united nations
educational, scientific
and cultural
organization

international atomic
energy agency

the
abdus salam
international centre for theoretical physics

ICTP 40th Anniversary

SMR1563/10

School on Commutative Algebra and Interactions with Algebraic Geometry and Combinatorics

(24 May - 11 June 2004)

Gröbner bases and Hilbert functions

L. Robbiano
Dipartimento di Matematica
Università di Genova
Via Dodecaneso 35
16146 Genova
Italy

Gröbner Bases and Hilbert Functions

Lorenzo Robbiano

Università di Genova (Italy)

M. Kreuzer- L. Robbiano
Computational Commutative Algebra 1 (Springer 2000)
Computational Commutative Algebra 2 (Almost ready)

`http://cocoa.dima.unige.it`
`http://www.dima.unige.it/~robbiano/triestecol.pdf`
`http://www.dima.unige.it/~robbiano/triestebw.pdf`

Trieste, May 2004

INDEX

Gradings

Begin at the beginning and go on till you come to the end; then stop.
(Lewis Carroll)

PROPOSITION 1.1. Let Γ be a monoid, and let $\gamma_1, \ldots, \gamma_n \in \Gamma$.

a) There exists exactly one Γ-grading on P such that the non-zero constant polynomials are homogeneous of degree 0 and, for $i = 1, \ldots, n$, the indeterminate x_i is homogeneous of degree γ_i.

b) Under this grading, the set $\{\gamma \in \Gamma \mid P_\gamma \neq 0\}$ is the submonoid of Γ generated by $\{\gamma_1, \ldots, \gamma_n\}$.

EXAMPLE. Let $P = K[x_1, x_2]$ be equipped with the $\mathbb{Z}$-grading defined by $K \subseteq P_0$, $x_1 \in P_{-1}$, and $x_2 \in P_1$. Then $\dim_K(P_0) = \infty$.

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.

REMARK. A standard graded K-algebra R is an algebra of the form $R \cong P/I$, where $P = K[x_1, \ldots, x_n]$ is $\mathbb{N}$-graded such that $K = P_0$, each x_i is homogeneous of degree one, and I is a homogeneous ideal in P.

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.**

a) **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. In other words, the columns of the degree matrix are the degrees of the indeterminates. The rows of the degree matrix are called the weight vectors of the indeterminates $x_1, \ldots, x_n$.**

b) **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.**

c) **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 if it is clear which grading we are considering. A polynomial $f \in P_{W,d}$ is also called homogeneous of degree d, and we write $\deg_W(f) = d$.**

Let us have a look at an easy example.

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 $(2, 1, 1)$, because $W \cdot \log(x_1x_4)^{\mathrm{tr}} = W \cdot \log(x_2x_3)^{\mathrm{tr}} = (2, 1, 1)^{\mathrm{tr}}$, and the principal ideal generated by f is a homogeneous ideal.

PROPOSITION 1.2. **Let I be an ideal of P. Then the following conditions are equivalent.**

a) The ideal I is monomial.

b) 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.

c) 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.

Proof. Since I is generated by terms, and terms are homogeneous with respect to the gradings we are considering, we see that a) implies c). Obviously, b) is a special case of c). Therefore is suffices to show that b) implies a). We take a homogeneous polynomial $f \in I_{W,d}$ and show that there is only one term in its support. Let $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $t' = x_1^{\beta_1} \cdots x_n^{\beta_n}$ be terms in the support of f. Then $d = \deg_W(t) = \deg_W(t')$ implies $W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} = W \cdot (\beta_1, \ldots, \beta_n)^{\mathrm{tr}}$. Since we have $\det(W) \neq 0$, the $\mathbb{Z}$-linear map defined by W is injective. We obtain $(\alpha_1, \ldots, \alpha_n) = (\beta_1, \ldots, \beta_n)$, and hence $t = t'$. □

Let a $\mathbb{Z}^m$-grading on the polynomial ring $P = K[x_1, \ldots, x_n]$ be defined by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$. According to Definition 1.7.6, we obtain an induced $\mathbb{Z}^m$-grading on the graded free P-module $F = \bigoplus_{i=1}^r P(-\delta_i)$: this grading is given by $F_d = \bigoplus_{i=1}^r P_{W,\, d-\delta_i}$ for all $d \in \mathbb{Z}^m$. Thus a term $te_i \in \mathbb{T}^n\langle e_1, \ldots, e_r\rangle$, where $i \in \{1, \ldots, r\}$ and $t \in \mathbb{T}^n$, is a homogeneous element of F of degree $\deg_W(te_i) = \deg_W(t) + \delta_i$. In particular, F is the graded free P-module such that $\deg_W(e_i) = \delta_i$ for $i = 1, \ldots, r$.

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.**

a) 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 all entries of $v = a_1w_1 + \cdots + a_mw_m$ are non-negative and the entries of v 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.

b) 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 $a_1w_1 + \cdots + a_mw_m$ are positive. In this case, we shall also say that W is a matrix of positive type.

Now we are ready to show that polynomial rings with gradings of positive type and finitely generated graded modules over them have finite dimensional homogeneous components.

PROPOSITION 1.3. **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.**

a) We have $P_0 = K$.

b) 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 $t \neq 1$ has positive $V \cdot W$-degree.
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. It suffices to prove the claim for F. We do this by showing it is true for each $P(-\delta_i)$. 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 see that $P_{W,d} \subseteq P_{V\cdot W, V\cdot d}$. Hence we only have to show that the K-vector spaces $P_{V\cdot W,i}$ are finite dimensional. Their 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, since $V \cdot W$ has positive entries only. □

A further advantage of considering finitely generated graded P-modules in the case of gradings of positive type is that Nakayama's Lemma applies to them.

DEFINITION. **Let R be a ring and M a finitely generated R-module.**

a) **A finite system of generators of M is called a minimal system of generators if its number of elements is minimal among all systems of generators of M.**

b) **A system of generators of M is called an irredundant system of generators if no proper subset generates M.**

Clearly, minimal systems of generators are irredundant. Over arbitrary rings, the two notions do not coincide. For instance, when $R = \mathbb{Z}$ and M is the ideal generated by $\{2\}$, the system of generators $\{4, 6\}$ is irredundant, but not minimal.

One of the most important consequences of Nakayama's Lemma is that, in the case of gradings of positive type, irredundant systems of homogeneous generators of finitely generated graded modules are minimal. This will be shown in Proposition 1.5.

To formulate our next result, we need two additional objects. Let P be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $M \neq 0$ be a graded P-module. Then the set $\Gamma = \{d \in \mathbb{Z}^m \mid P_d \neq 0\}$ is clearly a submonoid of $\mathbb{Z}^m$, and we can define the Γ-submonomodule Σ of $\mathbb{Z}^m$ generated by $\{d \in \mathbb{Z}^m \mid M_d \neq 0\}$. It is easy to see that $\Sigma = \{d \in \mathbb{Z}^m \mid M_d \neq 0\}$ if M is a submodule of a graded free P-module. If the grading on P is of non-negative type, these monomodules are well-ordered, as the following proposition shows.

PROPOSITION 1.4 **Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of non-negative type.**

a) There exists a monoid ordering τ on $\mathbb{Z}^m$ such that the restriction of τ to Γ is a well-ordering.

b) For every finitely generated, graded P-module M, the restriction of τ to the monomodule Σ is a well-ordering.

c) If W is of positive type, there exists a well-ordering τ on Γ such that the set $P_+ = \bigoplus_{d>_\tau 0} P_d$ is the ideal generated by $\{x_1, \ldots, x_n\}$.

Proof. See [KR2] . □

Using this proposition, we see that the hypotheses of the Graded Version of Nakayama's Lemma 1.7.15 are satisfied for gradings of non-negative type. If the grading is actually of positive type, we obtain the result we strived for.

PROPOSITION 1.5. **Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, and let $M \neq 0$ be a finitely generated graded P-module.**

a) 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 $M/(x_1, \ldots, x_n)M$.

b) Every homogeneous system of generators of M contains a minimal one. All irredundant systems of homogeneous generators of M are minimal and have the same number of elements.

Proof. By Proposition 1.4, there exists a well-ordering τ on Γ such that $P_+ = \bigoplus_{d>_\tau 0} P_d = (x_1, \ldots, x_n)$, and therefore $P/P_+ \cong K$. Hence a) follows from Corollary 1.7.16.a. Now we prove b). Since $P_0 = K$ is a field, Corollary 1.7.16.b shows that every homogeneous system of generators of M contains a subset which is minimal among the homogeneous systems of generators of M and whose residue classes form a K-basis of $M/(x_1, \ldots, x_n)M$. This subset is also minimal among all systems of generators of M because, for any set of generators of M, their set of residue classes generates $M/(x_1, \ldots, x_n)M$. □

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

EXAMPLE. Let $P = \mathbb{Q}[x, y]$ 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 $P/P_+ \cong K[x]$ here.

We introduce the following notions which are useful for computing.

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

a) 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.

b) 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.

Our next corollary shows that non-negative gradings are of non-negative type and positive gradings are of positive type, as their names suggests.

PROPOSITION 1.6. **Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$.**

a) If the grading defined by W is non-negative, it is of non-negative type.

b) If the grading defined by W is positive, it is of positive type.

Proof. To prove claim a), we let C_i denote for $i = 1, \ldots, m$ the set of all indices $j \in \{1, \ldots, n\}$ such that the j^{th} column of W has its first non-zero entry in the i^{th} row. If we add high enough multiples of the first row to the rows below, the resulting matrix has strictly positive entries in the columns indexed by C_1. In particular, the second row of this matrix has strictly positive entries in the columns indexed by $C_1 \cup C_2$, and if we add high enough multiples of that row to the rows below, rows $2, 3, \ldots, m$ of the resulting matrix have strictly positive entries in the columns indexed by $C_1 \cup C_2$. Continuing this way, we finally arrive at a matrix whose last row has strictly positive entries in columns $C_1 \cup \cdots \cup C_m$, i.e. in all non-zero columns. Claim b) follows in the same way, except that there are no zero columns in W, so that the last row of the final matrix has positive entries everywhere. □

COROLLARY 1.7. **Assume that $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ defines a non-negative grading on P. Let M be a finitely generated, graded P-module, and let Σ be the set $\{d \in \mathbb{Z}^m \mid M_{W,d} \neq 0\}$. Then the relation $\mathtt{Lex}|_\Sigma$ is a well-ordering.**

Proof. *(Hint)* Combine Proposition 1.4. with the definition of a non-negative grading. □

We conclude the first part with the following remark.

REMARK. Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$.

a) If the grading defined by W is of non-negative type, then there exists a non-singular matrix $V \in \mathrm{Mat}_m(\mathbb{Z})$ such that the grading defined by the matrix $W' = V \cdot W$ is non-negative and $P_{W',V\cdot d} = P_{W,d}$ for all $d \in \mathbb{Z}^m$.

b) Similarly, if the grading defined by W is of positive type, then there exists a non-singular matrix $V \in \mathrm{Mat}_m(\mathbb{Z})$ such that the grading defined by the matrix $W' = V \cdot W$ is positive and $P_{W',V\cdot d} = P_{W,d}$ for all $d \in \mathbb{Z}^m$.

Homogeneous Gröbner Bases

No problem is so formidable that you can't walk away from it.
(Charles Schulz)

THEOREM 2.1 (The Homogeneous Buchberger Algorithm)
Let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let M be a graded submodule of F, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors which generate M. Furthermore, let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Consider the following sequence of instructions.

1) Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, and $s' = 0$.

2) Let d be the smallest degree with respect to `Lex` of an element in B or in $\mathcal{W}$. Form the subset B_d of B, form the subtuple $\mathcal{W}_d$ of $\mathcal{W}$, and delete their entries from B and $\mathcal{W}$, respectively.

3) If $B_d = \emptyset$, continue with step 6). Otherwise, choose a pair $(i, j) \in B_d$ and remove it from B_d.

4) Compute the S-vector S_{ij} and its normal remainder $S'_{ij} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If $S'_{ij} = 0$, continue with step 3).

5) Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, and append the set $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 3).

6) If $\mathcal{W}_d = \emptyset$, continue with step 9). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.

7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v)$. If $v' = 0$, continue with step 6).

8) Increase s' by one, append $g_{s'} = v'$ to the tuple $\mathcal{G}$, and append the set $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 6).

9) If $B = \emptyset$ and $\mathcal{W} = \emptyset$, return the tuple $\mathcal{G}$ and stop. Otherwise, continue with step 2).

This is an algorithm which returns a deg-ordered tuple $\mathcal{G} = (g_1, \ldots, g_{s'})$ whose elements are a homogeneous σ-Gröbner basis of M.

Variants of this algorithm compute Truncated Gröbner Bases and Minimal Systems of Generators, Minimal Presentations and Minimal Free Resolutions.

EXAMPLE. Let $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 3 & 4 \end{smallmatrix}\right)$, and let I be the homogeneous ideal generated by $\{f_1, f_2, f_3, f_4\}$ where $f_1 = x_1x_4 - x_2x_3$, $f_2 = x_1^2x_3 - x_2^3$, $f_3 = x_1x_3^2 - x_2^2x_4$, $f_4 = x_2x_4^2 - x_3^3$. Thus we have $\deg_W(f_1) = \binom{2}{4}$, $\deg_W(f_2) = \binom{3}{3}$, $\deg_W(f_3) = \binom{3}{6}$, and $\deg_W(f_4) = \binom{3}{9}$.

The free resolution is

$$0 \longrightarrow P\left(-\tbinom{5}{10}\right) \xrightarrow{\lambda} P\left(-\tbinom{4}{6}\right) \oplus P\left(-\tbinom{4}{7}\right) \oplus P\left(-\tbinom{4}{9}\right) \oplus P\left(-\tbinom{4}{10}\right) \xrightarrow{\psi}$$
$$\xrightarrow{\psi} P\left(-\tbinom{2}{4}\right) \oplus P\left(-\tbinom{3}{3}\right) \oplus P\left(-\tbinom{3}{6}\right) \oplus P\left(-\tbinom{3}{9}\right) \xrightarrow{\varphi} I \longrightarrow 0$$

Here ψ and λ are given by

$$\begin{pmatrix} x_2^2 & -x_1x_3 & -x_2x_4 & -x_3^2 \\ -x_3 & x_4 & 0 & 0 \\ x_1 & -x_2 & x_3 & x_4 \\ 0 & 0 & x_1 & x_2 \end{pmatrix}$$

$$\begin{pmatrix} -x_4 & -x_3 & -x_2 & x_1 \end{pmatrix}$$

Hilbert Functions

Theorem: All positive integers are interesting.

Proof: Assume the contrary. Then there is a smallest non-interesting positive integer.

But, hey, that's pretty interesting! A contradiction. QED

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.

a) 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.

b) Let $\Delta^0 f = f$. For $r \geq 1$, we define an integer function $\Delta^r f : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $\Delta^r f = \Delta(\Delta^{r-1} f)$, and we call it the $\mathbf{r^{th}}$ difference function of f.

c) 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.

d) 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 $i < i_0$.

e) 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.

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 $\leq r$.

Some authors use the expression "numerical polynomial" to denote integer valued polynomials. Clearly, for every $r \geq 0$, the set $\mathbb{IP}_{\leq r}$ is a $\mathbb{Z}$-submodule of $\mathbb{Q}[t]$. Notice that $\mathbb{IP}$ is not contained in $\mathbb{Z}[t]$, as evidenced by the integer valued polynomial $\frac{1}{2}t(t+1)$.

EXAMPLE. Let $a, b \in \mathbb{Z}$ with $b \geq 1$, and let $p \in \mathbb{Q}[t]$ be the polynomial defined by $p(t) = \binom{t+a}{b} = \frac{1}{b!}(t+a)(t+a-1)\cdots(t+a-b+1)$. Then p is an integer valued polynomial.

PROPOSITION 3.1. (Basic Properties of Integer Valued Polynomials)
Let $a \in \mathbb{Z}$, $r \in \mathbb{N}$, and let $(a_0, a_1, a_2, \ldots)$ be a sequence of integers.

a) 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 $\Delta^r p(t) = \mathrm{LC}_{\mathtt{Deg}}(p)$.

b) Let p be an integer valued polynomial of degree r, and let $c = \mathrm{LC}_{\mathtt{Deg}}(p)$. Then $q = p - c\binom{t+a}{r}$ is an integer valued polynomial of degree $< r$.

c) 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 $\mathbb{IP}$.

d) For a map $f : \mathbb{Q} \longrightarrow \mathbb{Q}$, the following conditions are equivalent.

1) There exists an integer valued polynomial $p \in \mathbb{IP}$ such that $f(i) = p(i)$ for all $i \in \mathbb{Z}$.
2) 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 $i \in \mathbb{Z}$.

Proof. See KR2]. □

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

a) 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.

b) 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 $\mathrm{ri}(f) = -\infty$.

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 $j < i$.
Clearly, 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 $j \in \mathbb{Z}$.
But there is no integer valued polynomial $p \in \mathbb{IP}$ such that $\mathrm{bin}_i(j) = p(j)$ for all $j \in \mathbb{Z}$, because in this case we would get $p = \mathrm{HP}_{\mathrm{bin}_i}$ and $p(-1) = \binom{-1}{i} = (-1)^i$, in contradiction to $\mathrm{bin}_i(-1) = 0$.

DEFINITION. Let M be a finitely generated graded P-module and let W define a grading of positive type on P. Then, Proposition 1.3 shows that we have a well-defined map

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

This map is called the Hilbert function of M.

Henceforth, we assume that the grading on P is the **standard grading**.

• The Hilbert function of M is an invariant under homogeneous linear changes of coordinates.

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

PROPOSITION 3.2. (Basic Properties of Hilbert Functions)
Let M, M', and M'' be three finitely generated graded P-modules.

a) 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 $i \in \mathbb{Z}$.

b) 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 $i \in \mathbb{Z}$.

c) Given finitely many finitely generated graded P-modules $M_1, \ldots, M_r$, we have $\mathrm{HF}_{M_1 \oplus \cdots \oplus M_r}(i) = \mathrm{HF}_{M_1}(i) + \cdots + \mathrm{HF}_{M_r}(i)$ for all $i \in \mathbb{Z}$.

d) Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$. Then the Hilbert function of the graded free P-module $F = \bigoplus_{j=1}^r P(-\delta_j)$ is given by $\mathrm{HF}_F(i) = \sum_{j=1}^r \mathrm{HF}_P(i - \delta_j) = \sum_{j=1}^r \mathrm{bin}_{n-1}(i - \delta_j + n - 1)$ for all $i \in \mathbb{Z}$.

e) Given homogeneous generators $\{g_1, \ldots, g_s\}$ of M, we let $\delta_j = \deg(g_j)$ for $j = 1, \ldots, s$. Then we have $\mathrm{HF}_M(i) \leq \sum_{j=1}^s \mathrm{bin}_{n-1}(i - \delta_j + n - 1)$ for all $i \in \mathbb{Z}$. In particular, HF_M is an integer Laurent function.

Proof. Part a) follows from the definition of $M(j)$, since we have $M(j)_i = M_{i+j}$ for all $i \in \mathbb{Z}$. Now we prove b). Since the P-linear maps in the exact sequence are homogeneous, we have for every $i \in \mathbb{Z}$ an exact sequence of finite dimensional K-vector spaces $0 \longrightarrow M'_i \longrightarrow M_i \longrightarrow M''_i \longrightarrow 0$. Counting dimensions yields $\dim_K(M_i) = \dim_K(M'_i) + \dim_K(M''_i)$, i.e. the claim.

Next we prove c) by induction on r. Since the case $r = 1$ is clear, we may assume $r > 1$. Then the homogeneous exact sequence

$$0 \longrightarrow \bigoplus_{j=1}^{r-1} M_j \longrightarrow \bigoplus_{j=1}^{r} M_j \longrightarrow M_r \longrightarrow 0$$

together with b) and the induction hypothesis yields the claim.

Part d) follows by combining a) and c). Finally, claim e) is a consequence of d) and of the fact that the P-linear map $\bigoplus_{j=1}^{s} P(-\delta_j) \longrightarrow M$ defined by $e_j \mapsto g_j$ for $j = 1, \ldots, s$ is homogeneous and surjective. □

PROPOSITION 3.3. (The Multiplication Sequence)
Let M be a finitely generated graded P-module, and let $f \in P$ be a non-zero homogeneous polynomial of degree d.

a) There is a homogeneous exact sequence of graded P-modules
$0 \longrightarrow \left[M/(0 :_M (f))\right](-d) \xrightarrow{\varphi} M \longrightarrow M/fM \longrightarrow 0$
where the map φ is induced by multiplication by f.

b) For all $i \in \mathbb{Z}$, we have $\mathrm{HF}_{M/fM}(i) = \mathrm{HF}_M(i) - \mathrm{HF}_{M/(0:_M(f))}(i-d)$.

c) The polynomial f is a non-zerodivisor for the module M if and only if $\mathrm{HF}_{M/fM}(i) = \Delta_d \mathrm{HF}_M(i)$ for all $i \in \mathbb{Z}$.

COROLLARY 3.4. 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
$0 \longrightarrow \left[P/(I :_P (f))\right](-d) \xrightarrow{\varphi} P/I \longrightarrow P/(I+(f)) \longrightarrow 0$
and then $\mathrm{HF}_{P/(I+(f))}(i) = \mathrm{HF}_{P/I}(i) - \mathrm{HF}_{P/(I:_P(f))}(i-d)$ 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 $i \in \mathbb{Z}$.

THEOREM 3.5. (Macaulay's Theorem for Hilbert Functions) **Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$, let F be the graded free P-module $F = \bigoplus_{j=1}^{r} P(-\delta_j)$, let M be a graded submodule of F, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Then we have $\mathrm{HF}_M(i) = \mathrm{HF}_{\mathrm{LT}_\sigma(M)}(i)$ for all $i \in \mathbb{Z}$.**

Proof. By Macaulay's Basis Theorem 1.5.7, the residue classes of the terms in $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle \setminus \mathrm{LT}_\sigma\{M\}$ form a K-basis of both F/M and $F/\mathrm{LT}_\sigma(M)$. For every i, the residue classes of the terms of degree i of $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle \setminus \mathrm{LT}_\sigma\{M\}$ are therefore K-bases of both $(F/M)_i$ and $(F/\mathrm{LT}_\sigma(M))_i$. Hence we get $\mathrm{HF}_M(i) = \mathrm{HF}_F(i) - \mathrm{HF}_{F/M}(i) = \mathrm{HF}_F(i) - \mathrm{HF}_{F/\mathrm{LT}_\sigma(M)}(i) = \mathrm{HF}_{\mathrm{LT}_\sigma(M)}(i)$ for all $i \in \mathbb{Z}$. □

COROLLARY 3.6. 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 $i \in \mathbb{Z}$.

Proof. We choose a homogeneous presentation $M = F/N$ with a graded free P-module $F = \bigoplus_{j=1}^{r} P(-\delta_j)$, where $\delta_1, \ldots, \delta_r \in \mathbb{Z}$, and a graded submodule N of F. Then we let $\overline{P} = L[x_1, \ldots, x_n]$ and $\overline{F} = \bigoplus_{j=1}^{r} \overline{P}(-\delta_j)$. By definition, we have $M \otimes_K L = \overline{F}/N\,\overline{F}$. Since Lemma 2.4.16 yields $\mathrm{LT}_\sigma\{N\} = \mathrm{LT}_\sigma\{N\,\overline{F}\}$, the theorem shows $\mathrm{HF}_N(i) = \mathrm{HF}_{N\,\overline{F}}(i)$ for all $i \in \mathbb{Z}$, and the claim follows. □

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

a) The subring $R[[z]] \cap K(z)$ of the field $K[[z]]_z$ is called the ring of rational power series over R.

b) 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.

c) The ring $R[z]_z$ is called the ring of Laurent polynomials over R. It is sometimes also denoted by $R[z, z^{-1}]$.

d) Let f be an integer Laurent function. The power series $\sum_f(i)z^i$ is called the Hilbert Series associated to f and denoted by HS_f.

PROPOSITION 3.7. **Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be a non-zero integer Laurent function.**

a) 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 $\mathrm{HS}_{\Delta f}(z) = (1 - z) \cdot \mathrm{HS}_f(z)$.

b) We have $\mathrm{HS}_{\Sigma f}(z) = \mathrm{HS}_f(z)/(1 - z)$.

Proof. To prove a), we calculate $(1 - z^q)\,\mathrm{HS}_f(z) = (1 - z^q)\sum_{i\geq\alpha} f(i)\,z^i = \sum_{i\geq\alpha} f(i)\,z^i - \sum_{i\geq\alpha+q} f(i-q)\,z^i = \mathrm{HS}_{\Delta_q f}(z)$. Claim b) follows from a), because we have $\mathrm{HS}_f(z) = \mathrm{HS}_{\Delta(\Sigma f)}(z) = (1 - z)\,\mathrm{HS}_{\Sigma f}(z)$. □

THEOREM 3.8. (Characterization of Laurent Series of Integer Functions of Polynomial Type)
For a non-zero integer Laurent function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, the following conditions are equivalent.

a) The integer function f is of polynomial type.

b) The associated Laurent series of f is of the form $\mathrm{HS}_f(z) = \frac{p(z)}{(1-z)^n}$, where $n = \deg(\mathrm{HP}_f(t)) + 1$ and $p(z) \in \mathbb{Z}[z, z^{-1}]$ is a Laurent polynomial over $\mathbb{Z}$.

Proof. (*Hint*) First we prove that a) implies b). Let $n = \deg(\mathrm{HP}_f(t)) + 1$. The associated polynomial of the function $\Delta^n f$ is $\mathrm{HP}_{\Delta^n f}(t) = \Delta^n \mathrm{HP}_f(t) = 0$. Thus the Laurent series $p(z) = \mathrm{HS}_{\Delta^n f}(z)$ is actually a Laurent polynomial, and hence $\mathrm{HS}_f(z) = p(z)/(1-z)^n$.

Conversely, we observe that the associated Laurent series of $\Delta^n f$ is the Laurent polynomial $\mathrm{HS}_{\Delta^n f}(z) = p(z) \in \mathbb{Z}[z, z^{-1}]$. In particular, we see that $\Delta^n f(i) = 0$ for large integers i. Thus $\Delta^n f$ is an integer function of polynomial type, and hence f itself is of polynomial type. □

COROLLARY 3.9. **Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be a non-zero integer Laurent function of polynomial type.**

a) The associated Laurent series of f has the form $\mathrm{HS}_f(z) = p(z)/(1-z)^n$, where $n \in \mathbb{N}$ 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 $c_\beta \neq 0$.

b) If $n > 0$, then we have $\mathrm{HP}_f(t) = \sum_{i=\alpha}^{\beta} c_i \binom{t-i+n-1}{n-1}$, and if $n = 0$, then we have $\mathrm{HP}_f(t) = 0$.

c) We have $\mathrm{ri}(f) = \beta - n + 1$.

Proof. In the light of the theorem, to prove a) we have to show that the Laurent polynomial $p(z)$ starts in degree α. Since we have $p(z) = \mathrm{HS}_{\Delta^n f}(z)$, this follows from the fact that the first non-zero value of $\Delta^n f$ is $\Delta^n f(\alpha)$.

In order to prove claim b), we note that the case $n = 0$ is trivially true. For $n > 0$, we calculate $\mathrm{HS}_f(z) = p(z) \cdot (1-z)^{-n} = \big(\sum_{i=\alpha}^{\beta} c_i z^i\big)\big(\sum_{j \geq 1-n} \binom{j+n-1}{n-1} z^j\big)$

$= \sum_{i \geq \alpha+1-n} \Big(\sum_{j=\alpha}^{\min\{\beta, i+n-1\}} c_j \binom{i-j+n-1}{n-1} \Big) z^i$. For $i \geq \beta + 1 - n$, we therefore get $f(i) = \sum_{j=\alpha}^{\beta} c_j \binom{i-j+n-1}{n-1}$, and the claim follows. Claim c) follows from $\mathrm{ri}(\Delta^n f) = \beta + 1$. □

DEFINITION. **For a finitely generated graded P-module M, the associated Laurent series of the Hilbert function of M is called the Hilbert series of M and is denoted by HS_M. In other words, the Hilbert series of M is the Laurent series $\mathrm{HS}_M(z) = \sum_{i \geq \alpha} \mathrm{HF}_M(i)\, z^i \in \mathbb{Z}[[z]]_z$, where α is the initial degree of M.**

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

PROPOSITION 3.10. (Basic Properties of Hilbert Series)
Let M, M', M'' be three finitely generated graded P-modules.

a) **For all $j \in \mathbb{Z}$, we have $\mathrm{HS}_{M(j)}(z) = z^{-j}\, \mathrm{HS}_M(z)$.**

b) **Given a homogeneous exact sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, we have $\mathrm{HS}_M(z) = \mathrm{HS}_{M'}(z) + \mathrm{HS}_{M''}(z)$.**

c) **Given finitely generated graded P-modules $M_1, \ldots, M_r$ such that $M = M_1 \oplus \cdots \oplus M_r$, we have $\mathrm{HS}_M(z) = \mathrm{HS}_{M_1}(z) + \cdots + \mathrm{HS}_{M_r}(z)$.**

d) **For $\delta_1, \ldots, \delta_r \in \mathbb{Z}$, the Hilbert series of the graded free module $F = \bigoplus_{j=1}^r P(-\delta_i)$ is $\mathrm{HS}_F(z) = (\sum_{j=1}^r z^{\delta_j})/(1-z)^n$.**

PROPOSITION 3.11. **Let M be a finitely generated graded P-module, and let $f \in P \setminus \{0\}$ be a homogeneous polynomial of degree d. Then we have $\mathrm{HS}_{M/fM}(z) = \mathrm{HS}_M(z) - z^d \, \mathrm{HS}_{M/(0:_M(f))}(z)$.**

In particular, the polynomial f is a non-zerodivisor for the module M if and only if $\mathrm{HS}_{M/fM}(z) = (1 - z^d) \, \mathrm{HS}_M(z)$.

COROLLARY 3.12. **Let M be a finitely generated graded P-module, and let $f_1, \ldots, f_\ell \in P$ be homogeneous polynomials of degrees $d_1, \ldots, d_\ell$ respectively.**

a) The sequence $f_1, \ldots, f_\ell$ is a regular sequence for M if and only if $\mathrm{HS}_{M/(f_1,\ldots,f_\ell)M}(z) = \prod_{i=1}^{\ell}(1 - z^{d_i}) \, \mathrm{HS}_M(z)$.

b) The sequence $f_1, \ldots, f_\ell$ is a regular sequence for M if and only if, for every permutation $\sigma(1), \ldots, \sigma(\ell)$ of the sequence $1, \ldots, \ell$, the sequence $f_{\sigma(1)}, \ldots, f_{\sigma(\ell)}$ is a regular sequence for M.

THEOREM 3.13. (Macaulay's Theorem for Hilbert Series)
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

$$\mathrm{HS}_M(z) = \mathrm{HS}_{\mathrm{LT}_\sigma(M)}(z)$$

THEOREM 3.14. Let M be a non-zero finitely generated graded P-module, and let $\alpha = \min\{i \in \mathbb{Z} \mid M_i \neq 0\}$. Then the Hilbert series of M has the form

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

where $\mathrm{HN}_M(z) \in \mathbb{Z}[z]$ and $\mathrm{HN}_M(0) = \mathrm{HF}_M(\alpha) > 0$.
In particular, let I be a homogeneous ideal of P. Then

$$\mathrm{HS}_{P/I}(z) = \frac{\mathrm{HN}_{P/I}(z)}{(1-z)^n}$$

Computation of Hilbert Functions

I think there is a world market for maybe five computers. (Thomas J. Watson, IBM, 1943)

Computers in the future may weigh no more than 1.5 tons. (Popular Mechanics, 1949)

640K ought to be enough for anybody. (William H. Gates, 1981)

Prediction is very difficult, especially about the future. (Niels Bohr)

THEOREM 4.1. (The Classical Hilbert Numerator Algorithm)
Let I be a non-zero proper monomial ideal in P. Consider the procedure $\texttt{MonHN}(I)$ defined by the following instructions.

1) Let $\{t_1, \ldots, t_s\}$ be the minimal monomial system of generators of I. If $s = 1$, let $d = \deg(t_1)$, return the result $1 - z^d$, and stop. Otherwise, let $p \in \{t_1, \ldots, t_s\}$, and let J be the ideal generated by $\{t_1, \ldots, t_s\} \setminus \{p\}$.

2) Call the procedures $\texttt{MonHN}(J)$ and $\texttt{MonHN}(J{:}_P(p))$, and let $f_1(z)$ and $f_2(z)$ be the polynomials which they return.

3) Let $d = \deg(p)$. Return the polynomial $f_1(z) - z^d f_2(z)$ and stop.

This is an algorithm which computes the Hilbert numerator $\mathrm{HN}_{P/I}(z)$.

Proof. First we prove finiteness. In step 2), the procedure `MonHN`(...) calls itself twice. We show that in both instances the minimal number of generators of the ideal passed as argument is smaller than s. This fact is clear for J, and $J :_P (p)$ is the ideal generated by the terms $\operatorname{lcm}(t_i, p)/p$ with $t_i \neq p$. Hence we eventually reach $s = 1$, and the procedure stops in step 1).

To show correctness, we note that when the procedure reaches $s = 1$, we have $I = (t_1)$ and the claim follows from Corollary 3.12.a. Now we use induction on the minimal number of generators and assume that $f_1(z) = \mathrm{HN}_{P/J}(z)$ and $f_2(z) = \mathrm{HN}_{P/(J:_P(p))}(z)$. From Proposition 3.11, we get that $\mathrm{HS}_{P/I}(z) = \mathrm{HS}_{P/J}(z) - z^d \,\mathrm{HS}_{P/(J:_P(p))}(z)$. Thus the claim follows from the observation that a P-module of the form P/I with a homogeneous proper ideal I has its first non-zero homogeneous component in degree zero, and from Theorem 3.14. □

A number of further algorithms for computing Hilbert numerators of monomial ideals are based on the idea that we can use the formula

$$\mathrm{HS}_{P/(I+(p))}(z) = \mathrm{HS}_{P/I}(z) - z^d \, \mathrm{HS}_{P/(I:_P(p))}(z)$$

where p is a term and $d = \deg(p)$, in another way, namely by expressing $\mathrm{HN}_{P/I}(z)$ in terms of $\mathrm{HN}_{P/(I+(p))}(z)$ and $\mathrm{HS}_{P/(I:_P(p))}(z)$.
In the following we refer to p as the pivot. Again we have to make sure that this does not lead to an infinite loop. We need to show that the recursive calls are applied to sets generating *simpler* ideals. The following notion will help us achieve this.

DEFINITION. Let I be a monomial ideal and $\{t_1, \ldots, t_s\}$ its minimal monomial set of generators. Then we define $\Sigma\deg(I) = \deg(t_1)+\cdots+\deg(t_s)$ and call it the total degree of I.

The recursion stops when we reach ideals I so simple the we know the Hilbert numerator of P/I without further computation. These very simple ideals are called the base cases. For instance, the base cases in the Classical Hilbert Numerator Algorithm are the principal monomial ideals. For our more general procedures a richer collection of base cases is provided by the following proposition.

PROPOSITION 4.2. **Let I be a non-zero proper monomial ideal in P whose minimal monomial generators $\{t_1, \ldots, t_s\}$ are pairwise coprime. Then the Hilbert numerator of P/I is given by $\mathrm{HN}_{P/I}(z) = \prod_{i=1}^{s}(1-z^{\deg(t_i)})$.**

THEOREM 4.3. **(Computing Hilbert Numerators Using Strategies) Suppose there is a procedure $\mathtt{Pivot}(I)$ which applies to monomial ideals I in P that are not monomial complete intersections, and which returns a term p such that $\Sigma\deg(I:_P(p)) < \Sigma\deg(I)$ and $\Sigma\deg(I+(p)) < \Sigma\deg(I)$. Let I be a non-zero proper monomial ideal in P. Consider the procedure $\mathtt{MonHN}(I)$ defined by the following instructions.**

1) **Check whether I is a monomial complete intersection. If it is, let $d_1, \ldots, d_s$ be the degrees of the minimal monomial generators of I. Return the result $\prod_{i=1}^{s}(1-z^{d_i})$ and stop. Otherwise, let p be the term computed by $\mathtt{Pivot}(I)$.**

2) **Call the procedures $\mathtt{MonHN}(I:_P(p))$ and $\mathtt{MonHN}(I+(p))$, and let $f_1(z)$ and $f_2(z)$ be the polynomials which they return.**

3) **Let $d = \deg(p)$. Return the polynomial $z^d f_1(z) + f_2(z)$ and stop.**

This is an algorithm which computes the Hilbert numerator $\mathrm{HN}_{P/I}(z)$.

The Indeterminate Strategy.
The procedure `Pivot`(I) chooses $i \in \{1, \ldots, n\}$ such that x_i is a proper divisor of one of the minimal monomial generators of I and returns $p = x_i$.

The GCD Strategy.
Consider the following strategy which contains some "random" choice: Given a monomial ideal I which is not a complete intersection, having a minimal monomial system of generators $\{t_1, \ldots, t_s\}$, choose an indeterminate x_i such that $\#\{j \mid x_i \text{ divides } t_j\}$ is maximal. Then choose randomly two different terms t_j, t_k which are divisible by x_i, and return $p = \gcd(t_j, t_k)$.

The CoCoA Strategy.
As a compromise between the two previous strategies, we introduce the following one. Given a monomial ideal I which is not a complete intersection, let x_i be one of the indeterminates occurring most often in the minimal monomial generators $\{t_1, \ldots, t_s\}$ of I. Then choose randomly two (or three) minimal generators t_j, t_k divisible by x_i, and let p be the highest power of x_i dividing both t_j and t_k. Return p and stop.

Inflation's down except for what you actually buy.
(Chad Hudson)

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** $0 \leq d \leq n$ **and where** $\mathrm{hn}_M(z) \in \mathbb{Z}[z]$ **satisfies** $\mathrm{hn}_M(0) > 0$ **and also** $\mathrm{hn}_M(1) \neq 0$**.**

a) **The polynomial** $\mathrm{hn}_M(z) \in \mathbb{Z}[z]$ **is called the simplified Hilbert numerator of** M**.**

b) **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**.**

c) **The number** $\dim(M) = d$ **is called the dimension of** M**.**

d) **The number** $\mathrm{mult}(M) = \mathrm{hn}_M(1)$ **is called the multiplicity of** M**.**

PROPOSITION 4.4. For a finitely generated graded P-module $M \neq (0)$, we have $\mathrm{mult}(M) > 0$.

Proof. Let $d = \dim(M)$, and let $\mathrm{hv}(M) = (h_0, \ldots, h_\delta)$. We have $\mathrm{HS}_M(z) = \frac{z^\alpha \mathrm{hn}_M(z)}{(1-z)^d} = z^\alpha (h_0 + \cdots + h_\delta z^\delta) \sum_{i \geq 0} \binom{d+i-1}{d} z^i$. For $N \gg 0$, the coefficient of $z^{\alpha+N}$ of this power series is $h_0 \binom{d+N-1}{d-1} + \cdots + h_\delta \binom{d+N-1-\delta}{d-1}$. It is a polynomial of degree $d-1$ in N, and its leading form $\frac{1}{(d-1)!}(h_0 + \cdots + h_\delta) N^d$ is positive. Thus we have $\mathrm{mult}(M) = \mathrm{hn}_M(1) = h_0 + \cdots + h_\delta > 0$. □

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

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

b) The regularity index of HF_M is called the regularity index of M and is denoted by $\mathrm{ri}(M)$.

Our next theorem says that the simplified Hilbert numerator $\mathrm{hn}_M(z)$ can be used to calculate the Hilbert polynomial of M.

THEOREM 4.5. (Computation of Hilbert Polynomials)
Let M be a non-zero finitely generated graded P-module with initial degree $\alpha = \min\{i \in \mathbb{Z} \mid M_i \neq 0\}$, and let $d = \dim(M)$.

a) Let $\mathrm{hn}_M(z) = h_0 + h_1 z + \cdots + h_\delta z^\delta$, where $h_0 > 0$ and $h_\delta \neq 0$. We have

$$\mathrm{HP}_M(t) = \begin{cases} \sum_{i=0}^{\delta} h_i \binom{t-\alpha-i+d-1}{d-1} & \text{if } d > 0, \\ 0 & \text{if } d = 0. \end{cases}$$

b) We have $\dim(M) = \begin{cases} 1 + \deg(\mathrm{HP}_M(t)) & \text{if } \mathrm{HP}_M(t) \neq 0, \\ 0 & \text{if } \mathrm{HP}_M(t) = 0. \end{cases}$

c) We have $\mathrm{mult}(M) = \begin{cases} (d-1)!\ \mathrm{LC}_{\mathtt{Deg}}(\mathrm{HP}_M(t)) & \text{if } d > 0, \\ \dim_K(M) & \text{if } d = 0. \end{cases}$

d) The regularity index of M satisfies $\mathrm{ri}(M) = \alpha + \delta - d + 1$.

Next proposition provides some rules for the behaviour of Hilbert polynomials under certain ideal-theoretic operations.

PROPOSITION 4.6. **Let I and J be proper homogeneous ideals of P.**

a) We have $\mathrm{HP}_{P/(I\cap J)}(t) = \mathrm{HP}_{P/I}(t) + \mathrm{HP}_{P/J}(t) - \mathrm{HP}_{P/(I+J)}(t)$**.**

b) If $\sqrt{J} = P_+$**, we have** $\mathrm{HP}_{P/(I\cap J)}(t) = \mathrm{HP}_{P/I}(t)$**.**

Proof. (*Hint*) To prove a), it suffices to apply the additivity of Hilbert polynomials to the appropriate exact sequences.

Now we show b). The assumption on J implies that $\sqrt{I+J} = P_+$. Thus $\dim(P/J) = \dim(P/(I+J)) = \dim(P/P_+)$. On the other hand, it is clear that $\mathrm{HP}_{P/P_+}(t) = 0$. Hence $\dim(P/P_+) = 0$, and consequently $\mathrm{HP}_{P/J}(t) = \mathrm{HP}_{P/(I+J)}(t) = 0$. Now the conclusion follows from a). □

General Hilbert Functions

In order to make an apple pie from scratch, you must first create the universe.
(Carl Sagan)

For the purpose of defining multivariate Hilbert series, the power series ring $R[[z_1, \ldots, z_m]]$ is not big enough. As we shall see, we need to allow negative exponents. Sometimes there will even be infinitely many terms having negative exponents. The following object is big enough to contain all the series we need.

DEFINITION. The set $R^{\mathbb{Z}^m}$ is an R-module with respect to componentwise addition and scalar multiplication. We shall 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.

Unfortunately, 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. Therefore we have to find a submodule of $R[[\mathbf{z}, \mathbf{z}^{-1}]]$ which is both small enough to be a ring and big enough to contain all the Hilbert series we need. The following definition gets us off the horns of this dilemma.

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

a) An extended power series $f = \sum_{i \in \mathbb{Z}^m} a_i \, \mathbf{z}^i$ is called a σ-Laurent series if there exists a subset $\Sigma \subseteq \mathbb{Z}^m$ such that $a_i = 0$ for $i \notin \Sigma$ and such that the restriction of σ to Σ is a well-ordering.

b) The set of all σ-Laurent series is called the σ-Laurent series ring over R and will be denoted by $R[[\mathbf{z}, \mathbf{z}^{-1}]]_\sigma$.

PROPOSITION 5.1. **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**

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

EXAMPLE. Let $m = 1$ and $\sigma = \mathtt{Deg}$. Then the ring $R[[z_1, z_1^{-1}]]_\sigma$ agrees with the usual Laurent series ring $R[[z_1]]_{z_1}$, since, for every $f = \sum_{i \in \mathbb{Z}} a_i z_1^i$ in the ring $R[[z_1, z_1^{-1}]]_\sigma$, there exists an index $i_0 \in \mathbb{Z}$ such that $a_i = 0$ for $i < i_0$.

We let K be a field and $P = K[x_1, \ldots, x_n]$ a polynomial ring over K which is graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type. It makes sense to generalize the definition of Hilbert functions as follows.

DEFINITION. Let M be a finitely generated graded P-module. Then the map $\mathrm{HF}_M : \mathbb{Z}^m \longrightarrow \mathbb{Z}$ given by $(i_1, \ldots, i_m) \mapsto \dim_K(M_{(i_1,\ldots,i_m)})$ for all $(i_1, \ldots, i_m) \in \mathbb{Z}^m$ is called the multigraded Hilbert function of M. If we want to make the dependence on the grading explicit, we shall also denote it by $\mathrm{HF}_{M,W}$.
More generally, given any $\mathbb{Z}^m$-graded K-algebra R and any graded R-module M which has finite dimensional homogeneous components, we define the multigraded Hilbert function of M in the same way.

In order to actually use the rules for computing multigraded Hilbert functions (which are essentially the same as in the standard case), we still need to know the multigraded Hilbert function of the polynomial ring $P = K[x_1, \ldots, x_n]$. Unfortunately, there is no simple formula as in the standard graded case.

PROPOSITION 5.2. **Let $P = K[x_1, \ldots, x_n]$ be graded by a matrix by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, and let $W = (w_{ij})$, where $w_{ij} \in \mathbb{Z}$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$. For all $(i_1, \ldots, i_m) \in \mathbb{Z}^m$, the value $\mathrm{HF}_P(i_1, \ldots, i_m)$ of the multigraded Hilbert function of P is the number of solutions $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ of the Diophantine system of equations**

$$\begin{cases} w_{11}y_1 + \cdots + w_{1n}y_n &= i_1 \\ w_{21}y_1 + \cdots + w_{2n}y_n &= i_2 \\ \vdots & \vdots \quad \vdots \\ w_{m1}y_1 + \cdots + w_{mn}y_n &= i_m \end{cases}$$

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

Proof. To show this claim, we note that $\dim_K(P_{(i_1,\ldots,i_m)})$ is the number of terms $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ of multidegree $(i_1, \ldots, i_m)$. Using the definition, we see that $\deg_W(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}}$, and this equals $(i_1, \ldots, i_m)^{\mathrm{tr}}$ if and only if $(\alpha_1, \ldots, \alpha_m)$ solves the given Diophantine system of equations. □

DEFINITION. Let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, a matrix of positive type, and let M be a finitely generated graded P-module. Then the extended power series

$$\mathrm{HS}_M(z_1, \ldots, z_m) = \sum_{(i_1,\ldots,i_m)\in\mathbb{Z}^m} \mathrm{HF}_M(i_1, \ldots, i_m)\, z_1^{i_1} \cdots z_m^{i_m} \in \mathbb{Z}[[\mathbf{z}, \mathbf{z}^{-1}]]$$

is called the multivariate Hilbert series of M. We shall also denote it by $\mathrm{HS}_M(\mathbf{z})$, or by $\mathrm{HS}_{M,W}(\mathbf{z})$ if we want to stress the underlying grading. More generally, given any $\mathbb{Z}^m$-graded K-algebra R and any graded R-module M which has finite dimensional homogeneous components, we define the multivariate Hilbert series of M by the same formula.

REMARK. Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type. Let τ be a monoid ordering on $\mathbb{Z}^m$ constructed in the proof of Proposition 1.4.a. In the proof of part b) of that proposition we saw that the restriction of τ to the set $\{d \in \mathbb{Z}^m \mid M_{W,d} \neq 0\}$ is a well-ordering for every finitely generated graded P-module M. Therefore we have $\mathrm{HS}_M(\mathbf{z}) \in \mathbb{Z}[[\mathbf{z}, \mathbf{z}^{-1}]]_\tau$, i.e. the Hilbert series we are interested in are all contained in the ring of τ-Laurent series over $\mathbb{Z}$.

PROPOSITION 5.3. (Hilbert Series of Polynomial Rings)
Let $P = K[x_1, \ldots, x_n]$ be graded by $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, a matrix of positive type. Then we have

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

Proof. (*Hint*) For $n = 1$, we have $\deg_W(x_1^i) = (iw_{11}, \ldots, iw_{m1})$. Therefore we obtain $\mathrm{HS}_P(z_1, \ldots, z_m) = \sum_{i \geq 0} z_1^{iw_{11}} \cdots z_m^{iw_{m1}} = 1/(1 - z_1^{w_{11}} \cdots z_m^{w_{m1}})$, i.e. the formula holds. Then use induction on n. □

COROLLARY 5.4. For every finitely generated graded P-module M, the multivariate Hilbert series of M has the form

$$\mathrm{HS}_{M,W}(z_1, \ldots, z_m) = \frac{z_1^{\alpha_1} \cdots z_m^{\alpha_m} \cdot \mathrm{HN}_M(z_1, \ldots, z_m)}{\prod_{j=1}^{n} (1 - z_1^{w_{1j}} \cdots z_m^{w_{mj}})}$$

where $(\alpha_1, \ldots, \alpha_m)$ is the componentwise minimum of the degree sequence of M, and where $\mathrm{HN}_M(z_1, \ldots, z_m)$ is a polynomial in $\mathbb{Z}[z_1, \ldots, z_m]$. We call this polynomial the multivariate Hilbert numerator of M.

THEOREM 5.5. (Computation of General Hilbert Series)
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.**
Given a non-zero proper monomial ideal I **in** P**, consider the procedure** $\mathtt{MultMonHN}(I)$ **defined by the following instructions.**

a) Let $\{t_1, \ldots, t_s\}$ **be the minimal monomial system of generators of** I**.**
If $s = 1$**, let** $\deg_W(t_1) = (d_1, \ldots, d_m) \in \mathbb{Z}^m$**, return the following polynomial** $1 - z_1^{d_1} \cdots z_m^{d_m}$**, and stop. Otherwise, let** $J = (t_1, \ldots, t_{s-1})$**.**

b) Call the procedures $\mathtt{MultMonHN}(J)$ **and** $\mathtt{MultMonHN}(J :_P (t_s))$**, and let** $p_1(z_1, \ldots, z_m)$ **and** $p_2(z_1, \ldots, z_m)$ **be the polynomials which they return.**

c) Let $\deg_W(t_s) = (d_1, \ldots, d_m)$**. Return the following polynomial** $p_1(z_1, \ldots, z_m) - z_1^{d_1} \cdots z_m^{d_m}\, p_2(z_1, \ldots, z_m)$ **and stop.**

This is an algorithm which computes a polynomial $\mathrm{HN}_{P/I}(z_1, \ldots, z_m)$ **in** $\mathbb{Z}[z_1, \ldots, z_m]$ **such that the formula**

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

holds true.

EXAMPLE. Let $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 5 & 8 \end{smallmatrix}\right)$, 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 have to form $J = (x_1^2, x_2)$.
In the second step, we have to compute the Hilbert numerators of P/J and of $P/(J :_P (x_3^3))$ recursively, where $J :_P (x_3^3) = (x_1^2, x_2) = J$.
When we compute $\mathrm{HN}_{P/J}(z_1, z_2)$, we have to form the ideals $J' = (x_1^2)$ and $J'' = J :_P (x_2) = (x_1^2)$ and to apply the algorithm 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 $\mathrm{HN}_{P/J}(z_1, z_2) = \mathrm{HN}_{P/J'}(z_1, z_2) - z_1^2 \,\mathrm{HN}_{P/J''}(z_1, z_2) = (1 - z_1^2)^2$.
Thus the original algorithm computes

$$\mathrm{HN}_{P/J}(z_1, z_2) - z_1^9 z_2^{15} \,\mathrm{HN}_{P/(J:_P(x_3^3))}(z_1, z_2) = (1 - z_1^2)^2(1 - z_1^9 z_2^{15}).$$

Altogether, we have

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

What happens to the Hilbert series when we change the grading? In particular, what happens when we use a coarser grading than our original one?

Given a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ which defines a grading on P and a matrix $A \in \mathrm{Mat}_{\ell,m}(\mathbb{Z})$, where $1 \leq \ell \leq m$, the $\mathbb{Z}$-linear map $\varphi : \mathbb{Z}^m \longrightarrow \mathbb{Z}^\ell$ whose defining matrix is A yields a homomorphism of graded rings

$$(\mathrm{id}_P, \varphi) : \ (P, \mathbb{Z}^m) \ \longrightarrow \ (P, \mathbb{Z}^\ell)$$

Given a graded module M over $(P, \mathbb{Z}^m)$, we can equip it with the structure of a graded $(P, \mathbb{Z}^\ell)$-module by defining

$$M_{A \cdot W, e} = \begin{cases} \bigoplus_{\{d \in \mathbb{Z}^m \mid A \cdot d = e\}} M_{W,d} & \text{if } e \in \mathrm{Im}(\varphi), \\ 0 & \text{otherwise.} \end{cases}$$

We shall say that the graded module $M = \bigoplus_{e \in \mathbb{Z}^\ell} M_{A \cdot W, e}$ is obtained from $M = \bigoplus_{d \in \mathbb{Z}^m} M_{W,d}$ by a change of grading.

PROPOSITION 5.6. Let be given two matrices $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and $A = (a_{ij}) \in \mathrm{Mat}_{\ell,m}(\mathbb{Z})$ such that the gradings on $P = K[x_1, \ldots, x_n]$ 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

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

Proof. The assumption that both W and $A \cdot W$ define gradings of positive type implies that $\mathrm{rk}(W) = m$ and $\mathrm{rk}(A \cdot W) = \ell$. Therefore the matrix A has maximal rank $\mathrm{rk}(A) = \ell$. By the definition of the grading, we have $\mathrm{HS}_{M,A\cdot W}(z_1, \ldots, z_\ell) = \sum_{e\in\mathbb{Z}^\ell} \sum_{\{d\in\mathbb{Z}^m | A\cdot d=e\}} \dim_K(M_{W,d})\, z_1^{e_1} \cdots z_\ell^{e_\ell}$. Now we use $z_1^{e_1} \cdots z_\ell^{e_\ell} = z_1^{a_{11}d_1+\cdots+a_{1m}d_m} \cdots z_\ell^{a_{\ell 1}d_1+\cdots+a_{\ell m}d_m} = (z_1^{a_{11}} \cdots z_\ell^{a_{\ell 1}})^{d_1} \cdots (z_1^{a_{1m}} \cdots z_\ell^{a_{\ell m}})^{d_m}$ and get

$$\begin{aligned} \mathrm{HS}_{M,A\cdot W}(z_1, \ldots, z_\ell) &= \sum_{d\in\mathbb{Z}^m} \mathrm{HF}_{M,W}(d)(z_1^{a_{11}} \cdots z_\ell^{a_{\ell 1}})^{d_1} \cdots (z_1^{a_{1m}} \cdots z_\ell^{a_{\ell m}})^{d_m} \\ &= \mathrm{HS}_{M,W}(z_1^{a_{11}} \cdots z_\ell^{a_{\ell 1}}, \ldots, z_1^{a_{1m}} \cdots z_\ell^{a_{\ell m}}) \end{aligned}$$

as claimed. □

An important special case occurs when $A \cdot W$ is the submatrix of W which consists of the first ℓ rows of W. In this case we use the following terminology.

DEFINITION. Let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, a matrix of positive type, let $\ell \in \{1, \ldots, m\}$, and let $W = \binom{U}{V}$, where $U \in \mathrm{Mat}_{\ell,n}(\mathbb{Z})$ and $V \in \mathrm{Mat}_{m-\ell,n}(\mathbb{Z})$. Then we say that the grading on P given by W refines the grading given by U, or that the the grading given by W is a refinement of the grading given by U.

It is clear that we can represent a refinement by using the change of grading defined by $A = (\mathcal{I}_\ell \mid 0) \in \mathrm{Mat}_{\ell,m}(\mathbb{Z})$. Thus Proposition 5.6 specializes immediately to the following result.

COROLLARY 5.7. Let P be graded by $W = \binom{U}{V} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ a matrix of positive type, where $U \in \mathrm{Mat}_{\ell,n}(\mathbb{Z})$ defines a grading of positive type and $V \in \mathrm{Mat}_{m-\ell,n}(\mathbb{Z})$.

a) We have $\mathrm{HS}_{M,U}(z_1, \ldots, z_\ell) = \mathrm{HS}_{M,W}(z_1, \ldots, z_\ell, 1, \ldots, 1)$.

b) We have $\dim_K(M_{U,d}) = \sum_{e \in \mathbb{Z}^{m-\ell}} \dim_K(M_{(d,e)}) = \mathrm{HS}_{M_{U,d}}(1, \ldots, 1)$ for every $d \in \mathbb{Z}^\ell$.

Applications

Bear in mind that 400 years ago, arithmetic was a difficult art!
So great an educator as Melanchton did not trust the average student
to penetrate into the secrets of fractions.
(Wolfgang Krull)

We do not have time to discuss applications. Nevertheless, I hope you have been convinced that Hilbert Functions are a great tool. The efficiency of the new algorithms for their computation allows us to use them in many areas inside and outside Mathematics.

To give you an idea about some applications, let me mention a few topics taken from the book [KR2].

- Veronese Subrings
- Powers of Polynomials and Ehrhart Functions
- Hilbert Driven Gröbner Basis Computations
- Knight Moves and Chess Puzzles
- Photogrammetry
- Generic Initial Ideals
- Rees Rings
- Segre Products and Hadamard Series
- Hilbert Bases and Toric Ideals
- Magic Squares
- Ideals of Points and their Hilbert Functions
- Hilbert Functions of Primary Ideals
- Hilbert Functions and SAGBI Bases

In the end, everything is a gag.
(Charlie Chaplin)

The Generating Function of Elements NOT in a Monoid

Let $S \subseteq \mathbb{N}^n$ be a finitely generated additive submonoid. How can we compute the generating function of the "gaps" of S?

We construct the associated K-algebras and get

$$K[S] \subseteq K[\mathbb{N}^n] = K[x_1, \ldots, x_n]$$

We observe that the generating function of $\mathbb{N}^n$, equivalently of the power products in $K[x_1, \ldots, x_n]$, is $\frac{1}{\prod_{i=1}^{n}(1-z_i)}$.

To compute the generating function of the elements in S, equivalently of the power products in $K[S]$, we need to represent $K[S]$ as a quotient algebra.

To this end, let $s_1, \ldots, s_r$ be generators of S, let $y_1, \ldots y_r$ be indeterminates, and let $W \in \mathrm{Mat}_{n,r}(\mathbb{Z})$ be the matrix whose columns are the coordinates of $s_1, \ldots, s_r$ respectively.

It is clear that S is naturally W-graded, and we can equip $K[y_1, \ldots, y_r]$ with the W-grading so that the canonical homomorphism $\varphi : K[y_1, \ldots, y_r] \longrightarrow K[S]$ is a W-graded homomorphism of K-algebras.

The kernel of φ is by definition the toric ideal associated to $s_1, \ldots, s_r$, and it can be efficiently computed by smart algorithms which avoid elimination techniques.

We compute the Hilbert series of $R = K[y_1, \ldots, y_r]/\operatorname{Ker}(\varphi)$, and hence we get the generating function of S.

Observe that the number of rows in W is precisely n, therefore the Hilbert series is a series in n indeterminates.

In conclusion, the answer to our problem is

$$\frac{1}{\prod_{i=1}^{n}(1-z_i)} - \mathrm{HS}_{R,W}(z_1, \ldots, z_n)$$

For example, if $S = \langle 3, 4 \rangle$, we get $\frac{1}{(1-z)} - \frac{1-z^{12}}{(1-z^3)(1-z^4)} = z + z^2 + z^5$
Therefore the gaps of $S = \langle 3, 4 \rangle$ are $1, 2, 5$.

EXERCISE: Prove that for $a, b \in \mathbb{N}_{>1}$ such that $\gcd(a, b) = 1$, the "last" gap of $S = \langle a, b \rangle$ is

$$ab - (a + b)$$

THE TRUE END