Lattice Points in Polytopes

Richard P. Stanley
U. Miami & M.I.T.
A lattice polygon

Georg Alexander Pick (1859–1942)

\(P\): lattice polygon in \(\mathbb{R}^2\)
(vertices \(\in \mathbb{Z}^2\), no self-intersections)
Boundary and interior lattice points
Pick’s theorem

\[ A = \text{area of } P \]
\[ I = \# \text{ interior points of } P \ (= 4) \]
\[ B = \# \text{boundary points of } P \ (= 10) \]

Then

\[ A = \frac{2I + B - 2}{2}. \]
Pick’s theorem

\[ A = \text{area of } P \]
\[ I = \# \text{ interior points of } P \ (= 4) \]
\[ B = \# \text{boundary points of } P \ (= 10) \]

Then

\[ A = \frac{2I + B - 2}{2} . \]

Example on previous slide:

\[ 2 \cdot 4 + 10 - 2 \over 2 = 9 . \]
Two tetrahedra

Pick’s theorem (seemingly) fails in higher dimensions. For example, let $T_1$ and $T_2$ be the tetrahedra with vertices

$v(T_1) = \{(0,0,0), (1,0,0), (0,1,0), (0,0,1)\}$
$v(T_2) = \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\}$.
Failure of Pick’s theorem in dim 3

Then

\[ I(T_1) = I(T_2) = 0 \]
\[ B(T_1) = B(T_2) = 4 \]
\[ A(T_1) = 1/6, \quad A(T_2) = 1/3. \]
Let $\mathcal{P}$ be a convex polytope (convex hull of a finite set of points) in $\mathbb{R}^d$. For $n \geq 1$, let

$$n\mathcal{P} = \{ n\alpha : \alpha \in \mathcal{P} \}.$$
Polytope dilation

Let $\mathcal{P}$ be a convex polytope (convex hull of a finite set of points) in $\mathbb{R}^d$. For $n \geq 1$, let

$$n\mathcal{P} = \{ n\alpha : \alpha \in \mathcal{P} \}.$$
Let

\[ i(\mathcal{P}, n) = \#(n\mathcal{P} \cap \mathbb{Z}^d) = \#\{\alpha \in \mathcal{P} : n\alpha \in \mathbb{Z}^d\} \],

the number of lattice points in \( n\mathcal{P} \).
Similarly let

\[ P^\circ = \text{interior of } P = P - \partial P \]

\[
\bar{i}(P, n) = \#(nP^\circ \cap \mathbb{Z}^d) \\
= \# \{ \alpha \in P^\circ : n\alpha \in \mathbb{Z}^d \},
\]

the number of lattice points in the \textbf{interior} of \( nP \).
Similarly let

$$\mathcal{P}^\circ = \text{interior of } \mathcal{P} = \mathcal{P} - \partial \mathcal{P}$$

$$i(\mathcal{P}, n) = \#(n\mathcal{P}^\circ \cap \mathbb{Z}^d) = \#\{\alpha \in \mathcal{P}^\circ : n\alpha \in \mathbb{Z}^d\},$$

the number of lattice points in the **interior** of $n\mathcal{P}$.

**Note.** Could use any lattice $L$ instead of $\mathbb{Z}^d$. 

An example

\[ i(\mathcal{P}, n) = (n + 1)^2 \]

\[ \bar{i}(\mathcal{P}, n) = (n - 1)^2 = i(\mathcal{P}, -n). \]
The main result

**Theorem** (Ehrhart 1962, Macdonald 1963). Let

\[ \mathcal{P} = \text{lattice polytope in } \mathbb{R}^N, \quad \dim \mathcal{P} = d. \]

Then \( i(\mathcal{P}, n) \) is a polynomial (the **Ehrhart polynomial** of \( \mathcal{P} \)) in \( n \) of degree \( d \).
Reciprocity and volume

Moreover,

\[ i(\mathcal{P}, 0) = 1 \]

\[ \tilde{i}(\mathcal{P}, n) = (-1)^d i(\mathcal{P}, -n), \quad n > 0 \]

(reciprocity).
Moreover,

\[ i(P,0) = 1 \]
\[ i(P,n) = (-1)^d i(P,-n), \quad n > 0 \]

(reciprocity).

If \( d = N \) then

\[ i(P,n) = V(P)n^d + \text{lower order terms}, \]

where \( V(P) \) is the volume of \( P \).
Eugène Ehrhart

- April 29, 1906: born in Guebwiller, France
- 1932: begins teaching career in lycées
- 1959: Prize of French Sciences Academy
- 1963: begins work on Ph.D. thesis
- 1966: obtains Ph.D. thesis from Univ. of Strasbourg
- 1971: retires from teaching career
- January 17, 2000: dies
Self-portrait
Generalized Pick’s theorem

**Corollary.** Let $\mathcal{P} \subset \mathbb{R}^d$ and $\dim \mathcal{P} = d$. Knowing any $d$ of $i(\mathcal{P}, n)$ or $\tilde{i}(\mathcal{P}, n)$ for $n > 0$ determines $V(\mathcal{P})$. 
**Generalized Pick’s theorem**

**Corollary.** Let $\mathcal{P} \subset \mathbb{R}^d$ and $\dim \mathcal{P} = d$. Knowing any $d$ of $i(\mathcal{P}, n)$ or $\bar{i}(\mathcal{P}, n)$ for $n > 0$ determines $V(\mathcal{P})$.

**Proof.** Together with $i(\mathcal{P}, 0) = 1$, this data determines $d + 1$ values of the polynomial $i(\mathcal{P}, n)$ of degree $d$. This uniquely determines $i(\mathcal{P}, n)$ and hence its leading coefficient $V(\mathcal{P})$. $\square$
Example. Let $B_M \subset \mathbb{R}^{M \times M}$ be the Birkhoff polytope of all $M \times M$ doubly-stochastic matrices $A = (a_{ij})$, i.e.,

$$a_{ij} \geq 0$$

$$\sum_i a_{ij} = 1 \text{ (column sums 1)}$$

$$\sum_j a_{ij} = 1 \text{ (row sums 1)}.$$
Note. $B = (b_{ij}) \in nB_M \cap \mathbb{Z}^{M \times M}$ if and only if

$$b_{ij} \in \mathbb{N} = \{0, 1, 2, \ldots\}$$

$$\sum_i b_{ij} = n$$

$$\sum_j b_{ij} = n.$$
Example of a magic square

\[
\begin{bmatrix}
2 & 1 & 0 & 4 \\
3 & 1 & 1 & 2 \\
1 & 3 & 2 & 1 \\
1 & 2 & 4 & 0 \\
\end{bmatrix}
\]

(M = 4, n = 7)
Example of a magic square

\[
\begin{bmatrix}
2 & 1 & 0 & 4 \\
3 & 1 & 1 & 2 \\
1 & 3 & 2 & 1 \\
1 & 2 & 4 & 0 \\
\end{bmatrix}
\]

\( (M = 4, \ n = 7) \)

\( \in 7B_4 \)
$$H_M(n) := \#\{M \times M \mathbb{N}\text{-matrices, line sums } n\} = i(\mathcal{B}_M, n)$$
\[ H_M(n) := \# \{ M \times M \mathbb{N}\text{-matrices, line sums } n \} \]

\[ = i(B_M, n) \]

\[ H_1(n) = 1 \]

\[ H_2(n) = ?? \]
\( H_M(n) \) := \#\{M \times M \mathbb{N}\text{-matrices, line sums } n\}
= i(B_M, n)

\[
H_1(n) = 1
\]
\[
H_2(n) = n + 1
\]

\[
\begin{bmatrix}
  a & n - a \\
  n - a & a
\end{bmatrix}, \quad 0 \leq a \leq n.
\]
The case $M = 3$

$$H_3(n) = \binom{n+2}{4} + \binom{n+3}{4} + \binom{n+4}{4}$$

(MacMahon)
Values for small $n$

\[ H_M(0) = ?? \]
Values for small $n$

$H_M(0) = 1$
Values for small $n$

$H_M(0) = 1$
$H_M(1) = ??$
Values for small $n$

\[ H_M(0) = 1 \]
\[ H_M(1) = M! \text{ (permutation matrices)} \]
Values for small $n$

\[ H_M(0) = 1 \]
\[ H_M(1) = M! \text{ (permutation matrices)} \]

Anand-Dumir-Gupta, 1966:

\[ \sum_{M \geq 0} H_M(2) \frac{x^M}{M!^2} = ?? \]
Values for small $n$

$$H_M(0) = 1$$

$$H_M(1) = M! \text{ (permutation matrices)}$$

**Anand-Dumir-Gupta, 1966:**

$$\sum_{M \geq 0} H_M(2) \frac{x^M}{M!^2} = \frac{e^{x/2}}{\sqrt{1 - x}}$$
Theorem (Birkhoff-von Neumann). The vertices of $\mathcal{B}_M$ consist of the $M! \times M$ permutation matrices. Hence $\mathcal{B}_M$ is a lattice polytope.
Theorem (Birkhoff-von Neumann). The vertices of $B_M$ consist of the $M!$ $M \times M$ permutation matrices. Hence $B_M$ is a lattice polytope.

Corollary (Anand-Dumir-Gupta conjecture). $H_M(n)$ is a polynomial in $n$ (of degree $(M - 1)^2$).
Example. \( H_4(n) = \frac{1}{11340} \left( 11n^9 + 198n^8 + 1596n^7 ight. \\
+ 7560n^6 + 23289n^5 + 48762n^5 + 70234n^4 + 68220n^2 \\
\left. + 40950n + 11340 \right) \).
Reciprocity for magic squares

Reciprocity \Rightarrow \pm H_M(-n) =

\#\{M \times M \text{ matrices } B \text{ of positive integers, line sum } n\}.

But every such $B$ can be obtained from an $M \times M$ matrix $A$ of nonnegative integers by adding 1 to each entry.
Reciprocity for magic squares

Reciprocity ⇒ ±$H_M(-n) =$

$\#\{M \times M$ matrices $B$ of positive integers, line sum $n}\}$. 

But every such $B$ can be obtained from an $M \times M$ matrix $A$ of nonnegative integers by adding 1 to each entry.

**Corollary.** $H_M(-1) = H_M(-2) = \cdots = H_M(-M+1) = 0$

$H_M(-M - n) = (-1)^{M-1} H_M(n)$
Two remarks

- Reciprocity greatly reduces computation.
- Applications of magic squares, e.g., to statistics (contingency tables).
Zeros of $H_9(n)$ in complex plane
Zeros of $H_9(n)$ in complex plane

No explanation known.
Let $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{R}^d$. The zonotope $Z(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ generated by $\mathbf{v}_1, \ldots, \mathbf{v}_k$:

$$Z(\mathbf{v}_1, \ldots, \mathbf{v}_k) = \{\lambda_1 \mathbf{v}_1 + \cdots + \lambda_k \mathbf{v}_k : 0 \leq \lambda_i \leq 1\}$$
Zonotopes

Let \( \mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{R}^d \). The zonotope \( Z(\mathbf{v}_1, \ldots, \mathbf{v}_k) \) generated by \( \mathbf{v}_1, \ldots, \mathbf{v}_k \):

\[
Z(\mathbf{v}_1, \ldots, \mathbf{v}_k) = \{ \lambda_1 \mathbf{v}_1 + \cdots + \lambda_k \mathbf{v}_k : 0 \leq \lambda_i \leq 1 \}
\]

Example. \( \mathbf{v}_1 = (4,0) \), \( \mathbf{v}_2 = (3,1) \), \( \mathbf{v}_3 = (1,2) \)
Theorem. Let \( Z = Z(v_1, \ldots, v_k) \subset \mathbb{R}^d \), where \( v_i \in \mathbb{Z}^d \). Then

\[
i(Z, 1) = \sum_X h(X),
\]

where \( X \) ranges over all linearly independent subsets of \( \{v_1, \ldots, v_k\} \), and \( h(X) \) is the gcd of all \( j \times j \) minors (\( j = \#X \)) of the matrix whose rows are the elements of \( X \).
Example. $v_1 = (4, 0), \; v_2 = (3, 1), \; v_3 = (1, 2)$
Computation of $i(Z,1)$

$$i(Z,1) = \begin{vmatrix} 4 & 0 \\ 3 & 1 \end{vmatrix} + \begin{vmatrix} 4 & 0 \\ 1 & 2 \end{vmatrix} + \begin{vmatrix} 3 & 1 \\ 1 & 2 \end{vmatrix} + \gcd(4,0) + \gcd(3,1) + \gcd(1,2) + \det(\emptyset)$$

$$= 4 + 8 + 5 + 4 + 1 + 1 + 1 + 1$$

$$= 24.$$
Computation of $i(Z, 1)$

\[
i(Z, 1) = \begin{vmatrix} 4 & 0 \\ 3 & 1 \end{vmatrix} + \begin{vmatrix} 4 & 0 \\ 1 & 2 \end{vmatrix} + \begin{vmatrix} 3 & 1 \\ 1 & 2 \end{vmatrix} + \gcd(4, 0) + \gcd(3, 1) + \gcd(1, 2) + \det(\emptyset)
\]

\[
= 4 + 8 + 5 + 4 + 1 + 1 + 1
\]

\[
= 24.
\]
Corollary. If $Z$ is an integer zonotope generated by integer vectors, then the coefficients of $i(Z,n)$ are nonnegative integers.
Corollary. If $Z$ is an integer zonotope generated by integer vectors, then the coefficients of $i(Z, n)$ are nonnegative integers.

Neither property (nonnegativity, integrality) is true for general integer polytopes. There are numerous conjectures concerning special cases.
The permutohedron

$$\Pi_d = \text{conv}\{(w(1), \ldots, w(d)) : w \in S_d\} \subset \mathbb{R}^d$$
The permutohedron

\[ \Pi_d = \text{conv}\{(w(1), \ldots, w(d)): w \in S_d\} \subset \mathbb{R}^d \]

\[ \dim \Pi_d = d - 1, \text{ since } \sum w(i) = \binom{d+1}{2} \]
The permutohedron

\[ \Pi_d = \text{conv}\{(w(1), \ldots, w(d)) : w \in S_d\} \subset \mathbb{R}^d \]

\[ \dim \Pi_d = d - 1, \text{ since } \sum w(i) = \binom{d+1}{2} \]

\[ \Pi_d \approx Z(e_i - e_j : 1 \leq i < j \leq d) \]
$i(\Pi_3, n) = 3n^2 + 3n + 1$
(truncated octahedron)
Theorem. \( i(\Pi_d, n) = \sum_{k=0}^{d-1} f_k(d) n^k \), where

\[ f_k(d) = \#\{\text{forests with } k \text{ edges on vertices } 1, \ldots, d\} \]
Theorem. \( i(\Pi_d, n) = \sum_{k=0}^{d-1} f_k(d) n^k \), where

\[
f_k(d) = \#\{\text{forests with } k \text{ edges on vertices } 1, \ldots, d\}
\]

\[
i(\Pi_3, n) = 3n^2 + 3n + 1
\]
Theorem. \( i(\Pi_d, n) = \sum_{k=0}^{d-1} f_k(d) n^k \), where
\[
f_k(d) = \# \{ \text{forests with } k \text{ edges on vertices } 1, \ldots, d \}
\]
\[
i(\Pi_3, n) = 3n^2 + 3n + 1
\]
Can be greatly generalized (Postnikov, et al.).
Let $G$ be a graph (with no loops or multiple edges) on the vertex set $V(G) = \{1, 2, \ldots, n\}$. Let

$$d_i = \text{degree (\# incident edges) of vertex } i.$$ 

Define the **ordered degree sequence** $d(G)$ of $G$ by

$$d(G) = (d_1, \ldots, d_n).$$
Example of \( d(G) \)

Example. \( d(G) = (2, 4, 0, 3, 2, 1) \)
Let \( f(n) \) be the number of distinct \( d(G) \), where \( V(G) = \{1, 2, \ldots, n\} \).
$f(n)$ for $n \leq 4$

**Example.** If $n \leq 3$, all $d(G)$ are distinct, so $f(1) = 1$, $f(2) = 2^1 = 2$, $f(3) = 2^3 = 8$. For $n \geq 4$ we can have $G \neq H$ but $d(G) = d(H)$, e.g.,

In fact, $f(4) = 54 < 2^6 = 64$. 

![Graphs](image-url)
The polytope of degree sequences

Let $\text{conv}$ denote convex hull, and

$$D_n = \text{conv}\{d(G) : V(G) = \{1, \ldots, n\} \subset \mathbb{R}^n, \}$$

the polytope of degree sequences (Perles, Koren).
The polytope of degree sequences

Let \( \text{conv} \) denote convex hull, and

\[
D_n = \text{conv}\{d(G) : V(G) = \{1, \ldots, n\}\} \subset \mathbb{R}^n,
\]

the polytope of degree sequences (Perles, Koren).

Easy fact. Let \( e_i \) be the \( i \)th unit coordinate vector in \( \mathbb{R}^n \). E.g., if \( n = 5 \) then \( e_2 = (0, 1, 0, 0, 0) \). Then

\[
D_n = Z(e_i + e_j : 1 \leq i < j \leq n).
\]
The Erdős-Gallai theorem

Theorem. Let 
\[ \alpha = (a_1, \ldots, a_n) \in \mathbb{Z}^n. \]

Then \( \alpha = d(G) \) for some \( G \) if and only if

1. \( \alpha \in \mathcal{D}_n \)
2. \( a_1 + a_2 + \cdots + a_n \) is even.
Enumerative techniques leads to:

**Theorem.** Let

\[
F(x) = \sum_{n \geq 0} f(n) \frac{x^n}{n!} = 1 + x + 2 \frac{x^2}{2!} + 8 \frac{x^3}{3!} + 54 \frac{x^4}{4!} + \cdots.
\]

*Then:*

A generating function
A formula for $F(x)$

$$F(x) = \frac{1}{2} \left[ \left(1 + 2 \sum_{n \geq 1} \frac{n^n x^n}{n!} \right)^{1/2} \right.$$

$$\times \left(1 - \sum_{n \geq 1} (n - 1)^{n-1} \frac{x^n}{n!}\right) + 1 \right]$$

$$\times \exp \sum_{n \geq 1} n^{n-2} \frac{x^n}{n!} \quad (0^0 = 1)$$
Coefficients of $i(\mathcal{P}, n)$

Let $\mathcal{P}$ denote the tetrahedron with vertices $(0, 0, 0)$, $(1, 0, 0)$, $(0, 1, 0)$, $(1, 1, 13)$. Then

$$i(\mathcal{P}, n) = \frac{13}{6}n^3 + n^2 - \frac{1}{6}n + 1.$$
The “bad” tetrahedron
The “bad” tetrahedron

Thus in general the coefficients of Ehrhart polynomials are not “nice.” Is there a “better” basis?
Let $\mathcal{P}$ be a lattice polytope of dimension $d$. Since $i(\mathcal{P}, n)$ is a polynomial of degree $d$, $\exists \ h_i \in \mathbb{Z}$ such that

$$
\sum_{n \geq 0} i(\mathcal{P}, n)x^n = \frac{h_0 + h_1x + \cdots + h_dx^d}{(1 - x)^{d+1}}.
$$
Let $\mathcal{P}$ be a lattice polytope of dimension $d$. Since $i(\mathcal{P}, n)$ is a polynomial of degree $d$, $\exists h_i \in \mathbb{Z}$ such that

$$\sum_{n \geq 0} i(\mathcal{P}, n)x^n = \frac{h_0 + h_1x + \ldots + h_dx^d}{(1 - x)^{d+1}}.$$ 

**Definition.** Define

$$h^*(\mathcal{P}) = (h_0, h_1, \ldots, h_d),$$

the $h^*$-vector of $\mathcal{P}$. 

Example of an $h^*$-vector

**Example.** Recall

$$i(B_4, n) = \frac{1}{11340} (11n^9 + 198n^8 + 1596n^7 + 7560n^6 + 23289n^5 + 48762n^4 + 70234n^3 + 68220n^2 + 40950n + 11340).$$
Example of an $h^*$-vector

Example. Recall

\[ i(\mathcal{B}_4, n) = \frac{1}{11340} (11n^9 + 198n^8 + 1596n^7 + 7560n^6 + 23289n^5 + 48762n^4 + 70234n^3 + 68220n^2 + 40950n + 11340). \]

Then

\[ h^*(\mathcal{B}_4) = (1, 14, 87, 148, 87, 14, 1, 0, 0, 0). \]
Two terms of $h^*(\mathcal{P})$

- $h_0 = 1$
- $h_d = (-1)^{\dim \mathcal{P}} i(\mathcal{P}, -1) = I(\mathcal{P})$
Main properties of $h^*(\mathcal{P})$

**Theorem A (nonnegativity).** (McMullen, RS) $h_i \geq 0$. 
Main properties of $h^*(\mathcal{P})$

**Theorem A (nonnegativity).** (McMullen, RS) $h_i \geq 0$.

**Theorem B (monotonicity).** (RS) If $\mathcal{P}$ and $\mathcal{Q}$ are lattice polytopes and $\mathcal{Q} \subseteq \mathcal{P}$, then

$$h_i(\mathcal{Q}) \leq h_i(\mathcal{P}) \ \forall i.$$
Main properties of $h^*(\mathcal{P})$

**Theorem A (nonnegativity).** (McMullen, RS) $h_i \geq 0$.

**Theorem B (monotonicity).** (RS) If $\mathcal{P}$ and $\mathcal{Q}$ are lattice polytopes and $\mathcal{Q} \subseteq \mathcal{P}$, then

$$h_i(\mathcal{Q}) \leq h_i(\mathcal{P}) \quad \forall i.$$ 

B $\Rightarrow$ A: take $\mathcal{Q} = \emptyset$. 
Proofs: the Ehrhart ring

\( \mathcal{P} \): (convex) lattice polytope in \( \mathbb{R}^d \) with vertex set \( V \)

\[ x^\beta = x^{\beta_1} \cdots x^{\beta_d}, \beta \in \mathbb{Z}^d \]

Ehrhart ring (over \( \mathbb{Q} \)):

\[ \mathcal{R}_\mathcal{P} = \mathbb{Q} \left[ x^\beta y^n : \beta \in \mathbb{Z}^d, \ n \in \mathcal{P}, \ \frac{\beta}{n} \in \mathcal{P} \right] \]

\[ \deg x^\beta y^n = n \]
Proofs: the Ehrhart ring

\( \mathcal{P} \): (convex) lattice polytope in \( \mathbb{R}^d \) with vertex set \( V \)

\( x^\beta = x^{\beta_1} \cdots x^{\beta_d}, \ \beta \in \mathbb{Z}^d \)

**Ehrhart ring** (over \( \mathbb{Q} \)):

\[
R_\mathcal{P} = \mathbb{Q} \left[ x^\beta y^n : \beta \in \mathbb{Z}^d, \ n \in \mathcal{P}, \ \frac{\beta}{n} \in \mathcal{P} \right]
\]

\( \deg x^\beta y^n = n \)

\[
R_\mathcal{P} = (R_\mathcal{P})_0 \oplus (R_\mathcal{P})_1 \oplus \cdots
\]
Simple properties of $R_\mathcal{P}$

Hilbert function of $R_\mathcal{P}$:

$$H(R_\mathcal{P}, n) = \dim_Q(R_\mathcal{P})_n.$$
**Hilbert function** of $R_P$:

$$H(R_P, n) = \dim_Q (R_P)_n.$$  

**Theorem** (easy). $H(R_P, n) = i(P, n)$
Simple properties of $R_P$

**Hilbert function** of $R_P$:

$$H(R_P, n) = \dim_Q(R_P)_n.$$  

**Theorem** (easy). $H(R_P, n) = i(\mathcal{P}, n)$

$\mathcal{Q}[\mathcal{V}]$: subalgebra of $R_P$ generated by $x^\alpha y$, $\alpha \in \mathcal{V}$. 
Simple properties of $R_{\mathcal{P}}$

**Hilbert function** of $R_{\mathcal{P}}$:

$$H(R_{\mathcal{P}}, n) = \dim_{\mathbb{Q}}(R_{\mathcal{P}})_n.$$  

**Theorem** (easy). $H(R_{\mathcal{P}}, n) = i(\mathcal{P}, n)$

$\mathbb{Q}[V]$: subalgebra of $R_{\mathcal{P}}$ generated by $x^\alpha y$, $\alpha \in V$.

**Theorem** (easy). $R_{\mathcal{P}}$ is a finitely-generated $\mathbb{Q}[V]$-module.
The Cohen-Macaulay property

Theorem (Hochster, 1972). $R_P$ is a Cohen-Macaulay ring.
Theorem (Hochster, 1972). $R_P$ is a Cohen-Macaulay ring.

This means (using finiteness of $R_P$ over $\mathbb{Q}[V]$): if $\dim P = m$ then there exist algebraically independent $\theta_1, \ldots, \theta_m \in (R_P)_1$ such that $R_P$ is a finitely-generated free $\mathbb{Q}[\theta_1, \ldots, \theta_m]$-module.

$\theta_1, \ldots, \theta_m$ is a homogeneous system of parameters (h.s.o.p.).
The Cohen-Macaulay property

**Theorem** (Hochster, 1972). $R_P$ is a Cohen-Macaulay ring.

This means (using finiteness of $R_P$ over $\mathbb{Q}[V]$): if $\dim P = m$ then there exist algebraically independent $\theta_1, \ldots, \theta_m \in (R_P)_1$ such that $R_P$ is a finitely-generated free $\mathbb{Q}[\theta_1, \ldots, \theta_m]$-module.

$\theta_1, \ldots, \theta_m$ is a **homogeneous system of parameters** (h.s.o.p.).

Thus $R_P = \bigoplus_{j=1}^r \eta_j \mathbb{Q}[\theta_1, \ldots, \theta_m]$, where $\eta_j \in (R_P)_{e_j}$.
The Cohen-Macaulay property

**Theorem** (Hochster, 1972). $R_P$ is a Cohen-Macaulay ring.

This means (using finiteness of $R_P$ over $\mathbb{Q}[V]$): if $\dim P = m$ then there exist algebraically independent $\theta_1, \ldots, \theta_m \in (R_P)_1$ such that $R_P$ is a finitely-generated free $\mathbb{Q}[\theta_1, \ldots, \theta_m]$-module.

$\theta_1, \ldots, \theta_m$ is a **homogeneous system of parameters** (h.s.o.p.).

Thus $R_P = \bigoplus_{j=1}^r \eta_j \mathbb{Q}[\theta_1, \ldots, \theta_m]$, where $\eta_j \in (R_P)_{e_j}$.

**Corollary.** \[ \sum_{n \geq 0} H(R_{P}, n) x^n = \frac{x^{e_1} + \cdots + x^{e_r}}{(1 - x)^m}, \] so \( h^*(P) \geq 0. \)
Monotonicity

The result $Q \subseteq P \Rightarrow h^*(Q) \leq h^*(P)$ is proved similarly.

We have $R_Q \subset R_P$. The key fact is that we can find an h.s.o.p. $\theta_1, \ldots, \theta_k$ for $R_Q$ that extends to an h.s.o.p. for $R_P$. 
The canonical module

Let $R = R_0 \oplus R_1 \oplus \cdots$ be a Cohen-Macaulay graded algebra over a field $K = R_0$, with Krull dimension $m$ and Hilbert series

$$
\sum_{n \geq 0} (\dim_K R_n)x^n = \frac{\sum_{j=1}^{r} x^{e_j}}{(1 - x^{d_1}) \cdots (1 - x^{d_m})}.
$$

Let $R \simeq A/I$, where $A = K[x_1, \ldots, x_t]$. 
The canonical module

Let $R = R_0 \oplus R_1 \oplus \cdots$ be a Cohen-Macaulay graded algebra over a field $K = R_0$, with Krull dimension $m$ and Hilbert series

$$
\sum_{n \geq 0} (\dim_K R_n) x^n = \frac{\sum_{j=1}^{r} x^{e_j}}{(1 - x^{d_1}) \cdots (1 - x^{d_m})}.
$$

Let $R \cong A/I$, where $A = K[x_1, \ldots, x_t]$.

**canonical module:** $\Omega(R) = \text{Ext}_A^{t-m}(R, A)$, a graded $R$-module.
Reciprocity redux

Basic result in commutative/homological algebra:

$$\sum_{n \geq 0} (\dim_K \Omega(R)_n) x^n = \frac{x^c \sum_{j=1}^r x^{-e_j}}{(1 - x^{d_1}) \cdots (1 - x^{d_m})}.$$
Reciprocity redux

Basic result in commutative/homological algebra:

$$\sum_{n \geq 0} (\dim_K \Omega(R)_n) x^n = \frac{x^c \sum_{j=1}^r x^{-e_j}}{(1 - x^{d_1}) \cdots (1 - x^{d_m})}.$$

**Theorem.**

$$\Omega(R_\mathcal{P}) = \text{span}_Q \{ x^\beta y^n : \beta \in \mathbb{Z}^d, \ n \in \mathbb{P}, \ \frac{\beta}{n} \in \text{interior}(\mathcal{P}) \}$$
Reciprocity redux

Basic result in commutative/homological algebra:

\[
\sum_{n \geq 0} (\dim_K \Omega(R)_n) x^n = x^c \sum_{j=1}^{r} x^{-e_j} \frac{(1 - x^{d_1}) \cdots (1 - x^{d_m})}{(1 - x^{d_1}) \cdots (1 - x^{d_m})}.
\]

**Theorem.**

\(\Omega(R_P) = \text{span}_Q \{x^\beta y^n : \beta \in \mathbb{Z}^d, \ n \in \mathbb{P}, \frac{\beta}{n} \in \text{interior}(P)\}\)

**Corollary.** \(\overline{i}(P, n) = (-1)^d i(P, n)\).
Example. Let $\mathcal{P}$ be the polytope $[2, 5]$ in $\mathbb{R}$, so $\mathcal{P}$ is defined by

\begin{align*}
(1) & \quad x \geq 2, \\
(2) & \quad x \leq 5.
\end{align*}
Example. Let $\mathcal{P}$ be the polytope $[2, 5]$ in $\mathbb{R}$, so $\mathcal{P}$ is defined by

(1) $x \geq 2$,  \hspace{1cm} (2) $x \leq 5$.

Let

\[
F_1(t) = \sum_{n \geq 2, \; n \in \mathbb{Z}} t^n = \frac{t^2}{1 - t}
\]

\[
F_2(t) = \sum_{n \leq 5, \; n \in \mathbb{Z}} t^n = \frac{t^5}{1 - \frac{1}{t}}.
\]
\( F_1(t) + F_2(t) \)

\[
F_1(t) + F_2(t) = \frac{t^2}{1-t} + \frac{t^5}{1-\frac{1}{t}}
= t^2 + t^3 + t^4 + t^5
= \sum_{m \in P \cap \mathbb{Z}} t^m.
\]
Cone at a vertex

\(\mathcal{P}\): \(\mathbb{Z}\)-polytope in \(\mathbb{R}^N\) with vertices \(v_1, \ldots, v_k\)

\(\mathcal{C}_i\): cone at vertex \(v_i\) supporting \(\mathcal{P}\)
Cone at a vertex

\( \mathcal{P} \): \( \mathbb{Z} \)-polytope in \( \mathbb{R}^N \) with vertices \( v_1, \ldots, v_k \)

\( \mathcal{C}_i \): cone at vertex \( v_i \) supporting \( \mathcal{P} \)
The general result

Let \( F_i(t_1, \ldots, t_N) = \sum_{(m_1, \ldots, m_N) \in C_i \cap \mathbb{Z}^N} t_1^{m_1} \cdots t_N^{m_N} \).
The general result

Let \( F_i(t_1, \ldots, t_N) = \sum_{(m_1, \ldots, m_N) \in C_i \cap \mathbb{Z}^N} t_1^{m_1} \cdots t_N^{m_N}. \)

**Theorem (Brion).** Each \( F_i \) is a rational function of \( t_1, \ldots, t_N \), and

\[
\sum_{i=1}^{k} F_i(t_1, \ldots, t_N) = \sum_{(m_1, \ldots, m_N) \in \mathcal{P} \cap \mathbb{Z}^N} t_1^{m_1} \cdots t_N^{m_N}
\]

(as rational functions).
Computing $i(\mathcal{P}, n)$, or even $i(\mathcal{P}, 1)$ is $\#P$-complete. Thus an “efficient” (polynomial time) algorithm is extremely unlikely. However:
II. Complexity

Computing $i(\mathcal{P}, n)$, or even $i(\mathcal{P}, 1)$ is $\#P$-complete. Thus an “efficient” (polynomial time) algorithm is extremely unlikely. However:

**Theorem** (A. Barvinok, 1994). *For fixed dim $\mathcal{P}$, $\exists$ polynomial-time algorithm for computing $i(\mathcal{P}, n)$.***
Example. Let $S_M(n)$ denote the number of symmetric $M \times M$ matrices of nonnegative integers, every row and column sum $n$. Then

$$S_3(n) = \begin{cases} \frac{1}{8}(2n^3 + 9n^2 + 14n + 8), & n \text{ even} \\ \frac{1}{8}(2n^3 + 9n^2 + 14n + 7), & n \text{ odd} \end{cases}$$

$$= \frac{1}{16}(4n^3 + 18n^2 + 28n + 15 + (-1)^n).$$
III. Fractional lattice polytopes

Example. Let $S_M(n)$ denote the number of symmetric $M \times M$ matrices of nonnegative integers, every row and column sum $n$. Then

\[
S_3(n) = \begin{cases}
\frac{1}{8}(2n^3 + 9n^2 + 14n + 8), & n \text{ even} \\
\frac{1}{8}(2n^3 + 9n^2 + 14n + 7), & n \text{ odd}
\end{cases}
\]

\[
= \frac{1}{16}(4n^3 + 18n^2 + 28n + 15 + (-1)^n).
\]

Why a different polynomial depending on $n$ modulo 2?
The symmetric Birkhoff polytope

$\mathcal{T}_M$: the polytope of all $M \times M$ symmetric doubly-stochastic matrices.
The symmetric Birkhoff polytope

$\mathcal{T}_M$: the polytope of all $M \times M$ symmetric doubly-stochastic matrices.

Easy fact: $S_M(n) = \#(n\mathcal{T}_M \cap \mathbb{Z}^{M \times M})$
The symmetric Birkhoff polytope

$\mathcal{T}_M$: the polytope of all $M \times M$ symmetric doubly-stochastic matrices.

**Easy fact:** $S_M(n) = \# \left( n\mathcal{T}_M \cap \mathbb{Z}^{M \times M} \right)$

**Fact:** vertices of $\mathcal{T}_M$ have the form $\frac{1}{2}(P + P^t)$, where $P$ is a permutation matrix.
The symmetric Birkhoff polytope

\( \mathcal{T}_M \): the polytope of all \( M \times M \) symmetric doubly-stochastic matrices.

**Easy fact:** \( S_M(n) = \#(n\mathcal{T}_M \cap \mathbb{Z}^{M \times M}) \)

**Fact:** vertices of \( \mathcal{T}_M \) have the form \( \frac{1}{2}(P + P^t) \), where \( P \) is a permutation matrix.

Thus if \( v \) is a vertex of \( \mathcal{T}_M \) then \( 2v \in \mathbb{Z}^{M \times M} \).
Theorem. There exist polynomials \( P_M(n) \) and \( Q_M(n) \) for which

\[ S_M(n) = P_M(n) + (-1)^n Q_M(n), \quad n \geq 0. \]

Moreover, \( \deg P_M(n) = \left( \frac{M}{2} \right) \).
Theorem. There exist polynomials $P_M(n)$ and $Q_M(n)$ for which

$$S_M(n) = P_M(n) + (-1)^n Q_M(n), \quad n \geq 0.$$ 

Moreover, $\deg P_M(n) = \binom{M}{2}$.

Difficult result (Dahmen and Micchelli, 1988):

$$\deg Q_M(n) = \begin{cases} 
\binom{M-1}{2} - 1, & M \text{ odd} \\
\binom{M-2}{2} - 1, & M \text{ even}.
\end{cases}$$
For $\alpha > 0$ let $T_\alpha$ be the triangle in $\mathbb{R}^2$ with vertices $(0, 0), (0, \alpha), (1/\alpha, 0)$, so $\text{area}(T_\alpha) = \frac{1}{2}$. Can define $i(T_\alpha, n) = \#(nT_\alpha \cap \mathbb{Z}^2)$, $n \geq 1$. 
IV. Some curious triangles

For $\alpha > 0$ let $T_\alpha$ be the triangle in $\mathbb{R}^2$ with vertices $(0, 0), (0, \alpha), (1/\alpha, 0)$, so $\text{area}(T_\alpha) = \frac{1}{2}$. Can define

$$i(T_\alpha, n) = \#(nT_\alpha \cap \mathbb{Z}^2), \ n \geq 1.$$

Easy. $T_1$ is a lattice triangle with $i(T_1, n) = \binom{n+2}{2}$.

**Theorem (Cristofaro-Gardiner, Li, S).** Let $\alpha > 1$. We have $i(T_\alpha, n) = \binom{n+2}{2}$ for all $n \geq 1$ if and only if either:
IV. Some curious triangles

For $\alpha > 0$ let $T_\alpha$ be the triangle in $\mathbb{R}^2$ with vertices $(0, 0), (0, \alpha), (1/\alpha, 0)$, so $\text{area}(T_\alpha) = \frac{1}{2}$. Can define

$$i(T_\alpha, n) = \#(nT_\alpha \cap \mathbb{Z}^2), \ n \geq 1.$$ 

Easy. $T_1$ is a lattice triangle with $i(T_1, n) = \binom{n+2}{2}$.

Theorem (Cristofaro-Gardiner, Li, S). Let $\alpha > 1$. We have $i(T_\alpha, n) = \binom{n+2}{2}$ for all $n \geq 1$ if and only if either:

- $\alpha = \frac{F_{2k+1}}{F_{2k-1}}$ (Fibonacci numbers)
IV. Some curious triangles

For $\alpha > 0$ let $T_\alpha$ be the triangle in $\mathbb{R}^2$ with vertices $(0,0), (0,\alpha), (1/\alpha, 0)$, so area($T_\alpha$) = $\frac{1}{2}$. Can define

$$i(T_\alpha, n) = \#(nT_\alpha \cap \mathbb{Z}^2), \ n \geq 1.$$ 

Easy. $T_1$ is a lattice triangle with $i(T_1, n) = \binom{n+2}{2}$.

**Theorem** (Cristofaro-Gardiner, Li, S). Let $\alpha > 1$. We have $i(T_\alpha, n) = \binom{n+2}{2}$ for all $n \geq 1$ if and only if either:

- $\alpha = \frac{F_{2k+1}}{F_{2k-1}}$ (Fibonacci numbers)
- $\alpha = \frac{1}{2}(3 + \sqrt{5})$
The last slide
The last slide
The last slide 😞