I. INTRODUCTION

In cooperative communication, the compute-and-forward (C\&F) protocol \cite{1} built over lattice codes is one of the main approaches in physical layer network coding. An important aspect in C\&F is to design network coding matrices \cite{2}. Since algebraic lattice codes have brought more flexibility in the coding part of C\&F \cite{3, 4}, the corresponding algorithms for network coding over imaginary quadratic fields have to be addressed. Though the underlying problem is more non-trivial because the lattices are algebraic in the sense that direct-sums are defined by rings of imaginary quadratic integers.

There has been some work in generalizing Lenstra-Lenstra-Lovász (LLL) reduction to lattices over a number field \mathbb{K} \cite{5, 6, 7}. Napias’s work \cite{5} extends LLL to over Euclidean rings contained in a CM number field or a quaternion field. Fieker and Pohst’s approach \cite{6} defines LLL over Dedekind rings, and Fieker and Stehlé’s approach \cite{7} is to apply LLL to an equivalent higher dimensional \mathbb{Z}-module and return this to a \mathbb{Z}_K-module. Quite recently, Kim and Lee \cite{8} presented algorithms for arbitrary Euclidean domains. While the above approaches can efficiently find short generators for number field lattices in cryptography, the bases of lattices in C\&F (and similarly in detection and precoding \cite{9, 10}) lie in the complex field \mathbb{C}. For such lattices, LLL w.r.t. Gaussian integers was presented in \cite{9}, and \cite{10} had considered a variant w.r.t. Eisenstein integers. To the best of our knowledge, no systematic study on lattice reduction w.r.t. rings of quadratic fields has been conducted.

In this paper, we contribute to the literature in the following aspects. i) We analyze the characteristics of lattices over imaginary quadratic fields, including Hermite’s constant and Minkowski’s first and second theorems. These characteristics provide upper bounds for the successive minima of algebraic lattices, which describe how short a reduced basis can be. ii) We present an algebraic Lenstra-Lenstra-Lovász (ALLL) algorithm, and examine the proper definitions of Lovász’s conditions and size reduction conditions. In addition, we emphasis that lattice reduction based approaches are advantageous in C\&F as they can always generate full rank matrices over finite fields.

**Notations:** Matrices and column vectors are denoted by uppercase and lowercase boldface letters, respectively. The real and imaginary parts of a complex number are denoted as \Re(\cdot) and \Im(\cdot). \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\omega], \mathbb{Q}, \mathbb{R} and \mathbb{C} are used to denote the set of integers, Gaussian integers, Eisenstein integers, rational, real, and complex numbers, respectively. \mathbb{F}_p denotes a finite field with size \(p\). \((\cdot)^\dagger\) refers to the conjugate transpose of either a scalar or a matrix. \(|\cdot|^2\) and \(\|\cdot\|^2\) respectively denote Euclidean norm of a scalar and a vector. \(V_n\) refers to the volume of a unit ball in \(\mathbb{R}^n\). We define \(\log^+(x) \equiv \max(\log(x), 0)\).

II. PRELIMINARIES

**Definition 1** (Quadratic fields). A quadratic field is an algebraic number field \mathbb{K} of degree \([\mathbb{K} : \mathbb{Q}] = 2\) over \mathbb{Q}. In particular, we write \(\mathbb{K} = \mathbb{Q}(\sqrt{-d})\) where \(d \in \mathbb{Z}\) is square free. If \(d > 0\), we say \(\mathbb{Q}(\sqrt{-d})\) is an imaginary quadratic field.

**Definition 2** (Algebraic integers). An algebraic integer is a complex number which is a root of some monic polynomial whose coefficients are in \(\mathbb{Z}\). The set of all algebraic integers forms a subring \(\mathcal{S}\) of \(\mathbb{C}\). For any number field \(\mathbb{K}\), we write \(\mathcal{O}_\mathbb{K} = \mathbb{K} \cap \mathcal{S}\) and call \(\mathcal{O}_\mathbb{K}\) the ring of integers of \(\mathbb{K}\).

Regarding the ring of integers of a quadratic field \(\mathbb{Q}(\sqrt{-d})\), one has \(\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\xi]\) where

\[
\xi = \begin{cases} 
\sqrt{-d}, & \text{if } d \equiv 2, 3 \mod 4; \\
(1 + \sqrt{-d})/2 & \text{if } d \equiv 1 \mod 4.
\end{cases}
\]

We call \(\mathbb{Z}[\xi]\) a TYPE I (respectively TYPE II) ring if \(\xi = \sqrt{-d}\) (respectively \(\xi = (1 + \sqrt{-d})/2\)). We define the algebraic norm map as \(N_r : \mathbb{Z}[\xi] \rightarrow \mathbb{Z}, N_r(a + b\xi) = \)

...
\((a + b\xi) (a + b\xi)^\dagger\). Elements in \(Z[\xi]\) with norm \(\pm 1\) are called the units of \(Z[\xi]\). Together they form a unit group denoted by \(Z[\xi]^\times\).

In this work, we will call any free \(Z[\xi]\)-module an algebraic lattice, where a \(Z[\xi]\)-module is a finitely generated set of elements that is closed under additions and scalar multiplication by \(Z[\xi]\).

**Definition 3 (Algebraic lattices).** A \(Z[\xi]\)-lattice is a discrete \(Z[\xi]\)-submodule of \(C^n\) that has a basis. Such a rank \(n\) lattice \(\Lambda^\xi[\xi](B)\) with basis \(B = [b_1, \ldots, b_n] \subseteq C^{n \times n}\) can be represented by direct sums:

\[
\Lambda^\xi[\xi](B) = Z[\xi] b_1 + Z[\xi] b_2 + \cdots + Z[\xi] b_n.
\]

**Definition 4 (Successive minima).** The \(i\)th successive minimum of a \(Z[\xi]\)-lattice \(\Lambda^\xi[\xi]\) is the smallest real number \(r\) such that its embedded \(Z\)-lattice through a bijection \(\sigma\) contains \(i\) linearly \(Z[\xi]\)-independent vectors of length at most \(r\): 

\[
\lambda_i Z[\xi] = \inf \left\{ r \mid \dim \left( \text{span} \left( \sigma^{-1}(\Lambda^\xi[\xi]) \cap B(0, r) \right) \right) \geq i \right\},
\]

where \(B(t, r)\) denotes a ball centered at \(t\) with radius \(r\).

**Definition 5 (Lattice reduction).** For a given lattice \(\Lambda^\xi[\xi]\) with basis \(B \in C^{n \times n}\), find a new basis \(B = BU\) with favorable properties, where \(U \in \text{GL}_n\) (\(Z[\xi]\)) and \(\text{GL}_n\) (\(Z[\xi]\)) denotes the set of invertible matrices in the matrix ring \(\text{M}_{n \times n}(Z[\xi])\).

A. Hermite’s Constant and OD

To proceed, we first show the \(Z\)-basis (real generator matrix) of lattice \(\Lambda^\xi[\xi](B)\) is:

\[
B^{R, Z}[\xi] = \begin{cases} 
R(B) & \text{if } \xi = \sqrt{-d}; \\
\frac{1}{2}(R(B) - \sqrt{d}J(B)) & \text{if } \xi = \frac{1 + \sqrt{-d}}{2}; \\
\frac{1}{2}(R(B) + \sqrt{d}J(B)) & \text{if } \xi = \frac{1 - \sqrt{-d}}{2}.
\end{cases}
\]

Let ring coefficients of \(B\) be \(x = x_a + \xi x_b \in Z[\xi]^n\). If \(\xi = \sqrt{-d}, d > 0\), we have

\[
Bx = (R(B) + iJ(B)) \left( x_a + i\sqrt{d} x_b \right) = \left( \frac{1}{2}R(B) - \sqrt{d}J(B) \right) x_b + i \left( \frac{1}{2}R(B) + \sqrt{d}J(B) \right) x_b;
\]

and if \(\xi = \frac{1 + \sqrt{-d}}{2}, d > 0\), we have

\[
Bx = (R(B) + iJ(B)) \left( x_a + \frac{1}{2} x_b + i \frac{\sqrt{d}}{2} x_b \right) = \left( \frac{1}{2}R(B) x_a + \frac{1}{2}J(B) \right) x_b + i \left( \frac{1}{2}R(B) x_a + \frac{1}{2}J(B) \right) x_b.
\]

Define the function \(\Psi : C^n \to R^{2n}\) that maps the complex vector \([v_1, \ldots, v_n]^\dagger\) to the real vector:

\[
[\Re(v_1), \ldots, \Re(v_n), \Im(v_1), \ldots, \Im(v_n)]^T.
\]

For any lattice point \(Bx \in \Lambda^\xi[\xi]\), after applying the mapping function \(\Psi(\cdot)\) to Eqs. (2) and (3), we have \(\Psi(Bx) = B^{R, Z}[\xi] [x_a, x_b]^T\), where the expression for \(B^{R, Z}[\xi]\) is given in (1).

According to Eq. (1), the generator matrix of \(\Lambda^\xi[\xi](B)\) is related to that of the \(\Lambda[i]\) lattice \(\Lambda^\xi[\xi](B)\) via

\[
B^{R, Z}[\xi] = B^{R, Z}[i] \left( \Phi^\xi[\xi] \otimes I_n \right),
\]

where

\[
\Phi^\xi[\xi] \triangleq \begin{cases} 
1 & \text{if } \xi = \sqrt{-d}; \\
1 & \text{if } \xi = \frac{1 + \sqrt{-d}}{2}; \\
0 & \text{otherwise}.
\end{cases}
\]

is referred to as the generator matrix of \(Z[\xi]\) in \(\mathbb{R}^2\). It follows that we can define the volume of an algebraic lattice as \(\text{Vol} (\Lambda^\xi[\xi]) \triangleq \text{det} (B^{R, Z}[\xi]) = \text{det} (B^{R, Z}[i]) \text{det} (\Phi^\xi[\xi])^n\).

With the definition of volumes, we extend the definition of Hermite’s constant to over algebraic lattices. Previously, the supremum of \(\lambda_2(L)/\text{Vol}(L)^{1/2}\) for all rank \(n\) \(\mathbb{Z}\)-lattices \(L\) is often denoted by \(\gamma_n\) and called Hermite’s constant \([\Pi]\).

**Definition 6 (Algebraic Hermite’s constant, \([\Pi]\)).** We denote by \(\gamma_n[\xi]\) and find the supremum of \(\lambda_n^2 (\Lambda[\xi]) / \text{Vol} (\Lambda[\xi])^{1/n}\) for all rank \(n\) \(\mathbb{Z}[\xi]\)-lattices \(\Lambda[\xi]\) algebraic Hermite’s constant.

Obviously an algebraic lattice \(\Lambda[\xi](B)\) of dimension \(n\) can always be described by a real lattice \(\Lambda[\xi](B^{R, Z}[\xi])\) of dimension \(2n\). Moreover, since

\[
\lambda_2^2 \left( \Lambda[\xi] \right) / \text{Vol} \left( \Lambda[\xi] \right)^{1/n} \leq \gamma_{2n},
\]

we arrive at the following result:

\[
\gamma_n[\xi] \leq \gamma_{2n} \leq 4 \left( V_{2n}^{-1/n} \right)
\]

for all positive integers \(n\), in which the last inequality is from \([\Pi]\). This upper bound behaves independently of the chosen ring. The actual Hermite’s factor, \(\gamma_n^2 (\Lambda[\xi]) / \text{Vol} (\Lambda[\xi])^{1/n}\), however depends on the ring \(\mathbb{Z}[\xi]\).

Similarly, we introduce the orthogonality defect (OD) for algebraic lattices:

\[
\eta[\xi](B) \triangleq \prod_{i=1}^n \| b_i \| / \text{Vol} (\Lambda[\xi]),
\]

which quantifies how close the basis is to being “orthogonal”. For a \(\mathbb{Z}[i]\)-lattice, its lower bound is \(\eta[\xi](B) \geq 1\) according
to Hadamard’s inequality. More generally, it follows from Eq. \( [5] \) that
\[
\eta_{\mathbb{Z}[\xi]}(B) \geq \det \left( \Phi_{\mathbb{Z}[\xi]} \right)^{-n}.
\]
The volume of a lattice is fixed, so the smallest \( \eta_{\mathbb{Z}[\xi]}(B) \) is achieved only when each \( \|b_j\| \) is minimized.

**B. Minkowski’s Theorems**

Minkowski’s first and second theorems are crucial for analyzing the performance of a lattice reduction algorithm. These theorems over real lattices are well known. For an algebraic lattice where the basis does not belong to a number field, we need the following theorem:

**Theorem 7** (Minkowski’s first and second theorems over \( \mathbb{Z}[\xi] \)-lattices). For a \( \mathbb{Z}[\xi] \)-lattice \( \Lambda_{\mathbb{Z}[\xi]}(B) \) with basis \( B \in \mathbb{C}^{n \times n} \), it satisfies
\[
\lambda_2^{\mathbb{Z}[\xi]} \leq \gamma_2n \left| \det \left( \Phi_{\mathbb{Z}[\xi]} \right) \right| \left| \det (B) \right|^{2/n}, \tag{8}
\]
\[
\prod_{i=1}^{n} \lambda_{i,\mathbb{Z}[\xi]}^{\mathbb{Z}[\xi]} \leq \gamma_n^{\mathbb{Z}[\xi]} \left| \det \left( \Phi_{\mathbb{Z}[\xi]} \right) \right| \left| \det (B) \right| \tag{9}
\]

**Sketch of Proof:** \([6]\) is from \([6]\), and \([9]\) is obtained by first using Minkowski’s second theorem over a \( \mathbb{Z}[\xi] \)-lattice and then discuss the independence of \( 2n \) vectors.

**III. Algebraic LLL**

We now present the definition of algebraic LLL for algebraic lattices. Let \( Q_{\mathbb{Z}[\xi]}(\cdot) \) be a quantization function for a point \( x \in \mathbb{C} \) that returns its closest algebraic integer in \( \mathbb{Z}[\xi] \):
\[
Q_{\mathbb{Z}[\xi]}(x) = \arg \min_{\lambda \in \mathbb{Z}[\xi]} \| \lambda - x \|.
\]

**Definition 8** (Algebraic LLL). An \( n \times n \) complex matrix \( B \in \mathbb{C}^{n \times n} \) is called an ALLL-reduced basis of lattice \( \Lambda_{\mathbb{Z}[\xi]}(B) \) if its QR-decomposition \( B = QR \) satisfies the following two conditions:
\[
Q_{\mathbb{Z}[\xi]} \left( \frac{R_{j,k}}{R_{j,j}} \right) = 0, \quad \forall j < k; \quad \text{(size reduction condition)}
\]
\[
\delta \left| R_{j-1,j-1} \right|^2 \leq \left| R_{j,j} \right|^2 + \left| R_{j-1,j} \right|^2, \quad \text{(Lovász’s condition)} \tag{11}
\]
\[
2 \leq i \leq n. \quad R_{j,k} \text{ refers the } (j,k) \text{th entry of } R, \text{ and } \delta \text{ is called Lovász’s parameter.}
\]

If the lattice is a \( \mathbb{Z}[\xi] \)-lattice, then \([10]\) becomes \( \forall t \left( \frac{R_{j,k}}{R_{j,j}} \right) \leq \frac{1}{2} \) and \( \forall t \left( \frac{R_{j,k}}{R_{j,j}} \right) \leq \frac{1}{2} \), which is consistent with \([9]\) that generalizes the definition in \([5]\).

**A. Lovász’s parameter**

We first explain how the lower bound of \( \delta \) should be chosen based on the covering radius \( \rho_{\mathbb{Z}[\xi]} \) of \( \mathbb{Z}[\xi] \).

**Theorem 9** (Covering radius). Based on the Voronoi region partition, we have
\[
\rho_{\mathbb{Z}[\xi]} \begin{cases} 
\frac{\sqrt{1+\eta} - 1}{2} & \text{if } \xi = \sqrt{-d}, \ d > 0; \\
\frac{d+1}{4\sqrt{d}} & \text{if } \xi = \frac{1+\sqrt{-d}}{2}, \ d > 0.
\end{cases}
\]

**Sketch of Proof:** Both \([13]\) and \([14]\) are essentially the same as those of real LLL, while \([15]\) considers factors from ring \( \mathbb{Z}[\xi] \) since its analysis involves volumes and covering radii.
### C. Implementation

Regarding the implementation of $Q_{Z[\xi]}(\cdot)$, for a TYPE I ring we have

$$ Q_{Z[\xi]}(x) = \arg \min_y \{ |y - x|, \ y \in \{ Q_{Z[\sqrt{-d}]}(x), Q_{Z[\sqrt{-d}]}(x - d^*) + d^* \} \}. $$

**Algorithm 1: The algebraic LLL algorithm.**

**Input:** lattice basis $B \in \mathbb{C}^{n \times n}$, Lovász’s parameter $\delta$, primitive element $\xi$.

**Output:** reduced basis $B \in \mathbb{C}^{n \times n}$, unimodular matrix $U \in \text{GL}_n(\mathbb{Z}[\xi])$.

1. $[Q, R] = \text{qr}(B)$; $\triangleright$ The QR decomposition of $B$;
2. $j = 2$, $U = I_n$;
3. while $j \leq n$ do
   4. for $k = j - 1 : -1 : 1$ do
      5. $c = Q_{Z[\xi]}(R_{j,k}^{\top})$; $\triangleright$ Ring quantization;
      6. if $c \neq 0$ then
         7. $R_{1:n,j} \leftarrow R_{1:n,j} - cR_{1:n,k}$;
         8. $U_{1:n,j} \leftarrow U_{1:n,j} - cU_{1:n,k}$;
      9. if $\delta |R_{j-1,j-1}|^2 > |R_{j,j}|^2 + |R_{j-1,j}|^2$ then
         10. define $M_\omega \triangleq \begin{bmatrix} \sqrt{|R_{j-1,j-1}|^2 + |R_{j,j}|^2} & \sqrt{|R_{j-1,j-1}|^2 + |R_{j,j}|^2} \\ \sqrt{|R_{j-1,j-1}|^2 + |R_{j,j}|^2} & \sqrt{|R_{j-1,j-1}|^2 + |R_{j,j}|^2} \end{bmatrix}$;
         11. swap $R_{1:n,j}$ and $R_{1:n,j-1}$, $U_{1:n,j}$ and $U_{1:n,j-1}$;
         12. $R_{j-1,j} \leftarrow R_{j-1,j-1} M_\omega^{-1}$; $\triangleright$ Left rotation;
         13. $Q_{1:n,j-1} \leftarrow Q_{1:n,j-1} M_\omega^{-1}$; $\triangleright$ Right rotation;
         14. $j \leftarrow \max(j - 1, 2)$;
   15. else
      16. $j \leftarrow j + 1$;
   17. $B = QR$.

Now we present the pseudo-code of algebraic LLL in Algorithm 1. Compared with the LLL algorithm over Gaussian integers in [9], the major differences are: i) The rounding function in Step 5 is generalized from over $\mathbb{Z}[i]$ to over $\mathbb{Z}[\xi]$. ii) Formulas (7)-(15) in [9] are simplified as a rotation by quaternions, which is shown in Steps (10)-(13) of Algorithm 1.

### IV. Lattice Reduction and C&F

In this section, we apply the proposed algebraic lattice reduction algorithm to the C&F paradigm in [4], in which the network coding coefficients should be chosen judiciously so as to optimize the computation rate.

**Theorem 12 (Computation rate [4]).** At a relay with channel coefficients $h \in \mathbb{C}^n$ and combination coefficient $a \in \mathbb{Z}[\xi]^n$, a computation rate of

$$ R_{\text{comp}}(h, a) = \log^+ \left( \frac{1}{a^\top (I_n + P h h^\top) a} \right), $$

where $P$ denotes signal to noise ratio (SNR), is achievable.

By using LDL decomposition to get $I_n + P h h^\top = LDL^\top$ in [16], the denominators in (16) represents the square distance of a lattice vector in $\Lambda^{\mathbb{Z}[\xi]}(D^{-\frac{1}{2}} L^\top)$. The optimal solutions for them require solving a shortest vector problem (SVP). In this work, we concentrate on using lattice reduction algorithms to reduce the basis $B \triangleq D^{-\frac{1}{2}} L^\top$, so as to approximately solve SVP.

#### A. Information rates

To compare the averaged computation rates in C&F, we implement both algebraic LLL reductions (for Euclidean rings $\mathbb{Z}[\omega], \mathbb{Z}[i]$ and non-Euclidean ring $\mathbb{Z}[\sqrt{-5}]$) and classic LLL reductions for lattice bases in C&F, with Lovász’s parameter $\delta = 0.99$. An algebraic LLL algorithm for a ring $\mathbb{Z}[\xi]$ is noted as “$\mathbb{Z}[\xi]$-ALLL”, while its corresponding LLL algorithm for real lattices is noted as “$\mathbb{Z}[\xi]$-LLL”. The computation rates based on using SVP oracles in $\mathbb{Z}[\xi]$-lattices, denoted by “$\mathbb{Z}[\xi]$-SVP” are taken as performance upper bounds of their respective LLL algorithms. The comparison is shown in Fig. 1 with SNR $P \sim 0 - 40$dB, $n = 8$. Several observations can be made from the figure. First, as expected, the $\mathbb{Z}[\omega]$-ALLL algorithm has the best performance among those ALLL algorithms. However, its real counter-part $\mathbb{Z}[\omega]$-LLL has
smaller rates, and the gap is around 1dB in the SNR region of 10 – 20dB. Quite differently, \( \mathbb{Z} [i] \)-ALLL becomes slightly worse than \( \mathbb{Z} [i] \)-RLLL as the SNR increases. Lastly, for the non-Euclidean ring, \( \mathbb{Z} [\sqrt{-5}] \)-ALLL fails to achieve the degree-of-freedom bound, while \( \mathbb{Z} [\sqrt{-5}] \)-RLLL can do so.

Next, we compare the running time of the above algorithms in Fig. 2. Regarding the implementation of an SVP oracle, the depth-first sphere decoding based algorithm with theoretical \( O (n^{1.5} p^{0.5}) \) complexity is taken as the benchmark [14]. The figure shows that sphere decoding algorithms for the expanded \( \mathbb{Z} [\xi] \)-lattices have much higher complexity than lattice reduction based algorithms. In addition, the \( \mathbb{Z} [\omega] \)-ALLL and \( \mathbb{Z} [i] \)-ALLL algorithms are at least a factor of 2 faster than their real counter-parts. Although \( \mathbb{Z} [\sqrt{-5}] \)-ALLL has the lowest complexity, it cannot produce short vectors in general.

### B. Practical advantages

For C&F in multiple access channels (MACs), the optimization domain for the best coefficients are defined as \( \mathbf{A} \in \mathbb{Z} [\xi]^{n \times n} \) and \( \text{rank}(\mathbf{A}) = n \). The optimization is independent of the prime number \( p \) in Construction A, since \( p \) is set to grow to infinity as \( T \to \infty \), where \( T \) is the length of lattice codes. In practical implementations, the size of \( p \) should be limited, so an algebraic lattice reduction algorithm has to ensure that the coefficient matrix \( \mathbf{A} \) is not only full rank over \( \mathbb{Z} [\xi] \), but also full rank over a finite field \( \mathbb{F}_p \) after applying a ring homomorphism \( f : \mathbb{Z} [\xi] \to \mathbb{F}_p \).

The full rank over \( \mathbb{F}_p \) requirement can be easily met if the coefficient matrix \( \mathbf{A} \) is found by using lattice reduction such that \( \mathbf{A} \in \text{GL}_n(\mathbb{Z} [\xi]) \). First, the determinant function for measuring ranks defines a mapping \( \text{GL}_n(\mathbb{Z} [\xi]) \to \mathbb{Z} [\xi]^\times \) between general linear group over \( \mathbb{Z} [\xi] \) and the group of units \( \mathbb{Z} [\xi]^\times \). Since it respects the multiplication in both groups, the function \( \det(\cdot) \) defines a group homomorphism. Second, the determinant function respects the morphism \( f : \text{GL}_n(\mathbb{Z} [\xi]) \to \text{GL}_n(\mathbb{F}_p) \), so we have

\[
\det(f(\mathbf{A})) = \det(f(\mathbf{A})).
\]

As shown in the commutative diagram in Fig. 3 we always have \( \text{rank}(f(\mathbf{A})) = n \) if \( \mathbf{A} \in \text{GL}_n(\mathbb{Z} [\xi]) \).

\[
\begin{align*}
\text{GL}_n(\mathbb{Z} [\xi]) & \overset{f}{\longrightarrow} \text{GL}_n(\mathbb{F}_p) \\
\det & \downarrow \quad \det \\
\mathbb{Z} [\xi]^\times & \overset{f}{\longrightarrow} \mathbb{F}_p^\times \quad = \mathbb{F}_p \setminus \{0\}
\end{align*}
\]

Fig. 3. The commutative diagram of groups and units.

In summary, we have revisited the properties of algebraic lattices and investigated the proper design of lattice reduction operating in the complex domain. While constructing a network coding matrix with full rank over rings is generally not sufficient for making it injective over finite fields, the lattice reduction-based scheme can always do so.

### REFERENCES


