Lattices

A.E. Brouwer

2002-01-17

Abstract

Some lattice stuff for the current EIDMA course.

1 Intro

For many applications one needs dense arrangements of balls in Euclidean space. Parameters to be optimized are e.g. packing density, covering density, kissing number (the number of balls that touch a given ball). Just as in coding theory, where the best codes sometimes are nonlinear but most of the theory concerns the linear case, here the best arrangements sometimes are non-lattice, but most of the theory concerns lattice arrangements.

2 Lattices

Lattice

A lattice $\Lambda$ is a discrete additive subgroup of $\mathbb{R}^n$. Equivalently, it is a finitely generated free $\mathbb{Z}$-module with positive definite symmetric bilinear form.

Basis

Assume that our lattice $\Lambda$ has dimension $n$, i.e., spans $\mathbb{R}^n$. Let $\{a_1, ..., a_n\}$ be a $\mathbb{Z}$-basis of $\Lambda$. Let $A$ be the matrix with the vectors $a_i$ as rows. If we choose a different $\mathbb{Z}$-basis $\{b_1, ..., b_n\}$, so that $b_i = \sum s_{ij} a_j$, and $B$ is the matrix with the vectors $b_i$ as rows, then $B = SA$, with $S = (s_{ij})$. Since $S$ is integral and invertible, it has determinant $\pm 1$. It follows that $|\det A|$ is uniquely determined by $\Lambda$, independent of the choice of basis.
Volume

$\mathbb{R}^n/\Lambda$ is an $n$-dimensional torus, compact with finite volume. Its volume is the volume of the fundamental domain, which equals $|\det A|$. If $\Lambda'$ is a sublattice of $\Lambda$, then $\text{vol}(\mathbb{R}^n/\Lambda') = \text{vol}(\mathbb{R}^n/\Lambda)|\Lambda/\Lambda'|$.

Gram matrix

Let $G$ be the matrix $(a_i, a_j)$ of inner products of basis vectors for a given basis. Then $G = AA^\top$, so $\text{vol}(\mathbb{R}^n/\Lambda) = \sqrt{\det G}$.

Dual lattice

The dual $\Lambda^*$ of a lattice $\Lambda$ is the lattice of vectors having integral inner products with all vectors in $\Lambda$: $\Lambda^* = \{x \in \mathbb{R}^n|(x, r) \in \mathbb{Z} \text{ for all } r \in \Lambda\}$.

It has a basis $\{a_1^*, ..., a_n^*\}$ defined by $(a_i^*, a_j) = \delta_{ij}$.

Now $A^*A^\top = I$, so $A^* = (A^{-1})^\top$ and $\Lambda^*$ has Gram matrix $G^* = G^{-1}$.

It follows that $\text{vol}(\mathbb{R}^n/\Lambda^*) = 1/\text{vol}(\mathbb{R}^n/\Lambda)$.

We have $\Lambda^{**} = \Lambda$.

Integral lattice

The lattice $\Lambda$ is called integral when the inner products of lattice vectors are all integral.

For an integral lattice $\Lambda$ one has $\Lambda \subseteq \Lambda^*$.

The lattice $\Lambda$ is called even when $(x, x)$ is an even integer for each $x \in \Lambda$. An even lattice is integral. An integral lattice that is not even is called odd.

Discriminant

The determinant, or discriminant, $\text{disc} \Lambda$ of a lattice $\Lambda$ is defined by $\text{disc} \Lambda = \det G$. When $\Lambda$ is integral, we have $\text{disc} \Lambda = |\Lambda^*/\Lambda|$.

A lattice is called self-dual or unimodular when $\Lambda = \Lambda^*$, i.e., when it is integral with discriminant 1. An even unimodular lattice is called Type II, the remaining unimodular lattices are called Type I.

If there is an even unimodular lattice in $\mathbb{R}^n$, then $n$ is divisible by 8. (This follows by studying the associated theta series and modular forms. See also below under Leech lattice.)
3 Examples

3.1 \( \mathbb{Z}^n \)

\[
\begin{array}{cccc}
\vdots \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\end{array}
\]

Unimodular, type I.

3.2 \( \mathbb{A}_2 \)

\[
\begin{array}{cccc}
\bullet & \bullet & \bullet & \bullet \\
\vdots \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\end{array}
\]

Basis \( \{r, s\} \). Gram matrix \( G = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \), so that \( \det G = 3 \). A fundamental region for \( \mathbb{A}_2 \) is the parallelogram on \( 0, r, s \). A fundamental region for \( \mathbb{A}^*_2 \) is the parallelogram on \( 0, p, q \). Note that the area of the former \( (\sqrt{3}) \) is thrice that of the latter \( (1/\sqrt{3}) \).

The representation of this lattice in \( \mathbb{R}^2 \) has nonintegral coordinates. It is easier to work in \( \mathbb{R}^3 \), on the hyperplane \( \sum x_i = 0 \), and choose \( r = e_1 - e_2 = (1, -1, 0), s = e_2 - e_3 = (0, 1, -1) \). Then \( \mathbb{A}_2 \) consists of the points \( (x_1, x_2, x_3) \) with \( x_i \in \mathbb{Z} \) and \( \sum x_i = 0 \). The dual lattice \( \mathbb{A}^*_2 \) consists of the points \( (x_1, x_2, x_3) \) with \( x_1 \equiv x_2 \equiv x_3 \) (mod 1) and \( \sum x_i = 0 \) (so that \( 3x_1 \in \mathbb{Z} \)). It contains for example \( p = \frac{1}{3}(2r + s) = (\frac{2}{3}, -\frac{1}{3}, -\frac{1}{3}) \).

4 Constructions

Let \( \rho : \mathbb{Z}^n \to \mathbb{2}^n \) be coordinatewise reduction mod 2. Given a binary linear code \( C \), the lattice \( \rho^{-1}(C) \) is integral, since it is contained in \( \mathbb{Z}^n \), but never unimodular, unless it is all of \( \mathbb{Z}^n \), a boring situation.

It turns out to be more useful to look at \( \frac{1}{\sqrt{3}}\rho^{-1}(C) \). This is an integral lattice when inner products of code words are even, that is, when \( C \) is self-orthogonal. If \( \dim C = k \) then \( \operatorname{vol}(\mathbb{R}^n/\rho^{-1}(C)) = 2^{n-k} \) and hence \( \operatorname{vol}(\mathbb{R}^n/\frac{1}{\sqrt{3}}\rho^{-1}(C)) = 2^{3n-k} \). In particular, \( \frac{1}{\sqrt{3}}\rho^{-1}(C) \) will be unimodular when \( C \) is self-dual, and even when \( C \) is "doubly even".
Example
Let $C$ be the $[8,4,4]$ extended Hamming code. Then $\frac{1}{\sqrt{2}}\rho^{-1}(C)$ is a unimodular 8-dimensional lattice known as $E_8$.

The code $C$ has weight enumerator $1 + 14X^4 + X^8$ (that is, has one word of weight 0, 14 words of weight 4, and one word of weight 8). It follows that the roots (vectors $r$ with $(r, r) = 2$) in this incarnation of $E_8$ are the 16 vectors $\pm \frac{1}{\sqrt{2}}(2,0,0,0,0,0,0,0)$ (with 2 in any position), and the $16 \cdot 14 = 224$ vectors $\frac{1}{\sqrt{2}}(\pm 1, \pm 1, \pm 1, 0, 0, 0, 0, 0)$ with $\pm 1$ in the nonzero positions of a weight 4 vector. Thus, there are 240 roots.

5 Root lattices

A root lattice is an integral lattice generated by roots (vectors $r$ with $(r, r) = 2$). The set of roots in a root lattice is a (reduced) root system $\Phi$, i.e., satisfies

(i) If $r \in \Phi$ and $\lambda r \in \Phi$, then $\lambda = \pm 1$.

(ii) $\Phi$ is closed under the reflection $w_r$ that sends $s$ to $s - 2\frac{(r,s)}{(r,r)}r$ for each $r \in \Phi$.

(iii) $2\frac{(r,s)}{(r,r)} \in \mathbb{Z}$.

For example, $A_2$ and $E_8$ are root lattices.

Since $\Phi$ generates $\Lambda$ and $\Phi$ is invariant under $W = \langle w_r | r \in \Phi \rangle$, the same holds for $\Lambda$, so root lattices have a large group of automorphisms.

A fundamental system of roots $\Pi$ in a root lattice $\Lambda$ is a set of roots generating $\Lambda$ and such that $(r, s) \leq 0$ for distinct $r, s \in \Pi$. A reduced fundamental system of roots is a fundamental system that is linearly independent. A non-reduced fundamental system is called extended.

For example, in $A_2$ the set $\{r, s\}$ is a reduced fundamental system, and $\{r, s, -r - s\}$ is an extended fundamental system.

The Dynkin diagram of a fundamental system $\Pi$ such that $(r, s) \neq -2$ for $r, s \in \Pi$, is the graph with vertex set $\Pi$ where $r$ and $s$ are joined by an edge when $(r, s) = -1$. (The case $(r, s) = -2$ happens only for a non-reduced system with $A_1$ component. In that case we do not define the Dynkin diagram.)

Every root lattice has a reduced fundamental system: Fix some vector $u$, not orthogonal to any root. Put $\Phi^+(u) = \{r \in \Phi | (r, u) > 0\}$ and $\Pi(u) = \{r \in \Phi^+(u) \mid r \text{ cannot be written as } s + t \text{ with } s, t \in \Phi^+(u)\}$. Then $\Pi(u)$ is
a reduced fundamental system of roots, and written on this basis each root has only positive or only negative coefficients.

(Indeed, if \( r, s \in \Pi(u) \) and \((r, s) = 1\), then say \( r - s \in \Phi^+(u) \) and \( r = (r - s) + s \), contradiction. This shows that \( \Pi(u) \) is a fundamental system. If \( \sum \gamma_r r = 0 \), then separate the \( \gamma_r \) into positive and negative ones to get \( \sum \alpha_r r = \sum \beta_s s = x \neq 0 \) where all coefficients \( \alpha_r, \beta_s \) are positive. Now \( 0 < (x, x) = \sum \alpha_r \beta_s (r, s) \leq 0 \), contradiction. This shows that \( \Pi(u) \) is reduced. Each root in \( \Phi^+(u) \) has an expression over \( \Pi(u) \) with only positive coefficients.)

Proposition 5.1 Let \( \Pi \) be a reduced fundamental system.

(i) For all \( x \in \mathbb{R}^n \) there is a \( w \in W \) such that \( (w(x), r) \geq 0 \) for all \( r \in \Pi \).

(ii) \( \Pi = \Pi(u) \) for some \( u \). (That is, \( W \) is transitive on reduced fundamental systems.)

(iii) If \( \Lambda \) is irreducible (not an orthogonal direct sum), then there is a unique \( \tilde{r} \in \Phi \) such that \( \Pi \cup \{\tilde{r}\} \) is an extended fundamental system.

Proof: (i) Let \( G \) be the Gram matrix of \( \Pi \), and write \( A = 2I - G \). Since \( G \) is positive definite, \( A \) has largest eigenvalue less than 2. Using Perron-Frobenius, let \( \gamma = (\gamma_r)_{r \in \Pi} \) be a positive eigenvector of \( A \). If \( (x, s) < 0 \) for some \( s \in \Pi \), then put \( x' = w_s(x) = x - (x, s)s \). Now \( (x', \sum \gamma_r r) = (x, \sum \gamma_r r) - (G\gamma)_s(x, s) > (x, \sum \gamma_r r) \).

But \( W \) is finite, so after finitely many steps we reach the desired conclusion.

(ii) Induction on \( |\Pi| \). Fix \( x \) with \( (x, r) \geq 0 \) for all \( r \in \Pi \). Then \( \Pi_0 = \Pi \cap x^\perp \) is a fundamental system of a lattice in a lower-dimensional space, so of the form \( \Pi_0 = \Pi_0(u_0) \). Take \( u = x + \epsilon u_0 \) for small \( \epsilon > 0 \). Then \( \Pi = \Pi(u) \).

(iii) If \( r \in \Phi^+(u) \) has maximal \( (r, u) \), then \( \tilde{r} = -r \) is the unique root that can be added. It can be added, since \( (\tilde{r}, s) \geq 0 \) means \( (r, s) < 0 \), so that \( r + s \) is a root, contradicting maximality of \( r \). And it is unique because linear dependencies of an extended system correspond to an eigenvector with eigenvalue 2 of the extended Dynkin diagram, and by Perron-Frobenius up to a constant there is a unique such eigenvector when the diagram is connected, that is, when \( \Lambda \) is irreducible.

The examples

The irreducible root lattices one finds are \( A_n \) \((n \geq 0)\), \( D_n \) \((n \geq 4)\), \( E_6 \), \( E_7 \), \( E_8 \). Each is defined by its Dynkin diagram.
(1) $A_n$: The lattice vectors are: $x \in \mathbb{Z}^{n+1}$ with $\sum x_i = 0$. There are $n(n+1)$ roots: $e_i - e_j$ ($i \neq j$). The discriminant is $n+1$, and $A^*_n/A_n \cong \mathbb{Z}_{n+1}$, with the quotient generated by $\frac{1}{n+1}(e_1 + ... + e_n - ne_{n+1}) \in A^*_n$.

(2) $D_n$: The lattice vectors are: $x \in \mathbb{Z}^{n}$ with $\sum x_i \equiv 0 \pmod{2}$. There are $2n(n-1)$ roots $\pm e_i \pm e_j$ ($i \neq j$). The discriminant is 4, and $D^*_n/D_n$ is isomorphic to $\mathbb{Z}_4$ when $n$ is odd, and to $\mathbb{Z}_2 \times \mathbb{Z}_2$ when $n$ is even. $D^*_n$ contains $e_1$ and $\frac{1}{2}(e_1 + ... + e_n)$. Note that $D_3 \cong A_3$.

(3) $E_8$: (Recall that we already gave a construction of $E_8$ from the Hamming code.) The lattice is the span of $D_8$ and $c := \frac{1}{2}(e_1 + ... + e_8)$. There are $240 = 112 + 128$ roots, of the forms $\pm e_i \pm e_j$ ($i \neq j$) and $\frac{1}{2}(\pm e_1 \pm ... \pm e_8)$ with an even number of minus signs. The discriminant is 1, and $E_8^* = E_8$.

(4) $E_7$: Take $E_7 = E_8 \cap c^\perp$. There are $126 = 56 + 70$ roots. The discriminant is 2, and $E_7^*$ contains $\frac{1}{4}(1, 1, 1, 1, 1, 1, 3, -3)$.

(5) $E_6$: For the vector $d = -e_7 - e_8$, take $E_6 = E_8 \cap \{c, d\}^\perp$. There are $72 = 32 + 40$ roots. The discriminant is 3, and $E_6^*$ contains the vector $\frac{1}{3}(1, 1, 1, -2, -2, 0, 0)$.
That this is all, is an easy consequence of the Perron-Frobenius theorem: $A = 2I - G$ is the adjacency matrix of a graph, namely the Dynkin diagram, and it is easy to classify the connected graphs with largest eigenvalue less than 2—they are the Dynkin diagrams of reduced fundamental systems of irreducible root systems—and the connected graphs with largest eigenvalue 2—they are the Dynkin diagrams of extended root systems.

6 The Leech lattice

**Theorem 6.1** There exists a unique even unimodular lattice without roots in $\mathbb{R}^{24}$. It has 196560 vectors of weight 4.

Construction: a spanning set consists of the vectors $\frac{1}{\sqrt{8}}(\mp 3, \pm 1^{23})$ with $\mp 3$ in any position, and the upper signs in a code word of the extended binary Golay code.

For the vectors of weight 4 one finds the shapes $4^2 0^{22}, 3^1 2^{23}, 2^8 0^{16}$ (omitting the $\frac{1}{\sqrt{8}}$) with frequencies $2^2 \binom{24}{2}, 2^{12} 24$ and $2^7 759$, respectively.

Uniqueness is proved using $\theta$-functions and the theory of modular forms. Given a lattice $\Lambda$, define

$$\theta_\Lambda(z) = \sum_{x \in \Lambda} q^{\frac{1}{2}(x,x)}$$

where $q = e^{2\pi iz}$ and $\text{Im}(z) > 0$.

One has

$$\theta_{\Lambda^*}(z) = \det(\Lambda)^{\frac{1}{2}} \left( \frac{i}{z} \right)^{\frac{n}{2}} \theta_\Lambda(-\frac{1}{z}).$$

Here the Leech lattice has $\Lambda = \Lambda^*$ and $\det(\Lambda) = 1$, so that $\theta_\Lambda(z)$ is a modular form of weight 12.

The space of modular forms of weight 12 has dimension 2, and the two conditions: unique vector of norm 0, no vectors of norm 2, determine $\theta_\Lambda(z)$
uniquely. Thus, any even unimodular lattice without roots in $\mathbb{R}^{24}$ must have the same weight enumerator as the Leech lattice.

Some more work gives the desired conclusion.

7 The Barnes-Wall lattice

Take the first order Reed-Muller code $C$ of length 16. This is a binary linear $[16,5,8]$ code, with weight enumerator $1 + 30x^8 + x^{16}$.

Define the Barnes-Wall lattice $\Lambda_{16}$ by:

$$\frac{1}{\sqrt{2}}x \in \Lambda_{16} \text{ iff } x \mod 2 \in C \text{ and } \sum x_i \equiv 0 \pmod{4}.$$ 

This is a lattice of determinant $2^8$ and minimum norm 4. The kissing number equals $\tau = 4320$ (namely, 480 vectors of shape $\frac{1}{\sqrt{2}}(\pm 2^2, 0)$ and 3840 vectors of shape $\frac{1}{\sqrt{2}}(\pm 8, 0)$ with the 1’s at the positions of a code word.

(This type of construction is especially useful when $d = 8$, since two shapes contribute to the kissing number. For larger $n$ chains of binary codes are used to place the 1’s, 2’s, 4’s, etc.)

8 The Coxeter-Todd lattice

Let $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ be a cube root of unity, and put $\theta = \omega - \bar{\omega} = \sqrt{3}$. Let $\Lambda$ be the 6-dimensional $\mathbb{Z}[\omega]$-lattice spanned by the six vectors $(4,0,0,0,0,0)$, $(2,2,0,0,0,0)$, $(2,0,2,0,0,0)$, $(2,0,0,2,0,0)$, $(2,0,0,0,2,0)$, $(\theta,1,1,1,1,1)$, provided with the positive definite inner product $(u,v) = u^\top \bar{v}$. Since $\theta = 2\omega + 1$ all inner products are divisible by 4, and we see that $\frac{1}{2}\Lambda$ is a unimodular lattice $\mathbb{Z}[\omega]$-lattice.

This definition looks asymmetric, but in fact the group is large: the automorphism group of the 6-dimensional $\mathbb{Z}[\omega]$-lattice is $6.\text{U}_4(3).2$ of order $2^9.3^2.5.7$, inducing the symmetric group $\text{Sym}(6)$ on the coordinate positions.

This 6-dimensional $\mathbb{Z}[\omega]$-lattice $\Lambda$ is a 12-dimensional $\mathbb{Z}$-lattice. If the complex lattice has coordinate positions $e_h$ ($1 \leq h \leq 6$), then we can take 12 coordinate positions $e_h$, $ie_h$ for the real lattice, and given a $\mathbb{Z}[\omega]$-basis with vectors $u_j$, we find a $\mathbb{Z}$-basis with vectors $u_j$, $(\omega - 1)u_j$. A diagonal 2 now becomes $\left( \begin{array}{c} 2 \\ -3 \sqrt{3} \end{array} \right)$. Consequently, $K_{12} := \frac{1}{\sqrt{2}}\Lambda$ is an integral lattice with determinant $3^6$. (One checks that $(a + bi)(c - di) = ac + bd + (bc - ad)i$ and $(a,b), (c,d) = ac + bd$ so that the real inner product is the real part of the complex inner product. Since $\text{Re}(\omega) = -\frac{1}{2}$, we need an extra factor 2 to guarantee that the inner product is integral.)
The dual $K_{12}^*$ is spanned by the six vectors $\frac{1}{\sqrt{2}} u_j$ and the six vectors $\frac{1}{3\sqrt{2}} (\omega - 1) u_j$. (Thus, $K_{12}^* / K_{12}$ can be regarded as a 6-dimensional vector space over $GF(3)$.)

The minimum norm is 4, and the kissing number is 756. (Indeed, there are $32 \cdot 6 \cdot 3 = 576$ vectors of the form $\frac{1}{\sqrt{2}} \omega^j (\pm \theta, \pm 1, \ldots, \pm 1)$ with an even number of minus signs, the $\pm \theta$ in any position, and $j = 0, 1, 2$, and also $15 \cdot 4 \cdot 3 = 180$ vectors of the form $\frac{1}{\sqrt{2}} \omega^j (\pm 2, \pm 2, 0, 0, 0)$ with the $\pm 2$ in any positions.)

There are many equivalent descriptions. A short one: take the vectors $u + \omega \theta v$, with $u \in E_6$ and $v \in E_6^*$.  

## 9 Records

We quote a table from Conway & Sloane giving the best lattices known in low dimensional spaces.

<table>
<thead>
<tr>
<th>dimension</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>12</th>
<th>16</th>
<th>24</th>
</tr>
</thead>
<tbody>
<tr>
<td>densest packing</td>
<td>$\mathbb{Z}$</td>
<td>$A_2$</td>
<td>$A_3$</td>
<td>$D_4$</td>
<td>$D_5$</td>
<td>$E_6$</td>
<td>$E_7$</td>
<td>$E_8$</td>
<td>$K_{12}$</td>
<td>$\Lambda_{16}$</td>
<td>$\Lambda_{24}$</td>
</tr>
<tr>
<td>highest kissing number</td>
<td>$\mathbb{Z}$</td>
<td>$A_2$</td>
<td>$A_3$</td>
<td>$D_4$</td>
<td>$D_5$</td>
<td>$E_6$</td>
<td>$E_7$</td>
<td>$E_8$</td>
<td>$P_{12a}$</td>
<td>$\Lambda_{16}$</td>
<td>$\Lambda_{24}$</td>
</tr>
<tr>
<td>thinnest covering</td>
<td>2</td>
<td>6</td>
<td>12</td>
<td>24</td>
<td>40</td>
<td>72</td>
<td>126</td>
<td>240</td>
<td>840</td>
<td>4320</td>
<td>196560</td>
</tr>
<tr>
<td>best quantizer</td>
<td>$\mathbb{Z}$</td>
<td>$A_2$</td>
<td>$A_3^*$</td>
<td>$A_4^*$</td>
<td>$A_5^*$</td>
<td>$A_6^*$</td>
<td>$A_7^*$</td>
<td>$A_8^*$</td>
<td>$A_{12}^*$</td>
<td>$A_{16}^*$</td>
<td>$\Lambda_{24}$</td>
</tr>
</tbody>
</table>

Here $K_{12}$ is the Coxeter-Todd lattice, $\Lambda_{16}$ is the Barnes-Wall lattice, $\Lambda_{24}$ is the Leech lattice, and $P_{12a}$ is a certain non-lattice packing.