Hilbert Functions and Toric Ideals

Lorenzo Robbiano

University of Genoa
Department of Mathematics

CoCoA, COCOA and Preliminaries

The COCOA Schools

School 1 (COCOA VI): TORINO (Italy) - Sturmfels, Geramita/Robbiano - 1999

School 2 (COCOA VII): Kingston (Canada) - Recio, Peterson - 2001

School 3 (COCOA VIII): Cadiz (Spain) - Kemper, Kreuzer - 2003

School 4: Porto Conte (Italy) - Migliore, Hosten - 2005

School 5: Hagenberg (Austria) - Conca, Robbiano - 2007

School 6: Barcelona (Spain) - Rossi, Geramita - 2009

School 7: Passau (Germany) - Robbiano, Seiler - 2011
Tutors: Anna Bigatti, Alessio Del Padrone
Eduardo Sáenz de Cabezón

Preliminaries

- K a computable field ($\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Z}_p$, . . .).

- Term orderings on $\mathbb{T}^n$ (first non zero element on each column of the associated matrix is positive).

- Gröbner Bases.

- Macaulay's Basis Theorem:
  $\mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$ is a basis of P/I as a K-vector space.

- $\mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$ is computable using Buchberger's Algorithm.

A Simple (Standard) Grading

- Grading on $P = K[x]$: $\deg(x^i) = i$.
- P_i = {homogeneous polynomials of $\deg i\} = \{cx^i \mid c \in K\}$.
- They are K -vector spaces of dimension 1 for all $i \geq 0$.
- We say that the Hilbert function of P, i.e. the function from $\mathbb{N}$ to $\mathbb{N}$ defined by

  $$i \to \dim_K(P_i)$$

  is constant and equal to 1.
- The associated power series is

  $$\sum_{i=0}^{\infty}(\dim_K(P_i))z^i = \sum_{i=0}^{\infty} z^i = \frac{1}{1-z}$$

Formule di Postulazione

- How many independent linear conditions are requested for a vector to belong to a given subvector space V' of V ?
- The answer is $\mathrm{codim}_V(V') = \dim_K(V) - \dim_K(V')$.
- If V is the space of forms of a given degree, a linear condition is given for instance by imposing the vanishing at a point p .
- Given a finite set $\mathbb{X}$ of points in $\mathbb{P}^n$, the number of independent conditions imposed to the forms of degree i by the vanishing at $\mathbb{X}$, is exactly the codimension of $I(\mathbb{X})_i$ in $P_i = K[x_0, x_1, \dots, x_n]_i$.
- Let $\mathbb{X} = \{p_1, p_2, p_3\}$ where $p_1 = (1, 0, 0)$, $p_2 = (0, 1, 0)$, $p_3 = (0, 0, 1)$, then $I(\mathbb{X})_1 = (0)$, hence $\dim(P/I(\mathbb{X}))_1 = 3$, since the points impose independent conditions on the lines in the projective plane.
- Let $\mathbb{X} = \{p_1, p_2, q_3\}$ where $q_3 = (1, 1, 0)$, then the linear system $a_1 = 0; a_2 = 0; a_1 + a_2 = 0$ is equivalent to $a_1 = 0; a_2 = 0$. They impose only 2 independent conditions and we see that $\dim(P/I(\mathbb{X}))_1 = 2$.

Graded Rings and Modules

Γ-Graded Rings and Modules

Definition

- Let $(\Gamma, +)$ be a monoid.
- The ring R is called a Γ-graded ring (or a Γ-graded ring, or a ring graded over Γ) if there exists a family of additive subgroups $\{R_\gamma\}_{\gamma\in\Gamma}$ such that
  - $R = \oplus_{\gamma\in\Gamma} R_\gamma$,
  - $R_\gamma \cdot R_{\gamma'} \subseteq R_{\gamma+\gamma'}$ for all $\gamma, \gamma' \in \Gamma$.
- The elements of R_γ are called homogeneous of degree γ . For $r \in R_\gamma$ we write $\deg(r) = \gamma$.
- If $r \in R$ and $r = \sum_{\gamma\in\Gamma} r_\gamma$ is the decomposition of r , where $r_\gamma \in R_\gamma$, then r_γ is called the homogeneous component of degree γ of r .
- If R is a Γ-graded ring and M is an R-module, then M is called a (Γ, R)-graded module if if there exists a family of additive subgroups $\{M_\gamma\}_{\gamma\in\Gamma}$ such that $M = \oplus_{\gamma\in\Gamma} M_\gamma$, and $R_\gamma \cdot M_{\gamma'} \subseteq M_{\gamma+\gamma'}$ for all $\gamma, \gamma' \in \Gamma$.

Graded Submodules and Homogeneous Ideals

Proposition

Let R be a Γ-graded ring and M a graded R-module. Let $N \subseteq M$ be an R-submodule, and let $N_\gamma = N \cap M_\gamma$ for all $\gamma \in \Gamma$. Then the following conditions are equivalent.

- $N = \oplus_{\gamma \in \Gamma} N_\gamma$
- *If $n \in N$ and $n = \sum_{\gamma \in \Gamma} n_\gamma$ is the decomposition of n into its homogeneous components, then $n_\gamma \in N$ for all $\gamma \in \Gamma$.*
- *There is a system of generators of N which consists of homogeneous elements.*

Graded ideals are usually called homogeneous ideals.

Question:
Given an ideal in P, how is it possible to detect if it is homogeneous or not?

Shifting Degrees (1.7.6)

Definition

Let R be a γ -graded ring, M, N graded R -moduled, and $\varphi : M \longrightarrow N$ an R -homomorphism. φ is called a homomorphism of graded modules or a homogeneous P -linear map if $\varphi(M_\gamma) \subseteq N_\gamma$ for all γ .

Definition

Let R be a Γ -graded ring M a graded R -module, and $\gamma \in \Gamma$.

- For every $\delta \in \Gamma$ we define $M(\gamma)_\delta = M_{\delta+\gamma}$. We say that the Γ -graded R -module $M(\gamma)$ is obtained by shifting the degrees.
- Modules of the form $\oplus_{i\in I} R(\gamma_i)$, where I is a set and $\gamma_i \in \Gamma$ for $i \in I$ are called Γ -graded free R -modules. Here we let $\left(\oplus_{i\in I} R(\gamma_i)\right)_\delta = \oplus_{i\in I} R(\gamma_i)_\delta$ for all $\delta \in \Gamma$.

REMARK. Let R be a Γ-graded ring M a graded R -module. Given homogeneous elements $v_1, \ldots, v_r \in M$ with $\deg(v_i) = \gamma_i$ we consider the graded free module $F = \oplus_{i=1}^r R(\gamma_i)$. The R -linear map $\varphi : F \longrightarrow M$ defined by $e_i \longrightarrow v_i$ is a homomorphism of graded Γ-modules. We say that φ is the map induced by $(v_1, \ldots, v_r)$.

Standard Gradings

Definition

A K-algebra R is called a standard graded K-algebra if it is $\mathbb{N}$-graded, satisfies $R_0 = K$ and $\dim_K(R_1) < \infty$, and if R is generated by the elements of R_1 as a K-algebra.

Example

$K[x, y]/(x^2 - y^3)$ is not standard graded, but for instance it is graded by

$$\deg(x) = 3, \ \deg(y) = 2$$

Example

Let $P = K[x_1, x_2]$ be equipped with the standard grading.
Then the K-subalgebra $S = K[x_1^2, x_1 x_2, x_2^2]$ of P is a finitely generated $\mathbb{N}$-graded algebra, but it is not standard graded, since $S_1 = \{0\}$.

Example

Projective schemes. Closures of affine schemes. Tangent Cones.

Gradings Defined by Matrices I

Definition

Let $m \geq 1$, and let the polynomial ring $P = K[x_1, \ldots, x_n]$ be equipped with a $\mathbb{Z}^m$-grading such that $K \subseteq P_0$ and $x_1, \ldots, x_n$ are homogeneous elements.

- For $j = 1, \ldots, n$, let $(w_{1j}, \ldots, w_{mj}) \in \mathbb{Z}^m$ be the degree of x_j. The matrix $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ is called the degree matrix of the grading. So, the columns of the degree matrix are the degrees of $x_1, \ldots, x_n$. The rows are called the weight vectors of $x_1, \ldots, x_n$.
- Conversely, given a matrix $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, we can consider the $\mathbb{Z}^m$-grading on P for which $K \subseteq P_0$ and the indeterminates are homogeneous elements whose degrees are given by the columns of W. In this case, we say that P is graded by W.
- Let $d \in \mathbb{Z}^m$. The set of homogeneous polynomials of degree d is denoted by $P_{W,d}$ (or simply by P_d). A polynomial $f \in P_{W,d}$ is also called homogeneous of degree d, and we write $\deg_W(f) = d$.

Gradings Defined by Matrices II

If a grading on P is defined by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, the degree of a term $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is given by $\deg_W(t) = W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}}$.
So, we have

$$\{d \in \mathbb{Z}^m \mid P_{W,d} \neq 0\} = \{W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} \mid (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}$$

Example

Let $P = K[x_1, x_2, x_3, x_4]$ be graded by the matrix

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

and let $f = x_1x_4 - x_2x_3$. Then f is homogeneous of degree $(2,1,1)^{\mathrm{tr}}$, because $W \cdot \log(x_1x_4)^{\mathrm{tr}} = W \cdot \log(x_2x_3)^{\mathrm{tr}} = (2,1,1)^{\mathrm{tr}}$.

Example

Let $P = K[x_1, \ldots, x_n]$. Then the standard grading on P is defined by the matrix $(1\ 1 \ldots 1)$.

Homogeneous Buchberger (4.5.1)

Proposition

Let M *be a graded submodule of* F *and* $\{g_1, \dots, g_s\}$ *a set of non-zero homogeneous vectors which generate* M *.*

- *Buchberger's Algorithm applied to the tuple* $G = (g_1, \dots, g_s)$ *returns a homogeneous* σ *-Gröbner basis of* M *.*
- *The reduced* σ *-Gröbner basis of* M *consists of homogeneous vectors.*

The non-Normal Quartic Curve

Example

We consider the projective curve given parametrically by $x_0 = s^4,\ x_1 = s^3t,\ x_2 = st^3,\ x_3 = t^4$. In $K[s,t,x_0,x_1,x_2,x_3]$ we take the ideal $J = (x_0 - s^4,\ x_1 - s^3t,\ x_2 - st^3,\ x_3 - t^4)$. By assigning arbitrary degrees to $s,\ t$ we get the corresponding degrees of $x_0,\ x_1,\ x_2,\ x_3$. Consequently, the ideal J is W-homogeneous where

$$W = \begin{pmatrix} 1 & 0 & 4 & 3 & 1 & 0 \\ 0 & 1 & 0 & 1 & 3 & 4 \end{pmatrix}$$

Let $P = k[x_0,x_1,x_2,x_3]$ and $I = J \cap P$, the elimination ideal. Then

$$I = (x_0x_3 - x_1x_2,\ x_0^2x_2 - x_1^3,\ x_1x_3^2 - x_2^3,\ x_0x_2^2 - x_1^2x_3)$$

turns out to be W'-homogeneous, where

$$W' = \begin{pmatrix} 4 & 3 & 1 & 0 \\ 0 & 1 & 3 & 4 \end{pmatrix}$$

Adding the two lines, we see that I is $(4,4,4,4)$ homogeneous, hence also $(1,1,1,1)$, homogeneous. Therefore we may also consider P/I as a standard graded algebra.

Monomial Ideals

A non-trivial class of graded objects is given by the following characterization of monomial ideals as the most homogeneous ideals. Recall that a square matrix is called non-singular if its determinant is different from zero.

Proposition

Let I be an ideal of P. Then the following conditions are equivalent.

- *The ideal I is monomial.*
- *There is a non-singular matrix $W \in \mathrm{Mat}_n(\mathbb{Z})$ such that I is homogeneous with respect to the grading on P given by W.*
- *For every $m \geq 1$ and every matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, the ideal I is homogeneous with respect to the grading on P given by W.*

Positivity of Matrices

Matrices of Positive Type

Definition

Let $m \geq 1$, let P be graded by a matrix W of rank m in $\mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $w_1, \ldots, w_m$ be the rows of W .

- The grading on P given by W is called of non-negative type if there exist $a_1, \ldots, a_m \in \mathbb{Z}$ such that the entries of $v = a_1 w_1 + \cdots + a_m w_m$ corresponding to the non-zero columns of W are positive. In this case, we shall also say that W is a matrix of non-negative type.

- We say that the grading on P given by W is of positive type if there exist $a_1, \ldots, a_m \in \mathbb{Z}$ such that all entries of $a_1 w_1 + \cdots + a_m w_m$ are positive. In this case, we shall also say that W is a matrix of positive type.

Nakayama's Lemma

Proposition

Let P be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, a matrix of positive type, and let $M \neq 0$ be a finitely generated graded P-module.

- *A set of homogeneous elements $m_1, \ldots, m_s$ generates the P-module M if and only if their residue classes $\overline{m}_1, \ldots, \overline{m}_s$ generate the K-vector space $M/(x_1, \ldots, x_n)M$.*
- *Every homogeneous system of generators of M contains a minimal one.*
- *All irredundant systems of homogeneous generators of M are minimal.*

This proposition is not true in general if W is of non-negative type.

Example

Let $P = K[x, y]$ be graded by the matrix $W = (0\ 1)$, and let $I = (xy,\ y - xy)$. Then W is of non-negative type, I is a homogeneous ideal, and $\{xy,\ y - xy\}$ is an irredundant homogeneous system of generators of I. However, since $I = (y)$, this system of generators is not minimal. Notice that we have $P_+ = (y)$ and $P_0 \cong P/P_+ \cong K[x]$.

A Fundamental Theorem (4.1.19)

Theorem

Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, and let M be a finitely generated graded P-module.

- *We have $P_0 = K$.*
- *For all $d \in \mathbb{Z}^m$, we have $\dim_K(M_d) < \infty$.*

Proof.

First we show a). Let $V = (a_1\ a_2\ \cdots\ a_m) \in \mathrm{Mat}_{1,m}(\mathbb{Z})$ be such that $V \cdot W$ has positive entries only. We see that $P_{W,0} \subseteq P_{V \cdot W,0}$. Now it suffices to note that every term $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \neq 1$ has positive degree $\deg_{V \cdot W}(t) = V \cdot W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} > 0$.
In order to prove b), we choose a finite homogeneous system of generators of M and consider the corresponding representation $M \cong F/N$ where N is a graded submodule of F. Clearly, it suffices to prove the claim for F. We do this by showing it is true for each $P(-\delta_i)$. Since $P(-\delta_i)_d = P_{d-\delta_i}$, it suffices to prove that $\dim_K(P_d) < \infty$ for all $d \in \mathbb{Z}^m$. Since W is of positive type, there exists a matrix $V \in \mathrm{Mat}_{1,m}(\mathbb{Z})$ such that $V \cdot W$ has all entries positive. We have $P_{W,d} \subseteq P_{V \cdot W, V \cdot d}$.
Hence we only have to show that the K-vector spaces $P_{V \cdot W,i}$ are finite dimensional for all $i \in \mathbb{Z}$. Their vector space bases $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid V \cdot W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} = i\}$ are finite, because $V \cdot W$ has positive entries only. □

A Nice Property

Proposition

Let P *be graded by a matrix* $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ *of rank* m *, and let* $\mathbb{T}^n$ *be the set of terms in* P *. The following conditions are equivalent.*

- *The first non-zero element in each non-zero column of* W *is positive.*
- *For* $i = 1, \ldots, n$ *, we have* $\deg_W(x_i) \geq_{\mathtt{Lex}} 0$ *.*
- *The restriction of* $\mathtt{Lex}$ *to the monoid* $\Gamma = \{d \in \mathbb{Z}^m \mid P_{W,d} \neq 0\}$ *is a well-ordering.*
- *The restriction of* $\mathtt{Lex}$ *to the monoid* $\Gamma = \{d \in \mathbb{Z}^m \mid P_{W,d} \neq 0\}$ *is a term ordering.*
- *There exists a term ordering* τ *on* $\mathbb{T}^n$ *which is compatible with* $\deg_W$ *.*

Positive Matrices

Definition

Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be a matrix of rank m.

- The grading on P defined by W is called non-negative if the first non-zero element in each non-zero column of W is positive. In this case, we shall also say that W is a non-negative matrix.
- The grading on P defined by W is called positive if no column of W is zero and the first non-zero element in each column is positive. In this case, we shall also say that W is a positive matrix.

REMARK. The above proposition implies that, if W defines a non-negative grading, there exists a term ordering on $\mathbb{T}^n$ which is compatible with $\deg_W$. If W is positive, then we have $\deg_W(x_i) >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, n$, and hence $P_+ = \bigoplus_{d >_{\mathtt{Lex}} 0} P_{W,d} = (x_1, \ldots, x_n)$, and $P_0 \cong P/P_+ \cong K$.

Proposition

If the grading defined by W is positive, then it is of positive type. In particular, the claims of the Fundamental Theorem are valid under the assumption that W is positive.

Definition of Hilbert Function

Definition

Let M be a finitely generated graded P-module. Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be a matrix of rank m of positive type (in particular, positive).
Then there is a well-defined map

$$\begin{array}{rcl} \mathrm{HF}_M : \mathbb{Z}^m & \longrightarrow & \mathbb{Z} \\ i & \longmapsto & \dim_K(M_i) \end{array}$$

This map is called the Hilbert function of M.

Integer Functions

Integer Functions

Definition

A map $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ is called an integer function. Given an integer function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, we define the following operators.

- The integer function $\Delta f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $\Delta f(i) = f(i) - f(i-1)$ for $i \in \mathbb{Z}$ is called the (first) difference function of f.
- Let $\Delta^0 f = f$. For $r \geq 1$, we inductively define an integer function $\Delta^r f : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $\Delta^r f = \Delta(\Delta^{r-1} f)$ and call it the $\mathbf{r^{th}}$ difference function of f.
- Given a number $q \in \mathbb{Z}$, we define an integer function $\Delta_q f : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $\Delta_q f(i) = f(i) - f(i-q)$ for $i \in \mathbb{Z}$ and call it the q-difference function of f.
- An integer function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ is called an integer Laurent function if there exists a number $i_0 \in \mathbb{Z}$ such that $f(i) = 0$ for all $i < i_0$.
- Given an integer Laurent function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, we define another integer Laurent function $\Sigma f : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $\Sigma f(i) = \sum_{j \leq i} f(j)$ and call it the summation function of f.

Integer Valued Polynomials

Proposition

Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ *be an integer Laurent function. Then we have* $\Sigma\Delta f = \Delta\Sigma f = f$ *.*

Definition

A polynomial $p \in \mathbb{Q}[t]$ is called an integer valued polynomial if we have $p(i) \in \mathbb{Z}$ for all $i \in \mathbb{Z}$. The set of all integer valued polynomials will be denoted by $\mathbb{IP}$. Furthermore, for every $r \geq 0$, we let $\mathbb{IP}_{\leq r}$ be the set of all integer valued polynomials of degree $\leq r$.

Example

The polynomial $\binom{t}{2}$ is an integer valued polynomial.

Basic Properties of Integer Valued Polynomials

Proposition

Let $a \in \mathbb{Z}$ *,* $r \in \mathbb{N}$ *, and let* $(a_0, a_1, a_2, \dots)$ *be a sequence of integers.*

- *For an integer valued polynomial* p *, we have* $\deg(p) = r$ *if and only if* $\Delta^r p(t) \in \mathbb{Z} \setminus \{0\}$ *. If this holds true, we have* $\Delta^r p(t) = r!\, \mathrm{LC}_{\mathtt{Deg}}(p) \in \mathbb{Z}$ *.*
- *Let* p *be an integer valued polynomial of degree* r *. Then the polynomial* $q = p - r!\, \mathrm{LC}_{\mathtt{Deg}}(p) \binom{t+a}{r}$ *is an integer valued polynomial of degree* $< r$ *.*
- *For every* $r \geq 0$ *, the set of polynomials* $\{\binom{t+a_i}{i} \mid 0 \leq i \leq r\}$ *is a* $\mathbb{Z}$ *-basis of* $\mathbb{IP}_{\leq r}$ *. Consequently, the set* $\{\binom{t+a_i}{i} \mid i \in \mathbb{N}\}$ *is a* $\mathbb{Z}$ *-basis of* $\mathbb{IP}$ *.*
- *For a map* $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ *, the following conditions are equivalent.*
  - *There exists an integer valued polynomial* $p \in \mathbb{IP}$ *with* $f(i) = p(i)$ *for all* $i \in \mathbb{Z}$ *.*
  - *There exist a number* $i_0 \in \mathbb{Z}$ *and an integer valued polynomial* $q \in \mathbb{IP}$ *such that* $f(i_0) \in \mathbb{Z}$ *and* $\Delta f(i) = q(i)$ *for all* $i \in \mathbb{Z}$ *.*

Integer Functions of Polynomial Type

Definition

Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be an integer function.

- The map $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ is called an integer function of polynomial type if there exists a number $i_0 \in \mathbb{Z}$ and an integer valued polynomial $p \in \mathbb{IP}$ such that $f(i) = p(i)$ for all $i \geq i_0$. This polynomial is uniquely determined and denoted by HP_f .

- For an integer function f of polynomial type, the number

$$\mathrm{ri}(f) = \min\{i \in \mathbb{Z} \mid f(j) = \mathrm{HP}_f(j) \text{ for all } j \geq i\}$$

is called the regularity index of f . Whenever $f(i) = \mathrm{HP}_f(i)$ for all $i \in \mathbb{Z}$, we let $\mathrm{ri}(f) = -\infty$.

Integer Functions of Polynomial Type II

We introduce a fundamental family of integer functions of polynomial type.

Example

For every $i \in \mathbb{N}$, we define a map $\mathrm{bin}_i : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $\mathrm{bin}_i(j) = \binom{j}{i}$ for $j \geq i$ and by $\mathrm{bin}_i(j) = 0$ for $j < i$. The map bin_i is an integer Laurent function of polynomial type. It satisfies $\mathrm{HP}_{\mathrm{bin}_i}(t) = \binom{t}{i}$ and $\mathrm{ri}(\mathrm{bin}_i) = 0$. Moreover, if $i > 0$, then $\Delta\, \mathrm{bin}_i(j) = \mathrm{bin}_{i-1}(j-1)$ for all $j \in \mathbb{Z}$.
There is no integer valued polynomial $p \in \mathbb{IP}$ such that $\mathrm{bin}_i(j) = p(j)$ for all j .

Corollary

Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be an integer Laurent function of polynomial type.

- *We have $\mathrm{HP}_{\Delta f}(t) = \Delta\, \mathrm{HP}_f(t)$. In particular, if $\deg(\mathrm{HP}_f) > 0$, then we have $\deg(\mathrm{HP}_{\Delta f}) = \deg(\mathrm{HP}_f) - 1$.*
- *For every $q \geq 1$, we have $\mathrm{ri}(\Delta_q f) = \mathrm{ri}(f) + q$.*
- *If we write $\mathrm{HP}_f(t) = c_1\binom{t-1}{0} + \cdots + c_m\binom{t-1}{m-1}$ and choose $i_0 \geq \mathrm{ri}(f)$, then we have $\mathrm{HP}_{\Sigma f}(t) = c_1\binom{t}{1} + \cdots + c_m\binom{t}{m} + f(i_0)$.*
- *We have $\mathrm{ri}(\Sigma f) = \mathrm{ri}(f) - 1$.*

Hilbert Functions

Hilbert Functions in the Standard Case

Definition

Let M be a finitely generated graded P-module.
Then there is a well-defined map

$$\begin{aligned} \mathrm{HF}_M : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ i &\longmapsto \dim_K(M_i) \end{aligned}$$

This map is called the Hilbert function of M (with respect to the standard grading).

An isomorphism of vector spaces $\varphi : P_1 \longrightarrow P_1$ extends uniquely to an isomorphism $\Phi : P \longrightarrow P$ of graded K-algebras. Such a map Φ is called a homogeneous linear change of coordinates. We express this fact by saying that the Hilbert function of M is invariant under a homogeneous linear change of coordinates.

Proposition

For every $i \in \mathbb{N}$, we have $\mathrm{HF}_P(i) = \binom{i+n-1}{n-1}$ *.*

Hilbert Functions and Exact Sequences

Proposition

Let M *,* M' *, and* M'' *be three finitely generated graded* P *-modules.*

- *Let* $j \in \mathbb{Z}$ *. Then the Hilbert function of the module* $M(j)$ *obtained by shifting degrees by* j *is given by* $\mathrm{HF}_{M(j)}(i) = \mathrm{HF}_M(i+j)$ *for all* $i \in \mathbb{Z}$ *.*
- *Given a homogeneous exact sequence of graded* P *-modules*
  $$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$
  we have $\mathrm{HF}_M(i) = \mathrm{HF}_{M'}(i) + \mathrm{HF}_{M''}(i)$ *for all* $i \in \mathbb{Z}$ *.*

Proposition

Let I *be a homogeneous ideal in* P *, and let* $f \in P$ *be a non-zero homogeneous polynomial of degree* d *. Then we have a homogeneous exact sequence*

$$0 \longrightarrow [P/(I :_P (f))]\,(-d) \xrightarrow{\cdot f} P/I \longrightarrow P/(I+(f)) \longrightarrow 0$$

and therefore $\mathrm{HF}_{P/(I+(f))}(i) = \mathrm{HF}_{P/I}(i) - \mathrm{HF}_{P/(I:_P(f))}(i-d)$ *for all* $i \in \mathbb{Z}$ *.*
In particular, f *is a non-zerodivisor for* P/I *if and only if we have* $\mathrm{HF}_{P/(I+(f))}(i) = \Delta_d\, \mathrm{HF}_{P/I}(i)$ *for all* $i \in \mathbb{Z}$ *.*

Hilbert Functions and Leading Terms

Theorem

Let I be a homogeneous ideal of P and let σ be a term ordering on $\mathbb{T}^n$. Then we have $\mathrm{HF}_I(i) = \mathrm{HF}_{\mathrm{LT}_\sigma(I)}(i)$ for all $i \in \mathbb{Z}$.

Corollary

Let M be a finitely generated graded P-module, and let $K \subseteq L$ be a field extension. Then we have $\mathrm{HF}_M(i) = \mathrm{HF}_{M \otimes_K L}(i)$ for all $i \in \mathbb{Z}$.

Theorem

Let M be a finitely generated graded P-module. Then its Hilbert function $\mathrm{HF}_M : \mathbb{Z} \longrightarrow \mathbb{Z}$ is an integer function of polynomial type.

Power Series

Rational Power Series

Definition

Let R be an integral domain and K its field of fractions.

- We denote the ring of power series over R by $R[[z]]$.
- The subring $R[[z]] \cap K(z)$ of the field $K[[z]]_z$ is called the ring of rational power series over R .
- The localization $R[[z]]_z$ of the power series ring $R[[z]]$ in the element z is called the ring of Laurent series in one indeterminate z over R .
- Finally, the ring $R[z]_z$ is called the ring of Laurent polynomials over R . It is sometimes also denoted by $R[z, z^{-1}]$.

Characterization of Rational Power Series (5.2.6)

Theorem

Let $c_i \in \mathbb{Z}$ *for* $i \geq 0$ *, and let* $f = \sum_{i \geq 0} c_i z^i \in \mathbb{Z}[[z]]$ *. Then the following conditions are equivalent.*

- *The power series* f *is rational.*
- *There exist a polynomial* $g \in \mathbb{Z}[z]$ *and integers* $a_1, \ldots, a_m \in \mathbb{Z}$ *such that* $f = g/(1 - a_1 z - a_2 z^2 - \cdots - a_m z^m)$ *.*
- *There are natural numbers* $m, n \in \mathbb{N}$ *and integers* $a_1, \ldots, a_m \in \mathbb{Z}$ *such that* $c_i = a_1 c_{i-1} + a_2 c_{i-2} + \cdots + a_m c_{i-m}$ *for all* $i > n$ *.*

Example

Let $c_0, c_1, \ldots$ be the Fibonacci sequence, i.e. let $c_0 = c_1 = 1$ and $c_i = c_{i-1} + c_{i-2}$ for $i \geq 2$. Therefore the Fibonacci numbers are the coefficients of the power series $1/(1 - z - z^2) = c_0 + c_1 z + c_2 z^2 + \cdots$. The associated integer Laurent function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(i) = c_i$ for $i \in \mathbb{Z}$ is not an integer function of polynomial type, because if a polynomial $p \in \mathbb{IP}$ satisfies $p(i) = c_i$ for large enough i , then $p(i) = p(i-1) + p(i-2)$ implies $\Delta p(i) = p(i-2)$.

Properties of Power Series

Definition

Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be a non-zero integer Laurent function. The number $\min\{i \in \mathbb{Z} \mid f(i) \neq 0\}$ will be denoted by α_f or simply α.
Moreover, the associated Laurent series $\sum_{i \geq \alpha} f(i)\, z^i$ will be denoted by $\mathrm{HS}_f(z)$.

Proposition

Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be a non-zero integer Laurent function.

- *For every $q \geq 1$, we have $\mathrm{HS}_{\Delta_q f}(z) = (1 - z^q) \cdot \mathrm{HS}_f(z)$.*
  In particular, we have $\mathrm{HS}_{\Delta f}(z) = (1 - z) \cdot \mathrm{HS}_f(z)$.
- *We have $\mathrm{HS}_{\Sigma f}(z) = \mathrm{HS}_f(z)/(1 - z)$.*

Lemma

For all $n \geq 1$, we have $(1 - z)^{-n} = \sum_{i \geq 0} \binom{i+n-1}{n-1} z^i$.

Laurent Series and Integer Functions (5.2.10)

Theorem

For a non-zero integer Laurent function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ *, TFAE*

- *The integer function* f *is of polynomial type.*
- *The associated Laurent series of* f *is of the form* $\mathrm{HS}_f(z) = \frac{p(z)}{(1-z)^m}$ *where* $m \in \mathbb{N}$ *and* $p(z) \in \mathbb{Z}[z, z^{-1}]$ *is a Laurent polynomial over* $\mathbb{Z}$ *.*

If these conditions are satisfied, we have $m = \deg(\mathrm{HP}_f(t)) + 1$ *.*

Corollary

Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ *be a non-zero integer Laurent function of polynomial type, and let* $\alpha = \min\{i \in \mathbb{Z} \mid f(i) \neq 0\}$ *.*

- *The associated Laurent series of* f *has the form* $\mathrm{HS}_f(z) = p(z)/(1-z)^m$ *, where* $m \in \mathbb{N}$ *and* $p(z) \in \mathbb{Z}[z, z^{-1}]$ *is a Laurent polynomial of the form* $p(z) = \sum_{i=\alpha}^{\beta} c_i z^i$ *with* $\beta \geq \alpha$ *,* $c_\alpha, \ldots, c_\beta \in \mathbb{Z}$ *,* $c_\alpha \neq 0$ *, and* $c_\beta \neq 0$ *.*
- *If* $m > 0$ *, then we have* $\mathrm{HP}_f(t) = \sum_{i=\alpha}^{\beta} c_i \binom{t-i+m-1}{m-1}$ *, and if* $m = 0$ *, then we have* $\mathrm{HP}_f(t) = 0$ *.*
- *We have* $\mathrm{ri}(f) = \beta - m + 1$ *.*

The Standard Case

Proposition

The Hilbert series of P *is given by* $\mathrm{HS}_P(z) = \frac{1}{(1-z)^n}$.

Proposition

(Basic Properties of Hilbert Series)

Let M, M', M'' *be three finitely generated graded* P *-modules.*

- *For all* $j \in \mathbb{Z}$ *, we have* $\mathrm{HS}_{M(j)}(z) = z^{-j}\,\mathrm{HS}_M(z)$.
- *Given a homogeneous exact sequence* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *, we have* $\mathrm{HS}_M(z) = \mathrm{HS}_{M'}(z) + \mathrm{HS}_{M''}(z)$.
- *Let* $M = M_1 \oplus \cdots \oplus M_r$ *with finitely generated graded* P *-modules* $M_1, \ldots, M_r$ *. Then we have* $\mathrm{HS}_M(z) = \mathrm{HS}_{M_1}(z) + \cdots + \mathrm{HS}_{M_r}(z)$.
- *Let* $\delta_1, \ldots, \delta_r \in \mathbb{Z}$ *. Then the Hilbert series of the graded free module* $F = \bigoplus_{j=1}^r P(-\delta_i)$ *is* $\mathrm{HS}_F(z) = (\sum_{j=1}^r z^{\delta_j})/(1-z)^n$.

Macaulay's Theorem for Hilbert Series

Theorem

Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$ *, let* M *be a graded submodule of the graded free* P *-module* $\bigoplus_{i=1}^{r} P(-\delta_i)$ *, and let* σ *be a module term ordering on* $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ *. Then we have* $\mathrm{HS}_M(z) = \mathrm{HS}_{\mathrm{LT}_\sigma(M)}(z)$ *.*

Corollary

Let M *be a graded* P *-module, and let* $K \subseteq L$ *be a field extension. Then we have* $\mathrm{HS}_{M \otimes_K L}(z) = \mathrm{HS}_M(z)$ *.*

Theorem

Let M *be a non-zero finitely generated graded* P *-module, and let* $\alpha(M) = \min\{i \in \mathbb{Z} \mid M_i \neq 0\}$ *. Then the Hilbert series of* M *has the form*

$$\mathrm{HS}_M(z) = \frac{z^{\alpha(M)}\,\mathrm{HN}_M(z)}{(1-z)^n}$$

where $\mathrm{HN}_M(z) \in \mathbb{Z}[z]$ *and* $\mathrm{HN}_M(0) = \mathrm{HF}_M(\alpha(M)) > 0$ *. Note that* n *is the number of indeterminates of* P *.*

Dimension and Multiplicity

Definition

In the Hilbert series $\mathrm{HS}_M(z) = \frac{z^\alpha \, \mathrm{HN}_M(z)}{(1-z)^n}$, we simplify the fraction by cancelling $1 - z$ as often as possible. We obtain a representation $\mathrm{HS}_M(z) = \frac{z^\alpha \, \mathrm{hn}_M(z)}{(1-z)^d}$, where $0 \le d \le n$ and where $\mathrm{hn}_M(z) \in \mathbb{Z}[z]$ satisfies $\mathrm{hn}_M(0) = \mathrm{HF}_M(\alpha) > 0$.

- The polynomial $\mathrm{hn}_M(z) \in \mathbb{Z}[z]$ is called the simplified Hilbert numerator of M .
- Let $\delta = \deg(\mathrm{hn}_M(z))$, and let $\mathrm{hn}_M(z) = h_0 + h_1 z + \cdots + h_\delta z^\delta$. Then the tuple $\mathrm{hv}(M) = (h_0, h_1, \ldots, h_\delta) \in \mathbb{Z}^{\delta+1}$ is called the h-vector of M .
- The number $\dim(M) = d$ is called the dimension of M .
- The number $\mathrm{mult}(M) = \mathrm{hn}_M(1)$ is called the multiplicity of M .

The Hilbert Polynomial

Definition

Let t be an indeterminate over $\mathbb{Q}$.

- The integer valued polynomial associated to HF_M is called the Hilbert polynomial of M and is denoted by $\mathrm{HP}_M(t)$. Therefore we have $\mathrm{HP}_M(t) \in \mathbb{IP} \subset \mathbb{Q}[t]$ and $\mathrm{HF}_M(i) = \mathrm{HP}_M(i)$ for $i \gg 0$.
- The regularity index of HF_M is called the regularity index of M and is denoted by $\mathrm{ri}(M)$.

Proposition

For a non-zero finitely generated graded P-module M, we have $\mathrm{mult}(M) > 0$.

Multivariate Power Series

σ -Laurent Series

Definition

The set $R^{\mathbb{Z}^m}$ is an R -module with respect to componentwise addition and scalar multiplication. We denote an element $(a_i)_{i\in\mathbb{Z}^m}$ by $\sum_{i\in\mathbb{Z}^m} a_i\,\mathbf{z}^i$ and the module by $R[[\mathbf{z},\mathbf{z}^{-1}]]$. We call it the module of extended power series.

The module of extended power series is not a ring with respect to the usual multiplication. For instance, the constant coefficient of the product $(1+z_1+z_1^2+\cdots)\cdot(1+z_1^{-1}+z_1^{-2}+\cdots)$ would be an infinite sum. But it is important to be able to multiply Hilbert series.

Definition

Let σ be a monoid ordering on $\mathbb{Z}^m$.

- An extended power series $f=\sum_{i\in\mathbb{Z}^m} a_i\,\mathbf{z}^i$ is called a σ -Laurent series if its “support" is well-ordered by σ .
- The set of all σ -Laurent series is called the σ -Laurent series ring over R and will be denoted by $R[[\mathbf{z},\mathbf{z}^{-1}]]_\sigma$.

σ -Laurent Series and Positive Matrices

Proposition

Let σ be a monoid ordering on $\mathbb{Z}^m$. Then the set $R[[\mathbf{z}, \mathbf{z}^{-1}]]_\sigma$ of all σ -Laurent series is a ring with respect to componentwise addition and with respect to the multiplication given by the formula

$$\Big(\sum_{i \in \mathbb{Z}^m} a_i\, \mathbf{z}^i\Big) \cdot \Big(\sum_{j \in \mathbb{Z}^m} b_j\, \mathbf{z}^j\Big) = \sum_{k \in \mathbb{Z}^m} \Big(\sum_{i+j=k} a_i b_j\Big)\, \mathbf{z}^k$$

Corollary

Assume that $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ is positive, let M be a finitely generated graded P -module, and let Σ be the set $\{d \in \mathbb{Z}^m \mid M_{W,d} \neq 0\}$.

(a) *The relation $\mathtt{Lex}|_\Sigma$ is a well-ordering.*

(b) *The series $\mathrm{HS}_M(\mathbf{z})$ is an element of the ring $\mathbb{Z}[[\mathbf{z}, \mathbf{z}^{-1}]]_{\mathtt{Lex}}$.*

Multigraded Hilbert Functions

Definition

Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be positive and let M be a finitely generated W-graded P-module. Then the map $\mathrm{HF}_M : \mathbb{Z}^m \longrightarrow \mathbb{Z}$ given by the rule $(i_1, \ldots, i_m) \mapsto \dim_K(M_{(i_1,\ldots,i_m)})$ for all $(i_1, \ldots, i_m) \in \mathbb{Z}^m$ is called the multigraded Hilbert function of M.

Proposition

Let $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ *and* $(i_1, \ldots, i_m) \in \mathbb{Z}^m$. *Then the value* $\mathrm{HF}_P(i_1, \ldots, i_m)$ *of the multigraded Hilbert function of* P *is the number of solutions* $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ *of the system of Diophantine equations*

$$\left\{\begin{array}{rcl} w_{11}y_1 + \cdots + w_{1n}y_n & = & i_1 \\ w_{21}y_1 + \cdots + w_{2n}y_n & = & i_2 \\ \vdots & \vdots & \vdots \\ w_{m1}y_1 + \cdots + w_{mn}y_n & = & i_m \end{array}\right.$$

in the indeterminates $y_1, \ldots, y_n$.

Hilbert Functions of Polynomial Rings

Example

Let $P = K[x_1, x_2]$ be graded by $W = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$. We get the equations $y_2 = i_1$, $y_1 - y_2 = i_2$ to be solved for $y_1 \geq 0$ and $y_2 \geq 0$. We find solutions only if $i_1 \geq 0$ and $i_1 + i_2 \geq 0$. Then we have $P_{(i_1,i_2)} \neq 0$ if and only if $i_1 \geq 0$ and $i_2 \geq -i_1$. In these degrees we have $\dim_K(P_{(i_1,i_2)}) = 1$. Therefore we obtain

$$\mathrm{HS}_P(z_1, z_2) = \sum_{i_1 \geq 0} \sum_{i_2 \geq -i_1} z_1^{i_1} z_2^{i_2} = \Big(\sum_{i_1 \geq 0} z_1^{i_1} z_2^{-i_1} \Big) / (1 - z_2) = \frac{1}{(1 - z_1 z_2^{-1})(1 - z_2)}$$

Theorem

Let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type. Then we have

$$\mathrm{HS}_{P,W}(z_1, \ldots, z_m) = \frac{1}{\prod_{j=1}^{n} (1 - z_1^{w_{1j}} \cdots z_m^{w_{mj}})}$$

An Example

Example

Let $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ be graded by $W = \binom{1\,2\,3\,4}{0\,0\,5\,8}$, and let $I = (x_1^2, x_2, x_3^3)$.
We want to compute the multivariate Hilbert series of P/I.
In the first step, we form $J = (x_1^2, x_2)$.
In the second step, we compute the Hilbert numerators of P/J and of $P/(J :_P (x_3^3))$ recursively.
We have $J :_P (x_3^3) = (x_1^2, x_2) = J$. When we compute $\mathrm{HN}_{P/J}(z_1, z_2)$, we form $J' = (x_1^2)$ and $J'' = J :_P (x_2) = (x_1^2)$ and apply the algorithm recursively to them. Since $J' = J'' = (x_1^2)$ is a principal ideal, the algorithm yields $\mathrm{HN}_{P/J'}(z_1, z_2) = \mathrm{HN}_{P/J''}(z_1, z_2) = 1 - z_1^2$.
Then we find $\mathrm{HN}_{P/J}(z_1, z_2) = \mathrm{HN}_{P/J'}(z_1, z_2) - z_1^2\,\mathrm{HN}_{P/J''}(z_1, z_2) = (1 - z_1^2)^2$ in step 3). Thus the original algorithm computes $\mathrm{HN}_{P/I}(z_1, z_2) = \mathrm{HN}_{P/J}(z_1, z_2) - z_1^9 z_2^{15}\,\mathrm{HN}_{P/(J:_P(x_3^3))}(z_1, z_2) = (1 - z_1^2)^2(1 - z_1^9 z_2^{15})$.
Altogether, we have

$$\mathrm{HS}_{P/I}(z_1, z_2) = \frac{(1-z_1^2)^2(1-z_1^9 z_2^{15})}{(1-z_1)(1-z_1^2)(1-z_1^3 z_2^5)(1-z_1^4 z_2^8)} = \frac{(1+z_1)(1+z_1^3 z_2^5+z_1^6 z_2^{10})}{1-z_1^4 z_2^8}$$

Another Example

Example

Let $P = \mathbb{Q}[x_1, x_2, x_3]$ be graded by $W = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$, and let $I = (x_1^3 x_2,\ x_2 x_3^2,\ x_2^2 x_3,\ x_3^4)$. We want to compute the multivariate Hilbert series of P/I.

We form the ideals $J_1 = (x_1^3 x_2,\ x_2 x_3^2,\ x_2^2 x_3)$ and $J_2 = J_1 :_P (x_3^4) = (x_2)$ and apply the algorithm recursively to them. For J_2, it yields $\mathrm{HN}_{P/J_2}(z_1, z_2) = 1 - z_1$ in step 1). For J_1, we form $J_{11} = (x_1^3 x_2,\ x_2 x_3^2)$ and $J_{12} = J_1 :_P (x_2^2 x_3) = (x_1^3, x_3)$ and apply the algorithm recursively to these...

... bla bla bla...

... Therefore the multivariate Hilbert series of P/I is

$$\mathrm{HS}_{P/I}(z_1, z_2) = \frac{-z_1^5 z_2^{-1} + z_1^3 z_2^{-3} + z_1^2 z_2^{-2} + z_1^3 + z_1^2 z_2^{-1} + z_1^2 + z_1 z_2^{-1} + z_1 + 1}{1 - z_1}$$

Change of Grading (Subsection 5.8.C)

Proposition

Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ *and* $A = (a_{ij}) \in \mathrm{Mat}_{\ell,m}(\mathbb{Z})$ *be two matrices such that the gradings on* $P = K[x_1, \dots, x_n]$ *given by* W *and by* $A \cdot W$ *are both of positive type. Let* M *be a finitely generated* P*-module which is graded with respect to the grading given by* W*. Then the Hilbert series of* M *with respect to the grading given by* $A \cdot W$ *is*

$$\mathrm{HS}_{M,A\cdot W}(z_1, \dots, z_\ell) = \mathrm{HS}_{M,W}(z_1^{a_{11}} \cdots z_\ell^{a_{\ell 1}}, \dots, z_1^{a_{1m}} \cdots z_\ell^{a_{\ell m}})$$

Example

Let $P = K[x_1, x_2, x_3]$ be graded by $W = \begin{pmatrix} -1 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$, and let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then $\mathrm{HS}_{P,W}(z_1, z_2) = 1/((1 - z_1^{-1} z_2^2)(1 - z_1)(1 - z_1^2 z_2))$ and $A \cdot W = \begin{pmatrix} 1 & 1 & 3 \\ 2 & 0 & 1 \end{pmatrix}$. The Hilbert series of P with respect to the grading given by $A \cdot W$ is

$$\mathrm{HS}_{P,A\cdot W}(z_1, z_2) = 1/((1 - z_1 z_2^2)(1 - z_1)(1 - z_1^3 z_2)) = \mathrm{HS}_{P,W}(z_1, z_1 z_2)$$

in accordance with the proposition.

Change of Grading II

Corollary

Let $U \in \mathrm{Mat}_{\ell,n}(\mathbb{Z})$ *be a matrix of positive type, let* $V \in \mathrm{Mat}_{m-\ell,n}(\mathbb{Z})$ *, and let* $W = \binom{U}{V} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ *.*

- *We have* $\mathrm{HS}_{M,U}(z_1,\dots,z_\ell) = \mathrm{HS}_{M,W}(z_1,\dots,z_\ell,1,\dots,1)$ *.*
- *We have* $P_{U,0} = K$ *and for every* $d \in \mathbb{Z}^\ell$ *, we have the following equality* $\dim_K(M_{U,d}) = \sum_{e\in\mathbb{Z}^{m-\ell}} \dim_K(M_{(d,e)})$ *.*

Toric Ideals

Toric Ideals Associated to Matrices

Let K be a field and $P = K[x_1, \dots, x_n]$ a polynomial ring over K. Given further indeterminates $y_1, \dots, y_m$, we let $L = K[y_1, \dots, y_m, y_1^{-1}, \dots, y_m^{-1}]$ be the Laurent polynomial ring in the indeterminates $y_1, \dots, y_m$ over K.

Definition

An element of the form $y_1^{i_1} y_2^{i_2} \cdots y_m^{i_m} \in L$ with $i_1, \dots, i_m \in \mathbb{Z}$ is called an extended term. The group of all extended terms is denoted by $\mathbb{E}^m$.

Definition

Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $t_i = y_1^{a_{1i}} y_2^{a_{2i}} \cdots y_m^{a_{mi}}$ for $i = 1, \dots, n$. We define a K-algebra homomorphism $\varphi : P \longrightarrow L$ by $\varphi(x_i) = t_i$ for $i = 1, \dots, n$.

Then the ideal $I(\mathcal{A}) = \mathrm{Ker}(\varphi)$ in P is called the toric ideal associated to the matrix $\mathcal{A}$, or to the tuple of extended terms $(t_1, \dots, t_n)$.

Binomial Ideals

Proposition

Every toric ideal is a prime ideal.

Recall that a binomial in P is a polynomial of the form $at + a't'$ with coefficients $a, a' \in K \setminus \{0\}$ and distinct terms $t, t' \in \mathbb{T}^n$.
A binomial ideal is an ideal generated by binomials.

Definition

Let $S \subseteq P$ be a set of polynomials.

- A binomial in P is called unitary if it is of the form $t - t'$ with $t, t' \in \mathbb{T}^n$. The set of all unitary binomials in S will be denoted by $\mathrm{UB}(S)$.
- A binomial in P is called pure if it is of the form $t - t'$ with coprime terms $t, t' \in \mathbb{T}^n$. The set of all pure binomials in S will be denoted by $\mathrm{PB}(S)$.

Computing Toric Ideals

For an extended term $t \in \mathbb{E}^m$, there exists a unique minimal number $\tau(t) \in \mathbb{N}$ such that $(y_1 \cdots y_m)^{\tau(t)} \cdot t \in K[y_1, \ldots, y_m]$.

Proposition

Let $t_1, \ldots, t_n \in \mathbb{E}^m$, let $I \subseteq P$ be the toric ideal associated to $(t_1, \ldots, t_n)$, and let $J \subseteq K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ be the binomial ideal generated by $\{\pi^{\tau(t_1)}(x_1 - t_1), \ldots, \pi^{\tau(t_n)}(x_n - t_n)\}$ where $\pi = y_1 \cdots y_m$.

- *We have $I = (J : \pi^\infty) \cap K[x_1, \ldots, x_n]$.*
- *Let z be a new indeterminate, and let G be a Gröbner basis of the ideal $J + (\pi z - 1)$ with respect to an elimination ordering for $\{y_1, \ldots, y_m, z\}$. Then the toric ideal I is generated by $G \cap K[x_1, \ldots, x_n]$.*
- *The toric ideal I is generated by pure binomials.*

Efficiently Computing Toric Ideals

Theorem

Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ *, let* $\mathcal{L}(\mathcal{A})$ *be the kernel of the* $\mathbb{Z}$ *-linear map* $\mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ *defined by* $\mathcal{A}$ *, and let* $V = \{v_1, \ldots, v_r\} \subseteq \mathcal{L}(\mathcal{A})$ *generate the* $\mathbb{Z}$ *-module* $\mathcal{L}(\mathcal{A})$ *. Furthermore, let* $\pi = x_1 x_2 \cdots x_n$ *.*
Then we have

$$I(\mathcal{A}) = I_V :_P \pi^\infty$$

Corollary

Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ *. Consider the following sequence of instructions.*

(1) *Compute a system of generators* $V = \{v_1, \ldots, v_r\}$ *of* $\mathcal{L}(\mathcal{A})$ *.*

(2) *For* $i = 1, \ldots, r$ *, write* $v_i = v_i^+ - v_i^-$ *and let* $\varrho(v_i) = \mathbf{x}^{v_i^+} - \mathbf{x}^{v_i^-} \in P$ *. Form the lattice ideal* $I_V = (\varrho(v_1), \ldots, \varrho(v_r))$ *and compute the saturation* $I = I_V :_P (x_1 \cdots x_n)^\infty$ *.*

(3) *Return the ideal* I *and stop.*

This is an algorithm which computes the toric ideal $I(\mathcal{A})$ *associated to* $\mathcal{A}$ *.*

A common method ito perform Step (1) s via the computation of the Hermite normal form of $\mathcal{A}$.

Hilbert Bases

The Hilbert Basis

We let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. We consider the homogeneous system of linear Diophantine equations $\mathcal{A}\,\mathbf{z} = 0$ and we recall that $\mathcal{L}(\mathcal{A})$ is the subgroup of $\mathbb{Z}^n$ consisting of its solutions.

Then we let $\mathcal{L}_+(\mathcal{A}) = \mathcal{L}(\mathcal{A}) \cap \mathbb{N}^n$ be the set of its componentwise non-negative solutions. Clearly, the set $\mathcal{L}_+(\mathcal{A})$ is a submonoid of $\mathbb{N}^n$.

Next we consider the following partial ordering $\succ$ on $\mathcal{L}_+(\mathcal{A})$. Given two vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n) \in \mathcal{L}_+(\mathcal{A})$, we let $u \succ v$ if $u_i \geq v_i$ for $i = 1, \ldots, n$ and if this inequality is strict for some $i \in \{1, \ldots, n\}$.

The ordering `Lex` is a term ordering on $\mathbb{N}^n$, hence its restriction to $\mathcal{L}_+(\mathcal{A})$ is a well-ordering. Obviously, $u \succ v$ implies $u >_{\mathtt{Lex}} v$. Therefore there exist minimal elements in $\mathcal{L}_+(\mathcal{A}) \setminus \{0\}$ with respect to $\succ$.

Definition

The set of all minimal elements of $\mathcal{L}_+(\mathcal{A}) \setminus \{0\}$ with respect to the partial ordering $\succ$ is called the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$.

The Hilbert Basis Generates $\mathcal{L}_+(\mathcal{A})$

Proposition

Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let H be the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$. Then every element of $\mathcal{L}_+(\mathcal{A})$ can be written as a linear combination of elements of H with coefficients in $\mathbb{N}$.

Proof.

Let $S \subseteq \mathcal{L}_+(\mathcal{A})$ be the set of all vectors which can be written as a linear combination of elements of H with coefficients in $\mathbb{N}$. For a contradiction, assume that $\mathcal{L}_+(\mathcal{A}) \setminus S \neq \emptyset$. We have already noted that $\mathtt{Lex}$ is a well-ordering on $\mathcal{L}_+(\mathcal{A})$. Hence there exists a minimal element $u \in \mathcal{L}_+(\mathcal{A}) \setminus S \neq \emptyset$ with respect to $\mathtt{Lex}$. Clearly, we have $u \notin H$. Thus there exists a vector $v \in H$ such that $u \succ v$. Now we use that fact that $u - v \in \mathcal{L}_+(\mathcal{A})$ to conclude that $u \succ u - v$. This shows $u >_{\mathtt{Lex}} u - v$, and therefore $u - v \in S$. But this implies $u \in S$, a contradiction. $\square$

Lawrence Liftings

Definition

Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Then the matrix $\overline{\mathcal{A}} = \begin{pmatrix} \mathcal{A} & 0 \\ \mathcal{I}_n & \mathcal{I}_n \end{pmatrix}$ where $\mathcal{I}_n$ is the identity matrix of size n , is called the Lawrence lifting of $\mathcal{A}$.

The first connection between $\mathcal{A}$ and $\overline{\mathcal{A}}$ is that the map $\lambda : \mathcal{L}(\mathcal{A}) \longrightarrow \mathcal{L}(\overline{\mathcal{A}})$ defined by $\lambda(u) = (u, -u)$ is clearly bijective. But much more is true.

Proposition

Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(K)$ *, let* $\overline{\mathcal{A}}$ *be the Lawrence lifting of* $\mathcal{A}$ *, and let* $Q = K[x_1, \ldots, x_n, w_1, \ldots, w_n]$ *.*

- *The toric ideal* $I(\overline{\mathcal{A}}) \subseteq Q$ *has a system of generators consisting of binomials of the form* $x_1^{\alpha_1} \cdots x_n^{\alpha_n} w_1^{\beta_1} \cdots w_n^{\beta_n} - x_1^{\beta_1} \cdots x_n^{\beta_n} w_1^{\alpha_1} \cdots w_n^{\alpha_n}$ *where* $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{N}$ *.*
- *There is a bijection between* $\mathrm{PB}(I(\mathcal{A}))$ *and* $\mathrm{PB}(I(\overline{\mathcal{A}}))$ *which maps a binomial* $\mathbf{x}^\alpha - \mathbf{x}^\beta$ *to* $\mathbf{x}^\alpha \mathbf{w}^\beta - \mathbf{x}^\beta \mathbf{w}^\alpha$*.*
- *There is a bijection between* $\mathcal{L}_+(\mathcal{A})$ *and the elements in* $\mathrm{PB}(I(\overline{\mathcal{A}}))$ *of the form* $\mathbf{x}^\alpha - \mathbf{w}^\alpha$ *with* $\alpha \in \mathbb{N}^n$*.*

Primitive Separated Binomials

The last part of this proposition yields a bijection between the minimal elements of $\mathcal{L}_+(\mathcal{A}) \setminus \{0\}$ with respect to $\succ$ and the elements $\mathbf{x}^u - \mathbf{w}^u$ in $\mathrm{PB}(I(\overline{\mathcal{A}}))$ with the property that there is no other element $\mathbf{x}^v - \mathbf{w}^v$ in $\mathrm{PB}(I(\overline{\mathcal{A}}))$ for which $u \succ v$.
Let us call these elements the primitive separated binomials in $\mathrm{PB}(I(\overline{\mathcal{A}}))$.

Corollary

Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Then there exists a bijection between the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ and the set of primitive separated binomials in $\mathrm{PB}(I(\overline{\mathcal{A}}))$.

Finiteness and Computation of Hilbert Bases (6.1.7)

Theorem

Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let G be a reduced Gröbner basis of $I(\overline{\mathcal{A}})$. Then the set $H = \{\alpha \in \mathbb{N}^n \mid \mathbf{x}^\alpha - \mathbf{w}^\alpha \in G\}$ is finite, and it is the Hilbert basis of the monoid $\mathcal{L}_+(\mathcal{A})$.

Corollary

Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Then the K-vector space $P_{W,0}$ is a finitely generated K-algebra.

Proof.

A K-basis of $P_{W,0}$ is given by the set of terms $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ such that $W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} = 0$. Therefore the Hilbert basis of $\mathcal{L}_+(W)$ generates $P_{W,0}$ as a K-algebra. This Hilbert basis is finite by the theorem. □

Examples

Example 1

Example

Consider the Diophantine equation $3z_1 - 5z_2 + 4z_3 = 0$.
We want to find all triples $(a_1, a_2, a_3) \in \mathbb{N}^3$ which satisfy this equation.

Let $\mathcal{A} = (3\ -5\ \ 4)$. We compute the reduced `DegRevLex`-Gröbner basis of the toric ideal of the Lawrence lifting of $\mathcal{A}$. The result is
$\{x_2 x_3^2 w_1 - x_1 w_2 w_3^2,\ x_3 w_1^3 w_2 - x_1^3 x_2 w_3,\ x_1^2 x_2^2 x_3 - w_1^2 w_2^2 w_3,$
$x_3^3 w_1^4 - x_1^4 w_3^3,\ x_1^5 x_2^3 - w_1^5 w_2^3,\ x_2^4 x_3^5 - w_2^4 w_3^5,\ x_1 x_2^3 x_3^3 - w_1 w_2^3 w_3^3\}$.

Thus the set of primitive separated binomials in $\mathrm{PB}(I(\bar{\mathcal{A}}))$ is
$\{x_1^2 x_2^2 x_3 - w_1^2 w_2^2 w_3,\ x_1^5 x_2^3 - w_1^5 w_2^3,\ x_2^4 x_3^5 - w_2^4 w_3^5,\ x_1 x_2^3 x_3^3 - w_1 w_2^3 w_3^3\}$

The Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ is $\{(2,2,1), (5,3,0), (0,4,5), (1,3,3)\}$.
So, the non-negative solutions of $3z_1 - 5z_2 + 4z_3 = 0$ are precisely the triples
$(a_1, a_2, a_3) = n_1(2,2,1) + n_2(5,3,0) + n_3(0,4,5) + n_4(1,3,3)$
with $n_1, n_2, n_3, n_4 \in \mathbb{N}$.

This Hilbert basis can also be used to determine the subring $P_{\mathcal{A},0}$ where $P = K[x_1, x_2, x_3]$ is equipped with the $\mathbb{Z}$ -grading given by $\mathcal{A}$. The above corollary yields $P_{\mathcal{A},0} = K[x_1^2 x_2^2 x_3,\ x_1^5 x_2^3,\ x_2^4 x_3^5,\ x_1 x_2^3 x_3^3]$.

Example 2

Inhomogeneous Diophantine equations can be solved using a similar technique, but require an extra trick.

Example

We want to find the non-negative integer solutions of the Diophantine equation $2z_1 + 5z_2 + 3z_3 = 11$.
They are the non-negative integer solutions of the homogeneous equation $2z_1 + 5z_2 + 3z_3 - 11z_4 = 0$ having fourth coordinate one. Let $\mathcal{A} = (2\ \ 5\ \ 3\ -11)$. We compute the reduced `DegRevLex`-Gröbner basis of the toric ideal of the Lawrence lifting of $\mathcal{A}$ and get the following primitive separated binomials:

$$\{x_2x_3^2x_4 - w_2w_3^2w_4,\ x_1x_3^3x_4 - w_1w_3^3w_4,\ x_1^3x_2x_4 - w_1^3w_2w_4,\ x_1^4x_3x_4 - w_1^4w_3w_4,\ x_1x_2^4x_4^2 - w_1w_2^4w_4^2,\ x_1^2x_2^3x_3x_4^2 - w_1^2w_2^3w_3w_4^2,\ x_2^6x_3x_4^3 - w_2^6w_3w_4^3,\ x_1^{11}x_4^2 - w_1^{11}w_4^2,\ x_3^{11}x_4^3 - w_3^{11}w_4^3,\ x_2^{11}x_4^5 - w_2^{11}w_4^5\}$$

So, the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ is the set
$\{(0,1,2,1), (1,0,3,1), (3,1,0,1), (4,0,1,1), (1,4,0,2), (2,3,1,2), (0,6,1,3), (11,0,0,2), (0,0,11,3), (0,11,0,5)\}$.
The solutions are $(0,1,2)$, $(1,0,3)$, $(3,1,0)$, and $(4,0,1)$.

Example 3

Example

Consider the system of Diophantine equations
$$\begin{cases} z_1 + 4z_2 + z_3 - 2z_4 &= 5 \\ 2z_1 - \ z_2 + z_3 - 3z_4 &= 0 \end{cases}$$
To find its non-negative integer solutions, we determine the non-negative integer solutions of the associated homogeneous system
$$\begin{cases} z_1 + 4z_2 + z_3 - 2z_4 - 5z_5 &= 0 \\ \quad 2z_1 - z_2 + z_3 - 3z_4 &= 0 \end{cases}$$
which have last coordinate one. Let $\mathcal{A} = \left(\begin{smallmatrix} 1 & 4 & 1 & -2 & -5 \\ 2 & -1 & 1 & -3 & 0 \end{smallmatrix}\right)$. We get the following Hilbert basis of $\mathcal{L}_+(\mathcal{A})$:
$$\{(0,1,1,0,1),\ (1,0,1,1,0),\ (0,0,15,5,1),\ (5,10,0,0,9),\ (6,9,0,1,8),$$
$$(7,8,0,2,7),\ (8,7,0,3,6),\ (9,6,0,4,5),\ (10,5,0,5,4),\ (11,4,0,6,3),$$
$$(12,3,0,7,2),\ (13,2,0,8,1),\ (14,1,0,9,0)\}$$
Since we are interested in elements of $\mathcal{L}_+(\mathcal{A})$ whose last coordinate is one, the relevant solutions are those whose last coordinate is zero or one. Let $Z = \{n_1(1,0,1,1) + n_2(14,1,0,9) \mid n_1, n_2 \in \mathbb{N}\}$. Then we have three families of solutions, namely $(0,1,1,0) + Z$, $(0,0,15,5) + Z$, and $(13,2,0,8) + Z$.

Example 4

Example

How many matrices in $\mathrm{Mat}_2(\mathbb{N})$ have both row sums equal to two?

METHOD 1

We label each position in the matrix by an indeterminate.
Then we notice that the matrices $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$ with $a_{11} + a_{12} = a_{21} + a_{22} = 2$ are in 1–1 correspondence with the power products $x_1^{a_{11}} x_2^{a_{12}} x_3^{a_{21}} x_4^{a_{22}}$ in $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ which have degree $\left(\begin{smallmatrix} 2 \\ 2 \end{smallmatrix}\right)$ with respect to the grading given by $\left(\begin{smallmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{smallmatrix}\right)$.

The bivariate Hilbert series of P with respect to this grading is

$$\mathrm{HS}_P(z_1, z_2) = \frac{1}{(1-z_1)^2(1-z_2)^2}$$

Therefore the answer is simply the coefficient of $z_1^2 z_2^2$ in the expansion of this series. By expanding the product $(1 + z_1 + z_1^2 + \cdots)^2(1 + z_2 + z_2^2 + \cdots)^2$, we see that the answer is nine.

Example 4 continued

METHOD 2

Example

First we solve the homogeneous Diophantine equation $z_1 + z_2 = z_3 + z_4$ as in the previous examples.
Using $\mathcal{A} = (1 \ \ 1 \ -1 \ -1)$, the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ turns out to be $\{(1,0,1,0),\, (1,0,0,1),\ (0,1,0,1),\, (0,1,1,0)\}$.
The corresponding matrices $\binom{1\ 0}{1\ 0},\ \binom{1\ 0}{0\ 1},\ \binom{0\ 1}{0\ 1},\ \binom{0\ 1}{1\ 0}$ have row sums one. We are looking for all their $\mathbb{N}$ -linear combinations with row sums equal to two.
For this purpose, we use the above correspondence and represent them as power products $t_1 = x_1x_3$, $t_2 = x_1x_4$, $t_3 = x_2x_4$, and $t_4 = x_2x_3$ in P .
Since their row sums are one, we need to determine the power products of degree two in the terms t_i .

Example 4 continued

Example

To compute the value of the Hilbert function of the ring $Q = \mathbb{Q}[t_1, t_2, t_3, t_4]$ in degree two, we use the surjective $\mathbb{Q}$-algebra homomorphism $\varphi : \mathbb{Q}[y_1, y_2, y_3, y_4] \longrightarrow Q$ defined by $y_i \mapsto t_i$.
Its kernel I is the toric ideal of (t_1, t_2, t_3, t_4) and turns out to be $I = (y_1 y_3 - y_2 y_4)$. Therefore we get

$$\mathrm{HS}_Q(z) = \mathrm{HS}_{\mathbb{Q}[y_1,y_2,y_3,y_4]/I}(z) = \frac{1+z}{(1-z)^3} = 1 + 4z + 9z^2 + \cdots$$

and hence the desired number is $\mathrm{HF}_Q(2) = 9$. Using this method, we can even list the nine solution matrices. They correspond to the images under φ of the nine terms of degree two in $\mathbb{Q}[y_1, y_2, y_3, y_4]$ whose residue classes form a $\mathbb{Q}$-basis of $(\mathbb{Q}[y_1, y_2, y_3, y_4]/I)_2$. We find the following nine matrices:

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

Example 4 continued

METHOD 3

Example

The third method is to solve the system of inhomogeneous Diophantine equations

$$\begin{cases} z_1 + z_2 & = & 2 \\ z_3 + z_4 & = & 2 \end{cases}$$

using the technique explained in the preceding example. The Hilbert basis of the associated homogeneous system is

$$\{(1,1,0,2,1),\ (0,2,1,1,1),\ (1,1,2,0,1),\ (1,1,1,1,1),\ (2,0,1,1,1),$$
$$(2,0,0,2,1),\ (0,2,0,2,1),\ (2,0,2,0,1),\ (0,2,2,0,1)\}$$

It yields the same nine solution matrices.

METHOD 4

Example

Finally, we present the fourth method: hand calculation! Unfortunately, this method does not work in complicated examples. Guess what you need!!!

Bounds for Hilbert Functions

Binomial Representations

Proposition

Let $n, i \in \mathbb{N}_+$ *. The number* n *has a unique representation of the form*

$$n = \binom{n(i)}{i} + \binom{n(i-1)}{i-1} + \cdots + \binom{n(j)}{j}$$

such that $1 \leq j \leq i$ *and such that* $n(i), \ldots, n(j) \in \mathbb{N}$ *are natural numbers which satisfy* $n(i) > n(i-1) > \cdots > n(j) \geq j$ *.*

Definition

Let $n, i \in \mathbb{N}_+$.

- The representation $n = \binom{n(i)}{i} + \cdots + \binom{n(j)}{j}$ with the property that $1 \leq j \leq i$ and $n(i) > n(i-1) > \cdots > n(j) \geq j$ is called the binomial representation of n in base i , or the i^{th} Macaulay representation of n . We shall also denote it by $n_{[i]}$.
- The i -tuple $(n(i), \ldots, n(j), 0, \ldots, 0)$ is called the top binomial representation of n in base i and is denoted by $\mathrm{Top}_i(n)$. We also let $\mathrm{Top}_i(0) = (0, \ldots, 0)$.

Examples

Example

The binomial representation of 102 in base 5 satisfies $102_{[5]} = \binom{8}{5} + 46_{[4]}$, since $\binom{8}{5} = 56 \leq 102 < 126 = \binom{9}{5}$. Similarly, $\binom{7}{4} = 35 \leq 46 < 70 = \binom{8}{4}$ yields $46_{[4]} = \binom{7}{4} + 11_{[3]}$. Continuing this way, we finally get $102_{[5]} = \binom{8}{5} + \binom{7}{4} + \binom{5}{3} + \binom{2}{2}$ and thus $\mathrm{Top}_5(102) = (8, 7, 5, 2, 0)$.

Similarly, we have $13984_{[10]} = \binom{16}{10} + \binom{15}{9} + \binom{12}{8} + \binom{11}{7} + \binom{9}{6} + \binom{8}{5} + \binom{5}{4} + \binom{3}{3}$ and $\mathrm{Top}_{11}(13984) = (16, 15, 12, 11, 9, 8, 5, 3, 0, 0)$.

Some Functions

Definition

Let $n, i \in \mathbb{N}_+$ and consider the binomial representation $n_{[i]} = \binom{n(i)}{i} + \cdots + \binom{n(j)}{j}$ of n in base i.

- We let $(n_{[i]})^+ = \binom{n(i)+1}{i} + \cdots + \binom{n(j)+1}{j}$.
- We let $(n_{[i]})^- = \binom{n(i)-1}{i} + \cdots + \binom{n(j)-1}{j}$.
- We let $(n_{[i]})^+_+ = \binom{n(i)+1}{i+1} + \cdots + \binom{n(j)+1}{j+1}$.
- We let $(n_{[i]})^-_- = \binom{n(i)-1}{i-1} + \cdots + \binom{n(j)-1}{j-1}$.

Moreover, we let $(0_{[i]})^+ = 0$, $(0_{[i]})^- = 0$, $(0_{[i]})^+_+ = 0$, and $(0_{[i]})^-_- = 0$.

Example

The binomial representation of the number 4 in base 2 is $4_{[2]} = \binom{3}{2} + \binom{1}{1}$. Therefore we have $(4_{[2]})^- = \binom{2}{2} + \binom{0}{1} = 1$, but $1_{[2]} = \binom{2}{2}$. Similarly, we have $(4_{[2]})^-_- = \binom{2}{1} + \binom{0}{0} = 3$, but $3_{[1]} = \binom{3}{1}$.

Some Inequalities

Proposition

Let $n, i \in \mathbb{N}_+$, $i > 1$. *Then we have the inequality* $(((n_{[i]})^-_-)_{[i-1]})^+_+ \geq n$.

Theorem

Let $m > n > 0$ *and* $i > 1$.

- *We have* $(n_{[i]})^+ \leq m$ *if and only if* $n \leq (m_{[i]})^-$.
- *The conditions above are satisfied if* $n \leq (n_{[i]})^- + ((m-n)_{[i-1]})^-$.

Lex-Segments Spaces and Ideals

Definition

Let $d \in \mathbb{N}$, and let $t \in \mathbb{T}^n$ be a term of degree d.

- A set of terms of the form $\{t' \in \mathbb{T}^n \mid \deg(t') = d,\ t' \geq_{\texttt{Lex}} t\}$ is called a `Lex`-segment. The empty set is also considered a `Lex`-segment.
- A K-vector subspace V of P_d is called a `Lex`-segment space if $V \cap \mathbb{T}^n$ is both a K-basis of V and a `Lex`-segment. In this case we denote the K-basis $V \cap \mathbb{T}^n$ by $\mathbb{T}(V)$.

Lex-Segments Spaces and Ideals II

Proposition

(Basic Properties of Lex-Segment Spaces)
Let $n \geq 2$ *, let* $d \in \mathbb{N}$ *, let* $V \subset P_d$ *be a non-zero* $\mathtt{Lex}$*-segment space, and let* t *be the lexicographically biggest term of degree* d *which is not in* $\mathbb{T}(V)$ *. We write* $t = x_1^{\alpha_1} \cdots x_r^{\alpha_r} x_{r+1}^{\alpha_{r+1}}$ *where* $r \in \{1, \ldots, n-1\}$ *and* $\alpha_{r+1} > 0$ *, and we let* $d_i = d - \sum_{j=1}^{i} \alpha_j$ *for* $i = 1, \ldots, r$ *.*

- *The* K*-vector space* V *is the* d^{th} *homogeneous component of the ideal*

$$x_1^{\alpha_1+1} \cdot (x_1, \ldots, x_n)^{d_1-1} + x_1^{\alpha_1} x_2^{\alpha_2+1} \cdot (x_2, \ldots, x_n)^{d_2-1} + \cdots$$
$$\cdots + x_1^{\alpha_1} \cdots x_{r-1}^{\alpha_{r-1}} x_r^{\alpha_r+1} \cdot (x_r, \ldots, x_n)^{d_r-1}$$

  Conversely, the d^{th} *homogeneous component of this ideal is the* $\mathtt{Lex}$*-segment space such that the biggest term of degree* d *which is not contained in it is* $x_1^{\alpha_1} \cdots x_r^{\alpha_r} x_{r+1}^{\alpha_{r+1}}$ *.*

- *The binomial representation of* $\dim_K(V)$ *in base* $n-1$ *is given by*

$$\dim_K(V) = \binom{n-1+d_1-1}{n-1} + \binom{n-2+d_2-1}{n-2} + \cdots + \binom{n-r+d_r-1}{n-r}$$

Lex-Segments Spaces in the Next Degree

The following proposition shows that we can find explicit expressions for the dimension and codimension of the vector space generated by a $\mathtt{Lex}$-segment space in the next degree.

Proposition

Let $d \in \mathbb{N}$ *and let* $V \subset P_d$ *be a non-zero* $\mathtt{Lex}$*-segment space.*

- *We have* $\dim_K(P_1 \cdot V) = ((\dim_K(V))_{[n-1]})^+$ *.*
- *We have* $\mathrm{codim}_K(P_1 \cdot V) = ((\mathrm{codim}_K(V))_{[d]})^+_+$ *.*

Lex-Segments Spaces and Hyperplane Sections

Definition

Let V be a K-vector subspace of P, and let $\ell \in P_1$. Then the image of V in $\overline{P}^{\ell} = P/(\ell)$ is called the ℓ-reduction of V and denoted by $\overline{V}^{\ell}$.

For the next proposition, we are only interested in the x_n-reduction of a $\mathtt{Lex}$-segment space. We identify $\overline{P}^{x_n}$ with $K[x_1, \ldots, x_{n-1}]$ and let $\overline{V} = \overline{V}^{x_n}$.

Proposition

Let $d \in \mathbb{N}$, let $V \subset P_d$ be a non-zero $\mathtt{Lex}$*-segment space.*

- *We have* $\dim_K(\overline{V}) = ((\dim_K(V))_{[n-1]})^{-}_{-}$.
- *We have* $\mathrm{codim}_K(\overline{V}) = ((\mathrm{codim}_K(V))_{[d]})^{-}$.

The Theorem of Green

Theorem

(Green's Reduction Theorem)

Let K be an infinite field, let $P = K[x_1, \dots, x_n]$ be standard graded, let $d \in \mathbb{N}$, and let $V \subseteq P_d$ be a K-vector subspace. For a generic linear form $\ell \in P_1$, we have

$$\operatorname{codim}_K(\overline{V}^{\ell}) \leq ((\operatorname{codim}_K(V))_{[d]})^{-}$$

Here equality holds if V is a `Lex`*-segment space.*

Corollary

Let K be an infinite field, let $P = K[x_1, \dots, x_n]$ be standard graded, and let I be a homogeneous ideal in P. For a generic linear form $\ell \in P_1$ and $d \in \mathbb{N}_+$, we have

$$\mathrm{HF}_{\overline{P}^{\ell}/\overline{I}^{\ell}}(d) = \mathrm{HF}_{P/(I+(\ell))}(d) \leq ((\mathrm{HF}_{P/I}(d))_{[d]})^{-}$$

Here equality holds if I_d is a `Lex`*-segment space.*

The Theorem of Macaulay

Theorem

(Macaulay's Growth Theorem)
Let K be a field, let $d \in \mathbb{N}_+$, and let V be a K-vector subspace of P_d. Then we have

$$\operatorname{codim}_K(P_1 \cdot V) \leq ((\operatorname{codim}_K(V))_{[d]})_+^+$$

Here equality holds if V is a `Lex`*-segment space.*

Notice that this version provides us with a sharp bound on the growth of the Hilbert function of a standard graded K-algebra.

Corollary

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $I \subseteq P$ be a homogeneous ideal, and let $d \in \mathbb{N}_+$. Then we have

$$\mathrm{HF}_{P/I}(d+1) \leq ((\mathrm{HF}_{P/I}(d))_{[d]})_+^+$$

Here equality holds if I_d is a `Lex`*-segment space which satisfies $I_{d+1} = P_1 \cdot I_d$.*

An Example

Example

There is no standard graded K-algebra R for which $\mathrm{HF}_R(1) = 3$ and $\mathrm{HF}_R(2) = 5$ and $\mathrm{HF}_R(3) = 8$.

To see why this is true, we suppose that $R = P/I$ is such an algebra, where $P = K[x_1, \ldots, x_n]$ is standard graded and $I \subseteq P$ is a homogeneous ideal.

Then the corollary yields
$8 = \mathrm{HF}_{P/I}(3) \leq ((\mathrm{HF}_{P/I}(2))_{[2]})^+_+ = (5_{[2]})^+_+ = (\binom{3}{2} + \binom{2}{1})^+_+ = \binom{4}{3} + \binom{3}{2} = 7$, a contradiction.