ADVANCES IN MATHEMATICS 28, 57–83 (1978)

Hilbert Functions of Graded Algebras*

RICHARD P. STANLEY

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

1. INTRODUCTION

Let R be a Noetherian commutative ring with identity, graded by the nonnegative integers $\mathbb{N}$. Thus the additive group of R has a direct-sum decomposition $R = R_0 + R_1 + \cdots$, where $R_i R_j \subset R_{i+j}$ and $1 \in R_0$. If in addition R_0 is a field k, so that R is a k-algebra, we will say that R is a *G-algebra*. The assumption that R is Noetherian implies that a G-algebra is finitely generated (as an algebra over k) and that each R_n is a finite-dimensional vector space over k. The *Hilbert function* of R is defined by

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

Thus in particular $H(R, 0) = 1$. Our object will be to see what kind of conditions the structure of R imposes on the Hilbert function H, and conversely what we can deduce about R from knowledge of H. Although much of what we say can be extended to more general rings, for simplicity we will restrict ourselves to G-algebras as defined above.

This paper is partially expository in nature. Many results about Hilbert functions have been previously obtained, though frequently they have been stated in an obscure or cumbersome fashion. The most striking of these results are due to F. S. Macaulay. Our primary new results are Theorem 4.4 and its applications. We show that if a G-algebra R is a Cohen–Macaulay integral domain, then the question of whether or not R is Gorenstein is completely determined by the Hilbert function of R. This allows us to determine when rings arising in certain ways are Gorenstein, e.g., the ring of invariants of a finite group or of a torus acting in the usual way on a polynomial ring over a field of characteristic zero.

The following notation and terminology will be fixed throughout this paper. Let R be a G-algebra. An element x of R is said to be *homogeneous* if $x \in R_n$ for some $n \geqslant 0$, and we write $\deg x = n$. In particular, $\deg 0$ is arbitrary. Since R is finitely generated and graded, there exists a finite set of homogeneous generators for R. Fix such a set $y_1, y_2, \ldots, y_s$. We can assume that no $y_i \in R_0$,

* Supported in part by NSF Grant P36739.

0001-8408/78/0281-0057$05.00/0

so $\deg y_i = e_i \geqslant 1$. Let $A = k[Y_1, \ldots, Y_s]$ be a polynomial ring over k in s independent variables $Y_1, \ldots, Y_s$. If we define $\deg Y_i = e_i$, then A has the structure $A = A_0 + A_1 + \cdots$ of a G-algebra, with $Y_i \in A_{e_i}$. There is a canonical surjection $A \xrightarrow{p} R$ defined by $p(Y_i) = y_i$. Moreover, p is *degree preserving*, i.e., $p(A_n) \subset R_n$. Define the *Poincaré series* $F(R, \lambda)$ of R to be the formal power series

$$F(R, \lambda) = \sum_{n=0}^{\infty} H(R, n)\lambda^n \in \mathbb{Z}[[\lambda]].$$

This power series is not to be confused with the power series $\sum_{n=0}^{\infty} [\dim_k \operatorname{Tor}_n^R(k, k)]\lambda^n$, which is sometimes also called the Poincaré series of R and which has (almost) no connection with $F(R, \lambda)$. It is a consequence of the Hilbert syzygy theorem (which implies that R has a finite free resolution as an A-module) or otherwise (e.g., [1, Theorem 11.1] or [26, Theorem 4.2]) that we can write $F(R, \lambda)$ in the form

$$F(R, \lambda) = \frac{P(R, \lambda)}{\prod_{i=1}^{s} (1 - \lambda^{e_i})}, \tag{1}$$

where $P(R, \lambda)$ is a *polynomial* in λ with integer coefficients, i.e., $P(R, \lambda) \in \mathbb{Z}[\lambda]$. Moreover, if d denotes the Krull dimension of R, then d is the order to which $\lambda = 1$ is a pole of $F(R, \lambda)$. Thus d is the unique integer for which $\lim_{\lambda \to 1}(1 - \lambda)^d F(R, \lambda)$ is a nonzero, noninfinite complex number. (In evaluating this limit, and in similar instances throughout this paper, we are regarding $F(R, \lambda)$ as a rational function of λ.) A proof is essentially given in [1, Chap. 11] or [26, Theorem 5.5]. Thus $H(R, n)$ uniquely determines $d = \dim R$. This is a simple instance of the interplay between the structure of R and the behavior of $H(R, n)$. A special case of obvious interest is when each $e_i = 1$, so that A has its "usual" grading. In this case $H(R, n)$ is a polynomial for n sufficiently large (the *Hilbert polynomial* of R), and the degree of this polynomial is $d - 1$. If one can choose each $e_i = 1$ (i.e., if R is generated as a k-algebra by R_1), then we will call R a *standard G-algebra*. If R is standard, we assume that each y_i has been chosen to be in R_1, so that each $e_i = 1$.

Given a standard G-algebra R, we frequently will need to choose a system of parameters of R, or a maximal homogeneous R-sequence, consisting of homogeneous elements of degree one. This can always be done if k is infinite. If k is finite, we will always be able to reduce our arguments to the case where k is infinite by use of the next result. The proof is routine and essentially well known, and will be omitted.

1.1. LEMMA. *Let R be a G-algebra with $R_0 = k$, and let K be an extension field of k. Let $Q = R \otimes_k K$, so that Q is a G-algebra over K in an obvious way. Then*:

(i) $\dim R = \dim Q$;

(ii) depth R = depth Q, *where the* depth *of a G-algebra S is the length of the longest* homogeneous *regular sequence contained in S. (See Section 3 for a discussion of regular sequences.)*

(iii) *R is Cohen–Macaulay if and only if Q is Cohen–Macaulay (this follows from* (i) *and* (ii) *since a G-algebra S is Cohen–Macaulay if and only if* $\dim S$ = depth S).

(iv) *R is Gorenstein if and only if Q is Gorenstein.*

(v) *R is a complete intersection if and only if Q is a complete intersection.*

(vi) *R is a hypersurface if and only if Q is a hypersurface.*

(vii) *R and Q have the same Hilbert function, i.e., $H(R, n) = H(Q, n)$ for all $n \in \mathbb{N}$.* ∎

2. Hilbert Functions and Order Ideals of Monomials

In this section we consider what can be said about the Hilbert function of an arbitrary G-algebra (as defined in the previous section). To this end, let $Y_1, \ldots, Y_s$ be indeterminates. A nonvoid set M of monomials $Y_1^{a_1} \cdots Y_s^{a_s}$ in the variables $Y_1, \ldots, Y_s$ is said to be an *order ideal of monomials* if, whenever $m \in M$ and m' divides m, then $m' \in M$. Equivalently, if $Y_1^{a_1} \cdots Y_s^{a_s} \in M$ and $0 \leqslant b_i \leqslant a_i$, then $Y_1^{b_1} \cdots Y_s^{b_s} \in M$. In particular, since M is assumed nonvoid, $1 \in M$.

Recall the notation of Section 1 (which we will be using throughout this paper): R is a G-algebra with homogeneous generators $y_1, y_2, \ldots, y_s$, and we have a surjection $A = k[Y_1, \ldots, Y_s] \xrightarrow{p} R$ given by $p(Y_i) = y_i$. The following result is essentially due to Macaulay [19].

2.1. Theorem. *There exists an order ideal M of monomials in the variables $Y_1, \ldots, Y_s$, such that the elements $p(m)$, $m \in M$, form a k-basis for R.*

Proof. Let Φ denote the set of all monomials in the variables $Y_1, \ldots, Y_s$. Define a linear ordering of the elements of Φ as follows. If $u = Y_1^{a_1} \cdots Y_s^{a_s}$ and $v = Y_1^{b_1} \cdots Y_s^{b_s}$, then $u < v$ if either (1) $\sum a_i < \sum b_i$, or (2) $\sum a_i = \sum b_i$ and for some j satisfying $1 \leqslant j \leqslant s$, we have $a_s = b_s$, $a_{s-1} = b_{s-1}, \ldots, a_{j+1} = b_{j+1}$, and $a_j < b_j$. (This is just "reverse lexicographic order.")

It is easy to see that $(\Phi, <)$ forms an ordered semigroup (under multiplication). In particular,

$$u < v \Rightarrow uw < vw \qquad \text{for all } w \in \Phi. \tag{2}$$

Now define a sequence $u_1, u_2, \ldots$ (possibly finite or infinite) of elements of Φ as follows. First, $u_1 = 1$. Once $u_1, u_2, \ldots, u_i$ have been defined, let u_{i+1}

be the least element of Φ (in the linear ordering we have just defined) so that $p(u_1), p(u_2),\ldots, p(u_{i+1})$ are linearly independent (over k) in R. If u_{i+1} does not exist, the sequence terminates with u_i.

Let $M = \{u_1, u_2, \ldots\}$. We claim that M is the desired order ideal of monomials. Clearly $p(u_1), p(u_2),\ldots$ is a basis for R, so we have only to show M is an order ideal. Suppose not. Then for some $u, v \in \Phi$ we have $u \in M$, $v \mid u$, $v \notin M$. Since $v \notin M$, we have a linear dependence relation

$$p(v) = \sum \alpha_i p(u_i), \tag{3}$$

where $u_i \in \Phi$, $u_i < v$, and $\alpha_i \in k$. Let $u = vw$. Multiplying (3) by $p(w)$, we obtain $p(u) = \sum \alpha_i p(u_i w)$. By (2), each $u_i w < u = vw$. This contradicts the fact that $u \in M$ and completes the proof. ∎

From Theorem 2.1 we deduce the following result. Given positive integers $e_1, \ldots, e_s$, a function $H: \mathbb{N} \to \mathbb{N}$ is the Hilbert function of some G-algebra generated by elements of degrees $e_1, \ldots, e_s$ if and only if there is an order ideal M of monomials in variables $Y_1, \ldots, Y_s$, where $\deg Y_i = e_i$, such that $H(n) = \operatorname{card}\{u \in M: \deg u = n\}$. This condition is not very edifying since given H, it is by no means apparent whether the desired order ideal M exists. If, however, each $e_i = 1$, it is possible to give an explicit numerical characterization of valid Hilbert functions H. We will merely state this result here. The difficult part of the proof was first obtained by Macaulay [19], with subsequent simplifications and generalizations by Sperner [27], Whipple [39], and Clements and Lindström [5] (see [8, Sect. 8] for a survey of this subject). The explicit numerical form in which we state the result first appeared in [33] and is also considered in [34].

A finite or infinite sequence $(k_0, k_1, \ldots)$ of nonnegative integers is said to be an *O-sequence* if there exists an order ideal M of monomials in variables $Y_1, Y_2, \ldots, Y_s$, with each $\deg Y_i = 1$, such that $k_n = \operatorname{card}\{u \in M: \deg u = n\}$. In particular, $k_0 = 1$. If h and i are positive integers, then h can be written uniquely in the form

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

where $n_i > n_{i-1} > \cdots > n_j \geqslant j \geqslant 1$. Following McMullen [22], define

$$h^{\langle i \rangle} = \binom{n_i + 1}{i + 1} + \binom{n_{i-1} + 1}{i} + \cdots + \binom{n_j + 1}{j + 1}. \tag{4}$$

Also define $0^{\langle i \rangle} = 0$.

2.2. THEOREM. *Let $H: \mathbb{N} \to \mathbb{N}$ and let k be any field. The following four conditions are equivalent.*

(i) *There exists a standard G-algebra R with* $R_0 = k$ *and with Hilbert function H.*

(ii) $(H(0), H(1), H(2),...)$ *is an O-sequence.*

(iii) $H(0) = 1$ *and for all* $n \geqslant 1$, $H(n+1) \leqslant H(n)^{\langle n \rangle}$.

(iv) *Let* $s = H(1)$, *and for each* $n \geqslant 0$, *let* M_n *be the first (in the linear ordering defined above)* $H(n)$ *monomials of degree n in the variables* $Y_1, ..., Y_s$. *Define* $M = \bigcup_{n \geqslant 0} M_n$. *Then M is an order ideal of monomials.* ∎

Remark. The implication (i) ⇒ (ii) in Theorem 2.2 follows from Theorem 2.1. The implication (ii) ⇒ (i) is easy: given an O-sequence $(H(0), H(1),...)$, let M be an order ideal of monomials in the variables $Y_1, Y_2, ..., Y_s$, with each $\deg Y_i = 1$, such that $H(n) = \text{card}\{u \in M: \deg u = n\}$. Let I be the ideal of $A = k[Y_1, ..., Y_s]$ generated by all monomials not in M. Then $R = A/I$ is a standard G-algebra with $R_0 = k$ and with Hilbert function H. The equivalence of (iii) and (iv) is a simple counting argument; while the implication (iv) ⇒ (ii) is trivial. The difficult part of Theorem 2.2 is the implication (ii) ⇒ (iv). As mentioned above, we are referring the reader to the literature for the proof that (ii) ⇒ (iv).

To clarify Theorem 2.2, we present a few examples.

(a) Let us use condition (iv) to check whether (1, 3, 4, 5, 7) is an O-sequence. Writing $x = Y_1$, $y = Y_2$, $z = Y_3$, we have $M_0 = \{1\}$, $M_1 = \{x, y, z\}$, $M_2 = \{x^2, xy, y^2, xz\}$, $M_3 = \{x^3, x^2y, xy^2, y^3, x^2z\}$, $M_4 = \{x^4, x^3y, x^2y^2, xy^3, y^4, x^3z, x^2yz\}$. Now xyz divides an element of M_4 but $xyz \notin M_3$. Hence (1, 3, 4, 5, 7) is not an O-sequence. It follows that a standard G-algebra cannot have a Hilbert function H satisfying $H(3) = 5$ and $H(4) = 7$.

(b) We have $152 = \binom{9}{5} + \binom{6}{4} + \binom{5}{3} + \binom{2}{2}$. Hence $152^{\langle 5 \rangle} = \binom{10}{6} + \binom{7}{5} + \binom{6}{4} + \binom{3}{3} = 247$. It follows from Theorem 2.2 that if R is a standard G-algebra with $H(R, 5) = 152$, then $H(R, 6) \leqslant 247$, and this result is best possible.

(c) As a somewhat more general application of Theorem 2.2, we remark that the following result is a simple consequence of the equivalence of (i) and (iii) (or of (i) and (iv)). Suppose R is a standard G-algebra and that for some $m \geqslant 1$, we have $H(m) \leqslant m$. It then follows that $H(n) \geqslant H(n+1)$ for all $n \geqslant m$.

3. *R*-Sequences

Recall that a sequence $\theta_1, \theta_2, ..., \theta_r$ of elements of a Noetherian ring R is a ***regular sequence*** or an ***R-sequence*** if $(\theta_1, \theta_2, ..., \theta_r)R \neq R$ and if θ_i is not a zero-divisor modulo $(\theta_1, ..., \theta_{i-1})$ for $i = 1, 2, ..., r$. If R is a G-algebra, we say that an R-sequence $\theta_1, \theta_2, ..., \theta_r$ is ***homogeneous*** if each θ_i is homogeneous. If $\theta_1, ..., \theta_r$ are homogeneous elements of a G-algebra, the condition

$(\theta_1, \theta_2, \ldots, \theta_r)R \neq R$ is equivalent to $\deg \theta_i > 0$ for $i = 1, 2, \ldots, r$. We base our analysis of the relationship between R-sequences and Hilbert functions on the following simple result (Theorem 3.1). First observe that if I is a homogeneous ideal (or subring) of a G-algebra R, then I inherits a grading $I = I_0 + I_1 + I_2 + \cdots$ from R given by $I_n = I \cap R_n$. We can then define $H(I, n) = \dim_k I_n$ and $F(I, \lambda) = \sum_{n=0}^{\infty} H(I, n)\lambda^n$. Similarly the quotient ring R/I inherits a grading from R, and $H(R/I, n)$ and $F(R/I, \lambda)$ are always defined with respect to this "quotient grading."

3.1. THEOREM. *Let R be a G-algebra, and let θ be a homogeneous element of R of degree $f > 0$. Then*

$$F(R, \lambda) = \frac{F(R/(\theta), \lambda) - \lambda^f F(\operatorname{Ann} \theta, \lambda)}{1 - \lambda^f}$$

where $\operatorname{Ann} \theta = \{x \in R: x\theta = 0\}$.

Proof. For $n \geqslant 0$ we have $H((\theta), n + f) = \dim_k(\theta R_n) = \dim_k R_n - \dim_k(R_n \cap \operatorname{Ann} \theta) = H(R, n) - H(\operatorname{Ann} \theta, n)$, so

$$F((\theta), \lambda) = \lambda^f[F(R, \lambda) - F(\operatorname{Ann} \theta, \lambda)]. \tag{5}$$

On the other hand, it is clear that for any homogeneous ideal I of R,

$$F(R, \lambda) = F(I, \lambda) + F(R/I, \lambda). \tag{6}$$

Putting $I = (\theta)$ in (6) and combining with (5), we obtain the desired result. ∎

3.2. COROLLARY. *Let R be a G-algebra. Let $\theta_1, \theta_2, \ldots, \theta_r$ be a sequence of nonzero homogeneous elements of R of positive degree, say* $\deg \theta_i = f_i > 0$. *Let S be the quotient ring $R/(\theta_1, \theta_2, \ldots, \theta_r)$, endowed with the natural "quotient grading." If $\sum_0^\infty a_n\lambda^n$ and $\sum_0^\infty b_n\lambda^n$ are two power series with real coefficients, define $\sum_0^\infty a_n\lambda^n \leqslant \sum_0^\infty b_n\lambda^n$ if $a_n \leqslant b_n$ for all $n \geqslant 0$. Then*

$$F(R, \lambda) \leqslant F(S, \lambda) \Big/ \prod_{i=1}^{r} (1 - \lambda^{f_i}). \tag{7}$$

Equality holds in (7) *if and only if $\theta_1, \ldots, \theta_r$ is an R-sequence.*

Proof. Since $\theta_1, \ldots, \theta_r$ is an R-sequence if and only if θ_1 is a non-zero-divisor in R and $\theta_2, \ldots, \theta_r$ is an $R/(\theta_1)$-sequence, the proof reduces immediately to the case $r = 1$. Thus assume $S = R/(\theta)$ where $\deg \theta = f$. We wish to prove $F(R, \lambda) \leqslant F(S, \lambda)/(1 - \lambda^f)$, with equality if and only if θ is not a zero-divisor in R. But this is immediate from Theorem 3.1, since $\operatorname{Ann} \theta = 0$ if and only if θ is not a zero-divisor. ∎

Note that Corollary 3.2 implies that if $\theta_1, \theta_2, \ldots, \theta_r$ is a homogeneous R-sequence in a G-algebra R, then any permutation of $\theta_1, \theta_2, \ldots, \theta_r$ is also an R-sequence. This is the "graded analog" of the corresponding well-known result for local rings (see, e.g., [16, Theorem 119]).

As an immediate consequence of Corollary 3.2 and the fact that a G-algebra R is Cohen–Macaulay if and only if some (equivalently, every) homogeneous system of parameters is an R-sequence, we obtain the following characterization of Cohen–Macaulay G-algebras: Let R be a G-algebra, let $\theta_1, \ldots, \theta_d$ be a homogeneous system of parameters with $f_i = \deg \theta_i$, and let $S = R/(\theta_1, \ldots, \theta_d)$. Then R is Cohen–Macaulay if and only if

$$F(R, \lambda) = F(S, \lambda) \Big/ \prod_{i=1}^{d} (1 - \lambda^{f_i}).$$

A "direct" proof that equality holds in (7) when $\theta_1, \theta_2, \ldots, \theta_r$ is an R-sequence is as follows. Let B be a set of homogeneous elements of R whose images in $S = R/(\theta_1, \theta_2, \ldots, \theta_r)$ form a k-basis for S. It is easily seen that since $\theta_1, \theta_2, \ldots, \theta_r$ is an R-sequence, R is a free module over the polynomial subring $k[\theta_1, \theta_2, \ldots, \theta_r]$, and that B is a set of free generators for this module. (This is essentially a well-known property of homogeneous R-sequences in G-algebras, though an explicit statement is difficult to find in the literature. For the special case when $\theta_1, \theta_2, \ldots, \theta_r$ is a system of parameters, see [13, p. 1036] or [26, Proposition 6.8].) Hence if M is the set of all monomials in the θ_i's, then a k-basis for R consists of all elements bm, where $b \in B$ and $m \in M$. Therefore

$$\begin{aligned} F(R, \lambda) &= \sum_{b \in B} \sum_{m \in M} \lambda^{\deg bm} \\ &= \Big(\sum_{b \in B} \lambda^{\deg b} \Big) \Big(\sum_{m \in M} \lambda^{\deg m} \Big) \qquad (8) \\ &= F(S, \lambda) \Big/ \prod_{i=1}^{r} (1 - \lambda^{f_i}). \end{aligned}$$

Equation (8) is implicit in the work of Macaulay [18, Sect. 91]. He deals only with standard gradings, and he also assumes that the R-sequence $\theta_1, \theta_2, \ldots, \theta_r$ is a system of parameters all of degree one (so that R is a Cohen–Macaulay ring), but his method of proof easily extends to the more general (8). Some results on local rings similar to Theorem 3.1 and Corollary 3.2 can be found in [2] and [12]. These papers contain a number of interesting results about Hilbert functions of local rings, but we will not discuss them here.

Corollary 3.2 allows us to compute the Poincaré series $F(R, \lambda)$ of a G-algebra R which is a complete intersection. Let y_i, $e_i = \deg y_i$, $A = k[Y_1, \ldots, Y_s]$, and $A \xrightarrow{p} R$ be as in Section 1. Then R is a complete intersection if and only if $\ker p$ is generated by an A-sequence, which can be chosen to be homogeneous.

Since $F(A, \lambda) = 1/\prod_{i=1}^{s}(1 - \lambda^{e_i})$, we obtain as a special case of Corollary 3.2 the following result.

3.3. COROLLARY. *Let k be any field. Let $A = k[Y_1, \ldots, Y_s]$, with* $\deg Y_i = e_i$. *Let $\theta_1, \ldots, \theta_r$ be a homogeneous A-sequence with* $\deg \theta_j = f_j$. *Let R be the complete intersection $R = A/(\theta_1, \ldots, \theta_r)$, with the quotient grading. Then*

$$F(R, \lambda) = \frac{\prod_{j=1}^{r}(1 - \lambda^{f_j})}{\prod_{i=1}^{s}(1 - \lambda^{e_i})}. \quad \blacksquare$$

If A (and therefore R) is standard (i.e., $e_i = 1$) then given any positive integers $f_1, \ldots, f_r$ with $r \leqslant s$, we can find a homogeneous A-sequence $\theta_1, \ldots, \theta_r$ with $\deg \theta_j = f_j$. For instance, take $\theta_j = Y_j^{f_j}$. Hence we obtain a complete characterization of the possible Poincaré series of a standard G-algebra which is a complete intersection.

3.4. COROLLARY. *Let k be any field. A power series $F(\lambda)$ is the Poincaré series of a standard G-algebra R satisfying* (a) $R_0 = k$, (b) $\dim R = d$, *and* (c) *R is a complete intersection, if and only if $F(\lambda)$ has the form*

$$F(\lambda) = \frac{\prod_{i=1}^{t}(1 + \lambda + \lambda^2 + \cdots + \lambda^{g_i})}{(1 - \lambda)^d},$$

where t is any nonnegative integer and $g_1, g_2, \ldots, g_t$ are arbitrary positive integers. $\blacksquare$

Corollary 3.4 is another result essentially given by Macaulay [18, Sect. 58]. Gröbner [9, p. 164] obtains a result equivalent to Corollary 3.4, but his treatment is rather cumbersome since he deals with $H(R, n)$ rather than $F(R, \lambda)$.

It is natural to ask to what extent one can find converses to Corollaries 3.3 and 3.4. More specifically, if a G-algebra R has the Hilbert function of a complete intersection, under what circumstances can we conclude that R actually is a complete intersection? We give two very weak results along these lines, and some examples to show that not much more can be expected.

3.5. THEOREM. *Let R be a G-algebra generated (as an algebra over k) by the nonzero homogeneous elements $y_1, \ldots, y_s$ of positive degrees $e_1, \ldots, e_s$. Then the y_i's are algebraically independent over k if and only if $F(R, \lambda) = 1/\prod_{i=1}^{s}(1 - \lambda^{e_i})$.*

Proof. Since $y_1, \ldots, y_s$ generate R, the set M of monomials in $y_1, \ldots, y_s$ spans R as a vector space over k. Since $\sum_{m \in M} \lambda^{\deg m} = 1/\prod_{i=1}^{s}(1 - \lambda^{e_i})$, it follows that $F(R, \lambda) = 1/\prod_{i=1}^{s}(1 - \lambda^{e_i})$ if and only if the elements of M are linearly independent, i.e., if and only if the y_i's are algebraically independent. $\blacksquare$

3.6. THEOREM. *Let R be a standard Cohen–Macaulay G-algebra. The following conditions are equivalent:*

(i) *For some integer* $f > 0$,

$$F(R, \lambda) = \frac{1 + \lambda + \lambda^2 + \cdots + \lambda^f}{(1 - \lambda)^d}$$

where $d = \dim R$.

(ii) $H(R, 1) = 1 + \dim R$.

(iii) R *is a hypersurface, i.e.,* $R \cong k[Y_1, Y_2, \ldots, Y_{d+1}]/(\theta)$, *for some nonzero homogeneous* $\theta \in k[Y_1, Y_2, \ldots, Y_{d+1}]$ *of degree greater than one.*

Proof. (i) $\Rightarrow$ (ii). Trivial.

(ii) $\Rightarrow$ (iii). By Lemma 1.1, we may assume k is infinite. Thus R possesses a system of parameters $\theta_1, \theta_2, \ldots, \theta_d$ all homogeneous of degree 1 (see, e.g., [1, p. 69, Example 16]), where $d = \dim R$. Since R is Cohen–Macaulay, $\theta_1, \theta_2, \ldots, \theta_d$ is an R-sequence. Let $S = R/(\theta_1, \theta_2, \ldots, \theta_d)$. Since $H(R, 1) = 1 + d$, S is generated as a k-algebra by a single element x. Since $\dim S = 0$ and S is graded, we have $S \cong k[x]/(x^{f+1})$ for some $f \geqslant 0$. Hence S is a hypersurface, and it follows that R is also a hypersurface.

(iii) $\Rightarrow$ (i). This is a special case of Corollary 3.3. ∎

3.7. EXAMPLE. Let $R_1 = k[x, y]/(x^2, y^2)$ and $R_2 = k[x, y]/(x^3, xy, y^2)$, each with the standard grading ($\deg x = \deg y = 1$). Then $F(R_1, \lambda) = F(R_2, \lambda) = 1 + 2\lambda + \lambda^2$. Moreover, R_1 is a complete intersection but R_2 is not even Gorenstein.

3.8. EXAMPLE. Let G be the subgroup of $GL(3, \mathbb{C})$ generated by the two diagonal matrices with diagonals $(-1, -1, 1)$ and $(1, 1, i)$, where $i^2 = -1$. (Thus G is Abelian of order 8.) Let G act on the polynomial ring $R = \mathbb{C}[x, y, z]$ in the obvious way, and let R^G be the fixed ring. R^G is generated as a $\mathbb{C}$-algebra by the monomials x^2, xy, y^2, and z^4. If we let $\deg x = \deg y = \deg z = 1$, then $F(R^G, \lambda) = 1/(1 - \lambda^2)^3$. However, R^G is not isomorphic to a polynomial ring in three variables, each of degree two. This provides a counterexample to a conjecture of Mallows and Sloane [21].

3.9. EXAMPLE. Let $R = k[x_1, x_2, x_3, x_4, x_5, x_6, x_7]/I$, where $I = (x_1x_5 - x_2x_4, x_1x_6 - x_3x_4, x_2x_6 - x_3x_5, x_1^2x_4 - x_5x_6x_7, x_1^3 - x_3x_5x_7)$, with the standard grading ($\deg x_i = 1$). Then R is a normal Gorenstein integral domain, but is not a complete intersection. However, R has the Poincaré series of a complete intersection, viz., $F(R, \lambda) = (1 + \lambda)^3/(1 - \lambda)^4$.

As a further consequence of Corollary 3.2, we can characterize the Hilbert function of standard Cohen–Macaulay G-algebras. More generally, we have the following result, which was first explicitly stated in [33, Theorem 2].

3.10. COROLLARY. *Let $H(n)$ be a function from $\mathbb{N}$ to $\mathbb{N}$. Let r be a nonnegative integer, and let k be any field. The following two conditions are equivalent*:

(i) *There exists a standard G-algebra R with $R_0 = k$ such that R contains a homogeneous R-sequence of length r and $H(n)$ is the Hilbert function of R.*

(ii) $(h_{0r}, h_{1r}, h_{2r}, \ldots)$ *is an O-sequence, where*

$$(1 - \lambda)^r F(R, \lambda) = \sum_{i=0}^{\infty} h_{ir}\lambda^i.$$

Proof. Assume (i). By Lemma 1.1, we may assume k is infinite. Thus we can find a homogeneous R-sequence $\theta_1, \ldots, \theta_r$ such that $\deg \theta_i = 1$. Then (ii) follows from Corollary 3.2 and Theorem 2.2 (applied to the ring $R/(\theta_1, \ldots, \theta_r)$).

Assume (ii). Let S be a standard G-algebra with $S_0 = k$ and $H(S, n) = h_{nr}$. The existence of S is guaranteed by Theorem 2.2. Let $R = S[x_1, \ldots, x_r]$, with $\deg x_i = 1$. Then R is the desired standard G-algebra and $(x_1, \ldots, x_r)$ is the desired R-sequence. ∎

Suppose R is a G-algebra of dimension d. Since R is Cohen–Macaulay if and only if R contains a homogeneous R-sequence of length d, we obtain from Corollary 3.10 the following result.

3.11. COROLLARY. *Let $H(n)$ be a function from $\mathbb{N}$ to $\mathbb{N}$, and let $d \in \mathbb{N}$. Let k be any field. The following two conditions are equivalent.*

(i) *There exists a Cohen–Macaulay standard G-algebra R with $R_0 = k$, with $\dim R = d$, and with Hilbert function H.*

(ii) *The power series $(1 - \lambda)^d \sum_{n=0}^{\infty} H(n)\lambda^n$ is a polynomial in λ, say $h_0 + h_1\lambda + \cdots + h_s\lambda^s$. Moreover, $(h_0, h_1, \ldots, h_s)$ is an O-sequence.* ∎

Corollary 3.11 is another result essentially due to Macaulay [18, Sect. 91; 19, p. 552]. It also follows from [26, Corollary 6.9]. It was used in [34] to prove the "Upper-Bound Conjecture for Spheres." As a simpleminded example of its use, let R be the standard G-algebra $R = k[x, y, z]/(xy, xz)$. Then $\dim R = 2$ and $(1 - \lambda)^2 F(R, \lambda) = 1 + \lambda - \lambda^2$. Hence R is not Cohen–Macaulay (since $h_2 < 0$).

If $F(\lambda) = \sum_{n=0}^{\infty} H(n)\lambda^n$ is a power series and $r \in \mathbb{N}$, then $(1 - \lambda)^r F(\lambda) = \sum_{n=0}^{\infty} (\nabla^r H(n))\lambda^n$, where ∇ is the *backward-difference operator*, defined by $\nabla H(n) = H(n) - H(n - 1)$ (with the convention $H(n) = 0$ if $n < 0$). Thus Corollary 3.11 implies that if R is a standard G-algebra of depth at least r (recall that depth R is the length of the longest *homogeneous* R-sequence in R) and Hilbert function H, then $\nabla^r H(n) \geqslant 0$ for all $n \in \mathbb{N}$. For instance, if R is an integral domain, then either $R = k$ or depth $R \geqslant 1$. In the latter case we have $H(0) \leqslant H(1) \leqslant H(2) \leqslant \cdots$. This is easy to see directly since multi-

plication by a homogeneous non-zero-divisor of degree one is a monomorphism from R_n into R_{n+1}. If R is normal, then either $\dim R \leqslant 1$ or $\operatorname{depth} R \geqslant 2$. Thus in the latter case $\nabla^2 H(R, n) \geqslant 0$.

4. Gorenstein Rings

We now wish to examine what can be said about the Hilbert function of a Gorenstein G-algebra. Our first result gives a necessary (but by no means sufficient) condition for a function $H: \mathbb{N} \to \mathbb{N}$ to be the Hilbert function of a Gorenstein G-algebra. The special case that R is standard is due to Macaulay [18, Sect. 70].

4.1. Theorem. *Let R be a Gorenstein G-algebra of Krull dimension d. Then for some integer ρ, $F(R, 1/\lambda) = (-1)^d \lambda^\rho F(R, \lambda)$ (as rational functions of λ).*

First proof. Let $\theta_1, \ldots, \theta_d$ be a homogeneous R-sequence (which exists since R is Cohen–Macaulay), say with $\deg \theta_i = f_i$. Let $S = R/(\theta_1, \ldots, \theta_d)$. Then S is a 0-dimensional Gorenstein G-algebra, say $S = S_0 + S_1 + \cdots + S_s$, where $S_s \neq 0$. It follows from Corollary 3.2 that $F(R, \lambda) = (h_0 + h_1\lambda + \cdots + h_s\lambda^s)/\prod_{i=1}^{d}(1 - \lambda^{f_i})$, where $h_i = \dim_k S_i$. Now since S is 0-dimensional Gorenstein, S_s is the socle of S, i.e., $S_s = \{x \in S: x(S_1 + \cdots + S_s) = 0\}$, and $\dim_k S_s = 1$. Let y be a nonzero element of S_s. If $0 \leqslant i \leqslant s$, define a pairing $S_i \times S_{s-i} \to k$ by $(x_1, x_2) \mapsto \alpha$ if $x_1 x_2 = \alpha y$. It is well known and easily proved that this is a perfect pairing, so in particular $h_i = h_{s-i}$. Hence $F(R, 1/\lambda) = (-1)^d \lambda^\rho F(R, \lambda)$, where $\rho = \sum f_i - s$. ∎

Second proof. Our second proof, while not quite as simple as the first proof, has the advantage that it can be generalized to algebras graded by certain semigroups other than $\mathbb{N}$. We shall require such a generalization in Section 6.

Let A, Y_i, e_i, s be as in Section 1. Then R has a minimal free resolution as an A-module which looks like

$$0 \to M_h \to \cdots \to M_2 \to M_1 \to M_0 \to R \to 0, \tag{9}$$

where $h = s - d$ since R is Cohen–Macaulay. We can choose (9) so that each M_i is a *graded* (free) A-module and all homomorphisms preserve degree. Suppose in doing so M_i has free homogeneous generators $X_{i1}, X_{i2}, \ldots, X_{i\beta_i}$ with $\deg X_{ij} = g_{ij}$. Thus $\beta_0 = 1$ and $g_{01} = 0$. Since R is Gorenstein, $M_h \cong A$ so $\beta_h = 1$. Moreover, a result of Buchsbaum and Eisenbud [3, Theorem 1.5] shows that there is a pairing $M_i \otimes M_{h-i} \to M_h \cong A$ which induces an isomorphism $M_i \to M_{h-i}^* = \operatorname{Hom}_A(M_{h-i}, A)$ (so $\beta_i = \beta_{h-i}$). One easily sees that in the present situation this pairing can be chosen to preserve degree. Let us abbreviate $g = g_{h1}$. It follows that the generators X_{ij} and $X_{h-i,j}$ can be labeled so that $g_{ij} + g_{h-i,j} = g$, for $1 \leqslant j \leqslant \beta_i = \beta_{h-i}$.

We can define a Poincaré series $F(M_i, \lambda)$ (using the graded module structure of M_i) just as was done for G-algebras. It follows that

$$F(M_i, \lambda) = \left(\sum_{j=1}^{\beta_i} \lambda^{a_{ij}}\right) \Big/ \prod_{t=1}^{s} (1 - \lambda^{e_t}). \tag{10}$$

Now using a well-known property of exact sequences we obtain from (9) that

$$F(R, \lambda) = F(M_0, \lambda) - F(M_1, \lambda) + \cdots + (-1)^h F(M_h, \lambda). \tag{11}$$

Substituting (10) into (11) yields an explicit expression for $F(R, \lambda)$. Using the result $g_{ij} + g_{h-i,j} = g$, we see that $F(R, 1/\lambda) = (-1)^{s-h} \lambda^{\rho} F(R, \lambda)$, where $\rho = \sum e_i - g$. Since R is Cohen–Macaulay, we have $d = s - h$, and the proof follows. ∎

It is natural to ask for other restrictions on the Hilbert function of a Gorenstein G-algebra besides Theorem 4.1. Let us restrict our attention to standard G-algebras R. Since a rational function $F(\lambda)$ is the Poincaré series of some standard Gorenstein G-algebra of dimension d if and only if $(1 - \lambda)^d F(\lambda)$ is the Poincaré series of some 0-dimensional standard Gorenstein G-algebra, it suffices to consider the case dim $R = 0$. Thus we have the following problem:

Problem. What sequences $(h_0, h_1, \ldots, h_s)$, with $h_s \neq 0$, satisfy $h_i = H(R, i)$ for some 0-dimensional standard Gorenstein G-algebra R? (We call such a sequence a *Gorenstein sequence.*)

By Theorem 2.2, we have that a Gorenstein sequence $(h_0, h_1, \ldots, h_s)$ is an O-sequence; while by Theorem 4.1 we have $h_i = h_{s-i}$. These two conditions are by no means sufficient. For instance, the sequence (1, 3, 5, 4, 5, 3, 1) satisfies both conditions, but by Theorem 4.2 below is not a Gorenstein sequence. This writer [33, Conjecture 2], and, independently, Iarrobino, conjectured that $(h_0, h_1, \ldots, h_s)$ is a Gorenstein sequence if and only if $h_i = h_{s-i}$ and $(h_0, h_1 - h_0, h_2 - h_1, \ldots, h_t - h_{t-1})$ is an O-sequence, where $t = [s/2]$. In Example 4.3, we show that this conjecture, or even the weaker conjecture that the numbers $h_i - h_{i-1}$ are nonnegative for $1 \leqslant i \leqslant t$, is false. First we show that the above conjecture is true if $h_1 \leqslant 3$.

4.2. THEOREM. *Let* $\mathbf{h} = (h_0, h_1, \ldots, h_s)$ *be a sequence of nonnegative integers with* $h_1 \leqslant 3$ *and* $h_s \neq 0$. *Then* $\mathbf{h}$ *is a Gorenstein sequence if and only if the following two conditions are satisfied*:

(i) $h_i = h_{s-i}$ *for* $0 \leqslant i \leqslant s$, *and*

(ii) $(h_0, h_1 - h_0, h_2 - h_1, \ldots, h_t - h_{t-1})$ *is an O-sequence, where* $t = [s/2]$.

Proof. Buchsbaum and Eisenbud [3, Proposition 3.3] have shown (though they state it slightly differently) that there is a one-to-one correspondence between (a) Hilbert functions $H(R, n)$ of standard Gorenstein G-algebras R

satisfying $\dim R = d$ and $H(R, 1) \leqslant d + 3$, and (b) sequences $r_1 \leqslant r_2 \leqslant \cdots \leqslant r_{2m+1}$ of integers, either all even or all odd, satisfying $r_i + r_{2m+1-i} > 0$ for $1 \leqslant i \leqslant 2m$ and $r_i + r_j \neq 0$ for any i, j. This correspondence is given by

$$H(R, n) = \binom{d+2+n}{d+2} - \sum_{i=1}^{2m+1} \binom{d+2+n-\frac{1}{2}(\sigma - r_i)}{d+2} + \sum_{i=1}^{2m+1} \binom{d+2+n-\frac{1}{2}(\sigma + r_i)}{d+2} - \binom{d+2+n-\sigma}{d+2},$$

where $\sigma = \sum_1^{2m+1} r_i$ and where we take $\binom{a}{b} = 0$ if $a < b$. If we take $d = 0$ above, then for some $s \geqslant 0$ we will have $H(R, s) \neq 0$ and $H(R, n) = 0$ for $n > s$ (since H is the Hilbert function of a 0-dimensional G-algebra). We want to show that the sequences $h_0 = H(R, 0), \ldots, h_s = H(R, s)$ which arise in this way from all possible sequences $r_1 \leqslant \cdots \leqslant r_{2m+1}$ satisfying (b) above are just the sequences satisfying (i) and (ii).

Now for any integer $c \geqslant 0$ we have

$$\sum_{n=0}^{\infty} \binom{2+n-c}{2} \lambda^n = \frac{\lambda^c}{(1-\lambda)^3},$$

keeping our convention that $\binom{a}{b} = 0$ if $a < b$. Condition (b) on the r_i's ensures that $\frac{1}{2}(\sigma - r_i) \geqslant 0$, $\frac{1}{2}(\sigma + r_i) \geqslant 0$, and $\sigma \geqslant 0$. Hence with $d = 0$ we obtain

$$\sum_{n=0}^{s} H(R, n) \lambda^n = P(\lambda)/(1-\lambda)^3,$$

where

$$P(\lambda) = 1 - \sum_{i=1}^{2m+1} \lambda^{\frac{1}{2}(\sigma - r_i)} + \sum_{i=1}^{2m+1} \lambda^{\frac{1}{2}(\sigma + r_i)} - \lambda^{\sigma}.$$

Let

$$P(\lambda) = \sum_{i=0}^{\sigma} a_i \lambda^i,$$

$$P(\lambda)/(1-\lambda) = \sum_{i=0}^{\sigma-1} b_i \lambda^i,$$

$$P(\lambda)/(1-\lambda)^2 = \sum_{i=0}^{\sigma-2} c_i \lambda^i.$$

The conditions on the r_i's imply that the a_i's are integers satisfying the following: (A_1) $a_0 = 1$; (A_2) $a_i = -a_{\sigma-i}$; (A_3) for some $j \leqslant \tau = [\sigma/2]$, $a_1 = a_2 = \cdots = a_j = 0$, while $\sum_{i=0}^{b} a_i \leqslant 0$ if $j < b \leqslant \tau$; (A_4) if σ is odd, then

$\sum_{i=0}^{\tau}(\tau - i + \frac{1}{2})a_i = 0$; and (A_5) if σ is even, then $\sum_{i=0}^{\tau}(\tau - i)a_i = 0$. (Conditions (A_4) and (A_5) merely guarantee that $P(\lambda)$ is divisible by $(1 - \lambda)^2$.) Conversely, given integers $a_0, a_1, \ldots, a_\sigma$ satisfying (A_1)–(A_5), we obtain a set of r_i's satisfying (b) by defining a_j of the r_i's to be equal to $2j - \sigma$ whenever $a_j > 0$.

Now $b_j = \sum_{i=0}^{j} a_i$. Hence from (A_1)–(A_5) it follows that the allowable sequences $b_0, \ldots, b_{\sigma-1}$ are characterized by the conditions: (B_1) $b_0 = 1$; (B_2) $b_i = b_{\sigma-1-i}$; (B_3) for some $j \leqslant \tau' = [\frac{1}{2}(\sigma - 1)]$, $b_1 = b_2 = \cdots = b_j = 1$, while $b_i \leqslant 0$ if $j < i \leqslant \tau'$; (B_4) if σ is odd, then $\frac{1}{2}b_{\tau'} + \sum_{i=0}^{\tau'-1} b_i = 0$; and (B_5) if σ is even, then $\sum_{i=0}^{\tau'} b_i = 0$.

Now $c_j = \sum_{i=0}^{j} b_i$. Hence from (B_1)–(B_5) it follows that the allowable sequences $c_0, \ldots, c_{\sigma-2}$ have one of the following two forms (depending on whether σ is even or odd):

$$1, 2, 3, \ldots, j, c_{j+1}, c_{j+2}, \ldots, c_\delta, 0, -c_\delta, \ldots, -c_{j+2}, -c_{j+1}, -j, \ldots, -3, -2, -1;$$

$$1, 2, 3, \ldots, j, c_{j+1}, c_{j+2}, \ldots, c_\delta, -c_\delta, \ldots, -c_{j+2}, -c_{j+1}, -j, \ldots, -3, -2, -1;$$

where $j \geqslant c_{j+1} \geqslant c_{j+2} \geqslant \cdots \geqslant c_\delta \geqslant 0$. But by Theorem 2.2, a function $H: \mathbb{N} \to \mathbb{N}$ satisfying $H(1) \leqslant 2$ is the Hilbert function of a standard G-algebra if and only if for some $j \geqslant 0$, $H(i) = i + 1$ for $i \leqslant j$ and $H(j) \geqslant H(j + 1) \geqslant H(j + 2) \geqslant \cdots$. Since our allowable Hilbert functions $H(R, n)$ are given by $H(R, n) = \sum_{i=0}^{n} c_i$, the proof follows. ∎

4.3. EXAMPLE. We now show that Theorem 4.2 is false if we remove the condition that $h_1 \leqslant 3$. Let S be any 0-dimensional G-algebra (not necessarily standard or Gorenstein), say $S = S_0 + S_1 + \cdots + S_s$, with $S_s \neq 0$. Let $E = \mathrm{Hom}_k(S, k)$. E has the structure of an S-module in the usual way, viz., $(x\phi)(y) = \phi(xy)$, where $x \in S$, $y \in S$, $\phi \in E$. (In fact, E is the injective envelope of k, regarded as the residue class field of S.) Let $R = S \times E$, endowed with componentwise addition and the multiplication $(x, \phi) \cdot (y, \psi) = (xy, x\psi + y\phi)$. Then R is a 0-dimensional Gorenstein k-algebra (see, e.g., [25, Corollary 6]). Moreover, R can be graded so that its Hilbert function satisfies $H(R, n) = H(S, n) + H(S, s + 1 - n)$, $0 \leqslant n \leqslant s + 1$, and $H(R, n) = 0$ if $n > s + 1$. Finally, R will be standard if and only if S is standard and the socle of S is S_s. Now pick $S = k[x, y, z]/(x, y, z)^4$, with the standard grading. Then S is a 0-dimensional standard G-algebra whose Poincaré series is $1 + 3\lambda + 6\lambda^2 + 10\lambda^3$ and whose socle is S_3. Hence $R = S \times E$ is a 0-dimensional standard Gorenstein G-algebra with Poincaré series $F(R, \lambda) = 1 + 13\lambda + 12\lambda^2 + 13\lambda^3 + \lambda^4$. This provides the desired counterexample. More generally, taking $S = k[x, y, z]/(x, y, z)^s$, we obtain a Gorenstein sequence $(h_0, h_1, \ldots, h_s)$ satisfying $h_1 > h_2 > \cdots > h_t$, where $t = [s/2]$.

As a very special case of the problem of characterizing Gorenstein sequences, we raise the following question. Given an integer $n > 0$, what is the least

integer $f(n)$ for which $(1, n, f(n), n, 1)$ is a Gorenstein sequence? We can show $f(n) = n$ if $n \leqslant 5$, but no other values of $f(n)$ seem to be known. It can be shown that $f(n)$ has order of growth $n^{2/3}$. More precisely,

$$\tfrac{1}{2} \cdot 6^{2/3} \leqslant \liminf f(n)n^{-2/3} \leqslant \limsup f(n)n^{-2/3} \leqslant 6^{2/3}.$$

Presumably $\lim f(n)n^{-2/3}$ exists, and it would be interesting to find this limit.

We now turn to the problem of finding some kind of converse to Theorem 4.1. More specifically, if R is a G-algebra of dimension d such that $F(R, 1/\lambda) = (-1)^d \lambda^\rho F(R, \lambda)$ for some $\rho \in \mathbb{Z}$, then under what circumstances can we conclude R is Gorenstein? The ring R_2 of Example 3.7 shows that it is not sufficient to assume that R is Cohen–Macaulay. Somewhat surprisingly, it is sufficient to assume that R is a Cohen–Macaulay integral domain. This is the chief new result of this paper.

4.4. THEOREM. *Let R be a G-algebra. Suppose that R is a Cohen–Macaulay integral domain of Krull dimension d. Then R is Gorenstein if and only if for some $\rho \in \mathbb{Z}$, $F(R, 1/\lambda) = (-1)^d \lambda^\rho F(R, \lambda)$.*

Proof. The "only if" part follows from Theorem 4.1. To prove the "if" part, assume that R is any d-dimensional Cohen–Macaulay integral domain and a G-algebra. Let K_R be the canonical module of R. Using the notation of Section 1, we then have $K_R = \operatorname{Ext}_A^{s-d}(R, A)$. (This can be taken as the definition of K_R.) Recall that R is Gorenstein if and only if $K_R \cong R$.

We first prove that K_R can be graded (as an R-module) so that for some $q \in \mathbb{Z}$,

$$F(K_R, \lambda) = (-1)^d \lambda^q F(R, 1/\lambda). \tag{12}$$

Let the exact sequence $0 \to M_h \xrightarrow{\eta_h} \cdots \xrightarrow{\eta_2} M_1 \xrightarrow{\eta_1} M_0 \xrightarrow{\eta_0} R \to 0$ be as in the second proof to Theorem 4.1, and preserve the meaning of X_{ij}, g_{ij}, β_i from this proof. Let $*$ denote the functor $\operatorname{Hom}_A(-, A)$. Applying $*$ to (9) and using the fact that $\operatorname{Ext}_A^i(R, A) = 0$ if $i \neq s - d$ (since R is Cohen–Macaulay), we obtain

$$0 \longrightarrow M_0{}^* \xrightarrow{\eta_1{}^*} M_1{}^* \xrightarrow{\eta_2{}^*} \cdots \xrightarrow{\eta_h{}^*} M_h{}^* \longrightarrow K_R \longrightarrow 0 \tag{13}$$

as a minimal free resolution of K_R. Now as A-modules we have $M_i{}^* \cong M_i$. Let $X_{i1}^*, X_{i2}^*, \ldots, X_{i\beta_i}^*$ be the basis of $M_i{}^*$ dual to the basis $X_{i1}, X_{i2}, \ldots, X_{i\beta_i}$ of M_i. If we define $\deg X_{ij}^* = -g_{ij}$, then the homomorphisms $\eta_i{}^*$ will be degree preserving. With respect to this grading, K_R ($= \operatorname{coker} \eta_h{}^*$) will obtain the structure of a graded A-module and will keep the same grading when considered as an R-module. From (13) we have

$$F(K_R, \lambda) = F(M_h{}^*, \lambda) - F(M_{h-1}^*, \lambda) + \cdots + (-1)^h F(M_0{}^*, \lambda). \tag{14}$$

Moreover, since $\deg X_{ij}^* = -g_{ij}$, we have

$$F(M_i^*, \lambda) = \left(\sum_{j=1}^{\beta_i} \lambda^{-g_{ij}}\right) \Big/ \prod_{t=1}^{s} (1 - \lambda^{e_t}). \tag{15}$$

Comparing (14) and (15) with (10) and (11), we obtain $F(K_R, \lambda) = (-1)^d \lambda^q F(R, 1/\lambda)$, where $q = -\sum e_i$. This proves (12).

For convenience, let us shift the grading of K_R so that the least degree of a nonzero element is 0. (K_R will have an element of least degree since it is finitely generated as an R-module.) Now suppose that $F(R, 1/\lambda) = (-1)^d \lambda^\rho F(R, \lambda)$ for some $\rho \in \mathbb{Z}$. Since $H(R, 0) = 1$, it follows from (12) and our "shift" of K_R that the elements of K_R of degree 0 form a vector space over k of dimension one. Let x be a nonzero element of K_R of degree 0. We now invoke the result [11, Corollary 6.7] that since R is an integral domain, K_R is isomorphic to an ideal of R. (In [11] it is assumed that R is local, but the argument for graded algebras is almost identical. Also, [11] states only that K_R is isomorphic to a fractional ideal of R, but we can multiply K_R by a suitable element of R so that K_R becomes an ideal.) Let us identify K_R with this ideal. Now by (12), $F(K_R, \lambda) = F(R, \lambda)$, or equivalently, K_R and R have the same Hilbert function. Since R is a domain, $\dim_k xR_n = \dim_k R_n = H(R, n) = H(K_R, n)$. But by the definition of a graded R-module, $xR_n \subset (K_R)_n$, the nth homogeneous part of K_R. Hence since $\dim_k xR_n = H(K_R, n)$, we have $xR_n = (K_R)_n$. Thus $R \cong xR = K_R$, so R is Gorenstein. ∎

Remark. There is a generalization of Eq. (12) valid for any G-algebra R. Let $s = \dim A$, $d = \dim R$, and $\delta = \operatorname{depth} R$. Then there is a natural grading of the modules $E^i = \operatorname{Ext}_A^i(R, A)$ such that

$$\sum_{i=0}^{d-\delta} (-1)^i F(E^{n-d+i}, \lambda) = (-1)^d \lambda^q F(R, 1/\lambda).$$

It is natural to ask if the hypothesis in Theorem 4.4 that R is a Cohen–Macaulay integral domain can be weakened. It does not appear that a significant weakening is possible; the next example shows that we cannot merely assume that R is a reduced Cohen–Macaulay G-algebra.

4.5. EXAMPLE. Let $R = k[x, y, z, w]/(xw, yw, xyz)$, with the standard grading. Then R is a reduced Cohen–Macaulay G-algebra and $F(R, \lambda) = (1 + 2\lambda + \lambda^2)/(1 - \lambda)^2$. However, R is not Gorenstein.

As a curious consequence of Theorem 4.4, let S be a 0-dimensional G-algebra which is not Gorenstein but which satisfies $F(S, 1/\lambda) = (-1)^d \lambda^\rho F(S, \lambda)$. For instance, $S = k[x, y]/(x^3, xy, y^2)$. It then follows from Theorem 4.4 that S is not isomorphic to a G-algebra R which is an integral domain, modulo a homogeneous R-sequence. This suggests that it may be of interest to investigate

the question: what Noetherian rings are isomorphic to integral domains R modulo R-sequences?

We now discuss how the condition $F(R, 1/\lambda) = (-1)^d \lambda^e F(R, \lambda)$ can be reformulated in terms of the Hilbert function $H(R, n)$, in the special case that $\deg F(R, \lambda) < 0$. If R is a G-algebra, then the general form (1) of $F(R, \lambda)$ implies that there exist nonzero distinct complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_m$ (necessarily roots of unity) and polynomials $P_1, P_2, \ldots, P_m \in \mathbb{Q}[x]$ such that

$$H(R, n) = \sum_{i=1}^{m} P_i(n)\, \alpha_i{}^n \tag{16}$$

for all *sufficiently large* integers n. The condition $\deg F(R, \lambda) < 0$ (i.e., $\deg P(R, \lambda) < e_1 + e_2 + \cdots + e_s$, in the notation of (1)) is equivalent to saying that (16) holds for *all* $n \geqslant 0$. For instance, if R is standard then $m = 1$, $\alpha_1 = 1$, and $P_1(n)$ is the Hilbert polynomial of R. We have $H(R, n) = P_1(n)$ for all $n \geqslant 0$ if and only if $\deg F(R, \lambda) < 0$. We state without proof a result of Popoviciu [24] (see [31, Proposition 5.2] for further discussion and consequences).

4.6. THEOREM (Popoviciu). *Let $\alpha_1, \ldots, \alpha_m$ be distinct nonzero complex numbers, and let $P_1, \ldots, P_m$ be polynomials with complex coefficients. Define for all $n \in \mathbb{Z}$, $H(n) = \sum_{i=1}^{m} P_i(n)\alpha_i{}^n$. Let $F(\lambda) = \sum_{n=0}^{\infty} H(n)\lambda^n$, $\bar{F}(\lambda) = \sum_{n=1}^{\infty} H(-n)\lambda^n$. Then, as rational functions of λ, we have $\bar{F}(\lambda) = -F(1/\lambda)$.* ∎

4.7. COROLLARY. *Preserve the notation of Theorem* 4.6. *Let $d = m + \sum_{i=1}^{m} \deg P_i$. Then $F(1/\lambda) = (-1)^d \lambda^e F(\lambda)$ for some $e \in \mathbb{Z}$ if and only if $e \geqslant 1$, $H(-1) = H(-2) = \cdots = H(-e + 1) = 0$ and $H(n) = (-1)^{d-1} H(-e - n)$ for all $n \in \mathbb{Z}$.* ∎

Suppose that R is a d-dimensional G-algebra and a Cohen–Macaulay integral domain such that (16) holds for *all* $n \in \mathbb{N}$. Thus (16) defines $H(R, n)$ for all $n \in \mathbb{Z}$. It follows from Theorem 4.4 and Corollary 4.7 that R is Gorenstein if and only if for some integer $e \geqslant 1$, we have $H(R, -1) = H(R, -2) = \cdots = H(R, -e + 1) = 0$ and $H(R, n) = (-1)^{d-1} H(R, -e - n)$ for all $n \in \mathbb{Z}$.

5. SOME EXAMPLES OF GORENSTEIN G-ALGEBRAS

Theorem 4.4 is a powerful tool in proving certain rings are Gorenstein. In this section we shall give several applications of Theorem 4.4. These will include simple proofs of known results, and some new results.

a. *Numerical semigroups.* A *numerical semigroup* is a subsemigroup Γ of the additive semigroup $\mathbb{N}$ such that $0 \in \Gamma$ and $\mathbb{N} - \Gamma$ is finite. (Any subsemigroup

of $\mathbb{N}$ with 0 is isomorphic to a numerical semigroup.) If Γ is a numerical semigroup, the *conductor* $c = c(\Gamma)$ of Γ is defined by $c = \max\{n \in \mathbb{N}: n - 1 \notin \Gamma\}$. If k is a field, $k[\Gamma]$ denotes the subalgebra of $k[x]$ generated by all monomials x^α, $\alpha \in \Gamma$. (Thus the monomials x^α in fact form a k-basis for $k[\Gamma]$.) Since $k[\Gamma]$ is a one-dimensional integral domain, it is Cohen–Macaulay.

5.1. THEOREM (Herzog and Kunz [10]). *Let Γ be a numerical semigroup with conductor c. Then the following two conditions are equivalent:*

(i) *$k[\Gamma]$ is Gorenstein,*

(ii) *for all $0 \leqslant i \leqslant c - 1$, we have $i \in \Gamma$ if and only if $c - 1 - i \notin \Gamma$.*

Proof. If we define $\deg x = 1$, then $k[\Gamma]$ becomes a G-algebra. We have already observed that $k[\Gamma]$ is a Cohen–Macaulay integral domain, so Theorem 4.4 applies. Write $R = k[\Gamma]$. Then

$$F(R, \lambda) = \sum_{j \in \Gamma} \lambda^j = \frac{1}{1 - \lambda} - \sum_{\substack{i \in \mathbb{N} \\ i \notin \Gamma}} \lambda^i.$$

Then

$$-F(R, 1/\lambda) = \frac{\lambda}{1 - \lambda} + \sum_{\substack{i \in \mathbb{N} \\ i \notin \Gamma}} \lambda^{-i}.$$

The least degree of any term of $F(R, \lambda)$ is 0, while the least degree of any term of $-F(R, 1/\lambda)$ is $-(c - 1)$. Thus if $F(R, 1/\lambda) = -\lambda^\rho F(R, \lambda)$, then $\rho = 1 - c$ and

$$\frac{1}{1 - \lambda} - \sum_{\substack{i \in \mathbb{N} \\ i \notin \Gamma}} \lambda^i = \frac{\lambda^c}{1 - \lambda} + \sum_{\substack{i \in \mathbb{N} \\ i \notin \Gamma}} \lambda^{c-1-i}.$$

Hence $F(R, 1/\lambda) = -\lambda^{1-c} F(R, \lambda)$ if and only if (ii) holds, and the proof follows from Theorem 4.4. ∎

b. *Schubert varieties.* Let $0 \leqslant a_0 < a_1 \cdots < a_d$ be integers, and let R be the homogeneous coordinate ring of the Schubert variety $\Omega(a_0 \cdots a_d)$ (defined over a field k). For definitions, see [15, Chap. XIV], [17] or [35]. R is a (standard) G-algebra, and it is known that R is a Cohen–Macaulay integral domain (see [17, Sect. 5]). Moreover, the "postulational formula" of Hodge and Littlewood [15, Chap. XIV, Sect. 9] gives an explicit expression for $H(R, n)$ in terms of a determinant. Unfortunately, it is difficult to apply Theorem 4.4 directly to this expression for $H(R, n)$. If, however, the proof of the postulational formula is examined, one obtains an alternative description of $H(R, n)$, as follows. Define $b_i = a_i - i$, and let $P(b_0 \cdots b_d) = \{(i, j): 0 \leqslant i \leqslant d, 1 \leqslant j < b_{d-i}\}$. Define a partial ordering on $P(b_0 \cdots b_d)$ by $(i, j) \leqslant (i', j')$ if $i \geqslant i'$ and $j \geqslant j'$.

For instance, if $d = 9$ and $(a_0, a_1, \ldots, a_9) = (0, 1, 2, 4, 5, 8, 9, 12, 14, 15)$, then $(b_0, b_1, \ldots, b_9) = (0, 0, 0, 1, 1, 3, 3, 5, 6, 6)$ and $P(b_0 b_1 \cdots b_9)$ is depicted in Fig. 1. By examining the proof of the postulational formula [15, Chap. XIV, Sect. 9], one can prove the following:

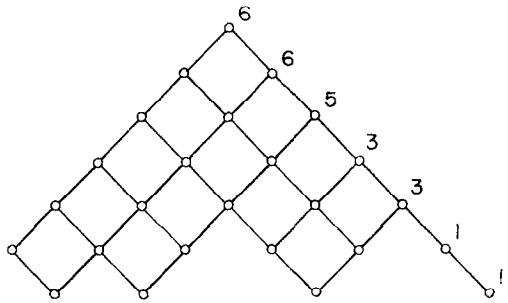

FIG. 1. The partially ordered set $P(0, 0, 0, 1, 1, 3, 3, 5, 6, 6)$.

5.2. THEOREM. *Let R be the homogeneous coordinate ring of the Schubert variety $\Omega(a_0 a_1 \cdots a_d)$, defined over a field k. Let $b_i = a_i - i$. Then $H(R, n)$ is equal to the number of order-preserving maps $\sigma\colon P(b_0 b_1 \cdots b_d) \to \{0, 1, \ldots, n\}$. (The statement that σ is "order preserving" means: $x \leqslant y$ in $P(b_0 b_1 \cdots b_d)$ implies $\sigma(x) \leqslant \sigma(y)$.)* ∎

In the terminology of [28], $H(R, n)$ is equal to the number of plane partitions whose shape is contained in $(b_d, b_{d-1}, \ldots, b_0)$ and whose largest part is at most n. Such plane partitions were studied prior to Hodge and Littlewood by MacMahon, and his formula for $GF(p_1 p_2 \cdots p_m, n)$ [20, Sect. X], in the case $x = 1$, is equivalent to the postulational formula (assuming the validity of Theorem 5.2). For further aspects of Theorem 5.2, see [35].

Now suppose P is *any* finite partially ordered set with p elements, and let $\Gamma(P, n)$ be the number of order-preserving maps $\sigma\colon P \to \{0, 1, \ldots, n\}$. It is easily seen that $\Gamma(P, n)$ is a polynomial in n of degree p. We deduce immediately from [29, Propositions 19.1(iii) and 19.3] the following result (our $\Gamma(P, n)$ is $\Omega(P; n + 1)$ in the terminology of [29]):

5.3. THEOREM. *Let P be a finite partially ordered set with p elements, and let ρ be a positive integer. The following two conditions are equivalent:*

(i) $\Gamma(P, -1) = \Gamma(P, -2) = \cdots = \Gamma(P, -\rho + 1) = 0$ *and* $\Gamma(P, n) = (-1)^p \Gamma(P, -\rho - n)$ *for all* $n \in \mathbb{Z}$.

(ii) *Every maximal chain of P has $\rho - 1$ elements.* ∎

Combining Theorem 4.4, Corollary 4.7, Theorem 5.2, Theorem 5.3, and the fact that the homogeneous coordinate ring of a Schubert variety is a Cohen–Macaulay integral domain, we obtain:

5.4. THEOREM. *Let R be the homogeneous coordinate ring of the Schubert variety $\Omega(a_0a_1 \cdots a_d)$, defined over a field k. Let $b_i = a_i - i$. Then R is Gorenstein if and only if all maximal chains of the partially ordered set $P(b_0b_1 \cdots b_d)$ have the same length.* ∎

For instance, every maximal chain of the partially ordered set $P(0, 0, 0, 1, 1, 3, 3, 5, 6, 6)$ of Fig. 1 has length 6. Hence the homogeneous coordinate ring of $\Omega(0, 1, 2, 4, 5, 8, 9, 12, 14, 15)$ is Gorenstein. The determination of which $\Omega(a_0a_1 \cdots a_d)$ are Gorenstein was first accomplished by Svanes [36, (5.5.5)]. Although his condition is stated differently from ours, it is of course equivalent.

In a manner similar to the above, one can treat the problem, first solved by Svanes [36, Theorem 5.5.6], of which of the "determinantal varieties" are Gorenstein. We omit the details.

c. *Invariants of finite groups.* We now come to an application of Theorem 4.4 which has not previously been proved by other means. Let k be a field of characteristic 0, and let H be a finite subgroup of $GL(m, k)$. H acts on the polynomial ring $R = k[x_1, x_2, \ldots, x_m]$ in the obvious way; let R^H denote the fixed ring.

5.5. THEOREM. *Let λ be an indeterminate. Then R^H is Gorenstein if and only the following identity holds in the field $k(\lambda)$:*

$$\sum_{h \in H} \frac{1}{\det(1 - \lambda h)} = \lambda^{-r} \sum_{h \in H} \frac{\det h}{\det(1 - \lambda h)}, \tag{17}$$

where r is the number of pseudoreflections in H. (An element of H is a pseudoreflection *if it has precisely one eigenvalue not equal to* 1.)

Sketch of proof. R^H is clearly a domain, and by a theorem of Hochster and Eagon [13, Proposition 13] R^H is Cohen–Macaulay. If we define $\deg x_i = 1$, then R^H becomes a G-algebra. Hence we can apply Theorem 4.4. A result of Molien [23], [4, Sect. 227] states that

$$F(R^H, \lambda) = \frac{1}{|H|} \sum_{h \in H} \frac{1}{\det(1 - \lambda h)}. \tag{18}$$

If we apply Theorem 4.4 directly to (18), we obtain (17) for *some* integer r. The value of r can be obtained by expanding both sides of (17) in a Laurent expansion about $\lambda = 1$. The routine details are omitted. ∎

5.6. COROLLARY (Watanabe [37, Theorem 1]). *If $H \subset SL(m, k)$, then R^H is Gorenstein.*

Proof. If $H \subset SL(m, k)$, then $r = 0$ and each $\det h = 1$. Hence (17) holds. ∎

5.7. COROLLARY (Watanabe [38, Theorem 1]). *If H contains no pseudo-reflections and R^H is Gorenstein, then $H \subset SL(m, k)$.*

Proof. Given the hypothesis, then (17) holds with $r = 0$. Now set $\lambda = 0$ in (17). We obtain $|H| = \sum_{h \in H} (\det h)$. Since each $\det h$ is a root of unity, we must have $\det h = 1$. ∎

6. RINGS GRADED BY $\mathbb{N}^s$

Let s be a positive integer, and let $\Phi = \mathbb{N}^s$, regarded as an additive monoid (a *monoid* is a semigroup with identity).

By a *Φ-graded ring*, we mean a Noetherian commutative ring R with identity graded by the semigroup Φ. In other words, the additive group of R can be written as a direct sum $R = \sum_{\alpha \in \Phi} R_\alpha$, where $R_\alpha R_\beta \subset R_{\alpha+\beta}$. We shall say that a Φ-graded ring R is a *Φ-algebra* if in addition $R_0 = k$, a field, so that R is an algebra over k. We can refine our definitions of $H(R, n)$ and $F(R, \lambda)$ to the case of Φ-algebras. If $\alpha = (\alpha_1, \ldots, \alpha_s) \in \mathbb{Z}^s$, let us write $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_s^{\alpha_s}$ and $\boldsymbol{\lambda}^\alpha = \lambda_1^{\alpha_1} \cdots \lambda_s^{\alpha_s}$. Then if R is a Φ-algebra, define

$$H(R, \alpha) = \dim_k R_\alpha, \qquad \alpha \in \Phi,$$

$$F(R, \boldsymbol{\lambda}) = \sum_{\alpha \in \Phi} H(R, \alpha) \boldsymbol{\lambda}^\alpha.$$

It is a consequence of the Hilbert syzygy theorem that $F(R, \boldsymbol{\lambda})$ is a rational function of $\lambda_1, \ldots, \lambda_s$ (the point being that in (9) we can take the M_i to be Φ-graded and all homomorphisms to be degree preserving with respect to the Φ-grading).

It is natural to consider extending our results about the Poincaré series $F(R, \lambda)$ to $F(R, \boldsymbol{\lambda})$, when R is Φ-graded. Unfortunately we quickly run into difficulties because we cannot always choose a maximal R-sequence in R which is homogeneous with respect to the Φ-grading. One result which does carry over is Theorem 4.1. We cannot generalize the first proof of Theorem 4.1 because that depended on choosing a homogeneous maximal R-sequence. The second proof, however, can be carried over, because in the exact sequence (9), the modules M_i can be chosen to be Φ-graded and all homomorphisms can be chosen to preserve degree. Similarly the proof of Theorem 4.4 can be carried out for Φ-gradings. We obtain the following results:

6.1. THEOREM. (i) *Let R be a Gorenstein Φ-algebra of Krull dimension d. Then for some vector $\alpha \in \mathbb{Z}^s$, $F(R, \boldsymbol{\lambda}) = (-1)^d \boldsymbol{\lambda}^\alpha F(R, 1/\boldsymbol{\lambda})$ (as rational functions of $\lambda_1, \ldots, \lambda_s$). Here $1/\boldsymbol{\lambda}$ denotes the substitution of $1/\lambda_i$ for λ_i, $1 \leqslant i \leqslant s$.*

(ii) *Let R be a Cohen–Macaulay Φ-algebra of dimension d. Then the canonical module K_R of R can be Φ-graded (as an R-module) in such a way that $F(K_R, \boldsymbol{\lambda}) = (-1)^d F(R, 1/\boldsymbol{\lambda})$.*

(iii) *Let R be a Φ-algebra of dimension d, and suppose that R is also a Cohen–Macaulay integral domain. Then R is Gorenstein if and only if for some vector $\alpha \in \mathbb{Z}^s$, $F(R, \lambda) = (-1)^d \lambda^\alpha F(R, 1/\lambda)$.* ∎

There is one additional result about Φ-algebras which will be useful to us.

6.2. LEMMA. *Let R be a Cohen–Macaulay Φ-algebra and an integral domain. Then the canonical module K_R of R, endowed with the natural grading of Theorem* 6.1(ii), *is isomorphic as a Φ-graded R-module to a Φ-homogeneous ideal I of R, up to a shift in grading. In other words, there is a fixed $\beta \in \mathbb{Z}^s$ and an R-module isomorphism θ: $K_R \to I$ such that I is an ideal of R generated by elements of various R_α for $\alpha \in \Phi$, and $\theta((K_R)_\gamma) = I_{\beta+\gamma}$ for all $\gamma \in \mathbb{Z}^s$, where by definition $I_\gamma = I \cap R_\gamma$.*

Proof. Let $T = R - \{0\}$, and let S be the set of nonzero Φ-homogeneous elements of R. Then $S^{-1}R \subset T^{-1}R$ and $S^{-1}R$ is a $\mathbb{Z}^s$-graded R-module in the obvious way. Now $T^{-1}K_R \cong K_{T^{-1}R} \cong T^{-1}R$ since $T^{-1}R$ is a field (and therefore Gorenstein). Hence K_R is isomorphic to an R-submodule of $T^{-1}R$. After multiplication by a suitable element of $T^{-1}R$, we obtain an embedding ι: $K_R \to T^{-1}R$ such that $\iota(X) = 1$ for some fixed Φ-homogeneous element $X \in K_R$ (say of degree α). If $Y \in K_R$ is Φ-homogeneous of degree β and $\iota(Y) = y$, then $yX = Y$. Hence $y \in S^{-1}R$ and $\deg y = \beta - \alpha$. Therefore ι is a degree-preserving embedding of K_R into $S^{-1}R$, up to a shift by α in the grading. Multiplying by a suitable Φ-homogeneous element of R, we obtain an embedding of K_R into R which is degree preserving up to a shift in grading. ∎

We now wish to apply Theorem 6.1 to a special class of Φ-algebras, viz., those generated by monomials. To be precise, let M be a submonoid of Φ (i.e., a subsemigroup containing 0), and let k be a field. By $k[M]$ we mean the subalgebra of $k[x_1, \ldots, x_s]$ spanned by the monomials $\mathbf{x}^\alpha$ where $\alpha \in M$. Thus $k[M]$ is the semigroup ring (over k) of M. More generally, if S is any *subset* of Φ, $k[S]$ will denote the subspace of $k[x_1, \ldots, x_s]$ spanned by the monomials $\mathbf{x}^\alpha$ where $\alpha \in S$. Thus $k[S]$ will be a subring with identity if and only if S is a monoid. When M is a monoid, the ring $k[M]$ has an obvious Φ-grading which satisfies

$$H(k[M], \alpha) = 1, \quad \text{if } \alpha \in M$$
$$= 0, \quad \text{if } \alpha \notin M;$$
$$F(k[M], \lambda) = \sum_{\alpha \in M} \lambda^\alpha.$$

6.3. THEOREM. *Let M be a submonoid of Φ such that $R = k[M]$ is Cohen–Macaulay of dimension d. Then in the Laurent expansion of $(-1)^d F(R, 1/\lambda)$ convergent in a deleted neighborhood of the origin, the coefficient of every monomial is either zero or one. Let K_M denote the set of those $\alpha \in \mathbb{N}^s$ such that the coefficient*

of λ^α *is one. Then* $M + K_M \subset K_M$, *so that* $k[K_M]$ *is an* R*-module. In fact,* $k[K_M] = K_R$, *the canonical module of* R.

Proof. By Lemma 6.2, we know that K_R is isomorphic as a Φ-graded R-module to some Φ-homogeneous ideal I of R, up to a shift in grading. Since $H(R, \alpha) = 0$ or $H(R, \alpha) = 1$ for all $\alpha \in \Phi$, it follows that every coefficient of $F(I, \lambda)$ is 0 or 1, and thus I is completely determined by $F(I, \lambda)$. Since I is an ideal, the set K_M of those $\alpha \in \mathbb{N}^s$ such that $H(I, \alpha) = 1$ satisfies $M + K_M \subset K_M$. Now by Theorem 6.1(ii) we have $F(I, \lambda) = (-1)^d \lambda^\beta F(R, 1/\lambda)$ for some $\beta \in \Phi$. The choice of β merely amounts to a shift in the grading of I since R is a domain, and the proof follows. ∎

Note that Theorem 6.3 gives necessary conditions for $k[M]$ to be Cohen–Macaulay, viz., every coefficient in $(-1)^d F(R, 1/\lambda)$ is zero or one, and $M + K_M \subset K_M$. We do not know whether these conditions are *sufficient* for R to be Cohen–Macaulay.

Monomial systems of parameters. Recently Goto *et al.* [7] and Goto [6] have studied rings $R = k[M]$, M a finitely generated submonoid of Φ (as defined above), with the property that there exist vectors $\alpha_1, \alpha_2, \ldots, \alpha_d \in M$ such that $\mathbf{x}^{\alpha_1}, \mathbf{x}^{\alpha_2}, \ldots, \mathbf{x}^{\alpha_d}$ is a system of parameters for R. (Goto *et al.* use a different but equivalent definition for such rings.) Let us call such a monoid M a *simplicial monoid.* (Note that these include the numerical semigroups of Section 5a.) We show how the techniques of this paper are of value in studying the rings $k[M]$ where M is simplicial.

6.4. THEOREM. *Let* M *be a simplicial submonoid of* Φ, *with* $\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_d}$ *a system of parameters for* $k[M]$. *The following three conditions are equivalent*:

(i) $k[M]$ *is Cohen–Macaulay,*

(ii) M *is a disjoint union of finitely many translates of the free commutative monoid* $\alpha_1\mathbb{N} + \alpha_2\mathbb{N} + \cdots + \alpha_d\mathbb{N}$.

Equivalently, there exist $\beta_1, \beta_2, \ldots, \beta_t \in M$ (*necessary unique*) *such that every element* γ *of* M *has a unique representation of the form* $\gamma = \beta_i + \sum_{j=1}^d a_j\alpha_j$, $a_j \in \mathbb{N}$.

(iii) *If* $\beta \in \mathbb{Z}^s$ *and for some* i *and* j $(1 \leqslant i < j \leqslant d)$ $\beta + \alpha_i \in M$ *and* $\beta + \alpha_j \in M$, *then* $\beta \in M$.

Proof. (i) ⇒ (ii). Let $S = R/(\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_d})$. Corollary 3.2 extends directly to Φ-gradings when R is Φ-graded and $\theta_1, \theta_2, \ldots, \theta_r$ are Φ-homogeneous. Thus we obtain that

$$F(R, \lambda) = F(S, \lambda) \Big/ \prod_{i=1}^d (1 - \lambda^{\alpha_i}) \tag{19}$$

if and only if $\mathbf{x}^{\alpha_1},\ldots,\mathbf{x}^{\alpha_d}$ is an R-sequence, i.e., if and only if R is Cohen–Macaulay. Suppose that R is Cohen–Macaulay. Since $H(S,\alpha) \leqslant H(R,\alpha)$ for all $\alpha \in \mathbb{N}^s$, we have that $F(S,\boldsymbol{\lambda}) = \sum_{i=1}^{t} \boldsymbol{\lambda}^{\beta_i}$ for some distinct $\beta_1,\ldots,\beta_t \in M$. Comparing the left- and right-hand sides of (19) yields (ii).

(ii) $\Rightarrow$ (i). If (ii) holds, then with S as above we have that $F(S,\boldsymbol{\lambda}) = \sum_{i=1}^{t} \boldsymbol{\lambda}^{\beta_i}$ and that (19) holds. Hence R is Cohen–Macaulay.

(ii) $\Rightarrow$ (iii). Assume (ii), and suppose for $\beta \in \mathbb{Z}^s$ that $\beta + \alpha_i \in M$ and $\beta + \alpha_j \in M$, say $\beta + \alpha_i = \beta_u + \sum_{r=1}^{d} a_r\alpha_r$, $\beta + \alpha_j = \beta_v + \sum_{r=1}^{d} b_r\alpha_r$, where $a_r, b_r \in \mathbb{N}$. Then $\beta_v + \alpha_i + \sum b_r\alpha_r = \beta_u + \alpha_j + \sum a_r\alpha_r$. By (ii), these representations coincide. In particular, $a_i > 0$, so from $\beta + \alpha_i = \beta_u + \sum a_r\alpha_r$ we conclude $\beta \in M$.

(iii) $\Rightarrow$ (i). Assume that $k[M]$ is not Cohen–Macaulay. Thus $\mathbf{x}^{\alpha_1},\ldots,\mathbf{x}^{\alpha_d}$ is not an R-sequence, so for some $i > 1$, $\mathbf{x}^{\alpha_i}$ is a zero-divisor modulo the ideal $I = (\mathbf{x}^{\alpha_1},\ldots,\mathbf{x}^{\alpha_{i-1}})$. (We can take $i > 1$ rather than $i \geqslant 1$ since $k[M]$ is a domain.) Thus $\mathbf{x}^{\alpha_i}X = Y$, where $X \notin I$ and $Y \in I$. It is easy to see that we can pick X and Y to be monomials. Since $Y \in I$, we get an equation $\mathbf{x}^{\alpha_i+\gamma} = \mathbf{x}^{\alpha_j+\delta}$, where $j < i$ and $\gamma, \delta \in M$. Thus $\gamma - \alpha_j = \delta - \alpha_i$. Call this element β. Now $\beta \notin M$ since otherwise $\gamma - \alpha_j \in M$, which implies $\mathbf{x}^{\gamma} \in I$. Moreover $\beta + \alpha_i = \delta \in M$ and $\beta + \alpha_j = \gamma \in M$. Hence (iii) fails. ∎

The equivalence of (i) and (iii) in Theorem 6.4 is one of the results of Goto *et al.* [7, Theorem 1]. They also give some other conditions equivalent to (i), (ii), and (iii) above. They then determine the canonical module K_R when R is Cohen–Macaulay, and they state a necessary and sufficient condition for R to be Gorenstein. We can do the same by applying Theorem 6.3. Note that if

$$F(R,\boldsymbol{\lambda}) = \left(\sum_{i=1}^{t} \boldsymbol{\lambda}^{\beta_i}\right) \Big/ \prod_{i=1}^{d} (1 - \boldsymbol{\lambda}^{\alpha_i}),$$

then

$$(-1)^d\, \boldsymbol{\lambda}^{-\alpha_1-\cdots-\alpha_d} F(R, 1/\boldsymbol{\lambda}) = \left(\sum_{i=1}^{t} \boldsymbol{\lambda}^{-\beta_i}\right) \Big/ \prod_{i=1}^{d} (1 - \boldsymbol{\lambda}^{\alpha_i}).$$

We therefore obtain from Theorem 6.3 (after shifting the grading of K_R) the following result.

6.5. COROLLARY. *Let M be a simplicial submonoid of Φ, and let α_i, β_j be as in Theorem* 6.4. *Let $R = k[M]$. Then the canonical module K_R is given by $k[K_M]$, where $K_M = \{\beta : \beta + \beta_i \in \alpha_1\mathbb{N} + \cdots + \alpha_d\mathbb{N}$ for some $i\}$. Moreover, R is Gorenstein if and only if the β_i's can be labeled so that $\beta_i + \beta_{t+1-i} = \beta_t$, $1 \leqslant i \leqslant t$.* ∎

Invariants of tori. Theorem 6.3 suffers from the defect that the description of K_R is not as explicit as may be desired. For a special class of monoids $M \subset \Phi$ we can give a much more explicit description of K_R. Namely, let $E_1(\mathbf{y}),\ldots, E_r(\mathbf{y})$ be a set of linear forms with integer coefficients in the variables $\mathbf{y} = (y_1,\ldots, y_s)$, and let

$$M = \{\alpha \in \mathbb{N}^s: E_1(\alpha) = \cdots = E_r(\alpha) = 0\}. \tag{20}$$

Let us call a monoid M of the form (20) a *toroidal monoid.* Our reason for this terminology stems from the fact that a monoid $M \subset \Phi$ is toroidal if and only if $k[M]$ is the ring of invariants of some torus $GL(1, k)^d$ acting linearly on the polynomial ring $k[x_1,\ldots, x_s]$ (see [14, p. 319]). By a theorem of Hochster [14, Theorem 1], $k[M]$ is Cohen–Macaulay if M is toroidal. (We also remark that Hochster shows that for a submonoid M of Φ, $k[M]$ is normal if and only if M is isomorphic to a toroidal monoid.)

Let M be a toroidal monoid. Without loss of generality we may assume that there is a vector $\alpha = (\alpha_1,\ldots, \alpha_s) \in M$ satisfying $\alpha_i > 0$ for $1 \leqslant i \leqslant s$. (Simply ignore all coordinates which do not appear in any $\beta \in M$.) We write $\alpha > 0$ for short. We then call M a *positive toroidal monoid.* If M is a positive toroidal monoid, then $\dim k[M]$ is equal to the corank (= number of variables minus the rank) of the system $E_1(\mathbf{y}),\ldots, E_r(\mathbf{y})$.

6.6. THEOREM [30, Theorem 4.1]. *Let M be a positive toroidal monoid. Let $R = k[M]$, and let $d = \dim R$. Then*

$$(-1)^d F(R, 1/\boldsymbol{\lambda}) = \sum_{\alpha} \boldsymbol{\lambda}^{\alpha},$$

where α ranges over all vectors $\alpha \in M$ such that $\alpha > 0$. ∎

For some additional discussion about and generalizations of this theorem, see [31] or [32]. Combining Theorems 6.3 and 6.6, we obtain:

6.7. THEOREM. *Let M be a positive toroidal monoid, and let $R = k[M]$. Then the canonical module K_R is given by $K_R = k[K_M]$, where $K_M = \{\alpha \in M: \alpha > 0\}$.*

Thus R is Gorenstein if and only if there is a unique "minimal" positive element of M, i.e., a unique $\alpha \in M$ such that $\alpha > 0$ and if $\beta \in M$ with $\beta > 0$, then $\beta - \alpha \in M$. (Equivalently, $K_M = \alpha + M$). ∎

Note that if $\alpha = (1, 1,\ldots, 1) \in M$, then this α is the minimal positive element of M so $k[M]$ is Gorenstein. This is the toroidal analog of Corollary 5.6.

We have mentioned that a monoid $M \subset \mathbb{N}^s$ is isomorphic to a toroidal monoid if and only if $k[M]$ is normal, in which case we call M a *normal* monoid. It is easily seen [14, p. 320] that M is normal if and only if the following con-

dition is satisfied: If n is a positive integer and if $\alpha, \beta, \gamma \in M$ satisfy $n\alpha = n\beta + \gamma$, then $\gamma = n\gamma'$ for some $\gamma' \in M$. If M is a normal monoid, define

$$K_M = \{\alpha \in M: \text{ for all } \beta \in M \text{ there is an integer } n > 0 \text{ and an element } \gamma \in M \text{ such that } n\alpha = \beta + \gamma\}. \tag{21}$$

If M is a positive toroidal monoid it is clear that this definition of K_M coincides with the definition given in Theorem 6.7. Since a normal monoid is isomorphic to a positive toroidal monoid, it follows that if M is normal and $R = k[M]$, then $K_R = k[K_M]$, with K_M defined as in (21). This gives a restatement of Theorem 6.7 solely in terms of the abstract structure of M.

References

1. M. F. Atiyah and I. G. MacDonald, "Introduction to Commutative Algebra," Addison–Wesley, Reading, Mass., 1969.
2. B. Bennett, On the characteristic functions of a local ring, *Ann. of Math.* **91** (1970), 25–87.
3. D. A. Buchsbaum and D. Eisenbud, Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3, *Amer. J. Math.* **99** (1977), 447–485.
4. W. Burnside, "Theory of Groups of Finite Order," 2nd ed., Cambridge Univ. Press, 1911; reprinted by Dover, New York, 1955.
5. G. Clements and B. Lindström, A generalization of a combinatorial theorem of Macaulay, *J. Combinatorial Theory* **7** (1969), 230–238.
6. S. Goto, "Remarks on Graded Rings with Application to Certain Monoid Algebras," preprint.
7. S. Goto, N. Suzuki, and K. Watanabe, "On Affine Semigroup Rings," preprint.
8. C. Greene and D. J. Kleitman, Proof techniques in the theory of finite sets, *in* "MAA Studies in Combinatorics" (G.-C. Rota, Ed.), Math. Assoc. of America, Washington D.C., to appear.
9. W. Gröbner, "Moderne Algebraische Geometrie," Springer–Verlag, Vienna, 1949.
10. J. Herzog and E. Kunz, Die Wertehalbgruppe eines lokalen Rings der Dimension 1, *Ber. Heidelberger Akad. Wiss.* 1971 **II** (1971).
11. J. Herzog and E. Kunz (Eds.), "Der kanonische Modul eines Cohen–Macaulay-Rings," Lecture Notes in Mathematics, no. 238, Springer–Verlag, Berlin, 1971.
12. H. Hironaka, Certain numerical characters of singularities, *J. Math. Kyoto Univ.* **10** (1970), 151–187.
13. M. Hochster and J. A. Eagon, Cohen–Macaulay rings, invariant theory, and the generic perfection of determimental loci, *Amer. J. Math.* **93** (1971), 1020–1058.
14. M. Hochster, Rings of invariants of tori, Cohen–Macaulay rings generated by monomials, and polytopes, *Ann. of Math.* **96** (1972), 318–337.
15. W. D. Hodge and D. Pedoe, "Methods of Algebraic Geometry," Vol. II, Cambridge Univ. Press, London/New York, 1968.
16. I. Kaplansky, "Commutative Rings," rev. ed., Univ. of Chicago Press, 1974.
17. S. L. Kleiman and D. Laksov, Schubert calculus, *Amer. Math. Monthly* **79** (1972), 1061–1082.
18. F. S. Macaulay, "The Algebraic Theory of Modular Systems," Cambridge Tracts in Mathematics and Mathematical Physics, No. 19, Cambridge Univ. Press, London, 1916.

19. F. S. MACAULAY, Some properties of enumeration in the theory of modular systems, *Proc. London Math. Soc.* **26** (1927), 531–555.
20. P. A. MACMAHON, "Combinatory Analysis," Vols. 1–2, Cambridge Univ. Press, London, 1915, 1916; reprinted by Chelsea, New York, 1960.
21. C. L. MALLOWS AND N. J. A. SLOANE, On the invariants of a linear group of order 336, *Proc. Cambridge Philos. Soc.* **74** (1973), 435–440.
22. P. MCMULLEN, The number of faces of simplicial polytopes, *Israel J. Math.* **9** (1971), 559–570.
23. T. MOLIEN, Über die Invarianten der Linearen Substitutionsgruppen, *Sitz. König. Preuss. Akad. Wiss.* (1897), 1152–1156.
24. T. POPOVICIU, Studie şi cercetari ştiintifice, *Acad. R.P.R. Filiala Cluj* **4** (1953), 8.
25. I. REITEN, The converse to a theorem of Sharp on Gorenstein modules, *Proc. Amer. Math. Soc.* **32** (1972), 417–420.
26. W. SMOKE, Dimension and multiplicity for graded algebras, *J. Algebra* **21** (1972), 149–173.
27. E. SPERNER, Über einen kombinatorischen Satz von Macaulay und seine Anwendung auf die Theorie der Polynomideale, *Abh. Math. Sem. Univ. Hamburg* **7** (1930), 149–163.
28. R. STANLEY, Theory and application of plane partitions, Parts 1 and 2, *Stud. in Appl. Math.* **50** (1971), 167–188, 259–279.
29. R. STANLEY, Ordered structures and partitions, *Mem. Amer. Math. Soc.* **119** (1972).
30. R. STANLEY, Linear homogeneous diophantine equations and magic labelings of graphs, *Duke Math. J.* **40** (1973), 607–632.
31. R. STANLEY, Combinatorial reciprocity theorems, *Advances in Math.* **14** (1974), 194–253.
32. R. STANLEY, Combinatorial reciprocity theorems, *in* "Combinatorics" (M. Hall, Jr. and J. H. Van Lint, Eds.), Part 2, pp. 107–118, Mathematical Centre Tracts, No. 56, Mathematisch Centrum, Amsterdam, 1974.
33. R. STANLEY, Cohen–Macaulay rings and constructible polytopes, *Bull. Amer. Math. Soc.* **81** (1975), 133–135.
34. R. STANLEY, The upper bound conjecture and Cohen–Macaulay rings, *Stud. in Appl. Math.* **54** (1975), 135–142.
35. R. STANLEY, Some combinatorial aspects of the Schubert calculus, *in* "Proc. Table Ronde, Combinatoire et Représentation du Groupe Symétrique, Strasbourg (26–30 Avril 1976)," Lecture Notes in Mathematics, no. 579, pp. 217–251. Springer, Berlin, 1977.
36. T. SVANES, Coherent cohomology of Schubert subschemes of flag schemes and applications, *Advances in Math.* **14** (1974), 369–453.
37. K. WATANABE, Certain invariant subrings are Gorenstein, I, *Osaka J. Math.* **11** (1974), 1–8.
38. K. WATANABE, Certain invariant subrings are Gorenstein, II, *Osaka J. Math.* **11** (1974), 379–388.
39. F. WHIPPLE, On a theorem due to F. S. Macaulay, *J. London Math. Soc.* **8** (1928), 431–437.