September 14-20, 2015

Ulaanbaatar (Mongolia)
School of Mathematatic and Computer Science,
National University of Mongolia.

Lattice Cryptography

Michel Waldschmidt

Institut de Mathématiques de Jussieu — Paris VI
http://webusers.imj-prg.fr/~michel.waldschmidt/

SEAMS School 2015

"Number Theory and Applications in Cryptography and Coding Theory"

University of Science, Ho Chi Minh, Vietnam

August 31 - September 08, 2015

Course on **Lattices and Applications** by

Dung Duong, University of Bielefeld,
Khuong A. Nguyen, HCMUT, VNU-HCM
Ha Tran, Aalto University

Slides :

http://www.math.uni-bielefeld.de/~dhoang/seams15/

CIMPA-ICTP School 2016

Lattices and application to
cryptography and coding theory
CIMPA-ICTP-VIETNAM
Research School co-sponsored with ICTP
Ho Chi Minh, August 1-12, 2016

http://www.cimpa-icpam.org/

http://ricerca.mat.uniroma3.it/users/valerio/hochiminh16.html

Applications : http://students.cimpa.info/login

Main references

- Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman : *An introduction to mathematical cryptography.* Springer Undergraduate Texts in Mathematics, 2008. Second ed. 2014.

- Wade Trappe and Lawrence C. Washington : *Introduction to Cryptography with Coding Theory.* Pearson Prentice Hall, 2006.
  http://en.bookfi.org/book/1470907

Further references

- A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovacz : *Factoring Polynomials with Rational Coefficients*. Math Annalen **261** (1982) 515–534.
- Daniele Micciancio & Oded Regev : *Lattice-based Cryptography* (2008).
  http://www.cims.nyu.edu/~regev/papers/pqc.pdf
- Joachim von zur Gathen & Jürgen Gerhard. *Modern Computer Algebra.* Cambridge University Press, Cambridge, UK, Third edition (2013).
  https://cosec.bit.uni-bonn.de/science/mca/
- Abderrahmane Nitaj : *Applications de l'algorithme LLL en cryptographie* . Informal notes.
  http://math.unicaen.fr/~nitaj/LLLapplic.pdf

Subgroups of $\mathbf{R}^n$

Examples

Finitely generated or not, finite rank or not

discrete or not, dense or not, closed or not

Classification of closed subgroups of $\mathbf{R}$

Classification of closed subgroups of $\mathbf{R}^2$, of $\mathbf{R}^n$

Subgroups of $\mathbf{R}^n$

Examples

Finitely generated or not, finite rank or not

discrete or not, dense or not, closed or not

Classification of closed subgroups of $\mathbf{R}$

Classification of closed subgroups of $\mathbf{R}^2$, of $\mathbf{R}^n$

Subgroups of $\mathbf{R}^n$

Examples

Finitely generated or not, finite rank or not

discrete or not, dense or not, closed or not

Classification of closed subgroups of $\mathbf{R}$

Classification of closed subgroups of $\mathbf{R}^2$, of $\mathbf{R}^n$

Subgroups of $\mathbf{R}^n$

Examples

Finitely generated or not, finite rank or not

discrete or not, dense or not, closed or not

Classification of closed subgroups of $\mathbf{R}$

Classification of closed subgroups of $\mathbf{R}^2$, of $\mathbf{R}^n$

Subgroups of $\mathbf{R}^n$

Examples

Finitely generated or not, finite rank or not

discrete or not, dense or not, closed or not

Classification of closed subgroups of $\mathbf{R}$

Classification of closed subgroups of $\mathbf{R}^2$, of $\mathbf{R}^n$

Quotient of $\mathbf{R}^n$ by a discrete subgroup

Additive group : $\mathbf{C}$

Multiplicative group : $\mathbf{C}^\times$

$$\mathbf{R}/\mathbf{Z} \simeq \mathbf{U} \qquad \mathbf{R} \longrightarrow \mathbf{U} \qquad t \longmapsto e^{2i\pi t}$$

$$\mathbf{C}/\mathbf{Z} \simeq \mathbf{C}^\times \qquad \mathbf{C} \longrightarrow \mathbf{C}^\times \qquad z \longmapsto e^{2i\pi z}$$

Elliptic curve : $\mathbf{C}/L$ $\qquad$ $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ lattice in $\mathbf{C} \simeq \mathbf{R}^2$

Abelian variety : $\mathbf{C}^g/L$ $\qquad$ L lattice in $\mathbf{C}^g \simeq \mathbf{R}^{2g}$

Commutative algebraic groups over $\mathbf{C}$.

Quotient of $\mathbf{R}^n$ by a discrete subgroup

Additive group : $\mathbf{C}$

Multiplicative group : $\mathbf{C}^\times$

$$\mathbf{R}/\mathbf{Z} \simeq \mathbf{U} \qquad \mathbf{R} \longrightarrow \mathbf{U} \qquad t \longmapsto e^{2i\pi t}$$

$$\mathbf{C}/\mathbf{Z} \simeq \mathbf{C}^\times \qquad \mathbf{C} \longrightarrow \mathbf{C}^\times \qquad z \longmapsto e^{2i\pi z}$$

Elliptic curve : $\mathbf{C}/L$ $\quad L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ lattice in $\mathbf{C} \simeq \mathbf{R}^2$

Abelian variety : $\mathbf{C}^g/L$ $\quad L$ lattice in $\mathbf{C}^g \simeq \mathbf{R}^{2g}$

Commutative algebraic groups over $\mathbf{C}$.

Quotient of $\mathbf{R}^n$ by a discrete subgroup

Additive group : $\mathbf{C}$

Multiplicative group : $\mathbf{C}^\times$

$$\mathbf{R}/\mathbf{Z} \simeq \mathbf{U} \qquad \mathbf{R} \longrightarrow \mathbf{U} \qquad t \longmapsto e^{2i\pi t}$$

$$\mathbf{C}/\mathbf{Z} \simeq \mathbf{C}^\times \qquad \mathbf{C} \longrightarrow \mathbf{C}^\times \qquad z \longmapsto e^{2i\pi z}$$

Elliptic curve : $\mathbf{C}/L$ $\qquad L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ lattice in $\mathbf{C} \simeq \mathbf{R}^2$

Abelian variety : $\mathbf{C}^g/L$ $\qquad L$ lattice in $\mathbf{C}^g \simeq \mathbf{R}^{2g}$

Commutative algebraic groups over $\mathbf{C}$.

Quotient of $\mathbf{R}^n$ by a discrete subgroup

Additive group : $\mathbf{C}$

Multiplicative group : $\mathbf{C}^\times$

$$\mathbf{R}/\mathbf{Z} \simeq \mathbf{U} \qquad \mathbf{R} \longrightarrow \mathbf{U} \qquad t \longmapsto e^{2i\pi t}$$

$$\mathbf{C}/\mathbf{Z} \simeq \mathbf{C}^\times \qquad \mathbf{C} \longrightarrow \mathbf{C}^\times \qquad z \longmapsto e^{2i\pi z}$$

Elliptic curve : $\mathbf{C}/L$ $\qquad L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ lattice in $\mathbf{C} \simeq \mathbf{R}^2$

Abelian variety : $\mathbf{C}^g/L$ $\qquad L$ lattice in $\mathbf{C}^g \simeq \mathbf{R}^{2g}$

Commutative algebraic groups over $\mathbf{C}$.

Quotient of $\mathbf{R}^n$ by a discrete subgroup

Additive group : $\mathbf{C}$

Multiplicative group : $\mathbf{C}^\times$

$$\mathbf{R}/\mathbf{Z} \simeq \mathbf{U} \qquad \mathbf{R} \longrightarrow \mathbf{U} \qquad t \longmapsto e^{2i\pi t}$$

$$\mathbf{C}/\mathbf{Z} \simeq \mathbf{C}^\times \qquad \mathbf{C} \longrightarrow \mathbf{C}^\times \qquad z \longmapsto e^{2i\pi z}$$

Elliptic curve : $\mathbf{C}/L$ $\qquad L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ lattice in $\mathbf{C} \simeq \mathbf{R}^2$

Abelian variety : $\mathbf{C}^g/L$ $\qquad L$ lattice in $\mathbf{C}^g \simeq \mathbf{R}^{2g}$

Commutative algebraic groups over $\mathbf{C}$.

Quotient of $\mathbf{R}^n$ by a discrete subgroup

Additive group : $\mathbf{C}$

Multiplicative group : $\mathbf{C}^\times$

$$\mathbf{R}/\mathbf{Z} \simeq \mathbf{U} \qquad \mathbf{R} \longrightarrow \mathbf{U} \qquad t \longmapsto e^{2i\pi t}$$

$$\mathbf{C}/\mathbf{Z} \simeq \mathbf{C}^\times \qquad \mathbf{C} \longrightarrow \mathbf{C}^\times \qquad z \longmapsto e^{2i\pi z}$$

Elliptic curve : $\mathbf{C}/L$ $\qquad$ $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ lattice in $\mathbf{C} \simeq \mathbf{R}^2$

Abelian variety : $\mathbf{C}^g/L$ $\qquad$ L lattice in $\mathbf{C}^g \simeq \mathbf{R}^{2g}$

Commutative algebraic groups over $\mathbf{C}$.

Quotient of $\mathbf{R}^n$ by a discrete subgroup

Additive group : $\mathbf{C}$

Multiplicative group : $\mathbf{C}^\times$

$$\mathbf{R}/\mathbf{Z} \simeq \mathbf{U} \qquad \mathbf{R} \longrightarrow \mathbf{U} \qquad t \longmapsto e^{2i\pi t}$$

$$\mathbf{C}/\mathbf{Z} \simeq \mathbf{C}^\times \qquad \mathbf{C} \longrightarrow \mathbf{C}^\times \qquad z \longmapsto e^{2i\pi z}$$

Elliptic curve : $\mathbf{C}/L$ $\qquad L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ lattice in $\mathbf{C} \simeq \mathbf{R}^2$

Abelian variety : $\mathbf{C}^g/L$ $\qquad L$ lattice in $\mathbf{C}^g \simeq \mathbf{R}^{2g}$

Commutative algebraic groups over $\mathbf{C}$.

Some acronymes

DES : Data Encryption Standard (1977)

AES : Advanced Encryption Standard (2000)

RSA : Rivest, Shamir, Adelman (1978)

LLL : Lenstra, Lenstra, Lovacz (1982)

SVP : Shortest Vector Problem (and approximate versions)

CVP : Closest Vector Problem (and approximate versions)

SBP : Shortest Basis Problem (and approximate versions)

Some acronymes

DES : Data Encryption Standard (1977)

AES : Advanced Encryption Standard (2000)

RSA : Rivest, Shamir, Adelman (1978)

LLL : Lenstra, Lenstra, Lovacz (1982)

SVP : Shortest Vector Problem (and approximate versions)

CVP : Closest Vector Problem (and approximate versions)

SBP : Shortest Basis Problem (and approximate versions)

Some acronymes

DES : Data Encryption Standard (1977)

AES : Advanced Encryption Standard (2000)

RSA : Rivest, Shamir, Adelman (1978)

LLL : Lenstra, Lenstra, Lovacz (1982)

SVP : Shortest Vector Problem (and approximate versions)

CVP : Closest Vector Problem (and approximate versions)

SBP : Shortest Basis Problem (and approximate versions)

Some acronymes

DES : Data Encryption Standard (1977)

AES : Advanced Encryption Standard (2000)

RSA : Rivest, Shamir, Adelman (1978)

LLL : Lenstra, Lenstra, Lovacz (1982)

SVP : Shortest Vector Problem (and approximate versions)

CVP : Closest Vector Problem (and approximate versions)

SBP : Shortest Basis Problem (and approximate versions)

Some acronymes

DES : Data Encryption Standard (1977)

AES : Advanced Encryption Standard (2000)

RSA : Rivest, Shamir, Adelman (1978)

LLL : Lenstra, Lenstra, Lovacz (1982)

SVP : Shortest Vector Problem (and approximate versions)

CVP : Closest Vector Problem (and approximate versions)

SBP : Shortest Basis Problem (and approximate versions)

Some acronymes

DES : Data Encryption Standard (1977)

AES : Advanced Encryption Standard (2000)

RSA : Rivest, Shamir, Adelman (1978)

LLL : Lenstra, Lenstra, Lovacz (1982)

SVP : Shortest Vector Problem (and approximate versions)

CVP : Closest Vector Problem (and approximate versions)

SBP : Shortest Basis Problem (and approximate versions)

Some acronymes

DES : Data Encryption Standard (1977)

AES : Advanced Encryption Standard (2000)

RSA : Rivest, Shamir, Adelman (1978)

LLL : Lenstra, Lenstra, Lovacz (1982)

SVP : Shortest Vector Problem (and approximate versions)

CVP : Closest Vector Problem (and approximate versions)

SBP : Shortest Basis Problem (and approximate versions)

Lattice based cryptosystems ($\sim$ 1995)

Ajtai - Dwork

GGH : Goldreich, Goldwasser, Halevi

NTRU : Number Theorists Are Us (Are Useful)
Hoffstein, Pipher and Silverman

Lattice based cryptosystems ($\sim$ 1995)

Ajtai - Dwork

GGH : Goldreich, Goldwasser, Halevi

NTRU : Number Theorists Are Us (Are Useful)
Hoffstein, Pipher and Silverman

Lattice based cryptosystems ($\sim$ 1995)

Ajtai - Dwork

GGH : Goldreich, Goldwasser, Halevi

NTRU : Number Theorists Are Us (Are Useful)
Hoffstein, Pipher and Silverman

An argument of Paul Turan

Theorem (Fermat). *An odd prime p is the sum of two squares if and only if p is congruent to 1 modulo 4.*

Proof.

Step 1. For an odd prime p, the following conditions are equivalent.
(i) $p \equiv 1 \pmod 4$.
(ii) -1 is a square in the finite field $\mathbf{F}_p$.
(iii) -1 is a quadratic residue modulo p
(iv) There exists an integer r such that p divides $r^2 + 1$.

An argument of Paul Turan

Theorem (Fermat). *An odd prime p is the sum of two squares if and only if p is congruent to 1 modulo 4.*

Proof.

Step 1. For an odd prime p, the following conditions are equivalent.
(i) $p \equiv 1 \pmod 4$.
(ii) -1 is a square in the finite field $\mathbf{F}_p$.
(iii) -1 is a quadratic residue modulo p
(iv) There exists an integer r such that p divides $r^2 + 1$.

An argument of Paul Turan

Step 2. If p is a sum of two squares, then p is congruent to 1 modulo 4.

An argument of Paul Turan

Step 3. Assume p divides $r^2 + 1$. Let $\mathcal{L}$ be the lattice with basis $(1, r)^T, (0, p)^T$. The determinant of $\mathcal{L}$ is p. Using Minkowski's Theorem with the disk of radius R, we deduce that $\mathcal{L}$ contains a vector $(a, b)^T$ of norm $\sqrt{a^2 + b^2} \leq R$ as soon as $\pi R^2 > 4p$. Take

$$R = \frac{2\sqrt{p}}{\sqrt{3}} \quad \text{so that} \quad \pi R^2 > 4p \quad \text{and} \quad R^2 < 2p.$$

Hence there exists such a vector with $a^2 + b^2 < 2p$.

Since $(a, b)^T \in \mathcal{L}$, there exists $c \in \mathbf{Z}$ with $b = ar + cp$. Since p divides $r^2 + 1$, it follows that $a^2 + b^2$ is a multiple of p. The only nonzero multiple of p of absolute value less than $2p$ is p. Hence $p = a^2 + b^2$.

An argument of Paul Turan

Step 3. Assume p divides r^2+1. Let $\mathcal{L}$ be the lattice with basis $(1,r)^T, (0,p)^T$. The determinant of $\mathcal{L}$ is p. Using Minkowski's Theorem with the disk of radius R, we deduce that $\mathcal{L}$ contains a vector $(a,b)^T$ of norm $\sqrt{a^2+b^2} \leq R$ as soon as $\pi R^2 > 4p$. Take

$$R = \frac{2\sqrt{p}}{\sqrt{3}} \quad \text{so that} \quad \pi R^2 > 4p \quad \text{and} \quad R^2 < 2p.$$

Hence there exists such a vector with $a^2+b^2 < 2p$.

Since $(a,b)^T \in \mathcal{L}$, there exists $c \in \mathbf{Z}$ with $b = ar + cp$. Since p divides r^2+1, it follows that a^2+b^2 is a multiple of p. The only nonzero multiple of p of absolute value less than $2p$ is p. Hence $p = a^2+b^2$.

An argument of Paul Turan

Step 3. Assume p divides r^2+1. Let $\mathcal{L}$ be the lattice with basis $(1,r)^T, (0,p)^T$. The determinant of $\mathcal{L}$ is p. Using Minkowski's Theorem with the disk of radius R, we deduce that $\mathcal{L}$ contains a vector $(a,b)^T$ of norm $\sqrt{a^2+b^2} \leq R$ as soon as $\pi R^2 > 4p$. Take

$$R = \frac{2\sqrt{p}}{\sqrt{3}} \quad \text{so that} \quad \pi R^2 > 4p \quad \text{and} \quad R^2 < 2p.$$

Hence there exists such a vector with $a^2+b^2 < 2p$.

Since $(a,b)^T \in \mathcal{L}$, there exists $c \in \mathbf{Z}$ with $b = ar + cp$. Since p divides r^2+1, it follows that a^2+b^2 is a multiple of p. The only nonzero multiple of p of absolute value less than $2p$ is p. Hence $p = a^2+b^2$.

An argument of Paul Turan

Step 3. Assume p divides r^2+1. Let $\mathcal{L}$ be the lattice with basis $(1,r)^T, (0,p)^T$. The determinant of $\mathcal{L}$ is p. Using Minkowski's Theorem with the disk of radius R, we deduce that $\mathcal{L}$ contains a vector $(a,b)^T$ of norm $\sqrt{a^2+b^2} \leq R$ as soon as $\pi R^2 > 4p$. Take

$$R = \frac{2\sqrt{p}}{\sqrt{3}} \quad \text{so that} \quad \pi R^2 > 4p \quad \text{and} \quad R^2 < 2p.$$

Hence there exists such a vector with $a^2+b^2 < 2p$.

Since $(a,b)^T \in \mathcal{L}$, there exists $c \in \mathbf{Z}$ with $b = ar + cp$. Since p divides r^2+1, it follows that a^2+b^2 is a multiple of p. The only nonzero multiple of p of absolute value less than $2p$ is p. Hence $p = a^2+b^2$.

An argument of Paul Turan

Step 3. Assume p divides r^2+1. Let $\mathcal{L}$ be the lattice with basis $(1,r)^T,(0,p)^T$. The determinant of $\mathcal{L}$ is p. Using Minkowski's Theorem with the disk of radius R, we deduce that $\mathcal{L}$ contains a vector $(a,b)^T$ of norm $\sqrt{a^2+b^2}\leq R$ as soon as $\pi R^2 > 4p$. Take

$$R=\frac{2\sqrt{p}}{\sqrt{3}} \quad \text{so that} \quad \pi R^2 > 4p \quad \text{and} \quad R^2 < 2p.$$

Hence there exists such a vector with $a^2+b^2<2p$.

Since $(a,b)^T\in\mathcal{L}$, there exists $c\in\mathbf{Z}$ with $b=ar+cp$. Since p divides r^2+1, it follows that a^2+b^2 is a multiple of p. The only nonzero multiple of p of absolute value less than $2p$ is p. Hence $p=a^2+b^2$.

An argument of Paul Turan

Step 3. Assume p divides r^2+1. Let $\mathcal{L}$ be the lattice with basis $(1,r)^T,(0,p)^T$. The determinant of $\mathcal{L}$ is p. Using Minkowski's Theorem with the disk of radius R, we deduce that $\mathcal{L}$ contains a vector $(a,b)^T$ of norm $\sqrt{a^2+b^2} \leq R$ as soon as $\pi R^2 > 4p$. Take

$$R = \frac{2\sqrt{p}}{\sqrt{3}} \quad \text{so that} \quad \pi R^2 > 4p \quad \text{and} \quad R^2 < 2p.$$

Hence there exists such a vector with $a^2+b^2 < 2p$.

Since $(a,b)^T \in \mathcal{L}$, there exists $c \in \mathbf{Z}$ with $b = ar + cp$. Since p divides r^2+1, it follows that a^2+b^2 is a multiple of p. The only nonzero multiple of p of absolute value less than $2p$ is p. Hence $p = a^2+b^2$.

An argument of Paul Turan

Step 3. Assume p divides $r^2 + 1$. Let $\mathcal{L}$ be the lattice with basis $(1, r)^T, (0, p)^T$. The determinant of $\mathcal{L}$ is p. Using Minkowski's Theorem with the disk of radius R, we deduce that $\mathcal{L}$ contains a vector $(a, b)^T$ of norm $\sqrt{a^2 + b^2} \leq R$ as soon as $\pi R^2 > 4p$. Take

$$R = \frac{2\sqrt{p}}{\sqrt{3}} \quad \text{so that} \quad \pi R^2 > 4p \quad \text{and} \quad R^2 < 2p.$$

Hence there exists such a vector with $a^2 + b^2 < 2p$.

Since $(a, b)^T \in \mathcal{L}$, there exists $c \in \mathbf{Z}$ with $b = ar + cp$. Since p divides $r^2 + 1$, it follows that $a^2 + b^2$ is a multiple of p. The only nonzero multiple of p of absolute value less than $2p$ is p. Hence $p = a^2 + b^2$.

Minkowski's first Theorem

Let K be a compact convex set in $\mathbf{R}^n$ symmetric about 0 such that 0 lies in the interior of K. Let $\lambda_1 = \lambda_1(K)$ be the infimum of the real numbers λ such that λK contains an integer point in $\mathbf{Z}^n$ distinct from 0. Let $V = V(K)$ be the volume of K. Set $\tilde{\lambda} = 2V^{-1/n}$. Then $\tilde{\lambda}K$ is a convex body with volume 2^n. By Minkowski's convex body theorem $\tilde{\lambda}K$ contains an integer point $\neq 0$. Therefore $\lambda_1 \leq 2V^{-1/n}$, which means

$$\lambda_1^n V \leq 2^n.$$

This is Minkowski's first Theorem.

Minkowski's second theorem

For each integer j with $1 \leq j \leq n$, let $\lambda_j = \lambda_j(K)$ be the infimum of all $\lambda > 0$ such that λK contains j linearly independent integer points. Then

$$0 < \lambda_1 \leq \lambda_2 \cdots \leq \lambda_n < \infty.$$

The numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the *successive minima* of K.

Theorem [Minkowski's second convex body theorem, 1907].

$$\frac{2^n}{n!} \leq \lambda_1 \cdots \lambda_n V \leq 2^n.$$

Minkowski's second theorem

For each integer j with $1 \leq j \leq n$, let $\lambda_j = \lambda_j(K)$ be the infimum of all $\lambda > 0$ such that λK contains j linearly independent integer points. Then

$$0 < \lambda_1 \leq \lambda_2 \cdots \leq \lambda_n < \infty.$$

The numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the *successive minima* of K.

Theorem [Minkowski's second convex body theorem, 1907].

$$\frac{2^n}{n!} \leq \lambda_1 \cdots \lambda_n V \leq 2^n.$$

Examples

Examples :

• for the cube $|x_i| \le 1$, the volume V is 2^n and the successive minima are all 1.

• for the octahedron $|x_1| + \cdots + |x_n| \le 1$, the volume V is $2^n/n!$ and the successive minima are all 1.

Remark : Minkowski's Theorems extend to any full rank lattice $\mathcal{L} \subset \mathbf{R}^n$: if $b_1, \ldots, b_n$ is a basis of $\mathcal{L}$, taking $b_1, \ldots, b_n$ as a basis of $\mathbf{R}^n$ over $\mathbf{R}$ amounts to replace $\mathcal{L}$ by $\mathbf{Z}^n$.

Reference :

W.M. Schmidt. *Diophantine Approximation*. Lecture Notes in Mathematics **785**, Chap. 4, Springer Verlag, 1980.

Examples

Examples :

• for the cube $|x_i| \leq 1$, the volume V is 2^n and the successive minima are all 1.

• for the octahedron $|x_1| + \cdots + |x_n| \leq 1$, the volume V is $2^n/n!$ and the successive minima are all 1.

Remark : Minkowski's Theorems extend to any full rank lattice $\mathcal{L} \subset \mathbf{R}^n$: if $b_1, \ldots, b_n$ is a basis of $\mathcal{L}$, taking $b_1, \ldots, b_n$ as a basis of $\mathbf{R}^n$ over $\mathbf{R}$ amounts to replace $\mathcal{L}$ by $\mathbf{Z}^n$.

Reference :

W.M. Schmidt. *Diophantine Approximation*. Lecture Notes in Mathematics **785**, Chap. 4, Springer Verlag, 1980.

Examples

Examples :

• for the cube $|x_i| \leq 1$, the volume V is 2^n and the successive minima are all 1.

• for the octahedron $|x_1| + \cdots + |x_n| \leq 1$, the volume V is $2^n/n!$ and the successive minima are all 1.

Remark : Minkowski's Theorems extend to any full rank lattice $\mathcal{L} \subset \mathbf{R}^n$: if $b_1, \ldots, b_n$ is a basis of $\mathcal{L}$, taking $b_1, \ldots, b_n$ as a basis of $\mathbf{R}^n$ over $\mathbf{R}$ amounts to replace $\mathcal{L}$ by $\mathbf{Z}^n$.

Reference :

W.M. Schmidt. *Diophantine Approximation*. Lecture Notes in Mathematics **785**, Chap. 4, Springer Verlag, 1980.

Simultaneous approximation

Proposition (A.K. Lenstra, H.W. Lenstra, L. Lovasz, 1982). There exists a polynomial-time algorithm that, given a positive integer n and rational numbers $\alpha_1, \ldots, \alpha_n, \epsilon$ satisfying $0 < \epsilon < 1$, finds integers $p_1, \ldots, p_n, q$ for which

$$|p_i - q\alpha_i| \le \epsilon \quad \text{for} \quad 1 \le i \le n \quad \text{and} \quad 1 \le q \le 2^{n(n+1)/4}\epsilon^{-n}.$$

Proof. Let $\mathcal{L}$ be the lattice of rank $n+1$ spanned by the columns of the $(n+1) \times (n+1)$ matrix

$$\begin{pmatrix} 1 & \cdots & 0 & -\alpha_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & -\alpha_n \\ 0 & \cdots & 0 & \eta \end{pmatrix}$$

with $\eta = 2^{-n(n+1)/4}\epsilon^{n+1}$. The inner product of any two columns is rational. By the LLL algorithm, there is a polynomial-time algorithm to find a reduced basis $b_1, \ldots, b_{n+1}$ for $\mathcal{L}$.

Simultaneous approximation

Proposition (A.K. Lenstra, H.W. Lenstra, L. Lovasz, 1982). There exists a polynomial-time algorithm that, given a positive integer n and rational numbers $\alpha_1, \ldots, \alpha_n, \epsilon$ satisfying $0 < \epsilon < 1$, finds integers $p_1, \ldots, p_n, q$ for which

$$|p_i - q\alpha_i| \leq \epsilon \quad \text{for} \quad 1 \leq i \leq n \quad \text{and} \quad 1 \leq q \leq 2^{n(n+1)/4}\epsilon^{-n}.$$

Proof. Let $\mathcal{L}$ be the lattice of rank $n+1$ spanned by the columns of the $(n+1)\times(n+1)$ matrix

$$\begin{pmatrix} 1 & \cdots & 0 & -\alpha_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & -\alpha_n \\ 0 & \cdots & 0 & \eta \end{pmatrix}$$

with $\eta = 2^{-n(n+1)/4}\epsilon^{n+1}$. The inner product of any two columns is rational. By the LLL algorithm, there is a polynomial-time algorithm to find a reduced basis $b_1, \ldots, b_{n+1}$ for $\mathcal{L}$.

Simultaneous approximation

Since $\det(L) = \eta$, we have

$$2^{n/4} \det(L)^{1/(n+1)} = \epsilon$$

and

$$|b_1| \leq \epsilon.$$

Since $b_1 \in \mathcal{L}$, we can write

$$b_1 = (p_1 - q\alpha_1, p_2 - q\alpha_2, \ldots, p_n - q\alpha_n, q\eta)^T$$

with $p_1, \ldots, p_n, q \in \mathbf{Z}$. Hence

$$|p_i - q\alpha_i| \leq \epsilon \quad \text{for} \quad 1 \leq i \leq n \quad \text{and} \quad |q| \leq 2^{n(n+1)/4}\epsilon^{-n}.$$

From $\epsilon < 1$ and $b_1 \neq 0$ we deduce $q \neq 0$. Replacing b_1 by $-b_1$ if necessary we may assume $q > 0$.

Dirichlet's theorems on simultaneous approximation

Let $\alpha_1, \ldots, \alpha_n$ *be real numbers and* $Q > 1$ *an integer.*
(i) There exists integers $p_1, \ldots, p_n, q$ *with*

$$1 \leq q < Q \quad \textit{and} \quad |\alpha_i q - p_i| \leq \frac{1}{Q^{1/n}}.$$

(ii) There exists integers $q_1, \ldots, q_n, p$ *with*

$$1 \leq \max\{|q_1|, \ldots, |q_n|\} < Q \quad \textit{and} \quad |\alpha_1 q_1 + \cdots + \alpha_n q_n - p| \leq \frac{1}{Q^n}.$$

The proofs are easy applications of Dirichlet Box Principle (see Chap. II of Schmidt LN 785).

Connection with SVP - (i)

Let $\epsilon > 0$. Define $\eta = \epsilon/Q$. Consider the $\mathcal{L}$ be the lattice of rank $n+1$ spanned by the columns vectors $v_1, \dots, v_{n+1}$ of the $(n+1)\times(n+1)$ matrix

$$\begin{pmatrix} 1 & \cdots & 0 & -\alpha_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & -\alpha_n \\ 0 & \cdots & 0 & \eta \end{pmatrix}.$$

If $v = p_1 v_1 + \cdots + p_n v_n + q v_{n+1}$ is an element of $\mathcal{L}$ which satisfies $0 < \max\{|v_1|, \dots, |v_{n+1}|\} < \epsilon$, then we have

$$1 \le q < Q \quad \text{and} \quad |\alpha_i q - p_i| \le \epsilon \cdot$$

The determinant of $\mathcal{L}$ is η. From Minkowski's first Theorem, we deduce that there exists such a vector with $\epsilon^{n+1} = 2^{n+1}\eta$. With $\eta = \epsilon/Q$ we obtain $\epsilon^n = 2^{n+1}/Q$

Connection with SVP - (ii)

Let $\epsilon > 0$. Define $\eta = \epsilon/Q$. Consider the $\mathcal{L}$ be the lattice of rank $n+1$ spanned by the columns vectors $v_1, \dots, v_{n+1}$ of the $(n+1)\times(n+1)$ matrix

$$\begin{pmatrix} \eta & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \eta & 0 \\ \alpha_1 & \cdots & \alpha_n & -1 \end{pmatrix}.$$

If $v = q_1v_1 + \cdots + q_nv_n + pv_{n+1}$ is an element of $\mathcal{L}$ which satisfies $0 < \max\{|v_1|, \dots, |v_{n+1}|\} < \epsilon$, then we have

$$1 \leq q_i < \epsilon/\eta = Q \quad \text{and} \quad |\alpha_1q_1 + \cdots + \alpha_nq_n - p| < \epsilon\cdot$$

The determinant of $\mathcal{L}$ is $-\eta^n$. From Minkowski's first Theorem, we deduce that there exists such a vector with $\epsilon^{n+1} = 2^{n+1}\eta^n$. With $\eta = \epsilon/Q$ we obtain $\epsilon = 2^{n+1}/Q^n$.