Received 5 August 2024; accepted 26 August 2024. Date of publication 29 August 2024; date of current version 11 September 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3452040

A Simpler Proof on the Existence of Good Nested Lattice Codes Over Imaginary Quadratic Integers for AWGN Channel

MARYAM SADEGHI [1] (Member, IEEE), RENMING QI [1], CHEN FENG [1] (Member, IEEE), HASSAN KHODAIEMEHR [1], AND YU-CHIH HUANG [2] (Senior Member, IEEE)

[1] School of Engineering, University of British Columbia (Okanagan Campus), Kelowna, BC V1V 1V7, Canada

[2] Institute of Communication Engineering, National Yang Ming Chiao Tung University, Hsinchu 300, Taiwan

CORRESPONDING AUTHOR: M. SADEGHI (e-mail: maryam.sadeghi@ubc.ca)

The work of Yu-Chih Huang was supported by the National Science and Technology Council, Taiwan, under Grant NSTC 113-2223-E-A49-005-MY3.

ABSTRACT This paper investigates nested lattice codes generated through Construction A from the ring of integers of an imaginary quadratic field. Our primary goal is to offer a streamlined proof of the existence of nested lattice codes that can attain the capacity of an Additive White Gaussian Noise (AWGN) channel. We alter the random ensemble of nested lattice codes by introducing discrete random dithers instead of continuous random dithers. This adjustment enables us to draw a parallel between nested lattice codes and nested linear codes, facilitating a proof that remains as straightforward as that used for nested linear codes. Furthermore, we demonstrate that this collection of lattices exhibits favorable properties for Mean Square Error (MSE) quantization under specific constraints.

INDEX TERMS Algebraic integers, AWGN channel, lattice codes, MSE quantization.

I. INTRODUCTION

LATTICES are discrete subgroups of $\mathbb{R}^n$ that serve as essential structures with applications spanning numerous disciplines such as sphere packing, quantization, modulation, and channel capacity optimization. Construction A, B, C, D, and E are notable lattice construction approaches that frequently use linear block codes for implementation [1]. The primary distinctions among Constructions A, B, and C lie in the types of codes they employ. In Construction B, a binary code with even weight is utilized, whereas Constructions A and C can employ any code. Additionally, as defined in [2], Construction B specifies that a vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is a lattice point if $\sum_{i=1}^{n} x_i$ is divisible by 4. In contrast, Construction C is described as a sphere packing in $\mathbb{R}^n$, which does not necessarily form a lattice. Furthermore, Construction D is a special case of Construction C that utilizes nested codes.

Algebraic lattices, formed from the ring of integers of number fields or their ideals, are a diverse family of lattices. Construction A generates lattices over $\mathbb{R}^n$ by using a linear code C of length n over a finite field $\mathbb{F}_p$, as well as a mapping from $\mathbb{Z}^n$ to $\mathbb{F}_p^n$ via reduction modulo p. These lattices, known as algebraic Construction A lattices, have been widely investigated [3], [4]. Despite their theoretical significance, algebraic lattices' practical application has been hampered by the inherent difficulty of their structured construction. Recent improvements expand Construction A to include a broader class of imaginary quadratic fields, allowing research of varied lattice structures outside typical Principle Ideal Domains (PIDs), such as Gaussian integers $\mathbb{Z}[i]$ and Eisenstein integers $\mathbb{Z}[\omega]$, where $\omega = e^{i2\pi/3}$ [4].

Algebraic lattices defined over imaginary quadratic fields, such as Gaussian integers and Eisenstein integers, prove to be a potent tool in combating errors in AWGN channels. By harnessing their properties, we can design robust error correction codes and construct cryptographic primitives, such as public-key cryptosystems, to secure data transmission over these channels. The unique algebraic structure of these lattices enables the construction of multilevel codes, which significantly enhance the spectral efficiency of communication systems. For example, using the dense packing properties of Gaussian and Eisenstein lattices, we

© 2024 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

can create error-correcting codes that are highly effective in mitigating noise and ensuring reliable data transmission. This is particularly beneficial in scenarios where maintaining data integrity is critical, such as wireless communication, satellite communication, and data storage systems. Moreover, the algebraic properties of these lattices facilitate the development of cryptographic schemes that are both secure and efficient. Public-key cryptosystems based on algebraic lattices offer strong security guarantees and can be used to protect sensitive information from eavesdroppers and cyber attacks. Importantly, these lattice-based cryptographic systems are considered to be resistant to quantum attacks, making them suitable for post-quantum security applications. This ensures that data remains secure even in the advent of quantum computing, which poses a significant threat to traditional cryptographic methods.

Despite extensive research, signal constellations utilizing algebraic lattices, aside from Gaussian integers and Eisenstein integers used in phase-shift keying modulation, have seen limited practical adoption, largely due to their typical outcome of signal points not being a power of two [5]. However, recent developments have proposed non-binary hexagonal modulation schemes for various uses, such as multicarrier modulation [6], multilevel coded modulation [7], and wireless video transmission [8].

As one specific instance of applying algebraic lattices, in [4], Construction A of lattices is extended to algebraic integers in general imaginary quadratic fields, which may not form a PID. This extension aims to create effective lattices for coding according to Poltyrev's criteria and for optimizing MSE quantization. The authors apply these lattices to the compute-and-forward paradigm with limited feedback, introducing an adaptive scheme that selects the optimal ring of imaginary quadratic integers based on channel state feedback. Simulation results show that this adaptive approach outperforms traditional compute-and-forward schemes based solely on Gaussian or Eisenstein integers. The proposed signal constellations in [4] also find application in generalized spatial modulation, a technique that improves spectral efficiency by selectively activating antennas for each transmitted symbol. Considering these applications and potentials, our work paves the way for the application of algebraic lattices in new domains, enabling researchers with a background in linear codes to develop algebraic lattice versions that are particularly well-suited for channel coding and quantization. By integrating algebraic lattices into communication systems, our approach demonstrates the potential for significant improvements in reliability, efficiency, and security. These advancements not only enhance existing paradigms but also open up new avenues for exploration in the design of robust communication protocols.

Seminal works like [9], [10] established the feasibility of creating nested lattices over $\mathbb{Z}$ using Construction A, exhibiting their usefulness in both coding and quantization problems. For example, [10] presented a simplified demonstration of the existence of nested integer lattices useful for coding and quantization. Extending the foundational proof in [4], [9] demonstrated the effectiveness of these lattices in coding and quantization, applying a groundbreaking technique for the compute-and-forward method across AWGN channels, therefore enabling greater computation rates. The covering radius r_{cov} of a lattice is a critical factor in this context, defined as the minimum radius r at which closed spheres of radius r centered at all lattice points wrap the entire space. This assures that each point within $span(\Lambda)$ stays within a distance of r_{cov} from the lattice. In [11], a Gaussian broadcast channel with a single transmitter and many receivers was analyzed using the methodology of [12]. Using Construction A over integers, they assumed a covering radius of $r_{cov(\Lambda_c)} = \sqrt{n}$ for the coarse lattice and established the quality of their random ensemble of lattices for covering. Previous studies have explored the efficiency of Construction A when applied to Gaussian integers and Eisenstein integers, utilizing PID properties in the construction of lattices over these rings [13], [14]. In [13], it was demonstrated that there is an infinite-dimensional sequence of nested lattices over Eisenstein integers, with the coarse lattice proving good for quantization and AWGN channel coding, and the fine lattice specifically for AWGN channel coding. Building on this, it was demonstrated that nested lattice codebooks over Eisenstein integers can reach greater information rates than those over integers. In [14], lattice network codes were created from Eisenstein integers, introducing quantization and error-correcting capacity, with a focus on decoding error probability. Campello et al. proposed the concept of generic random lattices derived from linear codes and demonstrated its packing quality [15]. In addition, using the compute-and-forward approach over block fading channels, it was demonstrated that algebraic lattices generated from linear codes over finite fields showed goodness in quantization [16]. While the aforementioned references predominantly employed continuous dither, [17] took a different approach. They considered $\mathbb{Z}$-lattices over AWGN channels and simplified previous proofs regarding their goodness in coding with high probability through the application of a uniformly distributed discrete random dither.

While previous studies, like [17], have shown that nested lattice codes using Construction A achieve the capacity of an AWGN channel without erasures, in [18], an AWGN channel with erasures, which operates as an AWGN channel with probability $1 - \epsilon$ and produces an erased output with probability ϵ, was examined. This study demonstrates that by employing a simplified decoder that discards erasures, the same codes presented in [17] can also achieve the capacity of an AWGN channel with erasures.

In the realm of Wyner-Ziv problems, Nested Lattice Coding (NLC) has emerged as a robust solution, offering a comprehensive framework for efficient compression. At the heart of NLC lies the label-set, a crucial codebook that plays a pivotal role in determining the scheme's performance. Recently, a significant enhancement to traditional NLC has been proposed, leveraging *algebraic* *label-set* and *geometric label-set*, which satisfy the coset property and geometric binning, respectively. This innovative approach, termed Nested Lattice Coding with Algebraic Encoding and Geometric Decoding (NLC-AC-GD), builds upon the strengths of conventional NLC, maintaining equivalent decoding reliability while achieving improved compression rates, thereby pushing the boundaries of efficient data compression [19]. Recently, algebraic lattices from complex bases and imaginary quadratic integer rings have been explored, yielding efficient reduction algorithms. Notably, the algebraic Gauss's algorithm and extended Lenstra-Lenstra-Lovász (LLL) reduction have been shown to effectively reduce lattice bases, with the latter demonstrating numerical efficiency in wireless communications and cryptography [20].

The study in [21] explores low-dimensional quantizers within the framework of complex lattices. It introduces checkerboard lattices $\mathcal{E}_m$ and $\mathcal{G}_m$, constructed using Eisenstein and Gaussian integers, respectively. These lattice constructions are intricately linked to associated cosets, which has led to the discovery of $\mathcal{E}_{m,2}^{+}$ lattices. The research also proposes fast quantization algorithms tailored for generalized checkerboard lattices, enabling efficient evaluation of normalized second moments using Monte Carlo integration techniques. In [22], a novel approach was presented to transform infinite lattice constellations, originally optimized for the unconstrained Gaussian channel, into a sequence of codes that achieve capacity in the power-constrained Gaussian channel. This transformation leverages lattice decoding and non-uniform signaling. Importantly, this method stands out from previous approaches by imposing no additional constraints on the lattices, such as quantization goodness or a vanishing flatness factor. This makes it a more general and versatile solution.

In communication systems, especially when transmitting over an AWGN channel, discrete dithers offer distinct advantages over continuous dithers. One primary benefit is their ease of implementation, as discrete dithers require less computational power and are more efficient to generate and apply in digital signal processing. This efficiency is particularly advantageous in scenarios where computational resources and power consumption are critical. Additionally, discrete dithers seamlessly integrate into existing digital frameworks, simplifying system design and maintenance. Their limited set of noise values can be precisely controlled to minimize quantization errors without significant computational overhead. Moreover, discrete dithers facilitate more efficient quantization and encoding, enhancing bandwidth efficiency and reducing complexity in transmitter and receiver design. They also exhibit greater resilience to channel noise and errors, promoting a more uniform distribution of lattice points that simplifies error detection and correction. In contrast, continuous dithers can lead to uneven lattice point distributions, which increases the risk of error propagation and reduces overall system performance.

The goal of this study is to present a more clear argument for the existence of an ensemble of lattices formed by Construction A using the imaginary quadratic ring of integers. Under certain conditions, these lattices can do both coding and quantization over the AWGN channel. Our study stands out from previous research, particularly [17]. In the conference version [17], we have successfully demonstrated a straightforward proof that nested lattice codes generated through Construction A over integers achieve the capacity of the AWGN channel. In this work, we further extend the construction and proof in [17] to a wider variety of imaginary quadratic rings of integers, rather than just integer lattices. We demonstrate the usefulness of these lattices for coding and quantization using a simplified discrete dither technique.

The key contributions of this paper are highlighted as follows:

- While the majority of existing literature employs continuous dithers, we introduce a novel approach by modifying the random ensemble of nested lattice codes to use discrete random dithers instead. It is important to note that an independent study explores lattice codes via Construction A over the imaginary quadratic ring of integers for the Compute-and-Forward scheme [4]. Our approach differs significantly in the generation of random dithers, leading to a simpler and more transparent proof. Specifically, we assume the dither is a random vector uniformly distributed over $\gamma\mathbb{Z}^n[\xi]$, whereas [4] uses a random dither uniformly distributed over the Voronoi region of the coding lattice $\mathcal{V}_{\Lambda_c}$. This difference in the distribution of the dither is a key aspect of our methodology.
- In contrast to our previous work focused on integer lattices [17], our current study extends this research by exploring lattices over general imaginary quadratic rings of integers. This expansion not only validates these lattices as effective coding tools but also establishes their utility in minimizing MSE under specific conditions. Algebraic lattices over imaginary quadratic integers, such as those within $\mathbb{Q}(\sqrt{-d})$ where $d > 0$, offer superior packing density compared to their integer counterparts. This denser packing enables more efficient utilization of signal space, leading to higher data rates and improved communication system performance. For example, lattices like the hexagonal lattice in $\mathbb{Q}(\sqrt{-3})$ exhibit denser packing than typical integer lattices such as the square lattice. Moreover, the geometric properties inherent in algebraic lattices contribute to enhanced error-correcting capabilities. These lattices facilitate more effective nearest-neighbor decoding, crucial for minimizing bit error rates (BER) in noisy channels.

The rest of this paper is organized as follows. In Section II, we provide some background on lattices and algebraic number theory. Section III is about Construction A integer lattices and transmission over AWGN channels. The error probability of coding scheme is calculated in Section IV.

Section V is allocated to the construction of lattices over imaginary quadratic integers and we discuss how these lattices can be used for transmission over AWGN channels to achieve the capacity of the channel. In Section VI, we show the constraints that must be met to achieve a substantially low probability of error and the necessity for the second moment of the coarse lattice to be small. Finally, we find the parameters for which the scheme is good for coding and quantization in Section VII. Section VIII contains the concluding remarks.

II. PRELIMINARIES

This section is dedicated to reviewing the fundamentals of this work, including lattices, nested lattice codes, and algebraic number theory.

A. LATTICES

An n dimensional lattice Λ is a discrete subgroup of the Euclidean space $\mathbb{R}^n$ with vector addition operation. This implies that for any two lattice points $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \Lambda$, both $\boldsymbol{\lambda}_1+\boldsymbol{\lambda}_2$ and $\boldsymbol{\lambda}_1-\boldsymbol{\lambda}_2$ are also in Λ. A lattice Λ can be specified in terms of a generator matrix $\mathbf{G}$ as $\Lambda = \{\mathbf{aG} : \mathbf{a} \in \mathbb{Z}^n\}$, where the rows of $\mathbf{G}$ form the lattice basis elements. A necessary condition for the generator matrix $\mathbf{G}$ to produce a lattice is that it possesses full rank over $\mathbb{R}$, as having full rank over $\mathbb{Z}$ is not sufficient. It is also evident that a rank-deficient $\mathbf{G}$ fails to define a lattice structure. In other words, the set of points generated by $\mathbf{G}$ only forms a lattice if and only if the matrix has full row rank over $\mathbb{R}$, emphasizing the importance of this requirement in lattice construction. We also account for this requirement and its probability in our analysis of the error probability for our coding scheme.

Example 1: Consider the $\mathbb{Z}$-module generated by the matrix $\mathbf{G} = \begin{bmatrix} 1 \\ \sqrt{2} \end{bmatrix}$ in $\mathbb{R}$, which generates the set $\mathcal{S} = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. We demonstrate that the set $\mathcal{S}$ is not a lattice. Although the rows of $\mathbf{G}$ are linearly independent over $\mathbb{Z}$, they are dependent over $\mathbb{R}$. Specifically, we prove that $\mathcal{S}$ is dense in $\mathbb{R}$ and thus not discrete. To establish the density of $\mathcal{S}$ in $\mathbb{R}$, we need to show that for any real number x and any $\epsilon > 0$, there exists $s \in \mathcal{S}$ such that $|x - s| < \epsilon$. It can be observed that this corresponds to the special case of Kronecker's theorem with $m = 1$ and $n = 1$, which is a significant result in diophantine approximations and extends Dirichlet's approximation theorem to multiple variables [23].

Theorem 1 [23]: Given real n-tuples $\boldsymbol{\alpha}_i = (\alpha_{i1}, \dots, \alpha_{in}) \in \mathbb{R}^n$, $i = 1, \dots, m$ and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n) \in \mathbb{R}^n$, the condition:

$$\forall\epsilon > 0 \ \exists\ q_i, p_j \in \mathbb{Z} : \left|\sum_{i=1}^{m} q_i\alpha_{ij} - p_j - \beta_j\right| < \epsilon, \ \ 1 \le j \le n,$$

holds if and only if for any $r_1, \dots, r_n \in \mathbb{Z}$ with $\sum_{j=1}^{n} \alpha_{ij} r_j \in \mathbb{Z}$, $i = 1, \dots, m$, the number $\sum_{j=1}^{n} \beta_j r_j$ is also an integer.

For the specific case when $m = 1$ and $n = 1$, Kronecker's theorem implies that for any $\alpha, \beta, \epsilon \in \mathbb{R}$ with α irrational and $\epsilon > 0$, there exist integers p and q, with $q > 0$, such that $|p + q\alpha - \beta| < \epsilon$.

The volume of the lattice Λ is defined as $\mathrm{V}(\Lambda) = |\det(\mathbf{G})|$. The Construction A lifting of a linear (n, k)-code C over $\mathbb{F}_p^n$ is the lattice

$$\Lambda_C = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \pmod{p} \text{ is a codeword in } C\};$$

such a lattice is called a modulo-p lattice. For any $\mathbf{x} \in \mathbb{R}^n$, the set $\mathbf{x} + \Lambda = \{\mathbf{x} + \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \Lambda\}$ is a lattice shift of Λ in $\mathbb{R}^n$. A nearest neighbor quantizer $Q_\Lambda : \mathbb{R}^n \to \Lambda$ associated with the lattice Λ maps a vector in $\mathbb{R}^n$ to its closest lattice point,

$$Q_\Lambda(\mathbf{x}) = \boldsymbol{\lambda} \in \Lambda, \text{ if } \|\mathbf{x} - \boldsymbol{\lambda}\| \le \|\mathbf{x} - \boldsymbol{\lambda}'\|, \ \forall \boldsymbol{\lambda}' \in \Lambda. \quad (1)$$

For each lattice point $\boldsymbol{\lambda}$, the Voronoi region $\mathcal{V}_\Lambda(\boldsymbol{\lambda})$ is the set of all $\mathbf{x}$'s in $\mathbb{R}^n$ such that $Q_\Lambda(\mathbf{x}) = \boldsymbol{\lambda}$. The modulo-$\Lambda$ operation with respect to Λ is defined as

$$\mathbf{x} \pmod{\Lambda} = \mathbf{x} - Q_\Lambda(\mathbf{x}), \quad (2)$$

which is also the quantization error of $\mathbf{x}$. The module-Λ operation has also a geometrical interpretation as follows:

$$\mathbf{x} \pmod{\Lambda} = (\mathbf{x} + \Lambda) \cap \mathcal{V}_\Lambda(\mathbf{0}).$$

Let $B(r)$ be an n-dimensional ball with center $\mathbf{0}$ and radius r. The set $\Lambda + B(r)$ composed of spheres centered around the lattice points, is a covering of Euclidean space if

$$\mathbb{R}^n \subset \Lambda + B(r).$$

Each point in space is covered by at least one sphere. Therefore, the covering radius is the minimum radius of balls that cover the entire space. Define the covering radius of the lattice $r_{cov}(\Lambda)$ by

$$r_{cov}(\Lambda) = \min\{r : \Lambda + B(r) \text{ covers } \mathbb{R}^n\}.$$

The radius of a sphere which has the same volume as the lattice cells is called the effective radius that is, $r_{\text{eff}}(\Lambda) = \left[\frac{\mathrm{V}(\Lambda)}{\mathrm{V}_n}\right]^{\frac{1}{n}}$ where V_n is the volume of a sphere of radius 1. The second moment of a lattice is also defined as

$$\sigma^2(\Lambda) = \frac{1}{n}\frac{1}{\mathrm{V}(\mathcal{V}_\Lambda)}\int_{\mathcal{V}_\Lambda} ||\mathbf{x}||^2 \, d\mathbf{x}, \quad (3)$$

and the normalized second moment of the lattice Λ is

$$G(\Lambda) = \frac{\sigma^2(\Lambda)}{\mathrm{V}(\mathcal{V}_\Lambda)^{\frac{2}{n}}}.$$

Therefore, a sequence of lattices is good for MSE quantization if $\lim_{n\to\infty} G(\Lambda) = \frac{1}{2\pi e}$.

Consider an AWGN channel in which the noise components are $Z_i \sim \mathcal{N}(0, \eta^2)$, then, Poltyrev goodness is defined as follows. A sequence of lattices is Poltyrev-good when, for $\eta^2 < \frac{\mathrm{V}(\mathcal{V}_\Lambda)^{\frac{2}{n}}}{2\pi e}$, the decoding error probability of transmitted signal $\mathbf{x}$ from the received signal $\mathbf{y}$ can be decreased to an arbitrary low value.

A sublattice Λ_c of Λ_f is a subset of Λ_f which itself is a lattice. Thus, a pair of lattices (Λ_c, Λ_f) is a nested lattice if Λ_c is a sublattice of Λ_f, that is, $\Lambda_c \subset \Lambda_f$. In this case, Λ_c and Λ_f are called the coarse and the fine lattices, respectively. For each $\boldsymbol{\lambda} \in \Lambda_f$, the lattice shift $\boldsymbol{\lambda} + \Lambda_c$ is a coset of Λ_c in Λ_f and the point $\boldsymbol{\lambda} \pmod{\Lambda_c}$ is called the coset leader or representitive of $\boldsymbol{\lambda} + \Lambda_c$. Two cosets $\boldsymbol{\lambda}_1 + \Lambda_c$ and $\boldsymbol{\lambda}_2 + \Lambda_c$ are either identical that is $(\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2) \in \Lambda_c$ or disjoint $(\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2) \notin \Lambda_c$. The set of all disjoint cosets of Λ_c in Λ_f, denoted by Λ_f/Λ_c, forms a partition of Λ_f. A nested lattice code $\mathcal{L}(\Lambda_c, \Lambda_f)$ is defined as the set of points of fine lattice Λ_f in the fundamental region of Λ_c, that is,

$$\mathcal{L}\big(\Lambda_c, \Lambda_f\big) = \Lambda_f \pmod{\Lambda_c} = \{\boldsymbol{\lambda} \pmod{\Lambda_c} : \boldsymbol{\lambda} \in \Lambda_f\}.$$

Thus, if $\dim(\Lambda_f) = \dim(\Lambda_c)$, the number of codewords in $\mathcal{L}(\Lambda_c, \Lambda_f)$ is equal to $\dfrac{\mathrm{V}(\Lambda_c)}{\mathrm{V}(\Lambda_f)}$.

Throughout this paper, Q_{Λ_f} denotes the quantizer function applied to the fine lattice Λ_f, and $\pmod{\Lambda_c}$ denotes the modulo operation relative to the coarse lattice Λ_c.

B. ALGEBRAIC NUMBERS AND ALGEBRAIC INTEGERS

Let $\mathbb{K}$ be a subfield of $\mathbb{C}$ such that $[\mathbb{K} : \mathbb{Q}]$ is finite, then $\mathbb{K}$ is called a number field. For a number field $\mathbb{K}$, the ordered pair (s, t) where s is the number of real embeddings of $\mathbb{K}$ and t is the number of complex conjugate pairs of embeddings, is called the signature of $\mathbb{K}$. The degree of $\mathbb{K}$ is defined as $n = s + 2t$. Let $\mathcal{B}$ is the set of all algebraic integers which is a subring of $\mathbb{C}$, then $\mathcal{O}_{\mathbb{K}} = \mathbb{K} \cap \mathcal{B}$ is called the ring of integers of $\mathbb{K}$. If $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$, we can define n distinct embedding $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta)$ where $\sigma_i(\theta) = \theta_i$ for $i = 1, 2, \ldots, n$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ form a basis for $\mathbb{Q}(\theta)$ over $\mathbb{Q}$. Then, the discrimiment of $\mathbb{Q}(\theta)$ is $\Delta = \det[\sigma_i(\alpha_j)]^2$ where $i, j = 1, 2, \ldots, n$.

Definition 1 (Quadratic Fields): A quadratic field is a number field $\mathbb{K}$ of degree 2 over $\mathbb{Q}$, that is, $[\mathbb{K} : \mathbb{Q}] = 2$. We can write $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ where d is a square free element in $\mathbb{Z}$. $\mathbb{K}$ is an imaginary quadratic field if $d < 0$.

Generally, for the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, its ring of integer $\mathcal{O}_K$ is defined as $\mathbb{Z}[\xi]$, where ξ is as follows:

$$\xi = \begin{cases} \sqrt{d}, & d \equiv 2, 3 \pmod 4, \\ \dfrac{1 + \sqrt{d}}{2}, & d \equiv 1 \pmod 4). \end{cases}$$

Therefore, $\Delta = 4d$ if $d \equiv 2, 3 \pmod 4$ and $\Delta = d$ if $d \equiv 1 \pmod 4$. When $d = -1$, we have Gaussian integers and when $d = -3$, we have Eisenstein integers. Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$. We say $\mathcal{P}$ lies above p if $\mathcal{P}|p\mathbb{Z}$. The ideal $p\mathcal{O}_{\mathbb{K}}$ can be uniquely factorized as $p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{m} \mathcal{P}_i^{e_l}$ where $\mathcal{P}_i$'s are distinct prime ideals of $\mathcal{O}_{\mathbb{K}}$. We call e_l the *ramification index* of $\mathcal{P}_l$ over p and $f_l = \left[\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_l} : \dfrac{\mathbb{Z}}{p\mathbb{Z}}\right]$ the inertia degree of $\mathcal{P}_l$ over p. Finally, since every prime ideal $\mathcal{P}$ of $\mathcal{O}_{\mathbb{K}}$ is maximal with norm $N(\mathcal{P}) = p^f$, where $f \in \{1, 2\}$ is the inertia degree, we have $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}} \cong \mathbb{F}_{p^f}$.

In the following, we have useful lemmas showing the number of lattice points which is in a ball of radius r.

Lemma 1 [10]: For any point $\mathbf{s} \in \mathbb{R}^n$, the number of points of $\mathbb{Z}^n$ inside $B(\mathbf{s}, r)$ can be bounded as

$$\Big(\max\{r - \frac{\sqrt{n}}{2}, 0\}\Big)^n V_n \le |\mathbb{Z}^n \cap B(\mathbf{s}, r)| \le \Big(r + \frac{\sqrt{n}}{2}\Big)^n V_n. \tag{4}$$

To determine the number of elements of $\mathcal{O}_{\mathbb{K}}$ that lies within a ball with radius r the following lemma is useful.

Lemma 2 [4]: For any point $\mathbf{s} \in \mathbb{R}^{2n}$ and $r > 0$, the number of points of $\mathcal{O}_K^n$ inside $2n$ dimensional ball $B(\mathbf{s}, r)$ can be bounded as

$$(\max\{r - \rho, 0\})^{2n} \le \frac{|\mathcal{O}_{\mathbb{K}}^n \cap B(\mathbf{s}, r)|}{\mu} \le (r + \rho)^{2n}, \tag{5}$$

where $\mu = \dfrac{V_{2n}}{(\frac{\sqrt{|\Delta|}}{2})^n}$ and $\rho = \dfrac{\sqrt{2n|\Delta|}}{2}$.

Lemma 3 [24]: There always exists a natural prime congruent to $1 \pmod 3$ between integers m and $2m$ where $m > 4$.

III. CODING SCHEME FOR NESTED LATTICES OVER INTEGERS

According to the construction of nested lattices, in this section, we define encoding and decoding for our coding scheme and prove that total error probability of the proposed scheme is very small under some constraints.

A. CONSTRUCTION A NESTED LATTICES OVER INTEGERS

Consider $C_2 \subset C_1$ as two nested linear codes generated by matrices $\mathbf{G}_1 \in \mathbb{F}_p^{k_1 \times n}$ and $\mathbf{G}_2 \in \mathbb{F}_p^{k_2 \times n}$, respectively. Let

$$\mathbf{G}_1 = \begin{bmatrix} \mathbf{G}_2 \\ \mathbf{G}' \end{bmatrix},$$

where $\mathbf{G}'$ is a matrix of size $(k_1 - k_2) \times n$. Therefore, the matrix $\mathbf{G}_2$ is full rank if $\mathbf{G}_1$ is.

By applying Construction A to these nested codes, we have the following nested lattices

$$\Lambda_2 = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \pmod p \in C_2\},$$
$$\Lambda_1 = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \pmod p \in C_1\},$$

with $\Lambda_2 \subset \Lambda_1 \subset \mathbb{Z}^n$. Let γ be a scaling factor, hence, we have the following coarse and fine lattices

$$\Lambda_c = \gamma\Lambda_2,$$
$$\Lambda_f = \gamma\Lambda_1,$$

where $\gamma p\mathbb{Z}^n \subset \Lambda_c \subset \Lambda_f \subset \gamma\mathbb{Z}^n$. In this case, the volumes of the voronoi region of the coarse and fine lattices are $V(\Lambda_c) = \gamma^n p^{n-k_2}$ and $V(\Lambda_f) = \gamma^n p^{n-k_1}$, respectively. Let $\varphi : \gamma\mathbb{Z}^n \to \mathbb{F}_p^n$ be a map from points in $\gamma\mathbb{Z}^n$ to vectors in $\mathbb{F}_p^n$ given by

$$\varphi(\mathbf{x}) = \frac{1}{\gamma}\mathbf{x} \bmod p.$$

Clearly, φ is a surjective homomorphism, i.e.,

$$\forall \mathbf{x}, \mathbf{y} \in \gamma\mathbb{Z}^n,\ \varphi(\mathbf{x}+\mathbf{y}) = \varphi(\mathbf{x}) + \varphi(\mathbf{x}),$$

hence, let us assume $\tilde{\varphi}$ is an inverse of φ that maps a vector $\mathbf{c}$ in $\mathbb{F}_p^n$ to a point $\mathbf{x}$ in $\gamma\mathbb{Z}^n$ with the shortest Euclidean norm such that $\varphi(\mathbf{x}) = \mathbf{c}$.

Now, according to the construction of nested lattices, we define encoding and decoding for our coding scheme and prove that total error probability of the proposed scheme is very small under some constraints.

B. ENCODING FOR NESTED LATTICES OVER INTEGERS

Let $\mathbf{G}_1 \in \mathbb{F}_p^{k_1 \times n}$ be a random matrix whose entries are independent and identically distributed (i.i.d) with uniform distribution over $\mathbb{F}_p$. Unlike prior approaches utilizing continuous dithers, our proposed scheme harnesses the benefits of discrete dithers, capitalizing on their simplicity of implementation, ease of design and maintenance, and encoding efficiency. Embracing discrete dithers leads to reduced complexity in both transmitter and receiver designs, thereby enhancing overall system performance. Discrete dithers also enable the parallelism and help simplify the proof so that rudimentary probability arguments suffice. This intentional design choice allows us to overcome the constraints associated with continuous dithers, resulting in superior outcomes. Let $\mathbf{U} \in \mathbb{F}_p^n$ be a vector which is drawn independently and uniformly over $\mathbb{F}_p^n$, then we use $\tilde{\varphi}(\mathbf{U}) \in \gamma\mathbb{Z}^n$ as our random dither. Our codebook consists of $p^{k_1-k_2}$ shifted cosets of the form

$$\left\{\tilde{\varphi}\left(\mathbf{m}\mathbf{G}'\right) + \tilde{\varphi}(\mathbf{U}) + \boldsymbol{\Lambda}_c \,:\, \mathbf{m} \in \mathbb{F}_p^{k_1-k_2}\right\}.$$

To send a message vector $\mathbf{m} \in \mathbb{F}_p^{k_1-k_2}$, the encoder first finds an "information-carrying" shifted coset $\tilde{\varphi}(\mathbf{m}\mathbf{G}')+\tilde{\varphi}(\mathbf{U})+\boldsymbol{\Lambda}_c$. The encoder then transmits a shortest vector $\mathbf{X} \in \mathbb{R}^n$ in the shifted coset, i.e.,

$$\mathbf{X} = \tilde{\varphi}\left(\mathbf{m}\mathbf{G}'\right) + \tilde{\varphi}(\mathbf{U}) \pmod{\Lambda_c}.$$

C. DECODING FOR NESTED LATTICES OVER INTEGERS

Upon receiving $\mathbf{Y} = \mathbf{X}+\mathbf{Z}$, the decoder searches for a unique vector $\hat{\mathbf{m}} \in \mathbb{F}_p^{k_1-k_2}$ such that the corresponding shifted coset $\tilde{\varphi}(\widehat{\mathbf{m}G'}) + \tilde{\varphi}(\mathbf{U}) + \Lambda_c$ and $\alpha\mathbf{Y}$ for the scaling factor $\alpha > 0$ has the minimum distance, i.e.,

$$\hat{\mathbf{m}} = \arg\min_{\mathbf{m}} d\left(\tilde{\varphi}(\mathbf{m}\mathbf{G}') + \tilde{\varphi}(\mathbf{U}) + \Lambda_c, \alpha\mathbf{Y}\right).$$

The decoder proceeds the decoding in a few steps. First, the decoder scales the received signal $\mathbf{Y}$ by α to obtain

$$\alpha\mathbf{Y} = \mathbf{X} + \mathbf{W}, \tag{6}$$

where $\mathbf{W} = (\alpha - 1)\mathbf{X} + \alpha\mathbf{Z}$ is called the effective noise. After subtracting $\tilde{\varphi}(\mathbf{U})$ from the scaled version of received signal and applying the module-Λ_c operation, the decoder quantizes the vector with the fine lattice to obtain

$$\begin{aligned}\tilde{\varphi}\left(\widehat{\mathbf{m}G'}\right) &= Q_{\Lambda_f}(\alpha\mathbf{Y} - \tilde{\varphi}(\mathbf{U})) \pmod{\Lambda_c} \\ &= Q_{\Lambda_f}\left(\mathbf{X} - \tilde{\varphi}(\mathbf{U})\right) \pmod{\Lambda_c} \\ &\quad + Q_{\Lambda_f}(\mathbf{W}) \pmod{\Lambda_c} \\ &= \tilde{\varphi}\left(\mathbf{m}\mathbf{G}'\right) + Q_{\Lambda_f}(\mathbf{W}) \pmod{\Lambda_c},\end{aligned} \tag{7}$$

where Q_{Λ_f} denotes the quantizer function on Λ_f as defined in (1), and $\pmod{\Lambda_c}$ represents the modulo operation on Λ_c per Definition 2.

The last step is to apply the labeling φ, hence,

$$\widehat{\mathbf{m}G'} = \mathbf{m}\mathbf{G}' + \varphi\left(Q_{\Lambda_f}(\mathbf{W}) \pmod{\Lambda_c}\right). \tag{8}$$

The decoding is successful if and only if $\varphi(Q_{\Lambda_f}(\mathbf{W}) \pmod{\Lambda_c}) = 0$, or equivalently, if and only if $Q_{\Lambda_f}(\mathbf{W}) \in \Lambda_c$.

IV. ANALYSIS OF ERROR PROBABILITIES FOR NESTED LATTICES OVER INTEGERS

The connection between the total error probability in our coding scheme and the rank of the generator matrix, as well as the error probabilities in both encoding and decoding, is readily evident. This correlation arises because the total error probability is defined as the union of the probabilities associated with not having independent lattice codes, as well as the probabilities of encoding and decoding errors. Consequently, to establish the effectiveness of the coding scheme, we establish an upper bound based on the generator matrix, as well as the error probabilities associated with encoding and decoding. This upper bound is shown to markedly decrease as the value of n grows towards infinity.

A. THE GENERATOR MATRIX $\mathbf{G}_1$ IS FULL RANK WITH HIGH PROBABILITY

A critical requirement for the generator matrix $\mathbf{G}_1$ is that it must have full rank over $\mathbb{R}$; otherwise, it cannot generate a lattice. When the components of $\mathbf{G}_1$ are integers, independency in $\mathbb{R}$ is equivalent to independency in $\mathbb{Z}$. Further, since we select the components of $\mathbf{G}_1$ from $\mathbb{F}_p$, independency in $\mathbb{F}_p$ is sufficient [25, Lemma 3]. It is clear that $\mathbf{G}_1$ is not full rank if and only if at least two rows are dependent. Thus, if we define $\mathcal{E}_1 = \{G_1 \in \mathbb{F}_p^{k_1\times n}$ s.t rank$(G_1) < k_1\}$, the probability of $\mathcal{E}_1$ is given by

$$\Pr(\mathcal{E}_1) = 1 - \prod_{i=0}^{k_1-1}\left(1 - \frac{p^i}{p^n}\right) \le \left(p^{k_1} - 1\right)p^{-n} < \frac{1}{p^{n-k_1}}. \tag{9}$$

Certainly, this probability approaches zero as long as k_1 is less than n.

B. THE ENCODING ERROR PROBABILITY FOR NESTED LATTICES OVER INTEGERS

The encoding is successful if and only if $\mathbf{X} \in B(\sqrt{nP})$ where P is the signal power. Additionally, we know, $\mathbf{X} \in \tilde{\varphi}(\mathbf{m}\mathbf{G}') + \tilde{\varphi}(\mathbf{U}) + \boldsymbol{\Lambda}_c$. Hence, the encoding succeeds if and only if $\tilde{\varphi}(\mathbf{m}\mathbf{G}') + \tilde{\varphi}(\mathbf{U}) + \boldsymbol{\Lambda}_c \cap B(\sqrt{nP}) \neq \emptyset$ and fails if and only if $\tilde{\varphi}(m\mathbf{G}') + \tilde{\varphi}(\mathbf{U}) + \boldsymbol{\Lambda}_c \cap B(\sqrt{nP}) = \emptyset$. Let

$$\mathcal{E}_2(\mathbf{m}) = \left\{\mathbf{m} \,:\, \tilde{\varphi}\left(\mathbf{m}\mathbf{G}'\right) + \tilde{\varphi}(\mathbf{U}) + \boldsymbol{\Lambda}_c \cap B\left(\sqrt{nP}\right) = \emptyset\right\}.$$

Clearly, because the set $\{\tilde{\varphi}(\mathbf{m}\mathbf{G}'+\mathbf{u}+\mathbf{l}\mathbf{G}_2):\mathbf{l}\in\mathbb{F}_p^{k_2}\}$ contains all the points of $\tilde{\varphi}(\mathbf{m}\mathbf{G}')+\tilde{\varphi}(\mathbf{U})+\mathbf{\Lambda}_c$ inside $[\frac{-\gamma p}{2},\frac{\gamma p}{2}]^n$, $\mathcal{E}_2$ is equivalent to

$$\sum_{\mathbf{l}\in\mathbb{F}_p^{k_2}}\mathbb{I}\Big(\tilde{\varphi}\big(\mathbf{m}\mathbf{G}'+\mathbf{u}+\mathbf{l}\mathbf{G}_2\big)\in B\Big(\sqrt{nP}\Big)\Big)=0,$$

where $\mathbb{I}$ is the characteristic function.

Let us denote $\tilde{\varphi}(\mathbf{m}\mathbf{G}'+\mathbf{u}+\mathbf{l}\mathbf{G}_2)$ by $\mathbf{t}_\mathbf{l}$, for $\mathbf{l}\in\mathbb{F}_p^{k_2}$, and define the set of points $\gamma\mathbb{Z}^n\cap[\frac{-\gamma p}{2},\frac{\gamma p}{2}]^n\cap B(\sqrt{nP})$ as $\mathbf{A}$. It is known that $\mathbf{t}_l$ is uniformly distributed over the grid $\gamma\mathbb{Z}^n\cap[\frac{-\gamma p}{2},\frac{\gamma p}{2}]^n$ which contains a total of p^n points, and $B(\sqrt{nP})\subset[\frac{-\gamma p}{2},\frac{\gamma p}{2}]^n$. According to the properties of the characteristic function and uniform distribution, we have

$$\begin{aligned}
&\mathrm{E}\Big(\mathbb{I}(\mathbf{t}_\mathbf{l})\in B\Big(\sqrt{nP}\Big)\Big)=\frac{|\mathbf{A}|}{\left|\gamma\mathbb{Z}^n\cap\left[\frac{-\gamma p}{2},\frac{\gamma p}{2}\right]^n\right|}\\
&=\frac{|\gamma\mathbb{Z}^n\cap B\Big(\sqrt{nP}\Big)|}{p^n},\\
&\mathrm{Var}\Big(\mathbb{I}(\mathbf{t}_\mathbf{l})\in B\Big(\sqrt{nP}\Big)\Big)\\
&=\frac{|\mathbf{A}|}{\left|\gamma\mathbb{Z}^n\cap\left[\frac{-\gamma p}{2},\frac{\gamma p}{2}\right]^n\right|}\left(1-\frac{|\mathbf{A}|}{\left|\gamma\mathbb{Z}^n\cap\left[\frac{-\gamma p}{2},\frac{\gamma p}{2}\right]^n\right|}\right)\\
&=\frac{\left|\gamma\mathbb{Z}^n\cap B\Big(\sqrt{nP}\Big)\right|}{p^n}\left(1-\frac{|\gamma\mathbb{Z}^n\cap B\Big(\sqrt{nP}\Big)|}{p^n}\right).
\end{aligned}$$

Hence,

$$\begin{aligned}
\Pr(\mathcal{E}_2)&=\Pr\left(\sum_{\mathbf{l}\in\mathbb{F}_p^{k_2}}\mathbb{I}\Big(\mathbf{t}_\mathbf{l}\in B\Big(\sqrt{nP}\Big)\Big)=0\right)\\
&\le\frac{\mathrm{Var}\Big(\sum_{\mathbf{l}\in\mathbb{F}_p^{k_2}}\mathbb{I}\Big(\mathbf{t}_\mathbf{l}\in B\Big(\sqrt{nP}\Big)\Big)=0\Big)}{\Big(\mathrm{E}\Big(\sum_{\mathbf{l}\in\mathbb{F}_p^{k_2}}\mathbb{I}\Big(\mathbf{t}_\mathbf{l}\in B\Big(\sqrt{nP}\Big)\Big)=0\Big)\Big)^2}\\
&\le\frac{p^{n-k_2}}{|\gamma\mathbb{Z}^n\cap B\Big(\sqrt{nP}\Big)|}\le\frac{p^{n-k_2}}{\Big(\max\Big\{0,\frac{\sqrt{nP}}{\gamma}-\frac{\sqrt{n}}{2}\Big\}\Big)^nV_n}
\end{aligned}\tag{10}$$

where the first inequality follows from Chebyshev's inequality, the second one follows from the pairwise independency of lattice points, and the third inequality follows from Lemma 1. We need to choose the prime p, γ, and k_2 such that Equation (10) goes to zero as n approaches infinity.

As the power constraint is not consistently met, and, in fact, there is a probability $\Pr(\mathcal{E}_2)$ of the power constraint being breached, a solution to this challenge is presented by introducing a spherical shaping strategy as follows:

$$\mathbf{X}_s=\begin{cases}\mathbf{X}\ \|\mathbf{X}\|^2\le nP\\ 0\ \text{ otherwise.}\end{cases}$$

Certainly, the power constraint is met with the new coding scheme. It's worth noting that the error probability for this scheme remains bounded by $\Pr(\mathcal{E}_1)+\Pr(\mathcal{E}_2)+\Pr(\mathcal{E}_3)$. This is due to the spherical shaping, which effectively transforms an encoding failure into a decoding failure. This concludes the proof that our random ensemble attains AWGN capacity through lattice encoding and decoding.

C. THE DECODING ERROR PROBABILITY FOR NESTED LATTICES OVER INTEGERS

Having received the vector $\mathbf{Y}$, the decoding fails if there exists a message $\mathbf{m}'$ such that

$$\begin{aligned}
&d\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}')+\tilde{\varphi}(\mathbf{U})+\Lambda_c,\alpha\mathbf{Y}\big)\\
&\quad<d\big(\tilde{\varphi}(\mathbf{m}\mathbf{G}')+\tilde{\varphi}(\mathbf{U})+\Lambda_c,\alpha\mathbf{Y}\big).
\end{aligned}\tag{11}$$

Equivalently, it is shown that the decoding declares failure if and only if $Q_{\Lambda_f}(\mathbf{W})\notin\Lambda_c$. Let define $\mathcal{E}_3=\{\mathbf{W}:Q_{\Lambda_f}(\mathbf{W})\notin\Lambda_c\}$. By Total Probability Theorem, there exists the radius r_e such that

$$\Pr(\mathcal{E}_3)\le\Pr(\mathbf{W}\notin B(r_e))+\Pr\big(Q_{\Lambda_f}(\mathbf{W})\notin\Lambda_c|\mathbf{W}\in B(r_e)\big).\tag{12}$$

Since $\mathbf{X}=\tilde{\varphi}(\mathbf{m}\mathbf{G}')+\tilde{\varphi}(\mathbf{U})\pmod{\Lambda_c}$ is the shortest vector in the corresponding coset,

$$\begin{aligned}
d\big(\tilde{\varphi}(\mathbf{m}\mathbf{G}')+\tilde{\varphi}(\mathbf{U})+\Lambda_c,\alpha\mathbf{Y}\big)&\le\|\mathbf{X}-\alpha\mathbf{Y}\|\\
&=\|(\alpha-1)\mathbf{X}+\alpha\mathbf{Z}\|\\
&=\|\mathbf{W}\|.
\end{aligned}$$

For a fixed representative $\mathbf{X}=\mathbf{x}$, we have

$$\|\mathbf{W}\|^2=(\alpha-1)^2\|\mathbf{x}\|^2+\alpha^2\|\mathbf{Z}\|^2+2\alpha(\alpha-1)\|\mathbf{x}\mathbf{Z}^T\|,\tag{13}$$

where we have $\mathbf{x}\mathbf{Z}^T\sim\mathcal{N}(0,\|\mathbf{x}\|^2\eta^2)$. We know $\|\mathbf{X}\|^2\le nP$ and $\|\mathbf{Z}\|^2\le n\eta^2$ with high probability. Additionally, it can be shown that $\mathbf{X}$ and $\mathbf{Z}$ are almost orthogonal for sufficiently large n. Therefore, for any $\epsilon>0$, the norm of the effective noise $\mathbf{W}$ is upper bounded by $\|\mathbf{W}\|^2\le(1+\epsilon)\frac{nP\eta^2}{P+\eta^2}$ for $\alpha=\frac{P}{P+\eta^2}$. We define $r_e=\sqrt{(1+\epsilon)\frac{nP\eta^2}{P+\eta^2}}$.

The first step is to find an upper bound for $\Pr(\mathbf{W}\notin B(r_e))$. For any $\epsilon>0$ and $\alpha>0$, according to Equation (13), $\mathbf{W}\notin B(r_e)$ if one of the following events occurs

$$\mathcal{E}_X=\Big\{\mathbf{X}:\|\mathbf{X}\|>\sqrt{nP}\Big\},\tag{14}$$

$$\mathcal{E}_Z=\Big\{\mathbf{Z}:\|\mathbf{Z}\|>n\eta^2\Big\},\tag{15}$$

$$\mathcal{E}_O=\Big\{\mathbf{X}\mathbf{Z}^T:\|\mathbf{X}\mathbf{Z}^T\|>n^{\frac{1}{4}}\sqrt{nP\eta^2}\Big\}.\tag{16}$$

Hence, $\Pr(\mathbf{W}\notin B(r_e))\le\Pr(\mathcal{E}_X)+\Pr(\mathcal{E}_Z)+\Pr(\mathcal{E}_O)$. In the previous part, it is shown that $\Pr(\{\|\mathbf{X}\|>\sqrt{nP}\})\le\frac{p^{n-k_2}}{|\gamma\mathbb{Z}^n\cap B(\sqrt{nP})|}$. Since $\mathbf{Z}\sim\mathcal{N}(0,\eta^2\mathbf{I}_n)$, we get $\Pr(\|\mathbf{Z}\|>$

$\sqrt{n\eta^2}) \leq \frac{1}{n}$ by Chebyshev's inequality. Additionally, we have

$$\begin{aligned}
&\Pr\Big(\|\mathbf{X}\mathbf{Z}^T\| > n^{\frac{3}{4}}\sqrt{P\eta^2}\Big) \\
&\leq \Pr\Big(\|\mathbf{X}\mathbf{Z}^T\| > n^{\frac{3}{4}}\sqrt{P\eta^2}|\|\mathbf{X}\| \leq \sqrt{nP}\Big) \\
&\quad + \Pr\Big(\|\mathbf{X}\| > \sqrt{nP}\Big) \\
&\leq \frac{\mathrm{E}\Big(\|\mathbf{X}\mathbf{Z}^T\|^2|\|\mathbf{X}\| \leq \sqrt{nP}\Big)}{n^{\frac{3}{2}}P\eta^2} + \frac{p^{n-k_2}}{|\gamma\mathbb{Z}^n \cap B\Big(\sqrt{nP}\Big)|},
\end{aligned}$$

where the last inequality follows since for any given $\mathbf{X} = \mathbf{x}$ with $\|\mathbf{x}\| \leq \sqrt{nP}$ and $\mathbf{x}\mathbf{Z}^T \sim \mathcal{N}(0, \|\mathbf{x}\|^2\eta^2)$, we get $\mathrm{E}(\|\mathbf{X}\mathbf{Z}^T\|^2|\|\mathbf{X}\| \leq \sqrt{nP}) \leq nP\eta^2$. Thus, $\Pr(\mathbf{W} \notin B(r_e))$ is upper bounded by

$$\Pr(\mathbf{W} \notin B(r_e)) \leq n^{-\frac{3}{2}} + 2\frac{p^{n-k_2}}{|\gamma\mathbb{Z}^n \cap B\Big(\sqrt{nP}\Big)|}. \tag{17}$$

Now, we need to find an upper bound for $\Pr(Q_{\Lambda_f}(\mathbf{W}) \notin \Lambda_c|\mathbf{W} \in B(r_e))$. For any fixed coarse lattice Λ_c, let us define $\tilde{\varphi}(\mathbf{U}) + \Lambda_c$ by Λ, then we have

$$\begin{aligned}
&\Pr\Big(Q_{\Lambda_f}(\mathbf{W}) \notin \Lambda_c|\mathbf{W} \in B(r_e), \mathbf{G_2} = G_2\Big) \\
&\leq \Pr\Big(\exists \mathbf{m}' \neq \mathbf{m}{:}d\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') + \Lambda, \alpha\mathbf{Y}\big) \leq \|\mathbf{W}\| \\
&\qquad |\mathbf{W} \in B(r_e), \mathbf{G_2} = G_2\Big) \\
&\leq \sum_{\mathbf{m}' \neq \mathbf{m}} \Pr\Big(d\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') + \Lambda, \alpha\mathbf{Y}\big) \leq \|\mathbf{W}\| \\
&\qquad |\mathbf{W} \in B(r_e), \mathbf{G_2} = G_2\Big) \\
&\leq \sum_{\mathbf{m}' \neq \mathbf{m}} \Pr\Big(d\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') + \Lambda, \alpha\mathbf{Y}\big) \leq r_e|\mathbf{W} \in B(r_e), \\
&\qquad \mathbf{G_2} = G_2\Big) \\
&\leq \sum_{\mathbf{m}' \neq \mathbf{m}} \Pr\Big(d\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') - \tilde{\varphi}_p(\mathbf{m}\mathbf{G}') + \Lambda_c, \mathbf{W}\big) \leq r_e \\
&\qquad |\mathbf{W} \in B(r_e), \mathbf{G_2} = G_2\Big),
\end{aligned}$$

where the last step follows by

$$\begin{aligned}
&d\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') + \tilde{\varphi}(\mathbf{U}) + \Lambda_c, \alpha\mathbf{Y}\big) \\
&= d\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') + \tilde{\varphi}(\mathbf{U}) + \Lambda_c, \mathbf{X} + (\alpha - 1)\mathbf{X} + \alpha\mathbf{Z}\big) \\
&= d\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') - \tilde{\varphi}(\mathbf{m}\mathbf{G}') + \Lambda_c, \mathbf{X} + \mathbf{W}\big) \\
&= d\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') - \tilde{\varphi}(\mathbf{m}\mathbf{G}') + \Lambda_c, \mathbf{W}\big).
\end{aligned}$$

Since $\mathbf{X}$ is uniformly distributed over $\gamma\mathbb{Z}^n \cap \mathcal{V}(\Lambda_c)$ and independent of $\mathbf{m}\mathbf{G}'$, it is independent of $\tilde{\varphi}_p(\mathbf{m}\mathbf{G}')$; consequently $\mathbf{W} = (\alpha - 1)\mathbf{X} + \alpha\mathbf{Z}$ and $\tilde{\varphi}(\mathbf{m}\mathbf{G}')$ are conditionally independent. By the Total Probability Theorem, we have

$$\begin{aligned}
&\Pr\Big(\mathrm{d}\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') - \tilde{\varphi}(\mathbf{m}\mathbf{G}') + \Lambda_c, \mathbf{W}\big) \leq r_e|\mathbf{W} \in B(r_e), \\
&\quad \mathbf{G}_2 = G_2\Big) = \int_{\mathbf{W}\in B(r_e)} \tilde{f}_{\mathbf{W}|G_2}(\mathbf{W} \mid G_2) \\
&\quad \Pr\Big(\mathrm{d}\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') - \tilde{\varphi}(\mathbf{m}\mathbf{G}') + \Lambda_c, \mathbf{W}\big) \leq r_e|\mathbf{G}_2 = G_2\Big)d\mathbf{W}
\end{aligned}$$

where

$$\tilde{f}_{\mathbf{W}|G_2}(\mathbf{W} \mid G_2) = \frac{f_{\mathbf{W}|G_2}(\mathbf{W} \mid G_2)}{\Pr(\mathbf{W} \in B(r_e) \mid \mathbf{G}_2 = G_2)}.$$

It turns out that the term $\Pr(\mathrm{d}(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') - \tilde{\varphi}(\mathbf{m}\mathbf{G}') + \Lambda_c, \mathbf{w}) \leq r_e|\mathbf{G}_2 = G_2)$ can be bounded by following the Loeliger's approach [26].

Since $\mathrm{d}(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') - \tilde{\varphi}(\mathbf{m}\mathbf{G}') + \Lambda_c, \mathbf{W}) \leq r_e$ implies

$$\Big[\tilde{\varphi}\big(\mathbf{m}'\mathbf{G}'\big) - \tilde{\varphi}\big(\mathbf{m}\mathbf{G}'\big)\Big] \pmod{\Lambda_c} \in B(\mathbf{W}, r_e) \pmod{\Lambda_c},$$

we have

$$\begin{aligned}
&\Pr\Big(\mathrm{d}\big(\tilde{\varphi}\big(\mathbf{m}'\mathbf{G}'\big) - \tilde{\varphi}\big(\mathbf{m}\mathbf{G}'\big) + \Lambda_c, \mathbf{W}\big) \leq r_e|\mathbf{G}_2 = G_2\Big) \\
&\leq \Pr\Big(\Big[\tilde{\varphi}\big(\mathbf{m}'\mathbf{G}'\big) - \tilde{\varphi}\big(\mathbf{m}\mathbf{G}'\big)\Big] \pmod{\Lambda_c} \\
&\quad \in [\mathbf{W} + B(r_e)] \pmod{\Lambda_c} \mid \mathbf{G}_2 = G_2\Big).
\end{aligned}$$

On the other hand, $[\tilde{\varphi}(\mathbf{m}'\mathbf{G}') - \tilde{\varphi}(\mathbf{m}\mathbf{G}')] \pmod{\Lambda_c}$ is uniformly distributed over $\gamma\mathbb{Z}^n \cap \mathcal{V}(\Lambda_c)$, so

$$\begin{aligned}
&\Pr\Big(\Big[\tilde{\varphi}\big(\mathbf{m}'\mathbf{G}'\big) - \tilde{\varphi}\big(\mathbf{m}\mathbf{G}'\big)\Big] \pmod{\Lambda_c} \in B(\mathbf{W}, r_e) \\
&\quad \pmod{\Lambda_c})|\mathbf{G}_2 = G_2\Big) = \frac{|\gamma\mathbb{Z}^n \cap \mathcal{V}(\Lambda_c) \cap B(\mathbf{W}, r_e)|}{p^{n-k_2}} \\
&\leq \frac{|\gamma\mathbb{Z}^n \cap B(\mathbf{W}, r_e)|}{p^{n-k_2}}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\Pr\Big(\mathrm{d}\big(\tilde{\varphi}(\mathbf{m}'\mathbf{G}') + \tilde{\varphi}(\mathbf{U}) + \Lambda_c, \alpha\mathbf{Y}\big) \leq \|\mathbf{W}\||\mathbf{W} \in B(r_e), \\
&\quad \mathbf{G}_2 = G_2\Big) \leq \max_{\mathbf{W}\in B(r_e)} \frac{|\gamma\mathbb{Z}^n \cap B(\mathbf{W}, r_e)|}{p^{n-k_2}},
\end{aligned}$$

and

$$\begin{aligned}
&\Pr\Big(Q_{\Lambda_f}(\mathbf{W}) \notin \Lambda_c|\mathbf{W} \in B(r_e), \mathbf{G_2} = G_2\Big) \\
&\leq p^{k_1-k_2} \max_{\mathbf{W}\in B(r_e)} \frac{|\gamma\mathbb{Z}^n \cap B(\mathbf{W}, r_e)|}{p^{n-k_2}} \\
&\leq \max_{\mathbf{W}\in B(r_e)} \frac{|\gamma\mathbb{Z}^n \cap B(\mathbf{W}, r_e)|}{p^{n-k_1}}.
\end{aligned} \tag{18}$$

Therefore, if $\mathcal{E}_3 = \{\mathbf{W}{:}Q_{\Lambda_f}(\mathbf{W}) \notin \Lambda_c\}$, the probability that the decoding fails is given by:

$$\begin{aligned}
\Pr(\mathcal{E}_3) &\leq n^{-1} + n^{\frac{-1}{2}} + 2\frac{p^{n-k_2}}{\left(\max\left\{0, \frac{\sqrt{nP}}{\gamma} - \frac{\sqrt{n}}{2}\right\}\right)^n V_n} \\
&\quad + \frac{\left(\frac{r_e}{\gamma} + \frac{\sqrt{n}}{2}\right)^n V_n}{p^{n-k_1}}.
\end{aligned} \tag{19}$$

D. THE TOTAL ERROR PROBABILITY FOR NESTED LATTICES OVER INTEGERS

According to Equations (9), (10), and (19), the total error probability of the coding scheme is given by:

$$
\begin{aligned}
\mathrm{P}_e &= \Pr(\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3) \\
&\leq \Pr(\mathcal{E}_1) + \Pr(\mathcal{E}_2) + \Pr(\mathcal{E}_3) \\
&\leq \frac{1}{p^{n-k_1}} + 3\frac{p^{n-k_2}}{\left(\max\left\{0, \dfrac{\sqrt{nP}}{\gamma} - \dfrac{\sqrt{n}}{2}\right\}\right)^n V_n} \\
&\quad + \frac{\left(\dfrac{r_e}{\gamma} + \dfrac{\sqrt{n}}{2}\right)^n V_n}{p^{n-k_1}}.
\end{aligned} \tag{20}
$$

Let $t > 0$ and $\delta \in (0, 1)$, then for parameters $p = \mu n^{1+t}$, $\gamma = n^{\frac{-1}{2}t}$, $k_1 = \lfloor n(1 - \log_p((r_e n^{\frac{t}{2}-\frac{1}{2}} + \frac{1}{2})\sqrt{(1-\delta)^{nV_n^{\frac{2}{n}}}}))\rfloor$, and $k_2 = \lceil n(1 - \log_p((\sqrt{P} n^{\frac{t}{2}} - \frac{1}{2})\sqrt{(1-\delta)^{nV_n^{\frac{2}{n}}}}))\rceil$, the total error probability of our coding scheme decreases as n approches infinity.

Now by substituting parameters chosen above, it can be verified that the rate approches the capacity:

$$
\begin{aligned}
\lim_{n\to\infty}\left(\frac{k_1 - k_2}{n}\right)\log_2 p &= \lim_{n\to\infty}\frac{1}{2}\log_2\left(\frac{nP}{r_e^2}\right) \\
&= \frac{1}{2}\log_2\left(\frac{1 + \frac{P}{\eta^2}}{1 + \epsilon}\right)
\end{aligned} \tag{21}
$$

Since ϵ can be made arbitrarily small, achieving an error probability close to zero is possible with lattice encoding and decoding for any rate below $\frac{1}{2}\log_2(1 + \frac{P}{\eta^2})$.

V. CODING SCHEME FOR NESTED LATTICES OVER IMAGINARY QUADRATIC INTEGERS

Building on the foundation of lattices over integers, we now explore the advantages of algebraic lattices. Algebraic lattices present several advantages over traditional integer lattices, including superior error correction, optimal packing densities, enhanced spectral efficiency, improved diversity, cryptographic security, energy efficiency through spherical shaping, and efficient implementation. These benefits make algebraic lattices a powerful tool in the design and analysis of modern communication systems. One notable feature of algebraic lattices is their ability to facilitate spherical shaping, where signal points are confined to a spherical region. This approach minimizes the average power required for transmission while maintaining the same error performance, resulting in a more energy-efficient communication. Additionally, lattices over imaginary quadratic fields, such as Gaussian integers and Eisenstein integers, often exhibit superior packing densities compared to integer lattices. This allows them to pack more points within a given volume without reducing the minimum distance between points, thereby decreasing the likelihood of errors.

In this section, we introduce Construction A lattices over imaginary quadratic integers and once again incorporate discrete dither into our coding scheme to achieve improved performance. We consider lattices over imaginary quadratic integers, that is $\mathbb{Z}[\xi]$-lattices. This choice is motivated by the ability of these lattices to achieve higher information rates in comparison to $\mathbb{Z}$-lattices. Following the construction of nested lattices in our framework, this section introduces the encoding and decoding procedures for our coding scheme and demonstrates that, subject to certain conditions, the overall error probability of the proposed scheme is highly negligible. Since one can define an isomorphism between $\mathbb{C}^n$ and $\mathbb{R}^{2n}$ as vector spaces for all $n > 0$, we can apply $\mathbb{R}^{2n}$ and $\mathbb{C}^n$ interchangeably.

A. CONSTRUCION A FOR IMAGINARY QUADRATIC INTEGERS

Due to the fact that not all rings of integers $\mathcal{O}_{\mathbb{K}}$ are principal ideal domains (PIDs), let's make the assumption that p is a splitting prime in $\mathcal{O}_{\mathbb{K}}$. This implies that $p\mathcal{O}_{\mathbb{K}}$ can be factored as $\prod_{i=1}^{m} P_i$, where there exists a prime ideal $\mathcal{P}_0$ with a norm of $N(\mathcal{P}_0) = p$. Additionally, it holds that $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}_0} \cong \mathbb{F}_p$. By the definition of canonical embedding, which associates an element in $\mathbb{Z}[\xi]$ with its coset leader in $\dfrac{\mathbb{Z}[\xi]}{\mathcal{P}_0}$, a one-to-one correspondence is established between the elements of an algebraic number field of degree n and the vectors within an n-dimensional Euclidean space. The objective is to establish a mapping from $\mathbb{Z}[\xi]$ to the finite field $\mathbb{F}_p$. Clearly, we can define a surjective homomorphism between $\mathbb{Z}[\xi]$ and the quotient ring $\dfrac{\mathbb{Z}[\xi]}{\mathcal{P}_0}$, along with an isomorphism between $\dfrac{\mathbb{Z}[\xi]}{\mathcal{P}_0}$ and $\mathbb{F}_p$. Consequently, there exists a surjective homomorphism, denoted as φ, from $\mathbb{Z}[\xi]$ to $\mathbb{F}_p$, implying the definition of an inverse operation $\tilde{\varphi}$ componentwise. This operation maps a vector in $\mathbb{F}_p^n$ to a point in $\mathbb{Z}^n[\xi]$.

Similar to $\mathbb{Z}$-lattices, we can apply Construction A for $\mathbb{Z}[\xi]$-lattices to generate nested lattices. Let C_1 and C_2 be two linear codes generated by matrices $\mathbf{G}_1 \in \mathbb{F}_p^{k_1\times n}$ and $\mathbf{G}_2 \in \mathbb{F}_p^{k_2\times n}$, respectively. Let $C_2 \subset C_1 \subset \mathbb{F}_p^n$ which means

$$\mathbf{G}_1 = \begin{bmatrix} \mathbf{G}_2 \\ \mathbf{G}' \end{bmatrix}.$$

If $\mathbf{G}_1$ is full rank, then the same holds true for $\mathbf{G}_2$. By applying Construction A, and lifting these two linear codes over $\mathbb{Z}[\xi]$, we can obtain the following nested lattices:

$$
\begin{aligned}
\Lambda_2 &= \{\mathbf{x} \in \mathbb{Z}^n[\xi] : \varphi(\mathbf{x}) \in C_2\}, \\
\Lambda_1 &= \{\mathbf{x} \in \mathbb{Z}^n[\xi] : \varphi(\mathbf{x}) \in C_1\},
\end{aligned}
$$

with $\Lambda_2 \subset \Lambda_1 \subset \mathbb{Z}^n[\xi]$. By introducing an scaling factor $\gamma > 0$, we have the following coarse and fine lattices

$$
\begin{aligned}
\Lambda_c &= \gamma\Lambda_2, \\
\Lambda_f &= \gamma\Lambda_1,
\end{aligned}
$$

where $\Lambda_c \subset \Lambda_f \subset \gamma\mathbb{Z}^n[\xi]$. Since $\mathrm{V}(\mathbb{Z}^n[\xi]) = (\frac{\sqrt{|\Delta|}}{2})^n$, $\mathrm{V}(\Lambda_c) = \gamma^{2n}p^{n-k_2}(\frac{\sqrt{|\Delta|}}{2})^n$ and $\mathrm{V}(\Lambda_f) = \gamma^{2n}p^{n-k_1}(\frac{\sqrt{|\Delta|}}{2})^n$.

Following the construction of nested lattices in our framework, first we introduce the encoding and decoding procedures for our coding scheme and demonstrate that, subject to certain conditions, the overall error probability of the proposed scheme is highly negligible. Since one can define an isomorphism between $\mathbb{C}^n$ and $\mathbb{R}^{2n}$ as vector spaces for all $n > 0$, we can apply $\mathbb{R}^{2n}$ and $\mathbb{C}$ interchangeably.

B. ENCODING FOR NESTED LATTICES OVER IMAGINARY QUADRATIC INTEGERS

Let $\mathbf{U}$ be a discrete dither. Since all shifted cosets can be expressed as

$$\left\{\tilde{\varphi}\left(\mathbf{mG}'\right) + \tilde{\varphi}(\mathbf{U}) + \Lambda_c{:}\mathbf{m} \in \mathbb{F}_p^{k_1-k_2}\right\},$$

to send a message $\mathbf{m} \in \mathbb{F}_p^{k_1-k_2}$, the encoder transmits $\mathbf{X} = \tilde{\varphi}(\mathbf{mG}') + \tilde{\varphi}(\mathbf{U}) \pmod{\Lambda_c}$.

Since the power constraint is not consistently satisfied, and, indeed, there exists a probability $\Pr(\mathcal{E}_2)$ of the power constraint being exceeded, with the following coding scheme the power constraint is assuredly met.

$$\mathbf{X}_s = \begin{cases} \mathbf{X} & ||\mathbf{X}||^2 \leq nP \\ 0 & \text{otherwise.} \end{cases}$$

This is attributed to the spherical shaping, effectively converting an encoding failure into a decoding failure.

C. DECODING FOR NESTED LATTICES OVER IMAGINARY QUADRATIC INTEGERS

The decoding procedure closely resembles the decoding process outlined in Section III-C. Therefore, upon receiving the signal $\mathbf{Y} \in \mathbb{C}^n$, the decoder initiates the process of estimating the message $\mathbf{m}$ as follows:

$$\hat{\mathbf{m}} = \arg\min d\left(\tilde{\varphi}(\mathbf{mG}') + \tilde{\varphi}(\mathbf{U}) + \Lambda_c, \alpha\mathbf{Y}\right).$$

VI. ANALYSIS OF ERROR PROBABILITIES FOR NESTED LATTICES OVER IMAGINARY QUADRATIC INTEGERS

In order to drive the total error probability of the extended scheme to zero, we require three conditions that bear resemblance to those described in Section IV as (9), (10), and (19). The main difference is considering $\mathbb{Z}[\xi]$-lattices instead of $\mathbb{Z}$-lattices. Consequently, we apply Lemma 2 to derive an upperbound for the total error probability of proposed coding scheme. To establish the goodness of the ensemble for coding, we establish an upper bound rooted in the generator matrix, as well as the probabilities of encoding and decoding errors. This upper bound is shown to decrease markedly as n approaches infinity. Furthermore, the goodness for quantization, as defined by the second moment of the coarse lattice, is demonstrated to be minimal through its covering radius under a specific constraint.

A. THE GENERATOR MATRIX $\mathbf{G}_1$ IS FULL RANK WITH HIGH PROBABILITY

As before, if we establish the set $\mathcal{E}_1 = \{G_1 \in F_p^{k_1 \times n}$ s.t $\mathrm{rank}(G_1) < k_1\}$, the probability associated with $\mathcal{E}_1$ is expressed as:

$$\Pr(\mathcal{E}_1) = 1 - \prod_{i=0}^{k_1-1}\left(1 - \frac{p^i}{p^n}\right) \leq \left(p^{k_1} - 1\right)p^{-n} < \frac{1}{p^{n-k_1}}. \quad (22)$$

Certainly, this probability approaches zero as long as k_1 is less than βn, where $0 < \beta < 1$.

B. THE ENCODING ERROR PROBABILITY FOR NESTED LATTICES OVER IMAGINARY QUADRATIC INTEGERS

Successful encoding occurs if and only if the coset leader $\mathbf{X}$ adheres to the power constraint.. Additionally, we know, $\mathbf{X} \in \tilde{\varphi}(\mathbf{mG}') + \tilde{\varphi}(\mathbf{U}) + \mathbf{\Lambda}_c$. Hence, the encoding fails if and only if $\tilde{\varphi}(m\mathbf{G}') + \tilde{\varphi}(\mathbf{U}) + \mathbf{\Lambda}_c \cap B(\sqrt{nP}) = \emptyset$. Let

$$\mathcal{E}_2(\mathbf{m}) = \{\mathbf{m} : \tilde{\varphi}\left(\mathbf{mG}'\right) + \tilde{\varphi}(\mathbf{U}) + \mathbf{\Lambda}_c \cap B\left(\sqrt{nP}\right) = \emptyset\}.$$

Let us denote $\tilde{\varphi}(\mathbf{mG}' + \mathbf{u} + \mathbf{lG}_2)$ by $\mathbf{t_l}$ for $\mathbf{l} \in \mathbb{F}_p^{k_2}$, then we have

$$\begin{aligned}
\Pr(\mathcal{E}_2) &= \Pr\left(\sum_{\mathbf{l}\in\mathbb{F}_p^{k_2}} \mathbb{I}\left(\mathbf{t_l} \in B\left(\sqrt{nP}\right)\right) = 0\right) \\
&\leq \frac{\mathrm{Var}\left(\sum_{\mathbf{l}\in\mathbb{F}_p^{k_2}} \mathbb{I}\left(\mathbf{t_l} \in B\left(\sqrt{nP}\right)\right) = 0\right)}{\mathrm{E}^2\left(\sum_{\mathbf{l}\in\mathbb{F}_p^{k_2}} \mathbb{I}\left(\mathbf{t_l} \in B\left(\sqrt{nP}\right)\right) = 0\right)} \\
&\leq \frac{p^{n-k_2}}{\left|\gamma\mathbb{Z}^n[\xi] \cap B\left(\sqrt{nP}\right)\right|} \\
&\leq \frac{\left(\frac{\sqrt{|\Delta|}}{2}\right)^n p^{n-k_2}}{\left(\max\left\{0, \frac{\sqrt{nP}}{\gamma} - \frac{\sqrt{2n|\Delta|}}{2}\right\}\right)^{2n} V_{2n}}, \quad (23)
\end{aligned}$$

where the first inequality follows from Chebyshev's inequality, the second one follows from the pairwise independency of lattice points, and the third inequality follows from Lemma 2. We need to choose the prime p such that Equation (23) goes to zero as n goes to infinity.

C. THE DECODING ERROR PROBABILITY FOR NESTED LATTICES OVER IMAGINARY QUADRATIC INTEGERS

Upon receiving the vector $\mathbf{Y}$, decoding failure occurs if for the effective noise $\mathbf{W}$, $Q_{\Lambda_f}(\mathbf{W}) \notin \Lambda_c$. Let define $\mathcal{E}_3 = \{\mathbf{W}{:}Q_{\Lambda_f}(\mathbf{W}) \notin \Lambda_c\}$. According to the Total Probability Theorem, there exists the radius r_e such that

$$\Pr(\mathcal{E}_3) \leq \Pr(\mathbf{W} \notin B(r_e)) + \Pr\left(Q_{\Lambda_f}(\mathbf{W}) \notin \Lambda_c | \mathbf{W} \in B(r_e)\right). \quad (24)$$

For a fixed representative $\mathbf{X} = \mathbf{x}$, we have

$$\|\mathbf{W}\|^2 = (\alpha - 1)^2\|\mathbf{x}\|^2 + \alpha^2\|\mathbf{Z}\|^2 + 2\alpha(\alpha - 1)\|\mathbf{xZ}^T\|, \quad (25)$$

where we have $\mathbf{x}\mathbf{Z}^T \sim \mathcal{N}(0, \|\mathbf{x}\|^2\eta^2)$.

The initial stage involves determining an upper bound for $\Pr(\mathbf{W} \notin B(r_e))$ where $r_e = \sqrt{(1+\epsilon)\frac{nP\eta^2}{P+\eta^2}}$. For any $\epsilon > 0$ and $\alpha > 0$, based on the expression in Equation (25), $\mathbf{W}$ is outside the set $B(r_e)$ if any of the following situations occurs:

$$\mathcal{E}_X = \left\{\mathbf{X} : \|\mathbf{X}\| > \sqrt{nP}\right\}, \tag{26}$$

$$\mathcal{E}_Z = \left\{\mathbf{Z} : \|\mathbf{Z}\| > \sqrt{n\eta^2}\right\}, \tag{27}$$

$$\mathcal{E}_O = \left\{\mathbf{X}\mathbf{Z}^T : \|\mathbf{X}\mathbf{Z}^T\| > n^{\alpha}\sqrt{nP\eta^2}\right\}. \tag{28}$$

Hence, $\Pr(\mathbf{W} \notin B(r_e)) \leq \Pr(\mathcal{E}_X) + \Pr(\mathcal{E}_Z) + \Pr(\mathcal{E}_O)$. We know $\Pr(\{\|\mathbf{X}\| > \sqrt{nP}\}) \leq \frac{p^{n-k_2}}{|\gamma\mathbb{Z}^n[\xi] \cap B(\sqrt{nP})|}$. Since $\mathbf{Z} \sim \mathcal{N}(0, \eta^2\mathbf{I}_n)$, we get $\Pr(\|\mathbf{Z}\| > \sqrt{n\eta^2}) \leq \frac{\eta^2}{n\eta^2}$ by Chebyshev's inequality. Additionally, we have

$$\begin{aligned}
&\Pr\Big(\|\mathbf{X}\mathbf{Z}^T\| > n^{\alpha}\sqrt{nP\eta^2}\Big) \\
&\quad\leq \Pr\Big(\|\mathbf{X}\mathbf{Z}^T\| > n^{\alpha}\sqrt{nP\eta^2}\,|\,\|\mathbf{X}\| \leq \sqrt{nP}\Big) \\
&\qquad + \Pr\Big(\|\mathbf{X}\| > \sqrt{nP}\Big) \\
&\quad\leq \frac{\mathrm{E}\Big(\|\mathbf{X}\mathbf{Z}^T\|^2|\|\mathbf{X}\| \leq \sqrt{nP}\Big)}{n^{2\alpha}nP\eta^2} + \frac{p^{n-k_2}}{|\gamma\mathbb{Z}^n[\xi] \cap B\Big(\sqrt{nP}\Big)|},
\end{aligned}$$

where the last inequality follows since for any given $\mathbf{X} = \mathbf{x}$ with $\|\mathbf{x}\| \leq \sqrt{nP}$ and $\mathbf{x}\mathbf{Z}^T \sim \mathcal{N}(0, \|\mathbf{x}\|^2\eta^2)$, we get $\mathrm{E}(\|\mathbf{X}\mathbf{Z}^T\|^2|\|\mathbf{X}\| \leq \sqrt{nP}) \leq nP\eta^2$. Thus, $\Pr(\mathbf{W} \notin B(r_e))$ is upper bounded by

$$\Pr(\mathbf{W} \notin B(r_e)) \leq \frac{\eta^2}{n\eta^2} + n^{-2\alpha} + 2\frac{p^{n-k_2}}{|\gamma\mathbb{Z}^n[\xi] \cap B\Big(\sqrt{nP}\Big)|}. \tag{29}$$

Now, we establish an upper bound for $\Pr(Q_{\Lambda_f}(\mathbf{W}) \notin \Lambda_c|\mathbf{W} \in B(r_e))$. For any fixed coarse lattice Λ_c,

$$\begin{aligned}
&\Pr\Big(Q_{\Lambda_f}(\mathbf{W}) \notin \Lambda_c|\mathbf{W} \in B(r_e), \mathbf{G}_2 = G_2\Big) \\
&\quad\leq p^{k_1-k_2} \max_{\mathbf{W}\in B(r_e)} \frac{|\gamma\mathbb{Z}^n[\xi] \cap B(\mathbf{W}, r_e)|}{p^{n-k_2}} \\
&\quad\leq \max_{\mathbf{W}\in B(r_e)} \frac{|\gamma\mathbb{Z}^n[\xi] \cap B(\mathbf{W}, r_e)|}{p^{n-k_1}}.
\end{aligned} \tag{30}$$

Therefore, if $\mathcal{E}_3 = \{\mathbf{W} : Q_{\Lambda_f}(\mathbf{W}) \notin \Lambda_c\}$, the probability that the decoding fails is given by:

$$\begin{aligned}
\Pr(\mathcal{E}_3) \leq \frac{\eta^2}{n\eta^2} + n^{-2\alpha} + 2\frac{\left(\frac{\sqrt{|\Delta|}}{2}\right)^n p^{n-k_2}}{\left(\max\left\{0, \frac{\sqrt{nP}}{\gamma} - \rho\right\}\right)^{2n} V_{2n}} \\
+ \frac{\left(\frac{r_e}{\gamma} + \rho\right)^{2n} V_{2n}}{\left(\frac{\sqrt{|\Delta|}}{2}\right)^n p^{n-k_1}}.
\end{aligned} \tag{31}$$

where $\rho = \frac{\sqrt{2n|\Delta|}}{2}$.

D. THE TOTAL ERROR PROBABILITY

According to Equations (22), (23), and (31), the total error probability of the coding scheme is given by:

$$\begin{aligned}
\mathrm{P}_e &= \Pr(\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3) \leq \Pr(\mathcal{E}_1) + \Pr(\mathcal{E}_2) + \Pr(\mathcal{E}_3) \\
&\leq \frac{1}{p^{n-k_1}} + \frac{\eta^2}{n\eta^2} + \frac{3\left(\frac{\sqrt{|\Delta|}}{2}\right)^n p^{n-k_2}}{V_{2n}\left(\max\left\{0, \frac{\sqrt{nP}}{\gamma} - \frac{\sqrt{2n|\Delta|}}{2}\right\}\right)^{2n}} \\
&\quad + \frac{\left(\frac{r_e}{\gamma} + \frac{\sqrt{2n|\Delta|}}{2}\right)^{2n} V_{2n}}{\left(\frac{\sqrt{|\Delta|}}{2}\right)^n p^{n-k_1}}.
\end{aligned} \tag{32}$$

E. GOOD NESTED LATTICES FOR QUANTIZATION OVER IMAGINARY QUADRATIC INTEGERS

In the presence of Gaussian noise, it is common to shape the lattice such that its second moment is less than the average power. This shaping strategy is frequently included in a rate-distortion optimization approach, aiming to strike a balance between the transmission rate of information and the distortion introduced by encoding. This trade-off is vital for achieving efficient communication while minimizing information loss.

Now, we will demonstrate the existence of a coarse lattice Λ_c within our proposed ensemble, satisfying the condition that its second moment is less than or equal to the average power. Let $\boldsymbol{\lambda}^*$ be a deep hole point which is a point in span (Λ_c) at distance $r_{cov}(\Lambda_c)$. We know that $\sigma^2(\Lambda_c) \leq \frac{1}{2n}\mathrm{E}(||\boldsymbol{\lambda}^*||^2)$. Therefore by substituting parameters we get

$$\begin{aligned}
\sigma^2(\Lambda_c) &\leq \frac{1}{2n}\mathrm{E}\Big(||\boldsymbol{\lambda}^*||^2\Big) \\
&\leq \frac{1}{2n}\Pr\Big(\boldsymbol{\lambda}^* \notin B(\sqrt{nP})\Big).E\Big(||\boldsymbol{\lambda}^*||^2|\boldsymbol{\lambda}^* \notin B(\sqrt{nP})\Big) \\
&\quad + \frac{1}{2n}E\Big(||\boldsymbol{\lambda}^*||^2|\boldsymbol{\lambda}^* \in B(\sqrt{nP})\Big) \\
&\leq \frac{p^{n-k_2}}{|\gamma\mathbb{Z}^n[\xi] \cap B\Big(\sqrt{nP}\Big)|}\frac{r^2_{cov}(\Lambda_c)}{2n} + \frac{P}{2} \\
&\leq \frac{\left(\frac{\sqrt{|\Delta|}}{2}\right)^n p^{n-k_2}\gamma^2 p|\Delta|}{4V_{2n}\left(\max\left\{0, \frac{\sqrt{nP}}{\gamma} - \frac{\sqrt{2n|\Delta|}}{2}\right\}\right)^{2n}} + \frac{P}{2},
\end{aligned} \tag{33}$$

where the second inequality can be derived using the law of total expectation, the third inequality is a result of our demonstration in Section VI along with the information that λ^* is a lattice point located at a distance of $r_{cov}(\Lambda_c)$, and the final inequality is a consequence of Equation (23) and the upper bound for the value of $r_{cov}(\Lambda_c)$ as described in Lemma 2.

F. CODING RATE

The coding rate of algebraic nested lattices of dimension $2n$ is $R = \frac{1}{2n}\log_2\frac{\mathrm{V}(\Lambda_c)}{\mathrm{V}(\Lambda_f)}$. Hence, for any $\epsilon > 0$, we get

$$R = \frac{1}{2n}\log_2\left(\frac{\mathrm{V}_{2n}r_c^{2n}}{\mathrm{V}_{2n}r_f^{2n}}\right) = \frac{1}{2}\log_2\left(\frac{nP}{r_e^2}\right)$$
$$= \frac{1}{2}\log_2\left(\frac{P+\eta^2}{(1+\epsilon)\eta^2}\right) = \frac{1}{2}\log_2(1+SNR) - \log_2(1+\epsilon), \tag{34}$$

where $r_e = \sqrt{(1+\epsilon)\frac{nP\eta^2}{P+\eta^2}}$.

VII. ESTIMATION OF PARAMETERS

In this part, we will define the constraints under which the proposed coding scheme is good for coding and MSE quantization. According to Lemma 3, let us assume the prime number $p = \mu n^{\frac{1}{t}+\epsilon}$ and $\gamma = n^{-\frac{1}{2t}-\epsilon}$ for any $t, \epsilon > 0$. Therefore, $\gamma p \to \infty$ and $\gamma^2 p \to 0$. Hence, we derive the constraints under which the following equations are satisfied.

$$\frac{1}{p^{n-k_1}} \to 0, \tag{35}$$

$$\frac{\left(\frac{\sqrt{|\Delta|}}{2}\right)^n p^{n-k_2}}{\left(\max\left\{0, \frac{\sqrt{nP}}{\gamma} - \frac{\sqrt{2n|\Delta|}}{2}\right\}\right)^{2n} V_{2n}} \to 0, \tag{36}$$

$$\frac{\left(\frac{r_e}{\gamma} + \frac{\sqrt{2n|\Delta|}}{2}\right)^{2n} V_{2n}}{\left(\frac{\sqrt{|\Delta|}}{2}\right)^n p^{n-k_1}} \to 0, \tag{37}$$

$$\frac{\left(\frac{\sqrt{|\Delta|}}{2}\right)^n p^{n-k_2}}{\left(\max\left\{0, \frac{\sqrt{nP}}{\gamma} - \frac{\sqrt{2n|\Delta|}}{2}\right\}\right)^{2n} V_{2n}} \cdot \frac{\gamma^2 p|\Delta|}{4} \to 0. \tag{38}$$

Since we already assumed $k_1 < \beta n$ for $0 < \beta < 1$, Equation (35) goes to zero. In the following, we will define k_1 and k_2 as functions of n. We consider

$$k_1 = n\left\lfloor 1 + \log_p\left(\frac{\left(\frac{\sqrt{|\Delta|}}{2}\right)(1-\delta)^{2nV_{2n}^{\frac{1}{n}}}}{\left(b\gamma^{-1} + \frac{\sqrt{|\Delta|}}{2}\right)^2}\right)\right\rfloor$$

$$\text{and } k_2 = n\left\lceil 1 + \log_p\left(\frac{\left(\frac{\sqrt{|\Delta|}}{2}\right)(1-\delta)^{2nV_{2n}^{\frac{1}{n}}}}{\left(a\gamma^{-1} - \frac{\sqrt{|\Delta|}}{2}\right)^2}\right)\right\rceil.$$

Equations (36), (37), and (38) will be very small as n grows, where $a = \sqrt{\frac{P}{2}}$ and $b = \sqrt{(1+\epsilon)\frac{P\eta^2}{P+\eta^2}}$ are constants. Using the facts that $\lim_{n\to\infty}(2n)V_{2n}^{\frac{1}{n}} = 2\pi e$ and $r_e^2 < nP$, for small ϵ, one can prove that $k_2 \leq k_1 \leq n$.

Example 2: Assume $\mathbb{K} = \mathbb{Q}[\sqrt{-3}]$ with discriminant $\Delta = -3$ and $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{-3}}{2}$. For any integer n, the volume of the lattice $(\mathbb{Z}[\omega])^n$ is $(\frac{\sqrt{3}}{2})^n$. Let $\mathcal{P}$ be a prime ideal in the factorization of $p\mathcal{O}_{\mathbb{K}}$ with norm $N(\mathcal{P}) = p$. Let Λ_c and Λ_f be a nested lattices generated according to Section V. Hence, for $t > 0$ and $\delta \in (0, 1)$, by assigning parameters $p = \mu n^{\frac{1}{t}+\epsilon}$, $\gamma = n^{-\frac{1}{2t}-\epsilon}$,

$$k_1 = n\left\lfloor 1 + \log_3\left(\frac{\left(\frac{\sqrt{3}}{2}\right)(1-\delta)^{2nV_{2n}^{\frac{1}{n}}}}{\left(\sqrt{(1+\epsilon)\frac{P\eta^2}{P+\eta^2}}n^{\frac{1}{2t}+\epsilon} + \frac{\sqrt{3}}{2}\right)^2}\right)\right\rfloor,$$

$$\text{and } k_2 = n\left\lceil 1 + \log_3\left(\frac{\left(\frac{\sqrt{3}}{2}\right)(1-\delta)^{2nV_{2n}^{\frac{1}{n}}}}{\left(\sqrt{\frac{P}{2}}n^{\frac{1}{2t}+\epsilon} - \frac{\sqrt{3}}{2}\right)^2}\right)\right\rceil$$

Equations (35)-(38) are satisfied for any $\epsilon > 0$. We can also determine the achievable rate R by substituting the values of k_1 and k_2 as follows:

$$R = \lim_{n\to\infty}\frac{k_1 - k_2}{2n}\log_2 p$$
$$= \lim_{n\to\infty}\frac{1}{2}\log_2\left(\frac{\sqrt{\frac{P}{2}} - \frac{\sqrt{3}}{2}\gamma}{\left(\sqrt{(1+\epsilon)\frac{P\eta^2}{P+\eta^2}} + \frac{\sqrt{3}}{2}\gamma\right)^2}\right)$$
$$= \frac{1}{2}\log_2\left(\frac{P+\eta^2}{\eta^2}\right) - \log_2(1+\epsilon)$$

In contrast, assume we have scaled ingeter lattices Λ_c and Λ_f such that $\gamma\Lambda_c \subset \gamma\Lambda_f \subset \gamma(\frac{\sqrt{3}}{2}\mathbb{Z})^n$ with the same volume of the lattices defined previously. Therefore, $p = \mu n^{1+t}$ and $\gamma = n^{\frac{-1}{2}t}$ for any $t > 0$. $k_1 = \lfloor n(1 - \log_p((r_e n^{\frac{t}{2}-\frac{1}{2}} + \frac{\sqrt{3}}{4})\sqrt{(1-\delta)^{nV_n^{\frac{2}{n}}}}))\rfloor$ and $k_2 = \lceil n(1 - \log_p((\sqrt{P}n^{\frac{t}{2}} - \frac{\sqrt{3}}{4})\sqrt{(1-\delta)^{nV_n^{\frac{2}{n}}}}))\rceil$. It is evident that in the case of quadratic lattice, by setting $p = \mu n^{\frac{1}{t}+\epsilon}$, we get a

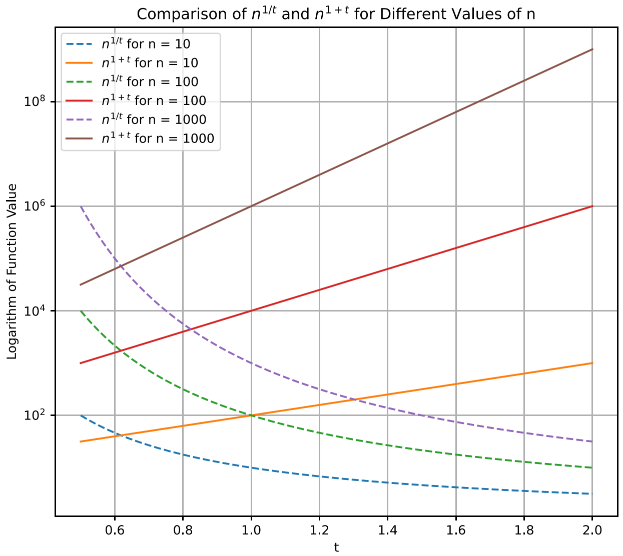

FIGURE 1. Comparison of $n^{1/t}$ and n^{1+t} for n values of 10, 100, and 1000, showing $n^{1/t}$ dominance at low values of t and rapid growth of n^{1+t} at higher values of t.

slower-growing prime number that ensures a denser lattice packing. To see this more clearly, we compare the behavior of the functions $n^{1/t}$ and n^{1+t} for different values of n and t in Figure 1.

At lower values of t, $n^{1/t}$ is significantly higher than n^{1+t}. As t increases, $n^{1/t}$ decreases and n^{1+t} increases, eventually leading to a crossover point where n^{1+t} becomes larger than $n^{1/t}$. For larger n, the crossover point occurs at a smaller t. This behavior is crucial for achieving higher data rates because it allows for denser packing within a given volume. The higher density of lattice points directly translates into increased throughput, which is essential for high-capacity communication channels. Additionally, this choice of p facilitates efficient use of the available bandwidth, making it well-suited for modern communication systems that demand high spectral efficiency. Furthermore, the scaling factor $\gamma = n^{-1/(2t)}$ plays a pivotal role in maintaining a balance between error performance and data rate. By adopting this scaling factor, we achieve a more conservative decrease in the minimum distance between lattice points as the dimension n increases. This gradual reduction in distance helps preserve the robustness of the lattice against noise, ensuring reliable communication even in challenging environments. This is particularly valuable for applications requiring high reliability and low bit error rates.

VIII. CONCLUSION

In this work, we have extended Construction A of nested lattice codes to the ring of algebraic integers of a general imaginary quadratic field. Our study has focused on evaluating the performance of the defined ensemble of lattices for coding and quantization over AWGN channels. Through our comprehensive analysis, we have demonstrated that these codes are highly effective and capable of achieving the channel capacity. Furthermore, we have demonstrated that these codes can achieve the capacity of AWGN channel when the prime number p is of the order $O(n^{\frac{1}{t}})$ for some $t > 0$.

ACKNOWLEDGMENT

The authors are grateful to the Editor and the referees for their very meticulous reading of this manuscript. Their suggestions were very helpful in creating the final version.

REFERENCES

[1] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, vol. 290, New York, NY, USA: Springer, 1998.

[2] J. Conway and N. Sloane, "Voronoi regions of lattices, second moments of polytopes, and quantization," *IEEE Trans. Inf. Theory*, vol. 28, no. 2, pp. 211–226, Mar. 1982.

[3] W. Kositwattanarerk, S. S. Ong, and F. Oggier, "Construction a of lattices over number fields and block fading (wiretap) coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2273–2282, May 2015.

[4] Y.-C. Huang, K. R. Narayanan, and P.-C. Wang, "Lattices over algebraic integers with an application to compute-and-forward," *IEEE Trans. Inf. Theory*, vol. 64, no. 10, pp. 6863–6877, Oct. 2018.

[5] J. Freudenberger and S. Shavgulidze, "Signal constellations based on Eisenstein integers for generalized spatial modulation," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 556–559, Mar. 2017.

[6] F.-M. Han and X.-D. Zhang, "Hexagonal multicarrier modulation: A robust transmission scheme for time-frequency dispersive channels," *IEEE Trans. Signal Process.*, vol. 55, no. 5, pp. 1955–1961, May 2007.

[7] M. Tanahashi and H. Ochiai, "A multilevel coded modulation approach for hexagonal signal constellation," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 4993–4997, Oct. 2009.

[8] Z. Yang, L. Cai, X. Wang, S. Xiang, and J. Pan, "Hierarchical hexagonal modulation with ternary symbols for wireless video transmission," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2014, pp. 245–250.

[9] U. Erez and R. Zamir, "Achieving log(1+SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.

[10] O. Ordentlich and U. Erez, "A simple proof for the existence of 'good' pairs of nested lattices," *IEEE Trans. Inf. Theory*, vol. 62, no. 8, pp. 4439–4453, Aug. 2016.

[11] L. Natarajan, Y. Hong, and E. Viterbo, "Lattice codes achieve the capacity of common message gaussian broadcast channels with coded side information," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1481–1496, Mar. 2018.

[12] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3401–3416, Oct. 2005.

[13] N. E. Tunali, K. R. Narayanan, J. J. Boutros, and Y.-C. Huang, "Lattices over Eisenstein integers for compute-and-forward," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, 2012, pp. 33–40.

[14] Q. T. Sun, J. Yuan, T. Huang, and K. W. Shum, "Lattice network codes based on Eisenstein integers," *IEEE Trans. Commun.*, vol. 61, no. 7, pp. 2713–2725, Jul. 2013.

[15] A. Campello, "Random ensembles of lattices from generalized reductions," *IEEE Trans. Inf. Theory*, vol. 64, no. 7, pp. 5231–5239, Jul. 2018.

[16] S. Lyu, A. Campello, and C. Ling, "Ring compute-and-forward over block-fading channels," *IEEE Trans. Inf. Theory*, vol. 65, no. 11, pp. 6931–6949, Nov. 2019.

[17] R. Qi, C. Feng, and Y.-C. Huang, "A simpler proof for the existence of capacity-achieving nested lattice codes," in *Proc. IEEE Inf. Theory Workshop (ITW)*, 2017, pp. 564–568.

[18] S. Rahman, C. Feng, and A. Chaaban, "A simplified approach to achieving the capacity of the AWGN channel with erasures using nested lattice codes," *IEEE Commun. Lett.*, vol. 26, no. 3, pp. 509–512, Mar. 2022.

[19] H. Dongbo, H. Gang, X. Yonggang, and Y. Hongsheng, "Nested lattice coding with algebraic encoding and geometric decoding," *IEEE Access*, vol. 9, pp. 11598–11609, 2021.

[20] S. Lyu, C. Porter, and C. Ling, “Lattice reduction over imaginary quadratic fields,” *IEEE Trans. Signal Process.*, vol. 68, pp. 6380–6393, Nov. 2020.

[21] S. Lyu, Z. Wang, C. Ling, and H. Chen, “Better lattice Quantizers constructed from complex integers,” *IEEE Trans. Commun.*, vol. 70, no. 12, pp. 7932–7940, Dec. 2022.

[22] A. Campello, D. Dadush, and C. Ling, “AWGN-goodness is enough: Capacity-achieving lattice codes based on dithered probabilistic shaping,” *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1961–1971, Mar. 2019.

[23] L. Kronecker, *Näherungsweise Ganzzahlige Auflösung Linearer Gleichungen*, vol. 3. New York, NY, USA: Chelsea, 1968.

[24] R. Breusch, “Zur Verallgemeinerung des Bertrandschen postulates, daß zwischenx und 2x stets Primzahlen liegen,” *Mathematische Zeitschrift*, vol. 34, no. 1, pp. 505–526, 1932.

[25] H. Khodaiemehr, M.-R. Sadeghi, and A. Sakzad, “Practical encoder and decoder for power constrained QC LDPC-lattice codes,” *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 486–500, Feb. 2017.

[26] H.-A. Loeliger, “Averaging bounds for lattices and linear codes,” *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1767–1773, Nov. 1997.

MARYAM SADEGHI (Member, IEEE) received the B.Sc. degree from the Department of Mathematics, Shiraz University, Iran, in 2009, the first M.Sc. degree from the Department of Mathematics, AmirKabir University of Technology, Iran, in 2013, and the second M.Sc. degree from the Department of Mathematics, University of British Columbia (Okanagan) in 2018, where she is currently pursuing the Ph.D. degree focusing on the construction of algebraic lattices and their performance.

RENMING QI received the B.Eng. degree from the Department of Electronic and Communications Engineering, University of Science and Technology of China, in 2016, and the M.A.Sc. degree from the School of Engineering, University of British Columbia (Okanagan). His research areas include information theory and coding theory.

CHEN FENG (Member, IEEE) received the B.Eng. degree from the Department of Electronic and Communications Engineering, Shanghai Jiao Tong University, China, in 2006, and the M.A.Sc. and Ph.D. degrees from the Department of Electrical and Computer Engineering, University of Toronto, Canada, in 2009 and 2014, respectively. From 2014 to 2015, he was a Postdoctoral Fellow with Boston University, USA, and École Polytechnique Fédérale de Lausanne, Switzerland. He joined the School of Engineering, University of British Columbia, Kelowna, Canada, in July 2015, where he is currently an Associate Professor, the Principal Research Chair in blockchain, and a Co-Cluster Lead of blockchain. He is interested in adapting new ideas and tools from information theory, coding theory, stochastic processes, and optimization to design better communication networks, with a particular emphasis on blockchain technology and quantum communications.

HASSAN KHODAIEMEHR received the bachelor’s degrees in pure mathematics and electrical engineering, the master’s degree in mathematics, and the Ph.D. degree in mathematics from the Amirkabir University of Technology in 2017. He was a Visitor with the University of Carleton, from October 2015 to August 2016 and later a Postdoctoral Fellow at IPM from October 2017 to February 2018. From February 2018 to July 2023, he served as an Assistant Professor with the Department of Computer Science and Statistics, K. N. Toosi University of Technology. Since January 2023, he has been a Postdoctoral Fellow with the University of British Columbia, a position he currently holds. His research interests span data science, blockchain, coding and information theory, cryptography, and quantum computing.

YU-CHIH HUANG (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Texas A&M University at College Station, College Station, TX, USA, in 2013, where he was a Postdoctoral Research Associate from 2013 to 2015. In 2015, he joined the Department of Communication Engineering, National Taipei University, Taiwan, as an Assistant Professor and was promoted to an Associate Professor in 2018. In 2020, he joined the Institute of Communications Engineering, National Yang Ming Chiao Tung University, Taiwan, where he is currently a Professor. His research interests include information theory, coding theory, wireless communications, and machine learning. He received the National Science and Technology Council Wu Ta-You Memorial Award in 2023, the Ministry of Science and Technology Young Scholar Fellowship in 2020, and the 2018 IEEE Information Theory Society Taipei Chapter and IEEE Communications Society Taipei/Tainan Chapter’s Best Paper Award for Young Scholars. He is currently serving as an Associate Editor for IEEE TRANSACTIONS ON COMMUNICATIONS and IEEE COMMUNICATIONS LETTERS.