Ehrhart theory I : introduction

J.L. Ramírez Alfonsín

Université de Montpellier

V Mexican School in Discrete Mathematics
CIMAT, Guanajuato
January 8-12, 2018

Lattice notions

Let $B = \{b_1, \ldots, b_n\}$ be a family of linear independent vectors in $\mathbb{R}^d$. The lattice generated by B is the set

$$\Lambda = \left\{ \sum_{i=1}^{n} x_i b_i | x_i \in \mathbb{Z} \right\}$$

Lattice notions

Let $B = \{b_1, \ldots, b_n\}$ be a family of linear independent vectors in $\mathbb{R}^d$. The lattice generated by B is the set

$$\Lambda = \left\{ \sum_{i=1}^{n} x_i b_i | x_i \in \mathbb{Z} \right\}$$

We say that B is a base of Λ of dimension n and that Λ is of full rank if $n = d$.

Lattice notions

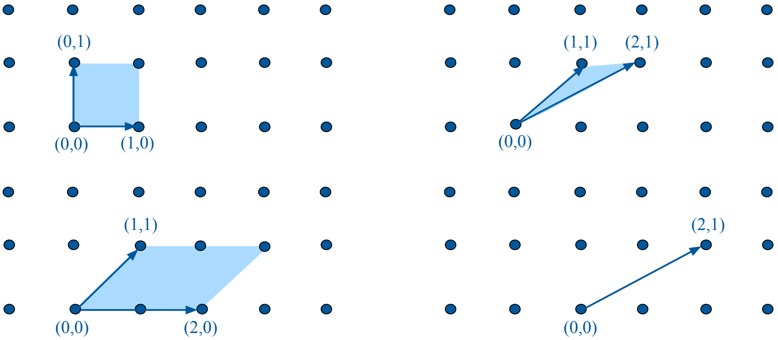
The fundamental parallelepiped of Λ with respect to B is defined as

$$P(B) := \{Bx | x \in [0,1)^r\}$$

Lattice notions

The fundamental parallelepiped of Λ with respect to B is defined as

$$P(B) := \{Bx | x \in [0,1)^r\}$$



Lemma Let Λ be a lattice of rank n and let $B = \{b_1, \ldots, b_n\}$ be n linearly independent vectors in Λ. Then, B is a base of Λ if and only if $P(B) \cap \Lambda = \{0\}$.

Lemma Let Λ be a lattice of rank n and let $B = \{b_1, \ldots, b_n\}$ be n linearly independent vectors in Λ. Then, B is a base of Λ if and only if $P(B) \cap \Lambda = \{0\}$.

Proof Suppose B a base of Λ.

Lemma Let Λ be a lattice of rank n and let $B = \{b_1, \ldots, b_n\}$ be n linearly independent vectors in Λ. Then, B is a base of Λ if and only if $P(B) \cap \Lambda = \{0\}$.

Proof Suppose B a base of Λ. By definition, Λ is the set of all integer combinations of B and $P(B)$ is the set of combinations of B with coefficients in $[0, 1)$. Then, $P(B) \cap \Lambda = \{0\}$.

Lemma Let Λ be a lattice of rank n and let $B = \{b_1, \ldots, b_n\}$ be n linearly independent vectors in Λ. Then, B is a base of Λ if and only if $P(B) \cap \Lambda = \{0\}$.

Proof Suppose B a base of Λ. By definition, Λ is the set of all integer combinations of B and $P(B)$ is the set of combinations of B with coefficients in $[0,1)$. Then, $P(B) \cap \Lambda = \{0\}$.

Suppose $P(B) \cap \Lambda = \{0\}$. Since Λ is of full rank and $b_1, \ldots, b_n$ are linearly independent then $x = \sum y_i b_i$ with $y_i \in \mathbb{R}$ for any $x \in \Lambda$.

Lemma Let Λ be a lattice of rank n and let $B = \{b_1, \ldots, b_n\}$ be n linearly independent vectors in Λ. Then, B is a base of Λ if and only if $P(B) \cap \Lambda = \{0\}$.

Proof Suppose B a base of Λ. By definition, Λ is the set of all integer combinations of B and $P(B)$ is the set of combinations of B with coefficients in $[0, 1)$. Then, $P(B) \cap \Lambda = \{0\}$.

Suppose $P(B) \cap \Lambda = \{0\}$. Since Λ is of full rank and $b_1, \ldots, b_n$ are linearly independent then $x = \sum y_i b_i$ with $y_i \in \mathbb{R}$ for any $x \in \Lambda$. Since Λ is closed under addition then

$$x' = \sum (y_i - \lfloor y_i \rfloor) b_i$$

belong to Λ.

Lemma Let Λ be a lattice of rank n and let $B = \{b_1, \ldots, b_n\}$ be n linearly independent vectors in Λ. Then, B is a base of Λ if and only if $P(B) \cap \Lambda = \{0\}$.

Proof Suppose B a base of Λ. By definition, Λ is the set of all integer combinations of B and $P(B)$ is the set of combinations of B with coefficients in $[0, 1)$. Then, $P(B) \cap \Lambda = \{0\}$.

Suppose $P(B) \cap \Lambda = \{0\}$. Since Λ is of full rank and $b_1, \ldots, b_n$ are linearly independent then $x = \sum y_i b_i$ with $y_i \in \mathbb{R}$ for any $x \in \Lambda$. Since Λ is closed under addition then

$$x' = \sum (y_i - \lfloor y_i \rfloor) b_i$$

belong to Λ. But, x' also belong to $P(B)$ and thus $x' = 0$, implying that $y_i - \lfloor y_i \rfloor = 0$ and thus all y_i are integers. Therefore, x is an integer combination of $b_1, \ldots, b_n$.

Lattice notions

The determinant of Λ, denoted by $\det(\Lambda)$, is defined as the volume of n-dimensionnel de $P(B)$, that is,

$$\det(\Lambda) := \sqrt{\det(B^T B)}.$$

Lattice notions

The determinant of Λ, denoted by $\det(\Lambda)$, is defined as the volume of n-dimensionnel de $P(B)$, that is,

$$\det(\Lambda) := \sqrt{\det(B^T B)}.$$

- When Λ is of full rank we have that B is an square matrix, and thus $\det(\Lambda) = |\det(B)|$.

Lattice notions

The determinant of Λ, denoted by $\det(\Lambda)$, is defined as the volume of n-dimensionnel de $P(B)$, that is,

$$\det(\Lambda) := \sqrt{\det(B^T B)}.$$

• When Λ is of full rank we have that B is an square matrix, and thus $\det(\Lambda) = |\det(B)|$.
• $\det(\Lambda)$ is well defined in the sense that it is independent of the choice of the base.

Lattice notions

The determinant of Λ, denoted by $\det(\Lambda)$, is defined as the volume of n-dimensionnel de $P(B)$, that is,

$$\det(\Lambda) := \sqrt{\det(B^T B)}.$$

- When Λ is of full rank we have that B is an square matrix, and thus $\det(\Lambda) = |\det(B)|$.
- $\det(\Lambda)$ is well defined in the sense that it is independent of the choice of the base.
- $\det(\Lambda)$ is proportionally inverse to its density : smaller is the determinant denser will be the lattice.

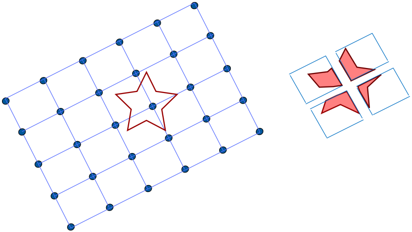
Blichfeldt's theorem

Theorem Let Λ be a lattice generated by a base B and let $S \subseteq span(B)$. If $vol(S) > \det(\Lambda)$ then there are $z_1, z_2 \in S$ such that $z_1 - z_2 \in \Lambda$.

Blichfeldt's theorem

Theorem Let Λ be a lattice generated by a base B and let $S \subseteq span(B)$. If $vol(S) > \det(\Lambda)$ then there are $z_1, z_2 \in S$ such that $z_1 - z_2 \in \Lambda$.

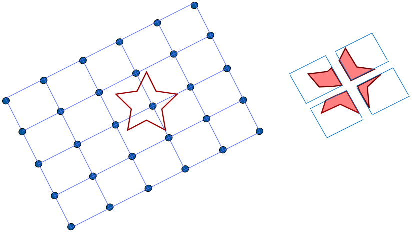
Proof Consider $S_x = S \cap (x + P(B))$ with $x \in \Lambda$. They are pairwise disjoint and $S = \bigcup_{x \in \Lambda} S_x$.



Blichfeldt's theorem

Theorem Let Λ be a lattice generated by a base B and let $S \subseteq span(B)$. If $vol(S) > \det(\Lambda)$ then there are $z_1, z_2 \in S$ such that $z_1 - z_2 \in \Lambda$.

Proof Consider $S_x = S \cap (x + P(B))$ with $x \in \Lambda$. They are pairwise disjoint and $S = \bigcup\limits_{x \in \Lambda} S_x$.



In particular we have $vol(S) = \sum\limits_{x \in \Lambda} vol(S_x)$.

Notice that $S_x - x = (S - x) \cap P(B)$ are all contained in $P(B)$.

Notice that $S_x - x = (S - x) \cap P(B)$ are all contained in $P(B)$. From $vol(S_x) = vol(S_x - x)$ we obtain

$$vol(P(B)) = \det(\Lambda) < vol(S) = \sum_{x \in \Lambda} vol(S_x) = \sum_{x \in \Lambda} vol(S_x - x)$$

Notice that $S_x - x = (S - x) \cap P(B)$ are all contained in $P(B)$.
From $vol(S_x) = vol(S_x - x)$ we obtain

$$vol(P(B)) = \det(\Lambda) < vol(S) = \sum_{x \in \Lambda} vol(S_x) = \sum_{x \in \Lambda} vol(S_x - x)$$

Since $S_x - x \subseteq P(B)$ and $\sum_{x \in \Lambda} vol(S_x - x) > vol(P(B))$ then there exist $x \neq y \in \Lambda$ such that $(S_x - x) \cap (S_y - y) \neq 0$.

Notice that $S_x - x = (S - x) \cap P(B)$ are all contained in $P(B)$.
From $vol(S_x) = vol(S_x - x)$ we obtain

$$vol(P(B)) = \det(\Lambda) < vol(S) = \sum_{x \in \Lambda} vol(S_x) = \sum_{x \in \Lambda} vol(S_x - x)$$

Since $S_x - x \subseteq P(B)$ and $\sum_{x \in \Lambda} vol(S_x - x) > vol(P(B))$ then there exist $x \neq y \in \Lambda$ such that $(S_x - x) \cap (S_y - y) \neq 0$.
Let $z \in (S_x - x) \cap (S_y - y)$ and define

$$z_1 = z + x \in S_x \subseteq S \text{ and } z_2 = z + y \in S_y \subseteq S.$$

These vectors satisfy $z_1 - z_2 = x - y \in \Lambda$.

Minkowski's convex body theorem

Theorem Let Λ be a full dimensional lattice. If $S \subset \mathbb{R}^n$ is a symmetric convex body with $vol(S) > 2^n \det(\Lambda)$ then S contains a nonzero lattice point.

Minkowski's convex body theorem

Theorem Let Λ be a full dimensional lattice. If $S \subset \mathbb{R}^n$ is a symmetric convex body with $vol(S) > 2^n \det(\Lambda)$ then S contains a nonzero lattice point.

Proof Consider $S/2 = \{x : 2x \in S\}$. The volume of $S/2$ satisfies

$$vol(S/2) = 2^{-n} vol(S) > \det(\Lambda)$$

Minkowski's convex body theorem

Theorem Let Λ be a full dimensional lattice. If $S \subset \mathbb{R}^n$ is a symmetric convex body with $vol(S) > 2^n \det(\Lambda)$ then S contains a nonzero lattice point.

Proof Consider $S/2 = \{x : 2x \in S\}$. The volume of $S/2$ satisfies

$$vol(S/2) = 2^{-n} vol(S) > \det(\Lambda)$$

By Blichfeldt theorem there exist $z_1, z_2 \in S/2$ such that $z_1 - z_2 \in \Lambda \setminus \{0\}$.

Minkowski's convex body theorem

Theorem Let Λ be a full dimensional lattice. If $S \subset \mathbb{R}^n$ is a symmetric convex body with $vol(S) > 2^n \det(\Lambda)$ then S contains a nonzero lattice point.

Proof Consider $S/2 = \{x : 2x \in S\}$. The volume of $S/2$ satisfies

$$vol(S/2) = 2^{-n} vol(S) > \det(\Lambda)$$

By Blichfeldt theorem there exist $z_1, z_2 \in S/2$ such that $z_1 - z_2 \in \Lambda \setminus \{0\}$. We thus have $2z_1, 2z_2 \in S$ and, by symmetry, we also have $-2z_2 \in S$.

Minkowski's convex body theorem

Theorem Let Λ be a full dimensional lattice. If $S \subset \mathbb{R}^n$ is a symmetric convex body with $vol(S) > 2^n \det(\Lambda)$ then S contains a nonzero lattice point.

Proof Consider $S/2 = \{x : 2x \in S\}$. The volume of $S/2$ satisfies

$$vol(S/2) = 2^{-n} vol(S) > \det(\Lambda)$$

By Blichfeldt theorem there exist $z_1, z_2 \in S/2$ such that $z_1 - z_2 \in \Lambda \setminus \{0\}$. We thus have $2z_1, 2z_2 \in S$ and, by symmetry, we also have $-2z_2 \in S$. Moreover, by convexity,

$$z_1 - z_2 = \frac{2z_1 - 2z_2}{2} \in S$$

is a non-zero lattice point vector contained in S.

Integer points and volume

Theorem Let K be a convex in $\mathbb{R}^n$ containing 0 and such that $K \cap \mathbb{Z}^n$ is not included in a hyperplan. Then, $Card(K \cap \mathbb{Z}^n) \leq n + n! vol(K)$.

Integer points and volume

Theorem Let K be a convex in $\mathbb{R}^n$ containing 0 and such that $K \cap \mathbb{Z}^n$ is not included in a hyperplan. Then,
$Card(K \cap \mathbb{Z}^n) \leq n + n! vol(K)$.

Proof Let $k = Card(K \cap \mathbb{Z}^n) - n$. The result follows if $k \leq 0$.
Suppose that $k \geq 1$.

Integer points and volume

Theorem Let K be a convex in $\mathbb{R}^n$ containing 0 and such that $K \cap \mathbb{Z}^n$ is not included in a hyperplan. Then, $Card(K \cap \mathbb{Z}^n) \leq n + n! vol(K)$.

Proof Let $k = Card(K \cap \mathbb{Z}^n) - n$. The result follows if $k \leq 0$. Suppose that $k \geq 1$.

We may find a simplex S_0 with $n+1$ integer vertices contained in K without integer points in its interior and thus $vol(S_0) = 1/n!$

Integer points and volume

Theorem Let K be a convex in $\mathbb{R}^n$ containing 0 and such that $K \cap \mathbb{Z}^n$ is not included in a hyperplan. Then, $Card(K \cap \mathbb{Z}^n) \leq n + n!vol(K)$.

Proof Let $k = Card(K \cap \mathbb{Z}^n) - n$. The result follows if $k \leq 0$. Suppose that $k \geq 1$.

We may find a simplex S_0 with $n+1$ integer vertices contained in K without integer points in its interior and thus $vol(S_0) = 1/n!$

Among the rest $k-1$ integer points in K, we pick the closest to S_0, say x_1.

Integer points and volume

Let S_1 be the simplexe generated by x_1 and the closest face of S_0 to x_1. We also have $vol(S_1) = 1/n!$.

Integer points and volume

Let S_1 be the simplexe generated by x_1 and the closest face of S_0 to x_1. We also have $vol(S_1) = 1/n!$.

We carry on this way to construct k simplex S_j, obtaining

$$vol(K) \geq \sum_{i=0}^{k-1} vol(S_i) = k/n!$$

Therefore

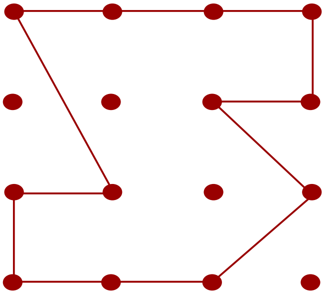
$$Card(K \cap \mathbb{Z}^n) \leq n + n!vol(K).$$

Pick's theorem

An integer polytope $P \subset \mathbb{R}^2$ is a polygon (not necessarily convex) with vertices in $\mathbb{Z}^2$.

Pick's theorem

An integer polytope $P \subset \mathbb{R}^2$ is a polygon (not necessarily convex) with vertices in $\mathbb{Z}^2$.



Pick's theorem

Theorem Let P be an integer polygon containing I integer points in its interior and B integer points on the frontier, $B \geq 3$. Then,

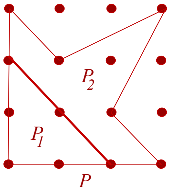
$$Area(P) = I + \frac{B}{2} - 1.$$

Pick's theorem

Theorem Let P be an integer polygon containing I integer points in its interior and B integer points on the frontier, $B \geq 3$. Then,

$$Area(P) = I + \frac{B}{2} - 1.$$

Proof (idea) Decompose P and use induction.



Let P be an integer polygon. By using Pick's theorem we obtain

$$Card(P \cap \mathbb{Z}^2) = 2vol(P) + 2$$

Let P be an integer polygon. By using Pick's theorem we obtain

$$Card(P \cap \mathbb{Z}^2) = 2vol(P) + 2$$

Theorem (Scott) Let $k \neq 0$ be the number of interior points of P then

$$Card(P \cap \mathbb{Z}^2) \leq 3k + 6$$

except if P is equivalent to a triangle with vertices $(0,0),(3,0),(0,3)$.

Theorem (Hensley) There exists a constant $B(n,k)$ depending only on k and n such that for any n-dimensional polytope P having exactly k integer points in its interior we have

$$vol(P) \leq B(n,k).$$

Theorem (Hensley) There exists a constant $B(n, k)$ depending only on k and n such that for any n-dimensional polytope P having exactly k integer points in its interior we have

$$vol(P) \leq B(n, k).$$

It is known that

$$B(n, k) \approx k(7(k+1))n2^n + 1.$$

Reeve's exemple

Can we generalise Pick's theorem ? Can we compute volume of 3-polytope by counting integers points ?

Reeve's exemple

Can we generalise Pick's theorem ? Can we compute volume of 3-polytope by counting integers points ? NO

Reeve's exemple

Can we generalise Pick's theorem ? Can we compute volume of 3-polytope by counting integers points ? NO

Example Let T_h be the tetrahedra with vertices $a = (0, 0, 0), b = (1, 0, 0), c = (0, 1, 0)$ et $d = (1, 1, h)$, $h \in \mathbb{Z}_{>0}$.

Reeve's exemple

Can we generalise Pick's theorem ? Can we compute volume of 3-polytope by counting integers points ? NO

Example Let T_h be the tetrahedra with vertices $a = (0,0,0), b = (1,0,0), c = (0,1,0)$ et $d = (1,1,h),\ h \in \mathbb{Z}_{>0}$.
We have

$$vol(T_h) = \frac{1}{3} \times \text{base} \times \text{heigh} = h/6.$$

Reeve's exemple

Can we generalise Pick's theorem ? Can we compute volume of 3-polytope by counting integers points ? NO

Example Let T_h be the tetrahedra with vertices $a=(0,0,0), b=(1,0,0), c=(0,1,0)$ et $d=(1,1,h)$, $h \in \mathbb{Z}_{>0}$.
We have

$$vol(T_h) = \frac{1}{3} \times \text{base} \times \text{heigh} = h/6.$$

Moreover, the only integer points in T_h are its 4 vertices.
Therefore, T_h only admits 4 integer points but the volume grows arbitrairily big as $h \to \infty$.

Ehrhart theory

An integer polytope $P \subset \mathbb{R}^d$ is a convex hull of a finite set of points in $\mathbb{Z}^d$.

Ehrhart theory

An integer polytope $P \subset \mathbb{R}^d$ is a convex hull of a finite set of points in $\mathbb{Z}^d$.
Let $k \in \mathbb{N}$. We define the k-dilation of P, as

$$kP := \{kx \mid x \in P\}.$$

Ehrhart theory

An integer polytope $P \subset \mathbb{R}^d$ is a convex hull of a finite set of points in $\mathbb{Z}^d$.
Let $k \in \mathbb{N}$. We define the k-dilation of P, as

$$kP := \{kx \mid x \in P\}.$$

For $k \in \mathbb{N}$, let

$$L_P(k) := \#(kP \cap \mathbb{Z}^d)$$

Ehrhart theory

The first investigations of $L_P(k)$ date back to the 1960's work of Ehrhart. As a lycée teacher he did many of his investigations as an amateur mathematician.

Eugène Ehrhart (1906-2000)

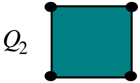
Ehrhart theory

Example

$Q_2 = conv\{(0,0),(1,0),(0,1),(1,1)\} = \{x, y \in \mathbb{R} : 0 \leq x, y \leq 1\}.$

Example

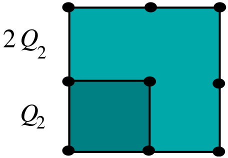
$Q_2 = conv\{(0,0),(1,0),(0,1),(1,1)\} = \{x, y \in \mathbb{R} : 0 \leq x, y \leq 1\}.$



k	1
$L_{Q_2}(k)$	4

Example

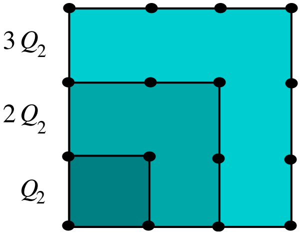
$Q_2 = conv\{(0,0),(1,0),(0,1),(1,1)\} = \{x, y \in \mathbb{R} : 0 \leq x, y \leq 1\}.$



k	1	2
$L_{Q_2}(k)$	4	9

Example

$Q_2 = conv\{(0,0),(1,0),(0,1),(1,1)\} = \{x, y \in \mathbb{R} : 0 \le x, y \le 1\}.$

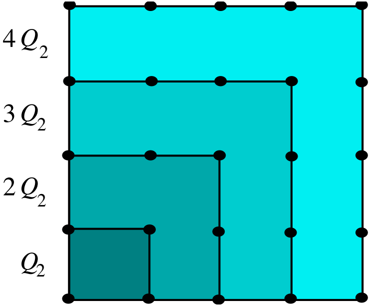


k	1	2	3
$L_{Q_2}(k)$	4	9	16

Ehrhart theory

Example

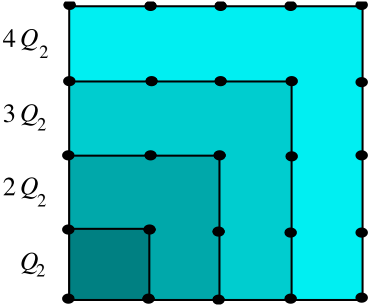
$Q_2 = conv\{(0,0),(1,0),(0,1),(1,1)\} = \{x, y \in \mathbb{R} : 0 \leq x, y \leq 1\}.$



k	1	2	3	4
$L_{Q_2}(k)$	4	9	16	25

Example

$Q_2 = conv\{(0,0),(1,0),(0,1),(1,1)\} = \{x, y \in \mathbb{R} : 0 \leq x, y \leq 1\}$.



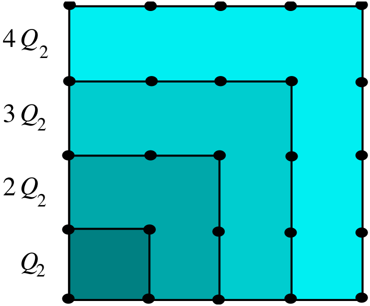
k	1	2	3	4
$L_{Q_2}(k)$	4	9	16	25

$\mathbf{L_{Q_2}(k) = (k+1)^2}$

Ehrhart theory

Example

$Q_2 = conv\{(0,0),(1,0),(0,1),(1,1)\} = \{x, y \in \mathbb{R} : 0 \leq x, y \leq 1\}$.



k	1	2	3	4
$L_{Q_2}(k)$	4	9	16	25

$\mathbf{L_{Q_2}(k) = (k+1)^2}$

***d*-dimensional cube :** $L_{Q_d}(k) = (k+1)^d = \sum_{i=0}^{d} \binom{d}{i} k^i$

Ehrhart polynomial

Theorem (Ehrhart 1962) Let P be an integer polytope. Then, $L_P(k)$ is a polynomial on k of degree $dim(P)$ with rational coefficients and constante term equals 1.

Ehrhart polynomial

Theorem (Ehrhart 1962) Let P be an integer polytope. Then, $L_P(k)$ is a polynomial on k of degree $dim(P)$ with rational coefficients and constante term equals 1.

Proof Let S be a simplex with vertices $0, s_1, \ldots, s_r$.

The set mS is the disjoint union of

$$S_{m,j} = \left\{ \lambda_1 s_1 + \cdots + \lambda_r s_r \mid \lambda_i \geq 0, \sum_{i=1}^{r} \lambda_i \leq m, \sum_{i=1}^{r} \lfloor \lambda_i \rfloor = m - j \right\}$$

for each $j \in \{0, \ldots, m\}$.

Ehrhart polynomial

The number of points in $S_{m,j}$ is given by the number of positive integer solutions to $\sum_{i=1}^{r} x_i = m - j$

Ehrhart polynomial

The number of points in $S_{m,j}$ is given by the number of positive integer solutions to $\sum_{i=1}^{r} x_i = m - j$
which is given by $\binom{m-j+r-1}{r-1} \times$ the number of integer points in

$$a_j = \left\{ \beta_1 s_1 + \cdots + \beta_r s_r \mid 0 \leq \beta_i < 1, \ \sum_{i=1}^{r} \beta_i \leq j \right\}.$$

Ehrhart polynomial

Since $a_j = a_r$ for all $j \geq r$, we have

$$
\begin{aligned}
Card(mS \cap \mathbb{Z}^n) &= \sum_{j=0}^{m} a_j \binom{m-j+r-1}{r-1} \\
&= \sum_{j=0}^{r-1} a_j \binom{m-j+r-1}{r-1} + a_r \sum_{j=r}^{m} \binom{m-j+r-1}{r-1} \\
&= \sum_{j=0}^{r-1} (a_j - a_r) \binom{m-j+r-1}{r-1} + a_r \sum_{j=0}^{m} \binom{m-j+r-1}{r-1} \\
&= \sum_{j=0}^{r-1} (a_j - a_r) \binom{m-j+r-1}{r-1} + a_r \binom{m+r}{r}.
\end{aligned}
$$

Ehrhart polynomial

Since $a_j = a_r$ for all $j \geq r$, we have

$$\begin{aligned}
Card(mS \cap \mathbb{Z}^n) &= \sum_{j=0}^{m} a_j \binom{m-j+r-1}{r-1} \\
&= \sum_{j=0}^{r-1} a_j \binom{m-j+r-1}{r-1} + a_r \sum_{j=r}^{m} \binom{m-j+r-1}{r-1} \\
&= \sum_{j=0}^{r-1} (a_j - a_r) \binom{m-j+r-1}{r-1} + a_r \sum_{j=0}^{m} \binom{m-j+r-1}{r-1} \\
&= \sum_{j=0}^{r-1} (a_j - a_r) \binom{m-j+r-1}{r-1} + a_r \binom{m+r}{r}.
\end{aligned}$$

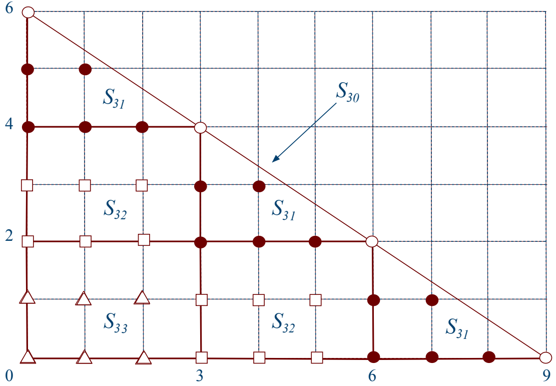
Therefore, $Card(mP \cap \mathbb{Z}^n)$ is a polynomial function on m of degree r and its value is equals 1 when $m = 0$. Moreover, its leading term is equals $\frac{1}{r!} a_r$.

Example

Triangle S with vertices $(0,0),(3,0)$, $(0,2)$ and take $m=6$.

Example

Triangle S with vertices $(0,0), (3,0)$, $(0,2)$ and take $m = 6$.



Decomposition of S in $S_{m,j}$. Points marked with $\circ, \bullet, \square, \triangle$ correspond to solutions of a_0, a_1, a_2 and a_3 respectively.

Example

$$
\begin{aligned}
L_S(m) &= \sum_{j=0}^{1}(a_j - a_2)\binom{m-j+2-1}{2-1} + a_2\binom{m+2}{2} \\
&= (a_0 - a_2)\binom{m+1}{1} + (a_1 - a_2)\binom{m}{1} + a_2\binom{m+2}{2} \\
&= (1-6)(m+1) + (5-6)m + 6\frac{(m+2)(m+1)}{2} \\
&= -5m - 5 - m + 3m^2 + 3m + 6m + 6 \\
&= 3m^2 + 3m + 1.
\end{aligned}
$$

Reciprocity law

Let P° denotes the interior of P.

Reciprocity law

Let P° denotes the interior of P.

Example : $L_{Q_d^\circ}(k) = (k-1)^d$

Reciprocity law

Let P° denotes the interior of P.

Example : $L_{Q_d^\circ}(k) = (k-1)^d = (-1)^d(1-k)^d$

Reciprocity law

Let P° denotes the interior of P.

Example : $L_{Q_d^\circ}(k) = (k-1)^d = (-1)^d(1-k)^d = (-1)^d L_{Q_d}(-k)$

Let P° denotes the interior of P.

Example : $L_{Q_d^\circ}(k) = (k-1)^d = (-1)^d(1-k)^d = (-1)^d L_{Q_d}(-k)$

Theorem (Macdonald 1971) $L_P(-k) = (-1)^{dim(P)} L_{P^\circ}(k)$.

Reciprocity law

Let P° denotes the interior of P.

Example : $L_{Q_d^\circ}(k) = (k-1)^d = (-1)^d(1-k)^d = (-1)^d L_{Q_d}(-k)$

Theorem (Macdonald 1971) $L_P(-k) = (-1)^{dim(P)} L_{P^\circ}(k)$.

Proof If P is a r-simplex, we just verify the formula.

Reciprocity law

Let P° denotes the interior of P.

Example : $L_{Q_d^\circ}(k) = (k-1)^d = (-1)^d(1-k)^d = (-1)^d L_{Q_d}(-k)$

Theorem (Macdonald 1971) $L_P(-k) = (-1)^{dim(P)} L_{P^\circ}(k)$.

Proof If P is a r-simplex, we just verify the formula.

If P is not a simplex with $dim(P) = r$ then there exists vertex s of P such that $Q = conv(P \setminus \{s\})$ is an integer polytope with $dim(P) = r$.

Reciprocity law

Let P° denotes the interior of P.

Example : $L_{Q_d^\circ}(k) = (k-1)^d = (-1)^d(1-k)^d = (-1)^d L_{Q_d}(-k)$

Theorem (Macdonald 1971) $L_P(-k) = (-1)^{dim(P)} L_{P^\circ}(k)$.

Proof If P is a r-simplex, we just verify the formula.

If P is not a simplex with $dim(P) = r$ then there exists vertex s of P such that $Q = conv(P \setminus \{s\})$ is an integer polytope with $dim(P) = r$.

We have thus that one facet F of Q separate s from Q.

Reciprocity law

Let $R = conv(\{s\} \cup F)$.

Reciprocity law

Let $R = conv(\{s\} \cup F)$. We have

$$L_P(m) = L_Q(m) + L_R(m) - L_F(m) \text{ and}$$

$$L_{P^\circ}(m) = L_{Q^\circ}(m) + L_{R^\circ}(m) + L_{F^\circ}(m).$$

Reciprocity law

Let $R = conv(\{s\} \cup F)$. We have

$$L_P(m) = L_Q(m) + L_R(m) - L_F(m) \text{ and}$$

$$L_{P^\circ}(m) = L_{Q^\circ}(m) + L_{R^\circ}(m) + L_{F^\circ}(m).$$

By induction on the number of vertices, we obtain

$$\begin{aligned} L_{P^\circ}(m) &= L_{Q^\circ}(m) + L_{R^\circ}(m) + L_{F^\circ}(m) \\ &= (-1)^r L_Q(-m) + (-1)^r L_R(-m) + (-1)^{r-1} L_F(-m) \\ &= (-1)^r (L_Q(-m) + L_R(-m) - L_F(-m)) \\ &= (-1)^r L_P(-m). \end{aligned}$$

Some coefficients

Proposition Let P be an integer polytope of dimension d in $\mathbb{R}^d$ and let $c_d t^d + c_{d-1} t^{d-1} + \cdots + c_0$ be its Ehrhart polynomial. Then,

$$c_d = vol_d(P) \text{ and } c_{d-1} = \frac{1}{2} \sum_{F \subset P} vol_{d-1}(F).$$

Some coefficients

Proposition Let P be an integer polytope of dimension d in $\mathbb{R}^d$ and let $c_d t^d + c_{d-1} t^{d-1} + \cdots + c_0$ be its Ehrhart polynomial. Then,

$$c_d = vol_d(P) \text{ and } c_{d-1} = \frac{1}{2} \sum_{F \subset P} vol_{d-1}(F).$$

Proof [first equality]

- $vol(P)$ can be computed by approximating P with d-dimensional cubes which get smaller and smaller.

Some coefficients

Proposition Let P be an integer polytope of dimension d in $\mathbb{R}^d$ and let $c_d t^d + c_{d-1} t^{d-1} + \cdots + c_0$ be its Ehrhart polynomial. Then,

$$c_d = vol_d(P) \text{ and } c_{d-1} = \frac{1}{2} \sum_{F \subset P} vol_{d-1}(F).$$

Proof [first equality]

- $vol(P)$ can be computed by approximating P with d-dimensional cubes which get smaller and smaller.
- Consider cubes of side $1/t$ (and thus of volume $\frac{1}{t^d}$).

Some coefficients

Proposition Let P be an integer polytope of dimension d in $\mathbb{R}^d$ and let $c_d t^d + c_{d-1} t^{d-1} + \cdots + c_0$ be its Ehrhart polynomial. Then,

$$c_d = vol_d(P) \text{ and } c_{d-1} = \frac{1}{2} \sum_{F \subset P} vol_{d-1}(F).$$

Proof [first equality]

- $vol(P)$ can be computed by approximating P with d-dimensional cubes which get smaller and smaller.
- Consider cubes of side $1/t$ (and thus of volume $\frac{1}{t^d}$).
- The vertices of these cubes can be thought in $(\frac{1}{t}\mathbb{Z})^d$.

Some coefficients

Proposition Let P be an integer polytope of dimension d in $\mathbb{R}^d$ and let $c_d t^d + c_{d-1} t^{d-1} + \cdots + c_0$ be its Ehrhart polynomial. Then,

$$c_d = vol_d(P) \text{ and } c_{d-1} = \frac{1}{2} \sum_{F \subset P} vol_{d-1}(F).$$

Proof [first equality]

- $vol(P)$ can be computed by approximating P with d-dimensional cubes which get smaller and smaller.
- Consider cubes of side $1/t$ (and thus of volume $\frac{1}{t^d}$).
- The vertices of these cubes can be thought in $(\frac{1}{t}\mathbb{Z})^d$.
- The volume can be approximated by counting theses cubes or, equivalently, the integer points in $(\frac{1}{t}\mathbb{Z})^d$.

Some coefficients

$$vol(P) = \lim_{t \to \infty} \frac{1}{t^d} \cdot Card\left(P \cap \left(\frac{1}{t}\mathbb{Z}\right)^d\right).$$

Some coefficients

$$vol(P) = \lim_{t\to\infty} \frac{1}{t^d} \cdot Card\left(P \cap \left(\frac{1}{t}\mathbb{Z}\right)^d\right).$$

But

$$Card\left(P \cap \left(\frac{1}{t}\mathbb{Z}\right)^d\right) = Card(tP \cap \mathbb{Z}^d),$$

and thus

$$vol(P) = \lim_{t\to\infty} \frac{1}{t^d} \cdot Card(tP \cap \mathbb{Z}^d).$$

Some coefficients

$$vol(P) = \lim_{t\to\infty} \frac{1}{t^d} \cdot Card\left(P \cap \left(\frac{1}{t}\mathbb{Z}\right)^d\right).$$

But

$$Card\left(P \cap \left(\frac{1}{t}\mathbb{Z}\right)^d\right) = Card(tP \cap \mathbb{Z}^d),$$

and thus

$$vol(P) = \lim_{t\to\infty} \frac{1}{t^d} \cdot Card(tP \cap \mathbb{Z}^d).$$

Obtaining

$$vol(P) = \lim_{t\to\infty} \frac{c_d t^d + c_{d-1} t^{d-1} + \cdots + c_0}{t^d} = c_d.$$

Some coefficients

[second equality] By the reciprocity law, we have

$$L_{P^\circ}(t) = a_d t^d - a_{d-1} t^{d-1} + \cdots .$$

Therefore,

$$\lim_{t\to\infty} t^{-d}(L_P(t) - L_{P^\circ}(t)) = 2a_{d-1}.$$

Some coefficients

[second equality] By the reciprocity law, we have

$$L_{P^\circ}(t) = a_d t^d - a_{d-1} t^{d-1} + \cdots .$$

Therefore,

$$\lim_{t\to\infty} t^{-d}(L_P(t) - L_{P^\circ}(t)) = 2a_{d-1}.$$

But $P \setminus P^\circ$ is the union of the $(d-1)$-faces of P (with relative interiors pairwise disjoint)

Some coefficients

[second equality] By the reciprocity law, we have

$$L_{P^\circ}(t) = a_d t^d - a_{d-1} t^{d-1} + \cdots .$$

Therefore,

$$\lim_{t\to\infty} t^{-d}(L_P(t) - L_{P^\circ}(t)) = 2a_{d-1}.$$

But $P \setminus P^\circ$ is the union of the $(d-1)$-faces of P (with relative interiors pairwise disjoint)

Thus,

$$\lim_{t\to\infty} t^{-d}(L_P(t) - L_{P^\circ}(t)) = \sum_{F\subset P} vol_{d-1}(F).$$

and the equality follows by same arguments as above.

Relative affine volume

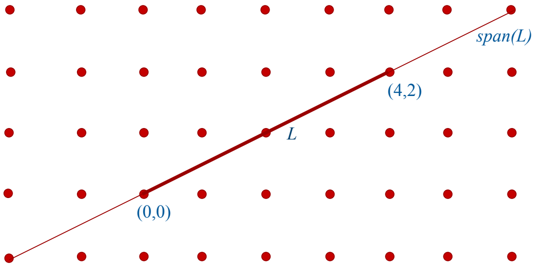
Let $S \subset \mathbb{R}^d$ of dimension $m < d$. As before, we can compute the volume with respect to the induced sublattice of $span(S) \cap \mathbb{Z}^d$.

Relative affine volume

Let $S \subset \mathbb{R}^d$ of dimension $m < d$. As before, we can compute the volume with respect to the induced sublattice of $span(S) \cap \mathbb{Z}^d$.
Example The segment L joining $(0,0)$ et $(4,2)$ in $\mathbb{R}^2$ has relative volume 2 since in the $span(L) = \{(x,y) \in \mathbb{R}^2 : y = x/2\}$ L is covered by two unit segments in the affine space.

Relative affine volume

Let $S \subset \mathbb{R}^d$ of dimension $m < d$. As before, we can compute the volume with respect to the induced sublattice of $span(S) \cap \mathbb{Z}^d$.
Example The segment L joining $(0,0)$ et $(4,2)$ in $\mathbb{R}^2$ has relative volume 2 since in the $span(L) = \{(x,y) \in \mathbb{R}^2 : y = x/2\}$ L is covered by two unit segments in the affine space.



Low dimension

$n = 1$ An interval $[p, q]$. It contains $q - p + 1$ integer points

$$L_P(m) = mq - mp + 1,$$
$$L_{P^\circ}(m) = mq - mp - 1 = -L_P(-m).$$

Low dimension

$n = 1$ An interval $[p, q]$. It contains $q - p + 1$ integer points

$$L_P(m) = mq - mp + 1,$$
$$L_{P^\circ}(m) = mq - mp - 1 = -L_P(-m).$$

$n = 2$ (Pick's theorem) Polygon P in $\mathbb{R}^2$. We have

$$Area(P) = I(P) + \frac{1}{2}B(P) - 1$$

Low dimension

$n = 1$ An interval $[p, q]$. It contains $q - p + 1$ integer points

$$L_P(m) = mq - mp + 1,$$
$$L_{P^\circ}(m) = mq - mp - 1 = -L_P(-m).$$

$n = 2$ (Pick's theorem) Polygon P in $\mathbb{R}^2$. We have

$$Area(P) = I(P) + \frac{1}{2}B(P) - 1$$

Let k be an integer. We have $Area(kP) = k^2 Area(P)$ and $B(kP) = kB(P)$. Obtaining

$$L_P(k) = Area(P)k^2 + \frac{1}{2}B(P)k + 1$$

Low dimension

$n = 1$ An interval $[p, q]$. It contains $q - p + 1$ integer points

$$L_P(m) = mq - mp + 1,$$
$$L_{P^\circ}(m) = mq - mp - 1 = -L_P(-m).$$

$n = 2$ (Pick's theorem) Polygon P in $\mathbb{R}^2$. We have

$$Area(P) = I(P) + \frac{1}{2}B(P) - 1$$

Let k be an integer. We have $Area(kP) = k^2 Area(P)$ and $B(kP) = kB(P)$. Obtaining

$$L_P(k) = Area(P)k^2 + \frac{1}{2}B(P)k + 1$$

$n = 3$ None of the coefficients a_i can be expressed in terms of $\sum_{F \subset P} vol_k(F)$. a_k is a linear combination of the $vol_k(F)$.

Voting theory

There are many types of voting systems :

Plurality **V**oting : the candidate with most votes wins the elections.

Voting theory

There are many types of voting systems :

Plurality **V**oting : the candidate with most votes wins the elections.

Plurality **R**unoff **V**oting : the candidate most obtain an absolute majority. If no candidate gets more than 50% of votes a second round of elections is held with only two candidates, those who had the highest plurality scores in the first round. The candidate with the absolute majority in the second round wins the elections.

Voting theory

There are many types of voting systems :

Plurality **V**oting : the candidate with most votes wins the elections.

Plurality **R**unoff **V**oting : the candidate most obtain an absolute majority. If no candidate gets more than 50% of votes a second round of elections is held with only two candidates, those who had the highest plurality scores in the first round. The candidate with the absolute majority in the second round wins the elections.
Will PV yield another candidate as winner as PRV for a given voting situation ?And if so, what is the probability of this happening ?

Voting theory

Consider an election on three candidates $\{a, b, c\}$. Assume that voters have complete linear preference ranking on these candidates.

Voting theory

Consider an election on three candidates $\{a, b, c\}$. Assume that voters have complete linear preference ranking on these candidates. There are 6 possible preferences orders :

$$abc,\ acb,\ bac,\ bca,\ cab,\ cba$$

In order to compute the probability that some event takes place, we assume that all voting situation is equally likely to occur (called Impartial Anonymous Culture condition).
Suppose that a voting situation occurs where PV will denote a as winner while PRV will claim that b has won.

$n_{abc} + n_{acb} > n_{bac} + n_{bca}$	a beats b
$n_{bac} + n_{bca} > n_{cab} + n_{cba}$	b beats c
$n_{abc} + n_{acb} + n_{cab} < N/2$	a loses the second round
$n_{abc} + n_{acb} + n_{bac} + n_{bca} + n_{cab} + n_{cba} = N$	all votes add up N
$n_i \geq 0$	for all $i \in S_{abc}$

$n_{abc} + n_{acb} > n_{bac} + n_{bca}$ — a beats b

$n_{bac} + n_{bca} > n_{cab} + n_{cba}$ — b beats c

$n_{abc} + n_{acb} + n_{cab} < N/2$ — a loses the second round

$n_{abc} + n_{acb} + n_{bac} + n_{bca} + n_{cab} + n_{cba} = N$ — all votes add up N

$n_i \geq 0$ — for all $i \in S_{abc}$

- The first two inequalities say that in the first round a has the most votes, then b and c has the least votes

$n_{abc} + n_{acb} > n_{bac} + n_{bca}$ — a beats b

$n_{bac} + n_{bca} > n_{cab} + n_{cba}$ — b beats c

$n_{abc} + n_{acb} + n_{cab} < N/2$ — a loses the second round

$n_{abc} + n_{acb} + n_{bac} + n_{bca} + n_{cab} + n_{cba} = N$ — all votes add up N

$n_i \geq 0$ — for all $i \in S_{abc}$

- The first two inequalities say that in the first round a has the most votes, then b and c has the least votes
- The second equality represent the second round. Here, candidate c does not participate anymore, that means that the voters with preferences cab and cba will vote for their second choice. Therefore cab would vote for a, as will abc and acb and so $n_{abc} + n_{acb} + n_{cab} < N/2$

$n_{abc} + n_{acb} > n_{bac} + n_{bca}$ — a beats b

$n_{bac} + n_{bca} > n_{cab} + n_{cba}$ — b beats c

$n_{abc} + n_{acb} + n_{cab} < N/2$ — a loses the second round

$n_{abc} + n_{acb} + n_{bac} + n_{bca} + n_{cab} + n_{cba} = N$ — all votes add up N

$n_i \geq 0$ — for all $i \in S_{abc}$

- The first two inequalities say that in the first round a has the most votes, then b and c has the least votes
- The second equality represent the second round. Here, candidate c does not participate anymore, that means that the voters with preferences cab and cba will vote for their second choice. Therefore cab would vote for a, as will abc and acb and so $n_{abc} + n_{acb} + n_{cab} < N/2$
- The fourth inequality represents the total number of voters.

$n_{abc} + n_{acb} > n_{bac} + n_{bca}$	a beats b
$n_{bac} + n_{bca} > n_{cab} + n_{cba}$	b beats c
$n_{abc} + n_{acb} + n_{cab} < N/2$	a loses the second round
$n_{abc} + n_{acb} + n_{bac} + n_{bca} + n_{cab} + n_{cba} = N$	all votes add up N
$n_i \geq 0$	for all $i \in S_{abc}$

- The first two inequalities say that in the first round a has the most votes, then b and c has the least votes
- The second equality represent the second round. Here, candidate c does not participate anymore, that means that the voters with preferences cab and cba will vote for their second choice. Therefore cab would vote for a, as will abc and acb and so $n_{abc} + n_{acb} + n_{cab} < N/2$
- The fourth inequality represents the total number of voters.
- The last makes sure that the number people with certain preference is not negative.

• The vote problem is thus represented by a finite set of linear inequalities, that is, by a polyhedron P_d (d for disagreement).

• The vote problem is thus represented by a finite set of linear inequalities, that is, by a polyhedron P_d (d for disagreement).
• By leaving out the first three inequalities this yield to a polyhedron P_t (t for total) - all possible voting outcomes.

• The vote problem is thus represented by a finite set of linear inequalities, that is, by a polyhedron P_d (d for disagreement).

• By leaving out the first three inequalities this yield to a polyhedron P_t (t for total) - all possible voting outcomes.

• By the IAC condition any of these voting situation is evenly likely to occur.

- The vote problem is thus represented by a finite set of linear inequalities, that is, by a polyhedron P_d (d for disagreement).
- By leaving out the first three inequalities this yield to a polyhedron P_t (t for total) - all possible voting outcomes.
- By the IAC condition any of these voting situation is evenly likely to occur.
- The above describe the situation where a is the PV winner while b is the PRV winner but there are 6 possible pairs of PV winner and PRV winner

• The vote problem is thus represented by a finite set of linear inequalities, that is, by a polyhedron P_d (d for disagreement).
• By leaving out the first three inequalities this yield to a polyhedron P_t (t for total) - all possible voting outcomes.
• By the IAC condition any of these voting situation is evenly likely to occur.
• The above describe the situation where a is the PV winner while b is the PRV winner but there are 6 possible pairs of PV winner and PRV winner Therefore,

$$Prob(PV\, and\, PRV\, disagree) = 6\frac{\#(P_d \cap \mathbb{Z}^d)}{\#(P_t \cap \mathbb{Z}^d)}.$$