HILBERT FUNCTIONS OF VERONESE ALGEBRAS

H E A CAMPBELL, A V GERAMITA, I P HUGHES,
G G SMITH, AND D L WEHLAU

Abstract. We study the Hilbert polynomials of non-standard graded algebras R, that are finitely generated on generators not all of degree one. Given an expression $P(R,t) = a(t)/(1-t^\ell)^n$ for the Poincaré series of R as a rational function, we study for $0 \le i \le \ell$ the graded subspaces $\oplus_k R_{k\ell+i}$ (which we denote $R[\ell;i]$) of R, in particular their Poincaré series and Hilbert functions. For example, we prove that if $R[\ell;i] \neq 0$ then its Hilbert polynomial has degree $n-1$. We investigate the algebraic invariants of finite groups in this context.

1. Introduction

We study commutative graded algebras $R = \oplus_{k=0}^{\infty} R_k$ over a field $\mathbf{F}$. We require that R be connected, that is, $R_0 = \mathbf{F}$, and that R be finitely generated so that $\dim_{\mathbf{F}}(R_k) < \infty$. The Poincaré series of R is the power series $P(R,t) = \sum_{k=0}^{\infty} \dim_{\mathbf{F}}(R_k) t^k$ with Hilbert function $H(R,\cdot) : \mathbf{N} \to \mathbf{N}$ defined as $H(R,k) = \dim_{\mathbf{F}}(R_k)$.

There are many results in the literature concerning the Poincaré series and Hilbert functions of standard graded algebras, notably the result of Macaulay. The wonderful book [1] is a good reference.

It is easy to see (and well-known) that $P(R,t)$ may be written $a(t)/(1-t^\ell)^n$, where ℓ is a positive integer, n is the Krull dimension of R and $a(t)$ is a polynomial with integer coefficients and $a(1) \neq 0$, see Proposition 3.1. Given an integer ℓ, and i a non-negative integer less than ℓ, we define $R[\ell;i]$ to be the graded vector space of elements of R of degree congruent to i modulo ℓ. The algebra $R[\ell;0]$ is called the *Veronese subring of order* ℓ. Of course $R[\ell;i]$ is a module over $R[\ell;0]$. It is easy to see that a the Krull dimension of a Veronese subring has the same Krull dimension as R, see Proposition 4.1. In special cases a Veronese subring is itself a standard graded algebra, see Corollary 4.3.

Now we suppose that ℓ is an integer such that $P(R,t)$ may be written in the form $a(t)/(1-t^\ell)^n$ where $a(t) \in \mathbf{Z}[\mathbf{t}]$. Then for each $i = 0, 1, \ldots, \ell-1$, there is a Hilbert polynomial $H_i(k)$ which gives the $\mathbf{F}$-dimension of $R[\ell,i]_k$. In general, H_0 has degree

Date: September 21, 2005.

1991 *Mathematics Subject Classification.* 13F20.

This research is supported in part by the Natural Sciences and Engineering Research Council of Canada.

$n-1$, although this cannot be said of H_i, see Example 4.9. However, if R is Cohen-Macaulay, then H_i has degree $n-1$ provided $R[\ell;i]$ is non-trivial, see Proposition 4.8. If R is a domain, then H_i is of degree $n-1$ and its leading coefficient is equal to the leading coefficient of H_0, see Corollary 4.11. We are also able to prove for R a Cohen-Macaulay domain, that for any homogeneous system of parameters for $R[\ell;0]$ all of the modules $R[\ell;i]$ have the same rank as free modules over the system, see Proposition 4.12.

We define the period of R, denoted $m(R)$, to be the least of the integers ℓ for which there exists an expression $P(R,t) = a(t)/(1-t^\ell)^n$ where $a(t) \in \mathbf{Z}[\mathbf{t}]$. We show that $m(R)$ divides any such ℓ. In general, it is not easy to determine the period of an arbitrary graded algebra. However if R is a polynomial algebra, then $m(R)$ is the least common multiple of the degrees of its generators, see Proposition 4.5. In the event that $R = \mathbf{F}[V]^G$ is a ring of invariants of a finite group G whose order is not divisible by the characteristic of the field $\mathbf{F}$ (a so-called non-modular group representation), we prove in Theorem 5.4 that (a) $m(\mathbf{F}[V]^G)$ divides the exponent of G and (b) the exponent of G divides the least common multiple of the degrees of the members of any homogeneous system of parameters of $\mathbf{F}[V]^G$. Gregor Kemper, [4], has extended (b) to the case where the characteristic of the field does divide the order of the group (the modular case).

Our paper has four sections. In the first section we recall, mostly from [1], a number of results about power series and what can be said about them when they admit expressions as rational functions. In the next section, we discuss the Poincaré series and Hilbert functions of graded algebras. This leads to the third section, where we examine properties of $R[\ell;i]$. Finally, in the fourth section, we examine the case where R is the invariant algebra of a finite group.

2. Power Series as rational functions

In this section, we collect results from [1, page 167] but our attention is focused on power series $P(t) = \sum_{k=0}^{\infty} p_k t^k$ with integer coefficients p_k, rather than Laurent series. In addition, we obtain some results for the case of a non-negative power series, i.e., with all $p_k \in \mathbf{N}$. We define the Hilbert function $H : \mathbf{N} \to \mathbf{Z}$ of a power series $P(t)$ by $H(k) = p_k$.

We are particularly interested in the case when $P(t)$ may be written as a rational function $a(t)/(1-t^\ell)^s$, for some strictly positive ℓ, in which case $a(t)$ has integer coefficients. We note that $P(t)$ has a pole of order s at $t=1$ if and only if $a(1) \neq 0$.

Lemma 2.1. *Let $P(t)$ be such an integral power series and define $\mathcal{T} := \{(\ell,s) \in \mathbf{N}^2 \mid P(t)(1-t^\ell)^s \in \mathbf{Z}[t]\}$, $\mathcal{L} := \{\ell \in \mathbf{N} \mid \exists s$ with $(\ell,s) \in \mathcal{T}\}$ and $\mathcal{S} := \{s \in \mathbf{N} \mid \exists \ell$ with $(\ell,s) \in \mathcal{T}\}$. Let m be the least integer in $\mathcal{L}$, and n the least integer in $\mathcal{S}$. Then m divides each integer in $\mathcal{L}$ and $P(t)(1-t^m)^n \in \mathbf{Z}[t]$ (i.e., $(m,n) \in \mathcal{T}$). We denote m by $m(P(t))$ and call it the period of $P(t)$.*

Proof. There exists r such that $(m,r) \in \mathcal{S}$. Let $(\ell,s) \in \mathcal{S}$ and put $k = \gcd(m,\ell)$, $a(t) = P(t)(1-t^m)^r$ and $b(t) = P(t)(1-t^\ell)^s$. Thus $a(t), b(t) \in \mathbf{Z}[t]$. Therefore

$$b(t)(1-t^m)^r = a(t)\left[\frac{(1-t^\ell)}{(1-t^k)}\right]^s (1-t^k)^s$$

Since $(1-t^m)^r$ and $\left[\frac{(1-t^\ell)}{(1-t^k)}\right]^s$ are co-prime in $\mathbf{Z}[t]$ we have $b(t) = \left[\frac{(1-t^\ell)}{(1-t^k)}\right]^s c(t)$ where $c(t) \in \mathbf{Z}[t]$. Therefore $P(t)(1-t^\ell)^s = \left[\frac{(1-t^\ell)}{(1-t^k)}\right]^s c(t)$and thus $P(t)(1-t^k)^s \in \mathbf{Z}[t]$ which implies that $k = m$.

Now suppose that $(\ell,n) \in \mathcal{S}$, that m divides ℓ, that $a(t) := P(t)(1-t^m)^r \in \mathbf{Z}[t]$ and that $b(t) := P(t)(1-t^\ell)^n \in \mathbf{Z}[t]$. Further assume that $r > n$. Then

$$a(t)\left[\frac{(1-t^\ell)}{(1-t^m)}\right]^n = b(t)(1-t^m)^{r-n}$$

and hence $a(t) = (1-t^m)^{r-n}c(t)$ where $c(t) \in \mathbf{Z}[t]$ since $(1-t^m)^{r-n}$ is co-prime to $\left[\frac{(1-t^\ell)}{(1-t^m)}\right]^n$. Therefore $P(t)(1-t^m)^n = c(t) \in \mathbf{Z}[t]$. □

Lemma 4.1.7 of [1] is the case $\ell = 1$ of the following proposition and is used in its proof.

Proposition 2.2. *Let $0 \neq P(t) = \sum_{i=0}^{\infty} p_j t^j$ be a power series with integer coefficients. The following two statements are equivalent.*

(a) *there exists $a(t) \in \mathbf{Z}[t]$ such that*

$$P(t) = \frac{a(t)}{(1-t^\ell)^n}$$

(b) *for $0 \le i < \ell$, there exists a polynomial $H_i(t) \in \mathbf{Q}[t]$ of degree at most $n-1$ such that $H_i(k) = p_{k\ell+i}$ for all $k >> 0$.*

Proof. Let $P(t) = \sum_{j=0}^{\infty} p_j t^j$. For $0 \le i < \ell$ we denote by $P_i(t)$ the power series $\sum_{k=0}^{\infty} p_{k\ell+i}t^k$. Then $P(t) = \sum_{i=0}^{\ell-1} t^i P_i(t^\ell)$. First we prove that (a) implies (b). We write $a(t) = \sum_{j=0}^{s} \alpha_j t^j$. We denote by $a_i(t)$ the polynomial $\sum_{k=0}^{s_i} \alpha_{k\ell+i}t^k$, where s_i denotes the greatest integer with the property that $s_i\ell + i \le \deg a(t) = s$. Clearly, $P_i(t) = a_i(t)/(1-t)^n$ and $a(t) = \sum_{i=0}^{\ell-1} t^i a_i(t^\ell)$.

Since

$$\left(\frac{1}{1-t}\right)^n = \sum_{k=0}^{\infty}\binom{-n}{k}(-t)^k = \sum_{k=0}^{\infty}\binom{n+k-1}{n-1}t^k$$

it follows that $P_i(t) = h(t) + \sum_{k=s_i}^{\infty} \sum_{j=0}^{s_i} \binom{n+k-j-1}{n-1} \alpha_{j\ell+i}$ where $h(t)$ is a polynomial of degree less than s_i. Therefore, we define $H_i : \mathbf{Z} \to \mathbf{Z}$ by

$$\begin{aligned} H_i(k) &= \sum_{j=0}^{s_i} \binom{n+k-j-1}{n-1} \alpha_{j\ell+i} \\ &= \frac{a_i(1)}{(n-1)!} k^{n-1} + \text{ terms of lower degree in } k. \end{aligned} \tag{2.1}$$

So H_i is a rational polynomial in k of degree $n-1$ or less with the property that $H_i(k) = p_{k\ell+i}$ for $k \geq s_i$. Hence we have proved (b).

Now we show that (b) implies (a). Assume (b) holds and let the degree of H_i be $d_i - 1$. By [1, Lemma 4.1.7] we can write $P_i(t) = \frac{b_i(t)}{(1-t)^{d_i}}$ where $b_i(t) \in \mathbf{Z}[t]$ and $b_i(1) \neq 0$. Thus we have $P_i(t) = \frac{a_i(t)}{(1-t)^n}$ where $a_i(t) \in \mathbf{Z}[t]$. Therefore

$$P(t) = \sum_{i=0}^{\ell-1} t^i P_i(t^\ell) = \sum_{i=0}^{\ell-1} \frac{t^i a_i(t^\ell)}{(1-t^\ell)^n} = \frac{a(t)}{(1-t^\ell)^n}$$

□

Remark 2.3. Suppose $P(t)$ satisfies (a) and (b) of the above proposition. Then $a(1) \neq 0$ implies that there exists i such that $a_i(1) \neq 0$ and therefore by Equation 2.1 H_i has degree $n-1$.

3. Graded Algebras and their Poincaré series

We study commutative graded algebras $R = \oplus_{k=0}^{\infty} R_k$ over a field $\mathbf{F}$. We require that R be connected, that is, $R_0 = \mathbf{F}$, and that R be finitely generated so that $\dim_{\mathbf{F}}(R_k) < \infty$. We define the Poincaré series of R to be the power series $P(R,t) = \sum_{k=0}^{\infty} \dim_{\mathbf{F}}(R_k) t^k$ with Hilbert function $H(R, \cdot) : \mathbf{N} \to \mathbf{N}$ defined as $H(R,k) = \dim_{\mathbf{F}}(R_k)$. We apply Lemma 2.1 to $P(R,t)$. We define the period of R, denoted $m(R)$ or just m if R is fixed, to be the period $m(P(R,t))$. We note that the number n of Lemma 2.1 is the Krull dimension of R.

Let n denote the Krull dimension of R. Then, by the (graded) Noether Normalization Theorem, there exists a homogeneous system of parameters $\{f_1, \ldots, f_n\}$ for R. Then R is finitely generated as a module over the polynomial subalgebra $S = \mathbf{F}[f_1, \ldots, f_n]$. We let d_i denote the degree of f_i. It is easy to see that

$$P(S,t) = \prod_{i=1}^{n} (1 - t^{d_i})^{-1}.$$

We observe that $P(S,t)$ has a pole of order n at $t = 1$.

In the literature, R is said to be a *standard* or *homogeneous graded* algebra if it is generated by its elements of degree 1. However, we will refer here to an algebra which is generated by elements all of the same degree as a standard graded algebra.

Proposition 3.1. *Let R be a finitely generated graded $\mathbf{F}$-algebra of dimension n and let ℓ be the least common multiple of the degrees of some homogeneous system of parameters of R. Then there exists a polynomial, $a(t) \in \mathbf{Z}[t]$ such that*

$$P(R,t) = \frac{a(t)}{(1-t^{\ell})^n}$$

with $a(1) \neq 0$.

Proof. Let $\{f_1, \dots, f_n\}$ be the homogeneous system of parameters and let d_i be the degree of f_i. Then $\{f_1^{\ell/d_1}, \dots, f_n^{\ell/d_n}\}$ is a homogeneous system of parameters for R with each element having the same degree, ℓ. The proposition now follows from the Hilbert-Serre Theorem [7, page 76]. □

We recall that R is said to be Cohen-Macaulay if R is free as a module over the polynomial subalgebra S generated by a homogeneous system of parameters as above. (If R is free over one such system, it is free over any such).

Remark 3.2. If R is Cohen-Macaulay, then the polynomial $a(t)$ in Proposition 3.1 is in $\mathbf{N}[\mathbf{t}]$. In fact, if $\{r_1, \dots, r_s\}$ is a homogeneous basis for R over S and $a(t) = \sum a_i t^i$, then a_i is the number of r_j of degree i. For arbitrary R, the most we can say is that $a(1)$ is positive.

4. Degree modules

In this section we study the decomposition of a finitely generated graded $\mathbf{F}$-algebra R of dimension n into "degree" modules and study their structure and Hilbert polynomials.

Proposition 4.1. *Let d be a positive integer. The Veronese algebra of order d, $R[d;0]$, is a finitely generated $\mathbf{F}$-algebra of dimension n over which R is finitely generated as a module, and therefore $R[d;0]$ has Krull dimension n.*

Proof. By elementary results of commutative algebra, it suffices to show that R is integral over $R[d;0]$. Suppose that R is generated as an algebra by $\{f_1, \dots, f_s\}$ of degrees d_i. Let $k = \operatorname{lcm}(d_1, \dots, d_s, d)$. We observe that, for all i, $1 \leq i \leq s$ we have

$$\deg(f_i^{k/d_i}) = k$$

Since f_i is integral over $\mathbf{F}[f_1^{k/d_1}, \dots, f_s^{k/d_s}] \subset R[d;0]$ and hence f_i is integral over $R[d;0]$. □

We now prove a purely combinatorial result concerning certain linear congruences. Given a sequence $\theta = (d_1, \dots, d_s)$ of positive integers and a positive integer ℓ, we say a non-negative sequence $I = (i_1, \dots, i_s)$ is in the additive monoid $\mathcal{M} = \mathcal{M}(\theta, \ell)$ if $\theta \cdot I = m\ell$ for some $m \geq 0$. We say that a sequence I is decomposable if $I = J + K$ for non-negative non-zero sequences $J,\ K \in \mathcal{M}$. Otherwise, we say I is indecomposable. It is clear that the set of indecomposable sequences generates the monoid. It is a difficult problem in general to characterize the indecomposable sequences, see [2]. However

Proposition 4.2. *Let $\theta = (d_1, \dots, d_s)$ be sequence of distinct positive integers such that $\gcd(d_i, d_j) = 1$ for $i \neq j$, and let $\ell = \prod d_i$ be the least common multiple of $\{d_1, \dots, d_s\}$. Then $\mathcal{M}(\theta, \ell)$ as defined in the previous paragraph is generated by the sequences I satisfying $\theta \cdot I = \ell$.*

Proof. The cases $s = 1, 2$ are easy to prove so we suppose here that $s \geq 3$. We suppose that I satisfies $\theta \cdot I = m\ell$ for some $m \geq 2$. We show that $I = J + K$ for non-negative non-zero sequences J and K with $j_k \leq i_k$ for all k, $1 \leq k \leq s$, and $\theta \cdot J = \ell$. We denote by Δ_k the sequence $(0, \dots, 0, 1, 0, \dots, 0)$ where the 1 occurs the k-th position from the left. We observe that if there is a k, $1 \leq k \leq s$, with $i_k d_k \geq \ell$ then we may choose $J = (\ell/d_k)\Delta_k$. So we suppose that $i_k d_k < \ell$ for all k.

After a permutation of the entries of θ, we may suppose, without loss of generality, that $i_1 d_1 \leq \dots \leq i_s d_s$. We consider the set

$$\Omega(I) = \Omega = \{J' \in \mathbf{N}^{s-2} \mid j_k \leq i_k,\ 1 \leq k \leq s-2,\ \theta' \cdot J' \leq \ell - (d_{s-1} - 1)(d_s - 1)\}.$$

Here θ' denotes the sequence $(d_1, \dots, d_{s-2})$. We have $(0, \dots, 0) \in \Omega$, so there exist elements $J' \in \Omega$ such that $\theta' \cdot J'$ is a maximum. Fix such a J'.

We have $\ell - \theta' J' \geq (d_{s-1} - 1)(d_s - 1)$ so, by the solution to the postage stamp problem, there exist non-negative integers j_{s-1} and j_s with $j_{s-1}d_{s-1} + j_s d_s = \ell - \theta' J'$. We set $J = (J', j_{s-1}, j_s)$. By construction, $\theta \cdot J = \ell$, so J is the needed sequence provided we can show $i_{s-1} \geq j_{s-1}$ and $i_s \geq j_s$.

Case 1. Suppose $I' = (i_1, \dots, i_{s-2}) \in \Omega$. Then $I' = J'$ and it follows that

$$(i_{s-1} - j_{s-1})d_{s-1} + (i_s - j_s)d_s = (m-1)\ell.$$

However, we have already seen that $i_{s-1}d_{s-1} < \ell$ and $i_s d_s < \ell$ so we must have $i_{s-1} - j_{s-1} \geq 0$ and $i_s - j_s \geq 0$ as required, since $m \geq 2$.

Case 2. Suppose $I' = (i_1, \dots, i_{s-2}) \notin \Omega$. Then there exists a k, $1 \leq k \leq s-2$ with $j_k < i_k$. Therefore

$$\theta' \cdot (J' + \Delta_k) = \theta' \cdot J' + d_k > \ell - (d_{s-1} - 1)(d_s - 1)$$

since J' is maximal in Ω, so that

$$j_{s-1}d_{s-1} + j_s d_s = \ell - \theta' J' < (d_{s-1} - 1)(d_s - 1) + d_k.$$

We consider three subcases: $d_{s-1} = 1$, $d_s = 1$, or both are larger than 1.

Case 2a. We suppose $d_{s-1} = 1$. Take $j = \ell - \theta' \cdot J' < d_k$. Since $j_k < i_k$ we have $1 \leq i_k$ and therefore, $j < d_k \leq i_k d_k \leq i_{s-1}d_{s-1} = i_{s-1}$. Hence in this case the sequence $L = (J', j, 0)$ may be used in place of J to decompose I.

Case 2b. The proof for the case $d_s = 1$ is very similar to that just given, so we omit it.

Case 2c. Here we have that $d_{s-1}d_s \neq 1$. Also $\theta' \cdot J' + j_{s-1}d_{s-1} + j_s d_s = \ell$ and that $\theta' \cdot J' + d_k > \ell - (d_{s-1}-1)(d_s-1)$. We obtain the equation

$$j_{s-1}d_{s-1} \leq j_{s-1}d_{s-1} + j_s d_s = \ell - \theta' \cdot J' < d_k + (d_{s-1}-1)(d_s-1).$$

Again, there are two cases to consider, $j_{s-1} > i_{s-1}$ or $j_s > i_s$. Both cases lead to contradictions via similar proofs, so we offer only the proof of the former case. In this case, we have $j_{s-1}d_{s-1} > i_{s-1}d_{s-1}$ so that $2\ell \leq \theta' \cdot I' + i_{s-1}d_{s-1} + i_s d_s \leq \theta' \cdot I' + i_{s-1}d_{s-1} + \ell$. Therefore, $\ell \leq \theta' \cdot I' + i_{s-1}d_{s-1} \leq (s-1)i_{s-1}d_{s-1} \leq (s-1)j_{s-1}d_{s-1}$. Combining this equation with the equation displayed above we obtain

$$\ell < (s-1)(d_k + (d_{s-1}-1)(d_s-1)).$$

We write the factor on the right hand side as $d_{s-1}d_s + (d_k - d_{s-1} - d_s + 1)$. Suppose we have $d_k \leq d_{s-1} + d_s - 1$. Then we obtain $d_1 d_2 \dots d_s = \ell < (s-1)(d_{s-1}d_s)$. This cannot happen if $s \geq 5$ since then the product of $s-2$ distinct positive integers cannot be less than $s-1$. If $s = 3$ then this can only happen if $d_k = d_1 = 1$, and the proof follows easily. If $s = 4$, then this can only happen if $\{d_1, d_2\} = \{1, 2\}$, say $d_1 = 1$, where we no longer assume $i_1 d_1 \leq i_2 d_2$. Suppose $i_1 d_1 + i_4 d_4 > \ell$. Then we can choose $k_1 < i_1$ so that $k_1 + i_4 d_4 = k_1 d_1 + i_4 d_4 = \ell$. But then the sequence $K = (k_1, 0, 0, i_4)$ may be used to decompose I. On the other hand, if $i_1 d_1 + i_4 d_4 \leq \ell$ then we must have $i_2 d_2 + i_3 d_3 > \ell$ since $i_1 d_1 + i_2 d_2 + i_3 d_3 + i_4 d_4 \geq 2\ell$. Therefore, since $d_2 = 2$, we may choose $k_2 < i_2$ so that $k_2 d_2 + i_3 d_3 = \ell - 1$ or ℓ. If $k_2 d_2 + i_3 d_3 = \ell$ then we decompose I using $L = (0, k_2, i_3, 0)$. If $k_2 d_2 + i_3 d_3 = \ell - 1$ then the sequence $L = (1, k_2, i_3, 0)$ may be used to decompose I, where we may assume $i_1 \neq 0$ because if $i_1 = 0$ then I may be decomposed using the case $s = 3$.

Finally, we may suppose that $d_k > d_{s-1} + d_s - 1$. Note that $d_{s-1} + d_s > 4$, since neither d_{s-1} nor d_s is 1. First we show that

$$d_{s-1}d_s + d_k - d_{s-1} - d_s + 1 \leq \frac{d_k d_{s-1} d_s}{4}.$$

This is true since

$$\begin{aligned} \frac{d_k d_{s-1} d_s}{4} - d_k &= d_k\left(\frac{d_{s-1}d_s - 4}{4}\right) > d_{s-1}d_s - 4 \\ &= (d_{s-1}-1)(d_s-1) + d_{s-1} + d_s - 5 \geq (d_{s-1}-1)(d_s-1). \end{aligned}$$

Hence $\ell < (d_k d_{s-1} d_s/4)(s-1)$. Again, it cannot happen that for $s \geq 3$ a product of $s-3$ distinct integers is less than $(s-1)/4$. □

Corollary 4.3. *Suppose R is generated by homogeneous elements any two of which either share the same degree or whose degrees are co-prime. If ℓ is the least common multiple of these degrees then $R[\ell; 0] = \mathbf{F}[R_\ell]$, that is, $R[\ell; 0]$ is a standard graded algebra, generated by its elements of degree ℓ.* □

However, we have

Example 4.4. Let $A = \mathbf{F}[x_1, x_2, x_3, x_4]$ be a standard graded polynomial algebra on generators of degree 1, and let R be the polynomial subalgebra generated by $\{f_1 = x_1, f_2 = x_2^6, f_3 = x_3^{10}, f_4 = x_4^{15}\}$. Then $m = m(R) = \operatorname{lcm}(1, 6, 10, 15) = 30$ by Proposition 4.5 below but $R[30; 0] \neq \mathbf{F}[R_{30}]$ since $z = f_1 f_2^4 f_3^2 f_4 \in R_{60}$ but $z \notin \mathbf{F}[R_{30}]$.

In general, in the situation of this example, we have

Proposition 4.5. *Let R be a polynomial algebra on generators $f_1, \dots, f_n$ of degrees d_i and let $\ell = \operatorname{lcm}(d_1, \dots, d_n)$. Then the period of R, $m(R)$ is ℓ.*

Proof. We have

$$P(R,t) = \frac{1}{\prod_{i=1}^{n}(1 - t^{d_i})} = \frac{b(t)}{(1 - t^{\ell})^n} = \frac{a(t)}{(1 - t^m)^n}$$

where $m \mid \ell$ by Lemma 2.1. Cross-multiplying we have $(1 - t^m)^n = a(t) \prod (1 - t^{d_i})$ which implies that $(1 - t^{d_i})$ divides $(1 - t^m)$ for all i. But then $d_i \mid m$ for all i so that $\ell \mid m$, as required. □

Let us fix an expression $P(R,t) = a(t)/(1-t^{\ell})^n$ with $a(1) > 0$ and $\deg a(t) = s$. We observe that $R[\ell; i]$ is a module over the Veronese algebra $R[\ell; 0]$. By Proposition 2.2 $P(R[\ell; 0], t) = t^i P_i(t^{\ell}) = t^i a_i(t^{\ell})/(1 - t^{\ell})^n$. The polynomial H_i, defined in the proof of Proposition 2.2, is called the *Hilbert polynomial* of $R[\ell; i]$. We recall from Equation 2.1 that $H_i(k) = H(k\ell + i)$ is a polynomial of degree at most $n-1$ in k with $a_i(1)/(n-1)!$ as the coefficient of k^{n-1}.

Proposition 4.6. *The Hilbert polynomial $H_0(k)$ of $R[\ell; 0]$ is a polynomial of degree $n - 1$ in k.*

Proof. Since $R[\ell; 0]$ has Krull dimension n by Proposition 4.1, we have an expression $P(R[\ell; 0], t) = b(t)/(1 - t^k)^n$ with $b(1) \neq 0$, for some $k > 0$, in addition to the expression $P(R[\ell; 0], t) = a_0(t)/(1 - t^{\ell})^n$ determined by $P(R, t)$. It is easy to see that $b(1) \neq 0$ implies $a_0(1) \neq 0$, and the result follows using Equation 2.1. □

The following result is observed in [3, Chapter 3]

Proposition 4.7. *Let d be a positive integer. If R is Cohen-Macaulay, then $R[d; 0]$ is also Cohen-Macaulay. If R is an integrally closed domain, then $R[d; 0]$ is also an integrally closed domain.*

In [3, Chapter 3] the relationship between the two conditions that R is Gorenstein and that $R[d; 0]$ is Gorenstein is examined in detail.

Proposition 4.8. *If R is Cohen-Macaulay and $R[\ell; i] \neq 0$ then $H_i(k)$ is of degree $n - 1$, $0 \leq i < \ell$.*

Proof. It is enough to show that $a_i(1) \neq 0$.

Since R is Cohen-Macaulay, we may write $P(R,t) = \frac{b(t)}{(1-t^s)^n}$ for some s (s may be chosen to be the least common multiple of the degrees of a homogeneous system of parameters for R all of whose degrees are divisible by ℓ so $\ell | s$). By Remark 3.2, $b(t) \in \mathbf{N}[t]$. In addition we have the usual expression $P(R,t) = \frac{a(t)}{(1-t^{\ell})^n}$ with $a(t) = \sum_j \alpha_j t^j \in \mathbf{Z}[t]$. So we may write

$$b(t) = a(t)(\frac{1-t^s}{1-t^{\ell}})^n = a(t)f(t^{\ell}),$$

where $f(t) = (1 + t + t^2 + \cdots + t^{\frac{s}{\ell}-1})^n$. Therefore

$$\sum_k b_{k\ell+i} t^{k\ell+i} = (\sum_k \alpha_{k\ell+i} t^{k\ell+i}) f(t^{\ell}).$$

If we now set $t = 1$ in this expression, we obtain $0 \leq \sum_k b_{k\ell+i} = (\sum_k \alpha_{k\ell+i})(s/\ell)^n$. Now we observe that if $R[\ell; i]$ is non-zero, then $\sum_k b_{k\ell+i} \neq 0$ and the result follows. □

However, the following example shows that the hypothesis that R be Cohen-Macaulay is necessary in Proposition 4.8

Example 4.9. Let $R = \mathbf{F}[x, y^2, z^2]/(x^2, xy^2)$ where each of the indeterminates x, y and z has degree 1. We note that the Krull dimension of R is 2. It is not difficult to show that $m(R) = 2$ and, moreover, that R_{2k+1} has basis $\{xz^{2k}\}$ while $R_{2k} = \mathbf{F}[y^2, z^2]_{2k}$. But then $R[\ell; 1]$ has a Hilbert polynomial of degree 0 while $R[\ell; 0]$ has a Hilbert polynomial of degree 1. It is easy to see that R is not Cohen-Macaulay.

Lemma 4.10. *Suppose there exists a non-zero divisor $f \in R[\ell; i]$. Then $H_i(k)$ has degree $n-1$, and, moreover, its lead coefficient $a_i(1)/(n-1)!$ is equal to the lead coefficient $a_0(1)/(n-1)!$ of the Hilbert polynomial $H_0(k)$ of $R[\ell; 0]$.*

Proof. From Equation 2.1 we see that it is sufficient to prove that $a_0(1) = a_i(1)$. The degree of f is of the form $j\ell + i$ for some j. We observe that multiplication by f injects $R[\ell; 0]_{k\ell}$ into $R[\ell; i]_{(k+j)\ell+i} = R_{(k+j)\ell+i}$, for all k. Therefore, $H_0(k) = \dim_{\mathbf{F}}(R[\ell; 0]_{k\ell}) \leq \dim_{\mathbf{F}}(R[\ell; i]_{(k+j)\ell+i}) = H_i(k+j)$ for all k. This can only happen if $a_0(1) \leq a_i(1)$.

We observe that multiplication by $f^{\ell-1}$ injects $R[\ell; i]_{k\ell+i}$ into $R[\ell; 0]_{\ell(k+i+\ell j-j)}$ for all k, so we also obtain $a_i(1) \leq a_0(1)$. □

Corollary 4.11. *If R is a domain, then the Hilbert polynomials of each of its non-trivial degree modules have the same degree $n-1$ and, moreover, each of the lead coefficients of these polynomials is the same.*

Proof. The proof follows from Proposition 4.6 and Proposition 4.10. □

Proposition 4.12. *Let $\{f_1, \ldots, f_n\}$ be a homogeneous system of parameters for $R[\ell; 0]$. If R is a Cohen-Macaulay domain, then all the non-zero degree modules $R[\ell; i]$ have the same rank as free modules over $\mathbf{F}[f_1, \ldots, f_n]$.*

Proof. The homogeneous system of parameters for $R[\ell; 0]$, $\{f_1, \ldots, f_n\}$ is also a homogeneous system of parameters for R. Consequently, each $R[\ell; i]$ is a free module over $S = \mathbf{F}[f_1, \dots, f_n]$. Let d_i denote the degree of f_i. We have

$$P(R[\ell; i], t) = \frac{t^i a_i(t^\ell)}{(1-t^m)^n} = \frac{c_i(t)}{\prod_{j=1}^n (1-t^{d_j})} = \frac{b_i(t)}{(1-t^\ell)^n}$$

for $\ell = \operatorname{lcm}(d_1, \dots, d_n)$ and polynomials $a_i(t) \in \mathbf{Z}[t]$ and $b_i(t), c_i(t) \in \mathbf{N}[t]$. We observe in particular that $c_i(1)$ is the rank of $R[\ell; i]$ as a module over S. Now $m \mid \ell$ by Lemma 2.1 and we obtain

$$b_i(t) = t^i a_i(t) (\frac{1-t^\ell}{1-t^m})^n.$$

Therefore $b_i(1) = a_i(1)(\ell/m)^n$. Now $a_i(1)$ is the sum of the coefficients in the polynomial $a_i(t)$ and so we have, by Corollary 4.11, that $b_i(1) = b_0(1)$ for all i. But now $c_i(1) \prod(\ell/d_j) = b_i(1)$ so that $c_i(1) = c_0(1)$, as required. □

5. Invariant theory

We assume throughout this section that we have some fixed faithful representation $\rho : G \to Gl(V)$ for V a vector space of dimension n over the field $\mathbf{F}$. Then the group G acts on the polynomial algebra $\mathbf{F}[V]$ as degree-preserving automorphisms. We denote the algebra of G-invariant polynomials by $\mathbf{F}[V]^G$.

Proposition 5.1. *Suppose the order of the finite group G is co-prime to the characteristic of $\mathbf{F}$. Then $m(\mathbf{F}[V]^G)$ divides $\exp(G)$ where $\exp(G)$ denotes the exponent of G.*

Proof. By Brauer lifting as described in [6, page 504] — we may assume the characteristic of $\mathbf{F}$ to be 0. Then, by Molien's Theorem, [7, Theorem 4.3.2, page 87], we have

$$P(t) = P(\mathbf{F}[V]^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - gt)}.$$

Extending the field does not affect either side of the equation, so we may assume that $\mathbf{F}$ is algebraically closed. Let g be in G. Then $\det(I - gt) = \prod_{i=1}^n (1 - \sigma_i(g)t)$ where g has eigenvalues $\sigma_1(g), \dots, \sigma_n(g)$. Furthermore, we have $\sigma_i(g)^{\exp(G)} = 1$ for all i, $1 \leq i \leq n$. Thus,

$$\begin{aligned} P(t) &= \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^n \frac{1}{1 - \sigma_i(g)t} \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\prod_{i=1}^n \frac{1 - t^{\exp(G)}}{1 - \sigma_i(g)t} \right) \frac{1}{(1 - t^{\exp(G)})^n} \\ &= \frac{b(t)}{(1 - t^{\exp(G)})^n}, \end{aligned}$$

for some polynomial $b(t) \in \mathbf{C}[t]$. But since $b(t) = P(t)(1 - t^{\exp(G)})^n$, we see that $b(t) \in \mathbf{Z}[t]$. It follows that m divides $\exp(G)$. □

Example 5.2. Let G be the group generated by the following two complex matrices:

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \imath \end{pmatrix}$$

Then, G is Abelian of order 8, exponent 4 and $P(t) = \frac{1}{(1-t^2)^3}$. Hence, m is strictly less than the exponent of G. We note that in [7, Example 1, page 77] it is shown that although the form the Poincaré series here suggests that $\mathbf{C}[V]^G$ is a polynomial algebra, this is not the case.

Example 5.3. Let G be the group of 3 by 3 upper triangular matrices over $\mathbf{F}_p$, $p \geq 3$ a prime. Now, from [5] or [7, Theorem 8.3.5, page 259] $\mathbf{F}_p[V]^G = \mathbf{F}_p[u_1, u_2, u_3]$ is a polynomial algebra with $\deg(u_i) = p^{i-1}$ and so $m = p^2$, by Proposition 4.5. However, $\exp(G) = p$ so Proposition 5.1 does not hold in the modular setting.

Theorem 5.4. *Let G be a finite group whose order is co-prime to the characteristic of $\mathbf{F}$, and let $\rho : G \to GL(V)$ be a representation of G on V a vector space of dimension n over $\mathbf{F}$. Let $\mathcal{F} = \{f_1, \dots, f_n\}$ be any homogeneous system of parameters for the ring of invariants $\mathbf{F}[V]^G$, and let ℓ be the least common multiple of their degrees. Then we have $m = m(\mathbf{F}[V]^G)$ divides $\exp(G)$ which in turn divides ℓ.*

Proof. We have already seen in Proposition 5.1 that $m \mid \exp(G)$.

Now we suppose p is a prime satisfying $p^r \mid\mid \exp(G)$. We may choose $g \in G$ of order p^r. Now $\mathcal{F}$ is a homogeneous system of parameters for $\mathbf{F}[V]^{<g>}$. Therefore, by extending the field if necessary, there exists a basis $\{x_1, \dots, x_n\}$ of V such that the matrix of $g = \operatorname{diag}(\sigma_1, \dots, \sigma_n)$, where the σ_is are the eigenvalues of g. As well, we may assume without loss of generality that σ_1 is a primitive p^r-th root of unity. Then $x_1^w \in \mathbf{F}[V]^{<g>}$ if and only if $p^r \mid w$. More generally, we observe that the group generated by g is diagonal and consequently monomials $x^I = x_1^{i_1} \cdots x_n^{i_n}$ are mapped to multiples of themselves by g. We have, therefore, that elements of $\mathbf{F}[V]^{<g>}$ are linear combinations of invariant monomials — in particular, this is true of the f_is.

Now x_1 is integral over $\mathbf{F}[f_1, \dots, f_n]$ so there exists a $s \in \mathbf{N}$ such that $x_1^s + \sum_{j=0}^{s-1} b_i x_1^j = 0$ for some choice of $b_i \in \mathbf{F}[f_1, \dots, f_n]$. We rewrite this equation in the form $x_1^s = \sum_{i=1}^n h_i f_i$ for some choice of $h_i \in \mathbf{F}[V]$. Of course, this can only happen if there is a k with $f_k = x_1^w +$ terms of lower degree in x_1. Moreover, w must be the degree of f_k. But f_k is a sum of invariant monomials in the x_is, and so $x_1^w \in \mathbf{F}[V]^{<g>}$ and $p^r \mid w = \deg(f_k) \mid \ell = \operatorname{lcm}(\deg f_1, \dots, \deg f_n)$. The result follows immediately. □

Example 5.5. If the ring of invariants is a polynomial algebra then its period m is the least common multiple of the degrees of its generators. However these form a homogeneous system of parameters and so by Theorem 5.4, $m = \exp(G)$. In particular, for a group G generated by complex pseudo-reflections the exponent of G equals the period of G is the least common multiple of the so-called degrees of G.

It is possible that for every choice of homogeneous system of parameters, $\exp(G) \neq \ell$ where ℓ is the least common multiple of the degrees occurring in the system, as shown in the following

Example 5.6. Consider, the group

$$G = \Big\langle x, y, z \ : \ x^3 = y^3 = z^3 = 1 \ , \ xz = zx \ , \ yz = zy \ , \ y^{-1}xy = xz \Big\rangle \, .$$

The group is of order 27 and exponent 3. Let $\rho : G \to \mathrm{Gl}(V)$ be one of the two inequivalent irreducible 3 dimensional representations of G over $\mathbf{C}$. Let f_1, f_2, f_3 be a homogeneous system of parameters for $\mathbf{C}[V]^G$, and let $\ell = \mathrm{lcm}(\deg f_i)$. If $\ell = 3$ then, since $27 = |G| \mid \prod \deg f_i$, we conclude that $\deg f_i = 3$, $i = 1, 2, 3$. It follows that $\mathbf{C}[V]^G = \mathbf{C}[f_1, f_2, f_3]$ is a polynomial algebra. But this cannot be, since (G, ρ) is not one of the groups and representations on the list of Shephard and Todd, see [7, page 199] classifying those groups and their complex representation with polynomial rings of invariants.

Remark 5.7. However, if G is an Abelian group of exponent e and the characteristic of the field does not divide the order of the group then every representation of the group can be diagonalized with respect to some basis $\{x_1, \dots, x_n\}$. Then $\{x_1^e, \dots, x_n^e\}$ is a homogeneous system of parameters.

Remark 5.8. We have just seen that the exponent of G divides the least common multiple of the degrees of any homogeneous system of parameters if the order of G is co-prime to the characteristic p of the field, $\mathbf{F}$ (i.e., in the "non-modular case"). However this result is true in general since this result for the case when $p \mid |G|$ (the "modular case") has been proved by Gregor Kemper, [4].

References

[1] Winfried Bruns and Jürgen Herzog, *Cohen-Macaulay rings*, 2nd ed., Studies in Advanced Mathematics, vol. 39, Cambridge University Press, New York, 1993.

[2] H E A Campbell, J C Harris, and D L Wehlau, *On rings of invariants of non-modular Abelian groups*, submitted, 12 pages.

[3] S Goto and K Watanabe, *On Graded Rings, I*, J. Math. Soc. Japan, **30** No. 2, 1978.

[4] G Kemper, preprint (1996).

[5] Huỳhn Mùi, *Modular invariant theory and the cohomology algebras of the symmetric groups*, J. Fac. Sci. Univ. Tokyo, Sec. IA (1975), 319–369.

[6] W M Singer, *The transfer in homological algebra*, Math. Z. **202** (1989), 493–523.

[7] L Smith, *Polynomial invariants of finite groups*, A K Peters, Wellesley, MA USA, 1995.

[8] R P Stanley, *Hilbert functions of graded algebras*, Adv. in Math. **28** (1978), 57–83.

Department of Mathematics and Statistics, Queen's University,
Kingston, Ontario, Canada, K7L 3N6
E-mail address: eddy@mast.queensu.ca, hughesi@queensu.ca, tony@mast.queensu.ca

Department of Mathematics, Brandeis University, Waltham, Massachusetts USA, 02254
E-mail address: ggsmith@math.berkeley.edu

Department of Mathematics and Computer Science, Royal Military College, Kingston, Ontario, Canada, K7K 7B4
E-mail address: wehlau@mast.queensu.ca, wehlau@rmc.ca