LECTURE 1: On Diophantine inequalities

July 22, 2014
Convex bodys
Minkowski’s convex body theorem I

Minkowski’s convex body theorem I: Let $n \in \mathbb{Z}^+$. Assume that $\Lambda \subseteq \mathbb{R}^n$ is a lattice with rank $\Lambda = n$ and $C \subseteq \mathbb{R}^n$ is symmetric (wrt origin) convex body with

$$V(C) > 2^n \det \Lambda \quad \text{or} \quad \geq \quad \text{if } C \text{ is compact} \quad (1)$$

Then, there exists a non-zero lattice point in $C$. In fact

$$\# C \cap \Lambda \geq 3. \quad (2)$$
Theorem A is a typical example from the theory of linear forms.

THEOREM A: Let

$$\alpha_1, \ldots, \alpha_m \in \mathbb{R}$$  \hspace{1cm} (3)

and

$$h_1, \ldots, h_m \in \mathbb{Z}^+$$  \hspace{1cm} (4)

be given. Then there exist $p, q_1, \ldots, q_m \in \mathbb{Z}$ with a $q_k \neq 0$, satisfying

$$|q_i| \leq h_i, \quad \forall i = 1, \ldots, m,$$  \hspace{1cm} (5)

and

$$|p + q_1\alpha_1 + \ldots + q_m\alpha_m| < \frac{1}{h_1 \cdots h_m} := \frac{1}{h}.$$  \hspace{1cm} (6)
Proof of Theorem A

Write

\[ L_0\overline{x} := x_0 + \alpha_1x_1 + \ldots + \alpha_mx_m, \]  
\[ L_k\overline{x} := x_k, \quad k = 1, \ldots, m. \]  

Put

\[ |L_0\overline{x}| < \frac{1}{h}, \]  
\[ |L_k\overline{x}| \leq h_k + 1/2, \quad k = 1, \ldots, m. \]
Proof of Theorem A

Then

\[(L_0, L_1, \ldots, L_m) : \mathbb{Z}^{m+1} \rightarrow \mathbb{R}^{m+1}\]  \hspace{1cm} (11)

defines a full lattice

\[\Lambda := \mathbb{Z}\bar{l}_0 + \mathbb{Z}\bar{l}_1 + \ldots + \mathbb{Z}\bar{l}_m = \]

\[\mathbb{Z}(1, 0, \ldots, 0)^T + \mathbb{Z}(\alpha_1, 1, 0, \ldots, 0)^T + \ldots + \mathbb{Z}(\alpha_m, 0, \ldots, 1)^T \]

\[\subseteq \mathbb{R}^{m+1}\]  \hspace{1cm} (12)

with determinant

\[\det \Lambda = 1.\]  \hspace{1cm} (13)
Proof of Theorem A

Determinant of the full lattice

$$\Lambda = \mathbb{Z}\ell_0 + \mathbb{Z}\ell_1 + \ldots + \mathbb{Z}\ell_m \subseteq \mathbb{R}^{m+1} \quad (14)$$

is given by

$$\det \Lambda = \left| \begin{array}{cccc} 1 & \alpha_1 & \alpha_2 & \ldots & \alpha_m \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{array} \right| = 1. \quad (15)$$
Proof of Theorem A

(From now on we will drop the transpose notation and think the row notation as a column vector when necessary.)

Now the conditions (9) and (10) determine a convex set

\[ C := \{(y_0, \ldots, y_m) | |y_0| < \frac{1}{h}, |y_k| \leq h_k + 1/2 \} \subseteq \mathbb{R}^{m+1} \]  \hspace{1cm} (16)

with volume

\[ \text{vol } C = \frac{2^{m+1}(h_1 + 1/2) \cdots (h_m + 1/2)}{h_1 \cdots h_m} > 2^{m+1}. \]  \hspace{1cm} (17)

By Minkowski’s convex body theorem I there exists

\[ \vec{0} \neq \vec{y} = (p + q_1 \alpha_1 + \ldots + q_m \alpha_m, q_1, \ldots, q_m) \in C \cap \Lambda. \]  \hspace{1cm} (18)
Proof of Theorem A

Hence we have

\[(p, q_1, \ldots, q_m) \in \mathbb{Z}^{m+1} \setminus \{0\}\] (19)

with

\[|q_i| \leq h_i, \quad \forall i = 1, \ldots, m,\] (20)

and

\[|p + q_1 \alpha_1 + \ldots + q_m \alpha_m| < \frac{1}{h_1 \cdots h_m}. \quad \square\] (21)
Primitive vector

An integer vector

\[(r_0, r_1, \ldots, r_m) \in \mathbb{Z}^{m+1}\]  \hfill (22)

is **primitive**, if the greatest common divisor satisfies

\[\text{g.c.d.}(r_0, r_1, \ldots, r_m) = 1.\]  \hfill (23)

Let

\[\text{g.c.d.}(p, q_1, \ldots, q_m) = d \in \mathbb{Z}_{\geq 2}\]  \hfill (24)

and suppose

\[(p, q_1, \ldots, q_m) = d(s, r_1, \ldots, r_m), \quad (s, r_1, \ldots, r_m) \in \mathbb{Z}^{m+1}\]  \hfill (25)

satisfies the equation

\[|p + q_1 \alpha_1 + \ldots + q_m \alpha_m| < \frac{1}{h}.\]  \hfill (26)
Primitive vector solution

Then

\[ |s + r_1 \alpha_1 + \ldots + r_m \alpha_m| < \frac{1}{dh} < \frac{1}{h}. \] (27)

Thus we have also a primitive solution

\[ (s, r_1, \ldots, r_m) \in \mathbb{Z}^{m+1} \] (28)

for equation

\[ |p + q_1 \alpha_1 + \ldots + q_m \alpha_m| < \frac{1}{h}. \] (29)
Diophantine inequalities

THEOREM B: Let

\[ \alpha_1, \ldots, \alpha_m \in \mathbb{R} \] \tag{30}

and

\[ h_1, \ldots, h_m \in \mathbb{Z}^+ \] \tag{31}

be given. Then there exist a primitive vector

\[ (p, q_1, \ldots, q_m) \in \mathbb{Z}^{m+1} \setminus \{0\} \] \tag{32}

with a \( q_k \neq 0 \), satisfying

\[ \left| q_i \right| \leq h_i, \quad \forall i = 1, \ldots, m, \] \tag{33}

and

\[ \left| p + q_1 \alpha_1 + \ldots + q_m \alpha_m \right| < \frac{1}{h_1 \cdots h_m} := \frac{1}{h}. \] \tag{34}
Infinite of primitive solutions

THEOREM C: Let

\[ 1, \alpha_1, \ldots, \alpha_m \in \mathbb{R} \]  \hspace{1cm} (35)

be linearly independent over \( \mathbb{Q} \). Then there exist infinitely many primitive vectors

\[ \overline{v}_k = (p_k, q_1,k, \ldots, q_m,k) \in \mathbb{Z}^{m+1} \setminus \{0\} \]  \hspace{1cm} (36)

with

\[ h_{i,k} := \max\{1, |q_{i,k}|\}, \quad \forall i = 1, \ldots, m, \]  \hspace{1cm} (37)

satisfying

\[ |p_k + q_{1,k} \alpha_1 + \ldots + q_{m,k} \alpha_m| < \frac{1}{h_{1,k} \cdots h_{m,k}} := \frac{1}{h_k}. \]  \hspace{1cm} (38)
Proof of Theorem C

Suppose on the contrary, that there exist only finitely many primitive solutions for (38). Then by the linear independence and assumption (36) there exists a minimum

$$\min |p_k + q_{1,k}\alpha_1 + \ldots + q_{m,k}\alpha_m| := \frac{1}{R} > 0. \quad (39)$$

Choose then

$$\hat{h}_i \in \mathbb{Z}^+, \quad \hat{h}_1 \cdot \ldots \cdot \hat{h}_m =: \hat{h}, \quad \frac{1}{\hat{h}} \leq \frac{1}{R}. \quad (40)$$

Now by Theorem B there exists a primitive solution
Proof of Theorem C

\[(\hat{p}, \hat{q}_1, \ldots, \hat{q}_m) \in \mathbb{Z}^{m+1} \setminus \{0\}\]  

(41)

with

\[
\max\{1, |\hat{q}_i|\} \leq \hat{h}_i, \quad \forall i = 1, \ldots, m,\]

(42)

satisfying

\[
|\hat{p} + \hat{q}_1 \alpha_1 + \ldots + \hat{q}_m \alpha_m| < \frac{1}{\hat{h}} \leq \frac{1}{R}.
\]

(43)

which contradicts (39).
Corollaries

THEOREM D: Let
\[ 1, \alpha_1, ..., \alpha_m \in \mathbb{R} \] (44)
be linearly independent over \( \mathbb{Q} \). If there exist positive constants \( c, \omega \in \mathbb{R}^+ \) such that
\[ |\beta_0 + \beta_1 \alpha_1 + ... + \beta_m \alpha_m| \geq \frac{c}{(h_1 \cdots h_m)\omega}. \] (45)
for all
\[ (\beta_0, \beta_1, ..., \beta_m) \in \mathbb{Z}^{m+1} \setminus \{0\}, \quad h_k = \max\{1, |\beta_k|\}, \] (46)
then
\[ \omega \geq 1. \] (47)
Proof of Theorem D

Assume on the contrary that

\[ \omega < 1. \tag{48} \]

By Theorem C there exists an infinite of primitive vectors satisfying

\[ |p_k + q_{1,k}\alpha_1 + \ldots + q_{m,k}\alpha_m| < \frac{1}{h_{1,k} \cdots h_{m,k}} \tag{49} \]

and by (45) we have

\[ \frac{c}{(h_{1,k} \cdots h_{m,k})^\omega} \leq |p_k + q_{1,k}\alpha_1 + \ldots + q_{m,k}\alpha_m| < \frac{1}{h_{1,k} \cdots h_{m,k}} \tag{50} \]

Choose

\[ \log(h_{1,k} \cdots h_{m,k}) \geq \frac{\log(1/c)}{1 - \omega}. \tag{51} \]

A contradiction with (50).
Corollaries

Usually the above results are only given in terms of

\[ H_k := \max_{i=1,\ldots,m} |q_{i,k}|. \] (52)

**THEOREM C2:** Let

\[ 1, \alpha_1, \ldots, \alpha_m \in \mathbb{R} \] (53)

be linearly independent over \( \mathbb{Q} \). Then there exist infinitely many primitive vectors

\[ \overline{v}_k = (p_k, q_{1,k}, \ldots, q_{m,k}) \in \mathbb{Z}^{m+1} \setminus \{0\} \] (54)

satisfying

\[ |p_k + q_{1,k}\alpha_1 + \ldots + q_{m,k}\alpha_m| < \frac{1}{H_k^m}. \] (55)
Corollaries

THEOREM D2: Let

\[ 1, \alpha_1, \ldots, \alpha_m \in \mathbb{R} \quad (56) \]

be linearly independent over \( \mathbb{Q} \). If there exist positive constants \( c, \omega \in \mathbb{R}^+ \) such that

\[ |p_k + q_{1,k}\alpha_1 + \ldots + q_{m,k}\alpha_m| > \frac{c}{H^\omega} \quad (57) \]

for all

\[ \overline{v}_k = (p_k, q_{1,k}, \ldots, q_{m,k}) \in \mathbb{Z}^{m+1}, \quad 1 \leq H_k = \max |q_{i,k}|, \quad (58) \]

then

\[ \omega \geq m. \quad (59) \]
Is the best bound for all

Let $\alpha$ be an algebraic integer of $\text{deg}_\mathbb{Q}\alpha = m + 1$ and $\alpha_i = \sigma_i(\alpha)$, where $\sigma_i$ are the field monomorphisms of the field $\mathbb{Q}(\alpha)$. Then

$$|p + q_1\alpha + \ldots + q_m\alpha^m| > \frac{1}{H^m(m + 1)^m A m^2},$$

where

$$A = 2 \max_{i=0,1,...,m} |\alpha_i| \quad (60)$$

for all

$$(p, q_1, \ldots, q_m) \in \mathbb{Z}^{m+1}, \quad 1 \leq H = \max |q_i|. \quad (61)$$
Better bound for a.a.

THEOREM F: For almost all

\[
\alpha_1, \ldots, \alpha_m \in \mathbb{R}, \tag{62}
\]

wrt Lebesgue measure, there exist infinitely many primitive vectors

\[
\overline{v}_k = (p_k, q_{1,k}, \ldots, q_{m,k}) \in \mathbb{Z}^{m+1} \setminus \{0\}, \tag{63}
\]

\[
H_k := \max |q_{i,k}|, \quad \forall i = 1, \ldots, m, \tag{64}
\]

satisfying

\[
|p_k + q_{1,k}\alpha_1 + \cdots + q_{m,k}\alpha_m| < \frac{1}{H_k^m \log H_k}. \tag{65}
\]

Further (65) is the best bound for a.a.
THEOREM AS: Let
\[ \alpha_1, \ldots, \alpha_m \in \mathbb{R} \quad (66) \]
be given. Then there exist
\[ q \in \mathbb{Z}^+, \ p_1, \ldots, p_m \in \mathbb{Z} \quad (67) \]
satisfying
\[ |q\alpha_i + p_i| < \frac{1}{q^{1/m}}, \quad \forall i = 1, \ldots, m. \quad (68) \]
Simultaneous linear forms

THEOREM AS MODIFIED: Let

\[ \alpha_1, \ldots, \alpha_m \in \mathbb{R}, \quad f_1 + \ldots + f_m = 1, \quad (69) \]

be given. Then there exist

\[ q \in \mathbb{Z}^+, \quad p_1, \ldots, p_m \in \mathbb{Z}, \quad (70) \]

satisfying

\[ |q\alpha_i + p_i| < \frac{1}{q^{f_i}}, \quad \forall i = 1, \ldots, m. \quad (71) \]
Proof

Define a set

\[ C = \{ (x_0, x_1, ..., x_m) \in \mathbb{R}^{m+1} \mid |x_0| \leq q + 1/2, \]

\[ |x_0 \alpha_i + x_i| < \frac{1}{q^{f_i}}, \quad i = 1, ..., m \} = \] (72)

\[ \{ (x_0, x_1, ..., x_m) \in \mathbb{R}^{m+1} \mid |x_0| \leq q + 1/2, \]

\[ -x_0 \alpha_i - \frac{1}{q^{f_i}} < x_i < -x_0 \alpha_i + \frac{1}{q^{f_i}}, \quad i = 1, ..., m; \} \] (73)
Proof/\mathcal{C} \text{ symmetric convex body}/\text{Vol } \mathcal{C}

\text{Vol } \mathcal{C} = (2q + 1) \frac{2}{q^{f_1}} \cdots \frac{2}{q^{f_m}} > 2^{m+1}. \quad (74)
Define a lattice

\[ \Lambda = \mathbb{Z}^{m+1}. \]  \hspace{1cm} (75)

By Minkowski’s convex body theorem there exists

\[ \bar{0} \neq \bar{x} = (p, q_1, \ldots, q_m) \in C \cap \Lambda. \]  \hspace{1cm} (76)

Hence we have

\[ (p, q_1, \ldots, q_m) \in \mathbb{Z}^{m+1} \setminus \{\bar{0}\} \]  \hspace{1cm} (77)

with ...
Simultaneous linear forms

THEOREM BS: Let

\[ \alpha_1, \ldots, \alpha_m \in \mathbb{R} \quad (78) \]

be given. Then there exists a primitive vector

\[ (q, p_1, \ldots, p_m) \in \mathbb{Z}^{m+1}, \quad q \in \mathbb{Z}^+ \quad (79) \]

satisfying

\[ |q\alpha_i + p_i| < \frac{1}{q^{1/m}}, \quad \forall i = 1, \ldots, m. \quad (80) \]
Infinite of primitive solutions

THEOREM CS: Let at least one of the numbers

$$\alpha_1, \ldots, \alpha_m \in \mathbb{R}$$  \hfill (81)

be irrational. Then there exist infinitely many primitive vectors

$$\overline{v}_k = (q_k, p_{1,k}, \ldots, p_{m,k}) \in \mathbb{Z}^{m+1} \setminus \{0\}, \quad q_k \in \mathbb{Z}^+$$  \hfill (82)

satisfying

$$|q_k \alpha_i + p_{i,k}| < \frac{1}{q_k^{1/m}}, \quad \forall i = 1, \ldots, m.$$  \hfill (83)
On Diophantine inequalities of linear forms/$\mathbb{C}$
THEOREM A\textsuperscript{C1}: Let

\[ \alpha_0 = 1, \alpha_1, \ldots, \alpha_m \in \mathbb{C} \quad (84) \]

and

\[ H \in \mathbb{Z}_{\geq 1} \quad (85) \]

be given. Then there exists a

\[ (\beta_0, \beta_1, \ldots, \beta_m) \in \mathbb{Z}^{m+1} \setminus \{0\}, \quad |\beta_i| \leq H, \quad \forall i = 0, 1, \ldots, m, \quad (86) \]

satisfying

\[ |\beta_0 + \beta_1 \alpha_1 + \ldots + \beta_m \alpha_m| \leq \frac{c}{H^{(m-1)/2}}, \quad c = \sqrt{2} \sum_{k=0}^{m} |\alpha_k|. \quad (87) \]
Let \( \mathbb{I} \) denote an imaginary quadratic field or the field \( \mathbb{Q} \) of rational numbers and \( \mathbb{Z}_\mathbb{I} \) its ring of integers.

For simplicity we consider the case

\[
\mathbb{I} = \mathbb{Q}(\sqrt{-1})
\]  \hspace{1cm} (88)

with Gaussian integers

\[
\mathbb{Z}_\mathbb{I} = \mathbb{Z} + i\mathbb{Z}.
\]  \hspace{1cm} (89)
An other linear Diophantine inequality in \( \mathbb{C} \)

**THEOREM A\(_{C2}\):** Let

\[
\alpha_1, \ldots, \alpha_m \in \mathbb{C}
\]  \hspace{2cm} (90)

and

\[
h_1, \ldots, h_m \in \mathbb{Z}^+
\]  \hspace{2cm} (91)

be given. Then there exists a non-zero integer vector

\[
(\beta_0, \beta_1, \ldots, \beta_m) \in \mathbb{Z}^{m+1}_+ \setminus \{0\}
\]  \hspace{2cm} (92)

satisfying

\[
|\beta_i| \leq h_i, \quad \forall i = 1, \ldots, m,
\]  \hspace{2cm} (93)

and

\[
|\beta_0 + \beta_1 \alpha_1 + \ldots + \beta_m \alpha_m| \leq \left(\frac{2}{\sqrt{\pi}}\right)^{m+1} \frac{1}{h_1 \cdots h_m} := R_0.
\]  \hspace{2cm} (94)
Let $a = c + id \in \mathbb{C}$. Define a disk

$$D_R = \{z \in \mathbb{C} \mid |z - a| \leq R\}, \quad \text{VOL} \ D_R = \pi R^2,$$

(95)

and another disk

$$C_R = \{(x_0, y_0) \in \mathbb{R}^2 \mid (x_0 - c)^2 + (y_0 - d)^2 \leq R^2\}, \quad \text{VOL} \ C_R = \pi R^2.$$

(96)

Note the following correspondence

$$z = x_0 + iy_0 \in D_R \iff (x_0, y_0) \in C_R.$$

(97)
Disks

Denote

\[ a + ib = -(z_1 \alpha_1 + \ldots + z_m \alpha_m), \quad z_i = x_k + iy_k, \quad k = 0, 1, \ldots, m. \]

(98)

Define sets

\[ D = \{ z = (z_0, z_1, \ldots, z_m) \in \mathbb{C}^{m+1} | \]

\[ |z_0 - (a + ib)| \leq R_0; \quad |z_k| \leq h_k, \quad k = 1, \ldots, m \} \]

(99)

and

\[ C = \{ (x_0, y_0, x_1, y_1, \ldots, x_m, y_m) \in \mathbb{R}^{2m+2} | \]

\[ (x_0 - a)^2 + (y_0 - b)^2 \leq R_0^2, \quad x_k^2 + y_k^2 \leq h_k^2, \quad k = 1, \ldots, m \}. \]

(100)
Proof $\mathcal{C}$ symmetric convex body

$\mathcal{C}$ is convex.
Proof/Vol $C$

$$\text{Vol } C = \int \ldots \int \left( \int \int dx_0 dy_0 \right) dx_1 dy_1 \ldots dx_m dy_m =$$

$$(101)$$

$$\pi R_0^2 \int \ldots \int \left( \int \int dx_1 dy_1 \right) dx_2 dy_2 \ldots dx_m dy_m =$$

$$(102)$$

$$\pi^2 R_0^2 h_1^2 \int \ldots \int \left( \int \int dx_2 dy_2 \right) dx_3 dy_3 \ldots dx_m dy_m =$$

$$(103)$$

$$\ldots$$
Proof/Vol $C$

\[ \text{Vol } C = \pi^{m+1} h_1^2 \cdots h_m^2 R_0^2 = \]

\[ \pi^{m+1} h_1^2 \cdots h_m^2 \left( \frac{4}{\pi} \right)^{m+1} \frac{1}{h_1^2 \cdots h_m^2} = 2^{2m+2}. \]
Define a lattice

\[ \Lambda = \mathbb{Z}^{2m+2}. \]  

(106)

By Minkowski’s convex body theorem there exists

\[ \vec{0} \neq \vec{x} = (x_0, y_0, x_1, y_1, \ldots, x_m, y_m) \in \mathcal{C} \cap \Lambda. \]  

(107)

Thus we get

\[ (\beta_0, \beta_1, \ldots, \beta_m) = (x_0 + iy_0, x_1 + iy_1, \ldots, x_m + iy_m) \]

\[ \in \mathcal{D} \cap \mathbb{Z}_I^{m+1} \setminus \{\vec{0}\} \]  

(108)

with
Proof/C

\[ |\beta_i| \leq h_i, \quad \forall i = 1, \ldots, m, \]  \hspace{1cm} (109)

and

\[ |\beta_0 + \beta_1 \alpha_1 + \ldots + \beta_m \alpha_m| \leq \left( \frac{2}{\sqrt{\pi}} \right)^{m+1} \frac{1}{h_1 \cdots h_m}. \]  \hspace{1cm} (110)
Siegel’s lemma or Thue-Siegel’s lemma is a powerful tool in Transcendental Number Theory. We may say that most transcendency proofs are based on Siegel’s lemma.
Siegel’s lemma

Let

\[ L_m(\vec{x}) = \overline{a}_m \cdot \vec{x} = \sum_{n=1}^{N} a_{mn}x_n, \quad m = 1, \ldots, M, \quad (111) \]

be \( M \) non-trivial linear forms with coefficients \( a_{mn} \in \mathbb{Z} \) in \( N \) variables \( x_k \). Denote

\[ A_m := \sum_{n=1}^{N} |a_{mn}| \in \mathbb{Z}^+, \quad m = 1, \ldots, M. \quad (112) \]
Siegel’s lemma

Suppose that
\[ M < N, \]  
(113)
then the system of equations
\[ L_m(\bar{x}) = 0, \quad m = 1, ..., M, \]  
(114)
has a non-zero integer solution \( \bar{z} = (z_1, ..., z_N)^T \in \mathbb{Z}^N \setminus \{0\} \) with
\[
1 \leq \max_{1 \leq n \leq N} |z_n| \leq \left[ (A_1 \cdots A_M)^{\frac{1}{N-M}} \right].
\]  
(115)
Siegel’s lemma/The system of equations

The system of equations

\[
\begin{cases}
    a_{11} x_1 + a_{12} x_2 + \ldots + a_{1N} x_N = 0 \\
    a_{21} x_1 + a_{22} x_2 + \ldots + a_{2N} x_N = 0 \\
    \vdots \\
    a_{M1} x_1 + a_{M2} x_2 + \ldots + a_{MN} x_N = 0
\end{cases}
\]

has an integer solution with

\[
1 \leq \max_{1 \leq n \leq N} |x_n| \leq \left[ (A_1 \cdots A_M)^{\frac{1}{N-M}} \right].
\]
Proof of Siegel’s lemma

I. Let

\[ A := [a_{mn}] \in M_{M \times N}(\mathbb{Z}) \quad (116) \]

be the matrix of the linear mapping

\[ \bar{L} = (L_1, \ldots, L_M)^T : \mathbb{Z}^N \to \mathbb{Z}^M, \quad N > M. \quad (117) \]

The linear mapping (117) is not injective and thus

\[ \text{Ker} \ \bar{L} \neq \{0\}. \quad (118) \]
Proof of Siegel’s lemma

II. Denote

\[ Z := \left( (A_1 \cdots A_M)^{\frac{1}{N-M}} \right) \]  \hspace{1cm} (119)

Then

\[ A_1 \cdots A_M < (Z + 1)^{N-M} \]  \hspace{1cm} (120)

and consequently

\[ (A_1 Z + 1) \cdots (A_M Z + 1) \leq \]  \hspace{1cm} (121)

\[ A_1 \cdots A_M (Z + 1)^M < \]  \hspace{1cm} (122)

\[ (Z + 1)^{N-M}(Z + 1)^M = (Z + 1)^N. \]  \hspace{1cm} (123)
III. Number of integer points in cubes. Define the first cube

$$\square_1 := \{\bar{x} \in \mathbb{Z}^N | 0 \leq x_n \leq Z\}$$ \hspace{1cm} (124)

where the number of points is

$$\#\square_1 = (Z + 1)^N.$$ \hspace{1cm} (125)
Proof of Siegel’s lemma

VI. Secondly, the linear mappings

\[ L_m(\bar{x}) = \sum_{n=1}^{N} a_{mn}x_n, \quad m = 1, \ldots, M \]  

(126)

are bounded in the cube (124) by

\[ \sum_{a_{mn}<0} a_{mn}x_n \leq L_m(\bar{x}) \leq \sum_{a_{mn}>0} a_{mn}x_n. \]  

(127)
Proof of Siegel’s lemma

Denote

\[- b_m := \sum_{a_{mn} < 0} a_{mn}, \quad c_m := \sum_{a_{mn} > 0} a_{mn} x_n. \quad (128)\]

and note

\[b_m + c_m = A_m. \quad (129)\]

Then we have

\[- b_m Z \leq L_m(\bar{x}) \leq c_m Z. \quad (130)\]
Proof of Siegel’s lemma

Define the second cube (box)

\[ \square_2 := \{ \bar{I} \in \mathbb{Z}^M \mid -b_m Z \leq l_m \leq c_m Z \}, \quad (131) \]

where

\[ \#\{l_m\} = (b_m + c_m)Z + 1 = A_m Z + 1. \quad (132) \]

Thus the number of points in the second cube (131) is

\[ \#\square_2 = (A_1 Z + 1) \cdots (A_M Z + 1). \quad (133) \]
Proof of Siegel’s lemma

Consequently,

$$\overline{L}(\square_1) \subseteq \square_2,$$  \hspace{1cm} (134)

where

$$\#\square_2 = (A_1Z + 1) \cdots (A_MZ + 1) < \#\square_1 = (Z + 1)^N.$$ \hspace{1cm} (135)

Hence

$$\overline{L} : \square_1 \rightarrow \square_2$$ \hspace{1cm} (136)

is not injective.
Proof of Siegel’s lemma

Therefore there exist two different vectors

\[ \bar{x}_1, \bar{x}_2 \in \Box_1 \]  \hspace{1cm} (137)

such that

\[ \bar{L}(\bar{x}_1) = \bar{L}(\bar{x}_2). \]  \hspace{1cm} (138)

Thus

\[ \bar{L}(\bar{x}_1 - \bar{x}_2) = 0, \]  \hspace{1cm} (139)

where

\[ \bar{z} := \bar{x}_1 - \bar{x}_2 \in \pm \Box_1 \setminus \{0\}. \]  \hspace{1cm} (140)
Proof of Siegel’s lemma

Finally, from

\[ z \in \pm \Box_1 \setminus \{0\} \]  

we get

\[ -Z \leq z_k \leq Z. \quad \Box \]
Successive minima

\[ \lambda_j = \inf\{\lambda > 0| \text{rank}(\langle \lambda C \rangle \cap \Lambda) = j\}. \]  \hspace{1cm} (143)

\[ 0 < \lambda_1 \leq \cdots \leq \lambda_n < \infty. \]  \hspace{1cm} (144)
Minkowski’s convex body theorem II

Let $n \in \mathbb{Z}^+$. Assume that $\Lambda \subseteq \mathbb{R}^n$ is a lattice with rank $\Lambda = n$ and $\mathcal{C} \subseteq \mathbb{R}^n$ is symmetric (wrt origin) convex body. Then

$$\frac{2^n}{n!} \det \Lambda \leq \lambda_1 \cdots \lambda_n V(\mathcal{C}) \leq 2^n \det \Lambda. \quad (145)$$

In particular $\Rightarrow$

$$\lambda_1^n V(\mathcal{C}) \leq 2^n \det \Lambda. \quad (146)$$