Geometry of Log-unit Lattices

Fernando Azpeitia Tellez, Christopher Powell, and Dr. Shahed Sharif
Department of Mathematics, California State University, San Marcos

Objective

To describe the geometry of log-unit lattices for certain classes of number fields.

Lattices

A **lattice** $\mathcal{L}(b_1, \ldots, b_m)$ is a subgroup of $\mathbb{R}^n$ of the form

$$\mathcal{L}(b_1, \ldots, b_m) = \sum_{i=1}^{m} \mathbb{Z} b_i,$$

where $b_1, \ldots, b_m \in \mathbb{R}^n$ are linearly independent. In other words, a lattice is a regularly spaced array of points. The set $B = \{b_1, \ldots, b_m\}$ is called a **basis** for $\mathcal{L}$. The **fundamental mesh** of $\mathcal{L}(B)$ is defined to be

$$\Phi(B) = \left\{ \sum_{i=1}^{m} x_i b_i \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1 \right\}$$

Geometrically, $\Phi(B)$ is a parallelopiped. The **co-volume** of $\mathcal{L}(B)$ is defined to be the volume of the $\Phi(B)$. A lattice is **orthogonal** if it has an orthogonal basis.

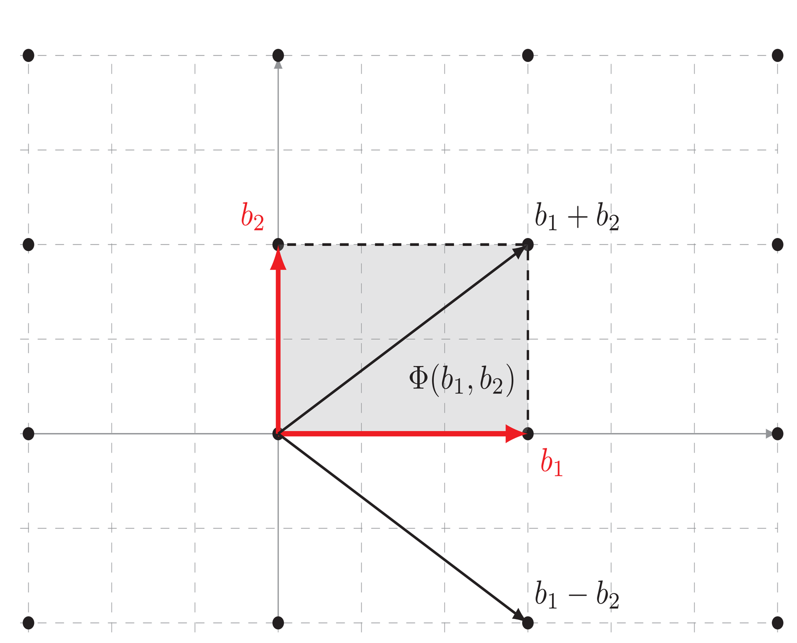

Figure 1. Orthogonal lattice $\mathcal{L}(b_1, b_2)$

The **covering radius** is, roughly, the largest radius ρ such that some open ball of radius ρ does not contain any lattice points.

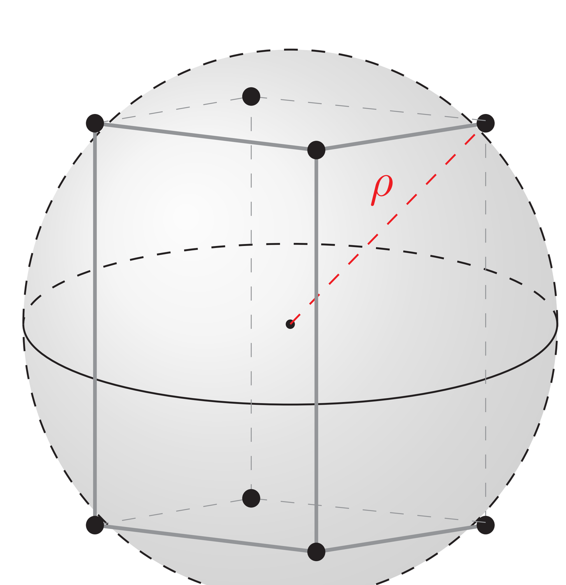

Figure 2. An open ball of radius ρ

Number Fields

A **number field** K is a finite-dimensional field extension of $\mathbb{Q}$. If

$$K = \mathbb{Q}\left(\sqrt{d_1}, \sqrt{d_2}\right)$$

where d_1 and d_2 are distinct square-free integers > 1, then we say K is a **real biquadratic number field**. In this case, elements of K are of the form

$$a + b\sqrt{d_1} + c\sqrt{d_2} + e\sqrt{d_1 d_2}$$

where $a, b, c, e \in \mathbb{Q}$. Each number field K contains an analogue of $\mathbb{Z} \subseteq \mathbb{Q}$, known as the **ring of integers** $\mathcal{O}_K$.

Post-Quantum Cryptography

The security of classical public-key cryptographic algorithms depends on the difficulty of two mathematical problems: the *integer factorization problem* and *discrete log problem*. However, both of these problems can be efficiently solved by a quantum computer running *Shor's algorithm*. In 2016, the National Institute for Standards and Technology (NIST) initiated *Post-Quantum Standardization*, a contest for evaluating and standardizing cryptographic algorithms that are secure against attacks by a quantum computer.

Lattice-based cryptosystems represent over one-third of all candidates submitted to NIST for evaluation. Many of these cryptosystems depend on a special type of lattice, known as a *log-unit lattice*, which are associated to number fields. The security of lattice-based cryptosystems depends on the difficulty of optimization problems such as the *closest vector problem*.

The Problem

With the exception of log-unit lattices associated to some cyclotomic number fields [2], the geometry of these lattices is not well-understood. Yet, the geometry is crucial to the implementation of lattice-based cryptosystems. If the geometry is too well-behaved, the algorithms fail to produce strong encryption (e.g., see attack in [1]).

The following diagrams help to illustrate the difference in complexity in computing the covering radius ρ between an orthogonal lattice and a non-orthogonal lattice.

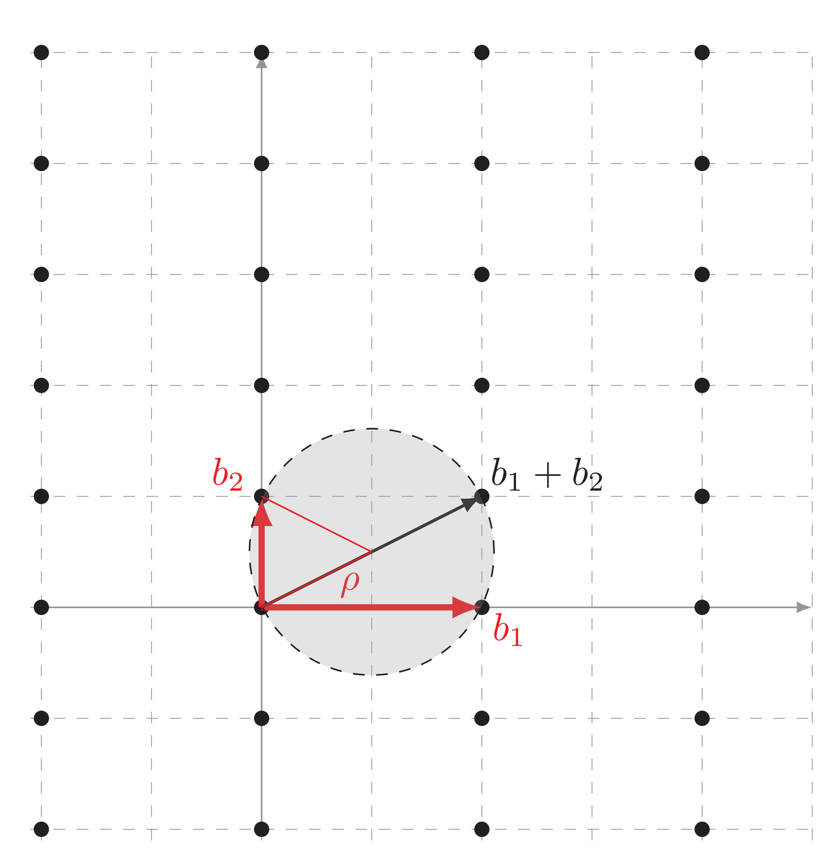

Figure 3. Orthogonal $\mathcal{L}(b_1, b_2)$ with $\rho = \frac{1}{2}(\|b_1 + b_2\|) = 1.1$

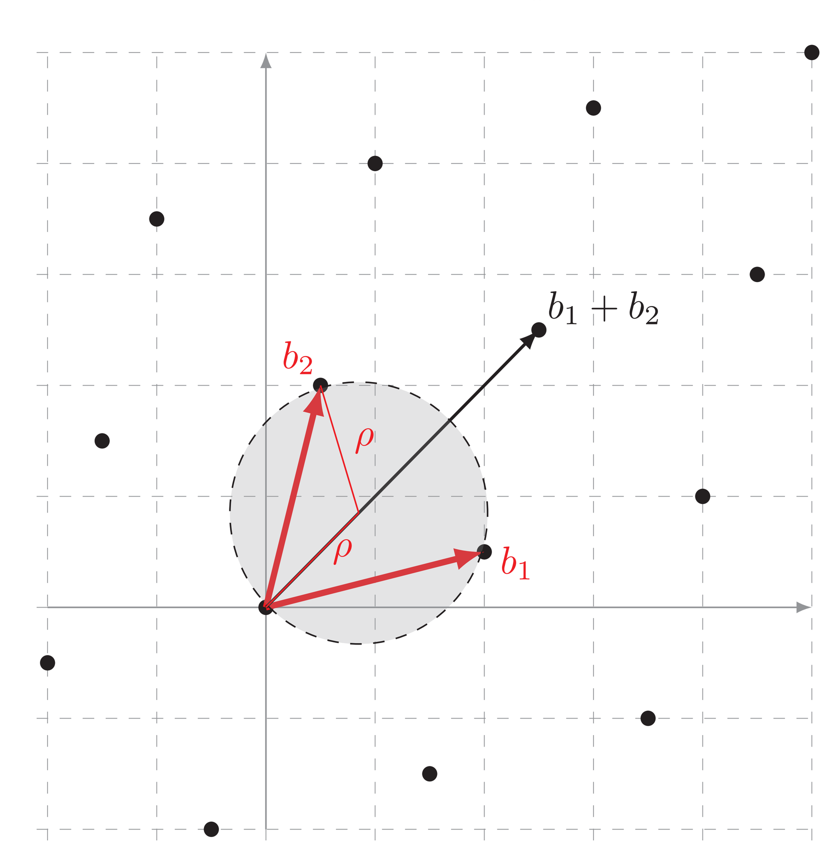

Figure 4. Non-orthogonal $\mathcal{L}(b_1, b_2)$ with $\rho = \frac{1.2\sqrt{2}}{5}\|b_1 + b_2\| = 1.2$

For this research, we mainly address the orthogonality of log-unit lattice associated to real biquadratic number fields, but also other invariants such as ρ.

Logarithmic Embedding

Dirichlet's Unit Theorem describes the structure of the **unit group** $\mathcal{O}_K^\times$, the set of invertible elements in $\mathcal{O}_K$. The proof of this theorem constructs a function $\mathrm{Log} : K^\times \to \mathbb{R}^n$ which maps $\mathcal{O}_K^\times$ to a lattice in a subspace of $\mathbb{R}^n$. In other words, $\Lambda = \mathrm{Log}(\mathcal{O}_K^\times)$ is a lattice, called the **log-unit lattice**. If K is a real biquadratic number field, then Λ is a 3-dimensional lattice in $\mathbb{R}^4$.

Theorem 1

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{d})$ be a real biquadratic number field, where d is prime. If $d \equiv 3 \mod 4$, then Λ is orthogonal.

Conjecture

Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ be a real biquadratic number field. If d_1 and d_2 are distinct primes congruent to $3 \mod 4$, then Λ is not orthogonal.

Exampe 1

For $d = 127$, we get that

$$b_1 = (8.03, 8.03, -8.03, -8.03)$$
$$b_2 = (-0.881, 0.881, -0.881, 0.881)$$
$$b_3 = (-3.12, 3.12, 3.12, -3.12)$$

is a basis for Λ. Note that all basis vectors are mutually orthogonal.

Example 2

For $d_1 = 7$ and $d_2 = 11$, we get that

$$b_1 = (-0.112, -2.88, 2.88, 0.112)$$
$$b_2 = (1.09, -1.09, -1.09, 1.09)$$
$$b_3 = (2.88, 0.112, -0.112, -2.88)$$

is a basis for Λ. Note that $b_1 \perp b_2, b_2 \perp b_3$, but $b_1 \not\perp b_3$.

Summary of Impact

Theorem 1 implies that a certain class of log-unit lattices have a very well-behaved geometry. Consequently, these lattices are too insecure for cryptographic application. Our conjecture, if true, would imply that a certain family of log-unit lattices are *not* orthogonal. However, these lattices contain orthogonal sublattices, which is also undesirable for security.

NTRU Prime

NTRU Prime is a lattice-based cryptosystem submitted to NIST which uses log-unit lattices associated to fields of the form $\mathbb{Q}[x]/\langle x^p - x - 1\rangle$, where p is prime. We implemented a program in SAGE which finds a set of elements $\{\varepsilon_1, \ldots, \varepsilon_m\}$, $m = \frac{p-1}{2}$ that generate the unit group. Our next step is to analyze the factors of $x^p - x$ to determine if a simpler set of generators can be found.

Future Directions

It remains to investigate log-unit lattices associated to other classes of biquadratic fields, cyclic cubic fields, and fields used in the NTRU Prime cryptosystem.

References

[1] Peter Campbell, Michael Groves, and Dan Shepherd, *SOLILOQUY: A Cautionary Tale*, 2014.

[2] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev, *Recovering Short Generators of Principal Ideals in Cyclotomic Rings*, February 25, 2016.

Acknowledgements

This project was possible thanks to generous support from

Special thanks to Dr. Kamel Haddad

Contact Information

- Fernando Azpeitia Tellez
  azpei002@cougars.csusm.edu
- Christopher Powell
  powel054@cougars.csusm.edu
- Dr. Shahed Sharif
  ssharif@csusm.edu