August 3, 2016

A joint CIMPA-ICTP research school on
Lattices and applications to cryptography and coding theory
Saigon University, Ho Chi Minh City, Vietnam.
August 1st - 12th, 2016

CIMPA

ICTP The Abdus Salam International Centre for Theoretical Physics

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

Lattices and geometry of numbers II

Michel Waldschmidt
Université Pierre et Marie Curie (Paris 6) France
http://www.imj-prg.fr/~michel.waldschmidt/

Update: 05/08/2016

Part II: August 3, 2016

- Convex sets and star bodies
- Minkowski's convex body Theorem
- Minkowski's theorems on linear forms
- Gauge functions
- Minkowsk's theorems on successive minima

Blichfeldt's Theorem

Theorem 1.
Let L be a lattice in $\mathbb{R}^n$ of determinant Δ and B a measurable subset of $\mathbb{R}^n$. Assume $\mu(B) > \Delta$. Then there exist $x \neq y$ in B such that $x - y \in L$.

Convex Bodies

A set $B \subset \mathbb{R}^n$ is *convex* if, for x and y in B and for $0 \le \theta \le 1$, $\theta x + (1-\theta)y$ is in B.

A *star subset* of $\mathbb{R}^n$ is a subset B such that, for any $x \in B$ and any θ with $0 \le \theta \le 1$, θx is in B. Hence a convex subset of $\mathbb{R}^n$ containing 0 is a star subset.

The characteristic function of a convex bounded subset of $\mathbb{R}^n$ is Riemann integrable.

If a convex subset B of $\mathbb{R}^n$ is not contained in a hyperplane, then its interior is not empty and is a convex open set.

A *convex body* is a nonempty bounded open convex subset of $\mathbb{R}^n$.

A subset B of $\mathbb{R}^n$ is *symmetric* if $x \in B$ implies $-x \in B$.

Minkowski's convex body Theorem

Theorem 2.

Let L be a lattice in $\mathbb{R}^n$ of determinant Δ and let B be a measurable subset of $\mathbb{R}^n$, convex and symmetric with respect to the origin, of measure $\mu(B)$, such that $\mu(B) > 2^n\Delta$. Then $B \cap L \neq \{0\}$.

Corollary 3.

With the notations of Corollary 2, if B is also compact in $\mathbb{R}^n$, then the weaker inequality $\mu(B) \geq 2^n\Delta$ suffices to reach the conclusion.

`Remark` The example of $L = \mathbb{Z}^n$ with $\Delta = 1$ and $B = \left\{(x_1, \ldots, x_n) \in \mathbb{R}^n \; ; \; |x_i| < 1\right\}$ with measure $\mu(B) = 2^n$, shows that Corollaries 2 and 3 are sharp.

Minkowski's Linear Form Theorem

Theorem 4 (Minkowski).

Let $L_1, \ldots, L_n$ be homogeneous linear forms in n variables with real coefficients and determinant Δ. Let $c_1, \ldots, c_n$ be positive numbers with

$$c_1 \cdots c_n \geq |\Delta|.$$

Then there exists $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n \setminus \{0\}$ such that

$$|L_i(\underline{x})| \leq c_i \quad (i = 1, \ldots, n).$$

Corollary 5.

There exists $\underline{x} \neq 0$ such that

$$\max_{1\leq i\leq n} |L_i(\underline{x})| \leq \sqrt[n]{|\Delta|}.$$

Homogeneous simultaneous approximation

Corollary 6.

There exist $\underline{x}$, $\underline{x}'$, $\underline{x}'' \neq 0$ in $\mathbb{Z}^n$ such that

$$\sum_{i=1}^n |L_i(\underline{x})| \leq \sqrt[n]{n!|\Delta|}.$$

$$\prod_{i=1}^n |L_i(\underline{x}')| \leq n^{-n} n! |\Delta|.$$

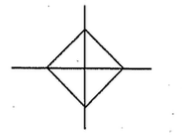
and

$$\sum_{i=1}^n |L_i(\underline{x}'')|^2 \leq c_n |\Delta|^{2/n}$$

with

$$c_n = \frac{4}{\pi}\Gamma(\frac{n}{2}+1)^{2/n}.$$

Volume of the octahedron



$$\sum_{i=1}^n |L_i(\underline{x})| \leq \sqrt[n]{n!|\Delta|}.$$

The volume of the octahedron $|x_1| + \cdots + |x_n| < 1$ in $\mathbb{R}^n$ is

$$2^n \int_0^1 \int_0^{1-x_1} \cdots \int_0^{1-x_1-\cdots-x_{n-1}} \mathrm{d}x_1 \mathrm{d}x_2 \cdots \mathrm{d}x_n = \frac{2^n}{n!}.$$

`Hint:` for $n \geq 1$,

$$\int_0^{1-t} \mathrm{d}x_1 \int_0^{1-x_1} \mathrm{d}x_2 \cdots \int_0^{1-x_{n-1}} \mathrm{d}x_n = \frac{1}{n!}(1-t)^n.$$

Arithmetico-geometric inequality

$$\prod_{i=1}^{n} |L_i(\underline{x}')| \leq n^{-n} n! |\Delta|.$$

For $x_1, \ldots, x_n$ in $\mathbb{R}$,

$$(x_1 \cdots x_n)^{1/n} \leq \frac{x_1 + \cdots + x_n}{n}.$$

Proof using the logarithmic function: convexity.

Proof by induction (Cauchy)

$$n = 2, \quad n \Rightarrow n-1, \quad n \Rightarrow 2n.$$

Volume of the unit sphere

$$\sum_{i=1}^{n} |L_i(\underline{x}'')|^2 \leq c_n |\Delta|^{2/n}$$

The volume V_n of the unit sphere

$$\{x \in \mathbb{R}^n \mid x_1^2 + \cdots + x_n^2 < 1\}$$

in $\mathbb{R}^n$ is

$$\frac{\pi^{n/2}}{\Gamma(1 + \frac{n}{2})}$$

with $\Gamma(x+1) = x\Gamma(x)$ and $\Gamma(1/2) = \sqrt{\pi}$.

Volume of the unit sphere

$$V_1 = 2, \quad V_2 = \pi, \quad V_3 = \frac{4}{3}\pi, \quad V_4 = \frac{\pi^2}{2},$$
$$V_n = \frac{2\pi}{n} V_{n-2}.$$

$$V_n = \begin{cases} \dfrac{\pi^{n/2}}{(\frac{n}{2})!} & \text{for } n \text{ even.} \\[2ex] \dfrac{\pi^{\frac{n-1}{2}} 2^{n+1} \left(\frac{n+1}{2}\right)!}{(n+1)!} & \text{for } n \text{ odd.} \end{cases}$$

Minkowski's Linear Forms Theorem for $\mathbb{Z}^n$.

Here is a consequence of Minkowski's Linear Forms Theorem for the lattice $\mathbb{Z}^n$.

Theorem 7.
Suppose that ϑ_{ij} $(1 \leq i, j \leq n)$ are real numbers with determinant ± 1 . Suppose that $A_1, \ldots, A_n$ are positive numbers with $A_1 \cdots A_n = 1$. Then there exists an integer point $\underline{x} = (x_1, \ldots, x_n) \neq 0$ such that

$$|\vartheta_{i1} x_1 + \cdots + \vartheta_{in} x_n| < A_i \qquad (1 \leq i \leq n-1)$$

and

$$|\vartheta_{n1} x_1 + \cdots + \vartheta_{nn} x_n| \leq A_n.$$

Simultaneous approximation

Corollary 8.
Let ϑ_{ij} $(1 \leq i \leq n,\ 1 \leq j \leq m)$ be mn real numbers. Let $Q > 1$ be a real number. There exist rational integers $q_1, \ldots, q_m, p_1, \ldots, p_n$ with

$$1 \leq \max\{|q_1|,\ \ldots,\ |q_m|\} < Q^{n/m}$$

and

$$\max_{1\leq i\leq n} |\vartheta_{i1}q_1 + \cdots + \vartheta_{im}q_m - p_i| \leq \frac{1}{Q}.$$

Gauge function associated to a convex body

Let B be a convex body. Let ∂B be the boundary of B and $\overline{B} = B \cup \partial B$ the closure of B.
The gauge function associated to B is the map $f : \mathbb{R}^n \to [0, \infty)$ defined by $f(0) = 0$ and, for $x \neq 0$,

$$f(x) = \inf\{\lambda > 0 \ \mid\ x \in \lambda B\}.$$

Hence $x = f(x)x'$ with $x' \in \partial B$ and

$$\begin{aligned} f(x) < 1 &\iff x \in B \\ f(x) = 1 &\iff x \in \partial B \\ f(x) \leq 1 &\iff x \in \overline{B} \end{aligned}$$

We will write $f(x) = \|x\|_B$.

Characterization of gauge functions

A gauge function $f : \mathbb{R}^n \to [0, \infty)$ attached to a convex body satisfies

$$\begin{aligned} &f(x) > 0 \quad \text{for} \quad x \neq 0, \qquad f(0) = 0, \\ &f(\lambda x) = \lambda f(x) \quad \text{for} \quad x \in \mathbb{R},\ \lambda \geq 0, \\ &f(x + y) \leq f(x) + f(y). \end{aligned}$$

Conversely, if f satisfies these conditions, then f is continuous and is the Gauge function associated to the convex body $B = \{x \ \mid\ f(x) < 1\}$.

A convex body is symmetric if and only if its Gauge function satisfies $f(-x) = f(x)$.

Minkowski's first convex body Theorems for $\mathbb{Z}^n$

Let B be a symmetric convex body in $\mathbb{R}^n$. Define

$$\lambda_1 = \min_{0\neq x\in\mathbb{Z}^n} f(x).$$

Hence λ_1 is the least real number such that $(\lambda_1\overline{B}) \cap \mathbb{Z}^n \neq \{0\}$.

Theorem 9 (Minkowski).
For a symmetric convex body B of volume $\mu(B)$, we have

$$\lambda_1^n \mu(B) \leq 2^n.$$

Minkowski's first convex body Theorems for the Euclidean ball

Denote by $\|\cdot\|$ the Euclidean norm and by V_n the volume of the unit Euclidean ball in $\mathbb{R}^n$.
Let L a lattice of determinant Δ. Define

$$\lambda_1 = \min_{0\neq x\in L} \|x\|.$$

Theorem 10 (Minkowski).
We have

$$\lambda_1^n V_n \leq 2^n \Delta.$$

Hermite's constant

Recall that for $n \geq 2$,

$$\gamma_n = \sup_L \frac{\lambda_1(L)^2}{(v(L))^{2/n}},$$

where L ranges over the set of lattices L in $\mathbb{R}^n$ of covolume $v(L)$ and first minimum $\lambda_1(L)$ with respect to the Euclidean ball in $\mathbb{R}^n$.

L. Lagrange proved $\gamma_2 = 2/\sqrt{3}$ (hexagonal lattice - Eisenstein integers).

Hermite proved $\gamma_n \leq \gamma_2^{n-1}$ for $n \geq 2$.

Hermite's constant

The values of γ_n is known for $n \leq 8$ and for $n = 24$:

d	2	3	4	5	6	7	8	24
γ_d	$2/\sqrt{3}$	$2^{1/3}$	$\sqrt{2}$	$8^{1/5}$	$(64/3)^{1/6}$	$64^{1/7}$	2	4
Approximation	1.1547	1.2599	1.4142	1.5157	1.6654	1.8114	2	4

Phong Q. Nguyen. *Hermite's Constant and Lattice Algorithms*. Chapter 2 pp. 19–69 of *The LLL Algorithm Survey and Applications*, Phong Q. Nguyen and Brigitte Vallée, Editors. Ser. Information Security and Cryptography, Springer Verlag (2010).

Minkowski's convex body Theorem and Hermite's constant

Minkowski deduced from his convex body theorem the upper bound

$$\gamma_n \leq \left(\frac{4}{V_n}\right)^{2/n}.$$

Using known estimates for

$$V_n = \frac{\pi^{n/2}}{\Gamma(1+\frac{n}{2})}$$

one deduces

$$\gamma_n \leq 1 + \frac{n}{4}.$$

Successive minima

Let B be a symmetric convex body in $\mathbb{R}^n$. The successive minima of B relative to a lattice Λ are the real numbers

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$$

such that, for $r = 1, \ldots, n$, λ_r is the least real number such that $\lambda_r \overline{B}$ contains at least r linearly independent elements of Λ.

`Examples with` $\Lambda = \mathbb{Z}^n$.
The rectangle in $\mathbb{R}^2$ with center $(0,0)$, length 4, width 1 has $\lambda_1 = 1/2$ and $\lambda_2 = 2$. Its volume is 4.

The closed disc in $\mathbb{R}^2$ with center $(0,0)$ and radius $1/2$ has $\lambda_1 = \lambda_2 = 1$. Its volume is $\pi^2/4$.

An example in dimension 4

Consider the sublattice L of $\mathbb{Z}^n$ which consists of (x_1, x_2, x_3, x_4) with $x_1 + x_2 + x_3 + x_4$ even. A basis is given by the row vectors of the matrix

$$\begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Hence the determinant of L is 2, the minima are all $\sqrt{2}$.
The row vectors of the matrix

$$\begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

are also shortest vectors but span a sublattice of index 2.

An example of Korkine and Zolotarev

Example of a lattice for which the successive minima of the Euclidean ball do not give a basis: for $n \geq 5$,

$$\mathbb{Z}^n + \mathbb{Z}\left(\frac{1}{2}, \ldots, \frac{1}{2}\right) = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n + \mathbb{Z}\left(\frac{e_1 + \cdots + e_n}{2}\right) \subset \mathbb{R}^n.$$

This corresponds to the lattice $\mathbb{Z}^n$ and the convex body

$$\Big\{(x_1, \ldots, x_n) \in \mathbb{R}^n \;\mid\; \left(x_1 + \frac{x_n}{2}\right)^2 + \cdots + \left(x_{n-1} + \frac{x_n}{2}\right)^2 + \left(\frac{x_n}{2}\right)^2 < 1\Big\}.$$

Bound for the index

Let K be a convex body and L a lattice in $\mathbb{R}^n$. Let $\omega_1, \ldots, \omega_n$ be linearly independent elements in L such that

$$\|\omega_i\|_K = \lambda_i \quad (i = 1, \ldots, n).$$

Let $\Omega = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$. Then $(L : \Omega) \leq n!$.

A basis almost given by the successive minima

Given a symmetric convex body K in $\mathbb{R}^n$ with gauge function $\|\cdot\|_K$ and a lattice L with successive minima $\lambda_1, \ldots, \lambda_n$, there exists a basis $(v_1, \ldots, v_n)$ of L with

$$\|v_i\|_K \leq \max\left\{1, \frac{i}{2}\right\} \lambda_i \quad (i = 1, \ldots, n).$$

Minkowski's second convex body Theorem for $\mathbb{Z}^n$

Theorem 11 (Minkowski).

The successive minima $\lambda_1, \lambda_2, \ldots, \lambda_n$ of a symmetric convex body B relative to $\mathbb{Z}^n$ satisfy

$$\frac{2^n}{n!} \leq \lambda_1 \lambda_2 \cdots \lambda_n \mu(B) \leq 2^n.$$

The cube $|x_i| \leq 1$ in $\mathbb{R}^n$ has $\lambda_1 = \cdots = \lambda_n = 1$, its volume is 2^n.

The octahedron $|x_1| + \cdots + |x_n| \leq 1$ in $\mathbb{R}^n$ has $\lambda_1 = \cdots = \lambda_n = 1$, its volume is $2^n/n!$.

The lower bound for $\lambda_1 \lambda_2 \cdots \lambda_n$ is easy, the proof of the upper bound is deep.

Dual lattice

Denote by $x \cdot y$ the standard inner product in $\mathbb{R}^n$:

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n.$$

Let L be a lattice in $\mathbb{R}^n$. The *dual* lattice of L is

$$L^\star = \{y \in \mathbb{R}^n \mid x \cdot y \in \mathbb{Z} \text{ for all } x \in L\}.$$

If $L_1 \subset L_2$, then $L_2^\star \subset L_1^\star$.
For $L = A\mathbb{Z}^n$, we have $L^\star = ({}^tA)^{-1}\mathbb{Z}^n$.
Hence the dual lattice is a lattice with covolume satisfying

$$v(L)v(L^\star) = 1.$$

Example: the lattice $\mathbb{Z}^n$ is selfdual.

Duality in simultaneous Diophantine approximation

Let $\theta_1, \ldots, \theta_m$ be real numbers.
The dual of the lattice in $\mathbb{R}^{m+1}$

$$\begin{aligned}\Lambda &= \{0\} \times \mathbb{Z}^m + \mathbb{Z}(1, \theta_1, \ldots, \theta_m) \\ &= \left\{(q, q\theta_1 - p_1, \ldots, q\theta_m - p_m) \mid (q, p_1, \ldots, p_m) \in \mathbb{Z}^{m+1}\right\}\end{aligned}$$

is the lattice

$$\begin{aligned}\Lambda^\star &= \mathbb{Z}(1, 0, \ldots, 0) + \mathbb{Z}(\theta_1, 1, 0, \ldots, 0) + \cdots + \mathbb{Z}(\theta_m, 0, \ldots, 0, 1) \\ &= \Big\{(a_0 + a_1\theta_1 + \cdots + a_m\theta_m, a_1, \ldots, a_m) \mid \\ &\qquad\qquad (a_0, a_1, \ldots, a_m) \in \mathbb{Z}^{m+1}\Big\}.\end{aligned}$$

Dual convex body

Let K be a symmetric convex body in $\mathbb{R}^n$. The *dual* (or polar) convex body is

$$K^\star = \{y \in \mathbb{R}^n \mid x \cdot y \leq 1 \text{ for all } x \in K\}.$$

If $K_1 \subset K_2$, then $K_2^\star \subset K_1^\star$.
Examples:

- The Euclidean ball $B : x_1^2 + \cdots + x_n^2 \leq 1$ is selfdual.
- The dual of $[-1, 1]^2$ in $\mathbb{R}^2$ is the polytope $|x| + |y| \leq 1$.
- More generally, the dual of $\prod_{i=1}^n [-a_i, a_i]$ with $a_i > 0$ is

$$\{x \in \mathbb{R}^n \mid a_1 x_1 + \cdots + a_n x_n \leq 1\}.$$

The Gauge functions associated to a convex body and its dual are related by

$$\|x\|_{K^\star} = \sup_{y \neq 0} \frac{x \cdot y}{\|y\|_K}.$$

Transference

Let K be a convex body and L a lattice in $\mathbb{R}^n$. Denote by $\lambda_1, \ldots, \lambda_n$ the successive minima of K relative to L, and by $\lambda_1^\star, \ldots, \lambda_n^\star$ the successive minima of the dual convex body $K^\star$ relative to the dual lattice $L^\star$. Then

$$1 \leq \lambda_i \lambda_{n-i+1}^\star \quad (i = 1, \ldots, n).$$

Transference

Let K be a convex body and L a lattice in $\mathbb{R}^n$. Denote by $\lambda_1, \ldots, \lambda_n$ the successive minima of K relative to L, and by $\lambda_1^\star, \ldots, \lambda_n^\star$ the successive minima of the dual convex body $K^\star$ relative to the dual lattice $L^\star$.Then

$$\lambda_i \lambda_{n-i+1}^\star \leq n! \quad (i = 1, \ldots, n).$$

Duality in simultaneous Diophantine approximation

Let $\theta_1, \ldots, \theta_m$ be real numbers. Let $Q > 1$ be a real number. The transference Theorem relates the minima $\lambda_1, \ldots, \lambda_{m+1}$ of the convex body

$$\left\{(x_0, x_1, \ldots, x_m) \in \mathbb{R}^m \mid |x_0| \leq Q^m, \max_{1 \leq i \leq m} |x_i| \leq Q^{-1}\right\}$$

with respect to the lattice

$$\left\{(q, q\theta_1 - p_1, \ldots, q\theta_m - p_m) \mid (q, p_1, \ldots, p_m) \in \mathbb{Z}^{m+1}\right\}$$

and the minima $\lambda_1^\star, \ldots, \lambda_{m+1}^\star$ of the convex body

$$\left\{(y_0, y_1, \ldots, y_m) \in \mathbb{R}^m \mid |y_0| \leq Q^{-m}, \max_{1 \leq i \leq m} |y_i| \leq Q\right\}$$

with respect to the lattice

$$\left\{(a_0 + a_1\theta_1 + \cdots + a_m\theta_m, a_1, \ldots, a_m) \mid (a_0, a_1, \ldots, a_m) \in \mathbb{Z}^{m+1}\right\}.$$

Further topics

The Grassmann algebra (exterior product)

Mahler's Theory of compound sets

Parametric geometry of numbers
(WM. Schmidt, L. Summerer, D. Roy)