PASCA 2.0

Summer School at CIMAT

CIMAT

Guanajuato, Mexico

Lecture Notes

Lattice Point Counting via Commutative Algebra

Lectures by **Federico Castillo**

Pontificia Universidad Católica

Notes prepared by **Soumyadeep Misra**

May 25–May 29, 2026

Contents

1 Lecture 1- May 25, 2026

Semigroups from Linear Algebra

Let A be a matrix with rational or integral entries. After clearing denominators, every rational matrix relevant to lattice-point questions may be replaced by an integral matrix.

Definition 1.1 (Semigroup)**.** A *semigroup* is a set S equipped with an associative binary operation. In the context of this lecture, we primarily consider additive subsemigroups of $\mathbb{Z}^n$, which are subsets $S \subseteq \mathbb{Z}^n$ that are closed under addition. That is, if $x, y \in S$, then $x + y \in S$.

The basic objects in the lecture are subsets of $\mathbb{Z}^n$ cut out by linear equalities and inequalities. For example, the set of solutions

$$\{x \in \mathbb{Z}^n \mid Ax = 0\}$$

forms an additive semigroup. Similarly, the set of nonnegative solutions

$$\{x \in \mathbb{Z}^n \mid Ax \geq 0\}$$

is a semigroup.

Definition 1.2 (Integral span)**.** Let $v_1, \ldots, v_\ell \in \mathbb{Z}^n$. The integral span of these vectors is

$$\mathrm{span}_{\mathbb{Z}}\{v_1, \ldots, v_\ell\} = \left\{ \sum_{i=1}^{\ell} \lambda_i v_i \,\middle|\, \lambda_i \in \mathbb{Z} \right\}.$$

Definition 1.3 (Positive span)**.** Let $v_1, \ldots, v_\ell \in \mathbb{Z}^n$. The positive span, or rational polyhedral cone generated by these vectors, is

$$\mathrm{pos}\{v_1, \ldots, v_\ell\} = \left\{ \sum_{i=1}^{\ell} \lambda_i v_i \,\middle|\, \lambda_i \geq 0 \right\}.$$

Example 1.4. The set

$$\{x \in \mathbb{Z}^n \mid Ax = 0\}$$

is an integral span, and

$$\{x \in \mathbb{Z}^n \mid Ax \geq 0\}$$

is the lattice points of a positive span.

Affine Semigroups

Definition 1.5 (Affine semigroup)**.** An *affine semigroup* is a finitely generated subsemigroup

$$S \subseteq (\mathbb{Z}^n, +).$$

That is, we can write

$$S = \mathbb{N}\{v_1, \ldots, v_\ell\} := \left\{ \sum_{i=1}^{\ell} n_i v_i \,\middle|\, n_i \in \mathbb{N} \right\}.$$

Here $v_i \in \mathbb{Z}^n$. Throughout these notes, $\Bbbk$ denotes an algebraically closed field of characteristic 0.

Definition 1.6 (Group generated by a semigroup)**.** Let S be a semigroup. The group generated by S is

$$\mathbb{Z}S = \{s_1 - s_2 \,|\, s_1, s_2 \in S\}.$$

If $S = \mathbb{N}\{v_1, \ldots, v_\ell\}$, then $\mathbb{Z}S = \operatorname{span}_{\mathbb{Z}}\{v_1, \ldots, v_\ell\}$.

Definition 1.7 (Rank)**.** The rank of an affine semigroup S is the rank of the abelian group $\mathbb{Z}S$:

$$\operatorname{rank}(S) = \operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}S).$$

If $\mathbb{Z}S = \mathbb{Z}^n$, then $\operatorname{rank}(S) = n$.

Definition 1.8 (Saturation)**.** Let S be an affine semigroup. We say that S is *saturated* if, whenever $x \in \mathbb{Z}S$ and $k \in \mathbb{N}_{>0}$ satisfy

$$kx \in S,$$

then $x \in S$. Equivalently, S is saturated if

$$S = \{x \in \mathbb{Z}S \,|\, kx \in S \text{ for some } k \in \mathbb{N}_{>0}\}.$$

Remark 1.9. Informally, a saturated semigroup has no missing lattice points inside its rational cone.

Numerical Semigroups and the Frobenius Problem

Definition 1.10 (Numerical semigroup)**.** A numerical semigroup is a subsemigroup $S \subseteq \mathbb{N}$ such that $\mathbb{N} \setminus S$ is finite.

Example 1.11. Let

$$S = \mathbb{N}\{a, b\} = \{ma + nb \mid m, n \in \mathbb{N}\} \subseteq \mathbb{N}.$$

Assume $\gcd(a, b) = 1$. If $\gcd(a, b) \neq 1$, then S generates a proper subgroup of $\mathbb{Z}$, so infinitely many natural numbers are missing from S. Conversely, if $\gcd(a, b) = 1$, the classical Frobenius theorem implies that all sufficiently large natural numbers lie in S.

Theorem 1.12 (Sylvester's theorem)**.** *Let* $a, b \in \mathbb{N}_{>0}$ *satisfy* $\gcd(a, b) = 1$*, and let* $S = \mathbb{N}\{a, b\}$*. Define* $f(a, b) = (a - 1)(b - 1)$*.*

(1) *If* $N \geq f(a, b)$*, then*
$$N \in S.$$
The largest integer not in S *is* $f(a, b) - 1 = ab - a - b$*.*

(2) *The number of gaps in*
$$\{0, 1, 2, \ldots, f(a, b)\}$$
is exactly $\frac{f(a,b)}{2}$*.*

Equivalently, the Frobenius number of S *is*

$$F(a, b) = ab - a - b.$$

Example 1.13. Let
$$S = \mathbb{N}\{3, 5\} \subseteq \mathbb{N}.$$

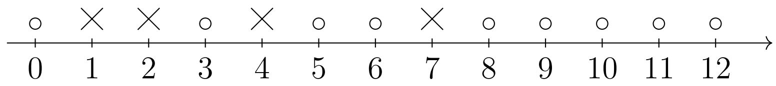
We can compute the elements of S:

$$S = \{0, 3, 5, 6, 8, 9, 10, 11, 12, \ldots\}.$$

The set of gaps is:
$$\mathbb{N} \setminus S = \{1, 2, 4, 7\}.$$

The Frobenius number is $F(3, 5) = 3 \cdot 5 - 3 - 5 = 7$.

$$S = \mathbb{N}\{3,5\}$$



gaps: $1, 2, 4, 7$

Question 1.14 (Three-generator Frobenius problem)**.** Let

$$S = \mathbb{N}\{a,b,c\} \subseteq \mathbb{N}$$

where $\gcd(a,b,c) = 1$. What is $F(a,b,c)$? For example, consider $S = \mathbb{N}\{9,10,11\}$. There is no general simple formula for the Frobenius number in three generators.

Examples and Nonexamples of Saturation

Example 1.15. Let

$$S = \mathbb{N}\{3,5\} \subseteq \mathbb{N}.$$

Because $\mathbb{N} \setminus S = \{1,2,4,7\}$, S is not saturated inside $\mathbb{N}$.

Example 1.16. Let

$$S = \mathbb{N}\{a,b\} \subseteq \mathbb{N}.$$

If $d = \gcd(a,b) \neq 1$, then $\mathbb{Z}S = d\mathbb{Z}$, so every nonnegative integer not divisible by d is missing from S.

Example 1.17 (A nonsaturated affine semigroup)**.** Let

$$S = \mathbb{N}\{(1,0),(1,2),(2,1)\} \subseteq \mathbb{Z}^2.$$

The cone generated by S is the same cone generated by $(1,0)$ and $(1,2)$, namely

$$\mathrm{Cone}(S) = \left\{(x,y) \in \mathbb{R}^2 \mid 0 \le y \le 2x\right\}.$$

Unlike the semigroup $\mathbb{N}\{(1,0),(1,2)\}$, this semigroup generates the whole lattice $\mathbb{Z}^2$.

Indeed,

$$\det \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = 1,$$

so the two elements $(1,0)$ and $(2,1)$ already generate $\mathbb{Z}^2$ as a group. Hence

$$\mathbb{Z}S = \mathbb{Z}^2.$$

We now show that S is not saturated. Consider the lattice point

$$(1,1) \in \mathbb{Z}S = \mathbb{Z}^2.$$

This point is not in S. Indeed, if

$$(1,1) = a(1,0) + b(1,2) + c(2,1)$$

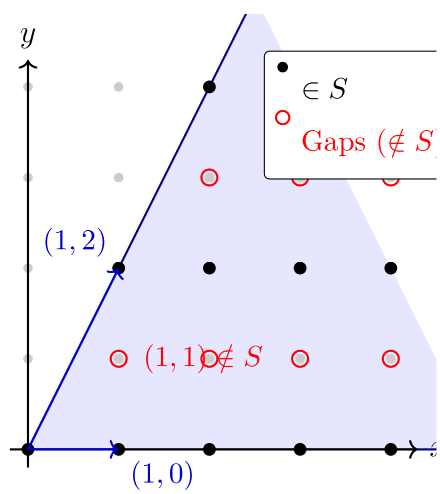
with $a, b, c \in \mathbb{N}$, then comparing coordinates gives

$$a + b + 2c = 1, \qquad 2b + c = 1.$$

The second equation forces either $b = 0, c = 1$, but then the first equation gives $a+2 = 1$, impossible. Hence $(1,1) \notin S$.
However,

$$2(1,1) = (2,2) = (1,0) + (1,2) \in S.$$

Thus there exists an element $x = (1,1) \in \mathbb{Z}S$ such that $x \notin S$, but $2x \in S$. Therefore S is not saturated.



Pointed Cones and Gordan's Lemma

A central source of affine semigroups is given by lattice points inside rational polyhedral cones.

Definition 1.18 (Pointed cone)**.** Let σ be a cone. We say that σ is *pointed* if

$$\sigma \cap (-\sigma) = \{0\}.$$

Geometrically, this says that the cone has its apex at 0.

Example 1.19. Let

$$\sigma = \{x \in \mathbb{R}^n \mid Ax \geq 0\}$$

be a pointed rational polyhedral cone. Then

$$S = \sigma \cap \mathbb{Z}^n$$

is a semigroup.

Proposition 1.20. *Let σ be a rational polyhedral cone, and set*

$$S = \sigma \cap \mathbb{Z}^n.$$

If $\mathbb{Z}S = \mathbb{Z}^n$, then S is saturated.

Proof. Suppose $x \in \mathbb{Z}S$ and $kx \in S$ for some $k \in \mathbb{N}_{>0}$. Since $S \subseteq \sigma$, we have

$$kx \in \sigma.$$

Since σ is a cone, it is closed under multiplication by positive real scalars. Hence

$$x = \frac{1}{k}(kx) \in \sigma.$$

Therefore $x \in \sigma \cap \mathbb{Z}S$. In the case $\mathbb{Z}S = \mathbb{Z}^n$, this is simply

$$x \in \sigma \cap \mathbb{Z}^n = S.$$

□

Theorem 1.21 (Gordan's lemma). *Let*

$$\sigma = \operatorname{pos}\{v_1, \dots, v_\ell\} \subseteq \mathbb{R}^n$$

be a rational cone, where $v_1, \dots, v_\ell \in \mathbb{Z}^n$. Then

$$S = \sigma \cap \mathbb{Z}^n$$

is an affine semigroup (it is finitely generated).

Proof. Let $v \in S$. Since $v \in \sigma$, there exist real numbers $\lambda_i \geq 0$ such that

$$v = \sum_{i=1}^{\ell} \lambda_i v_i.$$

Write $\lambda_i = \lfloor \lambda_i \rfloor + \{\lambda_i\}$, where

$$\lfloor \lambda_i \rfloor \in \mathbb{N}, \qquad 0 \leq \{\lambda_i\} < 1.$$

Then

$$v = \sum_{i=1}^{\ell} \lfloor \lambda_i \rfloor v_i + \sum_{i=1}^{\ell} \{\lambda_i\} v_i.$$

Define the fundamental parallelepiped

$$\operatorname{Par}(v_1, \dots, v_\ell) = \left\{ \sum_{i=1}^{\ell} \mu_i v_i \,\middle|\, 0 \leq \mu_i < 1 \right\}.$$

Since v and $\sum_{i=1}^{\ell} \lfloor \lambda_i \rfloor v_i$ are lattice points, the second summand is also a lattice point. Hence

$$\sum_{i=1}^{\ell} \{\lambda_i\} v_i \in \operatorname{Par}(v_1, \dots, v_\ell) \cap \mathbb{Z}^n.$$

The intersection $\operatorname{Par}(v_1, \dots, v_\ell) \cap \mathbb{Z}^n$ is a bounded discrete set, hence finite. It follows that every element of S is generated by the finite set

$$\{v_1, \dots, v_\ell\} \cup \Big(\operatorname{Par}(v_1, \dots, v_\ell) \cap \mathbb{Z}^n\Big).$$

□

Remark 1.22. The lecture conclusion was:

$$\text{generators of } S \subseteq \{v_1, \dots, v_\ell\} \cup \Big(\operatorname{Par}(v_1, \dots, v_\ell) \cap \mathbb{Z}^n\Big),$$

which proves the set is finitely generated.

Definition 1.23 (Hilbert basis). Let S be a positive affine semigroup. A minimal set of semigroup generators for S is called the Hilbert basis of S, denoted $\mathrm{Hilb}(S)$. For a positive affine semigroup, an element $g \in S \setminus \{0\}$ belongs to $\mathrm{Hilb}(S)$ if and only if it cannot be written as

$$g = v + v'$$

with nonzero $v, v' \in S$.

Semigroup Rings

Let S be an affine semigroup.

Definition 1.24 (Semigroup ring). The semigroup ring of S over $\Bbbk$ is

$$\Bbbk[S] = \Bbbk[t^m \mid m \in S].$$

For $m = (m_1, \ldots, m_n) \in \mathbb{Z}^n$, we write

$$t^m = t_1^{m_1} \cdots t_n^{m_n}.$$

The multiplication rule is $t^m t^{m'} = t^{m+m'}$.

Remark 1.25. When $S \subseteq \mathbb{N}^n$, the ring $\Bbbk[S]$ is a subalgebra of the polynomial ring $\Bbbk[t_1, \ldots, t_n]$. More generally, if $S \subseteq \mathbb{Z}^n$, then $\Bbbk[S]$ is naturally a subalgebra of the Laurent polynomial ring

$$\Bbbk[t_1^{\pm 1}, \ldots, t_n^{\pm 1}].$$

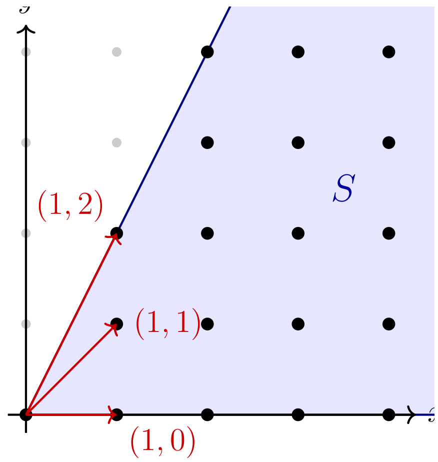
Example 1.26. Let

$$S = \mathbb{N}\{(1,0), (1,1), (1,2)\} \subseteq \mathbb{Z}^2.$$

Then

$$\Bbbk[S] = \Bbbk[t_1, t_1t_2, t_1t_2^2] \subseteq \Bbbk[t_1, t_2].$$

Notice that $(1,1) = \frac{1}{2}((1,0) + (1,2)) \in \mathrm{pos}\{(1,0), (1,2)\}$, but $(1,1)$ cannot be written as a sum of other nonzero elements in S, so it is a necessary Hilbert-basis element.



Proposition 1.27. *Let S be an affine semigroup. Then:*

(1) $\Bbbk[S]$ *is an integral domain.*

(2) $\dim \Bbbk[S] = \operatorname{rank}(S)$. *If $S = \sigma \cap \mathbb{Z}^n$, then* $\dim \Bbbk[S] = \dim \sigma$.

(3) $\Bbbk[S]$ *is a finitely generated* $\Bbbk$*-algebra.*

(4) *If S is saturated, then $\Bbbk[S]$ is integrally closed.*

Proof. Since $\Bbbk[S]$ embeds into the Laurent polynomial ring

$$\Bbbk[t_1^{\pm 1}, \dots, t_n^{\pm 1}],$$

it is an integral domain.

The dimension statement follows because the fraction field of $\Bbbk[S]$ is generated by the characters corresponding to the group $\mathbb{Z}S$. Therefore the transcendence degree of $\operatorname{Frac}(\Bbbk[S])$ over $\Bbbk$ is $\operatorname{rank}(S)$, and hence

$$\dim \Bbbk[S] = \operatorname{rank}(S).$$

If $S = \mathbb{N}\{m_1, \dots, m_r\}$, then

$$\Bbbk[S] = \Bbbk[t^{m_1}, \dots, t^{m_r}],$$

which proves it is finitely generated.

Finally, the equivalence between saturation of S and normality of $\Bbbk[S]$ is the standard normality criterion for affine semigroup rings □

Remark 1.28. The last point is the algebraic heart of the toric dictionary:

$$S \text{ saturated} \iff \Bbbk[S] \text{ normal}$$

Affine toric varieties are exactly spectra of saturated affine semigroup rings.

Presentations by Binomial Ideals

Let

$$S = \mathbb{N}\{m_1, \dots, m_r\} \subseteq \mathbb{Z}^n.$$

There is a surjective $\Bbbk$-algebra homomorphism

$$\varphi : \Bbbk[T_1, \dots, T_r] \longrightarrow \Bbbk[S]$$

given by

$$T_i \longmapsto t^{m_i}.$$

By the First Isomorphism Theorem,

$$\Bbbk[S] \cong \frac{\Bbbk[T_1, \dots, T_r]}{\ker \varphi}.$$

Example 1.29. Let

$$S = \mathbb{N}\{(1,0), (1,1), (1,2)\}.$$

Let

$$m_1 = (1,0), \qquad m_2 = (1,1), \qquad m_3 = (1,2).$$

The map is

$$\varphi : \Bbbk[T_1, T_2, T_3] \longrightarrow \Bbbk[S]$$

with

$$T_1 \longmapsto t_1, \qquad T_2 \longmapsto t_1 t_2, \qquad T_3 \longmapsto t_1 t_2^2.$$

Notice that

$$m_1 + m_3 = 2m_2,$$

which implies that

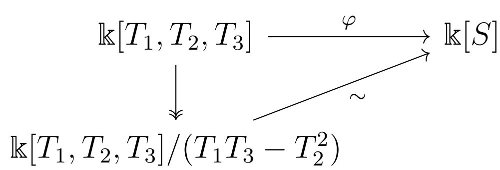
$$\varphi(T_1 T_3) = t_1^2 t_2^2 = \varphi(T_2^2).$$

Thus,

$$T_1 T_3 - T_2^2 \in \ker \varphi.$$

In fact, it is true that $\ker \varphi = (T_1T_3 - T_2^2)$, so

$$\Bbbk[S] \cong \frac{\Bbbk[T_1, T_2, T_3]}{(T_1T_3 - T_2^2)}.$$



Theorem 1.30 (Affine semigroup rings have binomial presentations)**.** *Let S be an affine semigroup generated by $m_1, \ldots, m_r$. Then*

$$\Bbbk[S] \cong \frac{\Bbbk[T_1, \ldots, T_r]}{I_S},$$

where I_S is a binomial ideal.

Proof. The map

$$\varphi : \Bbbk[T_1, \ldots, T_r] \to \Bbbk[S], \qquad T_i \mapsto t^{m_i},$$

maps monomials to monomials. For $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$, we have

$$\varphi(T^\alpha) = t^{\alpha_1 m_1 + \cdots + \alpha_r m_r}.$$

Thus $\varphi(T^\alpha) = \varphi(T^\beta)$ when

$$\sum_{i=1}^{r} \alpha_i m_i = \sum_{i=1}^{r} \beta_i m_i.$$

The kernel is generated by the binomials $T^\alpha - T^\beta$. □

Multigrading and Affine Toric Geometry

The semigroup ring $\Bbbk[S]$ is naturally graded by the group $\mathbb{Z}S$:

$$\deg(t^m) = m.$$

Under the presentation

$$\Bbbk[S] \cong \Bbbk[T_1, \ldots, T_r]/I_S,$$

this corresponds to setting

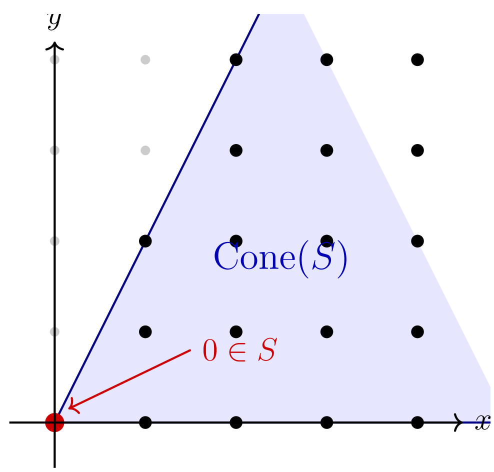
$$\deg(T_i) = m_i.$$

Geometrically, the presentation

$$\Bbbk[S] \cong \frac{\Bbbk[T_1, \ldots, T_r]}{I_S}$$

gives a closed embedding of the affine toric variety into affine space:

$$\operatorname{Spec} \Bbbk[S] \hookrightarrow \operatorname{Spec} \Bbbk[T_1, \ldots, T_r] \cong \mathbb{A}^r.$$



Remark 1.31. The final note from the lecture is that the minimal graded free resolution of binomial ideals is far from understood. Thus, even though affine semigroup rings have explicit binomial presentations, the homological algebra of their defining ideals can be highly nontrivial.

2 Lecture 2- May 26, 2026

Affine Semigroups and Hilbert Series

Let $G \subseteq \mathbb{R}^n$ be a rational polyhedral cone defined by:

$$\sigma = \{x \mid Ax \geq 0\} \subseteq \mathbb{R}^n, \quad A \in \mathbb{Z}^{m \times n},\ m \geq n$$

Assume that σ is strongly convex, meaning $\sigma \cap (-\sigma) = \{0\}$.

We define the affine semigroup S as:

$$S = \sigma \cap \mathbb{Z}^n$$

The cone σ can also be described as the positive hull of S:

$$\sigma = \text{pos}(S) = \left\{\sum \lambda_i s_i \mid \lambda_i \geq 0,\ s_i \in S\right\}$$

We assume $\dim(G) = n$.

Let K be a field with $\text{char}(K) = 0$. The semigroup ring is given by:

$$K[S] = K[\sigma \cap \mathbb{Z}^n]$$

This ring can be graded in two ways:

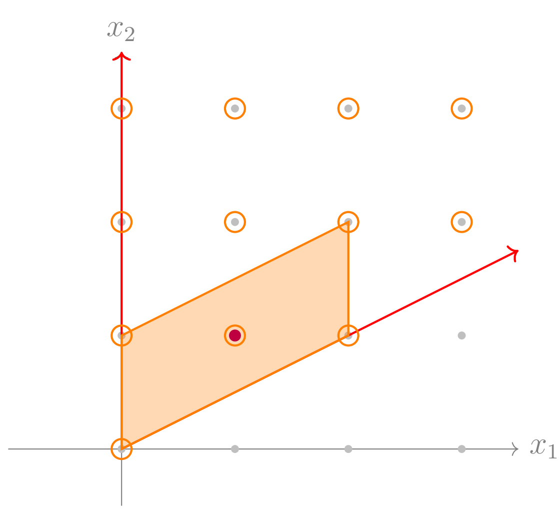
1. **Fine grading:** $K[S]$ is graded by $\mathbb{Z}^n$, where $\deg(t^m) = m$.
2. **Coarse grading:** $K[t^m \mid m \in S]$ is graded by $\mathbb{Z}$, where $\deg(t^m) = \sum m_i$.

Definition 2.1 (Hilbert Series)**.** Using the fine grading, the Hilbert series of $K[S]$ is given by:

$$\text{Hilb}(K[S]; z) = \sum_{m \in S} z^m$$

Example 2.2. Consider the cone in $\mathbb{R}^2$ defined by the inequalities $x_1 \geq 0$ and $-x_1+2x_2 \geq 0$. The rays of this cone are generated by the columns of the matrix:

$$\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}$$



Notice that the subsemigroup generated by the rays does not cover the entire intersection $\sigma \cap \mathbb{Z}^2$:

$$\mathbb{Z}\left[\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}\right] \subseteq \mathbb{Z}^2$$

It's not covering the whole thing; the point corresponding to $z_1 z_2$ (which is $(1,1)$) is missing from the ray generators.
The generating function for just the rays would be:

$$\begin{aligned} H\left(\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}\right) &= \left(\frac{1}{1-z_2}\right) \times \left(\frac{1}{1-z_1^2 z_2}\right) \\ &= (1 + z_2 + z_2^2 + \dots) \times (1 + z_1^2 z_2 + \dots) \\ &= 1 + z_2 + z_1^2 z_2 + z_2^2 + z_1^2 z_2^2 + \dots \end{aligned}$$

To get the full Hilbert series, we must account for the missing point $(1,1)$ inside the fundamental parallelogram. Thus, the correct Hilbert series is:

$$\begin{aligned} \mathrm{Hilb}(K[S]; z_1, z_2) &= \frac{1}{(1-z_2)(1-z_1^2 z_2)} + \frac{z_1 z_2}{(1-z_2)(1-z_1^2 z_2)} \\ &= \frac{1 + z_1 z_2}{(1-z_2)(1-z_1^2 z_2)} \end{aligned}$$

Now, assume σ is simplicial, meaning $\sigma = \mathrm{pos}\{v_1, \dots, v_n\}$ where the v_i are linearly independent and the gcd of the entries of each v_i is 1. We define the fundamental parallelogram as:

$$\mathrm{Par}\{v_1, \dots, v_n\} = \left\{\sum \lambda_i v_i \mid 0 \le \lambda_i < 1\right\}$$

Theorem 2.3. *If σ is simplicial, the Hilbert series is given by:*

$$Hilb(K[S]; z) = \frac{\sum_{m \in Par \cap \mathbb{Z}^n} z^m}{\prod_{i=1}^n (1 - z^{v_i})}$$

Remark 2.4. Refer to the graph on the previous page to explain how points in the fundamental parallelogram shift the ray-generated points to cover the entire semigroup cone.

Cohen-Macaulay Property and Free Resolutions

Let $\sigma = \mathrm{pos}\{v_1, \dots, v_e\}$ with $e \ge n$ being finite. We have:

$$K[t^{v_1}, \dots, t^{v_e}] \subseteq K[S] \quad \text{(finite)}$$

The polynomial ring $K[T_1, \ldots, T_e]$ (which is not finite) maps surjectively onto $K[S]$ via $T_i \mapsto t^{v_i}$. This implies that $K[S]$ is a finite $K[T]$-module.

Taking $Q = K[T]$, we can construct a graded free resolution of Q-modules:

$$0 \to F_p \to \cdots \to F_1 \to F_0 \to K[S] \to 0$$

This yields a rational expression for the Hilbert series:

$$\mathrm{Hilb}(K[S]; z) = \frac{P(z)}{\prod_{i=1}^{e}(1 - z^{v_i})}$$

Theorem 2.5 (Hochster)**.** *$K[S]$ is Cohen-Macaulay (CM). Recall that $K[S]$ is CM if and only if one (equivalently every) homogeneous system of parameters (hsop) is a regular sequence.*

Under the coarse grading, let $\theta_1, \theta_2, \ldots, \theta_n \in K[S]$ be a homogeneous system of parameters. If $K[S]$ is a finite module over $K[\theta_1, \ldots, \theta_n]$, then the hsop is a regular sequence if and only if $K[S]$ is a free module over $K[\theta_1, \ldots, \theta_n]$.

Theorem 2.6. *If $\theta_1, \ldots, \theta_n$ are a regular sequence, then:*

$$\mathit{Hilb}(K[S]; z) = \frac{\sum z^{\deg(\eta_i)}}{\prod_{i=1}^{n}(1 - z^{\deg(\theta_i)})}$$

where $\eta_1, \ldots, \eta_s$ are a basis for $K[S]$ as a $K[\theta_1, \ldots, \theta_n]$-module.

Remark 2.7. A homogeneous system of parameters exists in $K[S]$, existing in degree 1 by Noether Normalization. Here, the semigroup S needs to be saturated.

Local Cohomology and the Canonical Module

Proof Strategy: Stanley and Ishida compute the local cohomology to prove these properties.

Let $I \subseteq K[S]$ be the ideal $I = \langle t^m \mid m \in S,\, m \neq 0 \rangle$. Define the left exact additive functor:

$$L_I(M) = \{u \in M \mid I^n u = 0 \text{ for } n \gg 0\}$$

The local cohomology modules are defined as the right derived functors:

$$H_I^i(M) = R^i L_I(M)$$

We can compute this using the Čech / Ishida complex.

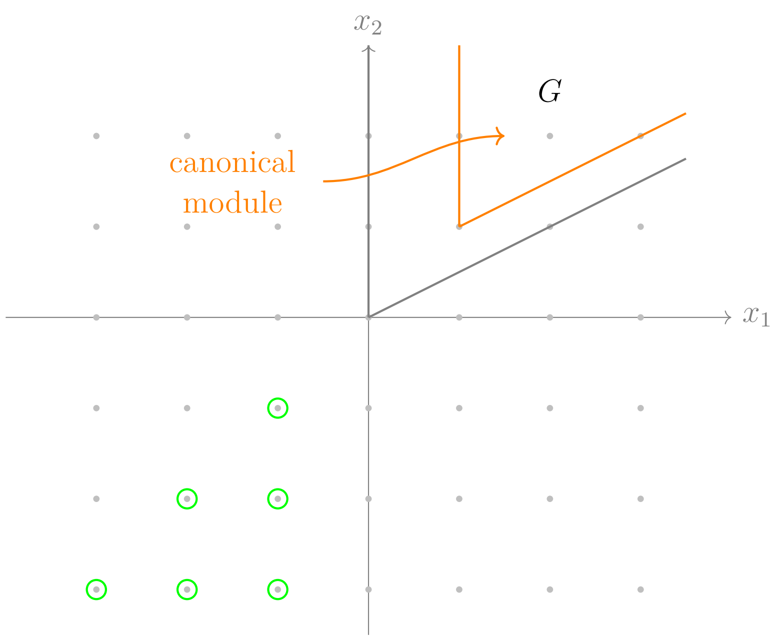
General picture:

$$H_I^i(K[S]) = 0 \text{ for } 0 \leq i < n$$

For the top cohomology:

$$H_I^n(K[S]) = K\{t^m \mid A(-m) > 0, \, m \in \mathbb{Z}^n\}$$

which is supported on $Am < 0$. Geometrically, this corresponds to lattice points in the strict interior of the opposite cone, $-\text{int}(\sigma)$.



> **Definition 2.8** (Canonical Module)**.** The canonical module $\Omega(K[S])$ is defined algebraically by:
> $$\Omega(K[S]) = K\{t^m \mid Am > 0\} = K\{\text{int}(\sigma)\}$$

This implies that $\Omega(K[S])$ is an ideal of $K[S]$. If $\Omega(K[S]) \sim K[S]$ as modules, it implies that $K[S]$ is a Gorenstein ring.

For the running example, the generator of the interior of the cone is $t^{(1,1)}$. Thus:

$$\Omega(K[S]) = t^{(1,1)} \cdot K[S] \implies \text{Gorenstein}$$

3 Lecture 3- May 27, 2026

Affine Semigroup Rings and Canonical Modules

Let $\sigma \subseteq \mathbb{R}^n$ be a rational polyhedral cone. We write it both by inequalities and by generators:

$$\sigma = \{x \in \mathbb{R}^n \mid Ax \geq 0\} = \operatorname{pos}\{v_1, \dots, v_\ell\}, \qquad v_i \in \mathbb{Z}^n, \qquad \ell > n.$$

Let

$$R = K[\sigma \cap \mathbb{Z}^n]$$

$$R = \bigoplus_{a \in \sigma \cap \mathbb{Z}^n} K \cdot x^a, \qquad \deg(x^a) = a.$$

$$\Omega_R = K\{\sigma^\circ \cap \mathbb{Z}^n\}.$$

$$\Omega_R = \bigoplus_{a \in \sigma^\circ \cap \mathbb{Z}^n} K \cdot x^a.$$

Remark 3.1. For a normal affine semigroup ring $R = K[\sigma \cap \mathbb{Z}^n]$, the formula

$$\Omega_R = K\{\sigma^\circ \cap \mathbb{Z}^n\}$$

Let

$$Q = K[T_1, \dots, T_\ell], \qquad \deg(T_i) = v_i \in \mathbb{Z}^n.$$

$$Q \longrightarrow R, \qquad T_i \longmapsto x^{v_i},$$

Since R is finite over Q, it admits a finite graded free resolution

$$0 \longrightarrow F_p \longrightarrow F_{p-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow R \longrightarrow 0.$$

$$0 \longrightarrow F_0^* \longrightarrow F_1^* \longrightarrow \cdots \longrightarrow F_p^* \longrightarrow \Omega_R \longrightarrow 0,$$

$$F_i^* = \operatorname{Hom}_Q(F_i, Q).$$

$$\operatorname{Hom}_Q(Q(a), Q) \cong Q(-a).$$

Theorem 3.2 (Hilbert-series reciprocity for affine semigroup rings)**.** *Let $R = K[\sigma \cap \mathbb{Z}^n]$ be a normal affine semigroup ring of dimension d, and let Ω_R be its canonical module. Then*

$$\operatorname{Hilb}(\Omega_R; \underline{z}) = (-1)^d \operatorname{Hilb}(R; \underline{z}^{-1}).$$

$$\operatorname{Hilb}(R; \underline{z}) = (-1)^d \operatorname{Hilb}(\Omega_R; \underline{z}^{-1}).$$

Lattice Polytopes and Ehrhart Functions

Let $P \subseteq \mathbb{R}^n$ be a bounded polytope. It may be described by inequalities

$$P = \{x \in \mathbb{R}^n \mid Ax \geq b\},$$

$$P = \operatorname{conv}(V), \qquad V \subseteq \mathbb{R}^n, \qquad |V| < \infty.$$

$$P = \left\{ \sum_i \lambda_i v_i \;\middle|\; v_i \in V,\ \lambda_i \geq 0,\ \sum_i \lambda_i = 1 \right\}.$$

Definition 3.3 (Lattice polytope)**.** A polytope $P \subseteq \mathbb{R}^n$ is called a *lattice polytope* if all of its vertices lie in the integer lattice:

$$V(P) \subseteq \mathbb{Z}^n.$$

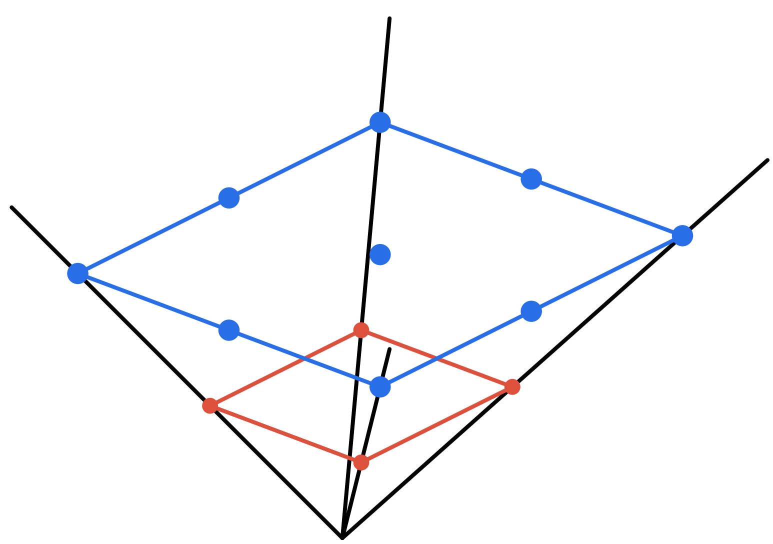
For $m \in \mathbb{N}$, define the Ehrhart counting function

$$i(P, m) = |mP \cap \mathbb{Z}^n|.$$

The Cone Over a Polytope

Let $P \subseteq \mathbb{R}^n$ be a lattice polytope. The cone over P is

$$\sigma_P = \operatorname{pos}\{(v, 1) \mid v \in V(P)\} \subseteq \mathbb{R}^{n+1}.$$



The intersection of σ_P with the hyperplane of height m is naturally identified with mP:

$$\sigma_P \cap \{x_{n+1} = m\} \cong mP.$$

$$\sum_i \lambda_i(v_i, 1) = \left(\sum_i \lambda_i v_i, \sum_i \lambda_i\right), \qquad \lambda_i \geq 0,$$

$$\sum_i \lambda_i v_i = m \sum_i \frac{\lambda_i}{m} v_i \in mP.$$

The semigroup ring

$$K[\sigma_P \cap \mathbb{Z}^{n+1}]$$

$$\deg(x^a t^m) = m.$$

$$K[\sigma_P \cap \mathbb{Z}^{n+1}] = \bigoplus_{m \geq 0} R_m, \qquad \dim_K R_m = |mP \cap \mathbb{Z}^n|.$$

Remark 3.4. The semigroup ring $K[\sigma_P \cap \mathbb{Z}^{n+1}]$ is not necessarily generated in degree 1. This is why one must be careful when using Noether normalization by linear forms. The degree-one part corresponds to lattice points of P, but these need not generate all lattice points of the cone.

The Hilbert series of $K[\sigma_P \cap \mathbb{Z}^{n+1}]$ is precisely the Ehrhart series of P:

$$\mathrm{Hilb}(K[\sigma_P \cap \mathbb{Z}^{n+1}]; z) = \sum_{m \geq 0} (\dim_K R_m) z^m = \sum_{m \geq 0} i(P, m) z^m.$$

$$E_P(z) = \sum_{m \geq 0} i(P, m) z^m.$$

Cohen–Macaulayness and Rationality of the Ehrhart Series

Theorem 3.5 (Hochster)**.** *Let σ be a rational polyhedral cone. If the affine semigroup $\sigma \cap \mathbb{Z}^n$ is normal, then the semigroup ring*

$$K[\sigma \cap \mathbb{Z}^n]$$

is Cohen–Macaulay.

Applying this to σ_P, the Ehrhart ring

$$K[\sigma_P \cap \mathbb{Z}^{n+1}]$$

is Cohen–Macaulay.

Let

$$R = K[\sigma_P \cap \mathbb{Z}^{n+1}].$$

$$\dim R = n + 1.$$

Choose a homogeneous system of parameters

$$\theta_0, \theta_1, \ldots, \theta_n$$

Remark 3.6. The notes indicate the existence of a linear homogeneous system of parameters via finite extensions. The relevant commutative algebra principle is Noether normalization: a finitely generated graded K-algebra admits a polynomial subring

$$K[\theta_0, \ldots, \theta_n] \subseteq R$$

over which it is module-finite.

Thus the Hilbert series has the form

$$\mathrm{Hilb}(R; z) = \frac{h_0^* + h_1^* z + \cdots + h_s^* z^s}{(1-z)^{n+1}},$$

$$h_j^* \in \mathbb{N}, \qquad 0 \leq s \leq n.$$

$$E_P(z) = \frac{\sum_{j=0}^{n} h_j^* z^j}{(1-z)^{n+1}}, \qquad h_j^* \in \mathbb{N}.$$

$$h^*(P) = (h_0^*, h_1^*, \ldots, h_n^*)$$

Remark 3.7. The handwritten note

$$\boxed{\deg(\mathrm{Hilb}) < 0 \text{ related } H^d(P) \text{ is negative degree}}$$

Ehrhart Polynomial

Expanding the denominator by the binomial series gives

$$\frac{1}{(1-z)^{n+1}} = \sum_{m \geq 0} \binom{n+m}{n} z^m.$$

$$E_P(z) = \left(\sum_{j=0}^{n} h_j^* z^j \right) \left(\sum_{m \geq 0} \binom{n+m}{n} z^m \right).$$

Comparing coefficients of z^m yields

$$i(P, m) = h_0^* \binom{n+m}{n} + h_1^* \binom{n+m-1}{n} + \cdots + h_n^* \binom{m}{n}.$$

$$\dim_K R_m = i(P, m) = |mP \cap \mathbb{Z}^n|.$$

Recall that

$$\binom{a}{b} = \frac{a!}{b!(a-b)!} = \frac{a(a-1)\cdots(a-b+1)}{b!}.$$

$$\binom{n+m}{n} = \frac{1}{n!}(n+m)(n+m-1)\cdots(m+1) \in \mathbb{Q}[m].$$

$$\frac{m^n}{n!}\left(h_0^* + h_1^* + \cdots + h_n^*\right).$$

Theorem 3.8 (Ehrhart's theorem)**.** *Let $P \subseteq \mathbb{R}^n$ be an n-dimensional lattice polytope. Then*

$$i(P, m) = |mP \cap \mathbb{Z}^n|$$

is a polynomial in m of degree n, and

$$i(P, m) = \operatorname{vol}(P) m^n + \textit{lower-degree terms},$$

where $\operatorname{vol}(P)$ is the normalized Euclidean volume.

Proof. The Ehrhart series has the rational form

$$E_P(z) = \frac{\sum_{j=0}^n h_j^* z^j}{(1-z)^{n+1}}.$$

$$i(P, m) = \sum_{j=0}^n h_j^* \binom{n+m-j}{n},$$

Each term $\binom{n+m-j}{n}$ is a polynomial in m of degree n with leading coefficient $1/n!$. Therefore

$$i(P, m) = \frac{h_0^* + \cdots + h_n^*}{n!} m^n + \text{lower-degree terms}.$$

$$\operatorname{vol}(P) = \frac{h_0^* + \cdots + h_n^*}{n!}.$$

□

The main consequences are:

(1) $i(P, m)$ is a polynomial in m.

(2) $\deg i(P, m) = n = \dim P$.

(3) The leading coefficient is

$$\frac{h_0^* + \cdots + h_n^*}{n!} = \operatorname{vol}(P).$$

Equivalently,

$$|mP \cap \mathbb{Z}^n| = \left|P \cap \frac{1}{m}\mathbb{Z}^n\right| = a_n m^n + a_{n-1}m^{n-1} + \cdots,$$

$$a_n = \mathrm{vol}(P).$$

Basic Properties of the h^*-Vector

The h^*-vector satisfies the following fundamental properties:

$$h_0^* = 1,$$

and

$$h_n^* = |P^\circ \cap \mathbb{Z}^n|.$$

Indeed, substituting $m = 0$ gives

$$i(P, 0) = 1,$$

$$i(P, 0) = h_0^*\binom{n}{n} + h_1^*\binom{n-1}{n} + \cdots + h_n^*\binom{0}{n}$$

Substituting $m = 1$ gives

$$|P \cap \mathbb{Z}^n| = h_0^*\binom{n+1}{n} + h_1^*\binom{n}{n} + h_2^*\binom{n-1}{n} + \cdots + h_n^*\binom{1}{n}.$$

$$\binom{k}{n} = 0 \qquad \text{for } 0 \le k < n,$$

$$|P \cap \mathbb{Z}^n| = (n+1)h_0^* + h_1^*.$$

$$h_1^* = |P \cap \mathbb{Z}^n| - n - 1.$$

Ehrhart–Macdonald Reciprocity

The binomial-coefficient expression for $i(P, m)$ can be evaluated at negative integers. Substituting $-m$ gives

$$i(P, -m) = h_0^*\binom{n-m}{n} + h_1^*\binom{n-m-1}{n} + \cdots + h_n^*\binom{-m}{n}.$$

$$\binom{-r}{n} = (-1)^n\binom{r+n-1}{n},$$

$$i(P, -m) = (-1)^n\left(h_n^*\binom{n+m-1}{n} + h_{n-1}^*\binom{n+m-2}{n} + \cdots + h_0^*\binom{m-1}{n}\right).$$

Theorem 3.9 (Ehrhart–Macdonald reciprocity). *Let $P \subseteq \mathbb{R}^n$ be an n-dimensional lattice polytope. Then, for every positive integer m,*

$$i(P, -m) = (-1)^n |mP^\circ \cap \mathbb{Z}^n|.$$

$$i(P^\circ, m)(-1)^n = i(P, -m),$$

$$i(P^\circ, m) = |mP^\circ \cap \mathbb{Z}^n|.$$

Taking $m = 1$ in Ehrhart–Macdonald reciprocity gives

$$i(P, -1) = (-1)^n |P^\circ \cap \mathbb{Z}^n|.$$

$$i(P, -1) = h_0^* \binom{n-1}{n} + h_1^* \binom{n-2}{n} + \cdots + h_{n-1}^* \binom{0}{n} + h_n^* \binom{-1}{n}.$$

$$\binom{k}{n} = 0 \qquad \text{for } 0 \leq k < n,$$

$$\binom{-1}{n} = (-1)^n.$$

$$i(P, -1) = (-1)^n h_n^*.$$

$$(-1)^n h_n^* = (-1)^n |P^\circ \cap \mathbb{Z}^n|,$$

$$h_n^* = |P^\circ \cap \mathbb{Z}^n|.$$

Example: The Unit Cube

Example 3.10 (The standard unit cube). Let

$$P = [0, 1]^n = \square_n$$

$$P = \{x \in \mathbb{R}^n \mid 0 \leq x_i \leq 1 \text{ for all } i\}.$$

$$mP = [0, m]^n.$$

$$i(P, m) = |[0, m]^n \cap \mathbb{Z}^n| = (m + 1)^n.$$

$$E_P(z) = \sum_{m \geq 0} (m + 1)^n z^m.$$

For $n = 5$, one obtains

$$E_P(z) = \sum_{m \geq 0} (m + 1)^5 z^m = \frac{1 + 26z + 66z^2 + 26z^3 + z^4 + 0 \cdot z^5}{(1 - z)^6}.$$

$$h^*(\square_5) = (1, 26, 66, 26, 1, 0).$$

4 Lecture 4- May 28, 2026

Ehrhart theory

Definition 4.1 (Lattice polytope)**.** A *lattice polytope* is a polytope

$$P = \mathrm{conv}(V) \subseteq \mathbb{R}^n$$

Definition 4.2 (Ehrhart function and Ehrhart polynomial)**.** Let $P \subseteq \mathbb{R}^n$ be a lattice polytope of dimension n. For $m \in \mathbb{N}$, define

$$i(P, m) = |mP \cap \mathbb{Z}^n|.$$

$$i(P, m) \in \mathbb{Q}[m].$$

Definition 4.3 (Ehrhart series)**.** The Ehrhart series of P is the generating function

$$E_P(z) = \sum_{m \geq 0} i(P, m) z^m \in \mathbb{Q}[[z]].$$

$$E_P(z) = \frac{h_P^*(z)}{(1-z)^{n+1}},$$

$$h_P^*(z) = h_0^* + h_1^* z + \cdots + h_s^* z^s$$

Theorem 4.4 (Stanley nonnegativity theorem)**.** *Let $P \subseteq \mathbb{R}^n$ be a lattice polytope. Then*

$$h_P^*(z) = h_0^* + h_1^* z + \cdots + h_s^* z^s$$

$$h_i^* \geq 0 \qquad \text{for all } i.$$

Remark 4.5 (Basic facts about the h^*-polynomial)**.** The constant term is always

$$h_0^* = 1.$$

$$h_P^*(1) = \sum_{i=0}^{s} h_i^*$$

Remark 4.6 (Monotonicity). If $P \subseteq P'$ are lattice polytopes, then the corresponding h^*-vectors satisfy coefficientwise monotonicity:

$$h^*(P) \leq h^*(P').$$

$$h_i^*(P) \leq h_i^*(P') \qquad \text{for all } i.$$

The affine semigroup ring of a polytope

Let $P = \text{conv}(V) \subseteq \mathbb{R}^n$ be a lattice polytope. Consider the cone over P:

$$\sigma_P = \text{pos}\{(v, 1) \mid v \in V\} \subseteq \mathbb{R}^{n+1}.$$

$$S_P = \sigma_P \cap \mathbb{Z}^{n+1}.$$

$$R = \Bbbk[S_P] = \Bbbk[\sigma_P \cap \mathbb{Z}^{n+1}].$$

The grading is given by the last coordinate:

$$\deg(a, m) = m \qquad \text{for } (a, m) \in S_P.$$

$$R = \bigoplus_{m \geq 0} R_m,$$

$$\dim_\Bbbk R_m = |mP \cap \mathbb{Z}^n| = i(P, m).$$

$$\text{Hilb}(R, z) = \sum_{m \geq 0} (\dim_\Bbbk R_m) z^m = E_P(z) = \frac{h_P^*(z)}{(1-z)^{n+1}}.$$

Remark 4.7. The semigroup $S_P = \sigma_P \cap \mathbb{Z}^{n+1}$ is saturated because it is the set of lattice points in a rational cone. Hochster's theorem states that the semigroup ring of a positive normal affine semigroup is Cohen–Macaulay. This is the commutative algebra input behind Stanley's proof of nonnegativity of the h^*-vector.

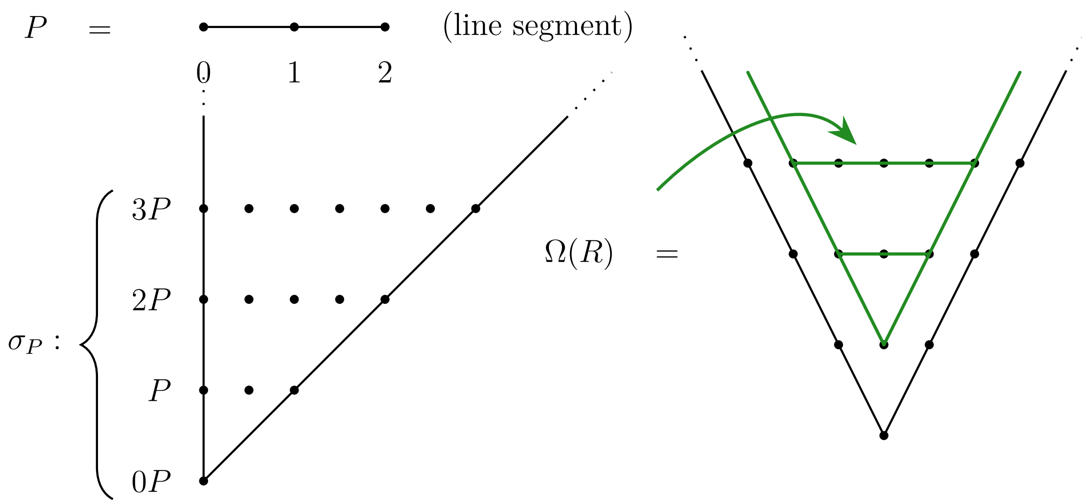
Choose a homogeneous system of parameters

$$\theta_1, \theta_2, \ldots, \theta_{n+1}$$

Then,

$$\text{Hilb}\Big(R/(\theta_1, \ldots, \theta_{n+1}), z\Big) = h_P^*(z).$$

$$h_i^* = \dim_\Bbbk \left(R/(\theta_1, \ldots, \theta_{n+1})\right)_i \geq 0.$$



A Stanley-Type Inequality for h^*-Vectors

Theorem 4.8 (Theorem 2)**.** *Let P be a lattice polytope and let*

$$h_P^*(z) = h_0^* + h_1^* z + \cdots + h_s^* z^s$$

$$h_0^* + h_1^* + \cdots + h_i^* \leq h_s^* + h_{s-1}^* + \cdots + h_{s-i}^*$$

Proof. Let

$$R = \Bbbk[\sigma_P \cap \mathbb{Z}^{n+1}]$$

$$\Omega = \Omega_0 \oplus \Omega_1 \oplus \Omega_2 \oplus \cdots .$$

$$H(\Omega, z) = \frac{h_s^* + h_{s-1}^* z + \cdots + h_0^* z^s}{(1-z)^{n+1}}.$$

Let $u \in \Omega_0$. $0 \longrightarrow uR \hookrightarrow \Omega \longrightarrow \Omega/uR \longrightarrow 0$. Let $M = \Omega/uR$.

$$H(uR, z) = H(R, z) = \frac{h_0^* + h_1^* z + \cdots + h_s^* z^s}{(1-z)^{n+1}}.$$

$$\begin{aligned} H(M, z) &= H(\Omega, z) - H(uR, z) \\ &= \frac{\left(h_s^* + h_{s-1}^* z + \cdots + h_0^* z^s\right) - \left(h_0^* + h_1^* z + \cdots + h_s^* z^s\right)}{(1-z)^{n+1}}. \end{aligned}$$

Equivalently,

$$H(M, z) = \frac{\sum_{j=0}^{s} \left(h_{s-j}^* - h_j^*\right) z^j}{(1-z)^{n+1}}.$$

There are now two cases.

First, suppose that $\Omega \cong uR$. $\implies$ R is Gorenstein $\implies$ $h_i^* = h_{s-i}^*$
Otherwise,

$$M = \Omega/uR$$

$$\dim M = \dim R - 1 = n.$$

$$H(M, z) = \frac{k_0 + k_1 z + \cdots + k_t z^t}{(1-z)^n},$$

where $k_j \geq 0$.

$$H(M, z) = \frac{\sum_{j=0}^{s} \left(h_{s-j}^* - h_j^*\right) z^j}{(1-z)^{n+1}}.$$

Let $k(z) = k_0 + k_1 z + \cdots + k_t z^t$.

$$\sum_{j=0}^{s} \left(h_{s-j}^* - h_j^*\right) z^j = (1-z)k(z).$$

$$k_i = \sum_{j=0}^{i} \left(h_{s-j}^* - h_j^*\right) = \left(h_s^* + h_{s-1}^* + \cdots + h_{s-i}^*\right) - \left(h_0^* + h_1^* + \cdots + h_i^*\right).$$

Since $k_i \geq 0$,

$$0 \leq \left(h_s^* + h_{s-1}^* + \cdots + h_{s-i}^*\right) - \left(h_0^* + h_1^* + \cdots + h_i^*\right),$$

$$h_0^* + h_1^* + \cdots + h_i^* \leq h_s^* + h_{s-1}^* + \cdots + h_{s-i}^*.$$

□

Remark 4.9. The key algebraic mechanism is the inclusion

$$uR \subseteq \Omega_R.$$

An Inequality from Uniform Position

Theorem 4.10 (Theorem 3)**.** *Let P be a lattice polytope such that the Ehrhart ring $\Bbbk[\sigma_P \cap \mathbb{Z}^{n+1}]$ is generated in degree 1, and let*

$$h_P^*(z) = h_0^* + h_1^* z + \cdots + h_s^* z^s.$$

For $p + q < s$,

$$h_1^* + \cdots + h_q^* \leq h_{p+1}^* + \cdots + h_{p+q}^*.$$

Sketch of proof from the notes. Let

$$R = \Bbbk[\sigma_P \cap \mathbb{Z}^{n+1}].$$

$$\operatorname{Proj}(R) \hookrightarrow \mathbb{P}^N.$$

$$R' = R/(\Theta_1, \dots, \Theta_{n-1}),$$

The Hilbert series of R' is

$$H(R', z) = \frac{h_0^* + h_1^* z + \cdots + h_s^* z^s}{(1-z)^2}.$$

Let $C \subseteq \mathbb{P}^N$.

$$\Gamma = C \cap H.$$

Let $h_\Gamma(d)$ denote the Hilbert function of Γ in degree d. Since the points are in uniform position, Harris' uniform position principle gives the inequality

$$h_\Gamma(i+j) \geq \min\left\{\#\Gamma,\, h_\Gamma(i) + h_\Gamma(j) - 1\right\}.$$

$$H(\Gamma, z) = \frac{h_0^* + h_1^* z + \cdots + h_s^* z^s}{1-z}.$$

Since $\frac{1}{1-z} = 1 + z + z^2 + \cdots$,

$$h_\Gamma(d) = h_0^* + h_1^* + \cdots + h_d^*$$

$$\#\Gamma = h_0^* + h_1^* + \cdots + h_s^*.$$

Substituting the partial-sum expression into the uniform position inequality yields

$$h_0^* + \cdots + h_{i+j}^* \geq \min\Big\{h_0^* + \cdots + h_s^*,\, (h_0^* + \cdots + h_i^*) + (h_0^* + \cdots + h_j^*) - 1\Big\}.$$

Which implies:

$$h_1^* + \cdots + h_q^* \leq h_{p+1}^* + \cdots + h_{p+q}^*$$

□

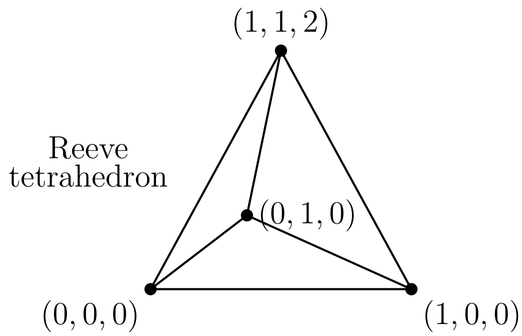
Remark 4.11. The assumption that R is generated in degree 1 is important because it allows the Ehrhart ring to define a standard graded projective embedding. This makes it possible to use projective-geometric tools such as Bertini's theorem and Harris' uniform position principle.

The Reeve tetrahedron

Example 4.12 (Reeve tetrahedron)**.** Consider the lattice polytope

$$P = \operatorname{conv}\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \subseteq \mathbb{R}^3.$$

$$(0,0,0), \quad (1,0,0), \quad (0,1,0), \quad (1,1,2).$$



The cone over P is generated by the columns of the matrix

$$\sigma_P = \operatorname{pos}\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Notice that the integer point $(1,1,1,2)^T$ belongs to σ_P. Because this point cannot be formed by adding integer points at height 1, the affine semigroup $\sigma_P \cap \mathbb{Z}^4$ is not generated in height 1.

For this Reeve tetrahedron, the h^*-vector is

$$(h_0^*, h_1^*, h_2^*, h_3^*) = (1,0,1,0).$$

$$3!\,\mathrm{Vol}(P) = 2,$$

$$h_P^*(1) = 1 + 0 + 1 + 0 = 2.$$

The failure of generation in degree 1 is reflected in the fact that the above uniform-position inequalities do not apply to this example.

Joins of Polytopes

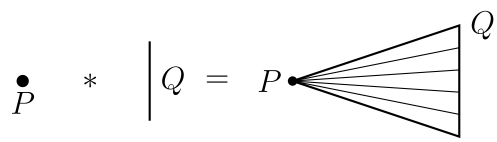
Definition and basic geometry

Definition 4.13 (Join of polytopes)**.** Let $P \subseteq \mathbb{R}^a$ and $Q \subseteq \mathbb{R}^b$ be nonempty polytopes. Their *join* is the polytope

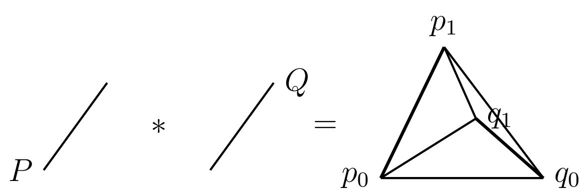
$$P * Q = \operatorname{conv}\Big(\{(p, 0_{\mathbb{R}^b}, 0) : p \in P\} \cup \{(0_{\mathbb{R}^a}, q, 1) : q \in Q\}\Big) \subseteq \mathbb{R}^{a+b+1}.$$

Remark 4.14. Geometrically, the join $P * Q$ is obtained by connecting every point of P to every point of Q by a line segment. If P and Q are nonempty, then

$$\dim(P * Q) = \dim P + \dim Q + 1.$$



join of a point and a segment



join of two segments: a tetrahedron

Example involving a segment

Example 4.15. Consider the join

$$P * [0, 3],$$

$$\dim P = 3 \qquad \text{and} \qquad \dim[0, 3] = 1,$$

$$\dim(P * [0, 3]) = 3 + 1 + 1 = 5.$$

The notes record the h^*-vector

$$(h_0^*, h_1^*, h_2^*, h_3^*, h_4^*) = (1, 2, 1, 2, 0).$$

Remark 4.16. The displayed h^*-vector has total sum

$$1 + 2 + 1 + 2 + 0 = 6.$$

Remark 4.17. There is a dimensional consistency issue in the raw notes: if P is the three-dimensional Reeve tetrahedron and $[0,3]$ is a one-dimensional segment, then the join has dimension 5, not 4. If instead the intended polytope has dimension 4, then the notation $P * [0,3]$ must refer to a lower-dimensional P or to a different construction. The mathematical content recorded above preserves the stated h^*-vector while flagging the dimensional ambiguity.

5 Lecture 5- May 29, 2026

Lattice polytopes and Ehrhart rings

Let

$$P = \operatorname{conv}(V) \subseteq \mathbb{R}^n$$

$$V \subseteq \mathbb{Z}^n.$$

Definition 5.1 (Cone over a lattice polytope)**.** The *cone over* P is the rational polyhedral cone

$$\sigma_P = \operatorname{pos}\Big\{(v, 1) \mid v \in V\Big\} \subseteq \mathbb{R}^{n+1}.$$

Remark 5.2. A point $(u, m) \in \mathbb{Z}^{n+1}$ lies in σ_P if and only if $m \geq 0$ and $u \in mP$. Hence the degree-m lattice points in σ_P encode the lattice points of the dilation mP.

Definition 5.3 (Ehrhart ring)**.** The *Ehrhart ring* of P is the affine semigroup ring

$$R = \Bbbk[\sigma_P \cap \mathbb{Z}^{n+1}].$$

$$\deg(x^u t^m) = m.$$

The canonical module of R is described by the interior lattice points of the cone:

$$\Omega_R = \Bbbk\Big[\operatorname{int}(\sigma_P) \cap \mathbb{Z}^{n+1}\Big].$$

Remark 5.4. This is an instance of Hochster's theorem: normal affine semigroup rings are Cohen–Macaulay. The semigroup $\sigma_P \cap \mathbb{Z}^{n+1}$ is saturated in its group, so its semigroup ring is normal.

Artinian reductions and the h^*-vector

Since R is Cohen–Macaulay of Krull dimension $n+1$, we may choose a linear system of parameters

$$\theta_1, \dots, \theta_{n+1} \in R.$$

$$A = R/(\theta_1, \dots, \theta_{n+1})R = \bigoplus_{i \geq 0} A_i.$$

$$\dim_{\Bbbk} A_i = h_i^*.$$

Definition 5.5 (Ehrhart polynomial and Ehrhart series)**.** The *Ehrhart function* of P is

$$i(P, m) = |mP \cap \mathbb{Z}^n|.$$

for $m \in \mathbb{N}$. The associated Ehrhart series is

$$E_P(z) = \sum_{m \geq 0} i(P, m) z^m.$$

The Ehrhart series has the rational form

$$E_P(z) = \frac{h_0^* + h_1^* z + \cdots + h_s^* z^s}{(1-z)^{n+1}}, \qquad s \leq n.$$

$$h_P^*(z) = h_0^* + h_1^* z + \cdots + h_s^* z^s$$

$$h^*(P) = (h_0^*, h_1^*, \dots, h_s^*, 0, \dots, 0) \in \mathbb{N}^{n+1}.$$

Remark 5.6. The equality

$$\dim_{\Bbbk} A_i = h_i^*$$

removes the denominator $(1-z)^{n+1}$ from the Hilbert series of R. Indeed,

$$\mathrm{Hilb}_R(z) = E_P(z) = \frac{h_P^*(z)}{(1-z)^{n+1}},$$

$$\mathrm{Hilb}_A(z) = h_P^*(z).$$

Reflexive polytopes

Definition 5.7 (Polar dual)**.** Assume that $0 \in \operatorname{int}(P)$. The *polar dual* of P is

$$P^{\vee} = \{y \in \mathbb{R}^n \mid \langle y, x\rangle \leq 1 \text{ for all } x \in P\}.$$

$$P^{\circ} = \{y \in \mathbb{R}^n \mid \langle y, x\rangle \geq -1 \text{ for all } x \in P\}.$$

Definition 5.8 (Reflexive lattice polytope)**.** A full-dimensional lattice polytope $P \subseteq \mathbb{R}^n$ is *reflexive* if

$$0 \in \operatorname{int}(P)$$

Remark 5.9. If P is reflexive, then P contains exactly one interior lattice point, namely the origin.

Remark 5.10. More generally, if a lattice polytope has a unique interior lattice point, then after translating this point to the origin one can ask whether the polar dual is a lattice polytope. Reflexivity is precisely this additional integrality condition on the polar dual.

Theorem 5.11 (Batyrev)**.** *Reflexive polytopes provide the combinatorial framework for a construction of mirror symmetry. In particular, the toric varieties associated to dual reflexive polytopes*

$$P \qquad \text{and} \qquad P^{\vee}$$

Theorem 5.12 (Lagarias–Ziegler; Batyrev)**.** *For every fixed dimension n, there are only finitely many reflexive n-dimensional lattice polytopes up to unimodular equivalence.*

Remark 5.13. The lecture notes indicate the finiteness theorem for reflexive polytopes. The standard references are Lagarias–Ziegler for finiteness phenomena of lattice polytopes with bounded data, and Batyrev for reflexive polytopes in the context of mirror symmetry.

Gorenstein polytopes and reflexive polytopes

Definition 5.14 (Gorenstein Ehrhart ring)**.** A lattice polytope P is called *Gorenstein* if its Ehrhart ring

$$R = \Bbbk[\sigma_P \cap \mathbb{Z}^{n+1}]$$

Remark 5.15. If P is Gorenstein, then the canonical module Ω_R is generated by one homogeneous monomial. Equivalently, the interior lattice points of σ_P are obtained from a single interior lattice point by adding the semigroup $\sigma_P \cap \mathbb{Z}^{n+1}$.

Theorem 5.16 (Hibi)**.** *A lattice polytope P is Gorenstein if and only if there exist $r \in \mathbb{N}$ and $\alpha \in \mathbb{Z}^n$ such that*

$$rP - \alpha$$

is reflexive.

Corollary 5.17. *If P is reflexive, then P is Gorenstein.*

Proof. If P is reflexive, then the statement follows from Hibi's criterion with $r = 1$ and $\alpha = 0$. □

Example 5.18 (The cube)**.** Let

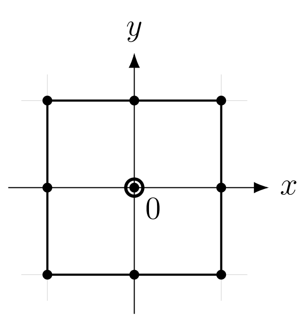
$$\square_n = [0, 1]^n.$$

over the affine semigroup, by

$$(1, \dots, 1, 2) \in \mathbb{Z}^{n+1}.$$

$$2\square_n - (1, \dots, 1) = [-1, 1]^n$$

For $n = 2$, the picture is the square $[-1, 1]^2$ with the origin as its unique interior lattice point.



$$2\square_2 - (1, 1) = [-1, 1]^2$$

Symmetry and unimodality of h^*-vectors

If P is reflexive of dimension n, then its Ehrhart ring is Gorenstein. Consequently, the h^*-polynomial is palindromic:

$$h_i^* = h_{n-i}^* \qquad \text{for all } 0 \le i \le n.$$

$$h^*(P) = (1, h_1^*, h_2^*, \dots, h_2^*, h_1^*, 1).$$

Definition 5.19 (Unimodality)**.** A sequence

$$(a_0, a_1, \dots, a_n)$$

is called *unimodal* if

$$a_0 \le a_1 \le \cdots \le a_j \ge a_{j+1} \ge \cdots \ge a_n.$$

If it is additionally symmetric, then unimodality means

$$a_0 \le a_1 \le \cdots \le a_{\lfloor n/2 \rfloor}.$$

Question 5.20 (Unimodality problem for reflexive polytopes)**.** If P is reflexive, must the h^*-vector of P be unimodal? Equivalently, must one have

$$h_0^* \le h_1^* \le \cdots \le h_{\lfloor n/2 \rfloor}^*?$$

Conjecture 5.21 (Ohsugi–Hibi [**?**])**.** For any IDP reflexive lattice polytope $P \subset \mathbb{R}^n$, the coefficients of the h^*-polynomial are unimodal:

$$h_0^* \le h_1^* \le \cdots \le h_{\lfloor d/2 \rfloor}^* = h_{\lceil n/2 \rceil}^* \ge \cdots \ge h_d^*.$$

This is the updated form of a conjecture of Hibi [**?**], after Mustaţă and Payne gave an example showing the necessity of the IDP assumption [**?**].

Remark 5.22. The statement sometimes appears with extra hypotheses, for example normality or standard generation of the Ehrhart ring. These hypotheses are important and should not be omitted. Reflexivity alone gives symmetry of the h^*-vector, but not unimodality.

Hard Lefschetz philosophy

Let

$$A = R/(\theta_1, \dots, \theta_{n+1})R = \bigoplus_{i=0}^{s} A_i$$

If R is Gorenstein, then A is an Artinian Gorenstein algebra. In this case the Hilbert function of A is symmetric:

$$\dim_{\Bbbk} A_i = \dim_{\Bbbk} A_{s-i}.$$

Definition 5.23 (Strong Lefschetz property)**.** The Artinian graded algebra A has the *strong Lefschetz property* if there exists a linear form $\ell \in A_1$ such that, for all k with $0 \le k \le \lfloor s/2 \rfloor$, the multiplication map

$$\times \ell^{s-2k} \colon A_k \longrightarrow A_{s-k}$$

is an isomorphism.

The Lefschetz maps have the form

$$A_0 \xrightarrow{\times \ell} A_1 \xrightarrow{\times \ell} A_2 \xrightarrow{\times \ell} A_3 \longrightarrow \cdots .$$

$$A_0 \xrightarrow{\quad \times \ell \quad} A_1 \xrightarrow{\quad \times \ell \quad} A_2 \xrightarrow{\quad \times \ell \quad} \cdots \xrightarrow{\quad \times \ell \quad} A_s$$

Proposition 5.24. *If A has the strong Lefschetz property, then the Hilbert function of A is unimodal. In particular, the h^*-vector of P is unimodal.*

Proof. For $i \le \lfloor s/2 \rfloor$, the strong Lefschetz property implies that multiplication by ℓ is injective:

$$\times \ell \colon A_{i-1} \hookrightarrow A_i.$$

$$\dim_{\Bbbk} A_{i-1} \le \dim_{\Bbbk} A_i.$$

$$h^*_{i-1} \le h^*_i \qquad \text{for } i \le \lfloor s/2 \rfloor.$$

imply unimodality. □

Equivalently, for $i \le \lfloor s/2 \rfloor$, if multiplication by ℓ is injective, then the quotient

$$B = A/\ell A$$

has dimension

$$\dim_{\Bbbk} B_i = \dim_{\Bbbk} A_i - \dim_{\Bbbk} A_{i-1} = h^*_i - h^*_{i-1} \ge 0.$$

Remark 5.25. The lecture notes mention work of Adiprasito, Papadakis, Petrotou, and Steinmeyer in connection with Lefschetz-type theorems for face rings and polyhedral or toric settings.

Question 5.26. Suppose P is normal, equivalently suppose the Ehrhart ring

$$\mathbb{k}[\sigma_P \cap \mathbb{Z}^{n+1}]$$

Remark 5.27. Normality or standard generation is a natural commutative-algebraic hypothesis because it says that every lattice point in mP decomposes as a sum of m lattice points in P. Equivalently, the semigroup of the cone is generated by its degree-1 elements.

Bounding lattice polytopes by h^*-data

Theorem 5.28 (Hensley, 1982)**.** *Fix positive integers n and K. If P is an n-dimensional lattice polytope with*

$$h_n^*(P) = K > 0,$$

only on n and K:

$$\mathrm{Vol}(P) < C(n, K).$$

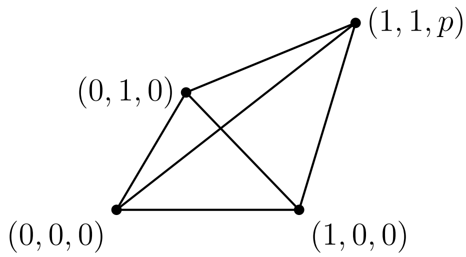
Remark 5.29. The assumption $K > 0$ is essential.

Example 5.30 (Unbounded volume when $h_n^* = 0$)**.** Consider the lattice simplex in $\mathbb{R}^3$ with vertices given as the columns of the matrix

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & p \end{bmatrix}.$$

$$P_p = \mathrm{conv}\{(0,0,0), (1,0,0), (0,1,0), (1,1,p)\}.$$

$$\mathrm{vol}(P_p) = \frac{p}{6}.$$



$\mathrm{vol}(P_p) = p/6$

Theorem 5.31 (Lagarias–Ziegler). *Fix n and $K > 0$. There are finitely many isomorphism classes, up to unimodular equivalence, of n-dimensional lattice polytopes satisfying*

$$h_n^*(P) = K.$$

Degree bounds and the theorem of Haase–Nill–Payne

Definition 5.32 (Degree of a lattice polytope)**.** The *degree* of P is the degree of its h^*-polynomial:

$$\deg(P) = s \qquad \text{where} \qquad h_P^*(z) = h_0^* + h_1^* z + \cdots + h_s^* z^s \quad \text{and } h_s^* \neq 0.$$

Theorem 5.33 (Haase–Nill–Payne, 2009)**.** *If P has degree s, then its volume is bounded above by a constant depending only on s and the leading nonzero h^*-coefficient h_s^*:*

$$\mathrm{Vol}(P) < C(s, h_s^*).$$

Corollary 5.34. *If P has fixed degree s and fixed leading coefficient*

$$h_s^*(P) = K,$$

$$h_0^* + h_1^* + \cdots + h_s^* = \mathrm{Vol}(P) < C(s, K),$$

Remark 5.35. The equality

$$h_0^* + \cdots + h_s^* = \mathrm{Vol}(P)$$

With Euclidean volume, the equality differs by the factor $n!$.

Consequently, if

$$h^*(P) = (h_0^*, h_1^*, \ldots, h_s^* = K),$$

$$h_i^* \le C(s, K, i).$$

h_n^* counts the number of interior lattice points of P:

$$h_n^* = |\operatorname{int}(P) \cap \mathbb{Z}^n|.$$

Socles of Artinian reductions

Let

$$A = A_0 \oplus A_1 \oplus \cdots \oplus A_s$$

$$\mathfrak{m} = A_+ = A_1 \oplus A_2 \oplus \cdots \oplus A_s.$$

Definition 5.36 (Socle)**.** The *socle* of A is

$$\operatorname{Soc}(A) = (0 :_A \mathfrak{m}) = \{a \in A \mid \mathfrak{m}a = 0\}.$$

homogeneous element of positive degree.

Remark 5.37. The standard socle definition is

$$\operatorname{Soc}(A) = (0 :_A \mathfrak{m}),$$

If A is Artinian Gorenstein with socle degree s, then

$$\operatorname{Soc}(A) = A_s$$

$$\dim_{\Bbbk} \operatorname{Soc}(A) = 1.$$

Remark 5.38. For a general Artinian reduction of a Cohen–Macaulay Ehrhart ring, it is not automatic that $\operatorname{Soc}(A) = A_s$. This equality holds in the Artinian Gorenstein case. In the non-Gorenstein case, the socle may have components in several degrees.

The lecture notes record the following guiding principle.

Proposition 5.39 (Guiding principle)**.** *Let P be a standard lattice polytope, so that its Ehrhart ring $R = \Bbbk[P]$ is generated in degree 1. Let*

$$A = R/(\ell_0, \ldots, \ell_n)$$

be an Artinian reduction by a linear system of parameters. Then

$$\dim_{\Bbbk} A_i = h_i^*(P).$$

If the top socle degree of A is bounded by s and the total socle dimension

$$\dim_{\Bbbk} \mathrm{Soc}(A)$$

is bounded by T, then the coefficients $h_i^*(P)$ are bounded in terms of s and T.

Remark 5.40. This principle reflects the fact that the Hilbert function of a standard graded Artinian algebra is constrained by Macaulay-type growth conditions. The socle records where multiplication by positive-degree elements fails to be injective, so controlling the socle gives information about the possible shape of the Hilbert function.

References

[Syl84] J. J. Sylvester. Mathematical questions with their solutions. *Educational Times*, 41:21, 1884.

[Gor73] Paul Gordan. Ueber die Auflösung linearer Gleichungen mit reellen Coefficienten. *Mathematische Annalen*, 6:23–28, 1873.

[Noe26] Emmy Noether. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 28–35, 1926.

[Hoc72] Melvin Hochster. Rings of invariants of tori, Cohen–Macauley rings generated by monomials, and polytopes. *Annals of Mathematics*, Second Series, 96(2):318–337, 1972.

[Sta74] Richard P. Stanley. Combinatorial reciprocity theorems. *Advances in Mathematics*, 14:194–253, 1974.

[Sta78] Richard P. Stanley. Hilbert functions of graded algebras. *Advances in Mathematics*, 28(1):57–83, 1978.

[Ish88] Masa-Nori Ishida. The local cohomology groups of an affine semigroup ring. In *Algebraic Geometry and Commutative Algebra, Vol. I*, pages 141–153. Kinokuniya, Tokyo, 1988.

[Ehr62] Eugène Ehrhart. Sur les polyèdres rationnels homothétiques à n dimensions. *Comptes rendus de l'Académie des Sciences de Paris*, 254:616–618, 1962.

[Ehr67] Eugène Ehrhart. Démonstration de la loi de réciprocité du polyèdre rationnel. *Comptes rendus de l'Académie des Sciences de Paris, Série A–B*, 265:A91–A94, 1967.

[Mac71] I. G. Macdonald. Polynomials associated with finite cell-complexes. *Journal of the London Mathematical Society*, Second Series, 4:181–192, 1971.

[Sta80] Richard P. Stanley. Decompositions of rational convex polytopes. *Annals of Discrete Mathematics*, 6:333–342, 1980.

[Sta91] Richard P. Stanley. On the Hilbert function of a graded Cohen–Macaulay domain. *Journal of Pure and Applied Algebra*, 73(3):307–314, 1991.

[Sta93] Richard P. Stanley. A monotonicity property of h-vectors and h^*-vectors. *European Journal of Combinatorics*, 14(3):251–258, 1993.

[ES96] David Eisenbud and Bernd Sturmfels. Binomial ideals. *Duke Mathematical Journal*, 84(1):1–45, 1996.

[Ree57] J. E. Reeve. On the volume of lattice polyhedra. *Proceedings of the London Mathematical Society*, Third Series, 7(1):378–395, 1957.

[Bat94] Victor V. Batyrev. Dual polyhedra and mirror symmetry for Calabi–Yau hypersurfaces in toric varieties. *Journal of Algebraic Geometry*, 3(3):493–535, 1994.

[Hib92] Takayuki Hibi. Dual polytopes of rational convex polytopes. *Combinatorica*, 12(2):237–240, 1992.

[OH06] Hidefumi Ohsugi and Takayuki Hibi. Special simplices and Gorenstein toric rings. *Journal of Combinatorial Theory, Series A*, 113(4):718–725, 2006.

[MP05] Mircea Mustaţă and Sam Payne. Ehrhart polynomials and stringy Betti numbers. *Mathematische Annalen*, 333(4):787–795, 2005.

[Hen83] Douglas Hensley. Lattice vertex polytopes with interior lattice points. *Pacific Journal of Mathematics*, 105(1):183–191, 1983.

[LZ91] Jeffrey C. Lagarias and Günter M. Ziegler. Bounds for lattice polytopes containing a fixed number of interior points in a sublattice. *Canadian Journal of Mathematics*, 43(5):1022–1035, 1991.

[HNP09] Christian Haase, Benjamin Nill, and Sam Payne. Cayley decompositions of lattice polytopes and upper bounds for h^*-polynomials. *Journal für die reine und angewandte Mathematik*, 637:207–216, 2009.

[Har80] Joe Harris. The genus of space curves. *Mathematische Annalen*, 249(3):191–204, 1980.

[Mac27] F. S. Macaulay. Some properties of enumeration in the theory of modular systems. *Proceedings of the London Mathematical Society*, Second Series, 26:531–555, 1927.

[APPS22] Karim Alexander Adiprasito, Stavros Argyrios Papadakis, Vasiliki Petrotou, and Johanna Kristina Steinmeyer. Beyond positivity in Ehrhart theory. *arXiv preprint arXiv:2210.10734*, 2022.