Lattices over Eisenstein Integers for Compute-and-Forward

Nihat Engin Tunali, *Member, IEEE,* Yu-Chih Huang, *Member, IEEE,* Joseph J. Boutros, *Senior Member, IEEE,* and Krishna R. Narayanan, *Senior Member, IEEE*

***Abstract*—In this paper, we consider the use of lattice codes over Eisenstein integers for implementing a compute-and-forward protocol in wireless networks when channel state information is not available at the transmitter. We extend the compute-and-forward paradigm of Nazer and Gastpar to decoding Eisenstein integer combinations of transmitted messages at relays by proving the existence of a sequence of pairs of nested lattices over Eisenstein integers in which the coarse lattice is good for covering and the fine lattice can achieve the Poltyrev limit. Using this result, we show that both the outage performance and error-correcting performance of nested lattice codebooks over Eisenstein integers surpasses lattice codebooks over integers considered by Nazer and Gastpar with no additional computational complexity.**

***Index Terms*—Compute-and-Forward, Lattice codes, Eisenstein integers**

I. Introduction

Compute-and-forward is a novel relaying paradigm in wireless communications in which relays in a network directly compute or decode functions of signals transmitted from multiple transmitters and forward them to a central destination. One of the most effective ways to implement a compute-and-forward scheme is to employ lattice codes at each transmitter. Since a lattice is closed under integer addition, lattice codes are naturally suited to decoding integer linear combinations of transmitted signals.

Lattice codes have been shown to be optimal for several problems in communications including coding for the point-to-point additive white Gaussian noise (AWGN) channel [1] and coding with side information problems such as the dirty paper coding problem and Wyner-Ziv problem [2]. The construction of optimal lattice codes for these problems requires a lattice that is good for channel coding. Since a lattice has unconstrained power, goodness for channel coding is measured using Poltyrev's idea of the unconstrained AWGN channel. In [3], Poltyrev derives the maximum noise variance that a lattice can tolerate while maintaining reliable communication over the unconstrained point-to-point AWGN channel, which is referred to as the Poltyrev limit in literature. Loeliger showed the existence of lattices that achieve the Poltyrev limit by means of Construction A in [4]. Then, Erez *et al.*, showed that there exists lattices which are simultaneously good for quantization and can achieve the Poltyrev limit in [5] which made it possible to construct nested lattice codes that were able to achieve a rate of $\frac{1}{2}\log\left(1+\mathrm{SNR}\right)$ over the point-to-point AWGN channel. There has also been great interest in constructing lattice codes with reasonable encoding and decoding complexities such as Signal Codes and Low Density Lattice Codes [6], [7].

In a bidirectional relay network when channel state information is available at the transmitters, the transmitters can compensate for the channel gains and the relay can decode to the sum of the transmitted signals, which is a special case of compute-and-forward. For this system model, it was shown that an exchange rate of $\frac{1}{2}\log\left(\frac{1}{2}+\mathrm{SNR}\right)$ can be achieved using nested lattice codes at the transmitters, which is optimal for asymptotically large signal-to-noise ratios and provides substantial gains over other relaying paradigms such as amplify-and-forward and decode-and-forward [8], [9]. In [10], a novel compute-and-forward implementation is proposed for the $K\times K$ AWGN interference network where channel state information is available at the transmitters, which achieves the full K degrees of freedom.

We consider the case when channel state information is not available at the transmitters. In this case, an effective way to implement a compute-and-forward scheme is to allow the relay to adaptively choose the integer coefficients depending on the channel coefficients. Nazer and Gastpar have introduced and analyzed such a scheme which uses lattices over integers and they have derived achievable information rates in [11]. In [12], Feng, Silva and Kschischang have introduced an algebraic framework for designing lattice codes for compute-and-forward. The framework in [12] is quite general in the sense that every lattice partition based compute-and-forward scheme can be put into this framework, including the one by Nazer and Gastpar in [11]. However, [12] does not provide a means to identify good lattice partition based schemes.

In this paper, we contribute to the literature by identifying a lattice partition based compute-and-forward scheme which is particularly good for approximating channel coefficients from the complex field. Our scheme can be regarded as an extension of the scheme in [11] to lattices over Eisenstein integers. We

Nihat Engin Tunali is with Xilinx Inc., 2100 Logic Drive, San Jose, CA, 95124, USA (email: engint@xilinx.com). Yu-Chih Huang is with the Department of Communication Engineering, National Taipei University, 237 Sanxia District, New Taipei City, Taiwan (email: ychuang@mail.ntpu.edu.tw). Joseph J. Boutros is with the Department of Electrical Engineering, Texas A&M University at Qatar, PO Box 23874, Education City, Doha, Qatar (email: boutros@tamu.edu). Krishna R. Narayanan is with the Department of Electrical and Computer Engineering Texas A&M University, College Station, TX, 77843, USA (email: krn@ece.tamu.edu). This paper was presented in part at the 2011 Banff Workshop on Algebraic Structure in Network Information Theory, at the 2012 Information Theory and its Application Workshop, and the 2012 Allerton Conference on Communications, Control and Computing. This work was supported by the National Science Foundation under Grant CCF 0729210 and by the Qatar National Research Foundation under grant NPRP 5-597-2-241.

show that an improvement in outage performance and error-correcting performance can be obtained compared to using lattices over integers. We proceed by proving the existence of a sequence of nested lattices over Eisenstein integers in which the coarse lattice is good for covering and the fine lattice achieves the Poltyrev limit. Using this result, we can show similar results to those in [11] with integers replaced by Eisenstein integers. The main improvement in outage and error-correcting performance is a consequence of that the use of lattices over Eisenstein integers permits the relay to decode to a linear combination of the transmitted signals where the coefficients are Eisenstein integers, which quantize channel coefficients better than Gaussian integers.

Recently, we became aware of an independent work by Sun *et. al.* [13] where lattice network codes over Eisenstein integers are also considered. The main focus in [13] is the analysis of the decoding error probability, which suggests that lattice network codes built over Eisenstein integers can provide significant coding gains over lattice network codes built over Gaussian integers. Our work differs from [13] in the following ways. While their focus is on constructing finite constellations from lattice partitions which are suitable for compute-and-forward, we consider construction of lattices (infinite constellations) over Eisenstein integers and show the optimality of such construction. Moreover, their coding scheme can be regarded as the concatenation of a linear code over an appropriate finite field and a constellation carved from a lattice partition. On the other hand, our scheme is a more general one which is formed by the quotient group of a lattice over Eisenstein integers and its sublattice. It can be shown that the scheme in [13] is a special case of ours with hypercube shaping[1]. This generalization is imperative in the sense that it allows us to show the achievable computation rates if one would use such lattices for compute-and-forward.

The structure of our paper is as follows. In Section I-A, we introduce the notation that will be used throughout the paper. In Section II, we present the system model that will be considered. In Section III, we provide some background on lattices and lattice codes. In Section IV, we discuss Nazer and Gastpar's framework for compute-and-forward [11]. In Section V, we discuss how lattices over Eisenstein integers can be used for compute-and-forward in Nazer and Gastpar's framework and what properties of these lattices are required in order to achieve computation rates formulated similarly to those in [11]. In Section VI, we provide numerical results and compare the outage performance and error-correcting performance of lattices over natural integers and lattices over Eisenstein integers in compute-and-forward. In Appendix A, we introduce the notation that is used in Appendix B and Appendix C, we prove that there exist a nested pair of Eisenstein lattices which the coarse lattice is good for covering and the fine lattice achieves the Poltyrev limit.

[1]Here, we use the term "hypercube shaping" to denote a scheme using a properly scaled version of Eisenstein integers as shaping (coarse) lattice. Thus, when $\mathbb{Z}$ or $\mathbb{Z}[i]$ are considered, the shape is a hypercube. However, it is in fact not a hypercube if $\mathbb{Z}[\omega]$ is considered.

A. Notational Convention

Throughout the paper, we use $\mathbb{R}$ to denote the field of real numbers, $\mathbb{C}$ to denote the field of complex numbers, and $\mathbb{F}_q$ to denote a finite field of size q. $\mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{Z}[\omega]$ are used to denote the set of integers, Gaussian integers, and Eisenstein integers, respectively. We use underlined variables to denote vectors and boldface uppercase variables to denote matrices, e.g., $\underline{x}$ and $\mathbf{X}$, respectively. We denote the i^{th} column of a matrix $\mathbf{X}$ as $\mathbf{X}_i$. Also, we use superscript H to denote the Hermitian operation, e.g., $\underline{x}^H$ and $\mathbf{X}^H$. We define $\log^+(x) \triangleq \max(\log_2(x), 0)$ and denote the Euclidean metric as $\|\cdot\|$. We denote the all zero vector in $\mathbb{R}^n$ as $\underline{0}$ and the $n \times n$ identity matrix as $\mathbf{I}$. We denote the volume of a bounded region $E \subset \mathbb{R}^n$ as $\mathrm{Vol}\,(E)$ and denote the n-dimensional sphere of radius r centered at $\underline{0}$ as $\mathcal{B}(r) \triangleq \{\underline{s} \,:\, \|\underline{s}\| \leq r\}$.

II. System Model

We consider an AWGN network as shown in Fig. 1 where L source nodes $S_1, S_2, \ldots, S_L$ wish to transmit information to M relay nodes $D_1, D_2, \ldots, D_M$, where $M \geq L$. It is assumed that relay nodes cannot collaborate with each other and are noiselessly connected to a final destination interested in the individual messages sent from all the source nodes. The objective of the relay nodes is to facilitate communication between the source nodes and the final destination.

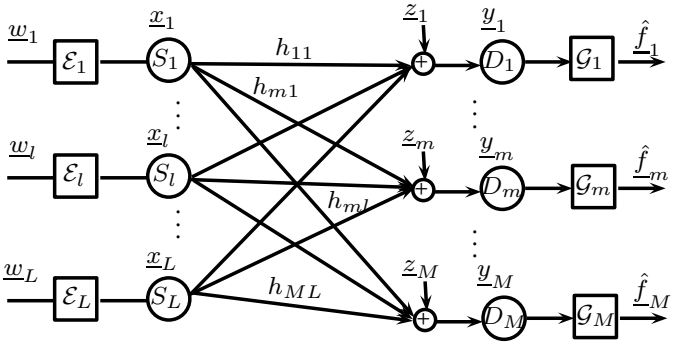

Fig. 1. The AWGN Network where $S_1, S_2, \ldots, S_L$ wish to transmit information to $D_1, D_2, \ldots, D_M$. The channel between the S_l and D_m is denoted as h_{ml}.

We denote the information vector at the source node S_l as $\underline{w}_l \in \mathbb{F}_q^k$. Without loss of generality, we assume that the length of the information vector at each transmitter l has the same length k. Each transmitter is equipped with an encoder $\mathcal{E}_l : \mathbb{F}_q^k \to \mathbb{C}^n$ that maps $\underline{w}_l$ to an n-dimensional complex codeword $\underline{x}_l = \mathcal{E}_l(\underline{w}_l)$. Each codeword is subject to the power constraint

$$\mathbb{E}||\underline{x}_l||^2 \leq nP. \tag{1}$$

The message rate R of each transmitter is the length of its message in bits normalized by the number of channel uses,

$$R = \frac{k}{n} \log q. \tag{2}$$

Due to the superposition nature of the wireless medium, each relay m observes

$$\underline{y}_m = \sum_{l=1}^{L} h_{ml}\underline{x}_l + \underline{z}_m, \tag{3}$$

where $h_{ml} \in \mathbb{C}$ is the channel coefficient between D_m and S_l. As it can be observed from (3), it is assumed that there is no inter-symbol interference and all $h_{ml}\underline{x}_l$ arrive at the relay simultaneously. Furthermore, $\underline{z}_m$ is an n-dimensional complex vector which consists of identically distributed (i.i.d.) circularly symmetric Gaussian random variables, i.e. $\underline{z}_m \sim \mathcal{CN}(0, \mathbf{I})$. Let $\underline{h}_m = [h_{m1}, \cdots, h_{mL}]^T$ denote the vector of channel coefficients to relay m from all the source nodes. We assume that the relay m only has the knowledge of the channel coefficient from each transmitter to itself, i.e., $\underline{h}_m$.

Each relay attempts to recover the linear combination $\underline{f}_m$ (over $\mathbb{F}_q$)

$$\underline{f}_m = \bigoplus_{l=1}^{L} \left(b_{ml}\underline{w}_l\right), \tag{4}$$

where $b_{ml} \in \mathbb{F}_q$ and let $\underline{b}_m = [b_{m1}, \ldots, b_{mL}]^T$. Typically b_{ml}s are chosen based on the network structure and/or the channel coefficients. It is desirable for the matrix $[\underline{b}_1, \ldots, \underline{b}_M]$ to be full-rank which enables each $\underline{w}_l$ to be recovered at the final destination. For each D_m, we define the decoder $\mathcal{G}_m : \mathbb{C}^n \to \mathbb{F}_q^k$ and $\hat{\underline{f}}_m = \mathcal{G}_m(y_m)$ is an estimate of $\underline{f}_m$. Let $\mathcal{P}$ denote a principal ideal domain in $\mathbb{C}$ such as $\mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$.

Definition 1 (Average probability of error): Equations with coefficient vectors $\underline{a}_1, \underline{a}_2, \ldots \underline{a}_M$, where each $\underline{a}_m \in \mathcal{P}^L$, are decoded with *average probability of error* ϵ if

$$\Pr\left(\bigcup_{m=1}^{M}\left\{\hat{\underline{f}}_m \neq \underline{f}_m\right\}\right) < \epsilon. \tag{5}$$

Definition 2 (Computation rate of relay m): For a given channel coefficient vector $\underline{h}_m$ and equation coefficient vector $\underline{a}_m \in \mathcal{P}^L$, the computation rate $R\left(\underline{h}_m, \underline{a}_m\right)$ is achievable at relay m if for any $\epsilon > 0$ and n large enough, there exist encoders $\mathcal{E}_1, \ldots, \mathcal{E}_L$ and there exists a decoder $\mathcal{G}_m$ such that relay m can recover its desired equation with average probability of error ϵ as long as the underlying message rate R satisfies

$$R < R\left(\underline{h}_m, \underline{a}_m\right). \tag{6}$$

Due to the fact that the relays cannot collaborate, each relay picks an integer vector $\underline{a}_m$ such that $R\left(\underline{h}_m, \underline{a}_m\right)$ is maximized.

Definition 3 (Computation rate of AWGN network): Given $\mathbf{H} = [\underline{h}_1, \ldots, \underline{h}_M]$ and $\mathbf{A} = [\underline{a}_1, \ldots, \underline{a}_M]$, the achievable computation rate of an AWGN network is defined as

$$\mathcal{R}\left(\mathbf{H}, \mathbf{A}\right) = \min_{m: a_{ml} \neq 0} R\left(\underline{h}_m, \underline{a}_m\right), \tag{7}$$

provided that the matrix $\sigma\left(\mathbf{A}\right) = [\underline{b}_1, \ldots, \underline{b}_M] \in \mathbb{F}_q^{L \times M}$, where $\sigma : \mathcal{P}^{L \times M} \to \mathbb{F}_q^{L \times M}$, is full rank. If $[\underline{b}_1, \ldots, \underline{b}_M]$ is not full rank, $\mathcal{R}\left(\mathbf{H}, \mathbf{A}\right) = 0$.

Note that in this paper, our coding scheme particularly considers the ring of Eisenstein integers, i.e., $\mathcal{P} = \mathbb{Z}[\omega]$. The reason will become clear in the following sections.

III. Background on Lattices

Due to the fact that the coding scheme that will be considered heavily relies on lattices, we now provide some background knowledge on lattices. For more details on lattices, please refer to [14], [5], and [1].

Definition 4 (Lattice over $\mathbb{Z}$): An n-dimensional *lattice over natural integers*, $\Lambda^{(n)}$, is a discrete set of points in $\mathbb{R}^n$ such that $\Lambda^{(n)}$ is a discrete additive subgroup of $\mathbb{R}^n$ with rank k where $k \leq n$. Such a lattice can be generated via a full rank generator matrix $\mathbf{B} \in \mathbb{R}^{n \times k}$

$$\Lambda^{(n)} = \left\{\underline{\lambda} = \mathbf{B}\underline{e} : \underline{e} \in \mathbb{Z}^k\right\}. \tag{8}$$

For notational convenience, we shall drop the superscript in $\Lambda^{(n)}$ in this paper and denote n-dimensional lattices as Λ. Also, we refer to lattices over integers as $\mathbb{Z}$-lattices throughout the paper.

Given a lattice Λ, we denote the *quantizer* operation with respect to Λ as Q_Λ, the *modulus* operation with respect to Λ as $\bmod \Lambda$, and the *fundamental Voronoi region* of Λ as $\mathcal{V}_\Lambda$. We denote the *covering radius* and *effective radius* of Λ as r_Λ^{cov} and r_Λ^{eff}, respectively. We denote the *second moment* and *normalized second moment* of Λ as σ_Λ^2 and $G\left(\Lambda\right)$, respectively. We refer the reader to [14] for these definitions.

Definition 5 (Goodness for covering): A sequence of lattices Λ is *good for covering* if

$$\lim_{n\to\infty} \frac{r_\Lambda^{\text{cov}}}{r_\Lambda^{\text{eff}}} = 1. \tag{9}$$

These lattices are also commonly referred to as *Rogers good*, since it was first shown by Rogers that such lattices exist [15].

Definition 6 (Goodness for quantization): A sequence of lattices Λ is *good for quantization* if

$$\lim_{n\to\infty} G\left(\Lambda\right) = \frac{1}{2\pi e}. \tag{10}$$

In other words, the normalized second moment of Λ converges to a sphere's normalized second moment as $n \to \infty$. Zamir *et al.*, have shown that such a sequence of lattices exist [16]. Erez *et al.* have also shown the existence of such a sequence of lattices and proved that goodness for covering implies goodness for quantization [5].

Definition 7 (Lattices that achieve the Poltyrev limit): Let $\underline{z}$ be an n-dimensional independent and identically distributed (i.i.d) Gaussian vector, $\underline{z} \sim \mathcal{N}\left(\underline{0}, \theta_{\underline{z}}^2\mathbf{I}\right)$. The *effective radius* of $\underline{z}$, which we denote as $r_{\underline{z}}$, is defined as

$$r_{\underline{z}} = \sqrt{n\theta_{\underline{z}}^2}. \tag{11}$$

Consider a $\mathbb{Z}$-lattice Λ and a lattice point $\underline{\lambda} \in \Lambda$, which is transmitted across an AWGN channel:

$$\underline{y} = \underline{\lambda} + \underline{z}. \tag{12}$$

The maximum likelihood decoder would decode to the lattice point nearest in Euclidean distance to $\underline{y}$. Therefore, an error would occur only if $\underline{y}$ leaves the Voronoi region of $\underline{\lambda}$. Due to lattice symmetry, this is equivalent to $\underline{z}$ leaving the fundamental Voronoi region $\mathcal{V}_\Lambda$.

$$P_e\left(\Lambda, r_{\underline{z}}\right) = \Pr\left\{\underline{z} \notin \mathcal{V}_\Lambda\right\}, \tag{13}$$

where $P_e\left(\Lambda, r_{\underline{z}}\right)$ denotes the probability of error.

A sequence of $\mathbb{Z}$-lattices Λ are *good for AWGN channel coding* if for any $r_{\underline{z}} < r_{\Lambda}^{\text{eff}}$, $\lim_{n\to\infty} P_e\left(\Lambda, r_{\underline{z}}\right) = 0$ and this decay may be bounded exponentially in n. Erez *et. al.* have shown the existence of such a sequence of lattices in [5] and they have referred to them as *Poltyrev good*.

Nonetheless, in order to achieve the Poltyrev capacity in the unconstrained AWGN channel, it is sufficient for $\lim_{n\to\infty} P_e\left(\Lambda, r_{\underline{z}}\right) = 0$ for any $r_{\underline{z}} < r_{\Lambda}^{\text{eff}}$, i.e., $P_e\left(\Lambda, r_{\underline{z}}\right)$ does not need to decay exponentially as $n \to \infty$. We refer to such a sequence of lattices as *lattices that achieve the Poltyrev limit* in this paper. Loeliger has shown the existence of such lattices in [4].

Definition 8 (Sublattice): A $\mathbb{Z}$-lattice Λ is a sublattice of (nested in) another $\mathbb{Z}$-lattice Λ_f if $\Lambda \subseteq \Lambda_f$. Λ is referred to as the *coarse lattice* and Λ_f is referred to as the *fine lattice*. The quotient group Λ_f/Λ is referred to as a lattice partition [17].

Definition 9 (Nesting ratio): Given a pair of n-dimensional nested lattices $\Lambda \subset \Lambda_f$, the *nesting ratio* ϑ is defined as,

$$\vartheta = \left(\frac{\text{Vol}(\mathcal{V}_\Lambda)}{\text{Vol}(\mathcal{V}_{\Lambda_f})}\right)^{\frac{1}{n}}. \tag{14}$$

Definition 10 (Nested Lattice Code): Given a fine $\mathbb{Z}$-lattice Λ_f and a coarse $\mathbb{Z}$-lattice Λ, where $\Lambda \subseteq \Lambda_f$, a *nested lattice code* (Voronoi code), which we refer to as $\mathcal{L}$, is the set of all coset leaders in Λ_f that lie in the fundamental Voronoi region of the coarse lattice Λ [18]:

$$\mathcal{L} = \mathcal{V}_\Lambda \cap \Lambda_f = \left\{\underline{\lambda}_f \ : \ Q_\Lambda\left(\underline{\lambda}_f\right) = \underline{0}, \underline{\lambda}_f \in \Lambda_f\right\}. \tag{15}$$

In other words, $\mathcal{L}$ is a set of coset representatives of the quotient group Λ_f/Λ.

The *coding rate* of a nested lattice code, denoted as R is defined as,

$$R = \log \vartheta. \tag{16}$$

A. Construction A for $\mathbb{Z}$-lattices

One way to construct $\mathbb{Z}$-lattices is to use the following procedure, which is referred to as *Construction A* [19]:

Let q be a natural prime and k, n be integers such that $k \leq n$. Then, let $\mathbf{G} \in \mathbb{F}_q^{n\times k}$.

1) Define the discrete codebook $\mathcal{C} = \{\underline{x} = \mathbf{G}\underline{y} : \underline{y} \in \mathbb{F}_q^k\}$ where all operations are over $\mathbb{F}_q$. Thus, $\underline{x} \in \mathbb{F}_q^n$.
2) Generate the $\mathbb{Z}$-lattice $\Lambda_\mathcal{C}$ as $\Lambda_\mathcal{C} \triangleq \{\underline{\lambda} \in \mathbb{Z}^n : \underline{\lambda} \bmod q \in \mathcal{C}\}$, where the $\bmod$ operation is applied to each component of $\underline{\lambda}$.
3) Scale $\Lambda_\mathcal{C}$ with q^{-1} to obtain $\Lambda = q^{-1}\Lambda_\mathcal{C}$.

We would like to note that only the first two steps that we have stated in Construction A is required to build a lattice, since the third step simply scales the lattice. However when Erez *et. al.* prove the existence of lattices built with Construction A that are good for covering in [5], they keep r_Λ^{eff} approximately constant as $n \to \infty$ and $q \to \infty$, which is possible only if the third step is used for scaling the lattice.

B. Nested $\mathbb{Z}$-lattices obtained from Construction-A [1]

Let Λ be an n-dimensional $\mathbb{Z}$-lattice obtained through Construction-A with a corresponding generator matrix $\mathbf{B}$. For a given $\mathbf{G} \in \mathbb{F}_q^{n\times k}$, denote Λ' as the corresponding $\mathbb{Z}$-lattice obtained through Construction-A using $\mathbf{G}$ as the generator matrix of the underlying linear code. Generate the $\mathbb{Z}$-lattice Λ_f as $\Lambda_f = \mathbf{B}\Lambda'$. It can be observed that $\Lambda \subset \Lambda_f$ with a coding rate of $\frac{k}{n}\log q$.

IV. Compute-and-Forward with $\mathbb{Z}$-lattices

One way to implement network coding for the system model considered in this paper is for each relay to decode to $\underline{w}_l$ individually, then form $\underline{f}_m$ and forward it through the network, which is commonly referred as decode-and-forward. As the number of source nodes L increase, decode-and-forward is limited by self-interference since other transmitted messages are treated as noise when decoding to $\underline{w}_l$ individually. Therefore, one way to mitigate the effect of self-interference would be for relay m to directly decode to $\underline{f}_m$ from $\underline{y}_m$ instead of decoding to $\underline{w}_l$'s individually. Such an approach is commonly referred to as compute-and-forward, which was introduced by Nazer and Gastpar in [11] and results in achieving substantially higher rates than other forwarding paradigms such as amplify-and-forward, decode-and-forward, compress-and-forward in many situations.

In [11], Nazer and Gastpar use nested lattice codes to implement the compute-and-forward paradigm. Since lattices are closed under integer combinations, the relays attempt to decode to a linear combination of codewords with integer coefficients. This can then be shown to correspond to decoding linear combinations over the finite field. We briefly discuss how lattice codes are constructed to implement the compute-and-forward paradigm in [11].

A fine $\mathbb{Z}$-lattice Λ_f and a coarse $\mathbb{Z}$-lattice Λ nested in Λ_f, is constructed as mentioned in Section III-B with a coding rate $R = \frac{k}{n}\log q$. If Λ is simultaneously good for covering and good for AWGN channel coding, it follows that Λ_f is good for AWGN channel coding [1]. Both Λ and Λ_f are scaled such that $\sigma_\Lambda^2 = P/2$. Following this, the lattice codebook $\Lambda_f \cap \mathcal{V}_\Lambda$ is constructed.

Source node l partitions its information vector $\underline{w}_l \in \mathbb{F}_q^{2k}$ into $\underline{w}_l^R, \underline{w}_l^I \in \mathbb{F}_q^k$, and maps them to lattice codewords $\underline{t}_l^R, \underline{t}_l^I \in \Lambda_f \cap \mathcal{V}$, respectively, via a bijective mapping $\tilde{\psi}$,

$$\tilde{\psi}(\underline{w}) = \left[\mathbf{B}q^{-1}g(\mathbf{G}\underline{w})\right], \tag{17}$$

where $\underline{w} \in \mathbb{F}_q^k$, and g is the trivial bijective mapping between $\{0, 1, \cdots, q-1\}$ and $\mathbb{F}_q$. Hence, $\underline{t}_l^R = \tilde{\psi}\left(\underline{w}_l^R\right), \underline{t}_l^I = \tilde{\psi}\left(\underline{w}_l^I\right)$. It then constructs dither vectors $\underline{d}_l^R, \underline{d}_l^I$, which are uniformly distributed within $\mathcal{V}$ and subtracts these dither vectors from the lattice codewords $\underline{t}_l^R, \underline{t}_l^I$, respectively, and transmits the following:

$$\underline{x}_l = \left(\left[\underline{t}_l^R - \underline{d}_l^R\right] \bmod \Lambda\right) + j\left(\left[\underline{t}_l^I - \underline{d}_l^I\right] \bmod \Lambda\right). \tag{18}$$

Recall that given a channel coefficient vector $\underline{h}_m \in \mathbb{C}^L$, relay

m observes

$$\underline{y}_m = \sum_{l=1}^{L} h_{ml}\underline{x}_l + \underline{z}_m. \tag{19}$$

The relay approximates $\underline{h}_m$, in some sense, by a Gaussian integer vector $\underline{a}_m \in \mathbb{Z}[i]^L$ and its goal will be to recover the following:

$$\underline{v}_m^R = \left[\sum_{l=1}^{L}\left[\Re\left(a_{ml}\right)\underline{t}_l^R - \Im\left(a_{ml}\right)\underline{t}_l^I\right]\right] \bmod \Lambda, \tag{20}$$

$$\underline{v}_m^I = \left[\sum_{l=1}^{L}\left[\Im\left(a_{ml}\right)\underline{t}_l^R + \Re\left(a_{ml}\right)\underline{t}_l^I\right]\right] \bmod \Lambda. \tag{21}$$

It proceeds by removing the dithers and scaling the observation with α_m and therefore,

$$\begin{aligned}\underline{\tilde{y}}_m^R &= \Re\left(\alpha_m\underline{y}_m\right) + \sum_{l=1}^{L}\Re\left(a_{ml}\right)\underline{d}_l^R - \Im\left(a_{ml}\right)\underline{d}_l^I \\ &= \underline{v}_m^R + \underline{z}_{eq,m}^R,\end{aligned} \tag{22}$$

and

$$\begin{aligned}\underline{\tilde{y}}_m^I &= \Im\left(\alpha_m\underline{y}_m\right) + \sum_{l=1}^{L}\Im\left(a_{ml}\right)\underline{d}_l^R + \Re\left(a_{ml}\right)\underline{d}_l^I \\ &= \underline{v}_m^I + \underline{z}_{eq,m}^I,\end{aligned} \tag{23}$$

where α_m is the MMSE scaling coefficient that minimizes the variance of $\underline{z}_{eq,m}^R + j\underline{z}_{eq,m}^I$. The relay quantizes $\underline{\tilde{y}}_m^I, \underline{\tilde{y}}_m^R$ to the closest lattice points in the fine lattice Λ_f modulo the coarse lattice Λ and estimates the following:

$$\underline{\hat{v}}_m^R = \left[Q\left(\underline{\tilde{y}}_m^R\right)\right] \bmod \Lambda, \tag{24}$$

$$\underline{\hat{v}}_m^I = \left[Q\left(\underline{\tilde{y}}_m^I\right)\right] \bmod \Lambda, \tag{25}$$

where Q denotes the quantization with respect to Λ_f. Finally, the relay maps $\underline{\hat{v}}_m^R$ and $\underline{\hat{v}}_m^I$ to $\underline{\hat{f}}_m^R$ and $\underline{\hat{f}}_m^I$, respectively, via $\tilde{\psi}^{-1}$,

$$\tilde{\psi}^{-1}(\underline{v}) = \left(\mathbf{G}^T\mathbf{G}\right)^{-1}\mathbf{G}^T g^{-1}\left(q\left(\left[\mathbf{B}^{-1}\underline{v} \bmod \Lambda\right]\right)\right), \tag{26}$$

where $\underline{v} \in \mathbb{F}_q^n$. Hence,

$$\tilde{\psi}^{-1}\left(\underline{\hat{v}}_m^R\right) = \underline{\hat{f}}_m^R = \bigoplus_{l=1}^{L}\left(b_{ml}^R\underline{\hat{w}}_l^R \oplus \left(-b_{ml}^I\right)\underline{\hat{w}}_l^I\right), \tag{27}$$

$$\tilde{\psi}^{-1}\left(\underline{\hat{v}}_m^I\right) = \underline{\hat{f}}_m^I = \bigoplus_{l=1}^{L}\left(b_{ml}^I\underline{\hat{w}}_l^R \oplus \left(b_{ml}^R\right)\underline{\hat{w}}_l^I\right), \tag{28}$$

where

$$b_{ml}^R = \Re\left(a_{ml}\right) \bmod q, \tag{29}$$

$$b_{ml}^I = \Im\left(a_{ml}\right) \bmod q. \tag{30}$$

Note that both $[\underline{b}_1^R, \ldots, \underline{b}_M^R]$ and $[\underline{b}_1^I, \ldots, \underline{b}_M^I]$ are required to be full rank so that decoding each $\underline{w}_l^R, \underline{w}_l^I$ at the final destination is feasible.

In [11], Nazer and Gastpar show the following theorem using the coding scheme we have described in this section.

Theorem 11 (Nazer and Gastpar): At relay m, given $\underline{h}_m \in \mathbb{C}^L$ and $\underline{a}_m \in \mathbb{Z}[i]^L$, a computation rate of

$$\mathcal{R}(\underline{h}_m, \underline{a}_m) = \log^+\left(\left(\|\underline{a}_m\|^2 - \frac{P|\underline{h}_m^H\underline{a}_m|^2}{1+P\|\underline{h}_m\|^2}\right)^{-1}\right), \tag{31}$$

is achievable.

Given $\mathbf{H}$ and assuming that the relays do not cooperate with each other, each relay would attempt to pick an integer vector $\underline{a}_m$ that maximizes its individual computation rate, i.e. $\underline{a}_m = \arg\max_{\underline{a}\in\mathbb{Z}[i]^L} \mathcal{R}(\underline{h}_m, \underline{a}_m)$ in order to maximize $\mathcal{R}(\mathbf{H}, \mathbf{A})$.

V. Compute-and-Forward with Lattices over Eisenstein Integers

The main result in this section is that for some channel realizations, higher information rates than those in Theorem 11 are achievable. The improved information rate is obtained by considering nested lattices over Eisenstein integers which allow the mth relay to decode a linear combination of the form $\sum_{l=1}^{L} a_{ml}\underline{t}_l$, where $a_{ml} \in \mathbb{Z}[\omega]$. This result is made precise in Theorem 15.

One of the key challenges in proving this achievability result is to show the existence of nested lattices over Eisenstein integers, which we refer to as $\mathbb{Z}[\omega]$-lattices, where the coarse lattice is good for covering and the fine lattice can achieve the Poltyrev limit. We would like to note that, we do not prove the existence of $\mathbb{Z}[\omega]$-lattices that are good for AWGN channel coding, i.e. lattices for which the error probability can be bounded exponentially in n, in this paper. Furthermore, we do not require the coarse lattice in the sequence of nested lattices to be simultaneously good for AWGN channel coding and good for covering. In order to state our main theorem, it suffices to show the existence of nested $\mathbb{Z}[\omega]$-lattices where the coarse lattice is good for covering and the fine lattice can achieve the Poltyrev limit. A similar result is obtained in [20], where the coarse lattice is chosen to be good only for quantization and the fine lattice to be good for AWGN channel coding in order to achieve $\frac{1}{2}\log(1+SNR)$ using lattice codes for the point-to-point AWGN channel.

In what follows, we first provide some preliminaries about Eisenstein integers and summarize Construction A for $\mathbb{Z}[\omega]$-lattices. Afterwards, we show that nested $\mathbb{Z}[\omega]$-lattices where the coarse lattice is good for quantization and the fine lattice achieves the Poltyrev limit can be obtained through Construction A. The existence result can then be used to prove Theorem 15, which is the main result of this paper. Since $\mathbb{Z}[\omega]$ quantizes $\mathbb{C}$ better than $\mathbb{Z}[i]$, on the average (over the channel realizations), higher information rates are achievable by using $\mathbb{Z}[\omega]$-lattices compared to using $\mathbb{Z}$-lattices. The superiority of the proposed scheme will be further confirmed in Section VI where we provide numerical results to compare the outage performance and error-correcting performance of lattices over natural integers and lattices over Eisenstein integers in compute-and-forward.

A. Preliminaries: Eisenstein Integers

An Eisenstein integer is a complex number of the form $a + b\omega$ where $a, b \in \mathbb{Z}$ and $\omega = -\frac{1}{2} + j\frac{\sqrt{3}}{2}$. The ring

of Eisenstein integers $\mathbb{Z}[\omega]$ is a principal ideal domain, i.e, a commutative ring without zero divisors where every ideal can be generated by a single element. Other well-known principal ideal domains are $\mathbb{Z}$ and $\mathbb{Z}[i]$. A *unit* in $\mathbb{Z}[\omega]$ is one of the following:$\{\pm 1, \pm\omega, \pm\omega^2\}$. An Eisenstein integer ϱ is an Eisenstein prime if either one of the following mutually exclusive conditions hold [21]:

1) ϱ is equal to the product of a unit and any natural prime congruent to $2 \bmod 3$.
2) $|\varrho|^2 = 3$ or $|\varrho|^2$ is any natural prime congruent to $1 \bmod 3$.

An n-dimensional $\mathbb{Z}[\omega]$-lattice can be written in terms of a complex lattice generator matrix $\mathbf{B} \in \mathbb{C}^{n\times k}$:

$$\Lambda = \{\underline{\lambda} = \mathbf{B}\underline{e} : \underline{e} \in \mathbb{Z}[\omega]^k\} \tag{32}$$

B. Construction A for $\mathbb{Z}[\omega]$-lattices

Let ϱ be an Eisenstein prime with $|\varrho|^2 = q$. Since $\mathbb{Z}[\omega]$ is a principal ideal domain, $\varrho\mathbb{Z}[\omega]$ is an ideal of $\mathbb{Z}[\omega]$ and together they form the quotient ring $\mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$. Moreover, since ϱ is an Eisenstein prime, $\varrho\mathbb{Z}[\omega]$ is a prime ideal and hence a maximal ideal (a property for principal ideal domains). Thus, the quotient ring is isomorphic to a field

$$\mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega] \cong \mathbb{F}_q. \tag{33}$$

i.e., there exists a ring isomorphism $\sigma : \mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega] \to \mathbb{F}_q$ [22, page 118]. Note that $\mathbb{Z}[\omega]$ is the union of q cosets of $\varrho\mathbb{Z}[\omega]$

$$\mathbb{Z}[\omega] = \bigcup_{s\in\mathcal{S}} (\varrho\mathbb{Z}[\omega] + s) \tag{34}$$

where $\mathcal{S}$ represents the set of q coset leaders of $\mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$. One has the canonical ring homomorphism [22, page 118] $\bmod \varrho\mathbb{Z}[\omega] : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$ to homomorphically map an element in $\mathbb{Z}[\omega]$ to its coset leader. Now composing $\bmod \varrho\mathbb{Z}[\omega]$ and σ, one obtains the ring homomorphism $\tilde{\sigma} \triangleq \sigma \circ \bmod \varrho\Lambda : \mathbb{Z}[\omega] \to \mathbb{F}_q$. Note that $\tilde{\sigma}$ can be extended to vectors in a straightforward manner by mapping the elements of the vector componentwise to another vector [14, page 197]. We would like to mention that the aforementioned properties also hold for lattices that are constructed over any other principal ideal domain such as $\mathbb{Z}$ or $\mathbb{Z}[i]$. For example, the $\bmod q$ operation in Construction A for $\mathbb{Z}$-lattices also provides a ring homomorphism. We now define Construction A for $\mathbb{Z}[\omega]$-lattices as follows.

Let ϱ be an Eisenstein prime and $q = |\varrho|^2$. Note that q is either a natural prime or the square of a natural prime. Also let k, n be integers such that $k \le n$ and let $\mathbf{G} \in \mathbb{F}_q^{n\times k}$. Similar to a $\mathbb{Z}$-lattice, a $\mathbb{Z}[\omega]$-lattice can be obtained by Construction A [14].

1) Define the discrete codebook $\mathcal{C} = \{\underline{x} = \mathbf{G}\underline{y} : \underline{y} \in \mathbb{F}_q^k\}$ where all operations are over $\mathbb{F}_q$. Thus, $\underline{x} \in \mathbb{F}_q^n$.
2) Generate the n-dimensional $\mathbb{Z}[\omega]$-lattice $\Lambda_{\mathcal{C}}$ as $\Lambda_{\mathcal{C}} \triangleq \{\lambda \in \mathbb{Z}[\omega]^n : \tilde{\sigma}(\lambda) \in \mathcal{C}\}$.
3) Scale $\Lambda_{\mathcal{C}}$ with ϱ^{-1} to obtain $\Lambda = \varrho^{-1}\Lambda_{\mathcal{C}}$.

Once again, we would like to note that only the first two steps that we have stated in Construction A is required to build a $\mathbb{Z}[\omega]$-lattice. However,due to the fact that we will prove the existence of $\mathbb{Z}[\omega]$-lattices that are good for covering in this paper using similar proof techniques in [5], we also require the third step which scales the lattice. An example of such a construction with $k = 1, n = 1, \mathbf{G} = [1]$, $\varrho = 2 - \sqrt{3}j$, $q = 7$ and the corresponding ring homomorphism is shown in Fig. 2. In this figure, the green circles represent $\varrho\mathbb{Z}[\omega]$ and the red lines represent the boundaries of their Voronoi regions. It can be observed that there are exactly $q = |\varrho|^2 = 7$ lattice points that belong to $\mathbb{Z}[\omega]$ that lie within each Voronoi region of the lattice points that belong to $\varrho\mathbb{Z}[\omega]$. It can also be verified that the mapping (labeling) in Fig. 2 from $\mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$ to $\mathbb{F}_q$, i.e., $\tilde{\sigma}$ is indeed a ring homomorphism. We would like to note that the lattice in Fig. 2 is trivially $\mathbb{Z}[\omega]$. Unfortunately, we were not able to provide a less trivial figure with a larger dimensional $\mathbb{Z}[\omega]$-lattice. This is due to the fact that even a two-dimensional $\mathbb{Z}[\omega]$-lattice requires four real dimensions to be drawn, which is not feasible.

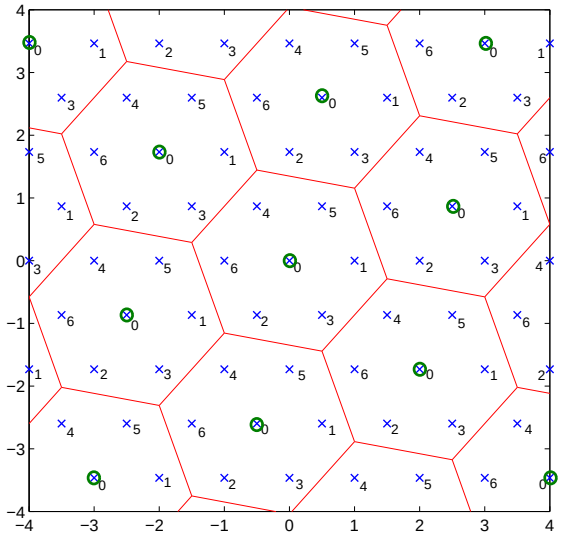

Fig. 2. $\Lambda_{\mathcal{C}}$ with $\mathbf{G} = [1]$ and the corresponding ring homomorphism

Given n, k, q, we define an $(n, k, q, \mathbb{Z}[\omega])$ ensemble as the set of $\mathbb{Z}[\omega]$-lattices obtained through Construction-A where for each of these lattices, $\mathbf{G}_{ij}$ are i.i.d with a uniform distribution over $\mathbb{F}_q$.

Theorem 12: A lattice Λ drawn from an $(n, k, q, \mathbb{Z}[\omega])$ ensemble, where $k < n$ but grows faster than $\log^2 n$, q is a natural prime congruent to $1 \bmod 3$, and where k, q satisfy

$$\begin{aligned} q^k &= \frac{\left(\frac{\sqrt{3}}{2}\right)^n}{V_{\mathcal{B}}\left(r_\Lambda^{\text{eff}}\right)} = \frac{\left(\frac{\sqrt{3}}{2}\right)^n \Gamma(n+1)}{\pi^n \left(r_\Lambda^{\text{eff}}\right)^{2n}} \\ &\approx \sqrt{2n\pi}\left(\frac{\sqrt{3}}{2}\right)^n \left(\frac{2n}{2\exp(1)\left(r_\Lambda^{\text{eff}}\right)^2}\right)^n, \end{aligned} \tag{35}$$

and

$$r_{min} < r_\Lambda^{\text{eff}} < 2r_{min}, \tag{36}$$

where $0 < r_{min} < \frac{1}{4}$, is good for covering, i.e,

$$\frac{r_{\Lambda^{\text{cov}}}}{r_{\Lambda}^{\text{eff}}} \to 1, \tag{37}$$

in probability as $n \to \infty$.

Proof: We would like to note that the steps we follow in this proof are similar to the proof of Theorem 2 in [5]. The most important differences are as follows. Instead of considering the lattice points that lie within the fundamental Voronoi region of the lattice $\mathbb{Z}^n$, which is an n-dimensional unit cube, we consider the lattice points that lie within the fundamental Voronoi region of the lattice $\mathbb{Z}[\omega]^n$, which is an n-dimensional hexagon. Furthermore, since we are constrained to q congruent to $1 \bmod 3$, Bertrand's postulate is not sufficient to show the existence of such q that satisfies (35) and (36) as k grows. Therefore, we use the result in [23] to show such prime numbers exist. For the rest of the proof, see Appendix B. ∎

We would like to note that a variant of Theorem 12 can also be proven for q congruent to $2 \bmod 3$, which in this case we can construct Λ from linear codes over $\mathbb{F}_{q^2}$.

Corollary 13: A lattice Λ drawn from an $(n, k, q, \mathbb{Z}[\omega])$ ensemble, where $k < n$ but grows faster than $\log^2 n$ and where k, q satisfy (35) and (36) is good for quantization, i.e.,

$$G(\Lambda) \to \frac{1}{2\pi e}, \tag{38}$$

in probability as $n \to \infty$.

Proof: It was shown in [16] that a lattice ensemble which is good for covering is necessarily good for quantization. Thus from Theorem 12, the result follows. ∎

C. Nested $\mathbb{Z}[\omega]$-lattices obtained from Construction-A

Nested $\mathbb{Z}[\omega]$-lattices can be obtained from Construction-A very similar to $\mathbb{Z}$-lattices as mentioned in Section III-B. The coarse lattice Λ is obtained through Construction-A as mentioned in Section V-B with a corresponding generator matrix $\mathbf{B}$. For a given $\mathbf{G} \in \mathbb{F}_q^{n \times k}$, denote Λ' as the corresponding $\mathbb{Z}[\omega]$-lattice obtained through Construction-A using $\mathbf{G}$ as the generator matrix of the underlying linear code. Generate the $\mathbb{Z}[\omega]$-lattice Λ_f as $\Lambda_f = \mathbf{B}\Lambda'$. It can be observed that $\Lambda \subset \Lambda_f$ with a coding rate of $\frac{k}{2n} \log q$. Given $n,\ k,\ q$ and Λ where Λ is a $\mathbb{Z}[\omega]$-lattice obtained from Construction-A, we define the $(n, k, q, \Lambda, \mathbb{Z}[\omega])$ ensemble as the set of lattices obtained from Λ and Construction-A as previously mentioned where for each of these lattices, the elements of the generator matrix of the underlying linear code $\mathbf{G}_{ij}$ is i.i.d with a uniformly distribution over $\mathbb{F}_q$.

Theorem 14: There exists a pair of nested $\mathbb{Z}[\omega]$-lattices where the coarse lattice is good for covering and the fine lattice achieves the Poltyrev limit.

Proof: For this proof, we build nested $\mathbb{Z}[\omega]$-lattices as mentioned above. Using our result from Theorem 12, we pick a coarse lattice Λ which is good for covering. We then pick Λ_f from the $(n, k, q, \Lambda, \mathbb{Z}[\omega])$ ensemble as described in Section V-C and show that the Minkowski-Hlawka theorem can be proven for this ensemble [4]. We would like to note that the steps we follow are very similar to the steps followed in [4]. Some of the important differences are as follows. Since we are constructing $\mathbb{Z}[\omega]$-lattices, we consider the fundamental Voronoi region of the lattice $\mathbb{Z}[\omega]^n$ which has a volume of $\left(\frac{\sqrt{3}}{2}\right)^n$. Therefore this should be taken into account when $\text{Vol}\left(\mathcal{V}_{\Lambda_f}\right)$ is kept constant as $n \to \infty$. In the detailed proof provided in Appendix C, it can be observed that a lattice Λ_f picked from the $(n, k, q, \Lambda, \mathbb{Z}[\omega])$ ensemble achieves the Poltyrev limit as long as the generator matrix $\mathbf{B}$ of Λ is full rank. We would like to note that this result is a generalized version of what was stated in [4] where $\mathbf{B}$ was assumed to be an identity matrix. One of the consequences of picking an arbitrary full rank matrix $\mathbf{B}$ would be that $\mathcal{V}_\Lambda$ might stretch out in some dimensions while shrinking in others. Nonetheless, since the growth of q in Theorem 12 ensures that $q \to \infty$, there is exactly one element in the kernel of $\tilde{\sigma}$ contained in the bounded region, i.e., the left term of (114) vanishes, and the result holds. ∎

Now, we are ready to state the main theorem in the paper.

Theorem 15: At relay m, given $\underline{h}_m$ and $\underline{a}_m$, a computation rate of

$$\mathcal{R}(\underline{h}_m, \underline{a}_m) = \log^+\left(\left(\|\underline{a}_m\|^2 - \frac{P|\underline{h}_m^H \underline{a}_m|^2}{1 + P\|\underline{h}_m\|^2}\right)^{-1}\right), \tag{39}$$

where $\underline{a}_{ml} \in \mathbb{Z}[\omega]$, is achievable.

Proof:

We would like to note that the steps we follow in this proof are very similar to the proof of Theorem 5 in [11]. Nonetheless, there are some important differences we would like to point out. Since a_{ml} are Eisenstein integers in our framework, their real and imaginary components are not independent and we cannot use a real and imaginary decomposition as in [11]. Therefore, the channel coefficients and channel noise cannot be decomposed into real and imaginary components either. Due to this, we are constrained to employ $\mathbb{Z}[\omega]$-lattices in our framework. Furthermore, in order to obtain b_{ml} from a_{ml}, we use a ring homomorphism σ, which can be thought of as the equivalent of a modulo operation for $a_{ml} \in \mathbb{Z}$. We would also like to mention that this proof can be trivially extended to the case where information vectors at transmitters have different lengths by considering a sequence of nested lattice codes. We proceed as follows.

Using the result from Theorem 14, a fine $\mathbb{Z}[\omega]$-lattice Λ_f and a coarse $\mathbb{Z}[\omega]$-lattice Λ, which is nested in Λ_f with a corresponding coding rate $\frac{R}{2} = \frac{k}{2n} \log q$, is chosen such that Λ_f achieves the Poltyrev limit and Λ is good for covering. Both Λ and Λ_f are scaled such that $\sigma_\Lambda^2 = P$. Following this, the lattice codebook $\Lambda_f \cap \mathcal{V}_\Lambda$ is constructed.

Source node l maps its information vector $\underline{w}_l \in \mathbb{F}_q^k$, where $q = |\varrho|^2$ and ϱ is an Eisenstein prime, to a lattice codeword $\underline{t}_l \in \Lambda_f \cap \mathcal{V}_\Lambda$, respectively, via a bijective mapping ψ,

$$\underline{t}_l = \psi(\underline{w}) = \left[\mathbf{B}\varrho^{-1}\sigma^{-1}(\mathbf{G}\underline{w})\right], \tag{40}$$

where σ was defined in Section V-B. It then constructs a dither vector $\underline{d}_l$, which is uniformly distributed within $\mathcal{V}_\Lambda$ and subtracts this dither vector from the lattice codeword $\underline{t}_l$ and

transmits the following:

$$\underline{x}_l = [\underline{t}_l - \underline{d}_l] \bmod \Lambda. \tag{41}$$

Given a channel coefficient vector $\underline{h}_m \in \mathbb{C}^L$, relay m observes

$$\underline{y}_m = \sum_{l=1}^{L} h_{ml}\underline{x}_l + \underline{z}_m. \tag{42}$$

The relay approximates $\underline{h}_m$, in some sense, by an Eisenstein integer vector $\underline{a}_m \in \mathbb{Z}[\omega]^L$ and its goal will be to recover the following:

$$\underline{v}_m = \left[\sum_{l=1}^{L}(a_{ml}\underline{t}_l)\right] \bmod \Lambda. \tag{43}$$

It proceeds by removing the dithers and scaling the observation with α_m, and therefore,

$$\underline{\tilde{y}}_m = \alpha_m \underline{y}_m + \sum_{l=1}^{L} a_{ml}\underline{d}_l, \tag{44}$$

where α_m is the MMSE coefficient.

Then $\underline{\tilde{y}}_m$ is quantized to the closest lattice point in the fine lattice Λ_f modulo the coarse lattice Λ and estimates the following:

$$\underline{\hat{v}}_m = \left[Q_{\Lambda_f}\left(\underline{\tilde{y}}_m\right)\right] \bmod \Lambda, \tag{45}$$

where Q_{Λ_f} denotes the quantization with respect to Λ_f. The remaining steps of the proof would be identical to the steps in the proof of Theorem 5 in [11] with the only difference being as follows. The relay maps $\underline{\hat{v}}_m$ to $\underline{\hat{f}}_m$ via ψ^{-1}, where

$$\psi^{-1}\left(\underline{\hat{v}}_m\right) = \underline{\hat{f}}_m = \left(\mathbf{G}^T\mathbf{G}\right)^{-1}\mathbf{G}^T\sigma\left(\varrho\left(\left[\mathbf{B}^{-1}\underline{\hat{v}}_m \bmod \Lambda\right]\right)\right) = \bigoplus_{l=1}^{L} b_{ml}\underline{\hat{w}}_l, \tag{46}$$

and $b_{ml} = \sigma(a_{ml})$.

Due to the fact that Λ is good for covering and the dithers are uniformly distributed in $\mathcal{V}_\Lambda$, the probability density function of the equivalent noise $\underline{z}_{eq,m}$ is upper-bounded by a zero-mean complex Gaussian with a variance that approaches $|\alpha_m|^2 + P||\alpha_m\underline{h}_m - \underline{a}_m||^2$ multiplied by a constant as $n \to \infty$ ([11, Lemma 8]). We would like to note that the error probability $\Pr\left(\underline{z}_{eq} \notin \mathcal{V}_{\Lambda_f}\right)$ goes to zero as $n \to \infty$, however this decay is not necessarily exponential in n, since we have only proven the existence of $\mathbb{Z}[\omega]$-lattices which achieve the Poltyrev limit and this result does not provide information about the error exponents of such lattices. Nonetheless, it is sufficient to achieve the computation rate in (39). ■

Given $\mathbf{H}$ and assuming that the relays do not cooperate with each other, each relay would attempt to pick $\underline{a}_m \in \mathbb{Z}[\omega]^L$ that maximizes its individual computation rate, i.e. $\underline{a}_m = \underset{\underline{a}\in\mathbb{Z}[\omega]^L}{\arg\max}\, \mathcal{R}(\underline{h}_m, \underline{a}_m)$ in order to maximize $\mathcal{R}(\mathbf{H}, \mathbf{A})$. A straightforward method to determine the optimal $\underline{a}_m$ would be to employ an exhaustive search over all $\underline{a}_m$ that satisfies $\|\underline{a}_m\|^2 < 1 + \|\underline{h}_m\|^2 P$ ([11, Lemma 1]). One major challenge in the compute-and-forward paradigm is that for large P and L, exhaustively searching optimal $\underline{a}_m$ becomes infeasible. Nonetheless, this problem can be molded into a different form which enables the utilization of much more efficient algorithms (see [12] for $\mathbb{Z}[i]$ and [13] for $\mathbb{Z}[\omega]$ for example.) In the following subsection, we review this approach for the sake of completeness.

D. An efficient algorithm for choosing $\underline{a}_m$

As can be seen in ([11]), upon scaling $\underline{y}_m$ with the MMSE coefficient α_m, the effective noise variance at relay m, which we denote as $\sigma^2_{\text{eff},m}$, can be computed as

$$\sigma^2_{\text{eff},m} = |\alpha_m|^2 + P\|\alpha_m\underline{h}_m - \underline{a}_m\|^2, \tag{47}$$

where

$$\alpha_m = \frac{P\underline{h}_m^H\underline{a}_m}{1 + \|\underline{h}_m\|^2}. \tag{48}$$

Furthermore, the achievable computation rate at each relay can be expressed in terms of P and $\sigma^2_{\text{eff},m}$ as

$$\mathcal{R}\left(\underline{h}_m, \underline{a}_m\right) = \log^+\left(\frac{P}{\sigma^2_{\text{eff},m}}\right). \tag{49}$$

Therefore,

$$\underset{\underline{a}_m\in\mathbb{Z}[\omega]^L}{\arg\max}\, \mathcal{R}\left(\underline{h}_m, \underline{a}_m\right) = \underset{\underline{a}_m\in\mathbb{Z}[\omega]^L}{\arg\min}\, \sigma^2_{\text{eff},m}. \tag{50}$$

We now take a closer look at $\sigma^2_{\text{eff},m}$. Substituting (48) in (47), it can be observed that

$$\begin{aligned}\sigma^2_{\text{eff},m} &= P\underline{a}_m^H\underline{a}_m - \frac{P^2\underline{a}_m^H\underline{h}_m\underline{h}_m^H\underline{a}_m}{1 + P\|\underline{h}_m\|^2} \\ &= P\underline{a}_m^H\left(\mathbf{I} - \frac{P\underline{h}_m\underline{h}_m^H}{1 + P\|\underline{h}_m\|^2}\right)\underline{a}_m\end{aligned} \tag{51}$$

Due to the Matrix Inversion Lemma [24],

$$\mathbf{I} - \frac{P\underline{h}_m\underline{h}_m^H}{1 + P\|\underline{h}_m\|^2} = \left(I + P\underline{h}_m\underline{h}_m^H\right)^{-1}, \tag{52}$$

and $\sigma^2_{\text{eff},m}$ can be expressed as

$$\sigma^2_{\text{eff},m} = P\underline{a}_m^H\left(I + P\underline{h}_m\underline{h}_m^H\right)^{-1}\underline{a}_m. \tag{53}$$

Note that $\left(I + P\underline{h}_m\underline{h}_m^H\right)$, which we denote as $\mathbf{S}$, is a Hermitian matrix. Therefore, the singular value decomposition of $\mathbf{S}$ can be expressed as $\mathbf{V}\mathbf{D}\mathbf{V}^H$, where $\mathbf{D}$ is a diagonal matrix which has the eigenvalues of $\mathbf{S}$ as non-zero entries and $\mathbf{V}$ is an orthogonal matrix which has the corresponding eigenvectors of $\mathbf{S}$ in its columns. Hence,

$$\begin{aligned}\sigma^2_{\text{eff},m} &= P\underline{a}_m^H\left(\mathbf{V}\mathbf{D}^{-1}\mathbf{V}^H\right) \\ &= P\|\mathbf{D}^{-1/2}\mathbf{V}^H\underline{a}_m\|^2,\end{aligned} \tag{54}$$

and therefore it can be concluded that

$$\underset{\underline{a}_m\in\mathbb{Z}[\omega]^L}{\arg\min}\, \sigma^2_{\text{eff},m} = \underset{\underline{a}_m\in\mathbb{Z}[\omega]^L}{\arg\min}\, \|\mathbf{D}^{-1/2}\mathbf{V}^H\underline{a}_m\|^2. \tag{55}$$

Thus, the search in (55) is equivalent to finding the non-zero minimal Euclidean norm point generated by $\mathbf{D}^{-1/2}\mathbf{V}^H$

as a $\mathbb{Z}[\omega]$-lattice, which is commonly referred to as the shortest vector problem (SVP). For reasonable values of L, e.g. $L \leq 32$, one of the shortest lattice vectors can be found via a Pohst enumeration or a Schnorr-Euchner enumeration in a way similar to standard sphere decoding [25][26]. A polynomial-time method to approximate (55) is based on LLL reduction [27]. For our lattices, an LLL over $\mathbb{Z}[\omega]$ should be used as devised by Napias for Euclidean rings [28] including both $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$. Also in [29], LLL has been proposed in a different methodology with no singular value decomposition of $\mathbf{S}$. Finding approximately optimal $\underline{a}_m$ efficiently is an active research area. The interested reader is referred to [30] and the references therein.

VI. Numerical Results

In this section, we present some numerical results on the achievable computation rates with $\mathbb{Z}[\omega]$-lattices and compare them to the maximum achievable rates with $\mathbb{Z}$-lattices. We consider the case of $L = 2$ transmitters and there is $M = 1$ relay. For a given channel coefficient vector $\underline{h}$, let $\mathcal{R}_E(\underline{h})$ and $\mathcal{R}_G(\underline{h})$, denote the maximum achievable rate using $\mathbb{Z}[\omega]$-lattices and $\mathbb{Z}$-lattices, respectively, i.e.,

$$\mathcal{R}_E(\underline{h}, P) = \max_{\underline{a} \in \mathbb{Z}[\omega]^2} \log^+ \left(\left(\|\underline{a}\|^2 - \frac{P|\underline{h}^H \underline{a}|^2}{1 + P\|\underline{h}\|^2} \right)^{-1} \right), \quad (56)$$

and

$$\mathcal{R}_G(\underline{h}, P) = \max_{\underline{\tilde{a}} \in \mathbb{Z}[i]^2} \log^+ \left(\left(\|\underline{\tilde{a}}\|^2 - \frac{P|\underline{h}^H \underline{\tilde{a}}|^2}{1 + P\|\underline{h}\|^2} \right)^{-1} \right). \quad (57)$$

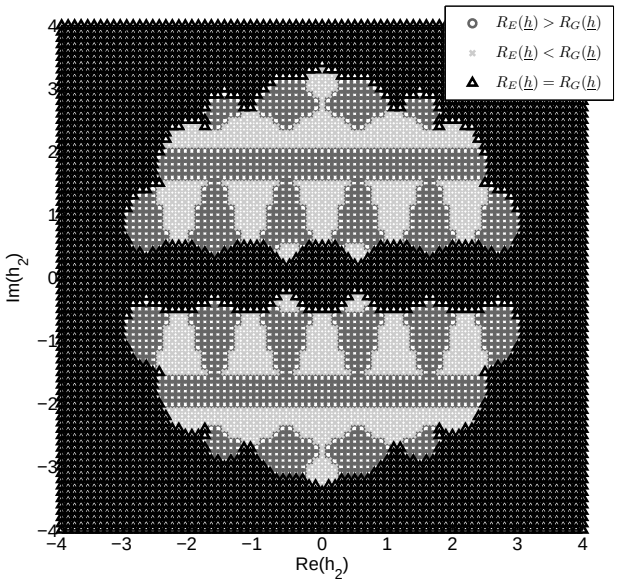

Fig. 3. Regions of $\Re(h_2), \Im(h_2)$ where $\mathcal{R}_G(\underline{h}, P) > \mathcal{R}_E(\underline{h}, P)$, $\mathcal{R}_G(\underline{h}, P) < \mathcal{R}_E(\underline{h}, P)$ or $\mathcal{R}_G(\underline{h}, P) = \mathcal{R}_E(\underline{h}, P)$: SNR=10 dB

In Fig. 3, we fix $h_1 = 1$ and choose h_2 such that $\Re(h_2), \Im(h_2) \in [-4, 4]$. We would also like to note that we do not impose a probability distribution on h_2. For each pair $(h_1 = 1, h_2)$, we plot the region where $\mathcal{R}_G(\underline{h}) > \mathcal{R}_E(\underline{h})$, $\mathcal{R}_G(\underline{h}) < \mathcal{R}_E(\underline{h})$ or $\mathcal{R}_G(\underline{h}) = \mathcal{R}_E(\underline{h})$. For the total number of realizations considered, $\mathcal{R}_E > \mathcal{R}_G$, $\mathcal{R}_E < \mathcal{R}_G$. and $\mathcal{R}_E = \mathcal{R}_G$ for 22.6%, 15.9%, and 61.5% of the realizations, respectively. One might expect that $\mathbb{Z}[\omega]$-lattices would attain a greater maximum achievable rate when h_2 is closer to an Eisenstein integer, $\mathbb{Z}$-lattices would attain a greater maximum achievable rate when h_2 is closer to a Gaussian integer and both lattices would achieve the same maximum achievable rate when h_2 is closer to a natural integer. However as seen from Fig. 3, other factors also contribute to the maximum achievable rate. For example when $\|h_2\| \gg \|h_1\|$ or $\|h_2\| \ll \|h_1\|$, the relay chooses $a_1 = 0, \|a_2\| = 1$ or $\|a_1\| = 1, \|a_2\| = 0$, respectively since treating the other transmitted signal as noise (decode-and-forward) results in maximum achievable rate. Also, the MMSE scaling coefficient α plays a very important role as seen in (22), (23) and (44). Note that (56) and (57) can be written as

$$\mathcal{R}_E(\underline{h}, P) = \max_{\underline{a} \in \mathbb{Z}[\omega]^2} \log^+ \left(\frac{1 + P\|\underline{h}\|^2}{\|\underline{a}\|^2 + P\left(\|\underline{a}\|^2 \|\underline{h}\|^2 - |\underline{h}^H \underline{a}|^2 \right)} \right) \quad (58)$$

and

$$\mathcal{R}_G(\underline{h}, P) = \max_{\underline{\tilde{a}} \in \mathbb{Z}[i]^2} \log^+ \left(\frac{1 + P\|\underline{h}\|^2}{\|\tilde{a}\|^2 + P\left(\|\underline{\tilde{a}}\|^2 \|\underline{h}\|^2 - |\underline{h}^H \underline{\tilde{a}}|^2 \right)} \right), \quad (59)$$

respectively.

As one can see from the denominators in (58) and (59), it is desirable to align $\underline{a}$ ($\underline{\tilde{a}}$) with $\underline{h}$ as much as possible in order to minimize the second term. However, when $\underline{h} \notin \mathbb{Z}[i]^2$,$\underline{h} \notin \mathbb{Z}[\omega]^2$, or the elements of $\underline{h}$ cannot be written as the ratio of Gaussian integers or Eisenstein integers, or $\underline{h}$ is not a rotated version of a Gaussian integer vector or Eisenstein integer vector, $\|\underline{a}\| \to \infty$ ($\|\underline{\tilde{a}}\| \to \infty$) for perfect alignment. Unfortunately, this results in the first term of the denominator to grow and hence there is a tradeoff. Therefore even though h_2 might be closer to an Eisenstein integer (Gaussian integer), i.e. $\underline{h}$ is aligned better with a vector in $\mathbb{Z}[i]^2$ ($\mathbb{Z}[\omega]^2$), the magnitude of this vector might be too large and thus a larger computation rate may be achieved by choosing $\underline{a} \in \mathbb{Z}[i]^2$ ($\underline{\tilde{a}} \in \mathbb{Z}[\omega]^2$).

In Fig. 4, we fix the channel realization to be $\underline{h} = [1.4193 + j0.2916; 0.1978 + j1.5877]$ and compare $\mathcal{R}_E(\underline{h}, P)$, $\mathcal{R}_G(\underline{h}, P)$ for different SNRs. For this particular $\underline{h}$, it can be observed that $\mathbb{Z}[\omega]$-lattices can achieve substantially higher rates than $\mathbb{Z}$-lattices in the medium SNR regime. We would like to note that this is not necessarily the case for every channel realization, nonetheless it is a perfect example of how channel realizations affect the performance of $\mathbb{Z}[\omega]$-lattices and $\mathbb{Z}$-lattices. Therefore, a larger number of channel realizations should be considered in order to make a fair comparison of their performance in the average sense.

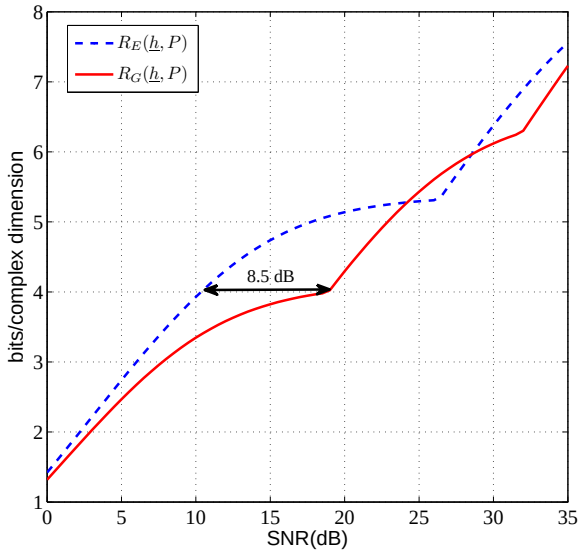

Fig. 4. A comparison of $\mathcal{R}_E(\underline{h}, P)$ and $\mathcal{R}_G(\underline{h}, P)$ for $\underline{h} = [1.4193 + j0.2916; 0.1978 + j1.5877]$

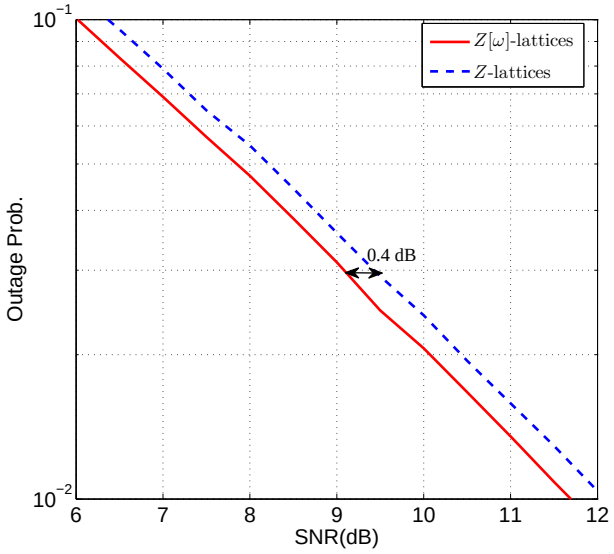

Fig. 5. Outage Probability of $\mathbb{Z}[\omega]$ Lattices vs $\mathbb{Z}$ Lattices

A. Outage performance comparison of $\mathbb{Z}$-lattices vs. $\mathbb{Z}[\omega]$-lattices in compute-and-forward

In this subsection, we compare the outage performance lattice codes over $\mathbb{Z}$ and lattice codes over $\mathbb{Z}[\omega]$ for compute-and-forward. Given a target rate R_T and a probability distribution $\mathcal{P}$ on $\underline{h}$, i.e. $\underline{h} \sim \mathcal{P}$, we define the outage event of using $\mathbb{Z}$-lattices and $\mathbb{Z}[\omega]$-lattices as $\mathcal{R}_G(\underline{h}) < R_T$ and $\mathcal{R}_E(\underline{h}) < R_T$, respectively. In Fig. 5, we plot the outage probability with $\mathbb{Z}[\omega]$-lattices and $\mathbb{Z}$-lattices as a function of SNR (P) where $\Re(h_1), \Im(h_1), \Re(h_2), \Im(h_2) \sim \mathcal{N}(0, 1)$. We average over 100000 realizations of $\underline{h}$ at each SNR and choose the target rate to be $R_T = 1/2 \log_2 7$ bits/symbol/Hz. As seen in Fig. 5, there is a 0.4 dB gain from using $\mathbb{Z}[\omega]$-lattices instead of $\mathbb{Z}$-lattices in terms of outage performance. We would like to note that this gain comes with no additional computational complexity.

B. Error correcting capability of $\mathbb{Z}$-lattices vs. $\mathbb{Z}[\omega]$-lattices in compute-and-forward

In this subsection, we compare the error-correcting capability of lattice codes over $\mathbb{Z}$ and lattice codes over $\mathbb{Z}[\omega]$ for compute-and-forward. Before we do that, we would like to point out that in general, the nested lattice shaping adopted in the previous sections is very difficult to be implemented. In fact, it is equivalent to the SVP and hence is NP-hard. In practice, one could trade performance for complexity by considering the use of hypercube shaping. Then the proposed scheme would reduce to the concatenation of a linear code over $\mathbb{F}_q$ with a constellation corresponding to a set of minimum energy coset leaders of the quotient ring $\mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$ (or $\mathbb{Z}/q\mathbb{Z}$). In the following, we compare the error-correcting capability for this practical scheme.

In order to construct a lattice code over Eisenstein integers, we have used a rate 1/2, regular (3,6), uniformly distributed edge weight, length 10000 LDPC code over $\mathbb{F}_{25}$ and mapped each codeword component to the constellation carved from $\mathbb{Z}[\omega]/5\mathbb{Z}[\omega]$ via a ring homomorphism. In order to construct a lattice code over natural integers, we have used a rate 1/2, regular (3,6), uniformly distributed edge weight, length 10000 LDPC code over $\mathbb{F}_5$ and mapped each codeword component to the coset leaders of the quotient ring $\mathbb{Z}/5\mathbb{Z}$, i.e. $\{-2, -1, 0, 1, 2\}$. Note that for the lattice code over natural integers, we consider $\mathbb{F}_5$ due to the real and imaginary decomposition. We have generated 100000 channel realizations, used these channel realizations over a range of SNR, and we have plotted the average symbol error probability of these lattice codes for the compute-and-forward framework. As seen in Fig. 6 simulation results show that lattice codes over Eisenstein integers outperform lattice codes over integers by roughly 0.4 dB, which is consistent with our outage simulation results.

VII. Conclusion

In this paper, we have shown the existence of lattices over Eisenstein integers that are simultaneously good for quantization and that achieve the Poltyrev limit. These lattices were then used to generate lattice codes over Eisenstein integers which were implemented for compute-and-forward and thus enable the relays to decode to linear combinations of lattice points with Eisenstein integer coefficients instead of Gaussian integers. Due to the fact that Eisenstein integers quantize channel coefficients better than Gaussian integers, one can expect an increased achievable computation rate on average. Simulation results suggest that for compute-and-forward, lattice codes over Eisenstein integers provide improved outage performance and error-correcting performance in the average sense compared to lattice codes over integers without the cost of additional computational complexity.

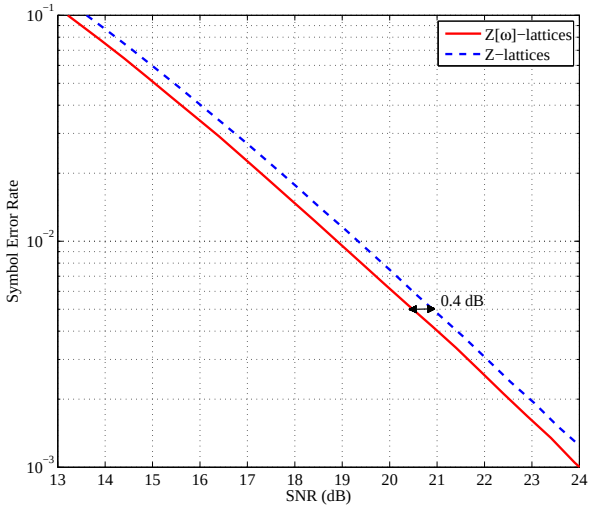

Fig. 6. Symbol error rate of $\mathbb{Z}[\omega]$ Lattices vs $\mathbb{Z}$ Lattices

APPENDIX

In this section, we provide the proofs for Theorem 12 and Theorem 14. We would like to note that the proof techniques used in proving Theorem 12 are very similar to those used in [5] and our proof of Theorem 14 is largely based on the proof in [4]. However, there are a few steps that have to be re-derived since Eisenstein integers are considered. We present the entire proof for the purpose of completeness. We first give some definitions and preliminaries that will be very useful for the proofs.

A. Notations and Definitions for $\mathbb{Z}[\omega]$-lattices

In [14, p. 54], it is stated that an n-dimensional complex lattice can be equivalently thought of as a $2n$-dimensional real lattice by the following mapping

$$[\lambda(1)\cdots\lambda(n)]^T \rightarrow [\Re(\lambda(1))\ \Im(\lambda(1))\cdots\Re(\lambda(n))\ \Im(\lambda(n))]^T \tag{60}$$

where the left hand side is an n-dimensional complex lattice point and the right hand side is its $2n$-dimensional real representation. Thus we shall consider n-dimensional Eisentein lattices as $2n$-dimensional real lattices and use $\mathbb{C}^n$ and $\mathbb{R}^{2n}$ interchangeably. We shall now introduce the notation that will be used in this section.

- S': $S \setminus 0$, where S is any discrete set.
- $\mathcal{V}$: Fundamental Voronoi region of the lattice $\mathbb{Z}[\omega]^n$.
- GRID: The lattice $\varrho^{-1}\mathbb{Z}[\omega]^n$, where ϱ is an Eisenstein prime.
- $\underline{x}^* = \underline{x} \bmod \mathcal{V} = \underline{x} \bmod \mathbb{Z}[\omega]^n = \underline{x} - Q_{\mathbb{Z}[\omega]^n}(\underline{x})$ where $\underline{x} \in \mathbb{C}^n$.
- $\mathcal{A}^* = \mathcal{A} \bmod \mathcal{V}$, where $\mathcal{A}$ is any set in $\mathbb{C}^n$ and the mod $\mathcal{V}$ operation is done element-wise.
- $\mathcal{A}' \triangleq \mathcal{A} \setminus \{0\}$ where $\mathcal{A} \subset \mathbb{R}^n$, $\mathcal{A} \subset \mathbb{C}^n$ or $\mathcal{A} \subset \mathbb{F}_q^n$
- Λ: An n-dimensional $\mathbb{Z}[\omega]$-lattice nested in GRID, i.e., $\Lambda \subset$ GRID .
- Vol$(\cdot)$: Volume of a closed set in $\mathbb{C}^n$, or equivalently volume of a closed set in $\mathbb{R}^{2n}$.
- GRID*: GRID $\cap\, \mathcal{V}$.
- $\mathcal{B}(r)$:A complex n-dimensional, or equivalently real $2n$-dimensional, closed set of points inside a sphere of radius r centered at the origin.
- Λ^*: The lattice constellation, i.e. $\Lambda^* = \Lambda \cap \mathcal{V}$. Note that Λ^* can generate Λ as follows:

$$\Lambda = \Lambda^* + \mathbb{Z}[\omega]^n. \tag{61}$$

- $M = |\Lambda^*|$: Cardinality of the lattice constellation.
- Λ_i^*: A point in Λ^*, $i \in \{0, \cdots, M-1\}$.

Note that by our construction, the lattices chosen from the $(n, k, q, \mathbb{Z}[\omega])$-lattice ensemble are periodic modulo the region $\mathcal{V}$. Thus we can restate all the properties of our lattice in terms of the lattice constellation Λ^* that lies within $\mathcal{V}$. The $(n, k, q, \mathbb{Z}[\omega])$-lattice ensemble has the following properties:

1) $\Lambda_0^* = \underline{0}$ deterministically.
   Proof: $\underline{0}$ is always a valid lattice point due to the definition of a lattice and $\underline{0}^* = \underline{0}$. Thus the result holds. ■
2) Λ_i^* is distributed uniformly over GRID* for $i \in \{1, \cdots, M-1\}$ where $M = q^k$.
   Proof: Each element of $\mathbf{G}$ is chosen uniformly over $\mathbb{F}_q$, therefore each codeword of the underlying linear code is distributed uniformly over $\mathbb{F}_q^n$. Due to last step in Construction A in Section V-B where the lattice is scaled with ϱ^{-1} and the ring homomorphism $\tilde{\sigma}$, the result holds. ■
3) The difference $(\Lambda_i^* - \Lambda_l^*)^*$ is uniformly distributed over GRID* for all $i \neq j$.
   Proof: This result holds due to the previous property and the definition of the $*$ operation. ■
4) $|\Lambda^*| = q^k$ with high probability if $n - k \rightarrow \infty$
   Proof:

$$\begin{aligned}\Pr\{\text{rank}(\mathbf{G}) < k\} &\leq \sum_{\underline{c} \neq \underline{0}} \Pr\left\{\sum_{i=1}^{k} c_i \mathbf{G}_i = \underline{0}\right\} \\ &= q^{-n}(q^k - 1),\end{aligned} \tag{62}$$

   where c_i would be elements of a $k \times 1$ coefficient vector $\underline{c}$. ■

We shall refer to $\mathcal{B}(r)^* = \mathcal{B}(r) \bmod \mathcal{V}$ as a $\mathcal{V}$-ball. Under the assumption that $r < \frac{1}{2}$, we say that $(\Lambda^* + \mathcal{B}(r))^*$ is a $\mathcal{V}$-covering if

$$\mathcal{V} \subseteq \bigcup_{\underline{\lambda} \in \Lambda^*} (\underline{\lambda} + \mathcal{B}(r))^*. \tag{63}$$

Note that $\Lambda + \mathcal{B}(r)$ is a covering if and only if $(\Lambda^* + \mathcal{B}(r))^*$is a $\mathcal{V}$-covering

In our lattice ensemble, we will constrain $k < \beta n$ for some $0 < \beta < 1$. Therefore $\Pr\{\text{rank}(\mathbf{G}) \neq k\}$ goes to zero at least exponentially. If $\mathbf{G}$ is full rank, there are $M = q^k$ many codewords that lie in $\mathcal{V}$. Also, an n-dimensional $\mathcal{V}$ is known to have a volume of $\left(\frac{\sqrt{3}}{2}\right)^n$. Then the volume of the Voronoi

region of our lattice is equal to $\left(\frac{\sqrt{3}}{2}\right)^n q^{-k}$. In our analysis very similar to [5], we will hold the effective radius of the Voronoi region of Λ, denoted as r_Λ^{eff} approximately constant as $n \to \infty$. This implies the following:

$$\begin{aligned} q^k &= \frac{\left(\frac{\sqrt{3}}{2}\right)^n}{V_{\mathcal{B}}\left(r_\Lambda^{\text{eff}}\right)} = \frac{\left(\frac{\sqrt{3}}{2}\right)^n \Gamma\left(n+1\right)}{\pi^n \left(r_\Lambda^{\text{eff}}\right)^{2n}} \\ &= \sqrt{2n\pi}\left(\frac{\sqrt{3}}{2\left(r_\Lambda^{\text{eff}}\right)^2}\right)^n \left(\frac{n}{e}\right)^n \left(1+O\left(\frac{1}{n}\right)\right). \end{aligned} \tag{64}$$

Note that q can either be a natural prime congruent to $1 \bmod 3$ or the square of a natural prime congruent to $2 \bmod 3$, nonetheless we shall restrict q to be a natural prime congruent to $1 \bmod 3$ for the sake of simplicity. We would like to note that it is not possible to keep r_Λ^{eff} constant as n grows since q has to be a natural prime congruent to $1 \bmod 3$ and k has to be an integer. Therefore, we will relax this condition to

$$r_{min} < r_\Lambda^{\text{eff}} < 2r_{min}, \tag{65}$$

as n grows, where $0 < r_{min} < \frac{1}{4}$. Although we have restricted q to be a natural prime congruent to $1 \bmod 3$, with the assumption of $k \leq \beta n$ for $\beta < 1$, (65) can be satisfied for any large enough n due to the following. Let q^* be the real number that satisfies (64) for a radius of $2r_{min}$. Then, ${q^*}^k = \frac{1}{V_{\mathcal{B}}(\sqrt{\frac{2}{\sqrt{3}}}2r_{min})}$ and from (65), q must satisfy

$$q^* < q < 2^{2n/k} q^*. \tag{66}$$

Finally, to show that for each $n > 4$ in our sequence a corresponding q exists that satisfies (66), we use the following lemma.

Lemma 16 ([23]): There always exists a natural prime congruent to $1 \bmod 3$ between integers m and $2m$ where $m > 4$.

We would also like to note that from (64), the growth of q is $O(n^{\frac{1}{\beta}})$. Thus,

$$\lim_{n\to\infty} \quad n/q = 0. \tag{67}$$

B. Proof: Existence of $\mathbb{Z}[\omega]$-lattices that are good for covering

The proof of this theorem is divided into two parts. In the first part, sufficient conditions are obtained such that most Eisenstein lattices in the ensemble are "almost complete" $\mathcal{V}$-coverings. In the second part, stricter conditions are imposed such that most of the Eisentein lattices in the ensemble are $complete$ $\mathcal{V}$-coverings and thus $complete$ coverings .

Part I: Almost complete covering

Denote d to be half of the largest distance between any two points that lie within the Voronoi region of an element in GRID.

$$d = \sqrt{\frac{n}{3q}}. \tag{68}$$

Note that by (66), $d \to 0$ as $n \to \infty$.

Consider the lattice constellation Λ^* of the ensemble and define k_1, k_2 such that $k_1 + k_2 = k$. We shall denote the Eisenstein lattice constellation obtained from the first k_1 columns of $\mathbf{G}$ by $\Lambda^*[k_1]$ and let $\Lambda^*[k_1+j], j = 1, \cdots, k_2$ denote the Eisenstein lattice constellation obtained from the first $k_1 + j$ columns of $\mathbf{G}$. Let $\underline{x}$ be an arbitrary point such that $\underline{x} \in \mathcal{V}$. Let $\mathcal{S}_1(\underline{x})$ denote the set of GRID points within a modulo distance $r-d$ from $\underline{x}$ where d was defined in (68).

$$\mathcal{S}_1(\underline{x}) = \text{GRID}^* \cap \left(\underline{x} + \mathcal{B}(r-d)\right)^*. \tag{69}$$

Furthermore, denote $\mathcal{S}_2(\underline{x})$ to be the set of GRID points such that their Voronoi regions intersect a sphere of radius $r-2d$ centered at $\underline{x}$.

$$\mathcal{S}_2(\underline{x}) = \left\{\underline{y} \in \text{GRID}^* : \left(\underline{y} + \varrho^{-1}\mathcal{V}\right) \cap \left(\underline{x} + \mathcal{B}(r-2d)\right)^*\right\}. \tag{70}$$

It can be observed that $\mathcal{S}_2(\underline{x}) \subset \mathcal{S}_1(\underline{x})$. Thus, the cardinality of $\mathcal{S}_1(\underline{x})$ can be bounded as:

$$\begin{aligned} |\mathcal{S}_1(\underline{x})| \geq |\mathcal{S}_2(\underline{x})| &\geq \left\lceil V_{\mathcal{B}}(r-2d)/\text{Vol}(\varrho^{-1}\mathcal{V})\right\rceil \\ &= \left\lceil q^n(\sqrt{3}/2)^{-n} V_{\mathcal{B}}(r-2d)\right\rceil. \end{aligned} \tag{71}$$

By the second property of the ensemble, the probability that $\underline{x}$ is covered by a sphere of radius $(r-d)$ centered at any point of $\Lambda^*[k_1]$ satisfies

$$\begin{aligned} \Pr\left\{\underline{x} \in (\Lambda_i^*[k_1] + \mathcal{B}(r-d))^*\right\} = \\ |\mathcal{S}_1(\underline{x})|/q^n \geq (\sqrt{3}/2)^{-n} V_{\mathcal{B}}(r-2d), \end{aligned} \tag{72}$$

for $i = 1, \cdots, M_1 - 1$ where $M_1 = q^{k_1}$ and Λ_i^* is the ith point of Λ^*. The indicator random variable η_i for $i = 1, \cdots, M_1 - 1$ is defined as

$$\eta_i = \eta_i(\underline{x}) \begin{cases} 1, & \text{if } \underline{x} \in (\Lambda_i^*[k_1] + \mathcal{B}(r-d))^* \\ 0, & \text{otherwise} \end{cases}$$

Note that $i = 0$ is not considered since $\Lambda_0^*[k_1] = 0$ deterministically. Thus, η_i is statistically independent of both i and $\underline{x}$. Define $\mathcal{X} = \mathcal{X}(\underline{x})$ as follows:

$$\mathcal{X} = \sum_{i=1}^{M_1-1} \eta_i. \tag{73}$$

Hence, $\mathcal{X}$ is equal to the number of nonzero codewords $(r-d)$-covering $\underline{x}$. Computing the expectation of $\mathcal{X}$ and using the lower bound from (72),

$$\begin{aligned} E(\mathcal{X}) &= \sum_{i=1}^{M_1-1} E(\eta_i) \\ &\geq (M_1 - 1)(\sqrt{3}/2)^{-n} V_{\mathcal{B}}(r-2d). \end{aligned} \tag{74}$$

Since the η_i's are pairwise independent and thus uncorrelated, similar to [5] one has

$$\text{Var}(\mathcal{X}) \leq E(\mathcal{X}). \tag{75}$$

Using (75), by Chebyshev's inequality, for any $\nu > 0$

$$\Pr\left\{|\mathcal{X} - E(\mathcal{X})| > 2^\nu \sqrt{E(\mathcal{X})}\right\} < \frac{\text{Var}(\mathcal{X})}{2^{2\nu} E(\mathcal{X})} \leq 2^{-2\nu}. \tag{76}$$

Define

$$\mu(\nu) = E(\mathcal{X}) - 2^\nu \sqrt{E(\mathcal{X})}. \tag{77}$$

Then from (76),

$$\Pr\{\mathcal{X} < \mu(\nu)\} < 2^{-2\nu}. \tag{78}$$

If $\mu(\nu) \geq 1$, $\Pr\{\mathcal{X} < 1\}$ is upper-bounded by $2^{-2\nu}$ as well.

A point $\underline{x} \in \mathcal{V}$ will be referred as *remote* from a discrete set of points $\mathcal{A}$ if it is not $r-d$-covered by $(\mathcal{A} + \mathcal{B}(r-d))^*$, i.e. if $\underline{x}$ does not belong to an $(r-d)$- sphere centered at any point of $\mathcal{A}$. Therefore, $\mathcal{X}(\underline{x}) < 1$ implies that "$\underline{x}$ is remote from $\Lambda^*[k_1]$". Define $\mathcal{Q}(\mathcal{A})$ to be the set of (continuous) points which are remote from the discrete set $\mathcal{A}$. Denote $\mathcal{Q}_i = \mathcal{Q}(\Lambda^*[k_1+i]), i = 0, 1, \cdots, k_2$ and define

$$q_i = |\mathcal{Q}_i|/\mathrm{Vol}(\mathcal{V}), \tag{79}$$

to be the fraction of (continuous) points in $\mathcal{V}$ which are remote from $\Lambda^*[k_1+i]$. Then,

$$|\mathcal{Q}_0| = \int_{\mathcal{V}} \mathbf{1}(\mathcal{X}(\underline{x}) < 1)\, d\underline{x} \tag{80}$$

$$\leq \int_{\mathcal{V}} \mathbf{1}(\mathcal{X}(\underline{x}) < \mu(\nu))\, d\underline{x}, \tag{81}$$

under the condition that $\mu(\nu) > 1$. Then, from (78) we have

$$E(q_0) < 2^{-2\nu}. \tag{82}$$

Applying Markov's inequality we get

$$\Pr\{q_0 > 2^{\nu} E(q_0)\} < 2^{-\nu}. \tag{83}$$

Using (82),

$$\Pr\{q_0 > 2^{-\nu}\} < 2^{-\nu}. \tag{84}$$

Therefore, by taking $\nu \to \infty$ and keeping $\mu(\nu) \geq 1$, this probability can be made arbitrarily small as $n \to \infty$. In order to satisfy these constraints it is sufficient to take $\nu = o(\log n)$ and $E(\mathcal{X}) > n^{\lambda}$ for some $\lambda > 0$. By (74) this would be satisfied if we choose a radius r such that

$$q^{k_1} - 1 = \frac{n^{\lambda}}{V_{\mathcal{B}}(r-2d)} \left(\sqrt{3}/2\right)^n. \tag{85}$$

Hence, we conclude that for these choice of parameters, for most lattices chosen from the $(n, k, q, \mathbb{Z}[\omega])$ ensemble, *almost all* points are covered by spheres of radius $r-d$.

Part II: Complete covering

We would like to obtain an ensemble of $\mathbb{Z}[\omega]$-lattices such that most of its members are able to cover all the points in $\mathcal{V}$. $\mathcal{Q}(\mathcal{A})$ is redefined to be the set of GRID* points, i.e., $\underline{x} \in$ GRID* which are remote from $\mathcal{A}$ and q_i is redefined to be the fraction of GRID* points that are remote from $\Lambda^*[k_1+i]$. Therefore, an $(r-d)$-covering of all GRID points implies an r-covering of all points in $\mathcal{V}$.

By augmenting the generator matrix $\mathbf{G}$ with an additional small number of columns $k_2 (k_2 \ll k_1)$, the fraction of uncovered GRID* points can be made smaller than $1/|\text{ GRID}^*|$ which implies that all GRID points are $r-d$-covered. We proceed as follows.

Choose k_1 and q such that k_1 grows faster than $\log^2 n$ and (64) and (65) are satisfied. Define the set

$$\mathcal{S} = \Lambda^*[k_1] \cup \left(\Lambda^*[k_1] + \left\{\sigma^{-1}(\mathbf{G}_{k_1+1}) \cap \mathcal{V}\right\}\right), \tag{86}$$

where σ is the ring isomorphism defined in section V-B. Also note that,

$$\Lambda^*[k_1+1] = \bigcup_{m=0}^{q-1} \left(\Lambda^*[k_1] + \sigma^{-1}\left([m \cdot (\mathbf{G}_{k_1+1})] \bmod q\right)\right). \tag{87}$$

Hence, $\mathcal{S} \subset \Lambda^*[k_1+1]$ and q_1 is upper-bounded by $\frac{\mathcal{Q}(\mathcal{S})}{|\text{GRID}|^*}$. Since $\Lambda^*[k_1] + \left\{\sigma^{-1}(\mathbf{G}_{k_1+1}) \cap \mathcal{V}\right\}$ is an independent shift of $\Lambda^*[k_1]$, conditioned on $\Lambda^*[k_1]$, the event that $\underline{x}$ is remote from $\Lambda^*[k_1] + \left\{\sigma^{-1}(\mathbf{G}_{k_1+1}) \cap \mathcal{V}\right\}$ is independent from whether $\underline{x}$ is remote from $\Lambda^*[k_1]$ and the probability of such an event is q_0. Then,

$$E\left\{\frac{|\mathcal{Q}(\mathcal{S})|}{|\text{GRID}^*|}\Big| q_0\right\} = q_0^2. \tag{88}$$

Due to the fact that $\mathcal{S} \subset \Lambda^*[k_1+1]$, we have $E\{q_1|q_0\} \leq q_0^2$. By Markov's inequality,

$$\Pr\Big\{q_1 > 2^{\gamma} E(q_1|q_0)\Big| q_0\Big\}. \tag{89}$$

Therefore,

$$\Pr\Big\{q_1 \leq 2^{\gamma-2\nu}\Big| q_0 \leq 2^{-\nu}\Big\} \geq 1 - 2^{-\gamma}. \tag{90}$$

From Bayes' rule and (84),

$$\Pr\Big\{q_1 \leq 2^{\gamma-2\nu}\Big\} \geq \Pr\Big\{q_1 < 2^{\gamma-2\nu}, q_0 \leq 2^{-\nu}\Big\} \tag{91}$$

$$\geq \left(1-2^{-\gamma}\right)\left(1-2^{-\nu}\right). \tag{92}$$

Repeating this procedure for $l = 0, 1, \ldots, k_2 - 1$, we obtain

$$q_{l+1} \leq 2^{\gamma} E(q_{l+1}|q_l) \tag{93}$$

$$\leq 2^{\gamma} q_l^2, \tag{94}$$

with probability at least $1-2^{-\gamma}$. Hence, the intersection of all these k_2 events and the event that $q_0 < 2^{-\nu}$ has the probability $(1-2^{-\nu})(1-2^{-\gamma})^{k_2}$, which implies

$$q_{k_2} \leq 2^{2^{k_2}(\gamma-\nu)-\gamma}. \tag{95}$$

We would like to choose k_2 such that

$$q_{k_2} < q^{-n} = 2^{-n \log q}. \tag{96}$$

The interpretation of (96) is $q_{k_2} = 0$ since there are q^n points in GRID*. Therefore, choosing $\gamma = \nu - 1$ and

$$k_2 = \lceil \log n + \log\log q \rceil, \tag{97}$$

or faster suffices. Due to the fact that $k = k_1 + k_2$, we conclude that with probability at least

$$\left(1-2^{-\nu}\right)\left(1-2^{-\nu+1}\right)^{(\log n + \log\log q)} \tag{98}$$

$\Lambda^*[k]$ satisfies $q_{k_2} < q^{-n}$, in other words every $\underline{x} \in$ GRID* is covered by at least one sphere of radius $(r-d)$. We would like to impose a condition on ν such that both $\nu \to \infty$ and the probability in (98) goes to 1 as $n \to \infty$. It suffices to choose

$$\nu = 2\log(\log n + \log\log q). \tag{99}$$

Note that as $\mu(\nu) \geq 1$, the probability that there remains a point $\underline{x} \in$ GRID* that is not $(r-d)$-covered is arbitrarily small as $n \to \infty$. If every point of GRID* is $(r-d)$-covered, then

$\mathcal{V}$ is r-covered. Thus, the probability of a complete covering with spheres of radius r goes to 1 where r satisfies(see (85))

$$M = q^{k_1+k_2} = \frac{n^\lambda}{V_{\mathcal{B}}(r-2d)} \left(\sqrt{3}/2\right)^n q^{k_2} \tag{100}$$

$$\leq \frac{n^\lambda}{V_{\mathcal{B}}(r-2d)} \left(\sqrt{3}/2\right)^n q^{(\log n + \log\log q)+1} \tag{101}$$

$$= \frac{n^\lambda}{V_{\mathcal{B}}(r-2d)} \left(\sqrt{3}/2\right)^n 2^{\log q[(\log n+\log\log q)+1]}. \tag{102}$$

From (100) and (102),

$$\frac{r}{r_\Lambda^{\text{eff}}} = \sqrt[2n]{\frac{V_{\mathcal{B}}(r)}{V_{\mathcal{B}}(r-2d)} n^\lambda q^{k_2}} \tag{103}$$

$$\leq \left(\frac{r}{r-2d}\right) \cdot n^{\lambda/2n} \cdot 2^{(\log q \log n + \log q \log\log q + \log q)/2n}. \tag{104}$$

For $\rho_{\text{cov}} \to 1$, the left-hand side of (103) should go to 1. Hence, we require each of the three terms on the right-hand side of (104) goes to 1. From (67) and (68), it follows that $d \to 0$ as $n \to \infty$ provided that $k \leq \beta n$ and $\beta < 1$. Therefore,

$$\lim_{n\to\infty} \left(\frac{r}{r-2d}\right) = 1. \tag{105}$$

For any fixed $\lambda > 0$, we have $\lim_{n\to\infty} n^{\lambda/2n} = 1$. Also, since k grows faster than $\log^2 n$, by (64) we have $\log p$ grows slower than $o\log(n/\log n)$. Then,

$$\lim_{n\to\infty} 2^{(\log q \log n + \log q \log\log q + \log q)/2n} = 1. \tag{106}$$

Thus, we have that $\frac{r_\Lambda^{\text{cov}}}{r_\Lambda^{\text{eff}}} \to 1$ in probability as $n \to \infty$ which completes the proof.

C. Proof: Existence of good nested $\mathbb{Z}[\omega]$-lattices

Using our result from Theorem 12, let Λ be an n-dimensional $\mathbb{Z}[\omega]$-lattice obtained through Construction-A with a corresponding generator matrix $\mathbf{B}$ which is good for covering.

Definition 17: A set $\mathcal{C}$ of linear (n,k) linear code over $\mathbb{F}_q^n$ is *balanced* if every nonzero element of $\mathbb{F}_q^n$ is contained in the same number, denoted by $N_{\mathcal{C}}$ of codes from $\mathcal{C}$.

Note that for fixed n, k, and q, the set of all linear (n,k) codes over $\mathbb{F}_q$ is balanced. We shall now state Lemma 1 in [4].

Lemma 18: Let $f(\cdot)$ be an arbitrary mapping $\mathbb{F}_q^n \to \mathbb{R}$ and let $\mathcal{C}$ be a balanced set of linear (n,k) codes over $\mathbb{F}_q$. Then, the average over all linear codes C in $\mathcal{C}$ of the sum $\sum_{c\in C'} f(c)$ is given by

$$\frac{1}{\mathcal{C}} \sum_{C\in\mathcal{C}} \sum_{c\in C'} f(c) = \frac{q^k-1}{q^n-1} \sum_{v\in\left(\mathbb{F}_q^n\right)'} f(v). \tag{107}$$

For proving Theorem 14, we shall use nested $\mathbb{Z}[\omega]$-lattices obtained from Construction-A as mentioned in Section V-C. A scaled version of Λ_C denoted as $\gamma\Lambda_C$, where $\gamma \in \mathbb{R}^+$ and Λ_C was defined in section V-B is constructed. Then, we multiply $\gamma\Lambda_C$ with the generator matrix $\mathbf{B}$ and obtain the lattice $\Lambda_f = \gamma\mathbf{B}\Lambda_C$. It can be observed that $\gamma\varrho\mathbb{Z}[\omega]^n \subset \gamma\varrho\Lambda \subset \Lambda_f$ and there are q^k elements of Λ_f that lie within the fundamental Voronoi region of $\gamma\varrho\Lambda$. Hence, the volume of the fundamental region of Λ_f is

$$\text{Vol}\left(\mathcal{V}_{\Lambda_f}\right) = \gamma^{2n} q^{n-k} \left(\frac{\sqrt{3}}{2}\right)^n \text{Vol}\left(\mathcal{V}_\Lambda\right). \tag{108}$$

We can now extend the Minkowski-Hlawka Theorem in [4] to Eisenstein lattices as follows, following similar steps.

Theorem 19: (*Minkowski-Hlawka Theorem:*) Let f be a Riemann integrable function $\mathbb{R}^{2n} \to \mathbb{R}$ of bounded support(i.e., $f(v) = 0$ (if $\|v\|$ exceeds some bound). Then for any integer k where $0 < k < n$, and any fixed Vol$(\mathcal{V}_{\Lambda_f})$, the approximation

$$\frac{1}{\mathcal{C}} \sum_{C\in\mathcal{C}} \sum_{v\in g(\gamma\mathbf{B}\Lambda_C')} f(v) \approx \text{Vol}(\mathcal{V}_{\Lambda_f})^{-1} \int_{\mathbb{R}^{2n}} f(v)dv, \tag{109}$$

where $\mathcal{C}$ is any balanced set of linear (n,k) codes over $\mathbb{F}_q$ and where $g(\cdot) : \mathbb{C}^n \to \mathbb{R}^{2n}$ as in (60), becomes exact in the limit $q \to \infty$, $\gamma \to 0$, $\gamma^{2n} q^{n-k} \left(\frac{\sqrt{3}}{2}\right)^n \text{Vol}\left(\mathcal{V}_\Lambda\right) = \text{Vol}\left(\mathcal{V}_{\Lambda_f}\right)$ fixed. Note that these conditions imply that $\gamma q \to \infty$.

Proof:

$$\frac{1}{|\mathcal{C}|} \sum_{C\in\mathcal{C}} \sum_{v\in g(\gamma\mathbf{B}\Lambda_C')} f(v) \tag{110}$$

$$= \frac{1}{|\mathcal{C}|} \sum_{C\in\mathcal{C}} \Big[\sum_{v\in g((\mathbb{Z}[\omega]^n)'):\tilde{\sigma}(v)=0} f(\gamma\mathbf{B}v) \ldots$$

$$\ldots + \sum_{v\in g(\mathbb{Z}[\omega]^n):\tilde{\sigma}(v)\in C'} f(\gamma\mathbf{B}v) \Big] \tag{111}$$

$$= \sum_{v\in(g(\mathbb{Z}[\omega]^n)'):\tilde{\sigma}(v)=0} f(\gamma\mathbf{B}v) + \frac{1}{|\mathcal{C}|} \sum_{C\in\mathcal{C}} \sum_{c\in\mathcal{C}'} \left[\sum_{v\in g(\mathbb{Z}[\omega]^n):\tilde{\sigma}(v)=c} f(\gamma\mathbf{B}v) \right] \tag{112}$$

$$= \sum_{v\in g((\mathbb{Z}[\omega]^n)'):\tilde{\sigma}(v)=0} f(\gamma\mathbf{B}v) + \frac{q^k-1}{q^n-1} \sum_{c\in(\mathbb{F}_q^n)'} \left[\sum_{v\in g(\mathbb{Z}[\omega]^n):\tilde{\sigma}(v)=c} f(\gamma\mathbf{B}v) \right] \tag{113}$$

$$= \sum_{v\in g((\mathbb{Z}[\omega]^n)'):\tilde{\sigma}(v)=0} f(\gamma\mathbf{B}v) + \frac{q^k-1}{q^n-1} \sum_{v\in g(\mathbb{Z}[\omega]^n):\tilde{\sigma}(v)\neq 0} f(\gamma\mathbf{B}v), \tag{114}$$

where the step from (112) to (113) is due to Lemma 18 and due to the fact that f has bounded support, the left term of (114) vanishes for sufficiently large γq and the right term of

(114) becomes

$$\frac{q^k-1}{q^n-1}\sum_{v\in g((\mathbb{Z}[\omega]^n)')} f(\gamma\mathbf{B}v) \approx \gamma^{-2n}q^{k-n}\left(\frac{2}{\sqrt{3}}\right)^n \mathrm{Vol}(\mathcal{V}_\Lambda)^{-1}\int_{\mathbb{R}^{2n}} f(v)dv, \quad (115)$$

which becomes exact in the limit as $\gamma \to 0$, $\gamma q \to \infty$, i.e, a Riemann sum approaching to a Riemann integral. Note that the term $\gamma^{-2n}q^{k-n}\left(\frac{2}{\sqrt{3}}\right)^n$ appears in front of the integral in (115) since it is the reciprocal of the volume of the fundamental Voronoi region of $\Lambda_f = \gamma\mathbf{B}\Lambda_C$. ■

Suppose now that a transmitter selects a codeword $\underline{x}$ from an Eisenstein lattice $\Lambda \in \mathbb{C}^n$ (or equivalently $\mathbb{R}^{2n}$) and $\underline{x}$ is transmitted over an AWGN channel where a random noise vector $\underline{z} \in \mathbb{C}^n$(or equivalently $\mathbb{R}^{2n}$) gets added with the variance of each $2n$ components equal to $P_{\underline{z}}/2$. The receiver obtains $\underline{y} = \underline{x} + \underline{z}$ and tries to recover $\underline{x}$. Furthermore, let $E \subset \mathbb{R}^{2n}$ be a set of typical noise vectors. We say that an *ambiguity* occurs if $\underline{y}$ can be written in more than one way as $\underline{y} = \underline{x} + \underline{e}$ where $\underline{x} \in \Lambda$ and $\underline{e} \in E$. Let $P_{\text{amb}|E}$ be the probability of ambiguity given that $\underline{z} \in E$. Assuming that the receiver is able to recover $\underline{x}$ whenever $\underline{z} \in E$ and there is no ambiguity, the probability of decoding error is upper-bounded by

$$P_e \le P_{\text{amb}|E} + P(\underline{z} \notin E). \quad (116)$$

Due to the fact that Minkowski-Hlawka theorem can be proven for Λ_f, the following theorem immediately follows.[4]

Theorem 20: Let E be a Jordan measurable bounded subset of $\mathbb{R}^{2n}$ and let k be an integer such that $0 < k < n$. Then, for any $\delta > 0$, for all sufficiently large q, and for all sufficiently small γ, the arithmetic average of $P_{\text{amb}|E}$ over all lattices $\Lambda_f = \gamma\mathbf{B}\Lambda_C$, $C \in \mathcal{C}$, which we denote as $\overline{P_{\text{amb}|E}}$, is bounded by

$$\overline{P_{\text{amb}|E}} < (1+\delta)\mathrm{Vol}(E)/\mathrm{Vol}\left(\mathcal{V}_{\Lambda_f}\right), \quad (117)$$

where $\mathcal{C}$ is any balanced set of linear (n,k) codes over $\mathbb{F}_q$ and where $\mathrm{Vol}\left(\mathcal{V}_{\Lambda_f}\right) \triangleq \gamma^{2n}q^{n-k}\mathrm{Vol}(\mathcal{V}_\Lambda)\left(\frac{\sqrt{3}}{2}\right)^n$ is the fundamental volume of the lattices $\Lambda_f = \gamma\mathbf{B}\Lambda_C$, $C \in \mathcal{C}$. Note that as $n \to \infty$, E will approach the shell of a $2n$-dimensional ball with radius $r_{\underline{z}} = \sqrt{nP_{\underline{z}}}$. Thus

$$\mathrm{Vol}(E) \le \mathrm{Vol}(\mathcal{B}(\sqrt{nP_{\underline{z}}})) = \frac{\left(\sqrt{\pi}r_{\underline{z}}^2\right)^n}{\Gamma(n+1)} \quad \text{as} \quad n \to \infty, \quad (118)$$

which immediately follows that

$$\overline{P_{\text{amb}|E}} \le (1+\delta)\left(\frac{r_{\underline{z}}}{r^{\text{eff}}_{\gamma\mathbf{B}\Lambda_C}}\right)^{2n}, \quad (119)$$

as $n \to \infty$. This implies that $\overline{P_{\text{amb}|E}} \to 0$ as $n \to \infty$ for $r_{\underline{z}} < r^{\text{eff}}_{\gamma\Lambda_C}$. Hence for a given lattice $\Lambda_f = \gamma\mathbf{B}\Lambda_C$, $P_{\text{amb}|E} \to 0$ in probability as $n \to \infty$. Taking into account that $P(\underline{z} \notin E) \to 0$ as $n \to \infty$, from (116) we conclude that $P_e \to 0$ in probability as $n \to \infty$. This completes the proof.

REFERENCES

[1] U. Erez and R. Zamir, "Achieving 1/2 log (1+ SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Info. Theory*, vol. 50, pp. 2293–2314, Oct. 2004.

[2] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Info. Theory*, vol. 48, pp. 1250–1276, Jun. 2002.

[3] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. Info. Theory*, vol. 40, pp. 409–417, Mar. 1994.

[4] H. A. Loeliger, "Averaging bounds for lattices and linear codes," *IEEE Trans. Info. Theory*, vol. 43, pp. 1767–1773, Nov. 1997.

[5] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. Info. Theory*, vol. 51, pp. 3401–3416, Oct. 2005.

[6] O. Shalvi, N. Sommer, and M. Feder, "Signal codes," *Info Theory Workshop*, pp. 332–336, Mar. 31–Apr. 4 2003.

[7] N. Sommer, M. Feder, and O. Shalvi, "Low density lattice codes," *IEEE Trans. Info. Theory*, vol. 54, pp. 1561–1585, Apr. 2008.

[8] M. P. Wilson, K. R. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bi-directional relaying," *IEEE Trans. Info. Theory*, vol. 56, pp. 5641–5654, Nov. 2010.

[9] W. Nam, S. Y. Chung, and Y. H. Lee, "Capacity of the gaussian two-way relay channel to within 1/2 bit," *IEEE Trans. Info. Theory*, vol. 56, pp. 5488–5494, Nov. 2010.

[10] U. Niesen and P. Whiting, "The degrees of freedom of compute-and-forward," *IEEE Trans. Info. Theory*, vol. 58, pp. 5214–5232, Aug. 2012.

[11] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Info. Theory*, vol. 57, pp. 6463–6486, Oct. 2011.

[12] C. Feng, D. Silva, and F. R. Kschischang, "An algebraic approach to physical-layer network coding," *IEEE Intl. Symp. on Info. Theory*, pp. 1017–1021, Jun. 2010.

[13] Q. T. Sun, J. Yuan, T. Huang, and K. W. Shum, "Lattice network codes based on Eisenstein integers," *IEEE Trans. Comm.*, vol. 61, pp. 2713–2725, 2013.

[14] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*. Springer-Verlag, 1999.

[15] C. A. Rogers, "A note on coverings," *Mathematica*, vol. 4, pp. 1–6, 1957.

[16] R. Zamir and M. Feder, "On lattice quantization noise," *IEEE Trans. Info. Theory*, vol. 42, pp. 1152–1–159, Jul. 1996.

[17] G. D. Forney Jr., "Coset codes. I. Introduction and geometrical classification," *IEEE Trans. Info. Theory*, vol. 34, pp. 1123–1151, Sep. 1988.

[18] J. H. Conway and N. J. A. Sloane, "A fast encoding method for lattice codes and quantizers," *IEEE Trans. Info. Theory*, vol. 29, pp. 820–824, Nov. 1983.

[19] J. Leech and N. J. A. Sloane, "Sphere packings and error correcting codes," *Canadian Journal of Mathematics*, vol. 23, pp. 718–745, Nov. 1971.

[20] O. Ordentlich and U. Erez, "A simple proof for the existence of "good" pairs of nested lattices," *arxiv.org*, Sep. 2012.

[21] J. H. Conway and D. Smith, *On Quaternions and Octonions*. CRC Press, 2003.

[22] T. W. Hungerford, *Algebra (Graduate Texts in Mathematics)*. Springer, 1974.

[23] R. Breusch, "Zur verallgemeinerung des bertrandsehen postulates, daß zwischen x und 2x stets primzalflen liegen," *Mathematische Zeitschrift*, vol. 34, pp. 505–526, 1932.

[24] H. V. Henderson and S. R. Searle, "On deriving the inverse sum of matrices," *SIAM Review*, pp. 53–60, 1981.

[25] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Info. Theory*, vol. 45, pp. 1639–1642, July 1999.

[26] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. Info. Theory*, vol. 48, pp. 2201–2214, Aug. 2002.

[27] A. K. Lenstra, H. Lenstra, and L. Lovasz, "Factoring polynomials with rational coefficients," *Math Ann.*, pp. 515–534, 1982.

[28] H. Napias, "A generalization of the LLL-algorithm over Euclidean rings or orders," *J. Theorie des Nombres de Bordeaux*, pp. 387–396, 1996.

[29] A. Sakzad, E. Viterbo, Y. Hong, and J. Boutros, "On the ergodic computation rate for compute-and-forward," *International Symposium on Network Coding (NetCod)*, pp. 131–136, 2012.

[30] A. Sakzad, J. Harshan, and E. Viterbo, "Integer-forcing MIMO linear receivers based on lattice reduction," *IEEE Trans. Wireless Comm.*, vol. 12, pp. 4905–4915, 2013.

Nihat Engin Tunali received his Ph.D degree in electrical and computer engineering from Texas A&M University (TAMU) in 2014. In July 2014, he joined Xilinx Inc., San Jose, CA where he is currently a senior design engineer. In 2012, he spent his summer as an intern in Xilinx Inc. His research interests are in wireless communications, coding theory for storage channels, information theory, network information theory, and lattice coding theory.

Yu-Chih Huang received his Ph.D degree in electrical and computer engineering from Texas A&M University (TAMU) in 2013. He was a postdoctoral research associate at TAMU from 2013 to 2015. In February 2015, he joined the department of communication engineering at the National Taipei University, Taiwan, where he is currently an assistant professor. In 2012, he spent the summer as a research intern in Bell Labs, Alcatel-Lucent. His research interests are in information theory, network information theory, lattice coding theory, and wireless communications.

Joseph J. Boutros received the M.S. degree in electrical engineering in 1992 and the Ph.D. degree in 1996, both from Ecole Nationale Superieure des Telecommunications (ENST, Telecom ParisTech), Paris, France. From 1996 to 2006, he was with the Communications and Electronics Department at ENST as an Associate Professor. Also, Dr Boutros was a member of the research unit UMR-5141 of the French National Scientific Research Center (CNRS) in Paris. In July 2007, Doctor Boutros joined Texas A&M University at Qatar (TAMUQ) as a full Professor in the electrical engineering program where he teaches courses in signal processing, communication theory, information theory, and wireless communications. His mathematical approach for teaching communication theory is combined with a strong practical computing component. Doctor Boutros has been a scientific consultant for Alcatel Space, Philips Research, and Motorola Semiconductors, and member of the Digital Signal Processing team at Juniper Networks Cable. His fields of research are codes on graphs, lattice sphere packing, iterative decoding, joint source-channel coding, space-time coding, physical-layer security, and physical-layer network coding. His research is mainly performed under grants and tight collaboration with private companies and public institutions such as Mitsubishi Electric Europe, Ooredoo (Qatar Telecom), and the Qatar National Research Fund (QNRF). Dr Boutros is a senior member of the IEEE society. He is active in technical and organization committees of numerous IEEE events, such as the International Symposium on Information Theory (ISIT), the Information Theory Workshop (ITW), and the International Symposium on Turbo Codes and related topics. Doctor Boutros is co-inventor of 13 industrial patents including algorithms and techniques in channel coding and digital communications.

Krishna R. Narayanan received the Ph.D. degree in electrical engineering from Georgia Institute of Technology in 1998 and is currently a professor in the department of electrical and computer engineering at Texas A&M University. His research interests are in coding theory, information theory, joint source-channel coding and signal processing with applications to wireless communications and data storage. He was the recipient of the 2006 best paper award from the IEEE technical committee for signal processing for data storage. He served as the area editor for the coding theory and applications area of the IEEE Transactions on Communications from 2007 until 2011.