Invent. math. 68, 175-193 (1982)

Inventiones mathematicae
© Springer-Verlag 1982

Linear Diophantine Equations and Local Cohomology

Richard P. Stanley
Massachusetts Institute of Technology, Department of Mathematics,
Cambridge, MA 02139, USA

1. Introduction

What can be said about the set E^α of solutions in nonnegative integers to a system of linear equations with integer coefficients? For many purposes, such as those of linear programming, this question has been adequately answered. However, when this question is regarded from the vantage point of commutative algebra, many additional aspects arise. In particular, there is a natural way to associate with E^α a graded module Λ^α (over an appropriate graded commutative ring Λ), and one can ask for such standard information about Λ^α as its depth, canonical module, etc. We will obtain such information by explicitly computing the Hilbert function of the local cohomology modules $H^i(\Lambda^\alpha)$ associated with Λ^α (with respect to the irrelevant ideal of Λ) in terms of the reduced homology groups of certain polyhedral complexes associated with E^α. This method was suggested by some work of M. Hochster concerning polynomial rings modulo ideals generated by square-free monomials (unpublished by him but discussed in [St_8]), and I am grateful to him for making his ideas available to me. Similar techniques were employed by Goto and Watanabe [G-W] to study arbitrary affine semigroup rings, though they did not consider modules over them.

As a consequence of our computations regarding $H^i(\Lambda^\alpha)$, we can give a general "reciprocity theorem" (Theorem 4.2), whose statement does not involve commutative algebra, connecting the set E^α of nonnegative integral solutions to the set of solutions in negative integers. This generalizes the results in [St_2], where only a special class of equations was considered.

It seems natural to find a purely combinatorial analogue to the algebraic results mentioned above. In Sect. 5 we discuss what we have accomplished along these lines, and offer a general ring-theoretic conjecture which would imply a much more definitive result.

The following notation concerning sets will be used throughout.

0020-9910/82/0068/0175/$03.80

Symbol	*Set*
$\mathbb{N}$	nonnegative integers
$-\mathbb{N}$	nonpositive integers
$\mathbb{P}$	positive integers
$-\mathbb{P}$	negative integers
$\mathbb{R}_+$	nonnegative real numbers
$[p]$	$\{1,2,\dots,p\}$, where $p\in\mathbb{N}$
$[p,q]$	$\{p,p+1,\dots,q\}$, where $p\leqq q$ and $p,q\in\mathbb{Z}$
$S\backslash T$	$\{x\in S\colon x\notin T\}$

The notation $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ is standard. If $\beta=(\beta_1,\dots,\beta_n)\in\mathbb{R}^n$ and $\gamma=(\gamma_1,\dots,\gamma_n)\in\mathbb{R}^n$, then $\beta\leqq\gamma$ means $\beta_i\leqq\gamma_i$ for all i, while $\beta<\gamma$ means $\beta_i<\gamma_i$ for all i. Similarly $\beta\geqq 0$ means $\beta_i\geqq 0$ for all i, and $\beta>0$ means $\beta_i>0$ for all i.

Let us now consider some background material concerning linear equations. Let Φ be an $r\times n$ matrix of integers (or $\mathbb{Z}$-matrix), and assume (without loss of generality in what follows) that rank $\Phi=r$. Let $\alpha\in\mathbb{Z}^r$, regarded as a column vector but written for convenience as a row vector. (We will write all column vectors as row vectors in this paper.) Define

$$E=\{\beta\in\mathbb{N}^n\colon \Phi\beta=0\}$$

$$E^\alpha=\{\beta\in\mathbb{N}^n\colon \Phi\beta=\alpha\}.$$

Hence E is a *submonoid* of $\mathbb{N}^n$ (i.e., closed under addition and containing 0), and E^α is an "E-module" in the sense that $E+E^\alpha\subset E^\alpha$. Here of course $E+E^\alpha=\{\beta+\gamma\colon \beta\in E \text{ and } \gamma\in E^\alpha\}$.

Let k be a field (though much of what we do goes through for an arbitrary commutative ring), and let $A=kE$ denote the monoid algebra of E over k. In order not to confuse the addition operations in E and in A, we will denote by x^β the element of A corresponding to $\beta\in E$. Hence A as a vector space has the basis $\{x^\beta\colon \beta\in E\}$, and multiplication in A is defined by $x^\beta\cdot x^\gamma=x^{\beta+\gamma}$. In fact, define a linear transformation

$$\omega\colon A\to k[x_1,\dots,x_n]$$

by $\omega(x^\beta)=x_1^{\beta_1}\dots x_n^{\beta_n}$, where $\beta=(\beta_1,\dots,\beta_n)$. This is clearly an isomorphism of A onto the subalgebra of $k[x_1,\dots,x_n]$ generated (in fact, spanned) by the monomials $x_1^{\beta_1}\dots x_n^{\beta_n}$. Hence we may regard A as a ring generated by monomials, and may identify x^β with $x_1^{\beta_1}\dots x_n^{\beta_n}$.

Similarly, let A^α denote the vector space with basis $\{x^\beta\colon \beta\in E^\alpha\}$. Then A^α is a A-module is a natural way, viz., if $\beta\in E$ and $\gamma\in E^\alpha$ then define $x^\beta\cdot x^\gamma=x^{\beta+\gamma}\in A^\alpha$.

The ring A and module A^α have an interpretation in terms of invariant theory. Suppose $\Phi=[\gamma_1,\gamma_2,\dots,\gamma_n]$, where γ_i is a column vector of length r. Define

$$T=\{\operatorname{diag}(u^{\gamma_1},u^{\gamma_2},\dots,u^{\gamma_n})\colon u\in(k^*)^r\},$$

where $k^*=k-\{0\}$ and $u^{\gamma_i}=u_1^{\gamma_{i1}}\dots u_r^{\gamma_{ir}}$, and where $u=(u_1,\dots,u_r)$ and $\gamma_i=(\gamma_{i1},\dots,\gamma_{ir})$. Since rank $\Phi=r$, T is a subgroup of $GL_n(k)$ isomorphic to $(k^*)^r$, and hence by definition is an r-dimensional (algebraic) *torus*. T acts in a natural way on the polynomial ring $R=k[x_1,\ldots,x_n]$, viz., if $\tau_u=\operatorname{diag}(u^{\gamma_1},\ldots,u^{\gamma_n})\in T$ then $\tau_u\cdot f(x_1,\ldots,x_n)=f(u^{\gamma_1}x_1,\ldots,u^{\gamma_n}x_n)$. Let

$$R^T=\{f\in R:\tau\cdot f=f \text{ for all } \tau\in T\},$$

the ring of invariants of T acting on R. One sees immediately that $\Lambda=R^T$, so that Λ may be regarded as a ring of invariants. From this observation several facts about Λ are clear. For instance, since T is linearly reductive it follows that Λ is finitely-generated as a k-algebra (e.g. [M]). This was first shown by Hilbert and in a simple combinatorial way by Gordan (see [G-Y, Sect. 151]). We will soon need a refinement of this result. It also follows from [H] or the more general [H-R] that Λ is a Cohen-Macaulay ring. This result will also be a consequence of our work. The reader unfamiliar with Cohen-Macaulay rings may wish to consult [St$_4$].

We also wish to interpret the module Λ^α in terms of invariant theory. Suppose that the equation $\Phi\beta=\alpha$ has at least one *integral* solution $\beta\in\mathbb{Z}^n$. Equivalently, the g.c.d. of all the $j\times j$ minors from any j rows of Φ must equal the g.c.d. of all the $j\times j$ minors from the corresponding j rows of the augmented matrix $[\Phi,\alpha]$. We then call the pair (Φ,α) or the equation $\Phi\beta=\alpha$ *non-trivial*, and henceforth we will automatically assume that (Φ,α) is non-trivial. In this case the map χ_α: $T\to k^*$ defined by $\chi_\alpha(\tau_u)=u^\alpha$ is a one-dimensional representation (or character) of T, and every rational irreducible representation of T is obtained in this way. Now define

$$R^T_{\chi_\alpha}=\{f\in R:\tau\cdot f=\chi_\alpha(\tau)f \text{ for all } \tau\in T\},$$

the module of *semi-invariants* or *relative invariants* of T with respect to the character χ_α. Again it is immediate that $\Lambda^\alpha=R^T_{\chi_\alpha}$. From this one can deduce that Λ^α is a finitely-generated Λ-module, or if preferred a direct combinatorial proof can be given. However, it is not in general true that Λ^α is a Cohen-Macaulay module, and one of our main aims is to give a necessary and sufficient condition for this to be the case.

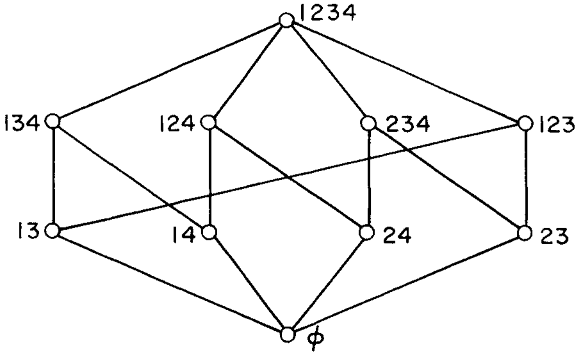
We have mentioned that Λ is a finitely-generated k-algebra (or equivalently, E is a finitely-generated monoid). Define $\beta\in E$ to be *fundamental* if whenever $\beta=\gamma+\delta$ with γ, $\delta\in E$ then $\gamma=0$ or $\delta=0$. The set of all fundamental elements of E is denoted FUND(E). It is easily seen that a subset $G\subset E$ generates E as a monoid if and only if FUND(E)$\subset G$. Hence FUND(E) is the unique minimal set of generators of E, and $\{x^\beta$: $\beta\in$FUND(E)$\}$ is a minimal set of generators of Λ. We need for later purposes, however, a minimal set B of elements of E for which Λ is integral over the subalgebra $k[x^B]=k[x^\beta:\beta\in B]$ generated by x^β, $\beta\in B$. (Equivalently, Λ is a finitely-generated $k[x^B]$-module.) To see that FUND(E) need not coincide with B, let $\Phi=[1,1,-2]$. Then FUND(E) $=\{(2,0,1),(0,2,1),(1,1,1)\}$, but we may take $B=\{(2,0,1),(0,2,1)\}$. This leads us to define an element $\beta\in E$ to be *completely fundamental* if whenever $m\beta=\gamma+\delta$ where $m\geq 1$ and γ, $\delta\in E$, then $\gamma=i\beta$ for some $0\leq i\leq m$. Let $CF(E)$ denote the set of completely fundamental elements of E.

1.1 Proposition. *Let B be any subset of E. Then Λ is integral over $k[x^B]$ if and only if B contains a non-zero multiple of every element of $CF(E)$.* □

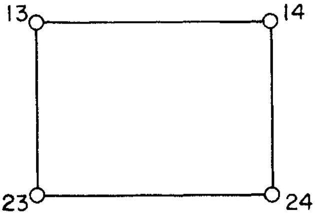
The proof is an easy consequence of [St$_1$, Lemma 2.4].

It is useful in what follows to view the set $CF(E)$ geometrically. Let $\mathscr{C}=\mathscr{C}_\Phi$ denote the set of all solutions $\beta\in\mathbb{R}^n_+$ to $\Phi\beta=0$. Thus $\mathscr{C}$ is an $(n-r)$-dimensional convex polyhedral cone in $\mathbb{R}^n$, with unique vertex at the origin. Let $\mathscr{P}=\mathscr{P}_\Phi$ denote any non-degenerate cross-section of $\mathscr{C}$ (e.g. $\mathscr{C}\cap\{(\beta_1,\ldots,\beta_n)\in\mathbb{R}^n: \Sigma\beta_i=1\}$). Thus $\mathscr{P}$ is an $(n-r-1)$-dimensional convex polytope (or $(n-r-1)$-polytope, for short), and any other non-degenerate cross-section of $\mathscr{C}$ is combinatorially equivalent to $\mathscr{P}$. An i-dimensional face $\mathscr{F}$ of $\mathscr{P}$ will be called an *i-face*. If $\beta=(\beta_1,\ldots,\beta_n)\in\mathbb{R}^n_+$, define the *support* of β by $\operatorname{supp}\beta=\{i: \beta_i>0\}$; and if $\beta=(\beta_1,\ldots,\beta_n)\in\mathbb{R}^n$, define the *negative support* of β by $\operatorname{supp}_-\beta=\{i: \beta_i<0\}$. If $\mathscr{F}$ is a face of $\mathscr{P}$, then all elements of the relative interior $\mathscr{F}^\circ$ of $\mathscr{F}$ have the same support, which we denote by $\operatorname{supp}\mathscr{F}$. It follows that the faces of $\mathscr{P}$ are in one-to-one correspondence with the supports of elements $\beta\in E$, and that two faces $\mathscr{F},\mathscr{G}$ satisfy $\mathscr{F}\subset\mathscr{G}$ if and only if $\operatorname{supp}\mathscr{F}\subset\operatorname{supp}\mathscr{G}$. If v is a vertex ($=0$-dimensional face) of $\mathscr{P}$, then those elements $\beta\in E$ satisfying $\operatorname{supp}\beta=\operatorname{supp}v$ are $\mathbb{N}$-multiples of a unique element $\beta_v\in E$. We leave to the reader to verify that $\{\beta_v: v$ is a vertex of $\mathscr{P}\}=CF(E)$. In other words, $CF(E)$ consists of those non-zero points β of E which lie on an extreme ray of $\mathscr{C}$ and for which no other points of E lie on the line segment joining 0 and β.

1.2 *Example.* Let $\Phi=[1,1,-1,-1]$. The supports of elements of E consist of the sets $\emptyset$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{2,4\}$, $\{1,2,3\}$, $\{1,2,4\}$, $\{1,3,4\}$, $\{2,3,4\}$, $\{1,2,3,4\}$. Hence the lattice of faces of $\mathscr{P}$ is given by



so $\mathscr{P}$ is a quadrilateral:



(1)

The vertices 13, 14, 23, 24 correspond to the completely fundamental elements 1010, 1001, 0110, 0101, respectively. □

The ring Λ and module Λ^α have in a natural way the structure of an $\mathbb{N}^n$-graded k-algebra and $\mathbb{Z}^n$-graded Λ-module respectively. Namely, we have the vector space direct sums

$$\Lambda = \coprod_{\beta\in E} \Lambda_\beta, \qquad \Lambda^\alpha = \coprod_{\beta\in E^\alpha} \Lambda^\alpha_\beta,$$

where Λ_β (respectively, Λ^α_β) denotes the one-dimensional vector space spanned by x^β for $\beta\in E$ (respectively, $\beta\in E^\alpha$). The *Hilbert series* of Λ and Λ^α are defined to be the formal power series

$$F(\Lambda, x) = \sum_{\beta\in E} x^\beta \in \mathbb{Z}[[x_1, \dots, x_n]]$$

$$F(\Lambda^\alpha, x) = \sum_{\beta\in E^\alpha} x^\beta \in \mathbb{Z}[[x_1, \dots, x_n]],$$

where if $\beta=(\beta_1, \dots, \beta_n)$ then $x^\beta = x_1^{\beta_1} \cdots x_n^{\beta_n}$. It follows from general facts about Hilbert series that $F(\Lambda, x)$ and $F(\Lambda^\alpha, x)$ represent rational functions of $x =(x_1, \dots, x_n)$. (This is because Λ is a finitely-generated k-algebra and Λ^α a finitely-generated Λ-module.) We should point out [St$_1$, Thm. 2.5], though we don't need this fact, that when $F(\Lambda, x)$ and $F(\Lambda^\alpha, x)$ are reduced to lowest terms (and assuming as always (Φ, α) is non-trivial) then they both have denominator $\prod_{\beta\in CF(E)} (1-x^\beta)$.

We conclude this section with a description of the Krull dimension of Λ and Λ^α. One can define $\dim \Lambda$ to be the maximal number of elements of Λ which are algebraically independent over k, and similarly we can set $\dim \Lambda^\alpha = \dim(\Lambda/\operatorname{Ann} \Lambda^\alpha)$ where $\operatorname{Ann} \Lambda^\alpha = \{f\in\Lambda \mid f\cdot\Lambda^\alpha = 0\}$. Clearly $\operatorname{Ann}\Lambda^\alpha=0$ (since (Φ, α) is non-trivial), so $\dim\Lambda^\alpha = \dim\Lambda$. Now a set $x^\beta, x^\gamma, \dots$ of monomials is algebraically independent if and only if the vectors $\beta, \gamma, \dots$ are linearly independent (over $\mathbb{R}$, say). Hence $\dim \Lambda$ is equal to any of the following quantities:

(i) the dimension of the real vector space $\mathbb{R}E$ spanned by E, regarded as a subset of $\mathbb{R}^n$,

(ii) the dimension of the cone $\mathscr{C}$,

(iii) the rank of the (free) abelian group $\mathbb{Z}E$ generated by E, regarded as a subset of $\mathbb{Z}^n$.

We will always denote $\dim \Lambda$ by the symbol d. If d' is the rank of the abelian group of all $\mathbb{Z}$-solutions β to $\Phi\beta=0$, then note that $d \leqq d'$, with equality if and only if there exists a $\mathbb{P}$-solution to $\Phi\beta=0$ (i.e., $E\cap\mathbb{P}^n \neq \emptyset$).

2. Local Cohomology

Let Λ_+ denote the irrelevant maximal ideal of Λ, i.e., the ideal generated (or spanned) by all monomials $x^\beta\in\Lambda$ with $\beta\neq 0$. Let $H^i(\Lambda^\alpha)$ denote the i^{th} local cohomology module of Λ^α with respect to the ideal Λ_+. (The usual notation is $H^i_{\Lambda_+}(\Lambda^\alpha)$, but we suppress Λ_+.) There are several equivalent ways of defining $H^i(\Lambda^\alpha)$ (see, e.g., [H-R, Sect. 5]). The definition which will be most useful for our purposes is the following [H-R, p. 133]. Let $y_1, \dots, y_s$ be any set of elements of Λ for which $\operatorname{rad}(y_1, \dots, y_s) = \Lambda_+$, i.e., for which $\Lambda_+^t \subset (y_1, \dots, y_s)$ for some $t > 0$. Let $\Lambda_{y_i} = y_i^{-1}\Lambda$ denote the ring of fractions of Λ with respect to y_i (or more accurately, with respect to the multiplicative set generated by y_i), and denote by $\mathcal{K}(y^\infty, \Lambda^\alpha)$ the complex

$$\bigotimes_{i=1}^{s} (0 \to \Lambda \to \Lambda_{y_i} \to 0) \otimes \Lambda^\alpha$$

$$= 0 \xrightarrow{\delta_0} \Lambda^\alpha \xrightarrow{\delta_1} \coprod_i \Lambda^\alpha_{y_i} \xrightarrow{\delta_2} \coprod_{i<j} \Lambda^\alpha_{y_i y_j} \xrightarrow{\delta_3} \dots \xrightarrow{\delta_s} \Lambda^\alpha_{y_1 \dots y_s} \to 0. \quad (2)$$

The map δ_{j+1} has the following explicit description. Let $u \in \Lambda^\alpha_{y_{i_1} y_{i_2} \dots y_{i_j}} = M$. Let $\{1, 2, , \dots, s\} \setminus \{i_1, i_2, \dots, i_j\} = \{\ell_1, \ell_2, \dots, \ell_{s-j}\}$, with $\ell_1 < \ell_2 < \dots < \ell_{s-j}$. Let ϕ_{ℓ_r}: $M \to M_{y_{\ell_r}}$ be the natural map (here an injection), for $1 \leqq r \leqq s-j$. Then

$$\delta_{j+1}(u) = \sum_{r=1}^{s-j} (-1)^{r-1} \phi_{\ell_r}(u). \quad (3)$$

We now define $H^i(\Lambda^\alpha)$ to be the i^{th} cohomology module of the complex $\mathcal{K}(y^\infty, \Lambda^\alpha)$, i.e.,

$$H^i(\Lambda^\alpha) = H^i(\mathcal{K}(y^\infty, \Lambda^\alpha)) = \ker \delta_{i+1} / \operatorname{im} \delta_i. \quad (4)$$

This definition is independent of the choice of $y_1, \dots, y_s$ (provided $\Lambda_+ = \operatorname{rad}(y_1, \dots, y_s)$). We will always choose $y_i = x^{\beta^i}$, where $\beta^1, \dots, \beta^r$ is some specified ordering of $CF(E)$. By Proposition 1.1, we indeed have in this case that $\Lambda_+ = \operatorname{rad}(y_1, \dots, y_s)$. Since the elements x^β are $\mathbb{N}^n$-homogeneous, each $H^i(\Lambda^\alpha)$ inherits from (4) the structure of a $\mathbb{Z}^n$-graded Λ-module. In other words, we have a direct sum decomposition

$$H^i(\Lambda^\alpha) = \coprod_{\beta \in \mathbb{Z}^n} H^i(\Lambda^\alpha)_\beta,$$

where $\Lambda_\gamma \cdot H^i(\Lambda^\alpha)_\beta \subset H^i(\Lambda^\alpha)_{\gamma+\beta}$. The modules $H^i(\Lambda^\alpha)$ are not in general finitely-generated, but we do have $\dim_k H^i(\Lambda^\alpha)_\beta < \infty$. Hence we can define the Hilbert series

$$F(H^i(\Lambda^\alpha), x) = \sum_{\beta \in \mathbb{Z}^n} (\dim_k H^i(\Lambda^\alpha)_\beta) x^\beta.$$

It is well-known that $H^i(\Lambda^\alpha)$ is an *artinian* Λ-module (though not necessarily of finite length). It follows that there exists a vector $\gamma \in \mathbb{N}^n$ for which

$$x^{-\gamma} F(H^i(\Lambda^\alpha), x) \in \mathbb{Z}[[x_1^{-1}, \dots, x_n^{-1}]].$$

Part of the importance of local cohomology stems from its depth sensitivity. A proof of this fundamental result (which we simply state for the case Λ^α at hand) may be found e.g. in [H-K, Satz 4.10 and 4.12].

2.1 **Theorem.** *Let* $e = \operatorname{depth} \Lambda^\alpha$ *and (as usual)* $d = \dim \Lambda$. *Then* $H^i(\Lambda^\alpha) = 0$ *unless* $e \leqq i \leqq d$. *Moreover* $H^e(\Lambda^\alpha) \neq 0$ *and* $H^d(\Lambda^\alpha) \neq 0$. □

We also record for later use the relationship between the Hilbert series of Λ^α and of $H^i(\Lambda^\alpha)$. If $F(x)$ is any rational function of $x=(x_1,\dots,x_n)$ possessing a Laurent series expansion about 0, then denote by $F(x)_\infty$ the Laurent series expansion of $F(x)$ about ∞ (i.e., which converges in some deleted neighborhood of ∞). For example, if $F(x)=\frac{1}{1-x}=-\frac{x^{-1}}{1-x^{-1}}$, then $F(x)_\infty=-\sum_{m\leqq -1} x^m$.

2.2 **Theorem.** *Let* $e=\operatorname{depth}\Lambda^\alpha$ *and* $d=\dim\Lambda^\alpha$ *as above. Then*

$$F(\Lambda^\alpha,x)_\infty=\sum_{i=e}^{d}(-1)^i F(H^i(\Lambda^\alpha),x). \quad \square \tag{5}$$

Perhaps the easiest way to verify this theorem (which is widely known though not conspicuously published) is to observe that both sides of (5) are additive functions (in the category of $\mathbb{Z}^n$-graded Λ-modules) and agree on free modules.

Now that we have disposed of the general facts we shall need concerning local cohomology, let us return to the subject of this paper. The following notation will be used. If $S\subset CF(E)$, then $\Lambda_S^\alpha=S^{-1}\Lambda^\alpha$ denotes the module of fractions of Λ^α with respect to the (multiplicative set generated by the) monomials x^β for $\beta\in S$. (There should be no confusion with the homogeneous component Λ_β^α, where $\beta\in\mathbb{Z}^n$.) Define $\mathscr{F}_S$ to be the face of $\mathscr{P}$ satisfying

$$\operatorname{supp}\mathscr{F}_S=\bigcup_{\beta\in S}\operatorname{supp}\beta.$$

If $\gamma\in\mathbb{Z}^n$, then $(\Lambda_S^\alpha)_\gamma$ denotes the γ-homogeneous part of Λ_S^α. We write $\bar{E}$ for the abelian group generated by $E\subset\mathbb{Z}^n$, and $\bar{E}^\alpha$ for the coset of $\bar{E}$ in $\mathbb{Z}^n$ containing E^α.

2.3 **Lemma.** *Let* $S\subset CF(E)$. *Then*

$$\dim_k(\Lambda_S^\alpha)_\gamma=\begin{cases}1, & \text{if } \gamma\in\bar{E}^\alpha \text{ and } \operatorname{supp}_-\gamma\subset\operatorname{supp}\mathscr{F}_S\\ 0, & \text{otherwise.}\end{cases}$$

Proof. Suppose $(\Lambda_S^\alpha)_\gamma\neq 0$. Then there are integers a_β for $\beta\in S$ and an element $\delta\in E^\alpha$ such that

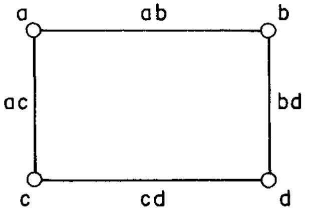
$$\gamma=\delta+\sum_{\beta\in S}a_\beta\cdot\beta. \tag{6}$$

Conversely, if γ can be written as (6) then $\dim_k(\Lambda_S^\alpha)_\gamma=1$. But γ can be written as (6) if and only if $\gamma\in\bar{E}^\alpha$ and $\operatorname{supp}_-\gamma\subset\bigcup_{\beta\in S}(\operatorname{supp}_-\beta)=\operatorname{supp}\mathscr{F}_S$, and the proof follows. $\square$

Now given $\gamma\in\bar{E}_\alpha$, define Δ_γ to be the abstract simplicial complex whose faces are those sets $S\subset CF(E)$ such that

$$\operatorname{supp}_-\gamma\subset\bigcup_{\delta\in CF(E)\setminus S}(\operatorname{supp}\delta)=\operatorname{supp}\mathscr{F}_{CF(E)\setminus S}.$$

2.4 *Example.* Let $\Phi=[1,1,-1,-1]$, $\alpha=2$, and $\gamma=(0,0,-1,-1)$. Let $a=(1,0,1,0)$, $b=(1,0,0,1)$, $c=(0,1,0,1)$, $d=(0,1,1,0)$, so $CF(E)=\{a,b,c,d\}$. Then $\operatorname{supp}_-\gamma=\{3,4\}$ and Δ_γ is given by



The crucial result for our analysis of $H^i(\Lambda^\alpha)$ is the following.

2.5 **Lemma.** *Let $\gamma\in\bar{E}^\alpha$. Restrict the complex $\mathscr{K}(y^\infty,\Lambda^\alpha)$ to its γ-homogeneous part, obtaining a complex $\mathscr{K}(y^\infty,\Lambda^\alpha)_\gamma$ of finite-dimensional vector spaces. Orient the simplicial complex Δ_γ by ordering the vertex set $CF(E)$ as $\beta^1<\dots<\beta^s$, where $y_i=x^{\beta^i}$. Then the complex $\mathscr{K}(y^\infty,\Lambda^\alpha)_\gamma$ is isomorphic to the augmented oriented chain complex $\tilde{C}(\Delta_\gamma)$ of Δ_γ (with coefficients in k), up to a shift in grading.*

Proof. Let $|CF(E)|=s$, and set

$$K_i=\coprod_{\substack{S\subset CF(E)\\ |S|=s-i-1}}(\Lambda_S^\alpha)_\gamma.$$

Hence $\mathscr{K}(y^\infty,\Lambda^\alpha)_\gamma$ has the form

$$0\to K_{s-1}\xrightarrow{\partial_{s-1}}\dots\xrightarrow{\partial_1}K_0\xrightarrow{\partial_0}K_{-1}\to 0$$

By Lemma 2.3, $(\Delta_S^\alpha)_\gamma=0$ unless $\operatorname{supp}_-\gamma\subset\operatorname{supp}\mathscr{F}_S$, and $\dim_k(\Lambda_S^\alpha)_\gamma=1$ if $\operatorname{supp}_-\gamma\subset\operatorname{supp}\mathscr{F}_S$. If x_S^γ denotes the obvious generator for $(\Lambda_S^\alpha)_\gamma$ (as a vector space), then we can identify $\pm x_S^\gamma$ with the face $CF(E)\backslash S$ of Δ_γ. In this way K_i can be identified with the space $\tilde{C}_i(\Delta_\gamma)$ of i-chains of Δ_γ (including the case $i=-1$, where we take a "-1-chain" to be a scalar multiple of the null set).

It remains to show that ∂_i coincides with the boundary map ∂_i': $\tilde{C}_i(\Delta_\gamma)\to\tilde{C}_{i-1}(\Delta_\gamma)$. Let $[v_0,v_1,\dots,v_i]\in\tilde{C}_i(\Delta_\gamma)$ denote the oriented simplex with vertex set $\{v_0,v_1,\dots,v_i\}$. Recall (e.g., [Sp, p. 159]) that ∂_i' is defined by

$$\partial_i'[v_0,v_1,\dots,v_i]=\sum_{j=0}^{i}(-1)^j[v_0,v_1,\dots,\hat{v}_j,\dots,v_i],$$

where $\hat{v}_j$ denotes that v_j is missing. Comparison with (3) yields $\partial_i=\partial_i'$ when the right sign of $\pm x_S^\gamma$ is chosen, as desired. □

Let us denote the reduced homology groups of Δ_γ by $\tilde{H}_i(\Delta_\gamma)$. It is understood that the coefficient group is always k. We remind the reader that for the null set $\emptyset$ we have

$$\tilde{H}_i(\emptyset)\cong\begin{cases}0, & i\neq-1\\ k, & i=-1.\end{cases}$$

2.6 **Corollary.** *Let $\gamma\in\mathbb{Z}^n$. Then*

$$\dim_k H^i(\Lambda^\alpha)_\gamma=\begin{cases}0, & \text{if } \gamma\notin\bar{E}^\alpha\\ \dim_k\tilde{H}_{s-i-1}(\Delta_\gamma), & \text{if } \gamma\in\bar{E}^\alpha.\ \square\end{cases}$$

While Corollary 2.6 in a sense "determines" the Hilbert function of $H^i(\Lambda^\alpha)$ and thus in particular depth Λ^α, it is not a very practical result because of the difficulty of computing $\tilde{H}(\Delta_\gamma)$. What we need to do is replace Δ_γ by a more tractable object. To this end, let $\mathscr{P}^*$ denote the dual polytope to $\mathscr{P}$. There is thus a one-to-one inclusion-reversing correspondence $\mathscr{F}\mapsto\mathscr{F}^*$ between the faces $\mathscr{F}$ of $\mathscr{P}$ and $\mathscr{F}^*$ of $\mathscr{P}^*$, satisfying

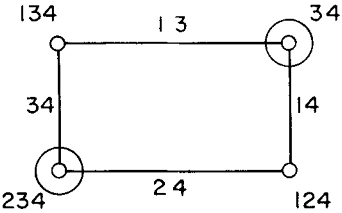
$$\dim\mathscr{F}+\dim\mathscr{F}^*=(\dim\mathscr{P})-1.$$

Given $\gamma\in\bar{E}^\alpha$, define a subset Γ_γ of $\mathscr{P}^*$ by

$$\Gamma_\gamma=\bigcup\{\mathscr{F}^*\colon \mathscr{F} \text{ is a face of } \mathscr{P} \text{ satisfying } \operatorname{supp}_-\gamma\subset\operatorname{supp}\mathscr{F}\} \tag{7}$$

Γ_γ has the structure of a polyhedral complex whose faces (or cells) are certain faces of $\mathscr{P}^*$; it is a subcomplex of the polytope $\mathscr{P}^*$.

2.7 *Example.* Let Φ, α, and γ be as in Example 2.4. $\mathscr{P}$ is given by (1). The faces $\mathscr{F}$ whose support contains $\{3,4\}=\operatorname{supp}_-\gamma$ are the edges joining 13 to 14, 23 to 24, together with $\mathscr{P}$ itself. Hence Γ_γ consists of the two disjoint vertices of $\mathscr{P}^*$ circled below:



$\mathscr{P}^*$

We now come to a crucial topological lemma which will lead to a significant simplification of Corollary 2.6.

2.8 **Lemma.** *Let $d=\dim\Lambda^\alpha$ and $s=|CF(E)|$, as usual. Then for all i,*

$$\tilde{H}_i(\Gamma_\gamma)\cong\tilde{H}_{s-d+i}(\Delta_\gamma),$$

where $\tilde{H}_i(\Gamma_\gamma)$ denotes reduced singular homology (with coefficient group k).

Proof. Let $L(\mathscr{P}^*)$ denote the poset of proper faces of $\mathscr{P}^*$ (i.e., excluding $\emptyset$ and $\mathscr{P}^*$), ordered by inclusion. Let $L(\Gamma_\gamma)=\{\mathscr{F}^*\in L(\mathscr{P}^*)\colon \mathscr{F}^*\subset\Gamma_\gamma\}$. Regard the posets $L(\mathscr{P}^*)$, $L(\Gamma_\gamma)$, and $L(\mathscr{P}^*)\backslash L(\Gamma_\gamma)$ as simplicial complexes whose faces are the chains of the corresponding poset. Now $L(\mathscr{P}^*)$ and $L(\Gamma_\gamma)$, regarded as simplicial complexes, are just the first barycentric subdivisions $sd(\partial\mathscr{P}^*)$ and $sd(\Gamma_\gamma)$ of $\partial\mathscr{P}^*$ and Γ_γ, regarded as polyhedral complexes. Hence the geometric realization

$|L(\mathscr{P}^*)|$ of $L(\mathscr{P}^*)$ is a $(d-2)$-sphere. By Alexander duality,

$$\tilde{H}_i(\Gamma_\gamma)\cong\tilde{H}_{d-i-3}(L(\mathscr{P}^*)\backslash L(\Gamma_\gamma)). \tag{8}$$

(Since we are working with field coefficients, homology and cohomology coincide.) Let Π_γ denote the collection of all subsets of maximal elements $(=(d-2)$-faces) of $L(\mathscr{P}^*)\backslash L(\Gamma_\gamma)$ whose intersection is not contained in $L(\Gamma_\gamma)$. Thus Π_γ is a simplicial complex on the vertex set $CF(E)$. By a theorem of Folkman [F] (see also [L] [B, Thm. 2.3] [W, Thm. 5.9]), Π_γ and $L(\mathscr{P}^*)\backslash L(\Gamma_\gamma)$ have isomorphic reduced homology (in fact, the same homotopy type), so

$$\tilde{H}_{d-i-3}(L(\mathscr{P}^*)\backslash L(\Gamma_\gamma))\cong\tilde{H}_{d-i-3}(\Pi_\gamma). \tag{9}$$

Let Ω denote the boundary complex of the abstract simplex on the vertex set $CF(E)$ (i.e., Ω consists of all subsets of $CF(E)$ except $CF(E)$ itself). By definition of Δ_γ and Γ_γ, we have

$$\Delta_\gamma=\{S\subset CF(E)\colon CF(E)\backslash S\not\subset\Pi\}.$$

Since $|\Omega|$ is an $(s-1)$-sphere, again by Alexander duality we have $\tilde{H}_i(\Delta_\gamma)\cong\tilde{H}_{s-3-i}(\Pi_\gamma)$, or equivalently

$$\tilde{H}_{s-d+i}(\Delta_\gamma)\cong\tilde{H}_{d-i-3}(\Pi_\gamma). \tag{10}$$

Combining (8), (9), and (10) completes the proof. □

Although not relevant to us here, the preceding lemma suggests the following conjecture.

2.9 **Conjecture.** *The spaces $|\Delta_\gamma|$ and $|\Sigma^{s-d}\Gamma_\gamma|$ have the same homotopy type, where Σ^{s-d} denotes the $(s-d)$-fold suspension.*

From Corollary 2.5 and Lemma 2.8 we deduce the main result of this paper.

2.10 **Theorem.** *Let $d=\dim\Lambda$. Then*

$$F(H^i(\Lambda^\alpha),x)=\sum_{\gamma\in\bar{E}^\alpha}(\dim_k\tilde{H}_{d-1-i}(\Gamma_\gamma))\,x^\gamma. \quad □$$

Recall that a topological space Γ is *acyclic* (over k) if $\tilde{H}_i(\Gamma)=0$ for all i. The null set is not acyclic since $\tilde{H}_{-1}(\emptyset)\cong k$. Since Λ^α is Cohen-Macaulay if and only if $H^i(\Lambda^\alpha)=0$ (equivalently, $F(H^i(\Lambda^\alpha),x)=0$) for $i\neq d$, we deduce from Theorem 2.10 a criterion for Λ^α to be Cohen-Macaulay.

2.11 **Corollary.** *The following two conditions are equivalent:*

(i) Λ^α is Cohen-Macaulay,

(ii) for all $\gamma\in\bar{E}^\alpha$, either $\Gamma_\gamma=\emptyset$ or Γ_γ is acyclic. □

To supplement Corollary 2.11, we collect a few observations on what it means for Γ_γ to be void.

2.12 **Proposition.** *Let $\gamma \in \bar{E}_\alpha$. Then:*

(a) $\Gamma_\gamma = \emptyset$ if and only if the only face $\mathscr{F}$ of $\mathscr{P}$ satisfying $\operatorname{supp}_-\gamma \subset \operatorname{supp} \mathscr{F}$ *is $\mathscr{P}$ itself.*

(b) If $\alpha = 0$, then

$$\Gamma_\gamma = \emptyset \Leftrightarrow \operatorname{supp}_-\gamma = \operatorname{supp} \mathscr{P}.$$

(c) Let $\alpha = 0$, and suppose there exists a $\mathbb{P}$-solution to $\Phi\beta = 0$, i.e., $E \cap \mathbb{P}^n \neq \emptyset$. Then

$$\Gamma_\gamma = \emptyset \Leftrightarrow \gamma \in (-\mathbb{P})^n.$$

Proof. (a) is an immediate consequence of the definition of Γ_γ. Now suppose $\alpha = 0$. To prove (b), we must show that if $\Phi\gamma = 0$ and $\operatorname{supp}_-\gamma \neq \operatorname{supp} \mathscr{P}$, then $\operatorname{supp}_-\gamma \subset \operatorname{supp} \mathscr{F}$ for some *proper* face of $\mathscr{P}$. Let $\beta \in E$ satisfy $\operatorname{supp} \beta = \operatorname{supp} \mathscr{P}$. Let $c = p/q$ be the least rational number for which $-\gamma + c\beta \geqq 0$, where $q \in \mathbb{P}$. Set $\delta = q(-\gamma + c\beta)$. Then $\delta \in E$ and $\operatorname{supp} \delta \neq \operatorname{supp} \mathscr{P}$, since $\operatorname{supp}_-\gamma \neq \operatorname{supp} \mathscr{P}$. But $\operatorname{supp}_-\gamma \subset \operatorname{supp} \delta$, so the proof of (b) follows. (c) is an immediate consequence of (b) since $E \cap \mathbb{P}^n \neq \emptyset \Leftrightarrow \operatorname{supp} \mathscr{P} = [n]$. □

Note that Proposition 2.12(b) is false if $\alpha \neq 0$. For instance, take $\Phi = [1, -1]$, $\alpha = 1$, $\gamma = (0, -1)$. Then $\Gamma_\gamma = \emptyset$, yet $\operatorname{supp}_-\gamma = \{2\} \neq \{1, 2\} = \operatorname{supp} \mathscr{P}$.

3. Applications

We certainly would like to be able to deduce Hochster's result that A is a Cohen-Macaulay ring from Corollary 2.11.

3.1 **Theorem.** *The ring A is Cohen-Macaulay.*

Proof. Let $\gamma \in \bar{E}$. By Corollary 2.11, we need to show that either Γ_γ is acyclic or $\Gamma_\gamma = \emptyset$. There are three cases.

Case 1. $\gamma \in E$. Then $\operatorname{supp}_-\gamma = \emptyset$ so $\Gamma_\gamma = \mathscr{P}^*$, which is acyclic.

Case 2. $\operatorname{supp}_-\gamma = \operatorname{supp} \mathscr{P}$. By Proposition 2.12(b), this is the condition for $\Gamma_\gamma = \emptyset$.

Case 3. $\gamma \notin E$ and $\operatorname{supp}_-\gamma \neq \operatorname{supp} \mathscr{P}$. Let $\mathbb{R}\mathscr{C}$ be the d-dimensional vector space spanned by the cone $\mathscr{C}$. Let $\mathscr{H}$ be a hyperplane (of dimension $d-1$) in $\mathbb{R}\mathscr{C}$ which separates γ from $\mathscr{C}$. Let $\mathscr{C}_\gamma$ be the portion of $\mathscr{C}$ "visible" from γ, where $\mathscr{C}$ is regarded as opaque, i.e.,

$$\mathscr{C}_\gamma = \{\beta \in \mathscr{C}\colon \text{the line segment } \ell(\gamma, \beta) \text{ joining } \gamma \text{ and } \beta \text{ intersects } \mathscr{C} \text{ only in } \beta\}.$$

The map $\mathscr{C}_\gamma \xrightarrow{\psi} \mathscr{H}$ which sends β to the unique element of $\ell(\gamma, \beta) \cap \mathscr{H}$ is a homeomorphism from $\mathscr{C}_\gamma$ to $\psi(\mathscr{C}_\gamma)$. Since $\mathscr{C}$ is convex of dimension d, $\psi(\mathscr{C}_\gamma)$ is a $(d-1)$-dimensional convex subset of $\mathscr{H}$. Since $\operatorname{supp}_-\gamma \neq \operatorname{supp} \mathscr{P}$, it follows that $\psi(\mathscr{C}_\gamma)$ is a convex cone whose vertex is $\psi(0)$, where 0 is the vertex of $\mathscr{C}$. A cross-section of $\psi(\mathscr{C}_\gamma)$ is therefore a $(d-2)$-dimensional ball. But such a cross-section is homeomorphic to the portion $\mathscr{P}_\gamma = \mathscr{P} \cap \mathscr{C}_\gamma$ of $\mathscr{P}$ visible from γ, so $\mathscr{P}_\gamma$ is acyclic.

Now let $L(\mathscr{P})$ denote the poset of proper faces of $\mathscr{P}$, regarded as a simplicial complex as in Lemma 2.8. The subposet $L(\mathscr{P}_\gamma)$ consisting of all non-void faces of $\mathscr{P}_\gamma$ is isomorphic, as a simplicial complex, to the barycentric subdivision $sd(\mathscr{P}_\gamma)$. The complementary poset $L(\mathscr{P})\backslash L(\mathscr{P}_\gamma)$ is isomorphic to $sd(\Gamma_\gamma)$, since the faces $\mathscr{F}$ of $\mathscr{P}$ not visible from γ are precisely those which satisfy $\mathrm{supp}_-\gamma \subset \mathrm{supp}\,\mathscr{F}$. Since $\mathscr{P}_\gamma$ is acyclic, so is $sd(\mathscr{P}_\gamma)$. It follows from Alexander duality that $sd(\Gamma_\gamma)$, and therefore Γ_γ, is also acyclic. □

The main idea of the above proof, that of considering the portion of $\mathscr{P}$ visible from γ, was also used in the proof of [St$_2$, Prop. 8.3]. With a little more care, we can adapt the preceding proof to give a relatively tractable sufficient (but not necessary) condition for Λ^α to be Cohen-Macaulay. A completely different proof of a somewhat more general result appears in [St$_5$, Thm. 3.5].

3.2 **Theorem.** *Suppose there exists a rational (or equivalently, real) solution $\beta = (\beta_1, \dots, \beta_n)$ to $\Phi\beta = \alpha$ satisfying $-1 < \beta_i \leqq 0$. Then Λ^α is Cohen-Macaulay.*

Proof. Let $\gamma \in \bar{E}^\alpha$, and let $q \in \mathbb{P}$ satisfy $q\beta \in \mathbb{Z}^n$. Then $q(\gamma - \beta) \in \bar{E}$. Since $-1 < \beta_i \leqq 0$, we have $\mathrm{supp}_-\gamma = \mathrm{supp}_- q(\gamma - \beta)$. Since by definition the space Γ_δ depends only on $\mathrm{supp}_-\delta$, we have $\Gamma_\gamma = \Gamma_{q(\gamma-\beta)}$. By Corollary 2.11 and Theorem 3.1, $\Gamma_{q(\gamma-\beta)}$ is void or acyclic, so the same is true of Γ_γ. Hence by Corollary 2.11, Λ^α is Cohen-Macaulay. □

The example $\Phi = [1, -1]$, $\alpha = 1$, shows that the converse to Theorem 3.2 is false.

While Theorem 2.10 is rather unwieldy for computing depth Λ^α for arbitrary (Φ, α), it can be used to give a simple formula for depth Λ^α when $r = 1$ (i.e., when Φ has just one row, or when the torus T is one-dimensional).

3.3. **Theorem.** *Let $a_1, \dots, a_s, b_1, \dots, b_t \in \mathbb{P}$, where $s, t > 0$. Let $\Phi = [a_1, \dots, a_s, -b_1, \dots, -b_t]$, and choose $\alpha \in \mathbb{Z}$. If $\beta = (\beta_1, \dots, \beta_{s+t}) \in \mathbb{Z}^{s+t}$, then let $\beta' = (\beta_1, \dots, \beta_s)$, $\beta'' = (\beta_{s+1}, \dots, \beta_{s+t})$. Let $0 \leqq i < d = \dim \Lambda = s + t - 1$. Then*

$$F(H^i(\Lambda^\alpha), x) = \begin{cases} \displaystyle\sum_{\substack{\beta \in \bar{E}^\alpha \\ \beta' < 0,\, \beta'' \geqq 0}} x^\beta, & \text{if } i = s \\ \displaystyle\sum_{\substack{\beta \in \bar{E}^\alpha \\ \beta' \geqq 0,\, \beta'' < 0}} x^\beta, & \text{if } i = t \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Note that $S \subset [s+t]$ is the support of some nonvoid face $\mathscr{F}$ of $\mathscr{P}$ if and only if $S \cap [s] \neq \emptyset$ and $S \cap [s+1, s+t] \neq \emptyset$. Let $\beta \in \bar{E}^\alpha$. We need to compute $\tilde{H}_i(\Gamma_\beta)$.

Case 1: $\mathrm{supp}_-\beta = [s+1, s+t]$, i.e., $\beta' \geqq 0$, $\beta'' < 0$. By the definition (7) of Γ_β, a face $\mathscr{F}^*$ of $\mathscr{P}^*$ is contained in Γ_β if and only if $\mathrm{supp}\,\mathscr{F} = T \cup [s+1, s+t]$, where T is a non-void subset of $[s]$. Hence Γ_β is the boundary of a simplex of dimension $s-1$, so

$$\dim_k \tilde{H}_i(\Gamma_\beta) = \begin{cases} 0, & i \neq s-1 \\ 1, & i = s-1. \end{cases}$$

Case 2: $\text{supp}\_\beta=[s]$, i.e., $\beta'<0$, $\beta''\geqq 0$. By reasoning parallel to the above,

$$\dim_k \tilde{H}_i(\Gamma_\beta)=\begin{cases}0, & \text{if } i\neq t-1\\ 1, & \text{if } i=t-1.\end{cases}$$

Case 3: $(\text{supp}\_\beta)\cap[s]\neq\emptyset$ and $(\text{supp}\_\beta)\cap[s+1, s+t]\neq\emptyset$. Then $\text{supp}\_\beta=\text{supp}\,\mathscr{F}$ for some face $\mathscr{F}$ of $\mathscr{P}$, so by Theorem 3.1, Γ_β is acyclic. (Alternatively, one can see directly that Γ_β is a simplex.)

Case 4: $\text{supp}\_\beta\subset[s]$ but $\text{supp}\_\beta\neq[s]$. Consider the poset $L(\Gamma_\beta)$ of all non-void faces $\mathscr{F}^*$ of Γ_β, ordered by inclusion, as in the proof of Lemma 2.8. Identify the face $\mathscr{F}^*$ of Γ_β with the set $[s+t]\backslash\text{supp}\,\mathscr{F}$. Then $L(\Gamma_\beta)$ consists of all non-void subsets of the set $T=[s+t]\backslash(\text{supp}\_\beta)$ which do not contain $[s+1, s+t]$. The set of all non-void subsets of T, regarded as a simplicial complex (whose faces are chains of subsets ordered by inclusion) is isomorphic to the first barycentric subdivision $sd(\partial\sigma)$ of the boundary $\partial\sigma$ of the simplex σ on the vertex set T. The subcomplex of $sd(\partial\sigma)$ consisting of all subsets of T containing $[s+1, s+t]$ is isomorphic to $sd(\tau)$ for a simplex τ with $s-|\text{supp}\_\beta|>0$ vertices. Hence $L(\Gamma_\beta)=sd(\partial\sigma)\backslash sd(\tau)$ is topologically a sphere of dimension $|T|-2$ with a (non-void) ball removed of dimension $s-|\text{supp}\_\beta|-1$. Thus $L(\Gamma_\beta)$, and therefore Γ_β, is acyclic.

Case 5: $\text{supp}\ \beta\subset[s+1,s+t]$ but $\text{supp}\ \beta\neq[s+1,s+t]$. By reasoning parallel to Case 4, we get that Γ_β is acyclic.

We have computed $\tilde{H}_i(\Gamma_\beta)$ for all possible β. Substituting these results into Theorem 2.10 completes the proof. □

3.4 **Corollary.** *Preserve the notation of Theorem 3.3. Let* $0\leqq i<d$. *Then* $H^i(A^\alpha)$ *is a finite-dimensional vector space, and* $H^i(A^\alpha)=0$ *unless possibly either* (*a*) $i=s$ *and* $\alpha<0$, *or* (*b*) $i=t$ *and* $\alpha>0$. *Moreover,*

$$\operatorname{depth} A^\alpha=\begin{cases}0, & \text{if } (\Phi,\alpha) \text{ is trivial (i.e., } A^\alpha=0)\\ s, & \textit{if there exists } \beta\in\bar{E}^\alpha \textit{ with } \beta'<0,\ \beta''\geqq 0 \ (\textit{in which case } \alpha<0)\\ t, & \textit{if there exists } \beta\in\bar{E}^\alpha \textit{ with } \beta'\geqq 0,\ \beta''<0 \ (\textit{in which case } \alpha>0)\\ s+t-1, & \textit{otherwise (so } A^\alpha \textit{ is Cohen-Macaulay).}\end{cases}$$

Proof. If $\beta'<0$ and $\beta''\geqq 0$, then $\Phi\beta<0$. Hence if $\beta\in\bar{E}^\alpha$ then $\alpha<0$. Clearly given $\alpha<0$ there are only finitely many $\beta\in\bar{E}^\alpha$ satisfying $\beta'<0$, $\beta''\geqq 0$. Similar reasoning holds for $\beta'\geqq 0$, $\beta''<0$, and the proof follows from Theorem 3.3. □

4. Reciprocity

The purpose of this section is to give a formula relating the $\mathbb{N}$-solutions β of $\Phi\beta=\alpha$ to those solutions β for which supp_β is "large." First we briefly discuss previous work in this area. Recall our notation from Theorem 2.2 – if $F(x)$ is a rational function of $x=(x_1,\dots,x_n)$ possessing a Laurent series expansion about 0, then $F(x)_\infty$ denotes the Laurent series expansion of $F(x)$ about

∞. In [St$_1$, Thm. 4.1] it was shown that if $E \cap \mathbb{P}^n \neq \emptyset$, then

$$F(\Lambda, x)_\infty = (-1)^d \sum_{\substack{\beta \in \bar{E} \\ \beta < 0}} x^\beta, \tag{11}$$

where $F(\Lambda, x) = \sum_{\beta \in E} x^\beta$ as usual. In [St$_3$, Thm. 7.7] this result was given an algebraic interpretation. Essentially it is equivalent to computing the canonical module $\Omega(\Lambda)$ of Λ (which we will define below). In [St$_2$, Sects. 8-11] it was shown that a direct analogue of (11) for Λ^α continues to remain true for *certain* choices of $\alpha \in \mathbb{Z}^r$ (provided $E \cap \mathbb{P}^n \neq \emptyset$). Namely, for certain α we have

$$F(\Lambda^\alpha, x)_\infty = (-1)^d \sum_{\substack{\beta \in \bar{E}_\alpha \\ \beta < 0}} x^\beta. \tag{12}$$

In general, however, the difference between the left- and right-hand sides of (12) is non-zero. For the case $r = 1$, this "error term" was explicitly computed in [St$_2$, Prop. 10.5]. In this section we compute the error term for arbitrary (Φ, α) and relate it to the structure of the module Λ^α.

First we have the following immediate corollary of Theorem 2.10 and the fact that $\tilde{H}_{-1}(\Gamma) = 0$ for any space $\Gamma \neq \emptyset$, while $\tilde{H}_{-1}(\emptyset) \cong k$.

4.1 **Corollary.** The Hilbert series of $H^d(\Lambda^\alpha)$ is given by

$$F(H^d(\Lambda^\alpha), x) = \sum_{\substack{\gamma \in \bar{E}^\alpha \\ \Gamma_\gamma = \emptyset}} x^\gamma.$$

(See Proposition 2.12 for a description of when $\Gamma_\gamma = \emptyset$.) □

Next we come to the main result of this section.

4.2 **Reciprocity Theorem.** We have

$$F(\Lambda^\alpha, x)_\infty = (-1)^d \sum_{\substack{\gamma \in \bar{E}^\alpha \\ \Gamma_\gamma = \emptyset}} x^\gamma + (-1)^{d-1} \sum_{\substack{\gamma \in \bar{E}^\alpha \\ \Gamma_\gamma \neq \emptyset}} \tilde{\chi}(\Gamma_\gamma) x^\gamma, \tag{13}$$

where $\tilde{\chi}(\Gamma_\gamma)$ denotes the reduced Euler characteristic of Γ_γ.

Proof. By Theorems 2.2 and 2.10,

$$\begin{aligned} F(\Lambda^\alpha, x)_\infty &= \sum_{i=0}^{d} (-1)^i F(H^i(\Lambda^\alpha), x) \\ &= \sum_{i=0}^{d} (-1)^i \sum_{\gamma \in \bar{E}^\alpha} (\dim_k \tilde{H}_{d-1-i}(\Gamma_\gamma)) x^\gamma \\ &= (-1)^d \sum_{\substack{\gamma \in \bar{E}^\alpha \\ \Gamma_\gamma = \emptyset}} x^\gamma + \sum_{i=0}^{d-1} (-1)^i \sum_{\substack{\gamma \in \bar{E}^\alpha \\ \Gamma_\gamma \neq \emptyset}} (\dim_k \tilde{H}_{d-1-i}(\Gamma_\gamma)) x^\gamma \\ &= (-1)^d \sum_{\substack{\gamma \in \bar{E}^\alpha \\ \Gamma_\gamma = \emptyset}} x^\gamma + (-1)^{d-1} \sum_{\substack{\gamma \in \bar{E}^\alpha \\ \Gamma_\gamma \neq \emptyset}} \left(\sum_{i=0}^{d-1} (-1)^{d-1-i} \dim_k \tilde{H}_{d-1-i}(\Gamma_\gamma) \right) x^\gamma. \end{aligned}$$

The proof follows from the definition of $\tilde{\chi}(\Gamma_\gamma)$. □

4.3 **Corollary.** *A necessary and sufficient condition on* (Φ, α) *in order for*

$$F(A^\alpha, x)_\infty = (-1)^d \sum_{\substack{\gamma \in E^\alpha \\ \Gamma_\gamma = \emptyset}} x^\gamma \tag{14}$$

is that $\tilde{\chi}(\Gamma_\gamma) = 0$ *whenever* $\Gamma_\gamma \neq \emptyset$. □

Note that by Corollary 2.11, (14) holds whenever A^α is Cohen-Macaulay. The converse is false. For instance, it follows from [St$_2$, Ex. 8.6] that if

$$\Phi = \left[\begin{array}{rrrr|c} 3 & 0 & 0 & -1 & \\ 3 & 0 & -1 & 0 & \\ 4 & -1 & -1 & 0 & \\ 1 & -1 & 1 & 0 & -I_7 \\ 1 & -1 & 0 & 1 & \\ 4 & -1 & 0 & -1 & \\ 2 & -1 & 0 & 0 & \end{array}\right],$$

$$\alpha = (2, 2, 1, -1, -1, 1, 1),$$

then (14) holds but A^α is not Cohen-Macaulay. (Here I_7 denotes the 7×7 identity matrix.) In general, Theorem 4.2 gives an expression for $F(A^\alpha, x)_\infty$ in which the right-hand side of (14) is the "main term." We may regard the terms arising from $\Gamma_\gamma \neq \emptyset$ (or rather $\tilde{\chi}(\Gamma_\gamma) \neq \emptyset$) as "error terms."

We now complement Theorem 4.2 by giving a more precise form of Corollary 4.1. Let B be a homomorphic image of a Gorenstein ring A, and let $d = \dim B$, $c = \dim A$. Then the *canonical module* $\Omega(B)$ (also denoted K_B) is defined to be

$$\Omega(B) = \operatorname{Ext}_A^{c-d}(B, A). \tag{15}$$

(As a B-module, $\Omega(B)$ does not depend on the choice of A.) Eq. (15) makes sense when B is replaced by *any* finitely-generated A-module M. Hence we define in general $\Omega(M) = \operatorname{Ext}_A^{c-d}(M, A)$, where A is Gorenstein, M is a finitely-generated A-module, $c = \dim A$, and $d = \dim M$.

Suppose $A = k[x_1, \dots, x_m]$, a polynomial ring over the field k, given an $\mathbb{N}^n$-grading so that $A_0 = k$. Let $A_+ = \coprod_{\beta \neq 0} A_\beta$ be the irrelevant ideal, and suppose that M is a finitely-generated $\mathbb{Z}^n$-graded A-module of dimension d. Let $I(A) = k[x_1^{-1}, \dots, x_m^{-1}]$, the injective envelope of $k = A/A_+$. Then there is a unique finitely-generated ($\mathbb{Z}^n$-graded) A-module $\Omega'(M)$ for which

$$\operatorname{Hom}_A(H_{A_+}^d(M), I(A)) \cong \Omega'(M) \otimes_A \hat{A}, \tag{16}$$

where $\hat{A}$ denotes the A_+-adic completion of A. It is well-known that $\Omega'(M) \cong \Omega(M)$ [H-K, Ch. 5], so if we wish we can take (16) rather than (15) as the definition of $\Omega(M)$. More generally, the local duality theorem [ibid.] asserts in the present context that

$$\operatorname{Hom}_A(H_{A_+}^i(M), I(A)) \cong \operatorname{Ext}_A^{c-i}(M, A) \otimes_A \hat{A}, \tag{17}$$

or equivalently,

$$\operatorname{Hom}_A(\operatorname{Ext}_A^{c-i}(M, A), I(A)) \cong H_{A_+}^i(M). \tag{18}$$

We also note that it follows from (17) or (18) (in the case $i=d$) that the Hilbert functions of $H^d_{A_+}(M)$ and $\Omega(M)$ are related by

$$\dim_k H^d_{A_+}(M)_{-\alpha} \cong \dim_k \Omega(M)_\alpha. \tag{19}$$

4.4 **Theorem.** *For any (Φ, α), let $\bar{\Lambda}^\alpha$ denote the vector space $k\bar{E}^\alpha$ with basis $\bar{E}^\alpha$, and regard $\bar{\Lambda}^\alpha$ in an obvious way as a Λ-module. Then $\Omega(\Lambda^\alpha)$ is isomorphic to the submodule Ψ of $\bar{\Lambda}^\alpha$ generated (in fact, spanned) by the monomials $x^\beta \in \bar{\Lambda}^\alpha$ such that $\Gamma_{-\beta}=\emptyset$.*

Proof. A straightforward generalization of [St$_3$, Lemma 6.2] shows that $\Omega(\Lambda^\alpha)$ is isomorphic, as a $\mathbb{Z}^n$-graded R-module, to a homogeneous submodule of $\bar{\Lambda}^\alpha$. By (19) and Corollary 4.1, the Hilbert functions of Ψ and $\Omega(\Lambda^\alpha)$ agree. But since every nonzero homogeneous component $\bar{\Lambda}^\alpha_\beta$ of $\bar{\Lambda}^\alpha$ is a one-dimensional vector space, every homogeneous submodule of $\bar{\Lambda}^\alpha$ is uniquely determined by its Hilbert function. Hence $\Psi \cong \Omega(\Lambda^\alpha)$. □

When $\alpha=0$ and (without loss of generality) $E \cap \mathbb{P}^n \neq \emptyset$, we obtain from Theorem 4.4 and Proposition 2.12(c) a simple description of $\Omega(\Lambda)$. This result was first proved in [St$_3$, Thm. 6.7].

4.5 **Corollary.** *Suppose $E \cap \mathbb{P}^n \neq \emptyset$. Then $\Omega(\Lambda)$ is isomorphic to the ideal of Λ generated (in fact, spanned) by all x^β with $\beta \in E \cap \mathbb{P}^n$.* □

We can now strengthen Corollary 4.1 (and therefore Theorem 4.2) by explicitly describing $H^d(\Lambda^\alpha)$, whose Hilbert series comprises the "main term" of the formula for $F(\Lambda^\alpha, x)_\alpha$.

4.6 **Corollary.** *Let V^α be the k-vector space with basis $\{x^\gamma : \Gamma_\gamma = \emptyset\}$. Define a Λ-module structure $\Lambda \times V^\alpha \to V^\alpha$ on V^α by the rule*

$$x^\beta \cdot x^\gamma = \begin{cases} x^{\beta+\gamma}, & \text{if } \Gamma_{\beta+\gamma}=\emptyset \text{ (i.e., } x^{\beta+\gamma} \in V^\alpha) \\ 0, & \text{otherwise.} \end{cases}$$

Then $V^\alpha \cong H^d(\Lambda^\alpha)$.

Proof. By (18), we have

$$H^d(\Lambda^\alpha) \cong \mathrm{Hom}_A(\Omega(\Lambda^\alpha), \mathrm{I}(A)),$$

where $A=k[x_1, \dots, x_m]$ is some polynomial ring over which Λ is a finitely-generated ($\mathbb{Z}^n$-graded) module. For every $\beta \in \bar{E}^\alpha$ such that $\Gamma_{-\beta}=\emptyset$, there is (using the description of $\Omega(\Lambda^\alpha)$ in Theorem 4.4) a unique $\phi_\beta \in \mathrm{Hom}_A(\Omega(\Lambda^\alpha), I(A))$ such that $\phi_\beta(x^\beta) = 1 \in I(A) = k[x_1^{-1}, \dots, x_m^{-1}]$. It is easily checked that the map $H^d(\Lambda^\alpha) \to V^\alpha$ which sends ϕ_β to $x^{-\beta}$ is an isomorphism. □

5. A Combinatorial Decomposition

Suppose that M is a $\mathbb{Z}^n$-graded finitely-generated module over an $\mathbb{N}^n$-graded k-algebra R. Let σ: $\mathbb{Z}^n \to \mathbb{Z}$ be a homomorphism of abelian groups such that (i) $\sigma(\mathbb{N}^n) \subset \mathbb{N}$, and (ii) if $\beta \in \mathbb{N}^n$ and $\sigma(\beta)=0$, then $\beta=0$. Define an $\mathbb{N}$-grading on R

by setting $\deg x = \sigma(\beta)$ whenever $x \in R_\beta$. We will call this procedure "specializing to an $\mathbb{N}$-grading." Similarly define a $\mathbb{Z}$-grading on M and call this "specializing to a $\mathbb{Z}$-grading." Given such a $\mathbb{Z}$-grading of M, the Noether normalization lemma (in the graded case) guarantees the existence of a system of parameters $\theta_1, \ldots, \theta_d$ which is homogeneous with respect to the $\mathbb{N}$-grading. (In general, there need not exist a system of parameters which is homogeneous with respect to the original $\mathbb{N}^n$-grading.) It is well-known that M is Cohen-Macaulay if and only if M is a free module (necessarily finitely generated) over the polynomial ring $S = k[\theta_1, \ldots, \theta_d]$. Moreover, since $\mathbb{Z}$-homogeneous elements $\eta_1, \ldots, \eta_t$ form a basis for M as an S-module if and only if their images in $M' = M/(\theta_1 M + \ldots + \theta_d M)$ are a k-basis for M', it follows that we can choose $\eta_1, \ldots, \eta_t$ to be $\mathbb{Z}^n$-homogeneous. More generally, if depth $M = e$ and if $\theta_1, \ldots, \theta_e$ is a maximal $\mathbb{N}$-homogeneous M-sequence, then M is a free $k[\theta_1, \ldots, \theta_e]$-module (but no longer finitely-generated when $e < d = \dim M$) which posesses a $\mathbb{Z}^n$-homogeneous basis.

There are many circumstances involving combinatorial considerations in which one would greatly desire that $\theta_1, \ldots, \theta_e$, as discussed above, are $\mathbb{N}^n$-homogeneous. Since this is in general impossible, we offer the following conjecture as a possible replacement.

5.1 **Conjecture.** *Let R be a finitely-generated $\mathbb{N}^n$-graded k-algebra (where $R_0 = k$ as usual), and let M be a finitely-generated $\mathbb{Z}^n$-graded R-module. Then there exist finitely many subalgebras $S_1, \ldots, S_t$ of R, each generated by algebraically independent $\mathbb{N}^n$-homogeneous elements of R, and there exist $\mathbb{Z}^n$-homogeneous elements $\eta_1, \ldots, \eta_t$ of M, such that*

$$M = \coprod_{i=1}^{t} \eta_i S_i, \qquad \textit{(vector space direct sum)}$$

where $\dim S_i \geqq$ depth M for all i, and where $\eta_i S_i$ is a free S_i-module (of rank one). Moreover, if k is infinite and under a given specialization to an $\mathbb{N}$-grading R is generated by R_1, then we can choose the ($\mathbb{N}^n$-homogeneous) generators of each S_i to lie in R_1. □

This conjecture is valid for $n = 1$. When M is Cohen-Macaulay we can pick $S_1 = S_2 = \ldots = S_t$; and for general M it follows e.g. from [B-G, Thm. 2.1] that there are $\mathbb{N}$-homogeneous elements $\theta_1, \ldots, \theta_d$ of R such that $S_i = k[\theta_1, \theta_2, \ldots, \theta_{s_i}]$ for some $0 \leqq s_i \leqq d$.

The main purpose of this section is to prove Conjecture 5.1 when $M = \Lambda = kE$ (ignoring the last sentence of the conjecture, which was included so that the question raised in [St$_6$, p. 149, line 6] or [G, Rmk. 5.2] would follow affirmatively). Equivalently:

5.2 **Theorem.** *There exist free (commutative) submonoids $E_1, \ldots, E_t$ of E, all of* rank $d = \dim \Lambda$, *and elements $\delta_1, \ldots, \delta_t$ of E, such that*

$$E = \dot{\bigcup_{i=1}^{t}} (\delta_i + E_i) \qquad \textit{(disjoint union)}. \tag{20}$$

Remark. Note that (20) establishes a "canonical form" for the elements of E. More precisely, if $\gamma_{i1}, \ldots, \gamma_{id}$ is a basis for E_i (as a free commutative monoid), then for every $\beta \in E$ there exists a unique integer $i \in [t]$ and unique integers $a_1, \ldots, a_d \in \mathbb{N}$ such that

$$\beta = \delta_i + \sum_{j=1}^{t} a_i \gamma_{ij}.$$

If one did not require rank $E_i = d$ in (20), then Theorem 5.2 would follow from very general considerations in [C-S]. Actually, Theorem 5.2 was essentially proved in [St$_7$, Sect. 1], but from a different point of view. Here we will sketch the argument in [St$_7$] using our current notation and terminology.

Proof of Theorem 5.2 (sketch). Let $\mathscr{P}$ be the convex $(d-1)$-polytope defined in Sect. 1.

Step 1. It follows from the process of "pulling the vertices" [M-S, p. 116] that there exists a triangulation Δ of $\partial \mathscr{P}$ with the following properties:

(a) the vertices of Δ and of $\mathscr{P}$ coincide, and

(b) Δ is the boundary complex of a simplicial convex polytope $\mathscr{P}'$.

Step 2. Let v be the vertex that was pulled first in Step 1. Let Δ_v be the subcomplex of Δ consisting of all faces F not containing v. Then the cone $C(v, \Delta_v)$ from v to Δ_v forms a (rectilinear) triangulation of $\mathscr{P}$.

Step 3. By property (b) above and the techniques of [B-M] (see [M-S, p. 177]), there exists a shelling $G_1, G_2, \ldots, G_s$ of Δ such that if $v \in G_i$ and $i < s$, then $v \in G_{i+1}$. By definition, $G_1, G_2, \ldots, G_s$ is a *shelling* of Δ if $G_1, G_2, \ldots, G_s$ is a linear ordering of the maximal (i.e., $(d-2)$-dimensional) faces of Δ such that if $2 \leqq i \leqq s$, then $(G_1 \cup G_2 \cup \ldots \cup G_{i-1}) \cap G_i$ is a union of $(d-3)$-faces of G_i.

Step 4. Let $j+1$ be the least integer for which $v \in G_{j+1}$. Then $G_1, G_2, \ldots, G_j$ is a shelling of Δ_v, so $C(v, G_1)$, $C(v, G_2), \ldots, C(v, G_j)$ is a shelling of $C(v, \Delta_v)$. Write $C_i = C(v, G_i)$.

Step 5. Let Q_i be the submonoid of E consisting of all $\beta \in E$ such that the ray in $\mathbb{R}^n$ with endpoint 0 and containing β passes through C_i. Since C_i is a $(d-1)$-simplex, $CF(Q_i)$ consists of d linearly independent vectors $\beta_{i1}, \beta_{i2}, \ldots, \beta_{id}$. Let $\mathbb{N} \cdot CF(Q_i)$ be the free monoid which they generate. Define $P_i = Q_i \cap \left\{ \sum_{j=1}^{d} a_j \beta_{ij} \colon 0 \leqq a_j < 1 \right\}$. Then $|P_i| < \infty$ and $Q_i = \dot{\bigcup}_{\gamma \in P_i} (\gamma + \mathbb{N} \cdot CF(Q_i))$.

Step 6. Let F_i be the unique face of C_i minimal with respect to being not contained in $(C_1 \cup \ldots \cup C_{i-1}) \cap C_i$. Let $T_i = \{\beta \in CF(Q_i)$: the ray from 0 through β intersects $F_i\}$. Given $\gamma \in P_i$, define

$$\hat{\gamma} = \gamma + \Sigma \{\beta \in T_i \colon \gamma \text{ is linearly dependent on } CF(Q_i) - \{\beta\}.$$

Then

$$E = \dot{\bigcup_{i=1}^{j}} \; \dot{\bigcup_{\gamma \in P_i}} (\hat{\gamma} + \mathbb{N} \cdot CF(Q_i)).$$

This yields the desired decomposition of E. □

References

[B-G] Baclawski, K., Garsia, A.M.: Combinatorial decompositions of a class of rings. Advances in Math. **39**, 155–184 (1981)

[B] Björner, A.: Homotopy type of posets and lattice complementation. J. Combinatorial Theory Ser. A **30**, 90–100 (1981)

[B-M] Brugesser, H., Mani, P.: Shellable decompositions of cells and spheres. Math. Scand. **29**, 197-205 (1971)

[C-S] Chomsky, N., Schützenberger, M.-P.: The algebraic theory of context-free languages. In: Computer programming and formal systems (Braffort, P., Hirschberg, D., eds.). Amsterdam: North-Holland Publications 1963

[F] Folkman, J.: The homology groups of a lattice. J. Math. Mech. **15**, 631-636 (1966)

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

[G-W] Goto, S., Watanabe, K.: On graded rings. II. (Z^n-graded rings). Tokyo J. Math. **1**, 237-261 (1978)

[G-Y] Grace, J.H., Young, A.: The Algebra of Invariants. Cambridge: Cambridge University Press 1903; reprinted by New York: Stechert 1941

[H-K] Herzog, J., Kunz, E. (eds.): Der kanonische Modul eines Cohen-Macaulay-Rings. Lecture Notes in Math., vol. 238. Berlin-Heidelberg-New York: Springer 1971

[H] Hochster, M.: Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes. Ann. of Math. **96**, 318-337 (1972)

[H-R] Hochster, M., Roberts, J.L.: Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay. Advances in Math. **13**, 115-175 (1974)

[L] Lakser, H.: The homology of a lattice. Discrete Math. **1**, 187-192 (1971)

[M-S] McMullen, P., Shephard, G.C.: Convex polytopes and the upper bound conjecture. London Math. Soc. Lecture Note Series, vol. 3. Cambridge: Cambridge University Press 1971

[M] Mumford, D.: Hilbert's fourteenth problem - the finite generation of subrings such as rings of invariants. In: Mathematical developments arising from Hilbert problems (Browder, F., ed.). Proc. Symposia Pure Math., vol. 28, pp. 431-444. Providence, R.I.: American Mathematical Society 1976

[Sp] Spanier, E.H.: Algebraic Topology. New York: McGraw-Hill 1966

[St_1] Stanley, R.: Linear homogeneous diophantine equations and magic labelings of graphs. Duke Math. J. **40**, 607-632 (1973)

[St_2] Stanley, R.: Combinatorial reciprocity theorems. Advances in Math. **14**, 194-253 (1974)

[St_3] Stanley, R.: Hilbert functions of graded algebras. Advances in Math. **38**, 57-83 (1978)

[St_4] Stanley, R.: Invariants of finite groups and their applications to combinatorics, Bull. Amer. Math. Soc. (new series) **1**, 475-511 (1979)

[St_5] Stanley, R.: Combinatorics and invariant theory. In: Relations between combinatorics and other parts of mathematics (Ray-Chaudhuri, D.K., ed.). Proc. Symposia in Pure Math., vol. 34, pp. 345-355. Providence, R.I.: American Mathematical Society 1979

[St_6] Stanley, R.: Balanced Cohen-Macaulay complexes. Trans. Amer. Math. Soc. **249**, 139-157 (1979)

[St_7] Stanley, R.: Decompositions of rational convex polytopes. Annals of Discrete Math. **6**, 333-342 (1980)

[St_8] Stanley, R.: Interactions between commutative algebra and combinatorics. Report. U. Stockholm, 1982 - No. 4

[W] Walker, J.: Topology and combinatorics of ordered sets. Thesis, M.I.T., 1981

Oblatum 22-X-1981