Minkowski's Successive Minima

and

The Lattice Point Enumerator

Martin Henk

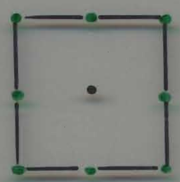
Magdeburg

- Let $\mathcal{K}_0^n$ be the set of all 0-symmetric convex bodies $K \subset \mathbb{R}^n$ with $\operatorname{int}(K) \neq \emptyset$.

K 0-symmetric $\Leftrightarrow$ $K = -K = \{-x : x \in K\}$

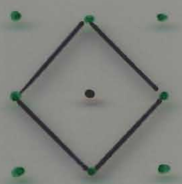
- For instance

$$C_n = \{x \in \mathbb{R}^n : |x_i| \leq 1,\ 1 \leq i \leq n\}$$



cube

$$C_n^* = \{x \in \mathbb{R}^n : \sum_{i=1}^{n} |x_i| \leq 1\}$$



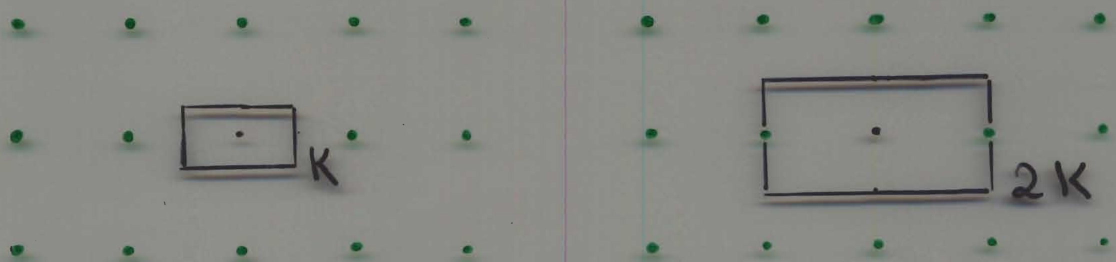
crosspolytope

$$B_n = \{x \in \mathbb{R}^n : \sum_{i=1}^{n} |x_i|^2 \leq 1\}$$

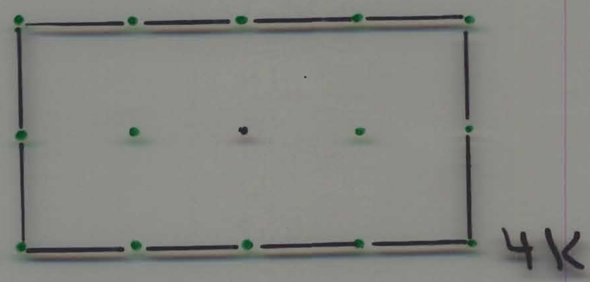
unit ball

- Let $\mathbb{Z}^n = \{z \in \mathbb{R}^n : z_i \in \mathbb{Z},\ 1 \le i \le n\}$ be the integral lattice.

- $\lambda_i(K) = \min\{\lambda > 0 : \dim(\lambda K \cap \mathbb{Z}^n) \geq i\}$ is called the i-th successive minimum, $1 \le i \le n$.



$\lambda_1(K) = 2$



$\lambda_2(K) = 4$

- $\lambda_i(K) \leq \lambda_{i+1}(K)$

- $\lambda_1(K) \geq 1 \iff K \cap \mathbb{Z}^n = \{0\}$

- $\lambda_i(\alpha \cdot K) = \frac{1}{\alpha} \cdot \lambda_i(K)$

- Let $Q = \{x \in \mathbb{R}^n : |x_i| \leq \alpha_i,\ 1 \leq i \leq n\}$,

  $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$.

$$\lambda_i(Q) = \frac{1}{\alpha_i},\quad 1 \leq i \leq n.$$

- Minkowski's 1st theorem, 1896.

$$\mathrm{vol}(K) \leq \left(\frac{2}{\lambda_1(K)}\right)^n$$

$$\left[\Longleftrightarrow \mathrm{vol}(K) \geq 2^n \Rightarrow K \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset. \right]$$

~~Proof~~: $\lambda_1 = \lambda_1(K)$;

$$\mathrm{int}(\lambda_1 \cdot K) \cap \mathbb{Z}^n = \{0\}$$

$$\Leftrightarrow \left(\mathrm{int}\left(\tfrac{\lambda_1}{2} K\right) - \mathrm{int}\left(\tfrac{\lambda_1}{2} K\right)\right) \cap \mathbb{Z}^n = \{0\}$$

$$\Leftrightarrow \left[z_1 + \mathrm{int}\left(\tfrac{\lambda_1}{2} K\right)\right] \cap \left[z_2 + \mathrm{int}\left(\tfrac{\lambda_1}{2} K\right)\right] = \emptyset,$$

$$\forall z_1, z_2 \in \mathbb{Z}^n,\ z_1 \neq z_2$$

$$\Rightarrow \mathrm{vol}\left(\tfrac{\lambda_1}{2} K\right) \leq 1.$$

Applications

- Dirichlet, 1842.

Let $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ and $0 < \varepsilon < 1$. Then there exist $p_1, \dots, p_n, q \in \mathbb{Z}$, $1 \le q \le \varepsilon^{-n}$, s.t.

$$\left| \frac{p_i}{q} - \alpha_i \right| < \frac{\varepsilon}{q}, \quad 1 \le i \le n.$$

- Lagrange, 1770.

Every positive integer is the sum of four integer squares.

(Proof by Davenport.)

~~Proof~~:

- Let $\tau < \varepsilon$ s.t. $\lfloor \tau^{-m} \rfloor \leq \varepsilon^{-m}$.

- For $x \in \mathbb{R}^{m+1}$ let

$$l_i(x) = x_i - \alpha_i \cdot x_{m+1}, \quad 1 \leq i \leq m,$$

$$l_{m+1}(x) = x_{m+1}.$$

- $$P = \{ x \in \mathbb{R}^m : \ |l_i(x)| \leq \tau, \ 1 \leq i \leq m, \ |l_{m+1}(x)| \leq \tau^{-m} \}$$

is a 0-symmetric parallelepiped with $\mathrm{vol}(P) = 2^{m+1}$

$\Longrightarrow$ $\exists \ p := (p_1, \dots, p_m, q) \in P \cap \mathbb{Z}^{m+1} \setminus \{0\}$. Let $q \geq 0$.

- $q = 0 \Rightarrow |p_i| = |l_i(p)| \leq \tau < 1$

$\Rightarrow p = 0$ contr.

$\Rightarrow q \geq 1$: $|l_i(p)| = |p_i - \alpha_i q| < \varepsilon, \ 1 \leq i \leq m$

and $|l_{m+1}(p)| = |q| \leq \lfloor \tau^{-m} \rfloor \leq \varepsilon^{-m}$.

Generalisations

- Blichfeldt, 1914; Mordell, 1934; v. d. Corput, 1936; ...

$$\mathrm{vol}(K) \geq k \cdot 2^n \Rightarrow \#(K \cap \mathbb{Z}^n \setminus \{0\}) \geq 2k$$

- Siegel, 1935.

$$K \cap \mathbb{Z}^n = \{0\}$$

$$\Rightarrow \quad 2^n = \mathrm{vol}(K) + \frac{4^n}{\mathrm{vol}(K)} \sum_{z \in \mathbb{Z}^n \setminus \{0\}} |\varphi(z)|^2 .$$

- Conjecture (Ehrhart, 1955).

Let $K \subset \mathbb{R}^n$ be a convex body with centroid 0.

$$\mathrm{vol}(K) \geq \frac{(n+1)^n}{n!} \implies K \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset.$$

- verified only in the plane

- Minkowski's 2nd theorem, 1896.

  - $\mathrm{vol}(K) \leq \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(K)}\right).$

"=", e.g., $Q = \{x \in \mathbb{R}^n : |x_i| \leq \alpha_i\}$,

$\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$. $\lambda_i(Q) = \frac{1}{\alpha_i}$ and

$\mathrm{vol}(Q) = 2^n \prod_{i=1}^{n} \alpha_i.$

[Bambah, Woods, Zassenhaus, 1965; Cassels, 1959; Danicic, 1969; Davenport, 1939; Estermann, 1946; Siegel, 1935; Weyl, 1942]

  - $\frac{1}{n!} \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(K)}\right) \leq \mathrm{vol}(K)$

"=", e.g., $C_n^* = \{x \in \mathbb{R}^n : \sum |x_i| \leq 1\}$

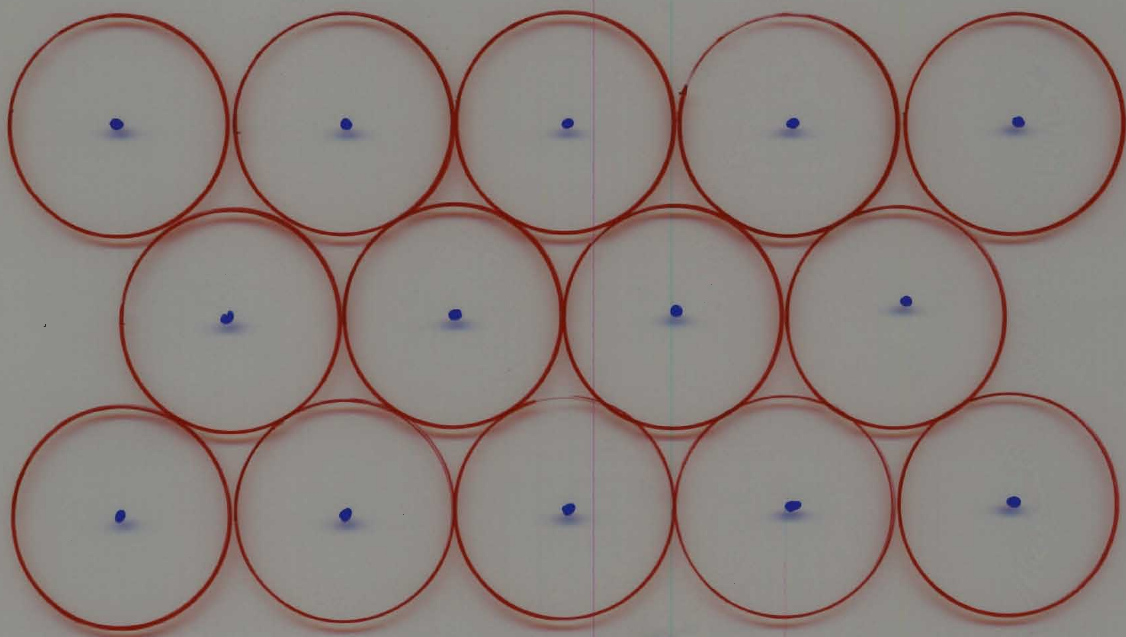
$\lambda_i(C_n^*) = 1$ and $\mathrm{vol}(C_n^*) = \frac{2^n}{n!}$.

Generalisations

- Let $\delta(K)$ be the density of a densest lattice packing of K, i.e.,

$$\delta(K) = \left[\sup\left\{ \frac{\mathrm{vol}(\Lambda + K)}{\mathrm{vol}(\mathbb{R}^n)} : \begin{array}{l}\Lambda \text{ packing} \\ \text{lattice of } K\end{array} \right\}\right]$$

$$= \sup\left\{ \left(\frac{\lambda_1(AK)}{2}\right)^n \mathrm{vol}(AK) : A \in GL(n, \mathbb{R}) \right\}.$$



$$\delta(B^2) = \frac{\pi}{2\sqrt{3}} \approx 0.906\ldots$$

- $0 < \delta(K) \leq 1$
- $\mathrm{vol}(K) \leq \left(\frac{2}{\lambda_1(K)}\right)^n \cdot \delta(K)$

- Conjecture (Davenport, 1946)

$$\mathrm{vol}(K) \leq \delta(K) \cdot \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(K)} \right)$$

- verified for:
    - $n=2$, ellipsoids, Minkowski, 1896
    - $n=3$, Woods, 1956

- Rogers, 1949; Chabauty, 1949.

$$\mathrm{vol}(K) \leq 2^{\frac{1}{2}(n-1)} \delta(K) \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(K)} \right)$$

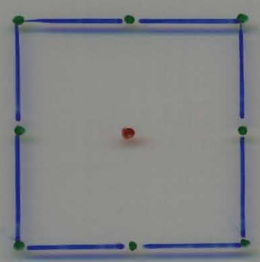
- Mahler, 1949; Chabauty, 1949.

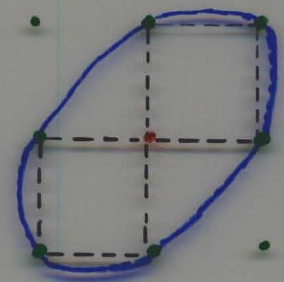
The factor $2^{\frac{1}{2}(n-1)}$ is best possible w.r.t. ray sets.

- Let $G(K) = \#(K \cap \mathbb{Z}^n)$.

- Minkowski, 1896. Let $\lambda_1(K) \geq 1$.

$$G(K) \leq \begin{cases} 3^n, & \\ 2^{n+1}-1, & K \text{ strictly convex.} \end{cases}$$





~~Proof~~: $G(K) > 3^n$.

- Since $|\mathbb{Z}^n : 3\mathbb{Z}^n| = 3^n$

$\Rightarrow \exists\, z_1, z_2 \in K \cap \mathbb{Z}^n,\ z_1 \neq z_2$ with

$$z_1 \equiv z_2 \bmod 3\mathbb{Z}^n$$

$\Rightarrow \mathbb{Z}^n \setminus \{0\} \ni \frac{1}{3}z_1 - \frac{1}{3}z_2$

$$= \frac{2}{3}\left(\frac{1}{2}z_1 - \frac{1}{2}z_2\right) \in \operatorname{int}(K)$$

$\Rightarrow \lambda_1(K) < 1$.

- Betke, H., Wills, 1993.

- $G(K) \leq \left(\frac{2}{\lambda_1(K)} + 1\right)^n$

- only for $n = 2$

$$G(K) \leq \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(K)} + 1\right)$$

- $G(K) \geq \frac{1}{n!} \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(K)}\right) \left(1 - \frac{\lambda_1(K)}{2}\right)^n$

- All these inequalities (would) imply Minkowski's bounds for the volume.

$$\mathrm{vol}(K) = \lim_{m \to \infty} \left(\frac{1}{m}\right)^n G(mK)$$

$$\leq \lim_{m \to \infty} \left(\frac{1}{m}\right)^n \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(mK)} + 1\right)$$

$$= \lim_{m \to \infty} \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(K)} + \frac{1}{m}\right)$$

$$= \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(K)}\right).$$

- He, 2002.

$$G(k) < 2^{n-1} \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(k)} + 1 \right)$$

- Let $m_1, \dots, m_n \in \mathbb{N}$ s.t.

i) $\left\lfloor \frac{2}{\lambda_i(k)} + 1 \right\rfloor \leq m_i$ and

ii) m_{i+1} divides m_i

$\Rightarrow \quad G(k) \leq m_1 \cdot \ldots \cdot m_n .$

- Let $L(K) = \prod_{i=1}^{m} \left\lfloor \left(\frac{2}{\lambda_i(K)} + 1 \right) \right\rfloor$

- Conjecture.

$$G(K) \leq L(K)$$

- For $s \in \mathbb{R}_{\geq 0}$

$$L(sK) = \prod_{i=1}^{m} \left(s \frac{2}{\lambda_i(K)} + 1 \right)$$

is a polynomial in s.

- Let $\mathcal{P}^n$ be the set of all lattice polytopes in $\mathbb{R}^n$.

- Ehrhart, 1967. Let $P \in \mathcal{P}^n$.

  For $m \in \mathbb{N}$

  $$G(mP) = \sum_{i=0}^{n} G_i(P)\, m^i$$

  is a polynomial in m.

- $G_n(P) = \mathrm{vol}(P)$

- $G_0(P) = 1$

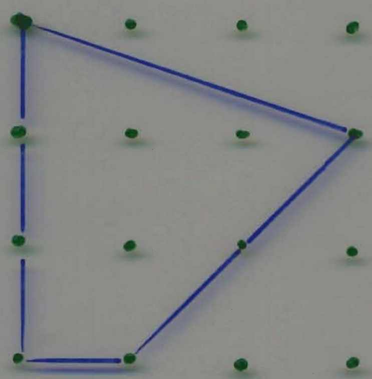
- Let $F_1, \dots, F_k$ be the facets ($(n-1)$-dim. faces) of P

  $$G_{n-1}(P) = \frac{1}{2} \sum_{i=1}^{k} \frac{\mathrm{vol}_{n-1}(F_i)}{\det(\operatorname{aff} F_i \cap \mathbb{Z}^n)}$$

Examples

- $n=2$; Pick's theorem, 1899.

$$G(mP) = \mathrm{vol}(P)\cdot m^2 + \frac{1}{2}\#(\mathrm{bd}\,P \cap \mathbb{Z}^2)\cdot m + 1.$$



$$G_2(P) = \frac{11}{2}$$

$$G_1(P) = \frac{7}{2}$$

$$G_0(P) = 1$$

- $n=3$; Reeve simplices.

$$T_\ell = \mathrm{conv}\left\{ \begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\\ell\end{pmatrix} \right\}, \quad \ell \geq 1.$$

- $G(T_\ell) = 4$, $\mathrm{vol}(T_\ell) = \frac{\ell}{6}$.

- $G_3(T_\ell) = \frac{\ell}{6}$, $G_2(T_\ell) = 1$,

  $G_1(T_\ell) = \frac{12-\ell}{6}$, $G_0(T_\ell) = 1$.

- Mordell-Sommersheim tetrahedron.

(Sommersheim, 1993)

$$T = \operatorname{conv}\left\{ \begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}a\\0\\0\end{pmatrix}, \begin{pmatrix}0\\b\\0\end{pmatrix}, \begin{pmatrix}0\\0\\c\end{pmatrix} \right\},$$

$a, b, c \in \mathbb{N}$, $\gcd(a, b, c) = 1$.

$$\Rightarrow G_1(T) = \frac{1}{4}\left(A + B + C + a + b + c \right)$$

$$+ \frac{1}{12}\left(\frac{bc}{a} + \frac{ac}{b} + \frac{ab}{c} + \frac{d^2}{abc} \right)$$

$$- A\, s\left(\frac{bc}{d}, \frac{aA}{d} \right) - B\, s\left(\frac{ac}{d}, \frac{bB}{d} \right)$$

$$- C\, s\left(\frac{ab}{d}, \frac{cC}{d} \right),$$

- $A = \gcd(b, c)$, $B = \gcd(a, c)$, $C = \gcd(a, b)$, $d = ABC$, and

$$s(p, q) = \frac{1}{4p} \sum_{m=1}^{p-1} \cot\frac{\pi m}{p} \cot\frac{\pi m q}{p}$$

denotes the Dedekind sum of $p, q \in \mathbb{N}$, $\gcd(p, q) = 1$.

- $C_n = \{ x \in \mathbb{R}^n : |x_i| \leq 1 \}$

$$G(m\, C_n) = (2m+1)^n$$

$$= \sum_{i=0}^{n} \binom{n}{i} 2^i m^i$$

$$\Rightarrow G_i(C_n) = \binom{n}{i} 2^i .$$

- $C_n^* = \{ x \in \mathbb{R}^n : \sum |x_i| \leq 1 \}$

$$G(m\, C_n^*) = \sum_{i=0}^{n} 2^{n-i} \binom{n}{i} \binom{m}{n-i}$$

$$\Rightarrow G_n(C_n^*) = \frac{2^n}{n!} , \quad G_{n-1}(C_n^*) = \frac{2^{n-1}}{(n-1)!}$$

- $T_n = \mathrm{conv}\{ 0, e_1, \ldots, e_n \}$

$$G(m\, T_n) = \binom{m+n}{n}$$

$$\Rightarrow G_n(T_n) = \frac{1}{n!} , \quad G_{n-1}(T_n) = \frac{1}{2} \frac{n+1}{(n-1)!}$$

- Stanley, 1980; Betke, Gritzmann, 1986.

Let $Z = \{ \alpha_1 v_1 + \cdots + \alpha_k v_k \ : 0 \leq \alpha_i \leq 1 \}$, $v_i \in \mathbb{Z}^n$, be a lattice zonotope. Then

$$G_i(Z) = \sum_{F \text{ } i\text{-face}} \frac{\mathrm{vol}_i(F)}{\det(\mathrm{aff} F \cap \mathbb{Z}^n)} \cdot \gamma(P, F),$$

where $\gamma(P,F)$ is the exterior angle of P at F.

- Liu, 2004.

Let $C(n,k)$ be a cyclic n-polytope with k integral vertices on the moment curve $t \to (t, t^2, \ldots, t^n)$. Then

$$G_i(C(n,k)) = \mathrm{vol}_i(C(i,k)).$$

- Betke, Kneser, 1985.

  Every additive and unimodular invariant functional on $\mathcal{P}^n$ is a linear combination of $G_0, \dots, G_n$.

- Ehrhart's reciprocity law, 1967.

$$G(\mathrm{int}(mP)) = (-1)^n \sum_{i=0}^{n} G_i(P)\,(-m)^i .$$

- Let $s \in \mathbb{C}$.

$$G(s\,P) = \sum_{i=0}^{m} G_i(P)\, s^i = \prod_{i=1}^{m} \left(1 + \frac{s}{\gamma_i(P)}\right)$$

zeros: $-\gamma_i(P) \in \mathbb{C}$

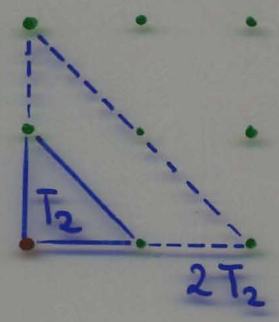
$$L(s\,K) = \prod_{i=1}^{m} \left(1 + s \cdot \frac{2}{\lambda_i(K)}\right)$$

zeros: $-\dfrac{\lambda_i(K)}{2} \in \mathbb{R}$

Examples

- $T_n = \mathrm{conv}\{0, e_1, \dots, e_n\}$

  $G(\mathrm{int}(m T_n)) = 0 \,, \quad m = 1, \dots, n$



  $\Rightarrow$ zeros $= \{-1, \dots, -n\}$.

- $Q = \{x \in \mathbb{R}^n : |x_i| \le m_i\}, \; m_i \in \mathbb{N}, \; m_1 \ge \dots \ge m_n$

  $$G(mQ) = \prod_{i=1}^{n} (1 + 2m \cdot m_i)$$

  $$\Rightarrow \gamma_i(Q) = \frac{1}{2m_i} = \frac{\lambda_i(Q)}{2} \,, \quad 1 \le i \le n$$

- G has no roots in $\mathbb{N}$.

- Bump, Choi, Kurlberg, Vaaler, 2004.

  Let $C_n^1 = \{x \in \mathbb{R}^n : \sum |x_i| \leq 1\}$.

  $$\mathrm{Re}\,(\gamma_i(C_n^1)) = \frac{1}{2}.$$

- Beck, de Loera, Develin, Pfeifle, Stanley, 2004.

  - $|\gamma_i(P)| \leq (n+1)!+1$.
  - The real roots lie in $[-n, \frac{n}{2})$ and for $n \leq 4$ in $[-n, 1)$.

(Work in progress)

- Let $P \in \mathcal{P}^n \cap \mathcal{K}_o^n$.

- Minkowski's 1st theorem:

$$\frac{\lambda_1(P)}{2} \leq \left(\prod_{i=1}^{n} \gamma_i(P) \right)^{1/n}$$

- H., Schürmann, Wills, 2005.

$$\frac{1}{n} \sum_{i=1}^{n} \gamma_i(P) \leq \frac{\lambda_n(P)}{2}$$

- Minkowski's 2nd theorem:

$$\left(\prod_{i=1}^{n} \frac{\lambda_i(P)}{2} \right)^{1/n} \leq \left(\prod_{i=1}^{n} \gamma_i(P) \right)^{1/n}$$

- H., Schürmann, Wills, 2005.

$$\frac{1}{n} \sum_{i=1}^{n} \gamma_i(P) \leq \frac{1}{n} \sum_{i=1}^{n} \frac{\lambda_i(P)}{2}$$

best possible, e.g., for the cube C_n and the crosspolytope C_n^*.

- The statement is equivalent to

$$\frac{G_{n-1}(P)}{\mathrm{vol}(P)} \leq \sum_{i=1}^{n} \frac{\lambda_i(P)}{2}$$

- Corollary.

Let $L(sP) = \sum_{i=0}^{n} L_i(P)\, s^i$. Then

$$G_{n-1}(P) \leq L_{n-1}(P).$$

$G_n(P) \leq L_n(P)$ ([illegible])

- Remark: For $n \leq 3$ we have

$$-\gamma_i(P) \geq -1.$$