Adaptive Compute-and-Forward with Lattice Codes Over Algebraic Integers

Yu-Chih Huang, Krishna R. Narayanan, and Ping-Chung Wang
Department of Electrical and Computer Engineering, Texas A&M University
{jerry.yc.huang@gmail.com, krn@ece.tamu.edu, michael422603@tamu.edu}

Abstract

We consider the compute-and-forward relay network with limited feedback. A novel scheme called adaptive compute-and-forward is proposed to exploit the channel knowledge by working with the best ring of imaginary quadratic integers. This is enabled by generalizing Construction A lattices to other rings of imaginary quadratic integers which may not form principal ideal domains and by showing such construction can produce good lattices for coding in the sense of Poltyrev and for MSE quantization. Since there are channel coefficients (complex numbers) which are closer to elements of rings of imaginary quadratic integers other than Gaussian and Eisenstein integers, by always working with the best ring among them, one expects to obtain a better performance than that provided by working over Gaussian or Eisenstein integers.

Index Terms

Compute-and-forward, physical-layer network coding, and lattice codes.

I. INTRODUCTION

The compute-and-forward paradigm [1] is a novel information forwarding strategy that allows relay nodes to compute functions of messages by exploiting the structure induced by the channel. The main enabler of the scheme in [1] is the use of lattice codes from Construction A over \( \mathbb{Z} \) the ring of integers. Lattices built from Construction A over the ring of Gaussian integers \( \mathbb{Z}[i] \) and the ring of Eisenstein integers \( \mathbb{Z}[\omega] \) were used in compute-and-forward in [2] and [3] and the goodness of these constructions was shown in [3]. One of the important advantages of using lattices over \( \mathbb{Z}[i] \) and \( \mathbb{Z}[\omega] \) is that in effect it is possible to quantize the channel coefficients to elements in these rings and decode linear combinations of lattice codewords with coefficients chosen from the ring of integers used to construct the lattice.

Since \( \mathbb{Z}[i] \) and \( \mathbb{Z}[\omega] \) are instances of imaginary quadratic integers, it seems natural to extend the compute-and-forward framework to general rings of imaginary quadratic integers. In this paper, we seek to better understand the role of rings of integers of algebraic number fields in constructing good lattices and to further benefit from this extension. One important difference between general rings of quadratic integers and the above two special cases (Gaussian and Eisenstein integers) is that the Gaussian integers and Eisenstein integers are not merely rings, they are principal ideal domains (PIDs) and the constructions over these two rings [2] [3] heavily rely on properties of PID. On the other hand a general ring of imaginary quadratic integers is not a PID. Therefore, in order to fully exploit the potential of rings of quadratic integers for the use of compute-and-forward, one has to work with ideals. In this paper, we generalize the famous Construction A to a general ring of imaginary quadratic integers (not necessary a PID). We show that such construction can produce lattices that are Poltyrev-good and MSE quantization-good. Based on this, we can obtain the achievable rate expression in [1] with replacement of those integers by elements in a ring of imaginary quadratic integers.

Since \( \mathbb{Z}[\omega] \) quantizes \( \mathbb{C} \) best among all imaginary quadratic integers, at first glance, it appears that there is no need to pursue lattices over rings other than \( \mathbb{Z}[\omega] \). However, this is not the case when we have feedback. This scenario was first studied by Niesen and Whiting in [4] where the global channel knowledge is perfectly feedback to the transmitters. Using the theory of Diophantine approximation, they
show that the traditional lattice-based scheme in [1] is inefficient in the asymptotically high signal-to-noise ratio (SNR) regime. They then propose a novel coding scheme which is a clever combination of compute-and-forward and real interference alignment. Their scheme achieves the full degrees of freedom (DoF); but in order to see a gain, it requires an enormously high SNR. Another approach proposed in [5] is to phase-precode the lattice-based scheme in [1]. In this approach, one rotates the transmitted signal space according to the channel realization in such a way that the received signal space is close to a linear integer combination of the codebook. Hence, instead of the global channel knowledge, the phase-precoding approach only requires limited feedback. i.e., transmitters only need to know the optimal (or reasonable) phases for precoding. In this paper, we propose a novel framework called adaptive compute-and-forward which makes use of the proposed lattices. The idea is to let the transmitters adaptively choose the best ring of imaginary quadratic integers to work with according to the channel coefficients. It is worth noting that this approach only requires the knowledge of which ring the transmitters should work with and hence limited feedback suffices. We show that the proposed adaptive compute-and-forward can achieve increased computation rates. Further, this can be used in conjunction with the phase precoding scheme in [5].

The idea of using different sets of algebraic integers for compute-and-forward was first proposed independently in [6] and [7]. In [6], Vazquez-Castro uses finite constellations carved from some rings of imaginary quadratic integers which also form Euclidean domains (hence PIDs) for compute-and-forward. In [7], instead of being confined in Euclidean domains or PIDs, we go beyond PIDs and construct lattices over rings of imaginary quadratic integers for compute-and-forward. However, their goodness has not been shown and the idea of adaptively choosing the rings of integers was only vaguely mentioned in [7]. This paper contributes to the literature by proving the optimality of the proposed lattices, and hence, deriving the achievable information rates with lattices over imaginary quadratic integers.

A. Notations

Throughout the paper, \( \mathbb{R} \) and \( \mathbb{C} \) represent the set of real numbers and complex numbers, respectively. We use \( j \triangleq \sqrt{-1} \) to denote the imaginary unit. For a complex number \( x = a + jb \in \mathbb{C} \) where \( a, b \in \mathbb{R} \), \( \bar{x} \triangleq a - jb \) denotes its complex conjugate. We use \( \mathbb{P}(E) \) to denote the probability of the event \( E \). Vectors are written in boldface and random variables are written in Sans Serif font. We use \( \times \) to denote the Cartesian product and use \( \oplus \) to denote the addition operation over a finite field where the field size can be understood from the context if it is not specified. Also, we do not distinguish the multiplication operation over the complex field and finite fields as it is understood from the context.

II. Problem Statement

The network considered in this paper is the compute-and-forward relay network first studied by Nazer and Gastpar in [1]. We consider an AWGN network with \( K \) source nodes and \( M \) destination nodes as shown in Fig 1. Each source node has a message \( w_k \in \{1, 2, \ldots, W\} \), \( k \in \{1, \ldots, K\} \) which can alternatively be expressed by a length-\( N' \) vector over some finite field, i.e., \( w_k \in \mathbb{F}_p^{N'} \) with \( W = p^{N'} \). This message is fed into an encoder \( E_k^{N} \) whose output is a length-\( N \) codeword \( x_k \in \mathbb{C}^{N} \).

The received signal at destination \( m \) is given by

\[
 y_m = \sum_{k=1}^{K} h_{mk} x_k + z_m,  \tag{1}
\]

where \( h_{mk} \in \mathbb{C} \) is the channel coefficient between the source node \( k \) and destination node \( m \), and \( z_m \sim \mathcal{CN}(0, I) \). One can think of a large network in which these destination nodes could be intermediate relay nodes which are only interested in forwarding signals. Thus, instead of individual messages, each destination node is only interested in recovering a function of messages which will be forwarded to the
Fig. 1. A compute-and-forward relay network where $S_1, \ldots, S_K$ are source nodes and $D_1, \ldots, D_M$ are destination nodes.

next layer. In Nazer and Gastpar’s setting, the functions are chosen to be linear combination of messages given by

$$u_m = b_{m1}w_1 \oplus \ldots \oplus b_{mK}w_K,$$

where $b_{m1}, \ldots, b_{mK}$ are elements in the same field $F_p$ with the elements in $w_k$ and the operations are elementwise. Upon observing $y_m$, the destination node $m$ forms $\hat{u}_m = G^N_m(y_m)$ an estimate of $u_m$.

**Definition 1 (Computation codes).** For a given equation coefficient vector $b_m \triangleq [b_{m1}, \ldots, b_{mK}]^T$, a $(N, N')$ computation code consists of a sequence of encoding/decoding functions $(E^1_N, \ldots, E^K_N)/(G^1_N, \ldots, G^M_N)$ described above and an error probability given by

$$P_e^{(N)} \triangleq \Pr \left( \bigcup_{m=1}^M \{ \hat{u}_m \neq u_m \} \right).$$

**Definition 2 (Computation rate for function $b_m$ at relay $m$).** For a given channel vector $h_m \triangleq [h_{m1}, \ldots, h_{mK}]^T$ and equation coefficient vector $b_m$, a computation rate $R(h_m, b_m, P)$ is achievable at relay $m$ if for any $\varepsilon > 0$ there is an $(N, N')$ computation code such that

$$N' \geq NR(h_m, b_m, P) / \log(p) \text{ and } P_e^{(N)} \leq \varepsilon.$$  

Note that the first condition is equivalent to saying that $W \geq 2^{NR(h_m, b_m, P)}$.

In this paper, we consider the symmetric case where all the encoders are of the same rate. Thus, for a given $H \triangleq [h_1, \ldots, h_M]$ and $B \triangleq [b_1, \ldots, b_M]$, the achievable computation rate is $R(H, B, P) \triangleq \min_m R(h_m, b_m, P)$. Moreover, suppose there is a final destination collecting all the functions, it would be able to recover all the messages if $B$ is full rank. Hence, one can also define the computation rate of the network as follows.

**Definition 3 (Computation rate of the network).** The achievable computation rate of the network is defined as

$$R(H, P) \triangleq \max_{B : B \text{ full rank}} R(H, B, P).$$

[1] In general, the functions are not limited to linear combinations of messages and some other functions have been considered in [8] [4] [9] for instance.
A. Open-Loop Compute-and-Forward

We first consider the open-loop setting where channel state information is only available at the receivers. In [1], Nazer and Gastpar propose a novel paradigm called compute-and-forward where each source node implements the same nested lattice code over $\mathbb{Z}$ of Erez and Zamir [10] and encode real and imaginary parts separately. This allows each relay to decode the received signal to linear combination of the transmitted lattice points with coefficients being integers. This results in the following computation rate at a relay.

**Theorem 4** (Nazer-Gastpar). At the $m$th relay, given $h_m \in \mathbb{C}^K$ and $a_m \in \mathbb{Z}[i]^K$, the following computation rate is achievable\(^2\)

$$R(h_m, a_m, P) = \log^+(\left(\frac{\|a_m\|^2 - \frac{P|h_m|^2}{1 + P\|h_m\|^2}}{1 + P\|h_m\|^2}\right)^{-1}). \quad (6)$$

One can then maximize the overall computation rate by judiciously choosing the matrix $A = [a_1, \ldots, a_M]$ whose finite field representatives $B = [b_1, \ldots, b_M]$ are full rank.

In [1], real and imaginary parts are separately considered. In what follows, we provide a high-level description of the scheme for the real part only but the other part works identically. Each source node adopts a same nested lattice code constructed over $\mathbb{Z}$. Since lattices are close under integer linear combinations, the $m$th destination can now decode the codeword corresponding to an integer linear combination of codewords which were sent. Note that the channel output is a noisy version of a linear combination of codewords; hence, extra noise will be introduced when we try to enforce real linear combinations into codewords that were sent. Note that the channel output is a noisy version of a linear combination of codewords, hence, extra noise will be introduced when we try to enforce real linear combinations into codewords that were sent.

The proof of the above result heavily relies on two key points. The first one is the existence of good lattices under this construction. Perhaps more importantly, the second one is that the mapping between $\mathbb{Z}$ and the finite field is a ring homomorphism so that integer combinations of lattice points will be corresponding to linear combinations over finite field. This ring homomorphism then allows one to map back and forth between the finite field and real filed without ruining the structure. In [3], Tunali et al. considered real and imaginary parts jointly and generalized the compute-and-forward paradigm to the Eisenstein lattices which are constructed by Construction A over $\mathbb{Z}[\omega]$. This has resulted in an increased achievable rate on average as the ring of Eisenstein integers approximates $\mathbb{C}$ better than Gaussian integers.

III. LATTICES OVER IMAGINARY QUADRATIC INTEGERS

Since both the Gaussian integers and Eisenstein integers are rings of integers of some number fields, it is natural to consider rings of integers of other number fields. In what follows, we particularly pick those rings of integers of imaginary quadratic fields. The reasons that we pick such rings are twofold. First of all, the channel coefficients we are trying to quantize lie in those rings of integers of imaginary quadratic fields. The reasons that we pick such rings are twofold.

1. It is natural to consider rings of integers of other number fields. In what follows, we particularly pick achievable rate on average as the ring of Eisenstein integers approximates $\mathbb{C}$ better than Gaussian integers.

2. Note that here $a_m \in \mathbb{Z}^K$ but in Definition 2, computation rate is defined for $b_m \in \mathbb{F}_p^K$. This is not an issue by letting $p$ the field size tend to $\infty$, which is exactly what required by the coding scheme in [1].
$p$, then $N(p) = p^f$ where $f \in \{1, 2\}$ is the inertial degree. Note that $\mathcal{O}_K/p \cong \mathbb{F}_{p^f}$; let $\mathcal{M} : \mathbb{F}_{p^f} \to \mathcal{O}_K/p$ be the ring isomorphism.

**Construction A**  \([11] \ [12]\) Let $n, N$ be integers such that $n \leq N$ and let $G$ be a generator matrix of an $(N, n)$ linear code over $\mathbb{F}_{p^f}$. Construction A over $\mathcal{O}_K$ consists of the following steps:

1. Define the discrete codebook $C = \{x = G \odot y : y \in \mathbb{F}^n_{p^f}\}$ where all operations are over $\mathbb{F}_{p^f}$.
2. Construct $\Lambda^* \triangleq \mathcal{M}(C)$ where $\mathcal{M} : \mathbb{F}_{p^f} \to \mathcal{O}_K/p$ is a ring isomorphism.
3. Tile $\Lambda^*$ to the entire $\mathbb{C}^N$ to form $\Lambda \triangleq \Lambda^* + \mathbb{N}^N$.

**Theorem 5.** $\Lambda$ is a lattice over $\mathbb{C}^N$. Moreover, a complex vector $\lambda$ belongs to $\Lambda$ if and only if $\sigma(\lambda) \in C$ where $\sigma \triangleq \mathcal{M}^{-1} \circ \mod p^N$ is a ring homomorphism.

**Proof:** Since $\mathcal{M}$ is a ring isomorphism, $\mathcal{M}(0) = 0$. Moreover, $0 \in p^N$. Thus, $0 \in \Lambda$. Let

$$\lambda_1 = \mathcal{M}(c_1) + p_1,$$

$$\lambda_2 = \mathcal{M}(c_2) + p_2,$$

where $c_1, c_2 \in C$ and $p_1, p_2 \in p^N$. We have

$$\lambda_1 + \lambda_2 = \mathcal{M}(c_1) + \mathcal{M}(c_2) + p_1 + p_2$$

$$\triangleq (a) \mathcal{M}(c_1 \oplus c_2) + p + p_1 + p_2$$

$$= \mathcal{M}(c_3) + p_3,$$

where $p, p_3 \in p^N$, $c_3 = c_1 \oplus c_2 \in C$ and (a) is due to the fact that $\mathcal{M}$ is a ring isomorphism. Moreover, choosing $c_2$ to be the inverse of $c_1$ and choosing $p_2 = -p_1 - p$ makes $\lambda_2$ the additive inverse of $\lambda_1$. Therefore, $\Lambda$ is a lattice.

To see that $\lambda$ is a lattice point if and only if $\sigma(\lambda) \in C$, we note that

$$\lambda \in \Lambda$$

$$\Leftrightarrow \lambda = \mathcal{M}(c) + p$$

$$\Leftrightarrow \lambda \mod p^N = \mathcal{M}(c)$$

$$\Leftrightarrow \mathcal{M}^{-1}(\lambda \mod p^N) = c.$$  \hspace{1cm} (11)

**Theorem 6.** For any $d < 0$ square free integer, consider $K = \mathbb{Q}(\sqrt{d})$, there exists a sequence of lattices from Construction A over $\mathcal{O}_K$ that is Poltyrev-good and good for quantization.

**Proof:** (Sketch. Please see Appendix B for details) For showing the Poltyrev-goodness, we tailor the Minkowski-Hlawka theorem specifically for $\mathcal{O}_K$ and then follow the steps of Loeliger in \([13]\) to show that with high probability, the random Construction A ensemble over $\mathcal{O}_K$ would produce Poltyrev-good lattices. For showing the MSE quantization-goodness, we modify the proof by Ordentlich and Erez \([14]\) where we first construct a sequence of prime ideals whose norms tend to $\infty$ for each $\mathcal{O}_K$ and show that randomly picking elements in $G$ induces uniform distribution over $(\mathcal{O}_K/p)^N$. One can then follow the steps in \([14]\) to show the MSE quantization-goodness.

In fact, similar to \([9]\), one can even build multilevel lattices over $\mathcal{O}_K$ by Construction $\pi_A$ \([9] \ [7]\) (previously called product construction). Let $\mathcal{I}$ be an ideal whose prime ideal factorization is given by $\mathcal{I} = \prod_{i=1}^L p_i$ with $p_i$ is relatively prime. From Chinese remainder theorem, we have

$$\mathcal{O}_K/\mathcal{I} \cong \mathcal{O}_K/\prod_{i=1}^L p_i$$

$$\cong \mathcal{O}_K/p_1 \times \ldots \times \mathcal{O}_K/p_L$$

$$\cong \mathbb{F}_{p_1^{f_1}} \times \ldots \times \mathbb{F}_{p_L^{f_L}}.$$  \hspace{1cm} (12)
where \( f_t \) is the inertial degree of \( p_t \) in \( \mathcal{O}_K \). We are ready to state Construction \( \pi_A \) over \( \mathcal{O}_K \).

**Construction \( \pi_A \)** Let \( n^l, N \) be integers such that \( n^l \leq N \) and let \( G_i \) be a generator matrix of an \((N, n^l)\) linear code over \( \mathbb{F}_{p_i^{[n]}} \). Construction \( \pi_A \) over \( \mathcal{O}_K \) consists of the following steps:

1. Define the discrete codebook \( C^l = \{ x = G_i \odot y : y \in (\mathbb{F}_{p_i^{[n]}})^n \} \) where all operations are over \( \mathbb{F}_{p_i^{[n]}} \).
2. Construct \( \Lambda^* \triangleq \mathcal{M}(C^1, \ldots, C^L) \) where \( \mathcal{M} : \times_{i=1}^L \mathbb{F}_{p_i^{[n]}} \rightarrow \mathcal{O}_K/\mathcal{I} \) is a ring isomorphism.
3. Tile \( \Lambda^* \) to the entire \( \mathcal{O}^N \) to form \( \Lambda \triangleq \Lambda^* + \mathcal{I}^N \).

Similar to Construction A, one can show that Construction \( \pi_A \) over \( \mathcal{O}_K \) always produces a lattice. One may also show that Construction \( \pi_A \) over \( \mathcal{O}_K \) can produce good lattices asymptotically with high probability; however, the focus of this paper is on achievable computation rates rather than complexity so we do not pursue this. The interested reader is referred to [9].

**IV. PROPOSED ADAPTIVE COMPUTE-AND-FORWARD**

In this section, we consider the scenario where there is limited feedback and propose the adaptive compute-and-forward scheme. We first use the proposed lattices to construct nested lattice codes and show that for each ring of imaginary quadratic integers, one can achieve the same rate expression (6) with elements in \( a_n \) chosen from that ring. The idea is then simply to work with the ring of integers that would result in the maximal computation rate. It is worth noting that our scheme only require limited feedback which describes with which ring the transmitters should work. This approach can be used in conjunction with the phase-precoded compute-and-forward to further improve the performance.

For a given \( \mathcal{O}_K \), we follow the construction in [14] to construct nested lattice codes. Let \( p \) be a prime ideal in \( \mathcal{O}_K \) with \( N(p) = p \) (the scheme and result for the other class of prime can be obtained in a similar way with slight modification of parameters) and \( \mathcal{M} : \mathbb{F}_p \rightarrow \mathcal{O}_K/p \). Let \((C_f, C_c)\) be a pair of nested linear code such that \( C_c \subseteq C_f \) as follows,

\[
C_c = \{ G_c \odot w | w \in \mathbb{F}_p^{m_c} \}, \\
C_f = \{ G_f \odot w | w \in \mathbb{F}_p^{m_f} \}.
\]

where \( G_c \) is a \( N \times m_c \) matrix and \( G_f = [G_c \ \tilde{G}] \) with \( \tilde{G} \) being a \( N \times (m_f - m_c) \) matrix. A pair of (scaled) nested lattice codes can be constructed by the construction described in Section [III] as

\[
\Lambda_c = \gamma p^{-1/2} \mathcal{M}(C_c) + \gamma p^{-1/2} p, \\
\Lambda_f = \gamma p^{-1/2} \mathcal{M}(C_f) + \gamma p^{-1/2} p,
\]

where \( \gamma \triangleq 2 \sqrt{2NPd^{-\frac{1}{2}}} \) is for power constraint. We then use \( \Lambda_f \cap \mathcal{V}(\Lambda_c) \) as our nested lattice code whose design rate is given by

\[
R_{\text{design}} = \frac{m_f - m_c}{N} \log(p).
\]

Each source node uses a same nested lattice code \( \Lambda_c \) as our nested lattice code whose design rate is given by

\[
x_k = (t_k - u_k) \mod \Lambda_c,
\]

where \( t_k \) is the lattice codeword corresponding to the message \( w_k \) and \( u_k \) is a random dither.

According to the channel parameters, the destination node \( m \) computes a linear combination of transmitted signals with coefficients \( a_m = [a_{m1}, \ldots, a_{mK}]^T \) being elements in \( \mathcal{O}_K \) by quantizing the following signal to the nearest lattice point in \( \Lambda_f \)

\[
y_m' = \left( a_m y_m + \sum_{k=1}^K a_{mk} u_k \right) \mod \Lambda_c \\
= (t_{eq,m} + z_{eq,m}) \mod \Lambda_c,
\]
where

$$t_{eq,m} = \sum_{k=1}^{K} a_{mk} t_{mk} \mod \Lambda_c,$$

(20)

is again a lattice codeword in \(\Lambda_f \cap V(\Lambda_c)\) since \(\Lambda_f\) and \(\Lambda_c\) are constructed over \(\mathcal{O}_K\) and

$$z_{eq,m} = \left( \alpha_m z_m + \sum_{k=1}^{K} (\alpha_m h_{mk} - a_{mk}) x_k \right),$$

(21)

is the effective noise. We then map \(t_{eq,m}\) to the following function over finite field via \(\sigma\) (recall that \(\sigma \triangleq \mathcal{M}^{-1} \circ \mod p\))

$$u_m = b_{m1} w_1 \oplus \ldots \oplus b_{mK} w_K,$$

(22)

where \(b_{mk} \triangleq \sigma(a_{mk}) \in \mathbb{F}_p\). Using the goodness results in Section II and choosing \(\alpha_m\) to be the MMSE estimator, one can follow the steps in [1] [14] to show that the following computation rate is achievable

$$R_{\mathcal{O}_K}(h_m, a_m, P) = \log^+ \left( \left( \|a_m\|^2 - \frac{P|h_m^* a_m|^2}{1 + P\|h_m\|^2} \right)^{-1} \right),$$

(23)

where \(\log^+(.) \triangleq \max\{0, \log(.)\}\). Note that here the subscript \(\mathcal{O}_K\) is used to emphasize that this is obtained by working over \(\mathcal{O}_K\). To obtain the highest computation rate for the proposed framework, one then solves the following optimization problem to decide which \(\mathcal{O}_K\) to work with.

$$R(H, P) = \max_{\mathcal{O}_K} \max_{\sigma(A) \text{ invertible}} R_{\mathcal{O}_K}(H, A, P),$$

(24)

where \(R_{\mathcal{O}_K}(H, A, P) = \min_m R_{\mathcal{O}_K}(h_m, a_m, P)\).

**Remark 7.** In this paper, we only consider the symmetric case in the sense that all the transmitters have the same power constraint \(P\) and all the encoders have the same rate. For constructions over \(\mathbb{Z}\) lattices, the asymmetric case has been discussed. For example, [1] also includes the case where the encoders may have different rates. This is enabled by constructing a sequence of nested fine lattices and allowing each transmitter to choose a different fine lattice in this sequence. In [15], Ntranos et al. further generalize the compute-and-forward paradigm to the scenario where transmitters may have unequal power constraints. This is done by allowing the transmitters to have different coarse and fine lattices. For the proposed scheme, one can extend it to the general case by following [1] and [15].

### A. Numerical Results

We now provide two numerical results to demonstrate the benefits of using the proposed lattices. For both the results, we consider the case where there are 2 source nodes and 2 destination nodes. In Fig. 2, we consider fixed channel coefficients \(h_{11} = h_{22} = 1\) and \(h_{12} = h_{21} = j2.449\) and show the achievable computation rates obtained by using lattices over \(\mathcal{O}_K\) of \(\mathbb{Q}(\sqrt{d})\) for \(d \in \{-1, -2, -3, -5, -6, -7\}\). One can see from Fig. 2 that although \(\mathbb{Z}[^{\sqrt{d}}]\) the ring of Eisenstein integers best approximates \(\mathbb{C}\) among all imaginary quadratic integers, for specific channel coefficients, it is possible that there are other rings of integers which have elements closer to those channel coefficients than \(\mathbb{Z}[^{\sqrt{d}}]\) does. In this example, \(\mathbb{Z}[^{\sqrt{-6}}]\) has elements closer to the specific channel coefficients than other rings considered in this simulation and hence provide the best computation rate among them.

In Fig. 3, we provide average achievable computation rates by using lattices over \(\mathcal{O}_K\) of \(\mathbb{Q}(\sqrt{d})\) for \(d \in \{-1, -2, -3, -5, -6, -7\}\). In this figure, each channel coefficient is randomly drawn from circularly symmetric Gaussian distribution with variance 1, i.e., its norm has Rayleigh distribution. We average over 10000 realizations and show that on average alternating between these 6 rings provides better performance than that provided by working over any of them individually.

\(^3\)We slightly abuse notation by allowing elements in \(a_m\) from \(\mathcal{O}_K\) while in Definition 2 it should be \(b_m\) from \(\mathbb{F}_p\). One can get around with this issue by noting that \(b_m = \sigma(a_m)\) and letting \(p \to \infty\).
Fig. 2. Comparison of computation rates for different $\mathcal{O}_K$ for the 2 by 2 case where $h_{11} = h_{22} = 1$ and $h_{12} = h_{21} = j2.449$.

Fig. 3. Comparison of average computation rates for different $\mathcal{O}_K$. The average is taken over 10000 pairs of channel realizations drawn from Rayleigh distribution.

B. Discussion

We now discuss some extensions and issues for the proposed scheme. As mentioned above, one can incorporate the idea of phase precoding into the proposed adaptive compute-and-forward framework to further improve the overall performance. Specifically, according to the channel realization, one can first choose a ring of integers to work with and then rotate the transmitted signal space towards the space formed by the linear functions at the destination nodes. Note that rotating channel coefficients and then use integers to approximate those channel coefficients is equivalent to using rotated integers to approximate the original
channel coefficients. But there are algebraic integers which cannot be expressed as rotated integers; hence in general, allowing working over other rings of algebraic integers will result in an increased computation rate.

A potential weakness of the proposed framework is the complexity issue. This comes from two different aspects. From the transmitter side, the optimization problem in (24) is in general very difficult to solve. Fortunately, good approximation algorithms have been proposed for some rings of integers. Moreover, simulation results shown above suggest that one does not have to consider too many $\mathcal{O}_K$ for getting improved performance. From the receiver side, the modulo operation with respect to an ideal may cause increased complexity. Fortunately, there are algorithms available which have polynomial running time. For example, [16, Algorithm 1.4.12] will produce a unique canonical coset representative very efficiently. Furthermore, for those $\mathcal{O}_K$ which also form Euclidean domains (there are exactly five of them corresponding to $d \in \{-1, -2, -3, -7, -11\}$), one can further reduce the complexity by taking advantage of Euclidean functions as reported in [6].

V. CONCLUSION

In this paper, we have moved beyond PIDs and generalized Construction A of lattices to general rings of algebraic integers of imaginary quadratic fields. We have then shown that such construction can produce good lattices in the sense of Poltyrev and MSE quantization. When used for compute-and-forward, these lattices have allowed us to reliably compute linear combinations of codewords with coefficients being elements in the underlying ring which the lattices are constructed over. A novel scheme named adaptive compute-and-forward has been proposed by simply working with the best ring of algebraic integers. This has allowed us to obtain higher computation rates. Moreover, one can phase-precode the proposed adaptive compute-and-forward scheme to further improve the performance.

ACKNOWLEDGE

The authors would like to thank Prof. Bobak Nazer for his question that motivated this work. The authors are thankful to Prof. Uri Erez for the discussion about showing the goodness for the proposed lattices during his visit at TAMU.

APPENDIX A

PRELIMINARIES

In this appendix, we provide background knowledge on algebra and algebraic number theory that will be useful in explaining our results. All the Lemmas are provided without proofs for the sake of brevity; however, their proofs can be found in standard textbooks, see for example [17] [18] [19].

A. Algebra

Let $\mathcal{R}$ be a commutative ring. Let $a, b \neq 0 \in \mathcal{R}$ but $ab = 0$, then $a$ and $b$ are zero divisors. If $ab = ba = 1$, then we say $a$ is a unit. Two elements $a, b \in \mathcal{R}$ are associates if $a$ can be written as the multiplication of a unit and $b$. A non-unit element $\tau \in \mathcal{R}$ is a prime if whenever $\tau$ divides $ab$ for some $a, b \in \mathcal{R}$, either $\tau$ divides $a$ or $\tau$ divides $b$. An integral domain is a commutative ring with identity and no zero divisors. An additive subgroup $\mathcal{I}$ of $\mathcal{R}$ satisfying $ar \in \mathcal{I}$ for $a \in \mathcal{I}$ and $r \in \mathcal{R}$ is called an ideal of $\mathcal{R}$. An ideal $\mathcal{I}$ of $\mathcal{R}$ is proper if $\mathcal{I} \neq \mathcal{R}$. An ideal generated by a singleton is called a principal ideal. A principal ideal domain (PID) is an integral domain in which every ideal is principal. Famous and important examples of PID include $\mathbb{Z}$, $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$. Let $a, b \in \mathcal{R}$ and $\mathcal{I}$ be an ideal of $\mathcal{R}$; then $a$ is congruent to $b$ modulo $\mathcal{I}$ if $a - b \in \mathcal{I}$. The quotient ring $\mathcal{R}/\mathcal{I}$ of $\mathcal{R}$ by $\mathcal{I}$ is the ring with addition and multiplication defined as

\[(a + \mathcal{I}) + (b + \mathcal{I}) = (a + b) + \mathcal{I}, \quad \text{and}\]
\[(a + \mathcal{I}) \cdot (b + \mathcal{I}) = (a \cdot b) + \mathcal{I}. \quad (25)\]

(26)
A proper ideal \( p \) of \( \mathcal{R} \) is said to be a **prime ideal** if for \( a, b \in \mathcal{R} \) and \( ab \in p \), then either \( a \in p \) or \( b \in p \). A proper ideal \( \mathcal{I} \) of \( \mathcal{R} \) is said to be a **maximal ideal** if \( \mathcal{I} \) is not contained in any strictly larger proper ideal. It should be noted that every maximal ideal is also a prime ideal but the reverse may not be true. Let \( \mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_L \) be a family of rings, the direct product of these rings, denoted by \( \mathcal{R}_1 \times \mathcal{R}_2 \times \ldots \times \mathcal{R}_L \), is the direct product of the additive abelian groups \( \mathcal{R}_i \) equipped with multiplication defined by the **componentwise** multiplication.

Let \( \mathcal{I}_1 \) and \( \mathcal{I}_2 \) be two ideals of \( \mathcal{R} \), we shall now define some operations of ideals. The sum of two ideals is the ideal defined as

\[
\mathcal{I}_1 + \mathcal{I}_2 \triangleq \{ a + b : a \in \mathcal{I}_1, b \in \mathcal{I}_2 \}.
\]

Two ideals are **relatively prime** if \( \mathcal{I} = \mathcal{I}_1 + \mathcal{I}_2 \). The product of two ideals is the ideal defined as

\[
\mathcal{I}_1\mathcal{I}_2 \triangleq \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathcal{I}_1, b_i \in \mathcal{I}_2, n \in \mathbb{N} \right\}.
\]

In general, we have \( \mathcal{I}_1\mathcal{I}_2 \subseteq \mathcal{I}_1 \cap \mathcal{I}_2 \); but if they are relatively prime, then \( \mathcal{I}_1\mathcal{I}_2 = \mathcal{I}_1 \cap \mathcal{I}_2 \). We say \( \mathcal{I}_1 \) divides \( \mathcal{I}_2 \) or \( \mathcal{I}_1|\mathcal{I}_2 \) if there is an ideal \( \mathcal{I}_3 \) such that \( \mathcal{I}_2 = \mathcal{I}_1\mathcal{I}_3 \) (this is equivalent to \( \mathcal{I}_2 \subseteq \mathcal{I}_1 \)).

Let \( \mathcal{R}_1 \) and \( \mathcal{R}_2 \) be rings. A function \( \sigma : \mathcal{R}_1 \rightarrow \mathcal{R}_2 \) is a **ring homomorphism** if

\[
\sigma(a + b) = \sigma(a) \oplus \sigma(b) \quad \forall a, b \in \mathcal{R}_1 \quad \text{and} \quad \sigma(ab) = \sigma(a) \odot \sigma(b) \quad \forall a, b \in \mathcal{R}_1,
\]

where \((+,\cdot)\) and \((\oplus,\odot)\) are operations in \( \mathcal{R}_1 \) and \( \mathcal{R}_2 \), respectively. A homomorphism is said to be **monomorphism** if it is injective and **isomorphism** if it is bijective. Let \( \mathcal{R} \) be a commutative ring, and \( \mathcal{I}_1, \ldots, \mathcal{I}_n \) be ideals in \( \mathcal{R} \). Then, from the Chinese Remainder Theorem, we have

\[
\mathcal{R}/ \cap_{i=1}^{n} \mathcal{I}_i \cong \mathcal{R}/\mathcal{I}_1 \times \ldots \times \mathcal{R}/\mathcal{I}_n.
\]

**B. Algebraic Numbers and Algebraic Integers**

Now, we provide some background knowledge on algebraic number theory. The materials are mostly from [18] [19] and proofs and algorithms can be found therein.

**Definition 8** (Algebraic Numbers and Algebraic Number Fields). An algebraic number is a root of some polynomial with coefficients in \( \mathbb{Z} \). The set of all algebraic numbers is a subfield \( \mathbb{A} \) of \( \mathbb{C} \). We define a number field to be a subfield \( \mathbb{K} \) of \( \mathbb{A} \) (hence a subfield of \( \mathbb{C} \)) such that the degree \( [\mathbb{K} : \mathbb{Q}] \) is finite.

Theorem 2.2 in [18] shows that any such \( \mathbb{K} \) is equal to \( \mathbb{Q}(\theta) \), the smallest subfield containing \( \mathbb{Q} \) and \( \theta \), for some algebraic number \( \theta \).

**Definition 9** (Algebraic Integers). An algebraic integer is a complex number which is a root of some monic polynomial (whose leading coefficient is 1) with coefficients in \( \mathbb{Z} \). The set of all algebraic integers forms a subring \( \mathbb{B} \) of \( \mathbb{C} \). For any number field \( \mathbb{K} \), we write \( \mathbb{O}_\mathbb{K} = \mathbb{K} \cap \mathbb{B} \) and call \( \mathbb{O}_\mathbb{K} \) the ring of integers of \( \mathbb{K} \). From Corollary 2.12 in [18], one has that if \( \mathbb{K} \) is a number field then \( \mathbb{K} = \mathbb{Q}(\theta) \) for an algebraic integer \( \theta \) which is called a primitive element for \( \mathbb{K} \) over \( \mathbb{Q} \). Also, in general, there will be several distinct \( \mathbb{Q} \)-monomorphisms (i.e., it fixes \( \mathbb{Q} \)) embedding \( \mathbb{K} \) into \( \mathbb{C} \). From Theorem 2.4 in [18], we know that for \( \mathbb{K} = \mathbb{Q}(\theta) \) a number field of degree \( n \) over \( \mathbb{Q} \), there are exactly \( n \) distinct \( \mathbb{Q} \)-monomorphism \( \sigma_i : \mathbb{K} \rightarrow \mathbb{C} \) and such monomorphisms form a group \( \text{Gal}(\mathbb{K}/\mathbb{Q}) \triangleq \{\sigma_1, \ldots, \sigma_n\} \) which is referred to as the Galois group. Moreover, for \( \alpha \in \mathbb{Q}(\theta) \), \( \sigma_i(\alpha) \) for \( i \in \{1,2,\ldots,n\} \) are the distinct zeros in \( \mathbb{C} \) of the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \). We call those \( \sigma_i(\alpha) \) the **conjugates** of \( \alpha \) and define the **norm** of \( \alpha \) to be the product of conjugates as

\[
N_{\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).
\]

(32)
Let \( \{\alpha_1, \ldots, \alpha_n\} \) be a \( \mathbb{Q} \)-basis for \( \mathbb{K} \). We define the discriminant of \( \{\alpha_1, \ldots, \alpha_n\} \) as

\[
\Delta[\alpha_1, \ldots, \alpha_n] \triangleq \det \begin{pmatrix}
\sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\
\sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\
\vdots & \vdots & \ddots & \vdots \\
\sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n)
\end{pmatrix}^2.
\] (33)

If \( \{\alpha_1, \ldots, \alpha_n\} \) is a \( \mathbb{Z} \)-basis for \( \mathcal{O}_K \), we define the discriminant of \( \mathbb{K} \) to be \( \Delta_K \triangleq \Delta[\alpha_1, \ldots, \alpha_n] \). Let \( \mathfrak{I} \) be an ideal of \( \mathcal{O}_K \). The norm of \( \mathfrak{I} \) is \( N(\mathfrak{I}) \triangleq |\mathcal{O}_K/\mathfrak{I}| \). Moreover, if \( \{\beta_1, \ldots, \beta_n\} \) is a \( \mathbb{Z} \)-basis for \( \mathfrak{I} \), then \( N(\mathfrak{I}) = \sqrt{\Delta[\beta_1, \ldots, \beta_n]} \). The norm is multiplicative, i.e., for two ideals \( \mathfrak{I}_1 \) and \( \mathfrak{I}_2 \) of \( \mathcal{O}_K \), \( N(\mathfrak{I}_1\mathfrak{I}_2) = N(\mathfrak{I}_1)N(\mathfrak{I}_2) \). It can be shown that if \( N(p) \) is a rational prime, then \( p \) is a prime ideal.

In this paper, we are particularly interested in imaginary quadratic fields and their algebraic integers whose definitions can be found in the following.

**Definition 10 (Quadratic Fields).** A quadratic field is an algebraic number field \( \mathbb{K} \) of degree \([\mathbb{K} : \mathbb{Q}] = 2\) over \( \mathbb{Q} \). Particularly, one may write \( \mathbb{K} = \mathbb{Q}(\sqrt{d}) \) where \( d \in \mathbb{Z} \) is square free. We say \( \mathbb{K} \) is an imaginary quadratic field if \( d < 0 \).

Let \( \mathbb{K} = \mathbb{Q}(\sqrt{d}) \). One can show that \( \mathcal{O}_K = \mathbb{Z}[\xi] \) where

\[
\xi = \begin{cases}
\sqrt{d}, & d \equiv 2,3 \mod 4, \\
\frac{1 + \sqrt{d}}{2}, & d \equiv 1 \mod 4.
\end{cases}
\] (34)

Also, \( \Delta_K = 4d \) if \( d \equiv 2,3 \mod 4 \) and \( \Delta_K = d \) if \( d \equiv 1 \mod 4 \). It can be easily seen that when \( d = -1 \) we have the Gaussian integers and when \( d = -3 \) we have the Eisenstein integers.

**Example 11.** Let us consider the case \( d = -5 \), i.e., \( \mathbb{K} = \mathbb{Q}(\sqrt{-5}) \). Let \( \alpha = a + b\sqrt{-5} \) where \( a, b \in \mathbb{Z} \). Since the degree is 2, there are exactly two \( \mathbb{Q} \)-monomorphisms. In order to have a \( \mathbb{Q} \)-monomorphism, one must have \( \sigma(\sqrt{-5}) \cdot \sigma(-\sqrt{-5}) = \sigma(-5) = -5 \), which implies that \( \sigma(\sqrt{-5}) = \pm\sqrt{-5} \). Thus one has that

\[
\begin{align*}
\sigma_1(\alpha) &= a + b\sqrt{-5} = a + b\sqrt{-5}, \\
\sigma_2(\alpha) &= a + b\sqrt{-5} = a - b\sqrt{-5}.
\end{align*}
\] (35)

Then the norm of \( \alpha \) is \( \sigma_1(\alpha) \cdot \sigma_2(\alpha) = a^2 + 5b^2 \) which coincides with the Euclidean norm. Since \( -5 \equiv 3 \mod 4 \), from (7), \( \{1, \sqrt{-5}\} \) is a \( \mathbb{Z} \)-basis for \( \mathcal{O}_K \). One can calculate the discriminant as follows,

\[
\Delta_K = \det \begin{pmatrix}
1 & \sqrt{-5} \\
1 & -\sqrt{-5}
\end{pmatrix}^2 = -20.
\] (36)

Consider a prime \( p \), \( p\mathbb{Z} \) is a prime ideal in \( \mathbb{Z} \). Let \( \mathfrak{p} \) be a prime ideal of \( \mathcal{O}_K \). We say \( \mathfrak{p} \) lies above \( p \) if \( p|\mathfrak{p}\mathcal{O}_K \). The ideal \( p\mathcal{O}_K \) can be uniquely factorized into \( p\mathcal{O}_K = \prod_{i=1}^L p_i^{e_i} \) with \( p_i \) distinct. We call \( e_i \) the ramification index of \( p_i \) over \( p \) and \( f_i = [\mathcal{O}_K/p_i : \mathbb{Z}/p\mathbb{Z}] \) the inertial degree of \( p_i \) over \( p \). Note that one must have \( N(p_i) = p^{f_i} \). Also, the ramification indices and inertial degrees must satisfy \( \sum_{i=1}^L e_if_i = n \). If \( e_i > 1 \) for some \( l \), we say \( p \) (or \( p\mathcal{O}_K \) to be precise) ramifies in \( \mathcal{O}_K \). If \( L > 1 \), we say \( p \) splits in \( \mathcal{O}_K \). If \( L = 1 \) and \( e_1 = 1 \) (i.e., \( f_1 = n \)), we say \( p \) remains inert in \( \mathcal{O}_K \). The following Lemma allows one to efficiently categorize primes.

**Lemma 12.** Let \( p \) be a rational prime. For a quadratic field \( \mathbb{K} \), one has

- if \( \left( \frac{\Delta_K}{p} \right) = 0 \), then \( p \) ramifies in \( \mathcal{O}_K \),
- if \( \left( \frac{\Delta_K}{p} \right) = 1 \), then \( p \) splits in \( \mathcal{O}_K \),
- if \( \left( \frac{\Delta_K}{p} \right) = -1 \), then \( p \) remains inert in \( \mathcal{O}_K \),
where \( \left( \frac{\Delta_K}{p} \right) \) is the Kronecker symbol \( \mod p \). Moreover, the Kronecker symbol \( \mod p \) operation can be efficiently computed. (See for example [20, Algorithm 1.4.10].)

It is well-known that not every ring of imaginary quadratic integers forms a PID. In fact, it was conjectured by Gauss and shown by Heegner and Stark that there are only 9 of them that are PIDs (corresponding to \( d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\} \)). Therefore, it is crucial to have a systematic way to identify prime ideals. The following theorem provides a means of doing this.

**Lemma 13.** Let \( p \) be an odd rational prime. For a quadratic field \( K = \mathbb{Q}(\sqrt{d}) \), one has

- if \( p \) ramifies in \( \mathcal{O}_K \), then \( p = (p, \sqrt{d}) \) is a prime ideal lying above \( p \),
- if \( p \) splits in \( \mathcal{O}_K \), then \( p = (p, a + \sqrt{d}) \) is a prime ideal lying above \( p \) for any \( a \) such that \( a^2 \equiv d \mod p \).

Moreover, such \( a \) can be efficiently found (See for example [20, Algorithm 1.5.1].)

One important property of \( \mathcal{O}_K \) is that every prime ideal is maximal. Therefore, we have that for every prime ideal \( p \) in \( \mathcal{O}_K \),

\[
\mathcal{O}_K/p \cong \mathbb{F}_{p^f},
\]

where \( f \) is the inertial degree described above.

**Example 14.** Again consider \( d = -5 \), i.e., \( K = \mathbb{Q}(\sqrt{-5}) \), and \( p = 23 \). We have that \( \left( \frac{\Delta_K}{p} \right) = 1 \); hence, \( 23\mathbb{Z} \) splits into two prime ideals in \( \mathcal{O}_K \). From the above theorem, one can check that \( 8^2 \equiv -5 \mod 23 \); thus, \( \mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}} \) where \( \mathfrak{p} = (23, 8 + \sqrt{-5}) \). Also, we have

\[
\Delta_K = \det \left( \begin{array}{cc} 23 & 8 + \sqrt{-5} \\ 23 & 8 - \sqrt{-5} \end{array} \right)^2 = -10580.
\]

Therefore, \( N(p) = \sqrt{-10580}/20 = 23 \). Moreover, \( \mathcal{O}_K/p \cong \mathbb{F}_{23} \). This coset decomposition and the corresponding ring isomorphism is shown in Fig. 4.

**Lemma 15** (Dirichlet’s prime theorem). For any two relatively prime integers \( a \) and \( d \), there are infinitely many rational primes of the form \( p \equiv a \mod d \).

Lemma 12 and Lemma 15 together imply that for any quadratic field \( K \), there exist infinitely many splitting primes and infinitely many inert primes as well. In what follows, we provide a weaker version of the Chebotarev’s density theorem which further tells us how those primes distribute asymptotically.
Lemma 16 (Chebotarev’s density theorem). In a ring of algebraic integers of a quadratic field, asymptotically, the density of each category of primes is 1/2, i.e., asymptotically, half of the rational primes split and half of them remain inert.

Appendix B
Proofs

In this appendix, we show that Construction A over \( \mathfrak{O}_K \) can produce good lattices with high probability. Throughout the proof, we only use those primes which split completely in \( \mathfrak{O}_K \) for the sake of simplicity; however, this is by no means necessary and the other class of primes can be used as well.

A. Poltyrev-Goodness

The proof closely follows the steps in [13]. Let \( p \) be a splitting prime in \( \mathfrak{O}_K \), i.e., \( p \mathfrak{O}_K \) splits into two prime ideals in \( \mathfrak{O}_K \), namely \( p \mathfrak{O}_K = \mathfrak{p} \mathfrak{p} \). Therefore, we have \( \mathfrak{O}_K / p \cong \mathfrak{O}_K / \mathfrak{p} \cong \mathbb{F}_p \). Let \( \mathcal{C} \) be the collection of all \((N, n)\) linear codes \( \mathcal{C} \) over \( \mathbb{F}_p \). The set \( \mathcal{C} \) is a balanced set and the basic averaging lemma [13, Lemma 1] applies. Thus, one has

\[
\frac{1}{|\mathcal{C}|} \sum_{\mathcal{C}} \sum_{\mathcal{C} \in \mathcal{C} \setminus \mathcal{C} \setminus \mathcal{C}} \frac{f(c)}{p^n - 1} \sum_{v \in (\mathbb{F}_p^N) \setminus 0} f(v),
\]

for an arbitrary mapping \( f : \mathbb{F}_p^N \to \mathbb{R}^N \). Since we can identify \( \mathbb{C} \) by \( \mathbb{R}^2 \), the basic averaging lemma works for arbitrary mapping \( f : \mathcal{M}(\mathbb{F}_p^N) \to \mathbb{C}^N \) as well and we use \( \mathbb{C}^N \) and \( \mathbb{R}^{2N} \) interchangeably in the following.

Theorem 17 (Modified Minkowski-Hlawka Theorem). Let \( f : \mathbb{R}^{2N} \to \mathbb{R} \) be a Riemann integrable function of bounded support. Then, for any integer \( 0 < n < N \), and any fixed \( \text{Vol}(\mathcal{V}_\lambda) \), the approximation

\[
\frac{1}{|\mathcal{C}|} \sum_{\mathcal{C} \in \mathcal{C} \setminus \mathcal{C} \setminus \mathcal{C}} f(v) \approx \text{Vol}(\mathcal{V}_\gamma)^{-1} \int_{\mathbb{R}^{2N}} f(v) dv,
\]

becomes exact in the limit \( p \to \infty \). \( \gamma \approx (\sqrt{\frac{|\mathcal{D}|}{2}})^{-N} \), \( \text{Vol}(\mathcal{V}_\gamma) = \gamma^{2N} (\sqrt{\frac{|\mathcal{D}|}{2}})^{Np^{-n}} \) fixed.

Before proceeding to the proof, we first note that due to Dirichlet’s prime theorem (Lemma 15) and Chebotarev’s density theorem (Lemma 16), there exist infinitely many splitting primes in every \( \mathfrak{O}_K \) so that one can safely let \( p \) go to infinity.

Proof: Note that by the basic averaging lemma,

\[
\frac{1}{|\mathcal{C}|} \sum_{\mathcal{C} \in \mathcal{C} \setminus \mathcal{C} \setminus \mathcal{C}} \sum_{v \in \mathcal{V}_\lambda \setminus \mathcal{C}} f(v) = \frac{1}{|\mathcal{C}|} \sum_{\mathcal{C} \in \mathcal{C} \setminus \mathcal{C} \setminus \mathcal{C}} \left[ \sum_{v \in (\mathcal{D}_K^N : \sigma(v) = 0) \setminus 0} f(\gamma v) + \sum_{v \in (\mathcal{D}_K^N : \sigma(v) = 0) \setminus 0} f(\gamma v) \right]
\]

\[
= \sum_{v \in (\mathcal{D}_K^N : \sigma(v) = 0) \setminus 0} f(\gamma v) + \frac{1}{|\mathcal{C}|} \sum_{\mathcal{C} \in \mathcal{C} \setminus \mathcal{C} \setminus \mathcal{C}} \left[ \sum_{v \in (\mathcal{D}_K^N : \sigma(v) = 0) \setminus 0} f(\gamma v) \right]
\]

\[
= \sum_{v \in (\mathcal{D}_K^N : \sigma(v) = 0) \setminus 0} f(\gamma v) + \frac{1}{|\mathcal{C}|} \sum_{\mathcal{C} \in \mathcal{C} \setminus \mathcal{C} \setminus \mathcal{C}} \left[ \sum_{v \in (\mathcal{D}_K^N : \sigma(v) = 0) \setminus 0} f(\gamma v) \right]
\]

\[
= \sum_{v \in (\mathcal{D}_K^N : \sigma(v) = 0) \setminus 0} f(\gamma v) + \frac{p^n - 1}{p^n - 1} \sum_{v \in (\mathcal{D}_K^N : \sigma(v) = 0) \setminus 0} f(\gamma v)
\]

\[
\approx p^n N \gamma^{-2N} \left( \frac{\sqrt{|\mathcal{D}|}}{2} \right)^{-N} \sum_{v \in (\mathcal{D}_K^N : \sigma(v) \neq 0)} f(v) \gamma^{2N} \left( \frac{\sqrt{|\mathcal{D}|}}{2} \right)^N
\]
\[
\text{Vol}(V_{\gamma A})^{-1} \int_{B^{2N}} f(v) dv. \tag{41}
\]

where (a) requires \( \gamma p \) being large and \( f \) having bounded support and (b) requires \( \gamma^2 \sqrt{|\Delta_2|} \) to be small so that the Riemann sum approaches the Riemann integral.

One can then follow the proof in [13] to show that with high probability, the proposed construction produces lattices that are Poltyrev-good.

**B. MSE Quantization-Goodness**

The proof closely follows the steps in [14]. We only consider \( \mathfrak{D}_K \) the ring of algebraic integers for \( \mathbb{Q}(\sqrt{d}) \) with \( d \equiv 2, 3 \mod 4 \); the case of \( d \equiv 1 \mod 4 \) can be proved similarly with slight modification of parameters. Denote by \( V_N \) the volume of an \( N \)-dimensional ball with unit radius and let \( B(s, r) \) be a \( 2N \)-dimensional ball with radius \( r \) centered at \( s \). We again prove the result for \( p \) primes splitting completely in \( \mathfrak{D}_K \) only, i.e., \( N(p) = p \) for a prime ideal \( p \) lying above \( p \). Note that scaling would not change lattice structure; in the sequel, we equivalently consider the scaled version

\[
\Lambda = \gamma p^{-1/2} M(C) + \gamma p^{-1/2} p,
\]

where \( \gamma = 2 \sqrt{2Np|d|^{-1/2}} \) and we pick \( p \geq 2N^3 \). Note that since here we constrain \( p \) to those splitting, one cannot use the Bertrand’s postulate to guarantee that for any \( N \), there always exists a \( \xi \in [1/2, 1] \) such that \( \xi^2 N^3 \) is a prime square as done in [14]. Although there are generalized versions of the Bertrand’s postulate that may solve the problem for some \( \mathfrak{D}_K \) (see for example [21] and reference therein), we do not pursue this as a bound would be sufficient.

**Lemma 18** (Modified Lemma 1 in [14]). For any \( s \in \mathbb{R}^{2N} \) and \( r > 0 \), the number of points of \( \mathfrak{D}_K^N \) inside \( B(s, r) \) can be bounded as

\[
\left( \max \{ r - \frac{\sqrt{2N|d|}}{2}, 0 \} \right)^{2N} \cdot \frac{V_{2N}}{(\sqrt{|\Delta_2|}/2)^N} \leq |\mathfrak{D}_K^N \cap B(s, r)| \leq \left( r + \frac{\sqrt{2N|d|}}{2} \right)^{2N} \cdot \frac{V_{2N}}{(\sqrt{|\Delta_2|}/2)^N}. \tag{43}
\]

**Proof:** Similar to [14, Lemma 1] and hence omitted.

For any \( x \in \mathbb{C}^N \), define

\[
d(x, \Lambda) = \frac{1}{2N} \min_{\lambda \in \Lambda} \| x - \gamma^{-1/2} M(c) - \gamma^{-1/2} a \|^2
\]

\[
= \frac{1}{2N} \min_{\| c \| = 1} \| x - \gamma^{-1/2} M(c) \|^2
\]

\[
= \frac{1}{2N} \min_{c \in C} \| (x - \gamma^{-1/2} M(c))^* \|^2.
\]

where \( y^* \equiv y \mod \gamma^{-1/2} p \). Also, note that

\[
d(x, \Lambda) \leq \frac{1 + |d|}{4} \gamma^2. \tag{45}
\]

Recall that for the case considered (\( d \equiv 2, 3 \mod 4 \)), \( \Delta_2 = 4d \). For any \( w \in \mathbb{F}_p^n \setminus 0 \), define the random vector \( C(w) = G \odot w^T \) which is uniformly distributed over \( \mathbb{F}_p^N \). Thus, \( M(C(w)) \) is uniformly distributed over \( (\mathfrak{D}_K/p)^N \).
For all \( w \in \mathbb{F}_p^n \setminus 0 \) and \( x \in \mathbb{C}^N \), we have

\[
\varepsilon \triangleq \Pr \left( \frac{1}{2N} \| (x - \gamma p^{-1/2} C(w))^* \|^2 \leq P \right)
\]

\[
= p^{-N} \left| \gamma p^{-1/2} (\mathcal{D}_K/p)^N \cap \mathcal{B}(x, \sqrt{2NP}) \right|
\]

\[
= p^{-N} \left| \gamma p^{-1/2} \mathcal{D}_K^N \cap \mathcal{B}(x, \sqrt{2NP}) \right|
\]

\[
\geq p^{-N} \left( \gamma^{-1} \sqrt{p \sqrt{2NP}} - \frac{\sqrt{2N|d|}}{2} \right)^{2N} \cdot \frac{V_{2N}}{\sqrt{|d|}^N}
\]

\[
= V_{2N}(\gamma^{-2}2NP|d|^{-\frac{1}{2}})^N \left( 1 - \frac{\gamma \sqrt{|d|}}{2\sqrt{p\sqrt{2NP}}} \right)^{2N}
\]

\[
\leq V_{2N}2^{-2N} \left( 1 - \frac{\sqrt{2N|d|}}{\sqrt{p}} \right)^{2N}
\]

\[
\geq V_{2N}2^{-2N} \left( 1 - \frac{\sqrt{|d|}}{N} \right)^{2N}
\]

\[
\geq \frac{1}{(2N)^2} V_{2N}2^{-2N}, \tag{46}
\]

where (a) is from Lemma 18, (b) is due to the choice \( \gamma = 2\sqrt{2N|d|^{-\frac{1}{2}}} \), (c) is due to the choice \( p \geq 2N^3 \), and (d) is true for sufficiently large \( N \). This can be verified by noting that \( (1 - \sqrt{|d|/N})^{2N} \) is a positive strictly increasing function for \( N \geq \sqrt{|d|} \) and will converge to \( \exp(-2\sqrt{|d|}) > 0 \) while \( 1/(2N)^2 \) is a positive strictly decreasing function and will converge to 0.

Let \( W = p^n - 1 \) and label each of the \( w \in \mathbb{F}_p^n \setminus 0 \) by \( i = 1, \ldots, W \). Define the indicator random variable related to \( x \in \mathbb{C}^N \) as

\[
\chi_i \triangleq \begin{cases} 
1, & \frac{1}{2N} \| (x - \gamma p^{-1/2} C_i)^* \|^2 \leq P \\
0, & \text{otherwise}
\end{cases}
\]

One has that for any \( x \in \mathbb{C}^N \)

\[
\Pr \left( \langle d(x, \Lambda) \rangle > P \right) = \Pr \left( \sum_{i=1}^W \chi_i = 0 \right)
\]

\[
\leq \Pr \left( \left| \sum_{i=1}^W \chi_i - \varepsilon \right| \geq \varepsilon \right)
\]

\[
\leq \frac{\var\left( \frac{1}{W} \sum_{i=1}^W \chi_i \right)}{\varepsilon^2}
\]

\[
= \frac{1}{W^2 \varepsilon^2} \sum_{i=1}^W \sum_{l=1}^W \text{Cov}(\chi_i, \chi_l)
\]

\[
\leq \frac{p}{W \varepsilon}
\]

\[
< (2N)^5 p^{n-2}N_{2N}^{-1}, \tag{48}
\]

where (a) follows from the Chebyshev’s inequality, (b) is due to the fact that \( C(w_1) \) and \( C(w_2) \) are statistically independent unless \( w_1 = a \cdot w_2 \) for \( a \in \mathbb{F}_q \), and (c) is by plugging in (46).
Following [14], one can show that for any distribution on $X$, we have
\[
\mathbb{E}_{X,\Lambda}(d(X,\Lambda)) \leq P \left( 1 + \delta (2N)^{62} \frac{\log(p) - \log\left(\frac{\delta}{\sqrt{2N}}\right)}{N} \right),
\]
(49)
where $\delta \triangleq (1 + |d|) \sqrt{|d|}$ is a constant. This in turn implies that
\[
\lim_{N \to \infty} \mathbb{E}_\Lambda \left( \sigma^2(\Lambda) \right) \leq P,
\]
(50)
if one chooses the coding rate to be
\[
\frac{n}{N} \log(p) = \log\left(\frac{4}{V_{2N}^2 N^2} \right) + \epsilon,
\]
(51)
for $\epsilon > 0$. The volume of the fundamental Voronoi region is lower bounded by
\[
\operatorname{Vol}(V_\Lambda)^{2/2N} \geq \left( \frac{\gamma^2}{p} \right)^{p N} \sqrt{|d|}^{N} \left( \frac{p N}{p^n} \right)^{2/2N}
= \left( \frac{\gamma^2}{p} \right)^{p^{-n/2}} |d|^N
= 4 \cdot 2N p^{-n/2}
= 2^{-\epsilon} 2NP V_{2N}^{2/2N}.
\]
(52)
Hence, we have
\[
\lim_{2N \to \infty} \mathbb{E}_\Lambda \left( G_\Lambda \right) = \lim_{2N \to \infty} \mathbb{E}_\Lambda \left( \frac{\sigma^2(\Lambda)}{(\operatorname{Vol}(V_\Lambda)^{2/2N})} \right)
\leq \lim_{2N \to \infty} \frac{\mathbb{E}_\Lambda(\sigma^2(\Lambda))}{2^{-\epsilon} 2NP V_{2N}^{2/2N}}
= 2^\epsilon \lim_{2N \to \infty} \frac{1}{V_{2N}^{2/2N}}
= 2^\epsilon \frac{1}{2\pi \exp(1)}.
\]
(53)
Similar to [14], one can then use the above result to show that asymptotically, most of the lattices thus constructed will be good for MSE quantization.

REFERENCES

[1] B. Nazer and M. Gastpar, “Compute-and-forward: Harnessing interference through structured codes,” IEEE Trans. Inf. Theory, vol. 57, pp. 6463–6486, Oct. 2011.
[2] C. Feng, D. Silva, and F. R. Kschischang, “An algebraic approach to physical-layer network coding,” IEEE Trans. Inf. Theory, vol. 59, pp. 7576–7596, Nov. 2013.
[3] N. E. Tunali, K. Narayanan, J. Boutros, and Y.-C. Huang, “Lattices over Eisenstein integers for compute-and-forward,” in Proc. Allerton Conf., Oct. 2012. arXiv:1404.1312 [cs.IT].
[4] U. Niesen and P. Whiting, “The degrees of freedom of compute-and-forward,” IEEE Trans. Inf. Theory, vol. 58, pp. 5214–5232, Aug. 2012.
[5] A. Sakzad, E. Viterbo, J. J. Boutros, and Y. Hong, “Phase precoded compute-and-forward with partial feedback,” in Proc. IEEE ISIT, June 2014.
[6] A. Vazquez-Castro, “Arithmetic geometry of compute and forward,” in Inf. Theory Workshop, 2014.
[7] Y.-C. Huang and K. Narayanan, “Lattices from codes for harnessing interference: An overview and generalizations,” in Inf. Theory Workshop, 2014. arXiv:1406.3368 [cs.IT].
[8] B. Hern and K. Narayanan, “Multilevel coding schemes for compute-and-forward with flexible decoding,” IEEE Trans. Inf. Theory, vol. 59, pp. 7613–7631, Nov. 2013.
[9] Y.-C. Huang and K. R. Narayanan, “Multistage compute-and-forward with multilevel lattice codes based on product constructions,” in Proc. IEEE ISIT, June 2014. arXiv:1401.2228 [cs.IT].
[10] U. Erez and R. Zamir, “Achieving $\frac{1}{2}\log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding,” IEEE Trans. Inf. Theory, vol. 50, pp. 2293–2314, Oct. 2004.
[11] J. Leech and N. J. A. Sloane, “Sphere packing and error-correcting codes,” Canad. J. Math., vol. 23, no. 4, pp. 718–745, 1971.
[12] J. H. Conway and N. J. A. Sloane, Sphere Packings, Lattices, and Groups. Springer Verlag, 1999.
[13] H.-A. Loeliger, “Averaging bounds for lattices and linear codes,” IEEE Trans. Inf. Theory, vol. 43, pp. 1767–1773, Nov. 1997.
[14] O. Ordentlich and U. Erez, “A simple proof for the existence of good pairs of nested lattices,” arXiv:1209.5083 [cs.IT], Sept. 2012.
[15] V. Ntranos, V. Cadambe, B. Nazer, and G. Caire, “Asymmetric compute-and-forward,” in Proc. Allerton Conf., pp. 1174–1181, Oct. 2013.
[16] H. Cohen, Advanced Topics in Computational Number Theory (Graduate Texts in Mathematics). Springer, 2000.
[17] T. W. Hungerford, Algebra (Graduate Texts in Mathematics). Springer, 1974.
[18] I. Steward and D. Tall, Algebraic Number Theory and Fermat’s Last Theorem. A K Peters, Ltd., 2001.
[19] S. Lang, Algebraic Number Theory (Graduate Texts in Mathematics). Springer Verlag, 1994.
[20] H. Cohen, A Course in Computational Algebraic Number Theory (Graduate Texts in Mathematics). Springer, 1993.
[21] P. Moree, “Bertrand’s postulate for primes in arithmetical progressions,” Computers Math. Applic., vol. 26, no. 5, pp. 35–43, 1993.