Geometry of log-unit lattices

Fatemeh Jalalvand

Department of Mathematics and Statistics
University of Calgary

March 23, 2024

Supervisor: Prof. Renate Scheidler
Co-Supervisor: Prof. Ha Tran

Motivation

- One motivation behind studying the geometry of log-unit lattices stems from lattice-based cryptography. See, for example, (Cramer, Ducas, Peikert, and Regev-2016) whose analysis of log-unit lattices of cyclotomic fields showed that the SOLILOQUY (Campbell, Groves, and Shepherd-2014) and Smart-Vercauteren cryptosystems (Smart and Vercauterenm-2010) are broken.
- Knowing that a lattice is orthogonal, provides useful information about the shortest vectors (SVP).
- Knowing the geometry of lattices helps bound the regulator.
- WR lattices have a variety of applications in coding theory.

Lattices

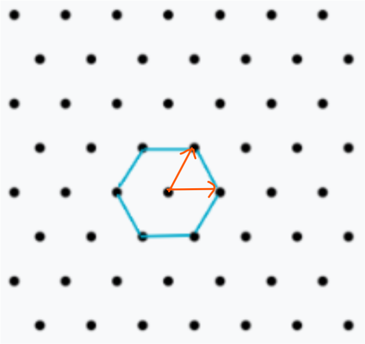
Definition 1

Let $\mathbb{R}^m$ be the m-dimensional Euclidean space. A lattice in $\mathbb{R}^m$ is the set

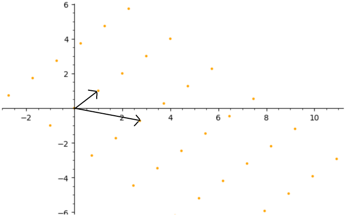
$$\Lambda\left(\mathbf{b}_1, \ldots, \mathbf{b}_k\right) = \left\{ \sum_{i=1}^{k} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}$$

of all integral combinations of k linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_k}$ in $\mathbb{R}^m (m \geq k)$. The integers k and m are called the rank and dimension of the lattice, respectively. The set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k$ is called a lattice basis.

Lattices



(a) Hexagonal lattice



(b) Lattice of rank and dimension 2

Orthogonal lattice

Definition 2

A basis is orthogonal if distinct basis vectors are pairwise orthogonal with respect to inner products in $\mathbb{R}^m$.

Definition 3

If lattice Λ has an orthogonal basis, we say that Λ is orthogonal.

Orthogonal lattice

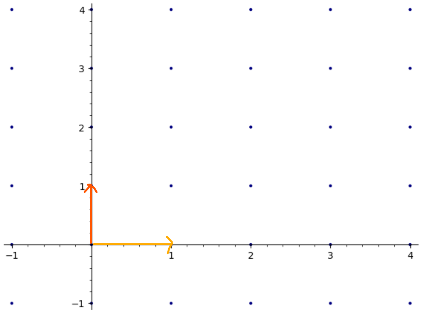


Figure: Orthogonal lattice

Gram matrix

Definition 4

Given a lattice Λ in $\mathbb{R}^m$ with basis $\{b_1, \ldots, b_k\}$, we form the Gram matrix of Λ, denoted $\mathrm{Gr}(\Lambda)$, by taking inner products of the basis vectors:

$$\mathrm{Gr}(\Lambda) = (\langle b_i, b_j \rangle)_{1 \leq i,j \leq k} .$$

Here are gram matrices corresponding to a hexagonal and orthogonal lattice:

$$\begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix},$$

$$\begin{bmatrix} 4 & 0 \\ 0 & 6 \end{bmatrix}.$$

Well rounded lattices

Definition 5

A shortest vector in a lattice is a vector of minimal Euclidean length. We define a lattice of rank k to be well-rounded if it contains k $\mathbb{Z}$-linearly independent shortest vectors, and strongly WR if it contains a minimal basis, i.e. a basis consisting of shortest vectors.

- Every strongly WR lattice is WR, but the converse does not necessarily hold for $4 \leq k$.
- Hexagonal lattice is a strongly WR lattice.

Logarithmic embedding

Let K be a number field of degree $n = r + s$ with U_K denoting its group of units.

Theorem 1

Consider the map Log $: U_K \to \mathbb{R}^{r+s}$ *given by:*

$$Log(\alpha) = (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, 2\log|\tau_1(\alpha)|, \ldots, 2\log|\tau_s(\alpha)|).$$

where σ_i and τ_i correspond to real and pairs of complex embeddings of K respectively. Let $\mathcal{H} \subset \mathbb{R}^{r+s}$ be the hyperplane

$$\mathcal{H} := \left\{(u_1, \ldots, u_{r+s}) \in \mathbb{R}^{r+s} : \sum_{i=1}^{r+s} u_i = 0\right\}.$$

Then $Log(U_K)$ is a lattice contained in $\mathcal{H}$ and called log-unit lattice of K and the kernel of this map are the roots of unity.

Fundamental units

- According to Dirichlet's unit theorem, U_K is a finitely generated abelian group of rank $r + s - 1$ whose torsion part is the roots of unity in K.
- A system of generators of the free part of U_K is called a system of fundamental units.
- Let K be a Galois extension of $\mathbb{Q}$. A unit u in U_K is called a Minkowski unit if u and its conjugates generate the group of units.

Cyclic cubics

- Hasse proved every cyclic cubic field has a Minkowski unit.

Example 6

Let $f = x^3 - x^2 - 2x + 1$ be the defining polynomial of the Galois number field K with root a. The roots are: $a, \frac{1}{1-a}, 1 - \frac{1}{a}$ and a pair of fundamental units are: $a, \frac{1}{1-a}$. Here the Galois generator sends a to $\frac{1}{1-a}$ and so a and $\frac{1}{1-a}$ are Minkowski units.

Numerical experiment - Cyclic quartics

If K is a cyclic quartic extension of $\mathbb{Q}$, it is shown by (Hardy, Hudson, Richman, Williams, and Holtz - 1987) that there are integers A, B, C, D such that

$$K = \mathbb{Q}(\sqrt{A(D + B\sqrt{D})})$$

where

$$\begin{cases} A \text{ is squarefree and odd,} \\ D = B^2 + C^2 \text{ is squarefree, } B > 0, C > 0, \\ A \text{ and } D \text{ are relatively prime.} \end{cases}$$

An experiment by Tran shows that running all possible integers $[A, B, C, D]$ up to 1000 give us 421496 fields among which 369267 have orthogonal log-unit lattices (thus about 87.6% of these fields have orthogonal log-unit lattices).

Numerical experiment - Real pure quartics

In my experiment involving a real pure quartic field extension, where the defining irreducible polynomial is given by $x^4 - a$ with a fourth power free integer a, it was observed that among 100,000 such pure quartic fields, the Gram matrix of 80 percent of them are orthogonal.

Quartic field - Biquadratic case $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$

There are three subfields of K, $k_1 = \mathbb{Q}(\sqrt{m}), k_2 = \mathbb{Q}(\sqrt{n})$, and $k_3 = \mathbb{Q}(\sqrt{\frac{m.n}{gcd(m,n)}})$ and $\varepsilon_1, \varepsilon_2$, and ε_3 are three corresponding fundamental units of the above subfields.

Quartic field - Biquadratic case $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$

There are three subfields of K, $k_1 = \mathbb{Q}(\sqrt{m})$, $k_2 = \mathbb{Q}(\sqrt{n})$, and $k_3 = \mathbb{Q}(\sqrt{\frac{m.n}{gcd(m,n)}})$ and $\varepsilon_1, \varepsilon_2$, and ε_3 are three corresponding fundamental units of the above subfields.

(Kubota-1956) proved there are the following possibilities of fundamental units for K:
Type I: Up to permutation of subscripts, one of (a) $\varepsilon_1, \varepsilon_2, \varepsilon_3$; (b) $\sqrt{\varepsilon_1}, \varepsilon_2, \varepsilon_3$; or (c) $\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \varepsilon_3$.

Type II: Up to permutation of subscripts, one of (a) $\sqrt{\varepsilon_1 \varepsilon_2}, \varepsilon_2, \varepsilon_3$ or (b) $\sqrt{\varepsilon_1 \varepsilon_2}, \varepsilon_2, \sqrt{\varepsilon_3}$.

Type III: $\sqrt{\varepsilon_1 \varepsilon_2}, \sqrt{\varepsilon_2 \varepsilon_3}, \sqrt{\varepsilon_1 \varepsilon_3}$.

Type IV: $\sqrt{\varepsilon_1 \varepsilon_2 \varepsilon_3}, \varepsilon_2, \varepsilon_3$.

Orthogonal and WR biquadratic lattices

Theorem 2 (Tellez, Powell, and Sharif - 2021)

Suppose K is a real biquadratic field. The log-unit lattice of K is orthogonal if and only if K is of type I.

- Conjecture(Cruz-Jalalvand): Suppose K is a real biquadratic number field. WR log unit lattices only occur in type IV.

Log-unit lattices as modules over group rings

- Thinking of lattices modulo rotation and scaling.
- Considering the Galois module structure of the lattices and their Gram matrix modulo above similarities.
- The shortest vectors are invariant under this similarity.
- Let K be a real bicyclic extension of $\mathbb{Q}$ with $Gal(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$. Let Λ be the log unit lattice of K. Note that Λ is a module over $\mathbb{Z}[\sigma, \tau]/ < \tau^2 - 1, \sigma^2 - 1, 1 + \sigma\tau + \sigma + \tau >$.

Real biquadratics

- Note that in this case, $v = \sqrt{\epsilon_1\epsilon_2\epsilon_3}$ is a Minkowski unit. Here is the Gram matrix of a basis corresponding to the Minkowski vector:

$$\begin{bmatrix} \langle v, v\rangle & \langle v, \sigma(v)\rangle & \langle v, \tau(v)\rangle \\ \langle \sigma(v), v\rangle & \langle \sigma(v), \sigma(v)\rangle & \langle \sigma(v), \tau(v)\rangle \\ \langle \tau(v), v\rangle & \langle \tau(v), \sigma(v)\rangle & \langle \tau(v), \tau(v)\rangle \end{bmatrix}.$$

which is similar to:

$$\begin{bmatrix} 1 & x & y \\ x & 1 & -1-x-y \\ y & -1-x-y & 1 \end{bmatrix},$$

where $x := \langle \sigma(v), \sigma(v)\rangle$ and $y =: \langle \sigma(v), \tau(v)\rangle$

Real biquadratics

Theorem 3

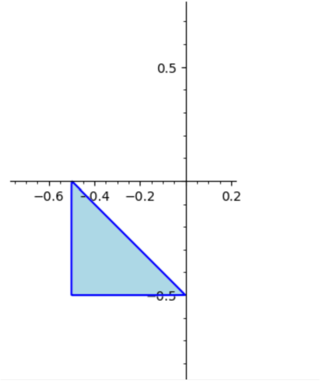
Let Λ be a lattice of rank 3. Then Λ is well-rounded if and only if there exists a basis $B = \{x, y, z\}$ of Λ whose associated Gram matrix is of the form

$$G_B = \begin{bmatrix} a & b & c \\ b & a & d \\ c & d & a \end{bmatrix}$$

where $a = \|x\|^2 = \|y\|^2 = \|z\|^2$ and the quantities a, b, c, d satisfy the inequalities

$$\begin{aligned} |b|, |c|, |d| &\leq a/2 \\ -b + c + d &\leq a \\ b - c + d &\leq a \\ b + c - d &\leq a \\ -b - c - d &\leq a \end{aligned}$$

So by the previous theorem ($a = 1, b = x, c = y,\ d = -1 - x - y$):



Thanks for your attention!

Successive Minima

Definition 7

The i-th successive minimum λ_i *of a lattice is the radius of the smallest sphere centered in the origin that contains i* $\mathbb{Z}$*-linearly independent lattice vectors.*

Numercal example for WR lattice

$(Q)(\sqrt{41}, \sqrt{317})$
[66.925330, -32.328653, -26.627351;
-32.328653, 66.925330, -7.9693252;
-26.627351, -7.969325, 66.925330],

[8, 66.925330, [0, 1, -1, 0; 0, 1, 0, 1; 1, 1, 0, 0]]]

Lattice without a minimal basis

An 11-dimensional gram matrix Λ

$$
\begin{bmatrix}
60 & 5 & 5 & 5 & 5 & 5 & -12 & -12 & -12 & -12 & -7 \\
5 & 60 & 5 & 5 & 5 & 5 & -12 & -12 & -12 & -12 & -7 \\
5 & 5 & 60 & 5 & 5 & 5 & -12 & -12 & -12 & -12 & -7 \\
5 & 5 & 5 & 60 & 5 & 5 & -12 & -12 & -12 & -12 & -7 \\
5 & 5 & 5 & 5 & 60 & 5 & -12 & -12 & -12 & -12 & -7 \\
5 & 5 & 5 & 5 & 5 & 60 & -12 & -12 & -12 & -12 & -7 \\
-12 & -12 & -12 & -12 & -12 & -12 & 60 & -1 & -1 & -1 & -13 \\
-12 & -12 & -12 & -12 & -12 & -12 & -1 & 60 & -1 & -1 & -13 \\
-12 & -12 & -12 & -12 & -12 & -12 & -1 & -1 & 60 & -1 & -13 \\
-12 & -12 & -12 & -12 & -12 & -12 & -1 & -1 & -1 & 60 & -13 \\
-7 & -7 & -7 & -7 & -7 & -7 & -13 & -13 & -13 & -13 & 96
\end{bmatrix}
$$

is generated by its 24 minimal vectors, but no set of 11 minimal vectors forms a basis.