Lattice - Introduction

Tomáš Kobrle

23. March 2012

Lattice

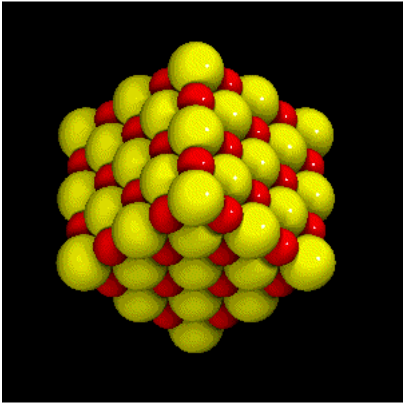

Figure: Lattice of NaCl

Definition of Lattice

Definition

A lattice is set points

$$L(v_1 \ldots v_n) = \left\{ v_1 a_1 + \ldots + v_n a_n \mid a_i \in \mathbb{Z} \; \forall i \in \{1, \ldots, n\} \right\},$$

where $v_1, \ldots, v_n$ *are linearly independant vectors in* $\mathbb{R}^m$. *These vector are called a basis of* L.

Definition of Lattice

Definition

A lattice is set points

$$L(v_1 \dots v_n) = \{v_1 a_1 + \dots + v_n a_n \mid a_i \in \mathbb{Z}\ \forall i \in \{1, \dots, n\}\},$$

where $v_1, \dots, v_n$ *are linearly independant vectors in* $\mathbb{R}^m$. *These vector are called a basis of* L.

If we define B as the $m \times n$ matrix with columns $v_1, \dots, v_n$, then we can write

$$L(v_1 \dots v_n) = L(B) = \{By \mid y \in \mathbb{Z}^n\}$$

Rank of lattice is n and dimension is m. If $m = n$ then the lattice is called full-rank.

Basis

Basis of lattice is not unique:

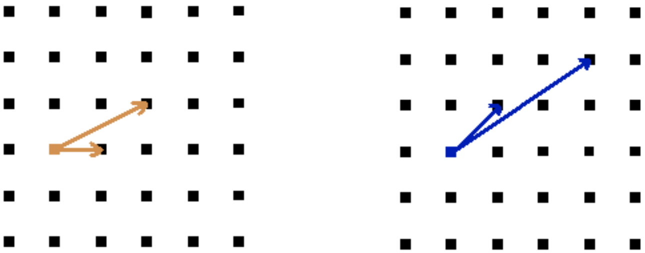

Figure: Two bases of the same lattices in $\mathbb{R}^2$

But not every n-tuple of vectors in $\mathbb{R}^n$ generate same lattice:

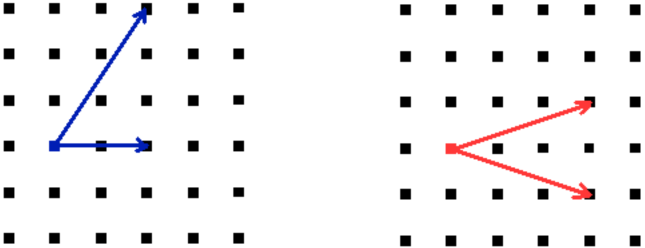

Figure: Two bases of different lattices in $\mathbb{R}^2$

Equivalency of lattices

A matrix $A \in \mathbb{Z}^{n \times n}$ is called unimodular if $det(A) = \pm 1$.

Remark

If matrix U is unimodular then U^{-1} is unimodular and $U^{-1} \in \mathbb{Z}^{n \times n}$

Equivalency of lattices

A matrix $A \in \mathbb{Z}^{n \times n}$ is called unimodular if $det(A) = \pm 1$.

Remark

If matrix U is unimodular then U^{-1} is unimodular and $U^{-1} \in \mathbb{Z}^{n \times n}$

Lemma

Two lattices $L(B_1), L(B_2)$ are the same if and only if there exists unimodular matrix U such that $B_1 = B_2 U$.

Proof of Equivalency

Since $L(B_1) = L(B_2)$, there exists matrix $U \in \mathbb{Z}^{n \times n}$ that $B_1 = B_2 U$. Similarly, there exist matrix $V \in \mathbb{Z}^{n \times n}$ such that $B_2 = B_1 V$.
Hence $B_2 = B_1 V = B_2 UV$, and we get $B_2^T B_2 = V^T U^T B_2^T B_2 UV$.
Taking determinants:

$$det(B_2^T B_2) = det(VU)^2 det(B_2^T B_2)$$

Hence $det(U)det(V) = \pm 1$ and since both matrices have integer $det(U) = \pm 1$, as required. $\square$
Assuming $B_1 = B_2 U$ for unimodular matrix U implies directly $L(B_1) \subseteq L(B_2)$. From remark we obtain that U^{-1} is unimodular too, so $B_1 U^{-1} = B_2$ implies $L(B_1) \supseteq L(B_2)$.
We get $L(B_1) = L(B_2)$. $\square$

Fundametal parallelepiped

Definition

A fundamental parallelepiped for lattice $L(B)$ is defined as

$$P(B) = \{Bx \mid x \in [0,1)^n\}.$$

We define determinant of lattice $detL(B) = |det(B)|$.

Fundametal parallelepiped

Definition

A fundamental parallelepiped for lattice $L(B)$ is defined as

$$P(B) = \{Bx \mid x \in [0,1)^n\}.$$

We define determinant of lattice $detL(B) = |det(B)|$.

Remark

The value of determinat is the volume of the fundamental parallelepiped.

From previous lemma we easily get that two lattice $L(B_1), L(B_2)$ are the same if and only if $detL(B_1) = detL(B_2)$.

Succesive minimum

Another parameter of lattice is the lenght of the shortest nonzero vector in the lattice. We denote this lenght by $\lambda_1(L)$. By lenght we mean Euclidean norm defined as

$$\|x\| = \sqrt{\sum_{i=1}^{n} x_i^2}.$$

More generally:

Definition

For lattice L of rank n and for $k \leq n$ k-th succesive minimum $\lambda_k(L)$ is defined as the smallest radius of closed ball around zero contains k linearly independant vectors in lattice L.

Blichfeldt's Theorem

Theorem

For lattice L and set $S \subseteq \mathbb{R}^n$ with $vol(S) > detL$ there exist nonequal points $z_1, z_2 \in S$ such that $z_1 - z_2 \in L$.

Blichfeldt's Theorem

Theorem

For lattice L and set $S \subseteq \mathbb{R}^n$ with $vol(S) > detL$ there exist nonequal points $z_1, z_2 \in S$ such that $z_1 - z_2 \in L$.

Proof: Let B is some basis of L. The sets $x + P(B)$ for $x \in L$ form a partition of $\mathbb{R}^n$.
For every $x \in L$ we define $S_x = S \cap (x + P(B))$.
Now we define $S_x^* = S_x - x$. Then $S_x^* \subseteq P(B)$ and because

$$\sum_{x \in L} vol(S_x^*) = \sum_{x \in L} vol(S_x) = vol(S) \geq detL = vol(P(B))$$

there are x, y in L, $x \neq y$, that $S_x^* \cap S_y^* \neq \emptyset$. Let z be a point $S_x^* \cap S_y^*$. Then $z + x \in S_x \subseteq S$ and $z + y \in S_y \subseteq S$ and $0 \neq (x + z) - (y + z) = x - y \in L$. $\square$

Minkowski's Theorem I.

Set $S \in \mathbb{R}^n$ is centrally-symetric if $x \in S \Rightarrow -x \in S$
Set $S \in \mathbb{R}^n$ is convex if for any $x, y \in S$ and $\lambda \in [0, 1]$

$$\lambda x + (1 - \lambda) y \in S$$

Theorem

Let L be lattice and S central symetric convex set in $\mathbb{R}^n$*. If* $vol(S) > 2^n \cdot detL$ *then set S contains a nonzero lattice point.*

Minkowski's Theorem I.

Set $S \in \mathbb{R}^n$ is centrally-symetric if $x \in S \Rightarrow -x \in S$
Set $S \in \mathbb{R}^n$ is convex if for any $x, y \in S$ and $\lambda \in [0,1]$

$$\lambda x + (1-\lambda)y \in S$$

Theorem

Let L be lattice and S central symetric convex set in $\mathbb{R}^n$*. If* $vol(S) > 2^n \cdot detL$ *then set S contains a nonzero lattice point.*

Proof

Define $S^* = \frac{1}{2}S = \{x \mid 2x \in S\}$*. Then* $vol(S^*) > detL$*.*
By Blichfeldt's theorem there exist $z_1, z_2 \in S^*$ *such that* $0 \neq z_1 - z_2 \in L$*.*
By properties of S $\frac{2z_1 - 2z_2}{2} = z_1 - z_2 \in S$*, as required.* $\square$

Minkowski's Theorem II.

Remark

Let $B(0, r)$ *denote open ball of radius* r *in* $\mathbb{R}^n$ *then*

$$vol(B(0, r)) \geq \left(\frac{2r}{\sqrt{n}}\right)^n$$

Theorem

Let L *be lattice of rank* n *then* $\lambda_1(L) \leq \sqrt{n}(det(L))^{1/n}$

Proof of Minkowski's theorem

Proof

By definition of λ_1, $B(0,\lambda_1(L))$ contains no nonzero lattice point. From previous theorem and remark we get

$$2^n detL \geq vol(B(0,\lambda_1(L))) \geq \left(\frac{2\lambda_1(L)}{\sqrt{n}}\right)^n.$$

By rearranging

$$\sqrt{n}(det(L))^{1/n} \geq \lambda_1(L). \quad \square$$

Easy Computational problems

Membership: Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ and a point $v \in \mathbb{Z}^m$, decide if $v \in L(B)$.
This problem is equivalent to question if system of m linear equation $Bx = v$ has solution in $\mathbb{Z}^n$. Solving by Gauss elimination.

Easy Computational problems

Membership: Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ and a point $v \in \mathbb{Z}^m$, decide if $v \in L(B)$.
This problem is equivalent to question if system of m linear equation $Bx = v$ has solution in $\mathbb{Z}^n$. Solving by Gauss elimination.

Equivalence: Given $B_1, B_2 \in \mathbb{Z}^{m \times n}$, decide if $L(B_1) = L(B_2)$.
If m=n we can use lemma about equivalency and compute and compare determinants of B_1 and B_2. Otherwise we can use membership problem for all columns of B_1 and matrix (basis) B_2 and then for all columns of B_2 and matrix B_1.

The Shortest Vector Problem - SVP

Search SVP: Given a basis B of lattice L find a vector $v \in L(B)$ such that $\|v\| = \lambda_1(L(B))$.

Optimization SVP: Given a basis B find $\lambda_1(L(B))$.

Decisional SVP: Given a basis B and rational r, determine if $\lambda_1(L(B)) \leq r$ or not.

Aproxiamtion variants of SVP

For $\gamma \geq 1$ we define following problems:

Search SVP: Given a basis B of lattice L find a nonzero vector $v \in L(B)$ such that $\|v\| \leq \gamma \cdot \lambda_1(L(B))$.

Optimization SVP$_\gamma$: Given a basis B find such d that $d \leq \lambda_1(L(B)) \leq d \cdot \gamma$.

Promise SVP$_\gamma$: Given a basis B and rational r, determine if $\lambda_1(L(B)) \leq r$ or $\lambda_1(L(B)) < r \cdot \gamma$.

Aproxiamtion variants of SVP

For $\gamma \geq 1$ we define following problems:

Search SVP: Given a basis B of lattice L find a nonzero vector $v \in L(B)$ such that $\|v\| \leq \gamma \cdot \lambda_1(L(B))$.

Optimization SVP$_\gamma$: Given a basis B find such d that $d \leq \lambda_1(L(B)) \leq d \cdot \gamma$.

Promise SVP$_\gamma$: Given a basis B and rational r, determine if $\lambda_1(L(B)) \leq r$ or $\lambda_1(L(B)) < r \cdot \gamma$.

Open question: Is the search variant harder than optimization variant ?

The Shortest Independant Vector Problem - SIVP

For $\gamma \geq 1$:

SIVP$_\gamma$: Given a basis B find n linearly independant vectors in $L(B)$ of lenght $\leq \gamma \cdot \lambda_n(L(B))$.

The Closest vector problem - CVP

For parameter $\gamma \geq 1$ we define:

Search CVP$_\gamma$: Given a lattice basis B and a vector $t \in \mathbb{Z}^n$, find $v \in L(B)$ such that $\|v - t\| \leq \gamma \cdot dist(t, L(B))$.

Optimization CVP$_\gamma$: Given a lattice basis B and a vector $t \in \mathbb{Z}^n$, find d such that $d \leq dist(t, (L(B)) \leq d \cdot \gamma$.

Promise CVP$_\gamma$: Given a lattice basis B and a vector $t \in \mathbb{Z}^n$ and rational r, determine if $dist(t, (L(B)) \leq r$ or $dist(t, (L(B)) < r \cdot \gamma$.

Facts about complexity

Genaral SVP and CVP are NP-hard problem.

Aproxiamating problems are probably not *NP*-hard but the best algorithm runs in exponential time even more there is no better quantum algorithm, which means that cryptosystems based on aproxiamting SVP or CVP are great promise for post-quantum cryptography.

Promise CVP$_\gamma$ and SVP$_\gamma$ are known as GapCVP$_\gamma$ respective GapSVP$_\gamma$. Both these problems are in $NP \cap coNP$ for $\gamma \approx c\sqrt{n}$ where c is some constant.

Cryptosystems based on lattices

- GGH encryption / signature scheme
- NTRUEncrypt and NTRUSign

End of prezentation

Thank you for your attention