An Introduction to Combinatorial Commutative Algebra

Richard P. Stanley

Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139

Abstract

In these lectures we will provide a brief introduction to the interactions between commutative algebra and combinatorics, and will discuss some applications to combinatorics. Our basic object of study will be graded algebras and graded modules over them. Let $\mathbb{N}$, $\mathbb{P}$, and $\mathbb{Z}$ denote the set of nonnegative integers, positive integers, and integers, respectively.

1. DEFINITION. Let k be a field. By an *$\mathbb{N}$-graded k-algebra* (or *graded algebra)* we will mean in this paper a commutative, associative ring R with identity, containing a copy of the field k (so that R is a vector space over k, i.e., a *k-algebra),* together with a collection of subspaces $\{R_i\}_{i\in\mathbb{N}}$, satisfying:

(i) R is the vector space direct sum of the subspaces R_i; written

$$R = \coprod_{i\in\mathbb{N}} R_i,$$

(ii) $R_0 = k$,

(iii) $R_i R_j \subset R_{i+j}$,

(iv) R is finitely-generated as a k-algebra, i.e., there exist finitely many elements $x_1, \ldots, x_r \in R$ such that every element in R is a polynomial (not necessarily unique) in $x_1, \ldots, x_r$ with coefficients in k. If we can choose each $x_i \in R_1$ (i.e., R is generated by R_1), then R is called *standard.*

An element $x \in R_i$ is said to be *homogeneous of degree i,* denoted deg $x = i$. In particular, deg 0 is arbitrary. For any set $S \subset R$ we let

ISBN 0-12-379120-0

$\mathbf{H}(S)$ denote the set of homogeneous elements of S. In particular, $\mathbf{H}(R)=\bigcup_{i\in\mathbb{N}} R_i$ (set union). Denote by R_+ the ideal $\coprod_{i\geq 1} R_i$ of R. It is easily seen that R is generated by finitely many *homogeneous* elements.

2. DEFINITION. Let R be a graded algebra. A *$\mathbb{Z}$-graded R-module* M (or *graded R-module*) is a unitary R-module ("unitary" means $1\cdot u=u$ for all $u\in M$), together with a collection of subspaces $\{M_i\}_{i\in\mathbb{Z}}$, satisfying:

(i) M is the vector space direct sum of the subspaces M_i, denoted

$$M=\coprod_{i\in\mathbb{Z}} M_i,$$

(ii) $R_iM_j\subset M_{i+j}$,

(iii) M is finitely-generated as an R-module, i.e., there exist finitely many elements $u_1,\ldots,u_s\in M$ such that $M=u_1R+\ldots+u_sR$.

Note that condition (iii) implies that $M_i=0$ for all but finitely many $i<0$. The notation $\deg x$, $\mathbf{H}(S)$, etc., is carried over in an obvious way to M. Again it is clear that M is generated by finitely many *homogeneous* elements.

Let us mention that one can define more generally $\mathbb{N}^m$-graded algebras and $\mathbb{Z}^m$-graded modules ($m>1$) in an obvious way, but to keep the exposition simple we confine ourselves to the $m=1$ case. However, many important applications to combinatorics require $m>1$.

Recall that if k is any noetherian ring (i.e., every ascending chain of ideals becomes stable), then the Hilbert basis theorem asserts that the polynomial ring $k[x]$ is also noetherian. From this it is easy to deduce our first basic result.

3. THEOREM. If the submodule N of M (or ideal I of R) is generated as an R-module by a subset $S\subset N$, then some finite subset of S generates N.

APPLICATION: Let ϕ be an $r\times s$ matrix with integer entries (or *$\mathbb{Z}$-matrix*). Let $\beta\in\mathbb{Z}^r$, and define

$$\Lambda=\{\alpha\in\mathbb{N}^s:\ \phi\alpha=0\} \tag{1}$$

$$\Lambda_\beta=\{\alpha\in\mathbb{N}^s:\ \phi\alpha=\beta\}$$

One of the main aims of these lectures is to understand the structure of Λ and Λ_β. Note that Λ is a *submonoid* of $\mathbb{N}^s$, and that Λ_β is a "Λ-module" in the sense that $\Lambda+\Lambda_\beta\subset\Lambda_\beta$.

4. THEOREM.

(a) Λ is a finitely-generated monoid, i.e., there exist $\alpha_1, \ldots, \alpha_t \in \Lambda$ such that $\Lambda = \alpha_1 \mathbb{N} + \ldots + \alpha_t \mathbb{N}$.

(b) Λ_β is a finitely-generated Λ-module, i.e., there exist $\beta_1, \ldots, \beta_j \in \Lambda_\beta$ such that $\Lambda_\beta = \cup(\beta_i + \Lambda)$.

SKETCH OF PROOF.

(a) Let $R = k\Lambda$ be the monoid algebra of Λ over the field k. We may think of R as the subalgebra of $A = k[x_1, \ldots, x_s]$ generated (or spanned as a vector space) be all monomials x^γ, $\gamma \in \Lambda$ (where $x^\gamma = x_1^{\gamma_1} \cdots x_s^{\gamma_s}$, $\gamma = (\gamma_1, \ldots, \gamma_s)$). By Theorem 3 some finite subset S of the x^γ generates I. It is now routine to verify that S generates R as a k-algebra, so that $\{\gamma : x^\gamma \in S\}$ generates Λ.

(b) As in (a), let $M_\beta = k\Lambda_\beta$ be the k-span of Λ_β, regarded as the k-subspace of A with basis x^γ, $\gamma \in \Lambda_\beta$. Thus M_β is an R-module. Let I_β be the ideal of I generated by M_β. Then I_β is generated by some finite subset $T \subset \{x^\gamma : \gamma \in \Lambda_\beta\}$, and one shows easily that T generates M_β as an R-module. Then $\{\gamma : x^\gamma \in T\}$ generates Λ_β as a Λ-module. □

5. EXERCISE. Find a submonoid of $\mathbb{N}^2$ which is not finitely-generated. Show that every submonoid of $\mathbb{N}$ is finitely-generated.

The fundamental combinatorial object associated with graded algebras and modules is their *Hilbert series*. Define

$$H(R,n) = \dim_k R_n, \quad n \in \mathbb{N},$$

$$H(M,n) = \dim_k M_n, \quad n \in \mathbb{Z}.$$

It follows from the finiteness properties of R and M that $H(R,n) < \infty$ and $H(M,n) < \infty$. The functions $H(R,n)$ and $H(M,n)$ are called the *Hilbert functions* of R and M, respectively. The generating functions

$$F(R,\lambda) = \sum_{n \in \mathbb{N}} H(R,n)\lambda^n$$

$$F(M,\lambda) = \sum_{n \in \mathbb{Z}} H(M,n)\lambda^n$$

are called the *Hilbert series* of R and M.

6. EXERCISE. (a) If $R = k[x_1, \ldots, x_r]$, graded by defining $\deg x_i = a_i \in \mathbb{P}$, then

$$F(R,\lambda)=\prod_{i=1}^{r}(1-\lambda^{a_i})^{-1}$$

(b) Suppose R is any graded algebra and M a *free* graded R-module with a homogeneous basis $y_1,\ldots,y_s$ where $\deg y_i=b_i\in\mathbb{Z}$. Then

$$F(M,\lambda)=(\lambda^{b_1}+\ldots+\lambda^{b_s})F(R,\lambda).$$

A submodule N of M (or ideal I of R) generated by homogeneous elements is called a *homogeneous submodule* (or *homogeneous ideal*) and has a natural grading $N=\coprod_{i\in\mathbb{Z}}N_i$ given by $N_i=N\cap M_i$. Similarly the quotient module M/N has a natural grading defined by $(M/N)_i=M_i/N_i$, where M_i/N_i is a quotient of vector spaces. It is clear that

$$F(M,\lambda)=F(N,\lambda)+F(M/N,\lambda).$$

Now let $\theta\in\mathbf{H}(R)$ and define $(0:\theta)=(0:\theta)_M=\{u\in M:\theta u=0\}$. This is a homogeneous submodule of M. The following lemma is straightforward to verify.

7. LEMMA. If $\theta\in R_i$, $i\neq 0$, then

$$F(M,\lambda)=\frac{F(M/\theta M,\lambda)-\lambda^{i}F((0:\theta),\lambda)}{1-\lambda^{i}}.$$

Using Lemma 7 and induction on the number of generators of R, the following basic result is obtained.

8. THEOREM. Let R be generated by homogeneous elements of degrees $a_1,\ldots,a_t>0$. Then

$$F(M,\lambda)=P(M,\lambda)\prod_{i=1}^{t}(1-\lambda^{a_i})^{-1}, \tag{2}$$

where $P(M,\lambda)\in\mathbb{Z}[\lambda,\lambda^{-1}]$ (i.e., $P(M,\lambda)$ is a polynomial in λ and λ^{-1} with integer coefficients). If M has no elements of negative degree (e.g., if $M=R$), then $P(M,\lambda)\in\mathbb{Z}[\lambda]$.

Standard results concerning coefficients of rational generating functions [15] yield:

9. COROLLARY. Let R be as in Theorem 8. Let $m=LCM\{a_1,\ldots,a_t\}$. Then there exist polynomials $P_0(n),\ldots,P_{m-1}(n)$ such that $H(M,n)=P_i(n)$ whenever $n\equiv i \pmod m$ and n is sufficiently large (denoted $n>>0$). In particular, if R is standard, $H(M,n)$ is a polynomial for $n>>0$, the *Hilbert polynomial* of M. If $M_i=0$ for $i<0$, then $H(M,n)$ is a polynomial for *all* $n\geq 0$ if and only if $\deg P(M,\lambda)<a_1+\ldots+a_t$, in the notation of (2).

10. APPLICATION. Let $\Lambda\subset\mathbb{N}^{n^2}$ be the set of all $n\times n$ $\mathbb{N}$-matrices

such that all row and column sums are equal. A matrix $\alpha=(\alpha_{ij})\in\Lambda$ may be regarded as an $\mathbb{N}$-solution to the system of equations $\sum_i \alpha_{ij}=\sum_i \alpha_{ji}=\alpha_{11}+\alpha_{12}+\ldots+\alpha_{1n}$, $1\le j\le n$, so Λ is a monoid of the type arising in Theorem 4. Define a grading on $R=k\Lambda$ by setting deg $x^\alpha=\alpha_{11}+\alpha_{12}+\ldots+\alpha_{1n}$, the line sum of the matrix $\alpha\in\Lambda$. Then a basis for R_i consists of all monomials x^α of degree i, so $H(R,i)$ is the number of $n\times n$ $\mathbb{N}$-matrices with every row and column sum equal to i. This number is usually denoted by $H_n(i)$. According to the Birkhoff-von Neumann theorem (e.g., [11, Th. 5.2]), every $\alpha\in\Lambda$ is a sum of permutation matrices. This is equivalent to saying that R is standard. By Corollary 9, it follows that $H_n(i)$ is a polynomial in i for $i>>0$. It can be shown (as was first done in [14]) that $H_n(i)$ is a polynomial for *all* $i\ge 0$, of degree $(n-1)^2$. Some further properties of $H_n(i)$ will be discussed later.

11. EXERCISE. Let $\Omega\subset\mathbb{N}^{n^2}$ be the set of all $n\times n$ *symmetric* $\mathbb{N}$-matrices with all row sums equal. Let S be the subalgebra of $R=k\Omega$ generated by R_1+R_2. Show that R is a finitely-generated S-module (though $R\neq S$ when $n\ge 7$). Deduce that if $S_n(i)$ is the number of $\alpha\in\Omega$ with line sum i, then there exist polynomials $P_n(i)$ and $Q_n(i)$ such that $S_n(i)=P_n(i)+(-1)^iQ_n(i)$ for $i>>0$. (Again, it can be shown that equality holds for all $i\ge 0$.)

We now come to a lemma of crucial importance for further progress. The analogue for non-graded rings appears in [7, Thm. 82], while a proof for the graded case stated below may be found in [1, Lemma 2.2]. This lemma will allow us to bypass techniques from homological algebra normally used to proved many of the subsequent results.

12. LEMMA. Let R be a graded algebra and $M\neq 0$ a graded R-module. Suppose every $x\in\mathbf{H}(R_+)$ is a zero-divisor on M (i.e., for some $0\neq u\in M$, $xu=0$). Then for some $0\neq u\in\mathbf{H}(M)$, $uR_+=0$.□

Now let M be a graded R-module. By the lemma, exactly one of the following two possibilities holds: (a) some $\theta\in\mathbf{H}(R_+)$ is a non-zero divisor (NZD) on M, or (b) some $u\in\mathbf{H}(M)$ satisfies $R_+u=0$. In either case we may consider the quotient module $M/\theta M$ or M/uR. In case (a), M will be a free module (not necessarily of finite rank) over the ring $k[\theta]$. A set $B\subset\mathbf{H}(M)$ will be a basis for M as a $k[\theta]$-module if and only if the image of B in $M/\theta M$ is a k-basis for $M/\theta M$. In particular, if deg $\theta=a$ then

$$F(M,\lambda)=(1-\lambda^a)^{-1}F(M/\theta M,\lambda). \tag{3}$$

In case (b), uR is a one-dimensional vector space and if deg $u=b$ then

$$F(M,\lambda)=\lambda^b+F(M/uR,\lambda). \tag{4}$$

Now apply (a) or (b), as the case may be, to $M/\theta M$ or M/uR, and form a new quotient module. As we continue this process, we obtain a sequence of smaller and smaller quotient modules of M. By the ascending chain condition on submodules, this process eventually terminates in 0. We then say that M has been "peeled." Using (3) and (4) the Hilbert series of M can be written down by inspection from the peeling. Moreover, we obtain a canonical form for writing the elements of M.

13. EXAMPLE. Let $\Lambda=\mathbb{N}^2-\{(1,0)\}$. Then the monoid algebra $R=k\Lambda$ is given by $R=k[x^2,x^3,y,xy]$. Now note the following:

(a) y is an NZD of R,

(b) R/yR is spanned by $\{1,x,x^2,\ldots,xy\}$ so $xyR_+=0$ in R/yR.

(c) x^2 is an NZD of $R/(yR+xyR)$.

(d) $S=R/(yR+xyR+x^2R)$ is spanned by $\{1,x^3\}$, so $x^3R_+=0$ in S, and $1\cdot R_+=0$ in S/x^3S.

It follows that every element f of R can be written uniquely in the form

$$f=xyp_1(y)+p_2(x^2,y)+x^3p_3(x^2,y),$$

where $p_1\in k[x_1]$ and p_2, $p_3\in k[x_2,x_3]$. (In effect, we have decomposed the monoid Λ into the disjoint subsets $(1,1)+(0,1)\,\mathbb{N}$, $(2,0)\,\mathbb{N}+(0,1)\,\mathbb{N}$, and $(3,0)+(2,0)\,\mathbb{N}+(0,1)\,\mathbb{N}$.) We also see that

$$F(R,\lambda)=\frac{\lambda^2}{1-\lambda}+\frac{1+\lambda^3}{(1-\lambda)(1-\lambda^2)}=\frac{1}{(1-\lambda)^2}-\lambda.$$

14. EXERCISE. Peel the rings $k[x,y,z,w]/(xz,xw,yw)$ and $k[x,y,z,w]/(xw,yw,zw,xyz)$ (with the standard grading), and compute their Hilbert series. Express each Hilbert series as a fraction reduced to lowest terms.

The following result is immediate from the way $F(M,\lambda)$ is computed from a peeling of M.

15. COROLLARY (and definition). Let M be a graded module. Then the order to which $\lambda=1$ is a pole of $F(M,\lambda)$ is equal to the total number of NZD's encountered in peeling M. This number is called the *Krull dimension* of M, denoted dim M.

It is not difficult to show at this stage that dim M is also equal to the maximum number of (homogeneous) elements of $R/Ann\ M$ which are algebraically independent over k, where $Ann\ M=\{x\in R: xM=0\}$. Note that $Ann\ R=0$.

If $\theta_1, \ldots, \theta_r\in H(R_+)$ then it is clear that dim $M/(\theta_1 M+\ldots+\theta_r M)\geq$dim $M-r$. If equality holds we call $\theta_1, \ldots, \theta_r$ a *partial homogeneous system of parameters* for M. Clearly $r\leq d=$dim M. If equality holds, we call $\theta_1, \ldots, \theta_d$ a *homogeneous system of parameters (h.s.o.p.)*.

16. THEOREM. Let $\theta_1, \ldots, \theta_d\in H(R_+)$, and let M be a $\mathbb{Z}$-graded R-module. The following conditions are equivalent:

(i) $\theta_1, \ldots, \theta_d$ are an h.s.o.p.

(ii) $\theta_1, \ldots, \theta_d$ are algebraically independent over k in R/*Ann* M, and dim $M/(\theta_1 M+\ldots+\theta_d M)=0$.

(iii) $\theta_1, \ldots, \theta_d$ are algebraically independent over k in R/*Ann* M, and M is a finitely-generated $k[\theta_1, \ldots, \theta_d]$-module.

(iv) $d=$dim M and M is a finitely-generated $k[\theta_1, \ldots, \theta_d]$-module.

17. THEOREM. If $\theta_1, \ldots, \theta_d$ are the NZD's encountered in a peeling of M, then $\theta_1, \ldots, \theta_d$ is an h.s.o.p. for M. Moreover, if R is standard and k infinite, we can take each deg $\theta_i=1$.

Theorem 17 is essentially the "Noether normalization lemma", which guarantees the existence of an h.s.o.p. for M.

The process of peeling M begins with the construction of a sequence $\theta_1, \ldots, \theta_r\in H(R_+)$ (which may be void) such that θ_i is an NZD in $M/(\theta_1 M+\ldots+\theta_{i-1}M)$ for $1\leq i\leq r$. Such a sequence is called a *homogeneous regular sequence* or *homogeneous M-sequence*. The length of the longest (homogeneous) M-sequence is called the *depth* of M, denoted depth M. Clearly $0\leq$depth $M\leq$ dim M. If depth $M=$dim M (i.e., if some h.s.o.p. for M is an M-sequence), then we call M a *Cohen-Macaulay* R-module. From Lemma 7 we deduce the following "combinatorial" characterization of M-sequences.

18. THEOREM. Let $\theta_1, \ldots, \theta_r\in \mathbf{H}(R_+)$, say deg $\theta_i=a_i>0$. Let $N=M/(\theta_1 M+\ldots+\theta_r M)$. Then $\theta_1, \ldots, \theta_r$ is an M-sequence if and only if

$$F(M,\lambda)=F(N,\lambda)\prod_{i=1}^{r}(1-\lambda^{a_i})^{-1}. \tag{5}$$

If M is Cohen-Macaulay and $\theta_1, \ldots, \theta_d$ is a maximal

homogeneous M-sequence, then $N=M/(\theta_1 M+\ldots+\theta_d M)$ is a finite-dimensional vector space over k. If (the images of) $\eta_1, \ldots, \eta_t \in \mathbf{H}(M)$ form a k-basis for N, then every $u \in M$ can be written uniquely in the form

$$u=\sum_{i=1}^{t} \eta_i p_i(\theta_1, \ldots, \theta_d),$$

where $p_i \in k[x_1, \ldots, x_d]$. In other words, M is a finitely-generated *free* module over $k[\theta_1, \ldots, \theta_d]$, with basis $\eta_1, \ldots, \eta_t$. Moreover, if $\deg \theta_i=a_i$ and $\deg \eta_i=b_i$, then

$$F(M,\lambda)=\left(\sum_{1}^{t} \lambda^{b_i}\right) \prod_{1}^{d}(1-\lambda^{a_i})^{-1}$$

We should also mention two "uniqueness" theorems concerning maximal M-sequences.

19. THEOREM. (a) Any two maximal M-sequences have the same length; (b) If M is Cohen-Macaulay, then every h.s.o.p. is an M-sequence.

20. EXAMPLE. Let $R=k[x,y]/(x^2,xy)$, with the standard grading. If $|k|=\infty$ then by Theorem 19 there is an h.s.o.p. for R of degree one. Alternatively, it can be easily seen that for any k, the element y forms an h.s.o.p. for R. Now

$$H(R,\lambda)=\frac{1}{1-\lambda}+\lambda=\frac{1+\lambda-\lambda^2}{1-\lambda}.$$

If R were Cohen-Macaulay, then $1+\lambda-\lambda^2=F(R/\theta R,\lambda)$ for any h.s.o.p. θ of degree one (since by Theorem 19 all h.s.o.p.'s are R-sequences). Clearly $H(R/\theta R,2)=-1$ is absurd, so we conclude that R is not Cohen-Macaulay. Although it sometimes is possible to show a ring or module is *not* Cohen-Macaulay by looking at its Hilbert series, in general one cannot deduce Cohen-Macaulayness from the Hilbert series alone. For instance, Exercise 14 gives two rings with the same Hilbert series, one Cohen-Macaulay and one not.

It often is an interesting combinatorial problem to find explicitly the decomposition

$$M=\coprod_{i=1}^{t} \eta_i k[\theta_1, \ldots, \theta_d]$$

of a Cohen-Macaulay module M, where $\theta_1, \ldots, \theta_d$ is an h.s.o.p. and $\eta_1, \ldots, \eta_t$ a k-basis for $M/(\theta_1 M+\ldots+\theta_d M)$. For instance, let $R=k[x_1, \ldots, x_n]$, with $\deg x_i=1$. R is clearly Cohen-Macaulay since $x_1, \ldots, x_n$ is an h.s.o.p. and an R-sequence. Now let θ_i be the i-th

elementary symmetric function in $x_1, \ldots, x_n$. It is not hard to see that $\theta_1, \ldots, \theta_n$ is an h.s.o.p. for R, so by Theorem 19 they form an R-sequence. Hence

$$R = \coprod_{i=1}^{t} \eta_i k[\theta_1, \ldots, \theta_n]$$

for certain $\eta_i \in \mathbf{H}(R)$. Since $\deg \theta_i = i$, we have

$$\sum_{i=1}^{t} \lambda^{\deg \eta_i} = \frac{(1-\lambda)(1-\lambda^2)\ldots(1-\lambda^n)}{(1-\lambda)^n}$$

$$= (1+\lambda)(1+\lambda+\lambda^2)\ldots(1+\lambda+\lambda^2+\cdots+\lambda^{n-1}). \quad (6)$$

Garsia [2, §6] has shown that for each permutation $\pi = a_1 a_2 \ldots a_n$ in the symmetric group S_n of all permutations of $\{1, \ldots, n\}$, if we define

$$\eta_\pi = \sum_{a_j > a_{j+1}} x_{a_1} x_{a_2} \ldots x_{a_j}$$

then $\{\eta_\pi : \pi \in S_n\}$ is indeed a k-basis for $R/(\theta_1, \ldots, \theta_n)$. In particular, we see from (5) that

$$\sum_{\pi \in S_n} \lambda^{\iota(\pi)} = (1+\lambda)(1+\lambda+\lambda^2)\ldots(1+\lambda+\ldots+\lambda^{n-1}) \quad (7)$$

where $\iota(\pi) = \sum_{a_j > a_{j+1}} j$ is the *major index* or *greater index* of π. Equation (7) is a well-known result of MacMahon [8, §104] [13, p.97], so here we have an algebraic elaboration. It would be very interesting to extend the result of Garsia to arbitrary permutation groups. Specifically, if G is a group of permutations of $\{1, \ldots, n\}$ and $R = k[x_1, \ldots, x_n]$, then define

$$R^G = \{f \in R : f(x_{\pi(1)}, \ldots, x_{\pi(n)}) = f(x_1, \ldots, x_n) \text{ for all } \pi \in G\}.$$

The elementary symmetric functions $\theta_1, \ldots, \theta_n$ still form an h.s.o.p. for R^G, and R^G is known to be Cohen-Macaulay (e.g., [18, Thm.3.2]). The problem of finding a k-basis for $R^G/(\theta_1, \ldots, \theta_n)$ may be regarded as a subtle elaboration of Polya's enumeration theorem. The result of Garsia concerns the case when G is the trivial group of order one. Some interesting additional cases appear in [3].

Suppose M is a $\mathbb{Z}$-graded Cohen-Macaulay R-module, with $\theta_1, \ldots, \theta_d$ an h.s.o.p. For any $\mathbb{Z}$-graded R-module N, the *socle* of N is defined by

$$\operatorname{soc} N=\{u\in N:\ uR_+=0\}$$

It is a finite-dimensional vector space. Now define

$$\text{type } M=dim_k \operatorname{soc}\left(M/(\theta_1 M+\ldots+\theta_d M)\right)$$

It can be shown (using homological algebra) that type M is independent of the choice of $\theta_1, \ldots, \theta_d$.

21. OPEN PROBLEM. Find an elementary proof of this last statement.

In the case $M=R$, we say that R is *Gorenstein* if type $R=1$. Suppose R is Gorenstein and let $S=R/(\theta_1, \ldots, \theta_d)$ for some h.s.o.p. $\theta_1, \ldots, \theta_d$. Then the grading of S looks like

$$S=S_0+S_1+\ldots+S_s,$$

where $S_s\neq 0$, for some $s\geq 0$. Since $S_s\subset \operatorname{soc} S$ and type $R=1$, we have $dim_k S_s=1$. The map $\phi_i: S_i\times S_{s-i}\to S_s$ defined by ring multiplication is easily seen to be a perfect pairing of S_i and S_{s-i} (since soc $R=S_s$), which means in particular $dim_k S_i=dim_k S_{s-i}$. It follows from (5) that if $a_i=deg\,\theta_i$ and

$$F(R,\lambda)=\frac{h_0+h_1\lambda+\ldots+h_s\lambda^s}{\Pi(1-\lambda^{a_i})} \tag{8}$$

then $h_i=h_{s-i}$.

22. EXERCISE. Show that the condition $h_i=h_{s-i}$ is not sufficient for a Cohen-Macaulay $\mathbb{N}$-graded algebra R to be Gorenstein, by considering the example $R=k[x,y]/(x^3,xy,y^2)$, with the standard grading.

In view of the above exercise, it is somewhat surprising that if R is a Cohen-Macaulay *domain* in (8), then $h_i=h_{s-i}$ is necessary and sufficient for R to be Gorenstein [17, Thm. 4.4]. This can be a useful combinatorial tool for showing rings are Gorenstein.

The symmetry $h_i=h_{s-i}$ of Gorenstein algebras is a manifestation of a deeper duality valid for any Cohen-Macaulay M (or, with somewhat more work, even non-Cohen-Macaulay M). Namely, if M is Cohen-Macaulay with h.s.o.p. $\theta_1, \ldots, \theta_d$ then let $S=k[\theta_1, \ldots, \theta_d]\subset R$ and define

$$\Omega(M)=Hom_S(M,S),$$

the set of S-module homomorphisms $\phi: M\to S$. We can give $\Omega(M)$ the structure of an R-module by defining $(x\phi)(u)=\phi(xu)$, for $x\in R$, $\phi\in\Omega(M)$, $u\in M$. Using homological algebra it can be shown that

$\Omega(M)$, as an R-module, is independent of $\theta_1, \ldots, \theta_d$. We call $\Omega(M)$ the *canonical module* of M. The minimum number of generators of $\Omega(M)$ is type M, and (when $M=R$) $\Omega(R)\cong R$ if and only if R is Gorenstein. There is a natural grading on $\Omega(M)$ so that

$$F(\Omega(M),\lambda)=(-1)^d F(M,1/\lambda) \text{ (as rational functions).}$$

$\Omega(M)$ is a kind of "dual" object to M, and when M has combinatorial significance we would expect $\Omega(M)$ to have some sort of "dual" significance. For instance, let $R=k\Lambda$ be the monoid algebra of the monoid Λ of (1). Assume without loss of generality that $\Lambda\cap\mathbb{P}^s\neq\emptyset$. Hochster [5] has shown that R is Cohen-Macaulay. The canonical module $\Omega(R)$ can be shown [17, Thm. 6.7] to be isomorphic to the ideal I of R spanned be all monomials x^α with $\alpha\in\Lambda\cap\mathbb{P}^s$. In particular, R is Gorenstein if the vector $\omega=(1,1,\ldots,1)\in\Lambda$, since then as R-modules we have $I\cong x^\omega R\cong R$. If we apply this observation to the polynomial $H_n(i)$ of Application 10, then (with the use of some standard properties of rational generating function [17, Cor. 4.6]) we obtain that

$$H_n(-1)=H_n(-2)=\ldots=H_n(-n+1)=0,$$
$$H_n(i)=(-1)^{n-1}H_n(-n-i).$$

Let us turn to the problem of obtaining restrictions on the Hilbert functions of various classes of graded modules. We will here concern ourselves only with the case of standard graded algebras. If such an algebra R is generated by elements $x_1, \ldots, x_r$ of degree one, then R has a k-basis B consisting of monomials in the x_i's, and $H(R,n)$ is equal to the number of monomials in B of degree n. Now choose B as follows: Define a linear ordering on the set $\mathbf{M}$ of all monomials in $x_1,\ldots,x_n$ by the rules: (a) $y_i<y_j$ if deg $y_i<$ degy_j, and (b) $y_i<y_j$ if deg $y_i=$ deg y_j and y_i precedes y_j in reverse lexicographic order (with respect to the order $x_1<\ldots<x_r$ of the x_i's). E.g., if $r=3$ and we set $x=x_1$, $y=x_2$, $z=x_3$, then the ordering begins

$$1<x<y<z<x^2<xy<y^2<xz<yz<z^2$$
$$<x^3<x^2y<xy^2<y^3<x^2z<\ldots.$$

Now choose the elements $y_1,y_2,y_3,\ldots$ by letting y_{i+1} be the least monomial which is linearly independent from $y_1,\ldots,y_i$. The basis B obtained in this way is readily seen to be an *order ideal of monomials*, i.e., if $x_1^{a_1}\ldots x_r^{a_r}\in B$ and $0\leq b_i\leq a_i$, then $x_1^{b_1}\ldots x_r^{b_r}\in B$. Conversely, if B is any order ideal of monomials and $B'=\mathbf{M}-B$, then B is a k-basis for $k[x_1,\ldots,x_r]/(B')$, where (B') denotes the ideal generated by B'.

A theorem essentially proved by Macaulay and generalized by Clements and Lindström (see [4]) characterizes the possible vectors $(h_0,h_1,\dots)$ for which h_i is the number of monomials of degree i in an order ideal B of monomials. It follows that this same condition characterizes the Hilbert functions of standard graded algebras. The condition of Macaulay is most succinctly (but certainly not least obscurely) stated as follows: Given integers $h,i>0$, write (uniquely)

$$h=\binom{n_i}{i}+\binom{n_{i-1}}{i-1}+\cdots+\binom{n_j}{j},$$

where $n_i>n_{i-1}>\cdots>n_j\geq j\geq 1$, and define

$$h^{<i>}=\binom{n_i+1}{i+1}+\binom{n_{i-1}+1}{i}+\cdots+\binom{n_j+1}{j+1}.$$

Also set $0^{<i>}=0$. We then have:

23. THEOREM. Let k be any field. The following two conditions are equivalent on a sequence $(h_0,h_1,\dots)$ of integers:

(i) There exists a standard graded k-algebra R satisfying $H(R,n)=h_n$ for all $n\geq 0$.

(ii) $h_0=1$ and $0\leq h_{n+1}\leq h_n^{<n>}$ for all $n\geq 1$.

Let us call a sequence $(h_0,h_1,\dots)$ (finite or infinite) an *M-vector* (after Macaulay) if it satisfies either of the above two (equivalent) conditions. We now have from Theorems 17 and 18 (leaving aside a minor technicality arising when k is finite):

24. COROLLARY. Let k be any field, let $d\geq 0$, and let $H\colon \mathbb{N}\to\mathbb{N}$. The following two conditions are equivalent:

(i) There exists a standard Cohen-Macaulay graded k-algebra of Krull dimension d with Hilbert function H.

(ii) For some $s\geq 0$ we have

$$\sum_{n\geq 0}H(n)\lambda^n=\frac{h_0+h_1\lambda+\dots+h_s\lambda^s}{(1-\lambda)^d}$$

where $(h_0,h_1,\dots h_s)$ is an M-vector.

25. OPEN PROBLEM. Find a "nice" characterization of the Hilbert function of a standard Gorenstein graded k-algebra. See [17, §4] for further information.

The above problem can be reformulated as a problem in linear algebra. Let M_i denote the set of all monomials of degree i in the variables $x_1,\dots,x_m$. Fix an integer $s\geq 0$ and a nonzero function $\sigma\colon M_s\to k$.

For $0 \le j \le s$ let $A^{(j)}$ be the matrix with rows indexed by M_j and columns by M_{s-j}, defined by $A^{(j)}_{uv} = \sigma(uv)$. Let $h_j = rank\ A_j$. Then for any $d \ge 0$ there is a standard graded Gorenstein k-algebra R of dimension d satisfying

$$F(R,\lambda) = (h_0 + h_1\lambda + \ldots + h_s\lambda^s)(1-\lambda)^{-d}.$$

Conversely, the Hilbert series of every standard graded Gorenstein k-algebra arises in this way. For instance, suppose $s=4$ and σ is chosen so $h_1 = rank\ A^{(1)} = m$. How small can $h_2 = rank\ A^{(2)}$ be? Letting $f(m) = min\ h_2$, it is known that $f(m) = m$ for $m \le 5$, $f(13) < 13$ and

$$\frac{1}{2} \cdot 6^{2/3} \le \liminf_{m\to\infty} f(m)m^{-2/3} \le \limsup_{m\to\infty} f(m)m^{-2/3} \le 6^{2/3}.$$

Does $f(6) = 6$? Does $\lim f(m)m^{-2/3}$ exist, and if so, then what is this limit?

Among the many applications of Corollary 24, we mention here only its connection with simplicial complexes. By a *simplicial complex* on the vertex set V, we mean a collection Δ of subsets of V satisfying (i) $\{x\} \in \Delta$ for all $x \in V$, and (ii) if $F \in \Delta$ and $G \subset F$, then $G \in \Delta$. An element F of Δ is called a *face*, and the integer $|F| - 1$ is called the *dimension* of F, denoted *dim* F. The dimension of Δ is defined by

$$dim\,\Delta = \max\{dim\ F\colon F \in \Delta\}.$$

Let $d = 1 + dim\ \Delta$ throughout this discussion. Let $f_i = f_i(\Delta)$ be the number of i-dimensional faces of Δ and call the vector $f = f(\Delta) = (f_0, f_1, \ldots, f_{d-1})$ the *f-vector* of Δ. Set $n = f_0 = |V|$. It is an interesting problem to obtain as much information as possible about the f-vector of various classes of simplicial complexes. For instance, a celebrated theorem of Kruskal and Katona (see [4] for a nice discussion) can be used to completely characterize the f-vector of an arbitrary simplicial complex.

To proceed further, let $|\Delta|$ denote the geometric realization (e.g., [12, pp. 110-111]) of Δ - it is a topological space obtained, intuitively speaking, by regarding the faces of Δ as vertices of actual Euclidean simplices and sticking these simplices together appropriately. If now $|\Delta|$ is a $(d-1)$-dimensional sphere S^{d-1}, then Motzkin and Klee raised the question of maximizing $f_i(\Delta)$ when $n = f_0$ and $d = 1 + dim\ \Delta$ are fixed. (Motzkin was concerned only with the more restrictive class of simplicial convex polytopes, and Klee realized Motzkin's conjecture could be made just as easily for spheres.) See [16] for references. They conjectured that a certain known simplicial complex $\Delta(n,d)$ (the boundary complex of a cyclic polytope $C(n,d)$) achieved the maximum. McMullen proved Motzkin's original

conjecture (for simplicial polytopes), but the case of spheres remained open.

The key step in proving this "Upper Bound Conjecture for spheres" (UBC) is to associate a certain graded algebra R_Δ with any simplicial complex Δ. Let $A=k[x_1,\ldots,x_n]$ be the polynomial ring in the vertices $V=\{x_1,\ldots,x_n\}$ (with deg $x_i=1$), and define I_Δ to be the ideal of A generated by all squarefree monomials $x_{i_1}x_{i_2}\cdots x_{i_j}$ for which $\{x_{i_1},\ldots,x_{i_j}\}\notin\Delta$. If $f(\Delta)=(f_0,\ldots,f_{d-1})$ then the Hilbert function of R_Δ is easily seen to be

$$H(R_\Delta,m)=\begin{cases}1, m=0\\ \sum_{i=0}^{d-1} f_i\binom{m-1}{i}, m>0\end{cases}.$$

In particular (see Corollary 9), dim $R_\Delta=d=1+dim\ \Delta$.

Since $H(R_\Delta,m)$ is a polynomial of degree $d-1$ for $m>0$, it follows that there exist integers $h_0,h_1,\ldots,h_d$ such that

$$\sum_{m\geq 0} H(R_\Delta,m)\lambda^m=(h_0+h_1\lambda+\ldots+h_d\lambda^d)(1-\lambda)^{-d}.$$

The vector $h(\Delta)=(h_0,h_1,\ldots,h_d)$ is called the *h-vector* of Δ. In McMullen's proof of the UBC for polytopes, he showed essentially that if $|\Delta|$ was a sphere then the UBC for Δ followed from the inequality $h_i\leq\binom{n-d+i-1}{i}$, $0\leq i\leq d$.

26. PROPOSITION. Let $|\Delta|=S^{d-1}$, with $f_0(\Delta)=n$. If R_Δ is Cohen-Macaulay, then the UBC holds for Δ.

PROOF. If R_Δ is Cohen-Macaulay, then by Corollary 24 $h(\Delta)$ is an M-vector, so there is an order ideal B of monomials for which $h_i=card\{y\in B: deg\ y=i\}$. Since $h_1=n-d$, this means that h_i cannot exceed the total number $\binom{n-d+i-1}{i}$ of monomials of degree i in $n-d$ variables, and the proof follows. □

To complete the proof of the UBC for spheres, it remains to show that R_Δ is Cohen-Macaulay whenever $|\Delta|$ is a sphere. A stronger result was proved by Reisner [10] using homological methods; he characterized all simplicial complexes Δ for which R_Δ is Cohen-Macaulay in terms of the homology groups of various subcomplexes of Δ. Although several other proofs of Reisner's theorem have since been found, none are really simple. Hochster [6] in fact has shown

that if $|\Delta|$ is a sphere then R_Δ is Gorenstein. In particular, we have $h_i = h_{d-i}$, which is equivalent to the Dehn-Sommerville equations (e.g., [9, p.171, eqn. (6)]).

An outstanding open problem in this area is to characterize completely the possible f-vectors (or h-vectors) of spheres. For simplicial polytopes this was done using deep results from algebraic geometry in addition to Reisner's theorem [19], but it remains open whether this characterization is valid for all spheres.

We have only given the briefest glimpse in these notes of the many fascinating connections between commutative algebra and combinatorics. In particular, we have omitted all reference to homological concepts, including the fundamental Hilbert syzygy theorem. Nevertheless, it is hoped that we have managed to convey some of the flavor of the subject and to make it more accessible to combinatorialists.

References

[1] K. Baclawski and A.M. Garsia, Combinatorial decompositions of a class of rings, Advances in Math. 39 (1981), 155-184.

[2] A.M. Garsia, Combinatorial methods in the theory of Cohen-Macaulay rings, Advances in Math. 38 (1980), 229-266.

[3] A.M. Garsia and D. Stanton, Group actions on Stanley-Reisner rings and invariants of permutation groups, Advances in Math. (to appear).

[4] C. Greene and D.J. Kleitman, Proof techniques in the theory of finite sets, in *Studies in Combinatorics* (G.-C. Rota, ed.), Math. Assoc. of America, Washington, D.C., 1978, pp. 22-79.

[5] M. Hochster, Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes, Ann. of Math. 96 (1972), 319-327.

[6] M. Hochster, Cohen-Macaulay rings, combinatorics, and simplicial complexes, in *Ring Theory and Algebra II* (B.R. McDonald, ed.), Dekker, New York and Basel 1977, pp. 171-223.

[7] I. Kaplansky, *Commutative Rings*, Univ. of Chicago Press, Chicago, 1974.

[8] P.A. MacMahon, Combinatory Analysis, vols. 1-2, Cambridge Univ. Press, London, 1915, 1916; reprinted by Chelsea, New York, 1960.

[9] P. McMullen and G.C. Shephard, *Convex Polytopes and the Upper Bound Conjecture*, London Math. Soc. Lecture Note Series, vol. 3, Cambridge Univ. Press, London/New York, 1971.

[10] G. Reisner, Cohen-Macaulay quotients of polynomial rings, Advances in Math. 21 (1976), 30-49.

[11] H.J. Ryser, *Combinatorial Mathematics*, Carus Math. Monograph no. 14, Math. Assoc. of America, Washington, D.C., 1963.

[12] E.H. Spanier, *Algebraic Topology*, McGraw-Hill, New York, 1966.

[13] R.P. Stanley, Ordered structures and partitions, Memoirs of the Amer. Math. Soc., no. 119, 1972.

[14] R.P. Stanley, Linear homogeneous diophantine equations and magic labelings of graphs, Duke Math. J. 40 (1973), 607-632.

[15] R.P. Stanley, Generating functions, in *Studies in Combinatorics* (G.-C. Rota, ed.), Math. Assoc. of America, Washington, D.C., 1978, pp. 100-141.

[16] R.P. Stanley, The Upper Bound Conjecture and Cohen-Macaulay rings, Studies in Applied Math. 54 (1975), 135-142.

[17] R.P. Stanley, Hilbert functions of graded algebras, Advances in Math. 28 (1978), 57-83.

[18] R.P. Stanley, Invariants of finite groups and their applications to combinatorics, Bull. Amer. Math. Soc. (new series) 1 (1979), 475-511.

[19] R.P. Stanley, The number of faces of a simplicial convex polytope, Advances in Math. 35 (1980), 236-238.