Lattices in Real, Complex, and Quaternionic Vector Spaces

Stephanie L. Vance

University of Washington

February 6, 2008

Lattices over $\mathbb{Z}$

Let E denote a finite-dimensional Euclidean space.

- A *lattice* in E is an additive subroup which is generated by some basis for E as a real vector space.
- A sub-Z-module of a lattice Λ is called a *relative lattice.* A relative lattice Λ' contained in Λ is a (full) lattice in the subspace of E obtained by taking the span of the lattice vectors in Λ' over $\mathbb{R}$.
- All lattices in E are discrete with respect to the Euclidean topology defined on E. So we can define the *norm of a lattice* Λ , denoted by $\mathrm{N}(\Lambda)$, to be the norm of its minimal vectors (non-zero vectors of minimal norm).

Generating and Gram Matrices

Let Λ be a lattice in E with lattice basis $\{b_1, \ldots, b_n\}$.

- A *generating matrix for* Λ is the matrix $M \in \mathrm{GL}_n(\mathbb{R})$ whose i^{th} row is the coordinates b_i determined by a fixed orthonormal basis for E.

Generating and Gram Matrices

Let Λ be a lattice in E with lattice basis $\{b_1, \ldots, b_n\}$.

- A *generating matrix for* Λ is the matrix $M \in \mathrm{GL}_n(\mathbb{R})$ whose i^{th} row is the coordinates b_i determined by a fixed orthonormal basis for E.
- The Gram matrix for Λ corresponding to the above basis is the matrix $A = (\langle b_i, b_j \rangle)_{1 \le i,j \le n} = MM^T$ which is a positive definite symmetric matrix in $\mathrm{GL}_n(\mathbb{R})$.

Generating and Gram Matrices

Let Λ be a lattice in E with lattice basis $\{b_1, \ldots, b_n\}$.

- A *generating matrix for* Λ is the matrix $M \in \mathrm{GL}_n(\mathbb{R})$ whose i^{th} row is the coordinates b_i determined by a fixed orthonormal basis for E.
- The Gram matrix for Λ corresponding to the above basis is the matrix $A = (\langle b_i, b_j \rangle)_{1 \leq i,j \leq n} = MM^T$ which is a positive definite symmetric matrix in $\mathrm{GL}_n(\mathbb{R})$.
- A generating matrix and Gram matrix for a lattice are not unique. However, the determinant of a gram matrix is and is called the *determinant of* Λ , denoted by $\det(\Lambda)$.

Fundamental regions and Lattice Determinants

Let Λ be a with basis $B = \{b_1, ..., b_n\}$.

- The *fundamental parallelotope of* Λ *with respect to* B is the set,
$$P = \{\sum_i \alpha_i b_i : 0 \leq \alpha_i < 1\}.$$
- E can be tiled with infinitely many copies of P. More explicitly,
$$E = \coprod_{x \in \Lambda} \{x + p : p \in P\}.$$
- Note that a fundamental parallelotope for Λ is dependent on the lattice basis B. However, its volume $|\det M|$ is not. The squared volume of a fundamental region is equal to $\det(\Lambda)$.

Fundamental regions of 2-dimensional lattices

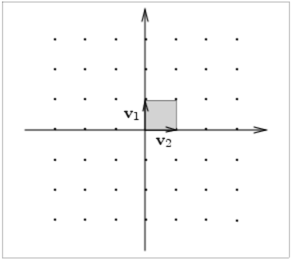

Figure: Integer Lattice $\mathbb{Z}^2$

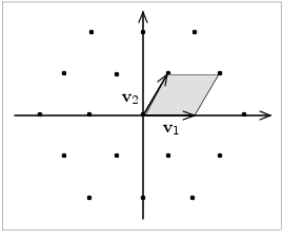

Figure: Hexagonal lattice

Constructing Lattices in f.d. Euclidean spaces

Let E be an n-dimensional Euclidean space.

- For any basis $\{b_1, \ldots, b_n\}$ for E, let Λ be the $\mathbb{Z}$-module generated by the basis vectors.

Constructing Lattices in f.d. Euclidean spaces

Let E be an n-dimensional Euclidean space.

- For any basis $\{b_1, \ldots, b_n\}$ for E, let Λ be the $\mathbb{Z}$-module generated by the basis vectors.
- Find the Cholesky decomposition of a positive definite symmetric matrix $Q = AA^T$.

Constructing Lattices in f.d. Euclidean spaces

Let E be an n-dimensional Euclidean space.

- For any basis $\{b_1, \ldots, b_n\}$ for E, let Λ be the $\mathbb{Z}$-module generated by the basis vectors.
- Find the Cholesky decomposition of a positive definite symmetric matrix $Q = AA^T$.
- Embed the Ring of Integers for a number field into $\mathbb{C}^n$

Constructing Lattices in f.d. Euclidean spaces

Let E be an n-dimensional Euclidean space.

- For any basis $\{b_1, \ldots, b_n\}$ for E, let Λ be the $\mathbb{Z}$-module generated by the basis vectors.
- Find the Cholesky decomposition of a positive definite symmetric matrix $Q = AA^T$.
- Embed the Ring of Integers for a number field into $\mathbb{C}^n$
- Find the pre-image of linear codes in ${F_p}^n$ under the natural projection map $\pi : \mathbb{Z}^n \mapsto {F_p}^n$

Dual Lattices

Let Λ be a lattice in an n-dimensional Euclidean space.

- The *dual of* Λ is defined to be the set of vectors

$$\Lambda^* = \{x \in K \ : \ \langle x, \Lambda \rangle \subseteq \mathbb{Z}\}.$$

Dual Lattices

Let Λ be a lattice in an n-dimensional Euclidean space.

- The *dual of* Λ is defined to be the set of vectors

$$\Lambda^* = \{x \in K \ : \ \langle x, \Lambda \rangle \subseteq \mathbb{Z}\}.$$

- The dual of Λ is a lattice in E. Moreover, a basis for Λ^* may be found by computing the dual basis for any lattice basis of Λ. This provides a bijective correspondence between ordered lattice bases for Λ and ordered lattice bases for Λ^*

Dual Lattices

Let Λ be a lattice in an n-dimensional Euclidean space.

- The *dual of* Λ is defined to be the set of vectors

$$\Lambda^* = \{x \in K \ : \ \langle x, \Lambda \rangle \subseteq \mathbb{Z}\}.$$

- The dual of Λ is a lattice in E. Moreover, a basis for Λ^* may be found by computing the dual basis for any lattice basis of Λ. This provides a bijective correspondence between ordered lattice bases for Λ and ordered lattice bases for Λ^*
- Λ is said to be *integral* if it is contained in its dual and it is said to be *unimodular (or self-dual)* if it is equal to its dual.

Dual Lattices (continued)

Dual Lattices (continued)

- If M is a generating matrix for Λ and M^* is a generating matrix for Λ^* corresponding to the basis dual to the rows of M, then $M^{-1} = (M^*)^T$.

Dual Lattices (continued)

- If M is a generating matrix for Λ and M^* is a generating matrix for Λ^* corresponding to the basis dual to the rows of M, then $M^{-1} = (M^*)^T$.

- For any $\mathbb{Z}$-lattice Λ, we always have $\det(\Lambda)\det(\Lambda^*) = 1$.

Relative and Dual Lattices

Let Λ be a lattice in E and let F be any subspace in E.

- The relative lattice $\Lambda \cap F$ is a lattice in F if and only if $\pi_{F^\perp}(\Lambda)$ is a lattice in $\mathrm{F}^\perp$
- $\Lambda \cap F$ is an lattice in F if and only if $\Lambda^* \cap F^\perp$ is a lattice in $F^\perp$.
- If $\Lambda \cap F$ is a $\mathbb{Z}$-lattice in F then,

$$\det \Lambda = \det(\Lambda \cap F) \det(\pi_{F^\perp}(\Lambda))$$

The Kissing Number Problem

- An argument between Isaac Newton and David Gregory in 1694

(missing)

Figure: 12 Spheres "Kissing" a Central Sphere

The Kissing Number Problem

- An argument between Isaac Newton and David Gregory in 1694
- Newton proved correct in 1874 (almost 200 years later!).

(missing)

Figure: 12 Spheres "Kissing" a Central Sphere

The Kissing Number Problem

- An argument between Isaac Newton and David Gregory in 1694
- Newton proved correct in 1874 (almost 200 years later!).
- The 4-dimensional case resolved in 2003 by Oleg Musin.

(missing)

Figure: 12 Spheres "Kissing" a Central Sphere

The Kissing Number Problem

- An argument between Isaac Newton and David Gregory in 1694
- Newton proved correct in 1874 (almost 200 years later!).
- The 4-dimensional case resolved in 2003 by Oleg Musin.
- Open problen in higher dimensions except eight and twenty-four.

(missing)

Figure: 12 Spheres "Kissing" a Central Sphere

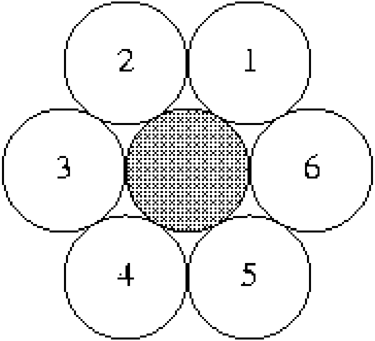

Figure: 2D Kissing # Solution

Packing Congruent Spheres in Euclidean Space

- Configurations of congruent non-overlapping spheres in finite-dimensional Euclidean space are called *sphere packings.*

Packing Congruent Spheres in Euclidean Space

- Configurations of congruent non-overlapping spheres in finite-dimensional Euclidean space are called *sphere packings.*
- Sphere packings in which the sphere centers form a lattice are called *lattice packings.*

Packing Congruent Spheres in Euclidean Space

- Configurations of congruent non-overlapping spheres in finite-dimensional Euclidean space are called *sphere packings.*
- Sphere packings in which the sphere centers form a lattice are called *lattice packings.*
- The problem of finding the densest lattice sphere packings remains open for dimensions larger than eight except for dimension twenty-four.

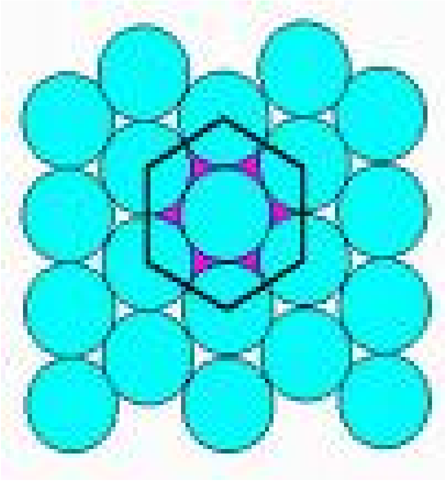

Figure: Hexagonal Sphere Packing

A Little History...

- Kepler's conjecture in 1611 for 3-dimensional FCC lattice.

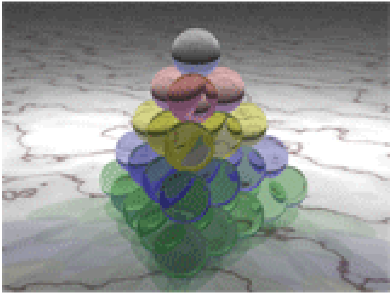

Figure: FCC Lattice Packing

A Little History...

- Kepler's conjecture in 1611 for 3-dimensional FCC lattice.
- Gauss proved conjecture for the lattice sphere packing problem (1831).

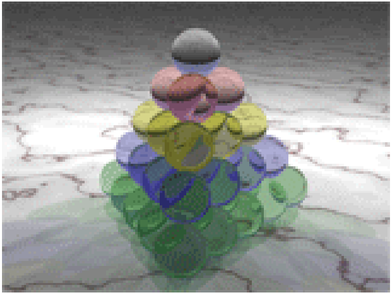

Figure: FCC Lattice Packing

A Little History...

- Kepler's conjecture in 1611 for 3-dimensional FCC lattice.
- Gauss proved conjecture for the lattice sphere packing problem (1831).
- Toth reduced the Kepler's conjecture to several special cases (1953).

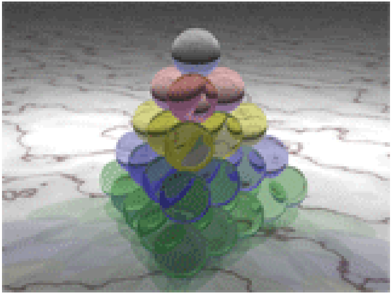

Figure: FCC Lattice Packing

A Little History...

- Kepler's conjecture in 1611 for 3-dimensional FCC lattice.
- Gauss proved conjecture for the lattice sphere packing problem (1831).
- Toth reduced the Kepler's conjecture to several special cases (1953).
- Thomas Hales found computer assisted proof in 1998.

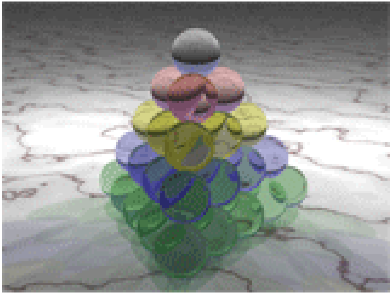

Figure: FCC Lattice Packing

Lattice Packing Quantites

- Packing Radius: $\frac{\sqrt{\mathrm{N}(\Lambda)}}{2}$
- Packing Density: $\frac{\mathrm{N}(\Lambda)^{n/2} V_n}{2^n \sqrt{\det(\Lambda)}}$
  V_n denotes the volume of unit sphere in $\mathbb{R}^n$.
- Hermite Invariant: $\gamma(\Lambda) = \frac{\mathrm{N}(\Lambda)}{\det(\Lambda)^{1/(n)}}$.
- Covering Radius

Preliminaries for lattices in $\mathbb{C}^n$

- Let F be a quadratic extension of $\mathbb{Q}$ such that $F = \mathbb{Q}(\sqrt{d})$ with $d < 0$.

Preliminaries for lattices in $\mathbb{C}^n$

- Let F be a quadratic extension of $\mathbb{Q}$ such that $F = \mathbb{Q}(\sqrt{d})$ with $d < 0$.
- Define an involution on $\mathbb{C} = \mathbb{R} \otimes F$ by $a + b\sqrt{d} \mapsto a - b\sqrt{d}$, with a and b real numbers. For each $x \in \mathbb{C}$, its image under this map will be denoted by $\overline{x}$ and is called its conjugate.

Preliminaries for lattices in $\mathbb{C}^n$

- Let F be a quadratic extension of $\mathbb{Q}$ such that $F = \mathbb{Q}(\sqrt{d})$ with $d < 0$.
- Define an involution on $\mathbb{C} = \mathbb{R} \otimes F$ by $a + b\sqrt{d} \mapsto a - b\sqrt{d}$, with a and b real numbers. For each $x \in \mathbb{C}$, its image under this map will be denoted by $\overline{x}$ and is called its conjugate.
- We can define lattices in finite-dimensional complex vector spaces over self-conjugate orders in F. Recall that an order in F is a subring $\mathcal{O}$ that is also a free sub-Z-module with $\mathrm{rank}_{\mathbb{Z}}\mathcal{O} = \mathrm{rank}_{\mathbb{Q}}F$.

$\mathcal{O}$-Lattices in complex vector spaces

Let $\mathcal{O}$ be a self-conjugate order in F and let E be an n-dimensional complex vector space. An *$\mathcal{O}$-lattice* in E is a free $\mathcal{O}$-module which is generated by some basis for E as a complex vector space.

- If Λ is an *$\mathcal{O}$-lattice* in any subspace of E, Λ is called a *relative $\mathcal{O}$-lattice*.
- Any $\mathcal{O}$-lattice in E has the structure as a $\mathbb{Z}$-lattice in a $(2n)$-dimensional real vector space.

Gaussian and Eisenstein Lattices

The Eisenstein lattices are lattices in complex vector spaces over the self-conjugate maximal order of Eisenstein integers

$$\mathcal{E} = \left\{ a + \left(\frac{1 + i\sqrt{3}}{2} \right) b : a, b \in \mathbb{Z} \right\}.$$

Examples:

- The root lattices D_4 and E_8
- The 16-dimensional Barnes-wall lattice Λ_{16}
- The Coxeter-Todd lattice K_{12}
- The Leech lattice Λ_{24}

Preliminaries for lattices in $\mathbb{H}^n$

- Let H denote the skew field of rational quaternions such that

$$H = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

with $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$.

Preliminaries for lattices in $\mathbb{H}^n$

- Let H denote the skew field of rational quaternions such that

$$H = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

  with $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$.
- Define a map on $\mathbb{H} = \mathbb{R} \otimes H$, by $a + bi + cj + dk \mapsto a - bi - cj - dk$, with $a, b, c, d \in \mathbb{R}$. This is commonly referred to as quaternionic conjugation and the image of an element $x \in \mathbb{H}$ under this map is denoted by $\overline{x}$.

Preliminaries for lattices in $\mathbb{H}^n$

- Let H denote the skew field of rational quaternions such that

$$H = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

  with $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$.
- Define a map on $\mathbb{H} = \mathbb{R} \otimes H$, by $a + bi + cj + dk \mapsto a - bi - cj - dk$, with $a, b, c, d \in \mathbb{R}$. This is commonly referred to as quaternionic conjugation and the image of an element $x \in \mathbb{H}$ under this map is denoted by $\overline{x}$.
- Quaterionic conjugation is an anti-involution on $\mathbb{H}$!

$\mathcal{O}$-Lattices in quaternionic vector spaces

Let $\mathcal{O}$ be a self-conjugate order in H and let E be an n-dimensional quaternionic vector space. An *$\mathcal{O}$-lattice* in E is a free $\mathcal{O}$-module which is generated by some basis for E as a quaternionic vector space.

- If Λ is an *$\mathcal{O}$-lattice* in any subspace of E, Λ is called a *relative $\mathcal{O}$-lattice*.
- Any $\mathcal{O}$-lattice in E has the structure as a lattice over $\mathbb{Z}$ in a $(4n)$-dimensional real vector space.

Hurwitz Lattices

The Hurwitz lattices are lattices in quaternionic vector spaces over the self-conjugate maximal order of Hurwitz integers

$$\mathcal{H} = \left\{ a + bi + cj + dk : \ a, b, c, d \in \mathbb{Z} \ \text{ or } \ a, b, c, d \in \mathbb{Z} + \frac{1}{2} \right\}.$$

The Hurwitz integers are nice to work over because they are a principal (right/left) ideal domain for which we have "division with small remainder".

Examples of Hurwitz Lattices:

- The root lattices D_4 and E_8
- The 16-dimensional Barnes-wall lattice Λ_{16}
- The Leech lattice Λ_{24}

Duality for $\mathcal{O}$-lattices

Let Λ be an $\mathcal{O}$-lattice in a complex or quaternionic vector space E. Using the hermitian structure defined on E by $h(x, y) = x\overline{y}$, we can construct an $\mathcal{O}$-dual lattice for Λ.

- The *dual of* Λ is defined to be the set of vectors

$$\Lambda^{\#} = \{x \in K \ : \ h(x, \Lambda) \subseteq \mathcal{O}\}.$$

- A basis for $\Lambda^{\#}$ may be found by computing the dual basis for any lattice basis of Λ (with respect to h).

Research Direction

- Extend existing theorems for lattices in $\mathbb{R}^n$ to $\mathcal{O}$-lattices in $\mathbb{C}^n$ and $\mathbb{H}^n$.

Research Direction

- Extend existing theorems for lattices in $\mathbb{R}^n$ to $\mathcal{O}$-lattices in $\mathbb{C}^n$ and $\mathbb{H}^n$.
- The sphere packing problem for $\mathcal{O}$-lattices in complex and quaternionic vector spaces.

Research Direction

- Extend existing theorems for lattices in $\mathbb{R}^n$ to $\mathcal{O}$-lattices in $\mathbb{C}^n$ and $\mathbb{H}^n$.
- The sphere packing problem for $\mathcal{O}$-lattices in complex and quaternionic vector spaces.
  - Find Upper bounds for sphere packing densities by looking at lower-dimensional $\mathcal{O}$-lattices.

Research Direction

- Extend existing theorems for lattices in $\mathbb{R}^n$ to $\mathcal{O}$-lattices in $\mathbb{C}^n$ and $\mathbb{H}^n$.
- The sphere packing problem for $\mathcal{O}$-lattices in complex and quaternionic vector spaces.
    - Find Upper bounds for sphere packing densities by looking at lower-dimensional $\mathcal{O}$-lattices.
    - Construct series of laminated $\mathcal{O}$-lattices for in $\mathbb{C}^n$

Computing Needs

- Construct lattices using one of the four methods given.

Computing Needs

- Construct lattices using one of the four methods given.
- Compute minimal vectors, lattice norm and determinant, packing density, and covering radius.

Computing Needs

- Construct lattices using one of the four methods given.
- Compute minimal vectors, lattice norm and determinant, packing density, and covering radius.
- Compute an LLL-reduced basis (A basis of relatively short vectors).

Computing Needs

- Construct lattices using one of the four methods given.
- Compute minimal vectors, lattice norm and determinant, packing density, and covering radius.
- Compute an LLL-reduced basis (A basis of relatively short vectors).
- Work with $\mathcal{O}$-lattices while using basis vectors in $\mathbb{C}^n$ or $\mathbb{H}^n$.

Computing Needs

- Construct lattices using one of the four methods given.
- Compute minimal vectors, lattice norm and determinant, packing density, and covering radius.
- Compute an LLL-reduced basis (A basis of relatively short vectors).
- Work with $\mathcal{O}$-lattices while using basis vectors in $\mathbb{C}^n$ or $\mathbb{H}^n$.
- Compute lattice automorphism groups and determine the existence of certain subgroups.

References:

1. J. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, third edition, Springer-Verlag, 1999.
2. H. Cohn and A. Kumar, *Optimality and uniqueness of the Leech lattice among lattices*, 2003.
3. W. V Ebeling, *Lattices and Codes: A course partially based on lectures by F. Hirzebruch*, Vieweg, 1994.
4. J. Martinet, *Perfect Lattices in Euclidean Space*, Springer Verlag, 2003.