]–[32]. We also introduce basic concepts and notation about lattices, mainly based on [33], [34].

### A. Rings and Ideals

We begin with some common definitions and notations for rings. All rings in this paper will be commutative with identity $1 \neq 0$. Let $R$ be a ring. We will let $R^*$ denote the nonzero elements of $R$, i.e., $R^* = R \setminus \{0\}$. An element $a$ is a *divisor* of an element $b$ in $R$, written $a \mid b$, if $b = ac$ for some element $c \in R$. An element $u \in R$ is called a *unit* of $R$ if $u \mid 1$. A non-unit element $p \in R$ is called a *prime* of $R$ if whenever $p \mid ab$ for some elements $a$ and $b$ in $R$, then either $p \mid a$ or $p \mid b$. An element $a$ of $R^*$ is a called a *zero-divisor* if $ab = 0$ for some $b \in R^*$. If $R$ contains no zero-divisors, then $R$ is an *integral domain*.

An *ideal* of $R$ is a nonempty subset $I$ of $R$ that is closed under addition and inside-outside multiplication, i.e., for all $a, b \in I$, $a + b \in I$ and for all $a \in I$ and all $r \in R$, $ar \in I$. If $A$ is any nonempty subset of $R$, let $\langle A \rangle$ be the smallest ideal of $R$ containing $A$, called the *ideal generated by* $A$. An ideal generated by a single element is called a *principal ideal*. A ring in which every ideal is principal is called a *principal ideal ring* (PIR).

Let $R$ be a ring and let $I$ be an ideal of $R$. Two elements $a$ and $b$ are said to be *congruent* modulo $I$ if $a - b \in I$. Congruence modulo $I$ is an equivalence relation whose equivalence classes are (additive) cosets $a + I$ of $I$ in $R$. The *quotient ring* of $R$ by $I$, denoted $R/I$, is the ring obtained by defining addition and multiplication operations on the cosets of $I$ in $R$ in the usual way, as

$$(a + I) + (b + I) = (a + b) + I \text{ and } (a + I) \times (b + I) = (ab) + I.$$

### B. Principal Ideal Domains

An integral domain in which every ideal is principal is called a *principal ideal domain* (PID). The integers $\mathbb{Z}$ form a PID. In the context of complex lattices, typical examples of a PID include the Gaussian integers $\mathbb{Z}[i]$ and the Eisenstein integers $\mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3}$. Formally, Gaussian integers are the set $\mathbb{Z}[i] \triangleq \{a + bi : a, b \in \mathbb{Z}\}$, and Eisenstein integers are the set $\mathbb{Z}[\omega] \triangleq \{a + b\omega : a, b \in \mathbb{Z}\}$.

The Gaussian integers $\mathbb{Z}[i]$ have four units ($\pm 1, \pm i$). A Gaussian integer is called a *Gaussian prime* if it is a prime in $\mathbb{Z}[i]$. A Gaussian integer $a + bi$ is a Gaussian prime if and only if it satisfies exactly one of the following:

1) $|a| = |b| = 1$;
2) one of $|a|, |b|$ is zero and the other is a prime number in $\mathbb{Z}$ of the form $4j + 3$ (with $j$ a nonnegative integer);
3) both of $|a|, |b|$ are nonzero and $a^2 + b^2$ is a prime number in $\mathbb{Z}$ of the form $4j + 1$.

Note that these properties are symmetric with respect to $|a|$ and $|b|$. Thus, if $a + bi$ is a Gaussian prime, so are $\{\pm a \pm bi\}$ and $\{\pm b \pm ai\}$.

The Eisenstein integers $\mathbb{Z}[\omega]$ have six units ($\pm 1, \pm\omega, \pm\omega^2$). An Eisenstein integer is called an *Eisenstein prime* if it is a prime in $\mathbb{Z}[\omega]$. An Eisenstein integer $a + b\omega$ is an Eisenstein prime if and only if it satisfies exactly one of the following:

1) $a + b\omega$ is a product of a unit in $\mathbb{Z}[\omega]$ and a prime number in $\mathbb{Z}$ of the form $3j + 2$;
2) $|a + b\omega|^2 = a^2 - ab + b^2$ is a prime number in $\mathbb{Z}$.

Let $T$ be a PID and let $\pi \in T$. Then it is known that the quotient $T/\langle \pi \rangle$ is a PIR [32].

## C. Modules

Modules are to rings as vector spaces are to fields. Formally, let $R$ be a commutative ring with identity $1 \neq 0$. An $R$-module is a set $M$ together with 1) a binary operation $+$ on $M$ under which $M$ is an abelian group, and 2) an action of $R$ on $M$ which satisfies the same axioms as those for vector spaces.

An $R$-submodule of $M$ is a subset of $M$ which itself forms an $R$-module. Let $N$ be a submodule of $M$. The quotient group $M/N$ can be made into an $R$-module by defining an action of $R$ satisfying, for all $r \in R$, and all $x + N \in M/N$, $r(x + N) = (rx) + N$. Hence, $M/N$ is often referred to as a *quotient $R$-module*.

Let $M$ and $N$ be $R$-modules. A map $\varphi : M \to N$ is called an *$R$-module homomorphism* if the map $\varphi$ satisfies

1) $\varphi(x + y) = \varphi(x) + \varphi(y)$, for all $x, y \in M$ and
2) $\varphi(rx) = r\varphi(x)$, for all $r \in R, x \in M$.

The *kernel of* $\varphi$ is defined as $\ker \varphi \triangleq \{m \in M : \varphi(m) = 0\}$. Clearly, $\ker \varphi$ is a submodule of $M$.

An $R$-module homomorphism $\varphi : M \to N$ is called an *$R$-module isomorphism* if it is both injective and surjective. In this case, the modules $M$ and $N$ are said to be *isomorphic*, denoted by $M \cong N$. An $R$-module $M$ is called a *free* module of *rank* $t$ if $M \cong R^t$ for some nonnegative integer $t$.

There are several isomorphism theorems for modules. The so-called "first isomorphism theorem" is useful for this paper.

*Theorem 1 (First Isomorphism Theorem for Modules [31, p. 349]):* Let $M, N$ be $R$-modules and let $\varphi : M \to N$ be an $R$-module homomorphism. Then $\ker \varphi$ is a submodule of $M$ and $M/\ker \varphi \cong \varphi(M)$.

## D. Modules over a PID

Finitely-generated modules over PIDs play an important role in this paper, and are defined as follows.

*Definition 1 (Finitely-Generated Modules):* Let $R$ be a commutative ring with identity $1 \neq 0$ and let $M$ be an $R$-module. For any subset $A$ of $M$, let $\langle A \rangle$ be the smallest submodule of $M$ containing $A$, called the *submodule generated by* $A$. If $M = \langle A \rangle$ for some finite subset $A$, then $M$ is said to be *finitely generated*.

A finite module (i.e., a module that contains finitely many elements) is always finitely generated, but a finitely-generated module is not necessarily finite. For example, the even integers $2\mathbb{Z}$ form a $\mathbb{Z}$-module generated by $\{2\}$.

The following structure theorem says that, if $T$ is a PID, then a finitely-generated $T$-module is isomorphic to a finite direct product of $T$-modules of the form $T$ or $T/\langle \pi \rangle$.

*Theorem 2 (Structure Theorem for Finitely-Generated Modules over a PID—Invariant Factor Form [31, p. 462]):* Let $T$ be a PID and let $M$ be a finitely-generated $T$-module. Then for some integer $t \geq 0$ and nonzero non-unit elements $\pi_1, \ldots, \pi_k$ of $T$ satisfying the divisibility relations $\pi_1 \mid \pi_2 \mid \cdots \mid \pi_k$,

$$M \cong T^t \times T/\langle \pi_1 \rangle \times T/\langle \pi_2 \rangle \times \cdots \times T/\langle \pi_k \rangle.$$

The elements $\pi_1, \ldots, \pi_k$, called the *invariant factors* of $M$, are unique up to multiplication by units in $T$. The integer $t$ is called the *free rank* of $M$.

### E. Matrices over a PID

Let $R^{m\times n}$ denote the set of all $m \times n$ matrices over $R$. For any matrix $\mathbf{A} \in R^{m\times n}$, we denote by $a_{i,j}$ the entry at the $i$th row and $j$th column of $\mathbf{A}$. A matrix $\mathbf{D} \in R^{m\times n}$ is called a *diagonal matrix* if $d_{i,j} = 0$ whenever $i \neq j$. Note that a diagonal matrix need not be square. A diagonal matrix $\mathbf{D}$ can be written as $\mathbf{D} = \operatorname{diag}(d_1, \ldots, d_r)$, where $r = \min\{m, n\}$, and $d_i = d_{i,i}$ for $i = 1, \ldots, r$.

A square matrix $\mathbf{U} \in R^{n\times n}$ is *invertible* if $\mathbf{UV} = \mathbf{VU} = \mathbf{I}_n$ for some $\mathbf{V} \in R^{n\times n}$, where $\mathbf{I}_n$ denotes the $n \times n$ identity matrix. The set of invertible matrices in $R^{n\times n}$, denoted as $\mathrm{GL}_n(R)$, forms a group—the so-called *general linear group*—under matrix multiplication. Two matrices $\mathbf{A}, \mathbf{B} \in R^{m\times n}$ are said to be *equivalent* if there exist invertible matrices $\mathbf{P} \in \mathrm{GL}_m(R)$ and $\mathbf{Q} \in \mathrm{GL}_n(R)$ such that $\mathbf{B} = \mathbf{PAQ}$. We will write $\mathbf{A} \approx \mathbf{B}$ if $\mathbf{A}$ and $\mathbf{B}$ are equivalent.

*Definition 2 (Smith Normal Form):* Let $\mathbf{A} \in R^{m\times n}$ and let $r = \min\{m, n\}$. A diagonal matrix $\mathbf{D} = \operatorname{diag}(d_1, \ldots, d_r)$ is called a *Smith normal form* of $\mathbf{A}$ if $\mathbf{D} \approx \mathbf{A}$ and $d_1 \mid d_2 \mid \cdots \mid d_r$ in $R$.

Note that $d_1 \mid d_2 \mid \cdots \mid d_r$ in $R$ if and only if $\langle d_1\rangle \supseteq \langle d_2\rangle \supseteq \cdots \supseteq \langle d_r\rangle$. In particular, if $d_i$ is a unit in $R$, then $d_1, \ldots, d_i$ are all units in $R$. Similarly, if $d_i = 0$, then $d_i, \ldots, d_r$ are all $0$. Thus, if $\mathbf{D} = \operatorname{diag}(d_1, \ldots, d_r)$ is a Smith normal form of $\mathbf{A}$, then the diagonal entries $d_1, \ldots, d_r$ of $\mathbf{D}$ can be expressed as

$$d_1, \ldots, d_r = \underbrace{u_1, \ldots, u_i}_{i}, \underbrace{d_{i+1}, \ldots, d_{i+j}}_{j}, \underbrace{0, \ldots, 0}_{k}$$

where $u_1, \ldots, u_i$ are units in $R$, $d_{i+1}, \ldots, d_{i+j}$ are nonzero, non-unit elements in $R$, and $i, j, k \geq 0$ with $i+j+k = r$. The nonzero entries $\{u_1, \ldots, u_i, d_{i+1}, \ldots, d_{i+j}\}$ are called a *sequence of invariant factors* of $\mathbf{A}$.

The Smith normal form theorem says that every matrix over a PID has a Smith normal form whose sequence of invariant factors is unique up to multiplication by units.

*Theorem 3 (Smith Normal Form Theorem [32, p. 194]):* Let $T$ be a PID. Then any $\mathbf{A} \in T^{m\times n}$ has a Smith normal form. Furthermore, if $\mathbf{D}_1 = \operatorname{diag}(d_1, \ldots, d_r)$ and $\mathbf{D}_2 = \operatorname{diag}(s_1, \ldots, s_r)$ are two Smith normal forms of $\mathbf{A}$, then $\langle d_i\rangle = \langle s_i\rangle$ for all $i = 1, \ldots, r$.

### F. Lattices and Lattice Codes

Recall that a real lattice $\Lambda \in \mathbb{R}^n$ is a regular array of points in $\mathbb{R}^n$. Algebraically, a real lattice is defined as a discrete $\mathbb{Z}$-submodule of $\mathbb{R}^n$. A lattice $\Lambda \in \mathbb{R}^n$ may be specified by a set of $m$ basis (row) vectors $\mathbf{g}_1, \ldots, \mathbf{g}_m \in \mathbb{R}^n$, consisting of all $\mathbb{Z}$-linear combinations of the basis vectors, i.e.,

$$\Lambda = \{\mathbf{r}\mathbf{G}_\Lambda : \mathbf{r} \in \mathbb{Z}^m\},$$

where $\mathbf{G}_\Lambda \triangleq \left[\mathbf{g}_1^T | \cdots | \mathbf{g}_m^T\right]^T \in \mathbb{R}^{m\times n}$ is called a *generator matrix* for $\Lambda$. Note that $\mathbf{G}_\Lambda$ is not unique for a given $\Lambda$. We call $m$ the *rank* of $\Lambda$, and $n$ the *dimension* of $\Lambda$. Clearly, $m \leq n$, because otherwise the basis vectors cannot be linearly independent. When $m = n$, $\Lambda$ is called a *full-rank* real lattice.

Complex lattices are natural generalizations of real lattices. Let $T$ be a discrete subring of $\mathbb{C}$ forming a PID. Typical examples of $T$ include the Gaussian integers $\mathbb{Z}[i]$ and the Eisenstein integers $\mathbb{Z}[\omega]$. A $T$-*lattice* $\Lambda$ in $\mathbb{C}^n$ is a discrete $T$-submodule of $\mathbb{C}^n$, consisting of all $T$-linear combinations of a set of basis vectors. Throughout this paper, we will focus on full-rank $T$-lattices for simplicity, but all the results can be easily extended to the case of non-full-rank $T$-lattices.

A few important notions are associated with a $T$-lattice. An $n$-dimensional $T$-lattice $\Lambda$ partitions the space $\mathbb{C}^n$ into *congruent cells*. Such a partition is not unique. The most important example is based on the *nearest neighbor quantizer* $\mathcal{Q}_\Lambda^{\text{NN}}$ that sends a point $\mathbf{x} \in \mathbb{C}^n$ to a nearest lattice point in Euclidean distance, i.e.,

$$\mathcal{Q}_\Lambda^{\text{NN}}(\mathbf{x}) = \boldsymbol{\lambda} \in \Lambda, \quad \text{if } \forall \boldsymbol{\lambda}' \in \Lambda \left( \|\mathbf{x} - \boldsymbol{\lambda}\| \leq \|\mathbf{x} - \boldsymbol{\lambda}'\| \right),$$

where ties are broken in a systematic manner. The *Voronoi cell* $\mathcal{V}_\Lambda(\boldsymbol{\lambda})$ associated with each $\boldsymbol{\lambda} \in \Lambda$ is defined as the set of all points in $\mathbb{C}^n$ that are closest to $\boldsymbol{\lambda}$, i.e., $\mathcal{V}_\Lambda(\boldsymbol{\lambda}) \triangleq \{\mathbf{x} \in \mathbb{C}^n : \mathcal{Q}_\Lambda^{\text{NN}}(\mathbf{x}) = \boldsymbol{\lambda}\}$. The cell $\mathcal{V}_\Lambda(\mathbf{0})$ associated with the origin is often referred to as the *Voronoi region* of $\Lambda$. Clearly, the Voronoi cells $\{\mathcal{V}_\Lambda(\boldsymbol{\lambda})\}$ have the following three properties:

1) Each cell $\mathcal{V}_\Lambda(\boldsymbol{\lambda})$ is a shift of the cell $\mathcal{V}_\Lambda(\mathbf{0})$ by $\boldsymbol{\lambda} \in \Lambda$, i.e., $\mathcal{V}_\Lambda(\boldsymbol{\lambda}) = \boldsymbol{\lambda} + \mathcal{V}_\Lambda(\mathbf{0})$.
2) The cells do not intersect, i.e., $\mathcal{V}_\Lambda(\boldsymbol{\lambda}) \cap \mathcal{V}_\Lambda(\boldsymbol{\lambda}') = \emptyset$ for all $\boldsymbol{\lambda} \neq \boldsymbol{\lambda}'$.
3) The union of the cells covers the whole space, i.e., $\bigcup_{\boldsymbol{\lambda} \in \Lambda} \mathcal{V}_\Lambda(\boldsymbol{\lambda}) = \mathbb{C}^n$.

In general, any collection of cells $\{\mathcal{R}_\Lambda(\boldsymbol{\lambda})\}$ that satisfies the above three conditions is called a set of *fundamental cells*. The cell $\mathcal{R}_\Lambda(\mathbf{0})$ associated with the origin is called a *fundamental region* and will also be denoted simply by $\mathcal{R}_\Lambda$. Note that every fundamental region of a lattice $\Lambda$ has exactly the same volume, which is denoted by $V(\Lambda)$.

A *lattice quantizer* $\mathcal{Q}_\Lambda : \mathbb{C}^n \to \Lambda$ corresponding to $\mathcal{R}_\Lambda$ sends every point $\mathbf{x} \in \mathbb{C}^n$ to the lattice point $\boldsymbol{\lambda}$ that is associated with the fundamental cell $\mathcal{R}_\Lambda(\boldsymbol{\lambda})$ containing $\mathbf{x}$, i.e.,

$$\mathcal{Q}_\Lambda(\mathbf{x}) = \boldsymbol{\lambda} \in \Lambda, \text{ if } \mathbf{x} \in \mathcal{R}_\Lambda(\boldsymbol{\lambda}).$$

Hence, any point $\mathbf{x}$ in $\mathbb{C}^n$ can be uniquely expressed as the sum of a lattice point and a point in the fundamental region $\mathcal{R}_\Lambda$, i.e., $\mathbf{x} = \mathcal{Q}_\Lambda(\mathbf{x}) + (\mathbf{x} - \mathcal{Q}_\Lambda(\mathbf{x}))$, where $\mathbf{x} - \mathcal{Q}_\Lambda(\mathbf{x})$ is a point in $\mathcal{R}_\Lambda$. This implies that, for all lattice points $\boldsymbol{\lambda} \in \Lambda$ and all vectors $\mathbf{z} \in \mathbb{C}^n$,

$$\mathcal{Q}_\Lambda(\boldsymbol{\lambda} + \mathbf{z}) = \boldsymbol{\lambda} + \mathcal{Q}_\Lambda(\mathbf{z}). \tag{1}$$

The modulo-$\Lambda$ operation is defined, for a fixed $\mathcal{Q}_\Lambda$, as

$$\mathbf{x} \bmod \Lambda = \mathbf{x} - \mathcal{Q}_\Lambda(\mathbf{x}).$$

Clearly, the modulo-$\Lambda$ operation always outputs a point in the fundamental region $\mathcal{R}_\Lambda$. The modulo-$\Lambda$ operation has a geometrical interpretation:

$$\mathbf{x} \bmod \Lambda = (\mathbf{x} + \Lambda) \cap \mathcal{R}_\Lambda,$$

where the *lattice shift* $\mathbf{x} + \Lambda$ is defined as $\mathbf{x} + \Lambda = \{\mathbf{x} + \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \Lambda\}$.

A *$T$-sublattice* $\Lambda'$ of $\Lambda$ is a subset of $\Lambda$ which is itself a $T$-lattice. Two lattices $\Lambda'$ and $\Lambda$ are said to be *nested* if $\Lambda'$ is a sublattice of $\Lambda$, i.e., $\Lambda' \subseteq \Lambda$.

For each $\boldsymbol{\lambda} \in \Lambda$, the lattice shift $\boldsymbol{\lambda} + \Lambda'$ is a coset of $\Lambda'$ in $\Lambda$, and the point $\boldsymbol{\lambda} \bmod \Lambda'$ is called the *coset leader* of $\boldsymbol{\lambda} + \Lambda'$. Two cosets $\boldsymbol{\lambda}_1 + \Lambda'$ and $\boldsymbol{\lambda}_2 + \Lambda'$ are either identical (when $\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2 \in \Lambda'$) or disjoint (when $\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2 \notin \Lambda'$). Thus, the set of all distinct cosets of $\Lambda'$ in $\Lambda$, denoted by $\Lambda/\Lambda'$, forms a partition of $\Lambda$. Algebraically, $\Lambda/\Lambda'$ is a quotient $T$-module, hereafter called a *$T$-lattice quotient*.

A *nested lattice code* $\mathcal{L}(\Lambda, \Lambda')$ is defined as the set of all coset leaders in $\Lambda/\Lambda'$, i.e.,

$$\mathcal{L}(\Lambda, \Lambda') = \Lambda \bmod \Lambda' = \{\boldsymbol{\lambda} \bmod \Lambda' : \boldsymbol{\lambda} \in \Lambda\}.$$

Geometrically, $\mathcal{L}(\Lambda, \Lambda')$ is the intersection of the lattice $\Lambda$ with the fundamental region $\mathcal{R}_{\Lambda'}$, i.e.,

$$\mathcal{L}(\Lambda, \Lambda') = \Lambda \cap \mathcal{R}_{\Lambda'}.$$

For this reason, the fundamental region $\mathcal{R}_{\Lambda'}$ is often interpreted as the *shaping region*. Note that there is a bijection between $\Lambda/\Lambda'$ and $\mathcal{L}(\Lambda, \Lambda')$; in particular,

$$|\Lambda/\Lambda'| = |\mathcal{L}(\Lambda, \Lambda')| = V(\Lambda')/V(\Lambda).$$

Finally, we mention that, for reasons of energy-efficiency, it is often useful to consider a translated version of nested lattice codes. For any fixed translation vector $\mathbf{d} \in \mathbb{C}^n$, a *translated nested lattice code* $\mathcal{L}(\Lambda, \Lambda', \mathbf{d})$ is defined as

$$\mathcal{L}(\Lambda, \Lambda', \mathbf{d}) = (\mathbf{d} + \Lambda) \bmod \Lambda' = (\mathbf{d} + \Lambda) \cap \mathcal{R}_{\Lambda'}.$$

## IV. Problem Statement

This section gives a general definition of a *linear* physical-layer network coding (or compute-and-forward) scheme, and also describes the assumptions on the system model made in this paper. We focus on the problem faced by a receiver node of decoding one or more linear combinations of simultaneously transmitted messages, as it is at the heart of any system employing physical-layer network coding (see [24] for such a discussion). We conclude the section by briefly describing some achievability results obtained by Nazer and Gastpar in [1].

While linear network coding is traditionally defined over a finite field [35], [36], our description considers a more general notion of linear network coding over a finite commutative ring $R$. In this context, the message space, i.e., the set from where message packets are drawn, is no longer a vector space, but an $R$-module [37]. As hinted at in Sec. II and as will become clear in Sec. V, ring-linear network coding is required if we wish to ensure compatibility with a *general* lattice network coding scheme.

### A. System Model

Consider a multiple-access channel with $L$ transmitters and a single receiver subject to block fading and additive white Gaussian noise, as illustrated in Fig. 4.

Channel inputs are denoted by $\mathbf{x}_1, \ldots, \mathbf{x}_L \in \mathbb{C}^n$ and the channel output is given by

$$\mathbf{y} = \sum_{\ell=1}^{L} h_\ell \mathbf{x}_\ell + \mathbf{z}$$

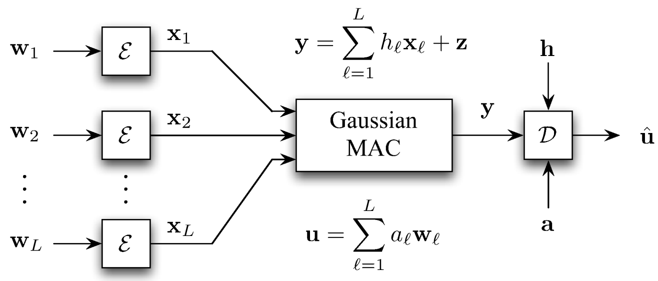



Fig. 4. Computing a linear function over a Gaussian multiple-access channel.

where $h_1, \ldots, h_L \in \mathbb{C}$ are channel gains (fading coefficients) and $\mathbf{z} \sim \mathcal{CN}(\mathbf{0}, N_0\mathbf{I}_n)$ is a circularly-symmetric jointly-Gaussian complex random vector. We assume that the channel gains are perfectly known at the receiver but are *unknown* at the transmitters.

Transmitter $\ell$ is subject to a power constraint given by

$$\frac{1}{n}E\left[\|\mathbf{x}_\ell\|^2\right] \leq P_\ell$$

where the expectation is taken with respect to a uniform distribution over the corresponding message space. For simplicity (and without loss of generality), we assume that the power constraint is symmetric, $P_1 = \cdots = P_L \triangleq P$, and that any asymmetric power constraints are incorporated by appropriately scaling the channel gains $h_\ell$.

For convenience, we define

$$\mathsf{SNR} \triangleq P/N_0.$$

Note that the received SNR corresponding to signal $\mathbf{x}_\ell$ is equal to $|h_\ell|^2 P/N_0$. Hence, the interpretation of $\mathsf{SNR}$ as the average received SNR is only valid when $E[|h_\ell|^2] = 1$.

### B. Linear Physical-Layer Network Coding

Let $R$ be a *finite* commutative ring with identity $1 \neq 0$ and let $T$ be some (usually infinite) commutative ring such that there exists a surjective ring homomorphism $\sigma : T \to R$. Let the *ambient space* $W$ be a finite $R$-module. Note that $\sigma$ automatically makes $W$ into a $T$-module by defining $a\mathbf{w} = \sigma(a)\mathbf{w}$, for all $a \in T$ and all $\mathbf{w} \in W$. As an example, we may have $T = \mathbb{Z}$, $R = \mathbb{Z}/\langle 2 \rangle$, $W = \mathbb{Z}/\langle 2 \rangle$, and $\sigma(a) = a + \langle 2 \rangle$. In the following setup, "digital-layer" network coding operates on $W$ over $R$, while physical-layer network coding operates on $W$ over $T$, and the ring homomorphism $\sigma$ guarantees the compatibility of such operations.

For each $\ell \in \{1, \ldots, L\}$, let the *message space* of transmitter $\ell$ be an $R$-submodule $W_\ell \subseteq W$. A $T$-linear PNC scheme with block length $n$ consists of $L$ encoders

$$\mathcal{E}_\ell : W_\ell \to \mathbb{C}^n$$

each taking a message vector $\mathbf{w}_\ell \in W_\ell$ to a signal vector $\mathbf{x}_\ell \in \mathbb{C}^n$, and a decoder

$$\mathcal{D} : \mathbb{C}^n \to W$$

that takes a received signal $\mathbf{y} \in \mathbb{C}^n$ and attempts to compute one (or more) $T$-linear combination(s) of the messages, such as

$$\mathbf{u} = \sum_{\ell=1}^{L} a_\ell \mathbf{w}_\ell \in W$$

whose coefficients $a_\ell \in T$ may or may not have been specified *a priori*. It is understood that any $T$-linear combinations computed by the decoder are subsequently delivered to the digital layer as $R$-linear combinations, such as

$$\mathbf{u} = \sum_{\ell=1}^{L} a_\ell \mathbf{w}_\ell = \sum_{\ell=1}^{L} \sigma(a_\ell) \mathbf{w}_\ell \in W$$

obtained by the application of $\sigma$ on each coefficient.

The above generic description of the decoder may be specialized depending on the problem at hand. Specifically, any further information given to the decoder (such as side information about the channel gains) will be denoted as additional arguments to $\mathcal{D}$. Similarly, any further information provided by the decoder will be denoted as additional outputs of $\mathcal{D}$. Note that, in this paper, we always assume that the channel-gain vector $\mathbf{h} \triangleq (h_1, \ldots, h_L) \in \mathbb{C}^L$ is perfectly known at the receiver.

For simplicity of notation, let $\mathbf{W} \in W^L$ be a matrix corresponding to the vertical stacking of $\mathbf{w}_1, \ldots, \mathbf{w}_L \in W$, taken as row vectors. If the coefficient vector $\mathbf{a} = (a_1, \ldots, a_L) \in T^L$ for the desired linear combination is specified *a priori*, we will write

$$\mathcal{D} : \mathbb{C}^n \times \mathbb{C}^L \times T^L \to W, \quad \hat{\mathbf{u}} = \mathcal{D}(\mathbf{y}|\mathbf{h}, \mathbf{a}).$$

In this case, a decoding error is made if $\hat{\mathbf{u}} \neq \mathbf{aW}$. The corresponding probability of error is denoted by $P_e(\mathbf{h}, \mathbf{a})$. This decoder is illustrated in Fig. 4.

If no coefficient vectors are given *a priori*, but instead are required to computed "on-the-fly" by the receiver, then we will write

$$\mathcal{D} : \mathbb{C}^n \times \mathbb{C}^L \to W^m \times T^{Lm}$$

$$(\hat{\mathbf{u}}_1, \ldots, \hat{\mathbf{u}}_m, \mathbf{a}_1, \ldots, \mathbf{a}_m) = \mathcal{D}(\mathbf{y}|\mathbf{h})$$

where $m$ denotes the number of linear combinations computed. In this case, a decoding error is made if $\hat{\mathbf{u}}_i \neq \mathbf{a}_i \mathbf{W}$, for some $i \in \{1, \ldots, m\}$.

Since a message is transmitted over $n$ (complex) channel uses, we define the *message rate* (spectral efficiency) for transmitter $\ell$ as $\mathsf{R}_{\mathsf{mes},\ell} \triangleq \frac{1}{n} \log_2 |W_\ell|$, measured in bits per complex dimension. Throughout the paper we assume that all encoders are identical, $\mathcal{E}_1 = \ldots = \mathcal{E}_\ell \triangleq \mathcal{E}$, thus there is a single message space $W$ with message rate

$$\mathsf{R}_{\mathsf{mes}} \triangleq \frac{1}{n} \log_2 |W|.$$

As the following examples illustrate, a number of existing PNC schemes can be described in this framework.

*Example 1:* Let $L = 2$, $n = 1$, $T = \mathbb{Z}$ and $R = W = \mathbb{Z}/\langle 2 \rangle$. Consider the encoder

$$\mathcal{E}(w) = \gamma \left( \tilde{\sigma}(w) - \frac{1}{2} \right), \; w \in \mathbb{Z}/\langle 2 \rangle$$

where $\gamma > 0$ is a scaling factor, and $\tilde{\sigma} : \mathbb{Z}/\langle 2\rangle \to \mathbb{Z}$ is defined as

$$\tilde{\sigma}(w) = \begin{cases} 1, & \text{when } w = 1 + \langle 2\rangle \\ 0, & \text{when } w = 0 + \langle 2\rangle. \end{cases}$$

Suppose $\mathbf{h} = [1\ 1] \in \mathbb{C}^2$. Let $\mathbf{a} = [1\ 1] \in \mathbb{Z}^2$ be a fixed coefficient vector. Then a decoder can be constructed as

$$\mathcal{D}(y|\mathbf{h}, \mathbf{a}) = \begin{cases} 1 + \langle 2\rangle, & \text{if } |\mathrm{Re}\{y\}| < \gamma/2 \\ 0 + \langle 2\rangle, & \text{otherwise.} \end{cases}$$

This is the simplest form of PNC [4], [5], which may be understood as XOR decoding under BPSK modulation, in the case of two users with equal channel gains.

*Example 2:* Let $L = 2$, $n = 1$, $T = \mathbb{Z}[i]$ and $R = W = \mathbb{Z}[i]/\langle m\rangle$, where $m$ is some positive integer. Consider the encoder

$$\mathcal{E}(w) = \gamma\left(\tilde{\sigma}(w) - d\right),\ w \in \mathbb{Z}[i]/\langle m\rangle$$

where $d = \left(\frac{m-1}{2}\right)(1 + i)$, $\gamma > 0$ is a scaling factor, and $\tilde{\sigma} : \mathbb{Z}[i]/\langle m\rangle \to \mathbb{Z}[i]$ is defined as

$$\tilde{\sigma}(a + bi + \langle m\rangle) = (a \bmod m) + (b \bmod m)i.$$

First, suppose $\mathbf{h} = [1\ 1] \in \mathbb{C}^2$. Let $\mathbf{a} = [1\ 1] \in \mathbb{Z}[i]^2$ be the fixed coefficient vector. Then a natural (although suboptimal) decoder is given by

$$\mathcal{D}(y|\mathbf{h}, \mathbf{a}) = (\lfloor \mathrm{Re}\{y'\}\rceil \bmod m) + (\lfloor \mathrm{Im}\{y'\}\rceil \bmod m)\, i + \langle m\rangle,$$

where $y' = y/\gamma + (a_1 + a_2)d$ and $\lfloor\cdot\rceil$ denotes the rounding operation. This scheme is known as the $m^2$-QAM PNC scheme [4]. Next, suppose $\mathbf{h} = [1\ i] \in \mathbb{C}^2$. Let $\mathbf{a} = [1\ i] \in \mathbb{Z}[i]^2$ be the fixed coefficient vector. Then the above decoder generalizes the example discussed in Sec. II.

### *C. Achievable Rates*

We now mention some known achievable rates for the case of a single given coefficient vector, under the assumptions of Section IV-A. These results were obtained by Nazer and Gastpar [1].

*Theorem 4 ([1]):* For all $\epsilon > 0$, all sufficiently large $n$, and some appropriately chosen prime integer $p$, there exists a $\mathbb{Z}[i]$-linear PNC scheme with block length $n$ satisfying the following properties:

1) the message space is $W = (\mathbb{Z}[i]/\langle p\rangle)^k$ for some $k$;
2) for any channel-gain vector $\mathbf{h} \in \mathbb{C}^L$ and any non-zero coefficient vector $\mathbf{a} \in \mathbb{Z}[i]^L$, the probability of decoding error $P_e(\mathbf{h}, \mathbf{a})$ is smaller than $\epsilon$ if $k$ is such that the message rate $\mathsf{R}_{\mathsf{mes}}$ is smaller than the computation rate

$$R_{\mathsf{comp}}(\mathbf{h}, \mathbf{a}) \triangleq \max_{\alpha \in \mathbb{C}} \log_2\left(\frac{\mathsf{SNR}}{\|\alpha\mathbf{h} - \mathbf{a}\|^2\,\mathsf{SNR} + |\alpha|^2}\right).$$

Moreover, the optimal value of $\alpha$ in the above expression is given by

$$\alpha_{\mathsf{opt}} = \frac{\mathbf{a}\mathbf{h}^{\mathsf{H}}\,\mathsf{SNR}}{\|\mathbf{h}\|^2\,\mathsf{SNR} + 1} \tag{2}$$

which results in

$$R_{\mathsf{comp}}(\mathbf{h},\mathbf{a}) = \log_2\left(\frac{\mathsf{SNR}}{\mathbf{a}\mathbf{M}\mathbf{a}^{\mathsf{H}}}\right),$$

where

$$\mathbf{M} = \mathsf{SNR}\,\mathbf{I}_L - \frac{\mathsf{SNR}^2}{\mathsf{SNR}\,\|\mathbf{h}\|^2+1}\mathbf{h}^{\mathsf{H}}\mathbf{h} \tag{3}$$

and $\mathbf{I}_L$ is the $L\times L$ identity matrix.

*Remark:* In the proof of the above result, $p$ has to grow appropriately with $n$ such that $n/p\to 0$ as $n\to\infty$ [1].

Theorem 4 is based on the existence of a "good" sequence of nested lattices of increasing dimension. Criteria to design low complexity, finite-dimensional PNC schemes are not immediately obvious from these results. In the remainder of this paper, we will develop an algebraic framework for studying linear PNC schemes, which facilitates the construction and analysis of practical PNC schemes.

## V. Lattice Network Coding

### A. Linear Labelings

Let $T$ be a discrete subring of $\mathbb{C}$ forming a PID, and let $\Lambda\subseteq\mathbb{C}^n$ and $\Lambda'\subseteq\Lambda$ be two full-rank $T$-lattices (called *fine* and *coarse*, respectively) so that the index $|\Lambda/\Lambda'|$ of $\Lambda'$ in $\Lambda$ is finite. Recall that $\Lambda/\Lambda'$ is a quotient $T$-module, i.e., it is a set closed under addition and multiplication by elements of $T$. Specifically, addition of cosets is defined as $(\boldsymbol{\lambda}_1+\Lambda')+(\boldsymbol{\lambda}_2+\Lambda')\triangleq(\boldsymbol{\lambda}_1+\boldsymbol{\lambda}_2+\Lambda')$, for all $\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2\in\Lambda$, multiplication by $r\in T$ is defined as $r(\boldsymbol{\lambda}+\Lambda')\triangleq(r\boldsymbol{\lambda}+\Lambda')$, for all $\boldsymbol{\lambda}\in\Lambda$, and multiplication distributes over addition. An immediate consequence is that $\sum_{\ell=1}^{L} r_\ell(\boldsymbol{\lambda}_\ell+\Lambda')=(\sum_{\ell=1}^{L} r_\ell\boldsymbol{\lambda}_\ell)+\Lambda'$, i.e., a $T$-linear combination of cosets is determined by the linear combination of their coset representatives. This is the main property exploited in a lattice network coding (LNC) scheme.

Conceptually, an LNC scheme is a $T$-linear PNC scheme based on a finite lattice quotient $\Lambda/\Lambda'$, in which each transmitter sends an information-embedding coset through a coset representative, and each receiver recovers one or more $T$-linear combinations of the transmitted coset representatives (which can potentially be forwarded to other nodes according to the same scheme). Upon receiving enough such combinations, the destination is able to decode all information-embedding cosets from the transmitters.

To facilitate practical implementation, we will specify a map $\varphi:\Lambda\to W$ from lattice points in $\Lambda$ to messages in the message space $W$ for use in the above architecture. The map $\varphi$ must satisfy two conditions:

1) all points in the same coset are mapped to the same message, i.e., if for any two points $\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2\in\Lambda$ with $\boldsymbol{\lambda}_1-\boldsymbol{\lambda}_2\in\Lambda'$, $\varphi(\boldsymbol{\lambda}_1)=\varphi(\boldsymbol{\lambda}_2)$;
2) the map $\varphi$ is $T$-linear, i.e., for all $r_1,r_2\in T$ and all $\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2\in\Lambda$, we have $\varphi\left(r_1\boldsymbol{\lambda}_1+r_2\boldsymbol{\lambda}_2\right)=r_1\varphi(\boldsymbol{\lambda}_1)+r_2\varphi(\boldsymbol{\lambda}_2)$.

We refer to the map $\varphi$ as a *linear labeling* of $\Lambda$. As we shall see, it is this linear labeling that induces a natural compatibility between the $\mathbb{C}$-linear arithmetic of the multiple access channel observed by the receiver and the $T$-linear arithmetic desired in the message space.

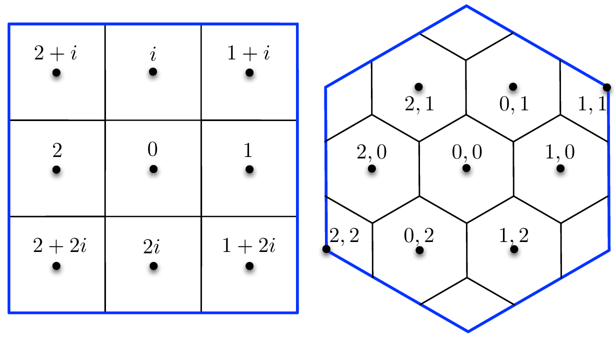



Fig. 5. Linear labelings for Examples 3 and 4.

The existence of the aforementioned linear labeling is guaranteed by the following theorem, which provides a *canonical decomposition* for any finite $T$-lattice quotient $\Lambda/\Lambda'$.

*Theorem 5:* Let $T$ be a PID and let $\Lambda$ and $\Lambda' \subseteq \Lambda$ be $T$-lattices such that $|\Lambda/\Lambda'|$ is finite. Then, for some nonzero, non-unit elements $\pi_1, \pi_2, \ldots, \pi_k \in T$ satisfying the divisibility relations $\pi_1 \mid \pi_2 \mid \cdots \mid \pi_k$, we have

$$\Lambda/\Lambda' \cong T/\langle \pi_1 \rangle \times T/\langle \pi_2 \rangle \times \cdots \times T/\langle \pi_k \rangle. \tag{4}$$

Moreover, there exists a surjective $T$-module homomorphism $\varphi : \Lambda \to T/\langle \pi_1 \rangle \times \cdots \times T/\langle \pi_k \rangle$ whose kernel is $\Lambda'$.

*Proof:* The first statement follows from Theorem 2 since $\Lambda/\Lambda'$ is a finite $T$-module. The second statement then follows from the First Isomorphism Theorem [31]. ∎

Evidently, the map $\varphi$ is obtained as the composition of the natural projection from $\Lambda$ to the quotient $\Lambda/\Lambda'$ with the isomorphism of (4). According to Theorem 5, when the message space $W$ is taken as the canonical decomposition in the right-hand side of (4), i.e.,

$$W = T/\langle \pi_1 \rangle \times T/\langle \pi_2 \rangle \times \cdots \times T/\langle \pi_k \rangle,$$

the map $\varphi$ is indeed a linear labeling. The following examples provide two concrete linear labelings, which are depicted in Fig. 5.

*Example 3:* Let $\Lambda = \mathbb{Z}[i]$ and $\Lambda' = 3\mathbb{Z}[i]$. Let $T = \mathbb{Z}[i]$ and $W = \mathbb{Z}[i]/\langle 3 \rangle$. Consider the map $\varphi : \Lambda \to W$ given by

$$\varphi(a + bi) = a + bi + \langle 3 \rangle.$$

It is easy to check that the map $\varphi$ is $\mathbb{Z}[i]$-linear and its kernel is $3\mathbb{Z}[i]$.

*Example 4:* Let $\Lambda$ be the (real) hexagonal lattice generated by $\mathbf{g}_1 = (1, 0)$ and $\mathbf{g}_2 = (1/2, \sqrt{3}/2)$. Let $\Lambda' = 3\Lambda$. Let $T = \mathbb{Z}$ and $W = \mathbb{Z}/\langle 3 \rangle \times \mathbb{Z}/\langle 3 \rangle$. Consider the map $\varphi : \Lambda \to W$ given by

$$\varphi(a\mathbf{g}_1 + b\mathbf{g}_2) = (a \bmod 3, b \bmod 3).$$

It is easy to check that the map $\varphi$ is $\mathbb{Z}$-linear and its kernel is $3\Lambda$.

Linear labelings play a key role in LNC, as they directly map a $T$-linear combination of transmitted lattice points to a $T$-linear combination of transmitted messages, i.e., the latter can be immediately extracted from the former.

It is also convenient to define an inverse operation, mapping a message to a corresponding lattice point; this is done through an *embedding map* $\tilde{\varphi} : W \to \Lambda$. This map must be an injective function compatible with the linear labeling, so it must satisfy

$$\varphi(\tilde{\varphi}(\mathbf{w})) = \mathbf{w}, \quad \text{for all } \mathbf{w} \in W.$$

Equipped with a linear labeling $\varphi$ and and embedding map $\tilde{\varphi}$, a high-level description of a generic LNC scheme can be given as follows. Each encoder $\ell$ maps a message $\mathbf{w}_\ell \in W$ to a lattice point $\mathbf{x}_\ell \in \Lambda$ labeled by $\mathbf{w}_\ell$, i.e., $\mathbf{x}_\ell = \tilde{\varphi}(\mathbf{w}_\ell)$. The decoder, upon the reception of $\mathbf{y}$, and given a coefficient vector $\mathbf{a} = (a_1, \ldots, a_L)$, attempts to compute the $T$-linear combination of transmitted lattice points

$$\boldsymbol{\lambda} = \sum_{\ell=1}^{L} a_\ell \mathbf{x}_\ell$$

from which it would be able to extract the corresponding linear combination of messages

$$\mathbf{u} = \varphi(\boldsymbol{\lambda}) = \sum_{\ell=1}^{L} a_\ell \varphi(\mathbf{x}_\ell) = \sum_{\ell=1}^{L} a_\ell \mathbf{w}_\ell.$$

In more detail, the decoder proceeds in three steps. First, it scales the received signal by a factor of $\alpha$, obtaining

$$\alpha \mathbf{y} = \alpha \sum_{\ell=1}^{L} h_\ell \mathbf{x}_\ell + \alpha \mathbf{z} = \boldsymbol{\lambda} + \mathbf{n} \tag{5}$$

where

$$\mathbf{n} = \sum_{\ell=1}^{L} (\alpha h_\ell - a_\ell) \mathbf{x}_\ell + \alpha \mathbf{z} \tag{6}$$

is called the *effective noise*. Note that we can view (5) as an *equivalent point-to-point channel* under lattice coding: an effective message $\mathbf{u}$ is encoded as a lattice point $\boldsymbol{\lambda}$, which is then additively corrupted by the (signal-dependent and not necessarily Gaussian) effective noise $\mathbf{n}$.

Second, the decoder quantizes the scaled received signal with the fine lattice to obtain

$$\hat{\boldsymbol{\lambda}} = \mathcal{Q}_\Lambda(\alpha \mathbf{y}) = \mathcal{Q}_\Lambda(\boldsymbol{\lambda} + \mathbf{n}) = \boldsymbol{\lambda} + \mathcal{Q}_\Lambda(\mathbf{n}) \tag{7}$$

where (7) follows from the property (1) of a lattice quantizer.

The last step is to apply the linear labeling, obtaining

$$\hat{\mathbf{u}} = \varphi(\hat{\boldsymbol{\lambda}}) = \varphi\left(\boldsymbol{\lambda} + \mathcal{Q}_\Lambda(\mathbf{n})\right) = \mathbf{u} + \varphi\left(\mathcal{Q}_\Lambda(\mathbf{n})\right).$$

The decoder makes an error if and only if $\varphi\left(\mathcal{Q}_\Lambda(\mathbf{n})\right) = \mathbf{0}$ and therefore if and only if $\mathcal{Q}_\Lambda(\mathbf{n}) \in \Lambda'$. This is intuitive: if $\mathcal{Q}_\Lambda(\mathbf{n}) \in \Lambda'$, then the decoded lattice point $\hat{\boldsymbol{\lambda}}$ is in the same coset as $\boldsymbol{\lambda}$ and is thus labeled with $\mathbf{u}$. On the other hand, if the decoded lattice point $\hat{\boldsymbol{\lambda}}$ is labeled with $\mathbf{u}$, then we must have $\varphi(\mathcal{Q}_\Lambda(\mathbf{n})) = \mathbf{0}$, which implies $\mathcal{Q}_\Lambda(\mathbf{n}) \in \Lambda'$, since the kernel of $\varphi$ is $\Lambda'$.

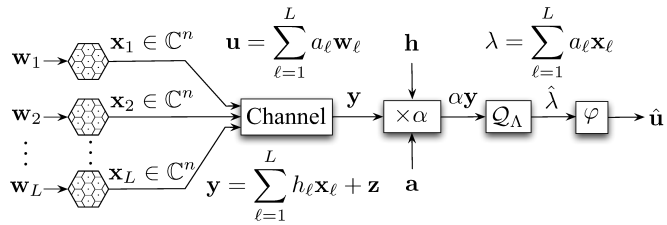



Fig. 6. Encoding and decoding architecture for LNC.

To sum up, the above encoding-decoding architecture is depicted in Fig. 6. The encoder $\mathcal{E} : W \to \mathbb{C}^n$ is given by

$$\mathbf{x}_\ell = \mathcal{E}(\mathbf{w}_\ell) = \tilde{\varphi}(\mathbf{w}_\ell)$$

and the decoder $\mathcal{D} : \mathbb{C}^n \times \mathbb{C}^L \times T^L$ is given by

$$\hat{\mathbf{u}} = \mathcal{D}(\mathbf{y}|\mathbf{h}, \mathbf{a}) = \varphi(\mathcal{Q}_\Lambda(\alpha\mathbf{y}))$$

where $\alpha$ is a scaling factor chosen by the decoder based on $\mathbf{h}$ and $\mathbf{a}$, which will be discussed fully in the next section. Intuitively, the purpose of $\alpha$ is to reduce the effective noise $\mathbf{n}$, by trading off between *self noise* (the first term in (6) due to non-integer channel gains) and Gaussian noise.

Clearly, the encoding-decoding complexity of an LNC scheme is not essentially different from that for a point-to-point channel using the same nested lattice code. Further, the error probability of the scheme can be characterized by Proposition 1, as explained before.

*Proposition 1:* The message $\mathbf{u} = \sum_{\ell=1}^{L} a_\ell \mathbf{w}_\ell$ is computed incorrectly if and only if $\mathcal{Q}_\Lambda(\mathbf{n}) \notin \Lambda'$. That is, $\Pr[\hat{\mathbf{u}} \neq \mathbf{u}] = \Pr[\mathcal{Q}_\Lambda(\mathbf{n}) \notin \Lambda']$.

In practice, the nearest-neighbor quantizer $\mathcal{Q}_\Lambda^{\mathrm{NN}}$ is often preferred in the implementation of the decoder. This is to reduce the error probability, as we will see in Sec. VI. Moreover, for reasons of energy-efficiency, a nested lattice code $\mathcal{L}(\Lambda, \Lambda')$ is usually preferred in the implementation of the encoder. In this case, the encoder takes the messages in $W$ to their *minimum-energy* coset representatives, i.e., the embedding map is chosen to satisfy

$$\tilde{\varphi}(\mathbf{w}_\ell) = \tilde{\varphi}(\mathbf{w}_\ell) \bmod \Lambda'$$

where the shaping region $\mathcal{R}_{\Lambda'}$ is chosen as the Voronoi region.

Sometimes, a *translated* nested lattice code can be used to further reduce the energy consumption. Such techniques are well studied in the area of Voronoi constellations (see, e.g., [38], [39]). Specifically, a translated version of a generic LNC scheme consists of an encoder $\mathcal{E} : W \times \mathbb{C}^n \to \mathbb{C}^n$

$$\mathbf{x}_\ell = \mathcal{E}(\mathbf{w}_\ell \mid \mathbf{d}_\ell) \triangleq (\mathbf{d}_\ell + \tilde{\varphi}(\mathbf{w}_\ell)) \bmod \Lambda'$$

and a decoder $\mathcal{D} : \mathbb{C}^n \times \mathbb{C}^L \times R^L \times (\mathbb{C}^n)^L \to W$

$$\hat{\mathbf{u}} = \mathcal{D}(\mathbf{y} \mid \mathbf{h}, \mathbf{a}, \{\mathbf{d}_\ell\}) \triangleq \varphi\left(\mathcal{Q}_\Lambda\left(\alpha\mathbf{y} - \sum_{\ell=1}^{L} a_\ell \mathbf{d}_\ell\right)\right).$$

Note that Proposition 1 holds unchanged in this case.

Finally, note that the message rate of an LNC scheme can be computed geometrically as well as algebraically, as

$$\begin{aligned}\mathsf{R}_{\mathsf{mes}} &= \frac{1}{n}\log_2\left(V(\Lambda')/V(\Lambda)\right)\\ &= \frac{1}{n}\sum_{i=1}^{k}\log_2|T/\langle\pi_i\rangle|.\end{aligned}$$

*B. Construction of the Linear Labeling*

In this section, by applying the Smith normal form theorem, we provide an explicit construction of the linear labeling $\varphi$ and an embedding map $\tilde{\varphi}$.

*Theorem 6:* Let $\Lambda/\Lambda'$ be a finite nested $T$-lattice quotient. Then there exist generator matrices $\mathbf{G}_\Lambda$ and $\mathbf{G}_{\Lambda'}$ for $\Lambda$ and $\Lambda'$, respectively, satisfying

$$\mathbf{G}_{\Lambda'} = \begin{bmatrix}\mathrm{diag}(\pi_1,\ldots,\pi_k) & \mathbf{0}\\ \mathbf{0} & \mathbf{I}_{n-k}\end{bmatrix}\mathbf{G}_\Lambda. \tag{8}$$

In this case,

$$\Lambda/\Lambda' \cong T/\langle\pi_1\rangle\times\cdots\times T/\langle\pi_k\rangle.$$

Moreover, the map

$$\varphi:\Lambda\to T/\langle\pi_1\rangle\times\cdots\times T/\langle\pi_k\rangle$$

given by

$$\varphi(\mathbf{r}\mathbf{G}_\Lambda) = (r_1+\langle\pi_1\rangle,\ldots,r_k+\langle\pi_k\rangle)$$

is a surjective $T$-module homomorphism with kernel $\Lambda'$.

*Proof:* Let $\tilde{\mathbf{G}}_\Lambda$ and $\tilde{\mathbf{G}}_{\Lambda'}$ be any generator matrices for $\Lambda$ and $\Lambda'$, respectively. Then $\tilde{\mathbf{G}}_{\Lambda'} = \mathbf{J}\tilde{\mathbf{G}}_\Lambda$, for some nonsingular matrix $\mathbf{J}\in T^{n\times n}$. Since $T$ is a PID, by Theorem 3, the matrix $\mathbf{J}$ has a Smith normal form $\mathbf{D} = \mathrm{diag}(d_1,\ldots,d_n)$. Since $\mathbf{J}$ is nonsingular, the diagonal entries $d_1,\ldots,d_n$ of $\mathbf{D}$ are all nonzero. Thus, $d_1,\ldots,d_n$ can be expressed as

$$d_1,\ldots,d_n = u_1,\ldots,u_{n-k},\pi_1,\ldots,\pi_k$$

where $u_1,\ldots,u_{n-k}$ are units in $T$, $\pi_1,\ldots,\pi_k$ are nonzero, non-unit elements in $T$. It follows that

$$\mathbf{D}\approx\tilde{\mathbf{D}}\triangleq\begin{bmatrix}\mathrm{diag}(\pi_1,\ldots,\pi_k) & \mathbf{0}\\ \mathbf{0} & \mathbf{I}_{n-k}\end{bmatrix}.$$

Therefore, $\mathbf{J}\approx\tilde{\mathbf{D}}$ and there exist invertible matrices $\mathbf{P},\mathbf{Q}\in\mathrm{GL}_n(T)$ such that $\tilde{\mathbf{D}} = \mathbf{P}\mathbf{J}\mathbf{Q}$. We take

$$\mathbf{G}_\Lambda = \mathbf{Q}^{-1}\tilde{\mathbf{G}}_\Lambda$$

$$\mathbf{G}_{\Lambda'} = \mathbf{P}\tilde{\mathbf{G}}_{\Lambda'}$$

as new generator matrices for $\Lambda$ and $\Lambda'$. Clearly, we have $\mathbf{G}_{\Lambda'} = \tilde{\mathbf{D}}\mathbf{G}_\Lambda$. This proves the first statement.

Since the second statement follows immediately from the third statement and the First Isomorphism Theory, we need only to prove the third statement here. That is, we must show that the map $\varphi$ is a surjective $T$-homomorphism with kernel $\Lambda'$. Since it is easy to check that the map $\varphi$ is surjective and $T$-linear, we will show that the kernel of $\varphi$ is $\Lambda'$. Note that

$$\varphi(\mathbf{r}\mathbf{G}_\Lambda) = \mathbf{0} \iff \forall i \in \{1, \ldots, k\} r_i \in \langle \pi_i \rangle.$$

Note also that

$$\Lambda' = \{\mathbf{r}\mathbf{G}_\Lambda : r_i \in \langle \pi_i \rangle\},$$

because $\mathbf{G}_{\Lambda'} = \tilde{\mathbf{D}}\mathbf{G}_\Lambda$. Hence, the kernel of $\varphi$ is indeed $\Lambda'$. ■

Theorem 6 constructs a linear labeling $\varphi : \Lambda \to W$ explicitly. The key step is to find two generator matrices $\mathbf{G}_\Lambda$ and $\mathbf{G}_{\Lambda'}$ satisfying the relation (8). This can be achieved by using the Smith normal form theorem. To construct an embedding map $\tilde{\varphi}$, one shall find a pre-image for each message $\mathbf{w} = (r_1 + \langle \pi_1 \rangle, \ldots, r_k + \langle \pi_k \rangle)$. Clearly, one natural choice of $\tilde{\varphi}(\mathbf{w})$ is given by

$$\tilde{\varphi}(\mathbf{w}) = (r_1, \ldots, r_k, \underbrace{0, \ldots, 0}_{n-k})\mathbf{G}_\Lambda,$$

which provides an explicit expression for $\tilde{\varphi}(\mathbf{w})$.

The use of the Smith normal form in coding theory is not new. In the work of Forney [39], [40], it was applied to study the structure of convolutional codes as well as the linear labeling for real lattices. The goal of the Smith normal form theorem is to reduce an arbitrary matrix to a diagonal matrix, whose diagonal entries are the invariant factors. In the context of complex $T$-lattices, such a diagonal matrix reveals the nesting structure between the fine lattice and the coarse lattice, leading to a transparent linear labeling.

### *C. End-to-End Perspective*

In this section, we study the use of LNC in a non-coherent network model (where destinations have no knowledge of the operations of relay nodes) rather than the coherent network model described in [1]. To provide a context for our study, we consider a Gaussian relay network in which a generic LNC scheme is used in conjunction with a scheduling algorithm. The scheduling algorithm indicates, at each time slot, which nodes are transmitters and which nodes are receivers. As a transmitter, a node first computes a random linear combination of the packets in its buffer and then maps this combination to a transmitted signal. As a receiver, a node first decodes the received signal into one or more linear combinations of the transmitted packets and then performs (some form of) Gaussian elimination in order to discard redundant (linearly dependent) packets in the buffer.

Initially, only the source nodes have nonempty buffers containing the message packets. When the communication ends, each destination node will have collected sufficiently many linear combinations of the message packets. This induces an end-to-end linear network-coding channel in which the message space $W$ is, in general, a $T$-module $T/\langle \pi_1 \rangle \times \cdots \times T/\langle \pi_k \rangle$. Since modules over PIDs share much in common with vector spaces over finite fields, it would be natural to expect that many useful techniques for non-coherent network coding can be adapted here.

We use the technique of headers as an illustrating example in this section. For convenience, we rewrite the message space as

$$W = T/\langle \pi_k \rangle \times \cdots \times T/\langle \pi_1 \rangle.$$

Similar to the vector-space case, we use the first $m$ components to store headers, and the last $k-m$ components to store payloads, where $m$ is the number of message packets. Specifically, the header for the $i$th message packet is a length-$m$ tuple with $1 + \langle \pi_{k-i+1} \rangle$ at position $i$ and $0 + \langle \pi_{k-j+1} \rangle$ at other positions (where $1 \le j \le m$ and $j \ne i$).

*Example 5:* Let the message space $W = \mathbb{Z}/\langle 12 \rangle \times \mathbb{Z}/\langle 6 \rangle \times \mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$. Suppose there are 2 original messages in the system. Then the matrix $\mathbf{W}$ of the source messages is of the form

$$\mathbf{W} = \begin{bmatrix} 1 + \langle 12 \rangle & 0 + \langle 6 \rangle & a + \langle 2 \rangle & b + \langle 2 \rangle \\ 0 + \langle 12 \rangle & 1 + \langle 6 \rangle & c + \langle 2 \rangle & d + \langle 2 \rangle \end{bmatrix},$$

where $a, b, c, d \in \mathbb{Z}$.

Recall that, when the message space is a vector space, Gauss-Jordan elimination is used to recover the payloads at the destinations. As one may expect, for a more general message space, some modification of Gauss-Jordan elimination is needed. It turns out that the key step in the modification is to transform a $2 \times 1$ matrix to a row echelon form: given $a, b \in T$, return $s, t, u, v, g \in T$ such that

$$\begin{bmatrix} s & t \\ u & v \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} g \\ 0 \end{bmatrix}$$

where the determinant, $sv - tu$, is a unit from $T$.

*Example 6:* Suppose that the matrix $\mathbf{W}$ of the message packets is given in Example 5. Suppose that a destination has received two linear combinations, $2\mathbf{w}_1 + 3\mathbf{w}_2$ and $3\mathbf{w}_1 + 2\mathbf{w}_2$. Then the matrix $\mathbf{Y}$ of the received packets at the destination is $\mathbf{Y} = \begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix} \mathbf{W}$, which is in the form of

$$\mathbf{Y} = \begin{bmatrix} 2 + \langle 12 \rangle & 3 + \langle 6 \rangle & c + \langle 2 \rangle & d + \langle 2 \rangle \\ 3 + \langle 12 \rangle & 2 + \langle 6 \rangle & a + \langle 2 \rangle & b + \langle 2 \rangle \end{bmatrix}.$$

To recover the payloads, we reduce the first column of $\mathbf{Y}$ to a row echelon form. Since

$$\begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

over $\mathbb{Z}$ and the determinant, $2 \times 2 - (-1) \times (-3) = 1$, is a unit in $\mathbb{Z}$, we multiply the matrix $\begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$ with $\mathbf{Y}$, obtaining

$$\begin{aligned} \mathbf{Y}_1 &= \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix} \mathbf{Y} \\ &= \begin{bmatrix} 1 + \langle 12 \rangle & 4 + \langle 6 \rangle & a + \langle 2 \rangle & b + \langle 2 \rangle \\ 0 + \langle 12 \rangle & 1 + \langle 6 \rangle & c + \langle 2 \rangle & d + \langle 2 \rangle \end{bmatrix}. \end{aligned}$$

In this way, we transform the matrix $\mathbf{Y}$ to a row echelon form. Next, we transform the matrix $\mathbf{Y}$ to a reduced row echelon form, which can be done by subtracting $4$ times the second row from the first row, i.e.,

$$\mathbf{Y}_2 = \begin{bmatrix} 1 & -4 \\ 0 & 1 \end{bmatrix} \mathbf{Y}_1.$$

Now it is easy to check that $\mathbf{Y}_2 = \mathbf{W}$. In other words, the payloads are recovered correctly.

Although Example 6 only illustrates the decoding procedure for the case of $m = 2$, it can be extended to the case of $m > 2$ through a simple mathematical induction.

Finally, we would like to point out that the design of headers in Example 5 is suboptimal, and a better design can be made by using matrix canonical forms. The development of this idea is beyond the scope of this paper and will instead be discussed in a separate paper [41].

## VI. Performance Analysis for Lattice Network Coding

In this section, we turn from algebra to geometry, presenting an error-probability analysis as well as its implications.

### A. *Error Probability for LNC*

Recall that, according to Proposition 1, the error probability of decoding a linear function $\mathbf{u}$ is $\Pr[\hat{\mathbf{u}} \neq \mathbf{u}] = \Pr[\mathcal{Q}_\Lambda(\mathbf{n}) \notin \Lambda']$, where $\mathbf{n}$ is the effective noise given by (6). Note that the effective noise $\mathbf{n}$ is not necessarily Gaussian, making the analysis nontrivial. To alleviate this difficulty, we focus on a special case in which the shaping region $\mathcal{R}_{\Lambda'}$ is a (rotated) hypercube in $\mathbb{C}^n$, i.e.,

$$\mathcal{R}_{\Lambda'} = \gamma \mathbf{U} \mathcal{H}_n \tag{9}$$

where $\gamma > 0$ is a scalar factor, $\mathbf{U}$ is any $n \times n$ unitary matrix, and $\mathcal{H}_n$ is a unit hypercube in $\mathbb{C}^n$ defined by $\mathcal{H}_n = ([-1/2, 1/2) + i[-1/2, 1/2))^n$. This case corresponds to the so-called *hypercube shaping* in [42]. The assumption of hypercube shaping not only simplifies the analysis of error probability, but also has some practical advantages, for example, the complexity of the shaping operation is generally low. However, as we will see later, there is no shaping gain under hypercube shaping. This is expected, since similar results hold for the use of lattice codes in point-to-point channels [39], [42].

In the sequel, we will provide an approximate upper bound for the error probability for LNC schemes admitting hypercube shaping. This upper bound is closely related to certain geometrical parameters of a lattice quotient as defined below.

Let us define the *minimum (inter-coset) distance* of a lattice quotient $\Lambda/\Lambda'$ as

$$\begin{aligned} d(\Lambda/\Lambda') &\triangleq \min_{\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \Lambda : \boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2 \notin \Lambda'} ||\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2|| \\ &= \min_{\boldsymbol{\lambda} \in \Lambda \setminus \Lambda'} ||\boldsymbol{\lambda}|| \end{aligned}$$

where $\Lambda \setminus \Lambda'$ denotes the set difference $\{\boldsymbol{\lambda} \in \Lambda : \boldsymbol{\lambda} \notin \Lambda'\}$. Note that $d(\Lambda/\Lambda')$ corresponds to the length of the shortest vectors in $\Lambda \setminus \Lambda'$. Let $K(\Lambda/\Lambda')$ denote the number of these shortest vectors.

We have the following union bound estimate on the error probability.

*Theorem 7 (Probability of Decoding Error):* Suppose that the shaping region $\mathcal{R}_{\Lambda'}$ is a (rotated) hypercube and that all the transmitted vectors are independent and uniformly distributed over $\mathcal{R}_{\Lambda'}$. Suppose that $\mathcal{Q}_\Lambda(\cdot)$ is a nearest-neighbor quantizer. Then a union bound estimate on the error probability in decoding a specified linear combination is

$$\begin{aligned} & P_e(\mathbf{h}, \mathbf{a}) \\ & \lessapprox \min_{\alpha \in \mathbb{C}} K(\Lambda/\Lambda') \exp\left( -\frac{d^2(\Lambda/\Lambda')}{4N_0(|\alpha|^2 + \mathsf{SNR}\,\|\alpha\mathbf{h} - \mathbf{a}\|^2)} \right). \end{aligned} \tag{10}$$

Moreover, the optimal value of $\alpha$, i.e., the value of $\alpha$ that minimizes the right-hand side of (10), is given by (2), which results in

$$P_e(\mathbf{h}, \mathbf{a}) \lessapprox K(\Lambda/\Lambda') \exp\left( -\frac{d^2(\Lambda/\Lambda')}{4N_0 \mathbf{a}\mathbf{M}\mathbf{a}^{\mathsf{H}}} \right) \tag{11}$$

where the matrix $\mathbf{M}$ is given by (3).

The proof is given in Appendix A. Note that the proof assumes the use of random dithering (translation by a random vector chosen uniformly at random from the shaping region) at the encoders, so that the transmitted vectors are uniformly distributed over the shaping region.

Theorem 7 implies that the lattice quotient $\Lambda/\Lambda'$ should be designed such that $K(\Lambda/\Lambda')$ is minimized and $d(\Lambda/\Lambda')$ is maximized (under a given message rate $\mathsf{R}_{\mathsf{mes}}$ and $\mathsf{SNR}$), which will be discussed fully in Sec. VII. Further, if the receiver has the freedom to choose the coefficient vector $\mathbf{a}$, it needs to minimize the term $\mathbf{a}\mathbf{M}\mathbf{a}^{\mathsf{H}}$, which, as observed in [18], is a shortest vector problem. Theorem 7 can be extended to other shaping methods. A particular example is provided in [28].

## B. Nominal Coding Gain

Similarly to the point-to-point case, we define the *nominal coding gain* of $\Lambda/\Lambda'$ as

$$\gamma_c(\Lambda/\Lambda') \triangleq \frac{d^2(\Lambda/\Lambda')}{V(\Lambda)^{1/n}}.$$

Note that the nominal coding gain is invariant to scaling. For an LNC scheme with hypercube shaping, we have $V(\Lambda') = \gamma^{2n}$ and $P = \gamma^2/6$ where $\gamma > 0$ is the scalar factor in (9). Thus, $V(\Lambda')^{1/n} = 6P$. Note also that $V(\Lambda)^{1/n} = 2^{-\mathsf{R}_{\mathsf{mes}}} V(\Lambda')^{1/n}$. It follows that the union bound estimate in (11) can be expressed as

$$P_e(\mathbf{h}, \mathbf{a}) \lessapprox K(\Lambda/\Lambda') \exp\left( -\frac{3}{2} \gamma_c(\Lambda/\Lambda') 2^{-\mathsf{R}_{\mathsf{mes}}} \frac{\mathsf{SNR}}{\mathbf{a}\mathbf{M}\mathbf{a}^{\mathsf{H}}} \right).$$

Thus, for a given spectral efficiency $\mathsf{R}_{\mathsf{mes}}$, the performance of such an LNC scheme can be characterized by the parameters $K(\Lambda/\Lambda')$ and $\gamma_c(\Lambda/\Lambda')$.

Note that the nominal coding gain of a baseline lattice quotient $\mathbb{Z}[i]^n/\pi\mathbb{Z}[i]^n$ is equal to $1$ for all $\pi \in \mathbb{Z}[i]^*$. Thus, $\gamma_c(\Lambda/\Lambda')$ provides a first-order estimate of the performance improvement of an LNC scheme over a baseline

LNC scheme. For this reason, $\gamma_c(\Lambda/\Lambda')$ will be used as a figure of merit of LNC schemes in the rest of this paper; yet the effect of $K(\Lambda/\Lambda')$ cannot be ignored in a more detailed assessment of LNC schemes.

## VII. Design of Nested Lattices

In this section, we adapt several known lattice constructions to produce pairs of nested lattices with simple message space and high coding gain.

### A. Constructions of Nested Lattices

Known methods for designing lattices include Construction A and Construction D as well as their complex versions (see, e.g., [34]). Here, we adapt these methods to construct pairs of nested lattices. In all of our examples, the Voronoi region of the coarse lattice is chosen as its fundamental region.

*1) Nested Lattices via Construction A:* Let $p > 0$ be a prime number in $\mathbb{Z}$. Let $\mathcal{C}$ be a linear code of length $n$ over $\mathbb{Z}/\langle p \rangle$. Without loss of generality, we may assume the linear code $\mathcal{C}$ is systematic. Define a "real Construction A lattice" [34] as

$$\Lambda_r \triangleq \{\boldsymbol{\lambda} \in \mathbb{Z}^n : \sigma(\boldsymbol{\lambda}) \in \mathcal{C}\},$$

where $\sigma : \mathbb{Z}^n \to (\mathbb{Z}/\langle p \rangle)^n$ is the natural projection map. (Here, the subscript $r$ stands for "real.") Define

$$\Lambda'_r \triangleq \{p\mathbf{r} : \mathbf{r} \in \mathbb{Z}^n\}.$$

It is easy to see that $\Lambda'_r$ is a sublattice of $\Lambda_r$. Hence, we obtain a pair of nested $\mathbb{Z}$-lattices $\Lambda_r \supseteq \Lambda'_r$ from the linear code $\mathcal{C}$.

Now we "lift" this pair of nested $\mathbb{Z}$-lattices to a pair of nested $\mathbb{Z}[i]$-lattices. Let $\Lambda = \Lambda_r + i\Lambda_r$, i.e.,

$$\Lambda = \{\boldsymbol{\lambda} \in \mathbb{Z}[i]^n : \mathrm{Re}\{\boldsymbol{\lambda}\}, \mathrm{Im}\{\boldsymbol{\lambda}\} \in \Lambda_r\}.$$

Similarly, let $\Lambda' = \Lambda'_r + i\Lambda'_r$. In this way, we obtain a pair of nested $\mathbb{Z}[i]$-lattices $\Lambda \supseteq \Lambda'$. A variant of this construction was used by Nazer and Gastpar in [1].

To study the message space induced by $\Lambda/\Lambda'$, we specify two generator matrices satisfying the relation (8). On the one hand, we note that the lattice $\Lambda_r$ has a generator matrix $\mathbf{G}_{\Lambda_r}$ given by

$$\mathbf{G}_{\Lambda_r} = \begin{bmatrix} \mathbf{I}_k & \mathbf{B}_{k\times(n-k)} \\ \mathbf{0}_{(n-k)\times k} & p\mathbf{I}_{n-k} \end{bmatrix},$$

where $\sigma([\mathbf{I}\ \mathbf{B}])$ is a generator matrix for $\mathcal{C}$. The lifted lattice $\Lambda$ has a generator matrix $\mathbf{G}_\Lambda$ that is identical to $\mathbf{G}_{\Lambda_r}$, but over $\mathbb{Z}[i]$. On the other hand, we note that the lattice $\Lambda'$ has a generator matrix $\mathbf{G}_{\Lambda'}$ given by

$$\mathbf{G}_{\Lambda'} = \begin{bmatrix} p\mathbf{I}_k & p\mathbf{B}_{k\times(n-k)} \\ \mathbf{0}_{(n-k)\times k} & p\mathbf{I}_{n-k} \end{bmatrix}.$$

These two generator matrices $\mathbf{G}_\Lambda$ and $\mathbf{G}_{\Lambda'}$ satisfy

$$\mathbf{G}_{\Lambda'} = \begin{bmatrix} p\mathbf{I}_k & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-k} \end{bmatrix} \mathbf{G}_\Lambda.$$

It follows from Theorem 6 that $\Lambda/\Lambda' \cong (\mathbb{Z}[i]/\langle p\rangle)^k$. That is, the message space under this construction is $W = (\mathbb{Z}[i]/\langle p\rangle)^k$. In particular, the message rate $\mathsf{R}_{\mathsf{mes}} = \frac{k}{n}\log_2(p^2)$, since $\mathbb{Z}[i]/\langle p\rangle$ contains $p^2$ elements.

Note that the message space $W$ can be viewed as a free $\mathbb{Z}[i]/\langle p\rangle$-module of rank $k$. In particular, $W$ is a vector space if and only if the prime number $p$ is a Gaussian prime, which is equivalent to saying that $p$ is of the form $4j+3$.

To study the nominal coding gain $\gamma_c(\Lambda/\Lambda')$ as well as $K(\Lambda/\Lambda')$, we relate them to certain parameters of the linear code $\mathcal{C}$. To each codeword $\mathbf{c} = (c_1 + \langle p\rangle, \ldots, c_n + \langle p\rangle) \in \mathcal{C}$, there corresponds a coset $(c_1, \ldots, c_n) + p\mathbb{Z}^n$ whose minimum-norm coset leader, denoted by $\sigma^*(\mathbf{c})$, is given by

$$\sigma^*(\mathbf{c}) = (c_1 - \lfloor c_1/p \rceil \times p, \ldots, c_n - \lfloor c_n/p \rceil \times p),$$

where $\lfloor x \rceil$ is a rounding operation. The Euclidean weight $w_E(\mathbf{c})$ of $\mathbf{c}$ can then be defined as the squared Euclidean norm of $\sigma^*(\mathbf{c})$, that is, $w_E(\mathbf{c}) = \|\sigma^*(\mathbf{c})\|^2$. Thus, for example, when $\mathbf{c} = (1+\langle 5\rangle, 3+\langle 5\rangle)$, $\sigma^*(\mathbf{c}) = (1,-2)$. Clearly, the Euclidean weight of $\mathbf{c}$ is equivalent to the 2-norm of $\mathbf{c}$ defined in [43]. Let $w_E^{\min}(\mathcal{C})$ be the minimum Euclidean weight of nonzero codewords in $\mathcal{C}$, i.e.,

$$w_E^{\min}(\mathcal{C}) = \min\{w_E(\mathbf{c}) : \mathbf{c} \neq \mathbf{0},\ \mathbf{c} \in \mathcal{C}\}.$$

Let $A(w_E^{\min})$ be the number of codewords in $\mathcal{C}$ with minimum Euclidean weight $w_E^{\min}(\mathcal{C})$. Then we have the following result.

*Proposition 2:* Let $\mathcal{C}$ be a linear code over $\mathbb{Z}/\langle p\rangle$ and let $\Lambda \supseteq \Lambda'$ be a pair of nested lattices constructed from $\mathcal{C}$. Then

$$\gamma_c(\Lambda/\Lambda') = \frac{w_E^{\min}(\mathcal{C})}{p^{2(1-k/n)}}$$

and

$$K(\Lambda/\Lambda') = \begin{cases} 2A\left(w_E^{\min}(\mathcal{C})\right) 2^{w_E^{\min}(\mathcal{C})}, & \text{when } p = 2, \\ 2A\left(w_E^{\min}(\mathcal{C})\right), & \text{when } p > 2. \end{cases}$$

The proof is in Appendix B.

Proposition 2 suggests that optimizing the nominal coding gain $\gamma_c(\Lambda/\Lambda')$ amounts to maximizing the minimum Euclidean weight $w_E^{\min}(\mathcal{C})$ of $\mathcal{C}$, and that optimizing $K(\Lambda/\Lambda')$ amounts to minimizing $A(w_E^{\min})$.

*2) Nested Lattices via Complex Construction A:* Let $\pi$ be a prime in $T$. Let $\mathcal{C}$ be a linear code of length $n$ over $T/\langle \pi\rangle$. Without loss of generality, we may assume the linear code $\mathcal{C}$ is systematic. Define a "complex Construction A lattice" [34] as

$$\Lambda \triangleq \{\boldsymbol{\lambda} \in T^n : \sigma(\boldsymbol{\lambda}) \in \mathcal{C}\},$$

where $\sigma : T^n \to (T/\langle \pi\rangle)^n$ is the natural projection map. Define

$$\Lambda' \triangleq \{\pi\mathbf{r} : \mathbf{r} \in T^n\}.$$

It is easy to see $\Lambda'$ is a sublattice of $\Lambda$. Hence, we obtain a pair of nested lattices $\Lambda \supseteq \Lambda'$ from the linear code $\mathcal{C}$.

To study the message space induced by $\Lambda/\Lambda'$, we specify two generator matrices satisfying the relation (8). It is well-known that $\Lambda$ has a generator matrix $\mathbf{G}_\Lambda$ given by

$$\mathbf{G}_\Lambda = \begin{bmatrix} \mathbf{I}_k & \mathbf{B}_{k\times(n-k)} \\ \mathbf{0}_{(n-k)\times k} & \pi\mathbf{I}_{n-k} \end{bmatrix},$$

and that $\Lambda'$ has a generator matrix $\mathbf{G}_{\Lambda'}$ given by

$$\mathbf{G}_{\Lambda'} = \begin{bmatrix} \pi\mathbf{I}_k & \pi\mathbf{B}_{k\times(n-k)} \\ \mathbf{0}_{(n-k)\times k} & \pi\mathbf{I}_{n-k} \end{bmatrix}.$$

These two generator matrices satisfy

$$\mathbf{G}_{\Lambda'} = \begin{bmatrix} \pi\mathbf{I}_k & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-k} \end{bmatrix} \mathbf{G}_\Lambda.$$

Hence, we have $\Lambda/\Lambda' \cong (T/\langle\pi\rangle)^k$. That is, the message space under this construction is $W = (T/\langle\pi\rangle)^k$. Since $\pi$ is a prime in $T$, $T/\langle\pi\rangle$ is a finite field and $W$ is a vector space of dimension $k$. Thus, this construction is preferable to the previous construction, if the message space is required to be a vector space. For instance, if $T = \mathbb{Z}[\omega]$ and $\pi = 2$, then the message space $W$ is a vector space over $\mathbb{F}_4$. This never happens under the previous construction, since $2$ is not a prime in $\mathbb{Z}[i]$.

To study the nominal coding gain $\gamma_c(\Lambda/\Lambda')$ as well as $K(\Lambda/\Lambda')$, we again relate them to the parameters of the linear code $\mathcal{C}$ with a particular focus on $T = \mathbb{Z}[i]$ (due to hypercube shaping). The definition of the minimum Euclidean weight $w_E^{\min}(\mathcal{C})$ is the same as the previous definition, except for the fact that the minimum-norm coset leader $\sigma^*(\mathbf{c})$ is given by

$$\sigma^*(\mathbf{c}) = (c_1 - \lfloor c_1/\pi \rceil \times \pi, \ldots, c_n - \lfloor c_n/\pi \rceil \times \pi),$$

where the rounding operation $\lfloor x \rceil$ sends $x \in \mathbb{C}$ to the closest Gaussian integer in the Euclidean distance.

*Proposition 3:* Let $\mathcal{C}$ be a linear code over $\mathbb{Z}[i]/\langle\pi\rangle$ and let $\Lambda \supseteq \Lambda'$ be a pair of nested lattices constructed from $\mathcal{C}$. Then

$$\gamma_c(\Lambda/\Lambda') = \frac{w_E^{\min}(\mathcal{C})}{|\pi|^{2(1-k/n)}}$$

and

$$K(\Lambda/\Lambda') = \begin{cases} A\left(w_E^{\min}(\mathcal{C})\right) 4^{w_E^{\min}(\mathcal{C})}, & \text{when } |\pi|^2 = 2, \\ A\left(w_E^{\min}(\mathcal{C})\right), & \text{otherwise.} \end{cases}$$

The proof is in Appendix C.

*3) Nested Lattices via Construction D:* Let $p > 0$ be a prime in $\mathbb{Z}$. Let $\mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_s$ be nested linear codes of length $n$ over $\mathbb{Z}/\langle p\rangle$, where $\mathcal{C}_i$ has parameters $[n, k_i]$ for $i = 1, \ldots, s$. As shown in [34], there exists a basis $\{\mathbf{g}_1, \ldots, \mathbf{g}_n\}$ for the vector space $(\mathbb{Z}/\langle p\rangle)^n$ such that

1) $\mathbf{g}_1, \ldots, \mathbf{g}_{k_i}$ span $\mathcal{C}_i$ for $i = 1, \ldots, s$; and
2) if $\mathbf{G}$ denotes the matrix with rows $\mathbf{g}_1, \ldots, \mathbf{g}_n$, some permutation of the rows of $\mathbf{G}$ gives an upper triangular matrix with diagonal elements equal to $1 + \langle p\rangle$.

(In fact, $\mathbf{G}$ can be constructed by applying Gaussian elimination to the generator matrices of the nested linear codes iteratively.)

Using the nested linear codes $\{\mathcal{C}_i, 1 \le i \le s\}$, we define a "real Construction D lattice" [34] as

$$\Lambda_r \triangleq \left\{ \sum_{i=1}^{s} \sum_{j=1}^{k_i} p^{i-1} \beta_{ij} \tilde{\sigma}(\mathbf{g}_j) : \beta_{ij} \in \{0, \ldots, p-1\} \right\} + p^s \mathbb{Z}^n \tag{12}$$

where $\tilde{\sigma}$ is the natural embedding map from $(\mathbb{Z}/\langle p \rangle)^n$ to $\{0, \ldots, p-1\}^n$. (For completeness, we will show in Appendix D that $\Lambda_r$ is indeed a lattice; we will also give an explicit generator matrix for $\Lambda_r$.)

Note that the lattice defined by $\Lambda_r' \triangleq \{p^s \mathbf{r} : \mathbf{r} \in \mathbb{Z}^n\}$ is a sublattice of $\Lambda_r$. Hence, we obtain a pair of nested $\mathbb{Z}$-lattices $\Lambda_r \supseteq \Lambda_r'$ from the nested linear codes $\{\mathcal{C}_i, 1 \le i \le s\}$.

Next, we lift this pair of nested $\mathbb{Z}$-lattices to a pair of nested $\mathbb{Z}[i]$-lattices. That is, we set $\Lambda = \Lambda_r + i\Lambda_r$ and $\Lambda' = \Lambda_r' + i\Lambda_r'$. In this way, we obtain a pair of nested $\mathbb{Z}[i]$-lattices $\Lambda \supseteq \Lambda'$. In Appendix E, we will show that there exist two generator matrices $\mathbf{G}_\Lambda$ and $\mathbf{G}_{\Lambda'}$ satisfying

$$\mathbf{G}_{\Lambda'} = \mathrm{diag}(\underbrace{p^s, \ldots, p^s}_{k_1}, \underbrace{p^{s-1}, \ldots, p^{s-1}}_{k_2 - k_1}, \ldots, \underbrace{1, \ldots, 1}_{n - k_s}) \mathbf{G}_\Lambda. \tag{13}$$

It follows from Theorem 6 that

$$\Lambda/\Lambda' \cong (\mathbb{Z}[i]/\langle p^s \rangle)^{k_1} \times \cdots \times (\mathbb{Z}[i]/\langle p \rangle)^{k_s - k_{s-1}}.$$

In particular, the message rate $\mathsf{R}_{\mathsf{mes}} = \frac{\sum_i k_i}{n} \log_2(p^2)$. When $s = 1$, this construction is reduced to the first construction. Although this construction induces a more complicated message space, it is able to produce pairs of nested lattices with higher nominal coding gains, as shown in the following result.

*Proposition 4:* Let $\mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_s$ be nested linear codes of length $n$ over $\mathbb{Z}/\langle p \rangle$ and let $\Lambda \supseteq \Lambda'$ be a pair of nested lattices constructed from $\{\mathcal{C}_i\}$. Then $\gamma_c(\Lambda/\Lambda')$ is lower bounded by

$$\gamma_c(\Lambda/\Lambda') \ge \frac{\min_{1 \le i \le s} \{ p^{2(i-1)} w_E^{\min}(\mathcal{C}_i) \}}{p^{2(s - \sum_{i=1}^{a} k_i / n)}},$$

and $K(\Lambda/\Lambda')$ is upper bounded by

$$K(\Lambda/\Lambda') \le \begin{cases} 2 \sum_{i=1}^{s} 2^{A_i} A_i, & \text{when } p = 2 \\ 2 \sum_{i=1}^{s} A_i, & \text{when } p > 2 \end{cases}$$

where $A_i$ is the number of codewords in $\mathcal{C}_i$ with minimum Euclidean weight $w_E^{\min}(\mathcal{C}_i)$.
The proof is given in Appendix F.

Now we will apply Propositions 2 and 4 to show the advantage of pairs of nested lattices constructed via Construction D. Let $\Lambda_{\mathrm{A}} \supseteq \Lambda_{\mathrm{A}}'$ be a pair of nested lattices constructed from a linear $[n, k]$ code $\mathcal{C}$ (over $\mathbb{Z}/\langle p \rangle$) via Construction A. Then by Proposition 2, $\gamma_c(\Lambda_{\mathrm{A}}/\Lambda_{\mathrm{A}}') = w_E^{\min}(\mathcal{C})/p^{2(1-k/n)}$. Suppose that the linear code $\mathcal{C}$ has an

TABLE I

POLYNOMIAL CONVOLUTIONAL ENCODERS THAT ASYMPTOTICALLY ACHIEVE THE UPPER BOUND.

| $\nu$ | $\mathbf{g}(D)$ | $\gamma_c(\Lambda/\Lambda')$ |
|---|---|---|
| 1 | $[1+(1+i)D,\ (1+i)+D]$ | 2 (3 dB) |
| 2 | $[1+D+(1+i)D^2,\ (1+i)+(1-i)D+D^2]$ | 3 (4.77 dB) |

$[n,k']$ subcode $\mathcal{C}'$ with $w_E^{\min}(\mathcal{C}') \geq p^2 w_E^{\min}(\mathcal{C})$. Let $\Lambda_{\mathrm{D}} \supseteq \Lambda'_{\mathrm{D}}$ be a pair of nested lattices constructed from $\mathcal{C}$ and $\mathcal{C}'$ via Construction D. Then by Proposition 4,

$$\begin{aligned}\gamma_c(\Lambda_{\mathrm{D}}/\Lambda'_{\mathrm{D}}) &\geq \frac{p^2 w_E^{\min}(\mathcal{C})}{p^{2(2-(k+k')/n)}} \\ &= \frac{w_E^{\min}(\mathcal{C})}{p^{2(1-(k+k')/n)}} \\ &> \gamma_c(\Lambda_{\mathrm{A}}/\Lambda'_{\mathrm{A}}).\end{aligned}$$

In other words, given a pair of nested lattices via Construction A, there exists a pair of nested lattices via Construction D with higher nominal coding gain if the linear code $\mathcal{C}$ has a subcode $\mathcal{C}'$ with $w_E^{\min}(\mathcal{C}') \geq p^2 w_E^{\min}(\mathcal{C})$.

### B. Design Examples

We present three design examples to illustrate the design tools developed in Sec. VII-A. All of our design examples feature short packet length and reasonable decoding complexity, since the purpose of this paper is to demonstrate the potential of LNC schemes in practical settings. (A more elaborate scheme, based on signal codes [44], is described in [22].)

*Example 7:* Consider a rate-$1/2$ terminated (feed-forward) convolutional code over $\mathbb{Z}[i]/\langle 3\rangle$ with $\nu$ memory elements. Suppose the input sequence $u(D)$ is a polynomial of degree less than $\mu$. Then this terminated convolutional code can be regarded as a $[2(\mu+\nu),\mu]$ linear block code $\mathcal{C}$. Using the method based on complex Construction A, we obtain a pair of nested lattices $\Lambda \supseteq \Lambda'$.

Note that the minimum Euclidean weight $w_E^{\min}(\mathcal{C})$ of $\mathcal{C}$ can be bounded as

$$w_E^{\min}(\mathcal{C}) \leq 3(1+\nu),$$

for all rate-$1/2$ terminated (feed-forward) convolutional codes over $\mathbb{Z}[i]/\langle 3\rangle$. This upper bound can be verified by considering the input sequence $u(D)=1$. Hence, the nominal coding gain $\gamma_c(\Lambda/\Lambda')$ satisfies

$$\gamma_c(\Lambda/\Lambda') \leq 1+\nu.$$

When $\nu = 1, 2$ and $\mu \gg \nu$, this upper bound can be asymptotically achieved by polynomial convolutional encoders shown in Table I.

Note that when $\nu = 1$ or $2$, the encoder state space size is $9$ or $81$. Note also that the lattice decoder $\mathcal{D}_\Lambda$ can be implemented through a modified Viterbi decoder as discussed in Appendix G. Thus, this example demonstrates that a nominal coding gain of $3$ to $5$ dB can be easily obtained with reasonable decoding complexity. ■

Our next example illustrates how to use our design tools to improve an existing construction presented in [45].

*Example 8:* Consider nested linear codes $\mathcal{C}_1 \subseteq \mathcal{C}_2$ of length $n$ over $\mathbb{Z}/\langle 2 \rangle$, where $\mathcal{C}_1$ is an $[n, k_1, d_1]$ code with $d_1 \geq 4$ and $\mathcal{C}_2$ is the $[n, n]$ trivial code. Using the method based on Construction D, we obtain a pair of nested lattices $\Lambda \supseteq \Lambda'$.

In this case, we will show that the nominal coding gain $\gamma_c(\Lambda/\Lambda') = 4/4^{(1-k_1/n)}$. On the one hand, by Proposition 4,

$$\gamma_c(\Lambda/\Lambda') \geq \frac{\min\{w_H^{\min}(\mathcal{C}_1), 4w_H^{\min}(\mathcal{C}_2)\}}{4^{(2-\sum_{i=1}^2 k_i/n)}} = 4/4^{(1-k_1/n)}.$$

On the other hand, by definition,

$$\begin{aligned}\gamma_c(\Lambda/\Lambda') &= d^2(\Lambda/\Lambda')/V(\Lambda')^{1/n} \\ &= d^2(\Lambda/\Lambda')/4^{(2-\sum_{i=1}^2 k_i/n)} \quad (14) \\ &\leq 4/4^{(1-k_1/n)} \quad (15)\end{aligned}$$

where (14) follows from the facts that $V(\Lambda') = V(\Lambda)4^{k_1+k_2}$ and $V(\Lambda') = 4^{2n}$; (15) follows from the fact that $(2, 0, \ldots, 0)$ is a lattice point in $\Lambda$ but not in $\Lambda'$.

Finally, in Table II we list several candidates for $\mathcal{C}_1$ as well as their corresponding nominal coding gains. These candidates are all extended Hamming codes with $d_1 = 4$. ■

We note that Ordentlich-Erez's construction in [45] can be regarded as a special case of Example 8. In their construction, $\mathcal{C}_1$ is chosen as a rate $5/6$ cyclic LDPC code of length $64800$. Example 8 suggests that their nominal coding gain is $4/4^{1/6}$ ($5.02$ dB) with message rate $2(1+5/6) \approx 3.67$. Example 8 also suggests that there are many ways to improve the nominal coding gain. For example, when $\mathcal{C}_1$ is chosen as a $[256, 247]$ extended Hamming code, the nominal coding gain is $5.81$ dB with message rate $2(1 + \frac{247}{256}) \approx 3.93$.

Our third example illustrates how to design high-coding-gain nested lattices based on turbo lattices [46].

*Example 9:* Consider nested Turbo codes $\mathcal{C}_1 \subseteq \mathcal{C}_2$ over $\mathbb{Z}/\langle 2 \rangle$. As shown in [46], $\mathcal{C}_1$ can be a rate-$1/3$ Turbo code with $d_1 = 28$ and $\mathcal{C}_2$ can be a rate-$1/2$ Turbo code with $d_2 = 13$. Using the method via Construction D, we obtain a pair of nested lattices $\Lambda \supseteq \Lambda'$. In this case, by Proposition 4,

$$\gamma_c(\Lambda/\Lambda') \geq \frac{\min\{d_1, 4d_2\}}{4^{(2-\sum_{i=1}^2 k_i/n)}} = 28/4^{(2-1/2-1/3)} = 7.45 \text{ dB}.$$

The message rate is given by $\mathsf{R}_{\mathsf{mes}} = 5/3 \approx 1.67$.

Finally, some other design examples of high-performance nested lattice codes, which are of a similar spirit, can be found, e.g., in [21], [22], [28], [29], [47], Also, similar methods of designing practical compute-and-forward have been recently proposed. See, e.g., [23], [48], [49].

## VIII. Decoding Multiple Linear Combinations

In this section, we consider the problem when a receiver has the freedom to choose coefficient vectors. For ease of presentation, we mainly focus on the case of complex Construction A in which the message space is a vector space over $T/\langle \pi \rangle$. The main result of this section is that, under separate decoding, the problem of decoding multiple

TABLE II

SEVERAL EXTENDED HAMMING CODES AND CORRESPONDING NOMINAL CODING GAINS.

| $n$ | $k$ | $\gamma_c(\Lambda/\Lambda')$ |
|---|---|---|
| 32 | 26 | 3.08 (4.89 dB) |
| 64 | 57 | 3.44 (5.36 dB) |
| 128 | 120 | 3.67 (5.64 dB) |
| 256 | 247 | 3.81 (5.81 dB) |

linear combinations is related to the *shortest independent vectors problem* [3], and can be solved through some existing methods.

In general, upon deciding the coefficient vectors $\mathbf{a}_1, \ldots, \mathbf{a}_m$, the receiver can perform joint decoding or separate decoding to recover the linear combinations $\mathbf{u}_i = \mathbf{a}_i \mathbf{W}$. Here, we confine our attention to separate decoding in which each linear combination $\mathbf{u}_i = \mathbf{a}_i \mathbf{W}$ is decoded independently through the use of $\mathcal{D}(\mathbf{y} \mid \mathbf{h}, \mathbf{a}_i)$. In this case, the union bound estimate on the decoding error for each $\mathbf{a}_i$ is

$$P_e(\mathbf{h}, \mathbf{a}_i) \lessapprox K(\Lambda/\Lambda') \exp\left(-\frac{d^2(\Lambda/\Lambda')}{4N_0 \mathbf{a}_i \mathbf{M} \mathbf{a}_i^{\mathsf{H}}}\right).$$

To optimize the above union bound estimates, the coefficient vectors $\mathbf{a}_1, \ldots, \mathbf{a}_m$ should be chosen such that each $\mathbf{a}_i \mathbf{M} \mathbf{a}_i^{\mathsf{H}}$ is made as small as possible under the constraint that $\bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_m$ are *linearly independent* over $T/\langle \pi \rangle$, where $\bar{\mathbf{a}}_i = \sigma(\mathbf{a}_i)$ is the natural projection of $\mathbf{a}_i$ (from $T$ to $T/\langle \pi \rangle$). Clearly, this constraint ensures that every recovered linear combination $\mathbf{u}_i$ is useful over $T/\langle \pi \rangle$.

We say a solution $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ is *feasible* if $\bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_m$ are linearly independent over $T/\langle \pi \rangle$. Since each $\bar{\mathbf{a}}_i$ is of dimension $L$, we assume that $m \leq L$ because otherwise no feasible solution exists.

In the sequel, we will show that there exists a feasible solution that *simultaneously* optimizes each $\mathbf{a}_i \mathbf{M} \mathbf{a}_i^{\mathsf{H}}$. We call such feasible solutions *dominant solutions*. Formally, let $\mathbf{M} = \mathbf{L}\mathbf{L}^{\mathsf{H}}$ be the Cholesky decomposition of $\mathbf{M}$, where $\mathbf{L}$ is some lower triangular matrix. (The existence of $\mathbf{L}$ comes from the fact that $\mathbf{M}$ is Hermitian and positive-definite.) Clearly, $\mathbf{a}\mathbf{M}\mathbf{a}^{\mathsf{H}} = \|\mathbf{a}\mathbf{L}\|^2$.

*Definition 3 (Dominant Solutions):* A feasible solution $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ (with $\|\mathbf{a}_1\mathbf{L}\| \leq \ldots \leq \|\mathbf{a}_m\mathbf{L}\|$) is called a *dominant solution* if for any feasible solution $\mathbf{a}'_1, \ldots, \mathbf{a}'_m$ (with $\|\mathbf{a}'_1\mathbf{L}\| \leq \ldots \leq \|\mathbf{a}'_m\mathbf{L}\|$), the following inequalities hold

$$\|\mathbf{a}_i\mathbf{L}\| \leq \|\mathbf{a}'_i\mathbf{L}\|, \ i = 1, \ldots, m.$$

Although the dominant solutions seem to be a natural concept, the existence of them is not immediate from the definition, and a separate argument is needed.

*Theorem 8:* A feasible solution $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ defined by

$$\begin{aligned}
\mathbf{a}_1 &= \arg\min \{\|\mathbf{a}\mathbf{L}\| \mid \bar{\mathbf{a}} \text{ is nonzero}\} \\
\mathbf{a}_2 &= \arg\min \{\|\mathbf{a}\mathbf{L}\| \mid \bar{\mathbf{a}}, \bar{\mathbf{a}}_1 \text{ are linearly independent}\} \\
&\vdots \\
\mathbf{a}_m &= \arg\min \{\|\mathbf{a}\mathbf{L}\| \mid \bar{\mathbf{a}}, \bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_{m-1} \text{ are linearly ind.}\}
\end{aligned}$$

always exists, and is a dominant solution.

The proof is given in Appendix H.

We now propose a three-step method of finding a dominant solution. In the first step, we construct a ball $\mathcal{B}(\rho) = \{\mathbf{x} \in \mathbb{C}^L \mid \|\mathbf{x}\| \leq \rho\}$ that contains $m$ lattice points $\mathbf{v}_1\mathbf{L}, \ldots, \mathbf{v}_m\mathbf{L}$ such that $\bar{\mathbf{v}}_1, \ldots, \bar{\mathbf{v}}_m$ are linearly independent, where $\bar{\mathbf{v}}_i = \sigma(\mathbf{v}_i)$ is the natural projection of $\mathbf{v}_i$. In the second step, we order all lattice points within $\mathcal{B}(\rho)$ based on their lengths, producing an ordered set $\mathcal{S}_\rho$ with $\|\mathbf{v}_1\mathbf{L}\| \leq \|\mathbf{v}_2\mathbf{L}\| \leq \cdots \leq \|\mathbf{v}_{|\mathcal{S}_\rho|}\mathbf{L}\|$. Finally, we find a dominant solution $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ by using a greedy search algorithm given as Algorithm 1.

**Algorithm 1** *Greedy Search for Dominant Solution*

*Input:* An ordered set $\mathcal{S}_\rho = \{\mathbf{v}_1\mathbf{L}, \mathbf{v}_2\mathbf{L}, \ldots, \mathbf{v}_{|\mathcal{S}_\rho|}\mathbf{L}\}$ with $\|\mathbf{v}_1\mathbf{L}\| \leq \|\mathbf{v}_2\mathbf{L}\| \leq \cdots \leq \|\mathbf{v}_{|\mathcal{S}_\rho|}\mathbf{L}\|$.

*Output:* An optimal solution $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$.

1. Set $\mathbf{a}_1 = \mathbf{v}_1$. Set $i = 1$ and $j = 1$.
2. **while** $i < |\mathcal{S}_b|$ and $j < m$ **do**
3. Set $i = i + 1$.
4. **if** $\bar{\mathbf{v}}_i, \bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_j$ are linearly independent **then**
5. Set $j = j + 1$. Set $\mathbf{a}_j = \mathbf{v}_i$.
6. **end if**
7. **end while**

The correctness of our proposed method follows immediately from Theorem 8. Our proposed method is in the spirit of sphere-decoding algorithms, since sphere-decoding algorithms also enumerate all lattice points within a ball centered at a given vector. The selection of the radius $\rho$ plays an important role here, just as it does for sphere-decoding algorithms. If $\rho$ is too large, then the second step may incur excessive computations. If $\rho$ is too small, then the first step may fail to construct a ball that contains $m$ linearly independent $\bar{\mathbf{v}}_1, \ldots, \bar{\mathbf{v}}_m$.

In practice, lattice-reduction algorithms [50] may be used to determine an appropriate radius $\rho$, as shown in the following proposition.

*Proposition 5:* Let $\{\mathbf{b}_1, \ldots, \mathbf{b}_L\}$ be a *reduced basis* [50] for $\mathbf{L}$. If $\rho$ is set to be $\|\mathbf{b}_m\|$, then the set $\mathcal{S}_\rho$ contains at least $m$ lattice points $\mathbf{v}_1\mathbf{L}, \ldots, \mathbf{v}_m\mathbf{L}$ such that $\bar{\mathbf{v}}_1, \ldots, \bar{\mathbf{v}}_m$ are linearly independent.

*Proof:* Let $\mathbf{v}_i = \mathbf{b}_i\mathbf{L}^{-1}$ for $i = 1, \ldots, L$. Let $\mathbf{V}$ be an $L \times L$ matrix with $\mathbf{v}_i$ as its $i$th row. Since $\{\mathbf{b}_1, \ldots, \mathbf{b}_L\}$ is a reduced basis, it follows that the matrix $\mathbf{V}$ is invertible. In particular, $\bar{\mathbf{v}}_1, \ldots, \bar{\mathbf{v}}_m$ are linearly independent for

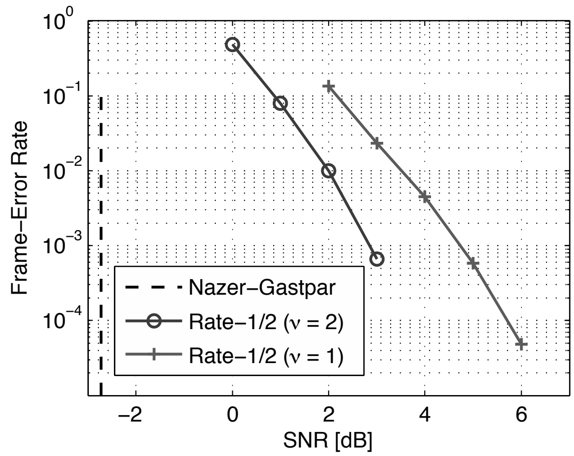



Fig. 7. Error performance of three LNC schemes in Scenario 1.

all integers $m \leq L$. ∎

There are many existing lattice-reduction algorithms in the literature. Among them, the Lenstra-Lenstra-Lovász (LLL) algorithm [51] is of particular importance. Moreover, the LLL algorithm has been extended from real lattices to complex lattices over Euclidean domains [52], [53]. Since $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are special cases of Euclidean domains, the extended LLL algorithm can be used to handle the cases of $T = \mathbb{Z}[i]$ and $T = \mathbb{Z}[\omega]$.

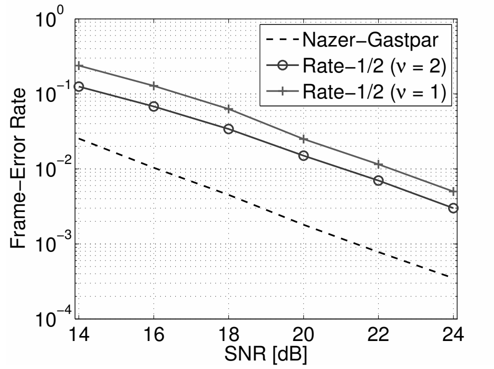
Interestingly, when $L$ is small, some efficient lattice-reduction algorithms can directly output dominant solutions. Such algorithms, which are generalizations of Gauss' algorithm (see, e.g., [54]), are described in [55], [56].

## IX. Simulation Results

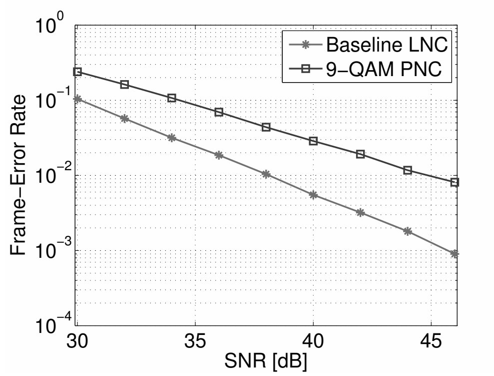
As described in Section I, there are many potential application scenarios for LNC, the most promising of which may involve multicasting from one (or more) sources to multiple destinations via a wireless relay network. Since we wish to avoid introducing higher-layer issues (e.g., scheduling), in this paper, we focus here on a two-transmitter, single receiver multiple-access configuration, which may be regarded as a building block component of a more complicated and realistic network application. In particular, we focus on the following three scenarios:

1) The channel gains are fixed; the receiver chooses a single linear function.
2) The channel gains are Rayleigh faded; the receiver chooses a single linear function.
3) The channel gains are Rayleigh faded; the receiver chooses two linear functions.

In each scenario, we evaluate the performance of four LNC schemes: the Nazer-Gastpar scheme, two LNC schemes proposed in Example 7, and the baseline LNC scheme over $\mathbb{Z}[i]/\langle 3 \rangle$ as defined in Sec. VII. Since we are interested in LNC schemes with short packet lengths, each transmitted signal consists of $200$ complex symbols in our simulations.




(a)




(b)

Fig. 8. Error performance of various LNC schemes in Scenario 2.

### *A. Scenario 1 (Fixed Channel Gains; Single Coefficient Vector)*

Fig. 7 depicts the frame-error rates of three LNC schemes as a function of $\mathsf{SNR}$. Here, the channel-gain vector $\mathbf{h}$ is set to $\mathbf{h} = [-1.17 + 2.15i \;\, 1.25 - 1.63i]$. Nevertheless, as we have shown in Sec. VII, the results are not particularly sensitive to the choice for $\mathbf{h}$; similar results are achieved for other fixed choices for $\mathbf{h}$. For the two LNC schemes proposed in Example 7, the parameter $\mu + \nu$ is set to $100$ and the corresponding message rates are $\frac{99}{100}\log_2(3)$ ($\nu = 1$) and $\frac{98}{100}\log_2(3)$ ($\nu = 2$), respectively. For the Nazer-Gastpar scheme, the message rate is set to $\log_2(3)$, which is quite close to the previous two message rates. The decoding rule for the Nazer-Gastpar scheme is as follows: a frame error occurs if and only if $\log_2(3) \geq \log_2(\mathsf{SNR} / \mathbf{a}\mathbf{M}\mathbf{a}^{\mathsf{H}})$, where $\mathbf{a}$ is the single coefficient vector. From Fig. 7, we observe that the gap to the Nazer-Gastpar scheme is around $5$ dB at an error-rate of $1\%$. We also observe that the second LNC scheme (with state space of size $81$) outperforms the first LNC scheme (with state space of size $9$) by about $2$ dB.

### *B. Scenario 2 (Rayleigh-faded Channel Gains; Single Coefficient Vector)*

Fig. 8(a) shows the frame-error rates of three LNC schemes as a function of $\mathsf{SNR}$. The setup is the same as in Scenario 1, except that the coefficient vector $\mathbf{a}$ changes with $\mathbf{h}$. As seen in Fig. 8(a), the gap to the Nazer-Gastpar

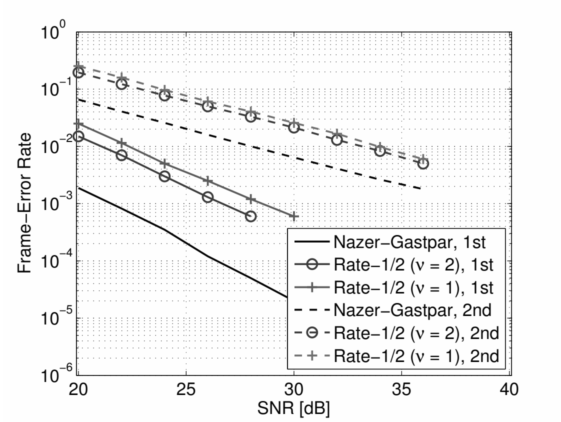



Fig. 9. Error performance of three LNC schemes in Scenario 3.

scheme is around $5$ dB at an error-rate of $1\%$.

Fig. 8(b) shows the frame-error rates of the baseline LNC scheme (over $\mathbb{Z}[i]^{200}/3\mathbb{Z}[i]^{200}$) and the $9$-QAM PNC scheme described in Example 2. For the $9$-QAM scheme, the coefficient vector $\mathbf{a}$ is set to $[1\ 1]$ as explained in Example 2. To make a fair comparison, the coefficient vector $\mathbf{a}$ in the baseline LNC scheme satisfies $a_1 \neq 0, a_2 \neq 0$, which comes from the "exclusive law of network coding" as discussed in [7], [8]. As seen in Fig. 8(b), the baseline LNC scheme outperforms the $9$-QAM scheme by more than $6$ dB at an error-rate of $1\%$. In other words, even the baseline LNC scheme is able to effectively mitigate phase misalignment due to Rayleigh fading. Finally, note that Fig. 8(a) and Fig. 8(b) are separated because they have different message rates ($\log_2(3)$ in Fig. 8(a) and $2\log_2(3)$ in Fig. 8(b)).

### *C. Scenario 3 (Rayleigh-faded Channel Gains; Two Coefficient Vectors)*

Fig. 9 depicts the frame-error rates of three LNC schemes as a function of $\mathsf{SNR}$. Here the two coefficient vectors are chosen by using the lattice-reduction algorithm proposed in [55]. The configurations for the three LNC schemes are precisely the same as those in Fig. 8. The frame-error rates for the first linear combination are depicted in solid lines, while the error rates for the second linear combination are depicted in dashed lines. From Fig. 9, we observe similar trends of error rates as in Fig. 8. We also observe that the first linear combination is much more reliable than the second one.

## X. CONCLUSION

In this paper, the problem of constructing LNC schemes via finite-dimensional nested lattices has been studied. A generic LNC scheme has been defined based on an arbitrary pair of nested lattices. The message space of the generic scheme is a finite module in general, whose structure may be analyzed using the Smith normal form theorem. These results not only give rise to a convenient characterization of the message space of the Nazer-Gastpar scheme, but also lead to several generalized constructions of LNC schemes. All of these constructions are compatible with header-based random linear network coding.

An estimate of the error probability for hypercube-shaped LNC schemes has been derived, showing that the pair of nested lattices $\Lambda \supseteq \Lambda'$ should be designed such that $d(\Lambda/\Lambda')$ is maximized and $K(\Lambda/\Lambda')$ is minimized. These criteria lead to several specific methods for optimizing nested lattices. In particular, the nominal coding gain for pairs of nested lattices has been introduced, which serves as an important figure of merit for comparing various LNC schemes. In addition, several concrete examples of practical LNC schemes have been provided, showing that a nominal coding gain of $3$ to $7.5$ dB is easily obtained under reasonable decoding complexity and short packet length. Finally, the problem of choosing multiple coefficient vectors is discussed, which is connected to some well-studied lattice problems, such as the shortest independent vectors problem and the lattice reduction problem.

We believe that there is still much work to be done in this area. One direction for follow-up work would be the design and analysis of higher-layer scheduling algorithms for LNC schemes. Another direction would be the study of more general shaping methods beyond hypercube shaping. A particular example along this direction is given in [28]. A third direction would be the construction of more powerful LNC schemes, which has been partially explored in several recent papers, e.g., [21], [22], [29], [47]. We believe that the algebraic framework given in this paper can serve as a good basis for these developments.

## Appendix

### A. Proof of Theorem 7

We upper bound the error probability $\Pr[\mathcal{Q}_\Lambda^{\text{NN}}(\mathbf{n}) \notin \Lambda']$. Consider the (non-lattice) set $\{\Lambda \setminus \Lambda'\} \cup \{\mathbf{0}\}$, i.e., the set difference $\Lambda \setminus \Lambda'$ adjoined with the zero vector. Let $\mathcal{R}_V(\mathbf{0})$ be the Voronoi region of $\mathbf{0}$ in the set $\{\Lambda \setminus \Lambda'\} \cup \{\mathbf{0}\}$, i.e.,

$$\mathcal{R}_V(\mathbf{0}) = \left\{\mathbf{x} \in \mathbb{C}^n : \forall \boldsymbol{\lambda} \in \Lambda \setminus \Lambda' \left(\|\mathbf{x} - \mathbf{0}\| \leq \|\mathbf{x} - \boldsymbol{\lambda}\|\right)\right\}.$$

We have the following upper bound for $\Pr[\mathcal{Q}_\Lambda^{\text{NN}}(\mathbf{n}) \notin \Lambda']$.

*Lemma 1:* $\Pr[\mathcal{Q}_\Lambda^{\text{NN}}(\mathbf{n}) \notin \Lambda'] \leq \Pr[\mathbf{n} \notin \mathcal{R}_V(\mathbf{0})]$.

*Proof:*

$$\begin{aligned}\Pr[\mathbf{n} \in \mathcal{R}_V(\mathbf{0})] &= \Pr[\forall \boldsymbol{\lambda} \in \Lambda \setminus \Lambda' \left(\|\mathbf{n} - \mathbf{0}\| \leq \|\mathbf{n} - \boldsymbol{\lambda}\|\right)] \\ &= \Pr[\forall \boldsymbol{\lambda} \in \Lambda \setminus \Lambda' \left(\|\mathbf{n} - \mathbf{0}\| < \|\mathbf{n} - \boldsymbol{\lambda}\|\right)].\end{aligned}$$

Note that if $\|\mathbf{n} - \mathbf{0}\| < \|\mathbf{n} - \boldsymbol{\lambda}\|$ for all $\boldsymbol{\lambda} \in \Lambda \setminus \Lambda'$, then $\mathcal{Q}_\Lambda^{\text{NN}}(\mathbf{n}) \notin \Lambda \setminus \Lambda'$, as $\mathbf{0}$ is closer to $\mathbf{n}$ than any element in $\Lambda \setminus \Lambda'$. Thus,

$$\Pr[\mathbf{n} \in \mathcal{R}_V(\mathbf{0})] \leq \Pr[\mathcal{Q}_\Lambda^{\text{NN}}(\mathbf{n}) \notin \Lambda \setminus \Lambda'] = \Pr[\mathcal{Q}_\Lambda^{\text{NN}}(\mathbf{n}) \in \Lambda'].$$

■

We further upper bound the probability $\Pr[\mathbf{n} \notin \mathcal{R}_V(\mathbf{0})]$. Let $\mathrm{Nbr}(\Lambda \setminus \Lambda') \subseteq \Lambda \setminus \Lambda'$ denote the set of neighbors of $\mathbf{0}$ in $\Lambda \setminus \Lambda'$, i.e., $\mathrm{Nbr}(\Lambda \setminus \Lambda')$ is the smallest subset of $\Lambda \setminus \Lambda'$ such that $\mathcal{R}_V(\mathbf{0})$ is precisely the set

$$\{\mathbf{x} \in \mathbb{C}^n : \forall \boldsymbol{\lambda} \in \mathrm{Nbr}(\Lambda \setminus \Lambda')\, (\|\mathbf{x} - \mathbf{0}\| \leq \|\mathbf{x} - \boldsymbol{\lambda}\|)\}\,.$$

Then, for any $\nu > 0$, we have

$$\begin{aligned}
&P[\mathbf{n} \notin \mathcal{R}_V(\mathbf{0})] \\
&= P\left[\|\mathbf{n}\|^2 \geq \|\mathbf{n} - \boldsymbol{\lambda}\|^2,\ \text{some } \boldsymbol{\lambda} \in \mathrm{Nbr}(\Lambda \setminus \Lambda')\right] \\
&= P\left[\mathrm{Re}\{\boldsymbol{\lambda}^{\mathsf{H}}\mathbf{n}\} \geq \|\boldsymbol{\lambda}\|^2/2,\ \text{some } \boldsymbol{\lambda} \in \mathrm{Nbr}(\Lambda \setminus \Lambda')\right] \\
&\leq \sum_{\boldsymbol{\lambda} \in \mathrm{Nbr}(\Lambda \setminus \Lambda')} P\left[\mathrm{Re}\{\boldsymbol{\lambda}^{\mathsf{H}}\mathbf{n}\} \geq \|\boldsymbol{\lambda}\|^2/2\right] && (16) \\
&\leq \sum_{\boldsymbol{\lambda} \in \mathrm{Nbr}(\Lambda \setminus \Lambda')} \exp(-\nu\|\boldsymbol{\lambda}\|^2/2) E\left[\exp(\nu \mathrm{Re}\{\boldsymbol{\lambda}^{\mathsf{H}}\mathbf{n}\})\right], && (17)
\end{aligned}$$

where (16) follows from the union bound and (17) follows from the Chernoff bound. Since $\mathbf{n} = \sum_\ell (\alpha h_\ell - a_\ell)\mathbf{x}_\ell + \alpha\mathbf{z}$, we have

$$\begin{aligned}
&E\left[\exp\left(\nu \mathrm{Re}\{\boldsymbol{\lambda}^{\mathsf{H}}\mathbf{n}\}\right)\right] \\
&= E\left[\exp\left(\nu \mathrm{Re}\left\{\boldsymbol{\lambda}^{\mathsf{H}}\left(\sum_\ell (\alpha h_\ell - a_\ell)\mathbf{x}_\ell + \alpha\mathbf{z}\right)\right\}\right)\right] \\
&= E\left[\exp(\nu \mathrm{Re}\{\boldsymbol{\lambda}^{\mathsf{H}}\alpha\mathbf{z}\})\right] \\
&\quad \cdot \prod_\ell E\left[\exp(\nu \mathrm{Re}\{\boldsymbol{\lambda}^{\mathsf{H}}(\alpha h_\ell - a_\ell)\mathbf{x}_\ell\})\right] && (18) \\
&= \exp\left(\frac{1}{4}\nu^2\|\boldsymbol{\lambda}\|^2|\alpha|^2 N_0\right) \\
&\quad \cdot \prod_\ell E\left[\exp(\nu \mathrm{Re}\{\boldsymbol{\lambda}^{\mathsf{H}}(\alpha h_\ell - a_\ell)\mathbf{x}_\ell\})\right] && (19)
\end{aligned}$$

where (18) follows from the independence of $\mathbf{x}_1, \ldots, \mathbf{x}_L, \mathbf{z}$ and (19) follows from the moment-generating function of a circularly symmetric complex Gaussian random vector.

*Lemma 2:* Let $\mathbf{x} \in \mathbb{C}^n$ be a complex random vector uniformly distributed over a hypercube $\gamma\mathbf{U}\mathcal{H}_n$ for some $\gamma > 0$ and some $n \times n$ unitary matrix. Then

$$E\left[\exp(\mathrm{Re}\{\mathbf{v}^{\mathsf{H}}\mathbf{x}\})\right] \leq \exp(\|\mathbf{v}\|^2\gamma^2/24).$$

*Proof:* First, we consider a special case where the unitary matrix $\mathbf{U} = \mathbf{I}_n$. In this case, we have

$$\begin{aligned}
& E\left[\exp(\mathrm{Re}\{\mathbf{v}^{\mathsf{H}}\mathbf{x}\})\right] \\
&= E\left[\exp(\mathrm{Re}\{\mathbf{v}\}^T\mathrm{Re}\{\mathbf{x}\} + \mathrm{Im}\{\mathbf{v}\}^T\mathrm{Im}\{\mathbf{x}\})\right] \\
&= E\left[\exp\left(\sum_{i=1}^{n}\left(\mathrm{Re}\{\mathbf{v}_i\}\mathrm{Re}\{\mathbf{x}_i\} + \mathrm{Im}\{\mathbf{v}_i\}\mathrm{Im}\{\mathbf{x}_i\}\right)\right)\right] \\
&= \prod_{i=1}^{n} E\left[\exp(\mathrm{Re}\{\mathbf{v}_i\}\mathrm{Re}\{\mathbf{x}_i\}\right] E\left[\exp \mathrm{Im}\{\mathbf{v}_i\}\mathrm{Im}\{\mathbf{x}_i\})\right] \qquad (20) \\
&= \prod_{i=1}^{n} \frac{\sinh(\mathrm{Re}\{\mathbf{v}_i\}\gamma/2)}{\mathrm{Re}\{\mathbf{v}_i\}\gamma/2}\frac{\sinh(\mathrm{Im}\{\mathbf{v}_i\}\gamma/2)}{\mathrm{Im}\{\mathbf{v}_i\}\gamma/2} \qquad (21) \\
&\le \prod_{i=1}^{n} \exp\left(\frac{(\mathrm{Re}\{\mathbf{v}_i\}\gamma)^2}{24}\right)\exp\left(\frac{(\mathrm{Im}\{\mathbf{v}_i\}\gamma)^2}{24}\right) \qquad (22) \\
&= \exp\left(\frac{\gamma^2}{24}\|\mathbf{v}\|^2\right)
\end{aligned}$$

where (20) follows from the independence among each real/imaginary component, (21) follows from the moment-generating function of a uniform random variable (note that both $\mathrm{Re}\{\mathbf{x}_i\}$ and $\mathrm{Im}\{\mathbf{x}_i\}$ are uniformly distributed over $[-\gamma/2, \gamma/2]$), and (22) follows from $\sinh(x)/x \le \exp(x^2/6)$ (which can be obtained by simple Taylor expansion).

Then we consider a general unitary matrix $\mathbf{U}$. In this case, we have $\mathbf{x} = \mathbf{U}\mathbf{x}'$, where $\mathbf{x}' \in \gamma[-1/2, 1/2]^{2n}$, i.e., both $\mathrm{Re}\{\mathbf{x}'_i\}$ and $\mathrm{Im}\{\mathbf{x}'_i\}$ are uniformly distributed over $[-\gamma/2, \gamma/2]$. Hence,

$$\begin{aligned}
E\left[\exp(\mathrm{Re}\{\mathbf{v}^{\mathsf{H}}\mathbf{x}\})\right] &= E\left[\exp(\mathrm{Re}\{\mathbf{v}^{\mathsf{H}}\mathbf{U}\mathbf{x}'\})\right] \\
&= E\left[\exp(\mathrm{Re}\{(\mathbf{U}^{\mathsf{H}}\mathbf{v})^{\mathsf{H}}\mathbf{x}'\})\right] \\
&\le \exp\left(\frac{\gamma^2}{24}\|\mathbf{U}^{\mathsf{H}}\mathbf{v}\|^2\right) \\
&= \exp\left(\frac{\gamma^2}{24}\|\mathbf{v}\|^2\right).
\end{aligned}$$

■

Note that $P = \frac{1}{n}E[\|\mathbf{x}_\ell\|^2] = \gamma^2/6$. Thus, we have

$$\begin{aligned}
& E\left[\exp(\nu\mathrm{Re}\{\boldsymbol{\lambda}^{\mathsf{H}}\mathbf{n}\})\right] \\
&\le \exp\left(\frac{1}{4}\nu^2\|\boldsymbol{\lambda}\|^2|\alpha|^2N_0\right)\prod_{\ell}\exp(\|\nu\boldsymbol{\lambda}(\alpha h_\ell - a_\ell)\|^2P/4) \\
&= \exp\left(\frac{1}{4}\nu^2\|\boldsymbol{\lambda}\|^2|\alpha|^2N_0 + \|\nu\boldsymbol{\lambda}\|^2\|\alpha\mathbf{h} - \mathbf{a}\|^2P/4\right) \\
&= \exp\left(\frac{1}{4}\|\boldsymbol{\lambda}\|^2\nu^2N_0Q(\mathbf{a},\alpha)\right),
\end{aligned}$$

where the quantity $Q(\mathbf{a}, \alpha)$ is given by

$$Q(\mathbf{a}, \alpha) = |\alpha|^2 + \mathsf{SNR}\,\|\alpha\mathbf{h} - \mathbf{a}\|^2$$

and $\mathsf{SNR} = P/N_0$.

It follows that, for all $\nu > 0$,

$$\begin{aligned}
&\Pr[\mathbf{n} \notin \mathcal{R}_V(\mathbf{0})] \\
&\le \sum_{\boldsymbol{\lambda} \in \mathrm{Nbr}(\Lambda \setminus \Lambda')} \exp\left(-\nu\|\boldsymbol{\lambda}\|^2/2 + \frac{1}{4}\|\boldsymbol{\lambda}\|^2 \nu^2 N_0 Q(\mathbf{a}, \alpha)\right).
\end{aligned}$$

Choosing $\nu = 1/(N_0 Q(\mathbf{a}, \alpha))$, we have

$$\begin{aligned}
\Pr[\mathbf{n} \notin \mathcal{R}_V(\mathbf{0})] &\le \sum_{\boldsymbol{\lambda} \in \mathrm{Nbr}(\Lambda \setminus \Lambda')} \exp\left(-\frac{\|\boldsymbol{\lambda}\|^2}{4 N_0 Q(\mathbf{a}, \alpha)}\right) \\
&\approx K(\Lambda/\Lambda') \exp\left(-\frac{d^2(\Lambda/\Lambda')}{4 N_0 Q(\mathbf{a}, \alpha)}\right)
\end{aligned}$$

for high signal-to-noise ratios. Therefore, we have

$$\begin{aligned}
\Pr[\mathcal{Q}_\Lambda^{\mathrm{NN}}(\mathbf{n}) \notin \Lambda'] &\le \Pr[\mathbf{n} \notin \mathcal{R}_V(\mathbf{0})] \\
&\lessapprox K(\Lambda/\Lambda') \exp\left(-\frac{d^2(\Lambda/\Lambda')}{4 N_0 Q(\mathbf{a}, \alpha)}\right).
\end{aligned}$$

Since $\alpha$ can be carefully chosen, we have

$$\Pr[\mathcal{Q}_\Lambda^{\mathrm{NN}}(\mathbf{n}) \notin \Lambda'] \lessapprox \min_{\alpha \in \mathbb{C}} K(\Lambda/\Lambda') \exp\left(-\frac{d^2(\Lambda/\Lambda')}{4 N_0 Q(\mathbf{a}, \alpha)}\right),$$

completing the proof for the first part of Theorem 7. The second part of Theorem 7 follows immediately when the optimal value of $\alpha$ is substituted.

### *B. Proof of Proposition 2*

Recall that $d(\Lambda_r/\Lambda_r')$ is the length of the shortest vectors in the set difference $\Lambda_r \setminus \Lambda_r'$. Hence, we have

$$d(\Lambda_r/\Lambda_r') = \min_{\mathbf{c} \neq \mathbf{0}} \|\sigma^*(\mathbf{c})\|;$$

equivalently, $d^2(\Lambda_r/\Lambda_r') = \min_{\mathbf{c} \neq \mathbf{0}} \|\sigma^*(\mathbf{c})\|^2 = w_E^{\min}(\mathcal{C})$. Recall that $\Lambda = \Lambda_r + i\Lambda_r$. That is, $\Lambda = \Lambda_r \times \Lambda_r$. Hence, we have

$$d^2(\Lambda/\Lambda') = d^2(\Lambda_r/\Lambda_r') = w_E^{\min}(\mathcal{C}).$$

Note that $V(\Lambda') = p^{2n}$ and $V(\Lambda')/V(\Lambda) = p^{2k}$. Hence, we have $V(\Lambda) = p^{2(n-k)}$. Combining the above two results, we have

$$\gamma_c(\Lambda/\Lambda') = w_E^{\min}(\mathcal{C})/p^{2(1-k/n)}.$$

We then turn to $K(\Lambda_r/\Lambda_r')$ and $K(\Lambda/\Lambda')$. When $p = 2$, the minimum Euclidean weight $w_E^{\min}(\mathcal{C})$ of $\mathcal{C}$ is precisely the minimum Hamming weight of $\mathcal{C}$. In this case, $K(\Lambda_r/\Lambda_r') = \left(w_E^{\min}(\mathcal{C})\right) 2^{w_E^{\min}(\mathcal{C})}$, as shown in [34]. When $p > 2$, the set different $\Lambda_r \setminus \Lambda_r'$ can be expressed as

$$\Lambda_r \setminus \Lambda_r' = \bigcup_{\mathbf{c} \neq \mathbf{0}} \left\{\sigma^*(\mathbf{c}) + \Lambda_r'\right\}.$$

In this case, $\sigma^*(\mathbf{c})$ is the unique coset leader for the coset $\sigma^*(\mathbf{c})+\Lambda'_r$. Thus, the number $K(\Lambda_r/\Lambda'_r)$ of the shortest vectors in $\Lambda_r \setminus \Lambda'_r$ is precisely the number $A\left(w_E^{\min}(\mathcal{C})\right)$ of coset leaders with $\|\sigma^*(\mathbf{c})\|^2 = w_E^{\min}(\mathcal{C})$. Hence, we have

$$K(\Lambda_r/\Lambda'_r) = \begin{cases} A\left(w_E^{\min}(\mathcal{C})\right) 2^{w_E^{\min}(\mathcal{C})}, & \text{when } p=2, \\ A\left(w_E^{\min}(\mathcal{C})\right), & \text{when } p>2. \end{cases}$$

Recall that $\Lambda' = \Lambda'_r + i\Lambda'_r$. That is, $\Lambda' = \Lambda'_r \times \Lambda'_r$. It follows that $K(\Lambda/\Lambda') = 2K(\Lambda_r/\Lambda'_r)$, completing the proof.

### *C. Proof of Proposition 3*

The proof is analogous to that of Proposition 2 with two differences. First, $p$ is replaced by $|\pi|$ in the expression of $\gamma_c(\Lambda/\Lambda')$. This difference comes from the fact that $V(\Lambda') = |\pi|^{2n}$ and $V(\Lambda')/V(\Lambda) = |\pi|^{2k}$. Second, the case of $|\pi| = 2$ gives an expression of $A\left(w_E^{\min}(\mathcal{C})\right) 4^{w_E^{\min}(\mathcal{C})}$ for $K(\Lambda/\Lambda')$. This is because if the coset $\mathbf{c}+\Lambda'$ contains one shortest vector in $\Lambda \setminus \Lambda'$, then a total of $4^{w_E^{\min}(\mathcal{C})}$ shortest vectors can be found in the coset $\mathbf{c}+\Lambda'$. Suppose that $(c_1,\ldots,c_n)$ is one such shortest vector in $\mathbf{c}+\Lambda'$. Then, $(c_1,\ldots,c_n)$ has precisely $w_E^{\min}(\mathcal{C})$ nonzero elements. Moreover, for each nonzero element, say $c_j$, if we change it to one of $\{-c_j, i\times c_j, (-i)\times c_j\}$, then the new vector has the same Euclidean norm and is still in the coset $\mathbf{c}+\Lambda'$. Therefore, the number of shortest vectors in $\mathbf{c}+\Lambda'$ is $4^{w_E^{\min}(\mathcal{C})}$.

### *D. $\Lambda_r$ in (12) is a Lattice*

Let $\tilde{\mathbf{g}}_j = \tilde{\sigma}(\mathbf{g}_j)$, for $j=1,\ldots,k_s$. It is easy to check that $\boldsymbol{\lambda} \in \Lambda_r$ if and only if $\boldsymbol{\lambda} = p^s\mathbf{r} + \sum_{j=1}^{k_s} c_j\tilde{\mathbf{g}}_j$ for some $\mathbf{r}\in\mathbb{Z}^n$ and $c_j \in \{0,\ldots,p^s-1\}$ satisfying the division condition: when $k_t < j \le k_{t+1}$, $p^t \mid c_j$ (where $t=1,\ldots,s-1$).

Let $\boldsymbol{\lambda}_i = p^s\mathbf{r}_i + \sum_{j=1}^{k_s} c_{ij}\tilde{\mathbf{g}}_j$ $(i=1,2)$ be two vectors from $\Lambda_r$. Then we have $\mathbf{r}_1,\mathbf{r}_2\in\mathbb{Z}^n$, and $c_{1j},c_{2j}\in\{0,\ldots,p^s-1\}$ satisfy the division condition. Now consider the difference

$$\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2 = p^s(\mathbf{r}_1-\mathbf{r}_2) + \sum_{j=1}^{k_s}(c_{1j}-c_{2j})\tilde{\mathbf{g}}_j.$$

We will show that $\boldsymbol{\lambda}_1-\boldsymbol{\lambda}_2\in\Lambda_r$. We need the following lemma from elementary arithmetic.

*Lemma 3:* Let $a,d\in\mathbb{Z}$ with $d\neq 0$. Then there exist unique $q,r\in\mathbb{Z}$ such that $a=qd+r$ and $0\le r<|d|$.

Using the above lemma, we have $c_{1j}-c_{2j} = q_jp^s + r_j$ for some $q_j\in\mathbb{Z}$ and $r_j\in\{0,\ldots,p^s-1\}$. Furthermore, if $p^t$ divides $c_{1j}-c_{2j}$, then $p^t$ divides $r_j$, where $t=1,\ldots,s-1$. Thus, $\{r_j\}$ satisfy the division condition. Note that

$$\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2 = p^s(\mathbf{r}_1-\mathbf{r}_2+\sum_j q_j\tilde{\mathbf{g}}_j) + \sum_j r_j\tilde{\mathbf{g}}_j.$$

Thus, $\boldsymbol{\lambda}_1-\boldsymbol{\lambda}_2\in\Lambda_r$, which implies that $\Lambda_r$ is indeed a lattice.

Next, we will construct a generator matrix for $\Lambda_r$. Let $\tilde{\mathbf{G}}$ denote the matrix with rows $\tilde{\mathbf{g}}_1,\ldots,\tilde{\mathbf{g}}_n$. Clearly, we have $\det(\tilde{\mathbf{G}})=1$ due to the way $\{\mathbf{g}_i\}$ are constructed. This implies that $\tilde{\mathbf{g}}_1,\ldots,\tilde{\mathbf{g}}_n$ span $\mathbb{Z}^n$ over $\mathbb{Z}$. That is, any vector $\mathbf{r}\in\mathbb{Z}^n$ can be expressed as an integer combination of $\tilde{\mathbf{g}}_1,\ldots,\tilde{\mathbf{g}}_n$. Consider the set of all integer combinations of the following vectors: $\tilde{\mathbf{g}}_1, \ldots, \tilde{\mathbf{g}}_{k_1}$, $p\tilde{\mathbf{g}}_{k_1+1}, \ldots, p\tilde{\mathbf{g}}_{k_2}$, …, $p^s\tilde{\mathbf{g}}_{k_s+1}, \ldots, p^s\tilde{\mathbf{g}}_n$. On the one hand, it is easy to see that any integer combination of these vectors is a lattice point in $\Lambda_r$. On the other hand, let $\boldsymbol{\lambda} = p^s\mathbf{r} + \sum_{j=1}^{k_s} c_j\tilde{\mathbf{g}}_j$ be a lattice point in $\Lambda_r$, where $\mathbf{r} \in \mathbb{Z}^n$ and $\{c_j\}$ satisfy the division condition. Recall that $\mathbf{r} = \sum_{j=1}^{n} b_j\tilde{\mathbf{g}}_j$ for some $b_j \in \mathbb{Z}$. Thus, we have

$$\boldsymbol{\lambda} = \sum_{i=1}^{k_s}(c_i + p^s b_i)\tilde{\mathbf{g}}_i + \sum_{j=k_s+1}^{n} p^s b_j\tilde{\mathbf{g}}_j.$$

Since $p^t \mid c_i$, when $k_t < i \le k_{t+1}$, we have $p^t \mid c_i + p^t b_i$, when $k_t < i \le k_{t+1}$. Hence, $\boldsymbol{\lambda}$ is indeed an integer combination of the above vectors. Let $\mathbf{G}_{\Lambda_r}$ be the matrix formed by these vectors. Then $\mathbf{G}_{\Lambda_r}$ is a generator matrix for $\Lambda_r$.

### E. *Proof of Relation (13)*

The following two observations simplify the proof of the relation (13). First, it suffices to consider the case of $s = 2$, since the case of $s > 2$ is essentially the same. Second, it suffices to prove the relation for the pair of nested $\mathbb{Z}$-lattices $\Lambda_r \supseteq \Lambda_r'$, i.e.,

$$\mathbf{G}_{\Lambda_r'} = \mathrm{diag}(\underbrace{p^2, \ldots, p^2}_{k_1}, \underbrace{p, \ldots, p}_{k_2-k_1}, \underbrace{1, \ldots, 1}_{n-k_2})\mathbf{G}_{\Lambda_r} \tag{23}$$

due to the lifting operation.

Next we will construct two generator matrices $\mathbf{G}_{\Lambda_r}$ and $\mathbf{G}_{\Lambda_r'}$ satisfying the above relation. Let $\tilde{\mathbf{g}}_i$ denote $\tilde{\sigma}(\mathbf{g}_i)$, for $i = 1, \ldots, n$. On the one hand, by Appendix D, there exists a generator matrix $\mathbf{G}_{\Lambda_r}$ of $\Lambda_r$ consisting of basis vectors $\tilde{\mathbf{g}}_1, \ldots, \tilde{\mathbf{g}}_{k_1}$, $p\tilde{\mathbf{g}}_{k_1+1}, \ldots, p\tilde{\mathbf{g}}_{k_2}$, $p^2\tilde{\mathbf{g}}_{k_2+1}, \ldots, p^2\tilde{\mathbf{g}}_n$. On the other hand, the vectors $\{p^2\tilde{\mathbf{g}}_1, \ldots, p^2\tilde{\mathbf{g}}_n\}$ form a basis of $\Lambda_r'$, because $\tilde{\mathbf{g}}_1, \ldots, \tilde{\mathbf{g}}_n$ span $\mathbb{Z}^n$ over $\mathbb{Z}$. By comparing these two bases for $\Lambda_r$ and $\Lambda_r'$, we conclude that there exist two generator matrices $\mathbf{G}_{\Lambda_r}$ and $\mathbf{G}_{\Lambda_r'}$ satisfying Relation (23).

### F. *Proof of Proposition 4*

It suffices to consider the case $s = 2$, since the case of $s > 2$ is essentially the same. Consider a lattice point $\boldsymbol{\lambda} \in \Lambda_r \setminus \Lambda_r'$ given by

$$\boldsymbol{\lambda} = p^2\mathbf{r} + \sum_{j=1}^{k_1}\beta_{1j}\tilde{\mathbf{g}}_j + \sum_{j=1}^{k_2}p\beta_{2j}\tilde{\mathbf{g}}_j,$$

where $\beta_{ij} \in \{0, \ldots, p-1\}$. Clearly, some $\beta_{ij}$ must be nonzero, because otherwise $\boldsymbol{\lambda} = p^2\mathbf{r} \in \Lambda_r'$. We consider the following two cases.

Case 1: some $\beta_{1j}$ is nonzero. In this case, we construct a new lattice $\Lambda_{r1} = \{p\mathbf{r} + \sum_{j=1}^{k_1}\beta_j\tilde{\mathbf{g}}_j : \mathbf{r} \in \mathbb{Z}^n, \beta_j \in \{0, \ldots, p-1\}\}$ and a new sublattice $\Lambda_{r1}' = \{p\mathbf{r} : \mathbf{r} \in \mathbb{Z}^n\}$. Clearly, we have $\boldsymbol{\lambda} \in \Lambda_{r1}$ and $\boldsymbol{\lambda} \notin \Lambda_{r1}'$. Thus, $\boldsymbol{\lambda} \in \Lambda_{r1} \setminus \Lambda_{r1}'$. Note that the nested lattice pair $\Lambda_{r1} \supseteq \Lambda_{r1}'$ can be obtained from the code $\mathcal{C}_1$ by Construction A. Thus, we have $\|\boldsymbol{\lambda}\|^2 \ge w_E^{\min}(\mathcal{C}_1)$ and the number of lattice points $\boldsymbol{\lambda}$ of the Euclidean weight $w_E^{\min}(\mathcal{C}_1)$ is upper bounded by $K(\Lambda_{r1}/\Lambda_{r1}')$.

Case 2: all $\beta_{1j}$ are zero, and some $\beta_{2j}$ is nonzero. In this case, we construct a new lattice $\Lambda_{r2} = \{p\mathbf{r} + \sum_{j=1}^{k_2}\beta_j\tilde{\mathbf{g}}_j : \mathbf{r} \in \mathbb{Z}^n, \beta_j \in \{0, \ldots, p-1\}\}$ and a new sublattice $\Lambda_{r2}' = \{p\mathbf{r} : \mathbf{r} \in \mathbb{Z}^n\}$. Clearly, we have

$\boldsymbol{\lambda} = p^2\mathbf{r} + \sum_{j=1}^{k_2} p\beta_{2j}\tilde{\mathbf{g}}_j \in p\Lambda_{r2}$ and $\boldsymbol{\lambda} \notin p\Lambda_{r2}'$. Thus, $\boldsymbol{\lambda} \in p\Lambda_{r2} \setminus p\Lambda_{r2}'$. Similar to Case 1, the nested lattice pair $\Lambda_{r2} \supseteq \Lambda_{r2}'$ can be obtained from the code $\mathcal{C}_2$ by Construction A. Thus, we have $\|\boldsymbol{\lambda}\|^2 \geq p^2 w_E^{\min}(\mathcal{C}_2)$, and the number of lattice points $\boldsymbol{\lambda}$ of the Euclidean weight $w_E^{\min}(\mathcal{C}_2)$ is upper bounded by $K(\Lambda_{r2}/\Lambda_{r2}')$.

Combining the above two cases, we have, for all $\boldsymbol{\lambda} \in \Lambda_r \setminus \Lambda_r'$, that $\|\boldsymbol{\lambda}\|^2 \geq \min\{w_E^{\min}(\mathcal{C}_1), p^2 w_E^{\min}(\mathcal{C}_2)\}$, which implies that $d^2(\Lambda_r/\Lambda_r') \geq \min\{w_E^{\min}(\mathcal{C}_1), p^2 w_E^{\min}(\mathcal{C}_2)\}$. Recall that $\Lambda = \Lambda_r \times \Lambda_r$. Hence, we have

$$\begin{aligned} d^2(\Lambda/\Lambda') &= d^2(\Lambda_r/\Lambda_r') \\ &\geq \min\{w_E^{\min}(\mathcal{C}_1), p^2 w_E^{\min}(\mathcal{C}_2)\}. \end{aligned}$$

Note that $V(\Lambda') = p^{4n}$ and $V(\Lambda')/V(\Lambda) = p^{2(k_1+k_2)}$, since each $\beta_{ij} \in \{0, \ldots, p-1\}$. Hence, we have $V(\Lambda) = p^{2(2n-k_1-k_2)}$ and

$$\begin{aligned} \gamma_c(\Lambda/\Lambda') &= d^2(\Lambda/\Lambda')/p^{2(2-(k_1+k_2)/n)} \\ &\geq \frac{\min\{w_E^{\min}(\mathcal{C}_1), p^2 w_E^{\min}(\mathcal{C}_2)\}}{p^{2(2-(k_1+k_2)/n)}}. \end{aligned}$$

We also have $K(\Lambda_r/\Lambda_r') \leq K(\Lambda_{r1}/\Lambda_{r1}') + K(\Lambda_{r2}/\Lambda_{r2}')$ and $K(\Lambda/\Lambda') = 2K(\Lambda_r/\Lambda_r')$, completing the proof for the case $s = 2$.

### *G. Modified Viterbi Decoder for Example 7*

We will show that the nearest neighbor quantizer $\mathcal{Q}_\Lambda^{\text{NN}}$ can be implemented through a modified Viterbi decoder. First, note that $\mathcal{Q}_\Lambda^{\text{NN}}$ solves the following optimization problem

$$\begin{aligned} \text{minimize} \quad & \|\boldsymbol{\lambda} - \alpha\mathbf{y}\| \qquad (24) \\ \text{subject to} \quad & \boldsymbol{\lambda} \in \Lambda. \end{aligned}$$

Second, note that the problem (24) is equivalent to

$$\begin{aligned} \text{minimize} \quad & \|\tilde{\sigma}(\mathbf{c}) + \boldsymbol{\lambda}' - \alpha\mathbf{y}\| \qquad (25) \\ \text{subject to} \quad & \mathbf{c} \in \mathcal{C} \qquad (26) \\ & \boldsymbol{\lambda}' \in \Lambda'. \end{aligned}$$

This is because each lattice point $\boldsymbol{\lambda} \in \Lambda$ can be expressed as $\boldsymbol{\lambda} = \tilde{\sigma}(\mathbf{c}) + \Lambda'$, where $\mathbf{c} = \sigma(\boldsymbol{\lambda})$ and $\boldsymbol{\lambda}' \in \Lambda'$.

Third, note that Problem (25) is equivalent to

$$\begin{aligned} \text{minimize} \quad & \|[\tilde{\sigma}(\mathbf{c}) - \alpha\mathbf{y}] \bmod \Lambda'\| \qquad (27) \\ \text{subject to} \quad & \mathbf{c} \in \mathcal{C}, \end{aligned}$$

where $[\mathbf{x}] \bmod \Lambda'$ is defined as $[\mathbf{x}] \bmod \Lambda' \triangleq \mathbf{x} - \mathcal{Q}_{\Lambda'}^{\text{NN}}(\mathbf{x})$. This is because $\boldsymbol{\lambda}' = -\mathcal{Q}_{\Lambda'}^{\text{NN}}(\tilde{\sigma}(\mathbf{c}) - \alpha\mathbf{y})$ solves Problem (25) for any $\mathbf{c} \in \mathcal{C}$.

Now it is easy to see the problem (27) can be solved through a modified Viterbi decoder with the metric given by $\|[\cdot] \bmod \Lambda'\|$ instead of $\|\cdot\|$. Therefore, the nearest neighbor quantizer $\mathcal{Q}_\Lambda^{\text{NN}}$ can be implemented through a modified Viterbi decoder.

### H. Proof of Theorem 8

First, we show the existence of the solution $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ by induction on $m$.

If $m = 1$, then the vector $\mathbf{a}_1$ can be chosen such that $\mathbf{a}_1\mathbf{L}$ is one of the shortest lattice points. Note that $\mathbf{a}_1$ is not divisible by $\pi$; otherwise it will not be one of the shortest lattice points. In other words, $\bar{\mathbf{a}}_1$ is indeed nonzero. Hence, the solution $\mathbf{a}_1$ always exists when $m = 1$.

Now suppose the solution $\{\mathbf{a}_1, \ldots, \mathbf{a}_k\}$ exists when $k < m$. We will show the existence of the vector $\mathbf{a}_{k+1}$.

Consider the following set

$$\mathcal{A} = \{\mathbf{a} \in T^L : \bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_k, \bar{\mathbf{a}} \text{ are linearly independent}\}.$$

Clearly, the set $\mathcal{A}$ is nonempty, since $k < m$. Then the vector $\mathbf{a}_{k+1}$ can be chosen as

$$\mathbf{a}_{k+1} = \arg\min_{\mathbf{a} \in \mathcal{A}} \|\mathbf{a}\mathbf{L}\|.$$

This proves the existence of the vector $\mathbf{a}_{k+1}$, which completes the induction.

Second, we show that the solution $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ is a dominant solution by induction on $m$.

If $m = 1$, then $\|\mathbf{a}_1\mathbf{L}\| \leq \|\mathbf{b}_1\mathbf{L}\|$ for any feasible solution $\mathbf{b}_1$, since $\mathbf{a}_1\mathbf{L}$ is one of the shortest lattice points.

Now suppose that $\{\mathbf{a}_1, \ldots, \mathbf{a}_k\}$ is a dominant solution when $k < m$. We will show that $\{\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{a}_{k+1}\}$ is also a dominant solution.

Suppose that $\{\mathbf{b}_1, \ldots, \mathbf{b}_k, \mathbf{b}_{k+1}\}$ is a feasible solution with $\|\mathbf{b}_1\mathbf{L}\| \leq \ldots \leq \|\mathbf{b}_{k+1}\mathbf{L}\|$. Since $\bar{\mathbf{b}}_1, \ldots, \bar{\mathbf{b}}_k$ are linearly independent, we have

$$\|\mathbf{a}_i\mathbf{L}\| \leq \|\mathbf{b}_i\mathbf{L}\|,\ i = 1, \ldots, k.$$

It remains to show $\|\mathbf{a}_{k+1}\mathbf{L}\| \leq \|\mathbf{b}_{k+1}\mathbf{L}\|$. We consider the following two cases.

1) If there exists some $\mathbf{b}_i$ $(i = 1, \ldots, k+1)$ such that $\bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_k, \bar{\mathbf{b}}_i$ are linearly independent, then by the construction of $\mathbf{a}_{k+1}$, we have

$$\|\mathbf{a}_{k+1}\mathbf{L}\| \leq \|\mathbf{b}_i\mathbf{L}\| \leq \|\mathbf{b}_{k+1}\mathbf{L}\|.$$

2) Otherwise, each $\bar{\mathbf{b}}_i$ can be expressed as a linear combination of $\bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_k$. That is,

$$\bar{\mathbf{b}}_i \in \text{Span}\{\bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_k\}.$$

This is contrary to the fact that $\bar{\mathbf{b}}_1, \ldots, \bar{\mathbf{b}}_{k+1}$ are linearly independent, since any $k+1$ vectors in a vector space of dimension $k$ are linearly dependent.

Therefore, we have $\|\mathbf{a}_{k+1}\mathbf{L}\| \leq \|\mathbf{b}_{k+1}\mathbf{L}\|$, which completes the induction.

## References

[1] B. Nazer and M. Gastpar, “Compute-and-forward: Harnessing interference through structured codes,” *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.

[2] R. Kötter and F. R. Kschischang, “Coding for errors and erasures in random network coding,” *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[3] J. Blömer, “Closest vectors, successive minima, and dual HKZ bases of lattices,” in *Proc. of Int. Colloq. Automata, Languages and Programming*, no. 248 – 259, Geneva, Switzerland, Jul. 2000.

[4] S. Zhang, S.-C. Liew, and P. P. Lam, “Hot topic: Physical layer network coding,” in *Proc. ACM Int. Conf. Mobile Compu. and Netw.*, Los Angeles, CA, USA, Sep. 24–29, 2006, pp. 358–365.

[5] P. Popovski and H. Yomo, “The anti-packets can increase the achievable throughput of a wireless multi-hop network,” in *Proc. of IEEE Int. Conf. on Commun.*, Istanbul, Turkey, Jun. 11–15, 2006, pp. 3885–3890.

[6] B. Nazer and M. Gastpar, “Computing over multiple-access channels with connections to wireless network coding,” in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, USA, Jul. 9–14, 2006, pp. 1354–1358.

[7] P. Popovski and H. Yomo, “Physical network coding in two-way wireless relay channels,” in *Proc. of IEEE Int. Conf. on Commun.*, Glasgow, Scotland, Jun. 24–28, 2007, pp. 707–712.

[8] T. Koike-Akino, P. Popovski, and V. Tarokh, “Optimized constellations for two-way wireless relaying with physical network coding,” *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 773–787, Jun. 2009.

[9] M. P. Wilson, K. R. Narayanan, H. D. Pfister, and A. Sprintson, “Joint physical layer coding and network coding for bidirectional relaying,” *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5641–5654, Nov. 2010.

[10] W. Nam, S.-Y. Chung, and Y. H. Lee, “Capacity bounds for two-way relay channels,” in *Proc. of Int. Zurich Seminar on commun.*, Zurich, Switzerland, Mar. 12–14, 2008.

[11] M. P. Wilson and K. R. Narayanan, “Power allocation strategies and lattice based coding schemes for bi-directional relaying,” in *Proc. IEEE Int. Symp. Inf. Theory*, Coex, Seoul, Korea, Jun. 28 – Jul. 3, 2009, pp. 344–348.

[12] A. S. Avestimehr, A. Sezgin, and D. N. C. Tse, “Capacity of the two-way relay channel within a constant gap,” *Eur. Trans. Telecomms.*, vol. 21, no. 4, pp. 363–374, Jun. 2010.

[13] P. Popovski and T. Koike-Akino, “Coded bidirectional relaying in wireless networks,” in *New Directions in Wireless Communications Research*, V. Tarokh, Ed. Springer, 2009, pp. 291–316.

[14] S. H. Lim, Y.-H. Kim, A. E. Gamal, and S.-Y. Chung, “Noisy network coding,” *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3132–3152, May 2011.

[15] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, “Wireless network information flow: A deterministic approach,” *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1872–1905, Apr. 2011.

[16] A. Özgür and S. N. Diggavi, “Approximately achieving Gaussian relay network capacity with lattice codes,” in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, Texas, USA, Jun. 13–18, 2010, pp. 669–673.

[17] U. Niesen and P. Whiting, “The degrees of freedom of compute-and-forward,” *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5214–5232, Aug. 2012.

[18] J. Zhan, B. Nazer, M. Gastpar, and U. Erez, “MIMO compute-and-forward,” in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, South Korea, Jun. 28– Jul. 3, 2009, pp. 2848–2852.

[19] J.-C. Belfiore and M. A. V. Castro, “Managing interference through space-time codes, lattice reduction and network coding,” in *IEEE Inf. Theory Workshop*, Cairo, Egypt, Jan. 6–8, 2010, pp. 1–5.

[20] B. Hern and K. R. Narayanan, “Multilevel coding schemes for compute-and-forward,” in *Proc. IEEE Int. Symp. Inf. Theory*, Saint Petersburg, Russia, Jul. 31– Aug. 5, 2011, pp. 1713–1717.

[21] O. Ordentlich, J. Zhan, U. Erez, M. Gastpar, and B. Nazer, “Practical code design for compute-and-forward,” in *Proc. IEEE Int. Symp. Inf. Theory*, Saint Petersburg, Russia, Jul. 31– Aug. 5, 2011, pp. 1876–1880.

[22] C. Feng, D. Silva, and F. R. Kschischang, “Lattice network coding via signal codes,” in *Proc. IEEE Int. Symp. Inf. Theory*, Saint Petersburg, Russia, Jul. 31– Aug. 5, 2011, pp. 2642–2646.

[23] J.-C. Belfiore, “Lattice codes for the compute-and-forward protocol: The flatness factor,” in *IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 16–20, 2011, pp. 1876–1880.

[24] B. Nazer and M. Gastpar, “Reliable physical layer network coding,” *Proc. IEEE*, vol. 99, no. 3, pp. 438–460, Mar. 2011.

[25] C. Feng, D. Silva, and F. R. Kschischang, “An algebraic approach to physical-layer network coding,” in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, Jun. 13–18, 2010, pp. 1017–1021.

[26] ——, “Design criteria for lattice network coding,” in *Proc. Conf. Inform. Sci. and Systems*, Baltimore, MD, Mar. 23–25, 2011, pp. 1–6.

[27] ——, “Lattice network coding over finite rings,” in *Proc. Canadian Workshop Inf. Theory*, Kelowna, Canada, May 17–20, 2011, pp. 78–81.

[28] S. Qifu and J. Yuan, “Lattice network codes based on Eisenstein integers,” in *Proc. 20012 IEEE Int. Conf. on Wireless and Mobile Comput.*, Barcelona, Spain, Oct. 2012, pp. 225–231.

[29] N. E. Tunali, K. R. Narayanan, J. J. Boutros, and Y.-C. Huang, “Lattices over Eisenstein integers for compute-and-forward,” in *Proc. 2012 Allerton Conf. Commun., Control, and Comput.*, Monticello, IL, Oct. 2012, pp. 33–40.

[30] B. R. McDonald, *Linear Algebra over Commutative Rings*. New York: Marcel Dekker, Inc., 1984.

[31] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed. John Wiley & Sons, Inc., 2004.

[32] W. C. Brown, *Matrices over Commutative Rings*. New York: Marcel Dekker, Inc., 1993.

[33] R. Zamir, *Lattice Coding for Signals and Networks*. Preprint, 2013.

[34] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York: Springer-Verlag, 1999.

[35] S.-Y. R. Li, R. W. Yeung, and N. Cai, “Linear network coding,” *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[36] R. Koetter and M. Médard, “An algebraic approach to network coding,” *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[37] R. Dougherty, C. Freiling, and K. Zeger, “Insufficiency of linear coding in network information flow,” *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2745–2759, Aug. 2005.

[38] J. H. Conway and N. Sloane, “A fast encoding method for lattice codes and quantizers,” *IEEE Trans. Inf. Theory*, vol. 29, no. 6, pp. 820–824, Nov. 1983.

[39] G. D. Forney, Jr., “Multidimensional constellations—part II: Voronoi constellations,” *IEEE J. Sel. Areas Commun.*, vol. 7, no. 6, pp. 941–958, Aug. 1989.

[40] ——, “Convolutional codes I: Algebraic structure,” *IEEE Trans. Inf. Theory*, vol. 16, no. 6, pp. 720–738, Nov. 1970.

[41] C. Feng, R. W. Nóbrega, F. R. Kschischang, and D. Silva, “Communication over finite-chain-ring matrix channels,” *Computing Research Repository (CoRR)*, Apr. 2013, submitted to the IEEE Trans. Inf. Theory. [Online]. Available: http://arxiv.org/abs/1304.2523

[42] N. Sommer, M. Feder, and O. Shalvi, “Shaping methods for low-density lattice codes,” in *IEEE Inf. Theory Workshop*, Taormina, Sicily, Italy, Oct. 11-16, 2009, pp. 238–242.

[43] J. A. Rush and N. Sloane, “An improvement to the Minkowski-Hlawka bound for packing superballs,” *Mathematika*, vol. 34, pp. 8–18, 1987.

[44] O. Shalvi, N. Sommer, and M. Feder, “Signal codes: Convolutional lattice codes,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5203–5226, Aug. 2011.

[45] O. Ordentlich and U. Erez, “Achieving the gains promised by integer-forcing equalization with binary codes,” in *Proc. of 26th Convention of Electr. and Electron. Eng. in Israel*, Eilat, Israel, Nov. 2010, pp. 703–707.

[46] A. Sakzad, M.-R. Sadeghi, and D. Panario, “Turbo lattices: Construction and performance analysis,” *submitted to IEEE Trans. Inf. Theory*, 2010.

[47] N. E. Tunali and K. R. Narayanan, “Concatenated signal codes with applications to compute and forward,” in *Proc. of IEEE Global Commun. Conf.*, Houston, TX, Dec. 5–9, 2011, pp. 1–5.

[48] B. Hern and K. R. Narayanan, “Multilevel coding schemes for compute-and-forward with flexible decoding,” *Computing Research Repository (CoRR)*, Dec. 2011, submitted to the IEEE Trans. Inf. Theory. [Online]. Available: http://arxiv.org/abs/1112.2690

[49] S.-N. Hong and G. Caire, “Compute-and-forward strategies for cooperative distributed antenna systems,” *Computing Research Repository (CoRR)*, Sep. 2012, submitted to the IEEE Trans. Inf. Theory. [Online]. Available: http://arxiv.org/abs/1210.0160

[50] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*. Springer-Verlag, 1971.

[51] A. K. Lenstra, H. W. Lenstra, and L. Lovász, “Factoring polynomials with rational coefficients,” *Math. Ann.*, vol. 261, no. 4, pp. 515–534, 1982.

[52] H. Napias, “A generalized of the LLL-algorithm over Euclidean rings or orders,” *J. Théorie des Nombres de Bordeaux*, pp. 387–396, 1996.

[53] Y. H. Gan, C. Ling, and W. H. Mow, “Complex lattice reduction algorithm for low-complexity full-diversity MIMO detection,” *IEEE Trans. Signal Process.*, vol. 57, no. 7, pp. 2701 – 2710, Jul. 2009.

[54] B. Vallée, “Gauss’ algorithm revisited,” *J. Algorithms*, vol. 12, pp. 556–572, 1991.

[55] H. Yao and G. W. Wornell, “Lattice-reduction-aided detectors for MIMO communication systems,” in *Proc. of IEEE Global Commun. Conf.*, Taipei, Taiwan, R.O.C., Nov. 17–21, 2002, pp. 424–428.

[56] P. Q. Nguyen and D. Stehlé, “Low-dimensional lattice basis reduction revisited,” *ACM Trans. Algorithms*, vol. 5, no. 46, pp. 1–48, Oct. 2009.

**Chen Feng** received the B.E. degree from Shanghai Jiao Tong University in 2006 and the M.A.Sc. degree from the University of Toronto in 2009. He is currently a Ph.D. student in the Department of Electrical and Computer Engineering, University of Toronto. His research interests are in network coding, coding theory, information theory, and their applications to computer networking.

During his Ph.D. studies, Chen Feng won several awards for his academic achievement, including the Chinese Government Award for Outstanding Students Abroad in 2012, and the Shahid U. H. Qureshi Memorial Scholarship in 2013.

**Danilo Silva** received the B.Sc. degree from the Federal University of Pernambuco (UFPE), Recife, Brazil, in 2002, the M.Sc. degree from the Pontifical Catholic University of Rio de Janeiro (PUC-Rio), Rio de Janeiro, Brazil, in 2005, and the Ph.D. degree from the University of Toronto, Toronto, Canada, in 2009, all in electrical engineering.

From 2009 to 2010, he was a Postdoctoral Fellow at the University of Toronto, at the École Polytechnique Fédérale de Lausanne (EPFL), and at the State University of Campinas (UNICAMP). In 2010, he joined the Department of Electrical Engineering, Federal University of Santa Catarina (UFSC), Brazil, where he is currently an Assistant Professor. His research interests include channel coding, information theory, and network coding.

Dr. Silva was a recipient of a CAPES Ph.D. Scholarship in 2005, the Shahid U. H. Qureshi Memorial Scholarship in 2009, and a FAPESP Postdoctoral Scholarship in 2010.

**Frank R. Kschischang** received the B.A.Sc. degree (with honors) from the University of British Columbia in 1985 and the M.A.Sc. and Ph.D. degrees from the University of Toronto in 1988 and 1991, respectively, all in electrical engineering. He is a Professor and Canada Research Chair at the University of Toronto, where he has been a faculty member since 1991. Between 2011 and 2013 he was a Hans Fischer Senior Fellow at the Institute for Advanced Study, Technische Universität München.

His research interests are focused primarily on the area of channel coding techniques, applied to wireline, wireless and optical communication systems and networks. He is the recipient of the 2010 Killam Research Fellowship, the 2010 Communications Society and Information Theory Society Joint Paper Award and the 2012 Canadian Award in Telecommunications Research. He is a Fellow of IEEE, of the Engineering Institute of Canada, and of the Royal Society of Canada.

During 1997-2000, he served as an Associate Editor for Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY. He also served as technical program co-chair for the 2004 IEEE International Symposium on Information Theory (ISIT), Chicago, and as general co-chair for ISIT 2008, Toronto. He served as the 2010 President of the IEEE Information Theory Society.