ELSEVIER
Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Pure and Applied Algebra 196 (2005) 313–321
JOURNAL OF PURE AND APPLIED ALGEBRA
www.elsevier.com/locate/jpaa

The F-signature of an affine semigroup ring

Anurag K. Singh[1]

School of Mathematics, Georgia Institute of Technology, 686 Cherry Street, Atlanta, GA 30332-0160, USA

Received 29 March 2004; received in revised form 18 June 2004
Communicated by A.V. Geramita
Available online 30 September 2004

Dedicated to Professor Kei-ichi Watanabe on the occasion of his 60th birthday

Abstract

We prove that the F-signature of an affine semigroup ring of positive characteristic is always a rational number, and describe a method for computing this number. We use this method to determine the F-signature of Segre products of polynomial rings, and of Veronese subrings of polynomial rings. Our technique involves expressing the F-signature of an affine semigroup ring as the difference of the Hilbert-Kunz multiplicities of two monomial ideals, and then using Watanabe's result that these Hilbert-Kunz multiplicities are rational numbers.

MSC: 13A35; 13D40; 14M12

1. Introduction

Let $(R, \mathfrak{m})$ be a Cohen–Macaulay local or graded ring of characteristic $p > 0$, such that the residue field $R/\mathfrak{m}$ is perfect. We assume that R is reduced and F-finite. Throughout q shall denote a power of p, i.e., $q = p^e$ for $e \in \mathbb{N}$. Let

$$R^{1/q} \approx R^{a_q} \oplus M_q,$$

where M_q is an R-module with no free summands. The number a_q is unchanged when we replace R by its $\mathfrak{m}$-adic completion, and hence is well-defined by the Krull–Schmidt

E-mail address: singh@math.gatech.edu (A.K. Singh).
[1]Supported in part by the National Science Foundation under Grants DMS-0070268 and DMS-0300600.

0022-4049/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2004.08.001

theorem. In [7] Huneke and Leuschke define the *F-signature* of R as

$$s(R) = \lim_{q\to\infty} \frac{a_q}{q^{\dim R}},$$

provided this limit exists. In this note we study the F-signature of normal monomial rings, and our main result is

Theorem 1. *Let K be a perfect field of positive characteristic, and R be a normal subring of a polynomial ring $K[x_1, \dots, x_n]$ which is generated, as a K-algebra, by monomials in the variables $x_1, \dots, x_n$. Then the F-signature $s(R)$ exists and is a positive rational number.*

Moreover, $s(R)$ depends only on the semigroup of monomials generating R and not on the characteristic of the perfect field K.

We also develop a general method for computing $s(R)$ for monomial rings, and use it to determine the F-signature of Segre products of polynomial rings, and of Veronese subrings of polynomial rings.

In general, it seems reasonable to conjecture that the limit $s(R)$ exists and is a rational number. Huneke and Leuschke proved that the limit exists if R is a Gorenstein ring, [7, Theorem 11]. They also proved that a ring R is weakly F-regular whenever the limit is positive, and this was extended by Aberbach and Leuschke in [2].

Theorem 2. (Huneke and Leuschke [7], Aberbach and Leuschke [2]). *Let $(R, \mathfrak{m})$ be an F-finite reduced Cohen–Macaulay ring of characteristic $p > 0$. Then R is strongly F-regular if and only if*

$$\limsup_{q\to\infty} \frac{a_q}{q^{\dim R}} > 0.$$

Further results on the existence of the F-signature are obtained by Aberbach and Enescu in the recent preprint [1]. Also, the work of Watanabe and Yoshida [12] and Yao [13] is closely related to the questions studied here.

We mentioned that a graded R-module decomposition of $R^{1/q}$ was used by Peskine–Szpiro, Hartshorne and Hochster, to construct small Cohen–Macaulay modules for R in the case where R is an $\mathbb{N}$-graded ring of dimension three, finitely generated over a field R_0 of characteristic $p > 0$, see [5, Section 5 F]. The relationship between the R-module decomposition of $R^{1/q}$ and the singularities of R was investigated by Smith and Van den Bergh in [9].

2. Semigroup rings

The semigroup of nonnegative integers will be denoted by $\mathbb{N}$. Let $x_1, \dots, x_n$ be variables over a field K. By a *monomial* in the variables $x_1, \dots, x_n$, we will mean an element $x_1^{h_1} \cdots x_n^{h_n} \in K[x_1, \dots, x_n]$ where $h_i \in \mathbb{N}$. We frequently switch between semigroups of monomials in $x_1, \dots, x_n$ and subsemigroups of $\mathbb{N}^n$, where we identify a monomial $x_1^{h_1} \cdots x_n^{h_n}$ with $(h_1, \dots, h_n) \in \mathbb{N}^n$. A semigroup M of monomials is *normal* if it is finitely generated, and whenever a, b and c are monomials in M such that $ab^k = c^k$ for some positive integer k, then there exists a monomial $\alpha \in M$ with $\alpha^k = a$. It is well-known that a semigroup M of monomials is normal if and only if the subring $K[M] \subseteq K[x_1, \dots, x_n]$ is a normal ring, see [3, Proposition 1].

A semigroup M of monomials is *full* if whenever a, b and c are monomials such that $ab = c$ and $b, c \in M$, then $a \in M$. By Hochster [3, Proposition 1], a normal semigroup of monomials is isomorphic (as a semigroup) to a full semigroup of monomials in a possibly different set of variables.

Lemma 3. *Let $A = K[x_1, \dots, x_n]$ be a polynomial ring over a field K, and $R \subseteq A$ be a subring generated by a full semigroup of monomials. Let $\mathfrak{m}$ denote the homogeneous maximal ideal of R, and assume that R contains a monomial μ in which each variable x_i occurs with positive exponent. For positive integers t, let $\mathfrak{a}_t$ denote the ideal of R generated by the monomials in R which do not divide μ^t.*

(1) *The ideals $\mathfrak{a}_t$ are irreducible and $\mathfrak{m}$-primary, and the image of μ^t generates the socle of the ring $R/\mathfrak{a}_t$.*
(2) *The ideals $\mathfrak{a}_t$ form a non-increasing sequence $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \mathfrak{a}_3 \supseteq \dots$ which is cofinal with the sequence $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \dots$.*
(3) *Let M be a finitely generated R-module with no free summands. Then $\mu^t M \subseteq \mathfrak{a}_t M$ for all $t \gg 0$.*
(4) *Let K be a perfect field of characteristic $p > 0$, and $R^{1/q} \approx R^{a_q} \oplus M_q$ be an R-module decomposition of $R^{1/q}$ where M_q has no free summands. Then*

$$a_q = \ell\left(\frac{R}{\mathfrak{a}_t^{[q]} :_R \mu^{tq}}\right) \quad \text{for all } t \gg 0.$$

Proof. (1) It suffices to consider $t = 1$ and $\mathfrak{a} = \mathfrak{a}_1$. Every non-constant monomial in R has a suitably high power which does not divide μ, so $\mathfrak{a}$ is $\mathfrak{m}$-primary. If $\alpha \in R$ is any monomial of positive degree, then $\alpha\mu \in \mathfrak{a}$, and so $\mathfrak{m} \subseteq \mathfrak{a} :_R \mu$. Also $\mu \notin \mathfrak{a}$, so we conclude that $\mathfrak{a} :_R \mu = \mathfrak{m}$. Since $\mathfrak{a}$ is a monomial ideal, the socle of $R/\mathfrak{a}$ is spanned by the images of some monomials. If $\theta \in R$ is a monomial whose image is a nonzero element of the socle of $R/\mathfrak{a}$, then $\mu = \beta\theta$ for a monomial $\beta \in R$. If $\beta \in \mathfrak{m}$ then $\mu \in \mathfrak{m}\theta \subseteq \mathfrak{a}$, a contradiction. Consequently we must have $\beta = 1$, i.e., $\theta = \mu$.

(2) Since each x_i occurs in $\mu \in R$ with positive exponent and R is generated by a full semigroup of monomials, we see that

$$\mathfrak{a}_t \subseteq (x_1^{t+1}, \dots, x_n^{t+1})A \cap R.$$

It follows that $\{\mathfrak{a}_t\}_{t\in\mathbb{N}}$ is cofinal with the sequence of ideals $\{\mathfrak{m}^t\}_{t\in\mathbb{N}}$.

(3) For an arbitrary element $m \in M$, consider the homomorphism $\phi : R \to M$ given by $r \mapsto rm$. Since the module M has no free summands, ϕ is not a split homomorphism. By Hochster [4, Remark 2], there exists $t_0 \in \mathbb{N}$ such that $\mu^{t_0} m \in \mathfrak{a}_{t_0} M$, equivalently, such that the induced map

$$\overline{\phi}_{t_0} : R/\mathfrak{a}_{t_0} \to M/\mathfrak{a}_{t_0} M$$

is not injective. If $\overline{\phi_t} : R/\mathfrak{a}_t \to M/\mathfrak{a}_t M$ is injective for some $t \geqslant t_0$, then it splits since $R/\mathfrak{a}_t$ is a Gorenstein ring of dimension zero; however this implies that the map

$$\overline{\phi}_{t_0} : R/\mathfrak{a}_t \bigotimes_{R/\mathfrak{a}_t} R/\mathfrak{a}_{t_0} \to M/\mathfrak{a}_t M \bigotimes_{R/\mathfrak{a}_t} R/\mathfrak{a}_{t_0}$$

splits as well, which is a contradiction. Consequently $\overline{\phi_t}(\overline{\mu^t}) = 0$, and hence $\mu^t m \in \mathfrak{a}_t M$ for all $t \gg t_0$. The module M is finitely generated, and so we must have $\mu^t M \subseteq \mathfrak{a}_t M$ for all $t \gg 0$.

(4) For any ideal $\mathfrak{b} \subseteq R$, we have

$$\frac{R^{1/q}}{\mathfrak{b}R^{1/q}} \cong \left(\frac{R}{\mathfrak{b}R}\right)^{a_q} \oplus \frac{M_q}{\mathfrak{b}M_q}$$

and so

$$\ell\left(\frac{R}{\mathfrak{b}^{[q]}}\right) = \ell\left(\frac{R^{1/q}}{\mathfrak{b}R^{1/q}}\right) = a_q \ell\left(\frac{R}{\mathfrak{b}}\right) + \ell\left(\frac{M_q}{\mathfrak{b}M_q}\right).$$

Using this for the ideals $\mathfrak{a}_t$ and $\mathfrak{a}_t + \mu^t R$ and taking the difference, we get

$$a_q\left[\ell\left(\frac{R}{\mathfrak{a}_t}\right) - \ell\left(\frac{R}{\mathfrak{a}_t + \mu^t R}\right)\right] + \ell\left(\frac{M_q}{\mathfrak{a}_t M_q}\right) - \ell\left(\frac{M_q}{\mathfrak{a}_t M_q + \mu^t M_q}\right)$$
$$= \ell\left(\frac{R}{\mathfrak{a}_t^{[q]}}\right) - \ell\left(\frac{R}{\mathfrak{a}_t^{[q]} + \mu^{tq} R}\right) = \ell\left(\frac{R}{\mathfrak{a}_t^{[q]} :_R \mu^{tq}}\right)$$

By (3) $\mu^t M_q \subseteq \mathfrak{a}_t M_q$ for all $t \gg 0$, and the result follows. □

Lemma 4. *Let K be a perfect field of characteristic $p > 0$, and R be a subring of $A = K[x_1, \ldots, x_n]$ generated by a full semigroup of monomials with the property that for every i with $1 \leqslant i \leqslant n$, there exists a monomial $a_i \in A$ in the variables $x_1, \ldots, \widehat{x_i}, \ldots, x_n$ such that $a_i/x_i = \mu_i/\eta_i$ for monomials $\mu_i, \eta_i \in R$. Let $\mu_0 \in R$ be a monomial in which each x_i occurs with positive exponent, and set $\mu = \mu_0\mu_1 \cdots \mu_n$. For $t \geqslant 1$, let $\mathfrak{a}_t$ be the ideal of R generated by monomials in R which do not divide μ^t. Then, for every prime power $q = p^e$ and integer $t \geqslant 1$, we have*

$$\mathfrak{a}_t^{[q]} :_R \mu^{tq} = \mathfrak{m}_A^{[q]} \cap R$$

where $\mathfrak{m}_A = (x_1, \ldots, x_n)A$ is the maximal ideal of A. If $R^{1/q} \approx R^{a_q} \oplus M_q$ is an R-module decomposition of $R^{1/q}$ where M_q has no free summands, then

$$a_q = \ell\left(\frac{R}{\mathfrak{a}_t^{[q]} :_R \mu^{tq}}\right) = \ell\left(\frac{R}{\mathfrak{m}_A^{[q]} \cap R}\right) \quad \textit{for all } q = p^e \textit{ and } t \geqslant 1.$$

Proof. By Lemma 3(4), it suffices to prove that

$$\mathfrak{a}_t^{[q]} :_R \mu^{tq} = \mathfrak{m}_A^{[q]} \cap R \quad \text{for all } q = p^e \text{ and } t \geqslant 1.$$

Given a monomial $r \in \mathfrak{a}_t^{[q]}:_R \mu^{tq}$, there exists a monomial $\eta \in R$ which does not divide μ^t for which $r\mu^{tq} \in \eta^q R$. Since μ^t/η is an element of the fraction field of R which is not in R, we must have $\mu^t/\eta \notin A$ and so $\eta A:_A \mu^t \subseteq \mathfrak{m}_A$. Taking Frobenius powers over the regular ring A, we get

$$\eta^q A:_A \mu^{tq} \subseteq \mathfrak{m}_A^{[q]}$$

and hence $r \in \mathfrak{m}_A^{[q]} \cap R$. This shows that $\mathfrak{a}_t^{[q]}:_R \mu^{tq} \subseteq \mathfrak{m}_A^{[q]} \cap R$.

For the reverse inclusion, consider a monomial $bx_i^q \in R$ where $b \in A$. Then

$$bx_i^q \mu^{tq} = ba_i^q \left(\frac{\mu^t \eta_i}{\mu_i}\right)^q,$$

where ba_i^q and $\mu^t\eta_i/\mu_i$ are elements of R. It remains to verify that $\mu^t\eta_i/\mu_i \in \mathfrak{a}_t$, i.e., that it does not divide μ^t in R. Since

$$\frac{\mu^t}{\mu^t\eta_i/\mu_i} = \frac{a_i}{x_i},$$

this follows immediately. □

Lemma 5. *Let R' be a normal monomial subring of a polynomial ring over a field K. Then R' is isomorphic to a subring R of a polynomial ring $A = K[x_1, \dots, x_n]$ where R is generated by a full semigroup of monomials, and for every $1 \leqslant i \leqslant n$, there exists a monomial $a_i \in A$ in the variables $x_1, \dots, \widehat{x_i}, \dots, x_n$, for which a_i/x_i is an element of the fraction field of R.*

Proof. *Let* $M \subseteq \mathbb{N}^r$ be the subsemigroup corresponding to the inclusion of rings $R' \subseteq K[y_1, \dots, y_r]$. Let $W \subseteq \mathbb{Q}^r$ denote the $\mathbb{Q}$-vector space spanned by M, and $W^* = \operatorname{Hom}_{\mathbb{Q}}(W, \mathbb{Q})$ be its dual vector space. Then

$$U = \{w^* \in W^* : w^*(m) \geqslant 0 \quad \text{for all } m \in M\}$$

is a finite intersection of half-spaces in W^*. Let $w_1^*, \dots, w_n^* \in U$ be a minimal $\mathbb{Q}_+$-generating set for U, where $\mathbb{Q}_+$ denotes the nonnegative rationals. Replacing each w_i^* by a suitable positive multiple, we may ensure that $w_i^*(m) \in \mathbb{N}$ for all $m \in M$, and also that $w_i^*(M) \nsubseteq a\mathbb{Z}$ for any integer $a \geqslant 2$. It is established in [3, Section 2] that the map $T : W \to \mathbb{Q}^n$ given by

$$T = (w_1^*, \dots, w_n^*)$$

takes M to an isomorphic copy $T(M) \subseteq \mathbb{N}^n$, which is a full subsemigroup of $\mathbb{N}^n$. Let $R \subseteq A = K[x_1, \dots, x_n]$ be the monomial subring corresponding to $T(M) \subseteq \mathbb{N}^n$.

Fix i with $1 \leqslant i \leqslant n$. Since $w_i^*(M) \nsubseteq a\mathbb{Z}$ for any integer $a \geqslant 2$, the fraction field of R contains an element $x_1^{h_1} \cdots x_n^{h_n}$ such that $h_1, \dots, h_n \in \mathbb{Z}$ and $h_i = -1$. Also, there exists $m \in M$ such that $w_i^*(m) = 0$ and $w_j^*(m) \neq 0$ for all $j \neq i$. Consequently R contains a monomial $\alpha = x_1^{s_1} \cdots x_n^{s_n}$ with $s_i = 0$ and $s_j > 0$ for all $j \neq i$. For a suitably large integer $t \geqslant 1$, the element

$$x_1^{h_1} \cdots x_n^{h_n} \alpha^t = a_i/x_i$$

belongs to the fraction field of R where $a_i \in A$ is a monomial in the variables $x_1, \dots, \widehat{x_i}, \dots, x_n$. $\square$

Proof of Theorem 1. By Lemma 5, we may assume that R is a monomial subring of $A = K[x_1, \dots, x_n]$ satisfying the hypotheses of Lemma 4. For the choice of μ as in Lemma 4, the ideals $\mathfrak{a}_t^{[q]} :_R \mu^{tq}$ do not depend on $t \in \mathbb{N}$. Setting $\mathfrak{a} = \mathfrak{a}_1$ we get

$$a_q = \ell\left(\frac{R}{\mathfrak{a}^{[q]} :_R \mu^q}\right) = \ell\left(\frac{R}{\mathfrak{a}^{[q]}}\right) - \ell\left(\frac{R}{\mathfrak{a}^{[q]} + \mu^q R}\right),$$

i.e., a_q, as a function of $q = p^e$, is a difference of two Hilbert–Kunz functions. Let $d = \dim R$. By Monsky [8] the limits

$$e_{\mathrm{HK}}(\mathfrak{a}) = \lim_{q\to\infty} \frac{1}{q^d}\, \ell\left(\frac{R}{\mathfrak{a}^{[q]}}\right) \quad \text{and} \quad e_{\mathrm{HK}}(\mathfrak{a} + \mu R) = \lim_{q\to\infty} \frac{1}{q^d}\, \ell\left(\frac{R}{\mathfrak{a}^{[q]} + \mu^q R}\right)$$

exist, and by Watanabe [11] they are rational numbers. Consequently the limit

$$\lim_{q\to\infty} \frac{a_q}{q^d} = e_{\mathrm{HK}}(\mathfrak{a}) - e_{\mathrm{HK}}(\mathfrak{a} + \mu R)$$

exists and is a rational number. The ring R is F-regular, so the positivity of $s(R)$ follows from the main result of [2]; as an alternative proof, we point out that $\mu \notin \mathfrak{a}^*$, and consequently $e_{\mathrm{HK}}(\mathfrak{a}) > e_{\mathrm{HK}}(\mathfrak{a} + \mu R)$ by Hochster and Huneke [6, Theorem 8.17].

By Watanabe [11] the Hilbert–Kunz multiplicities $e_{\mathrm{HK}}(\mathfrak{a})$ and $e_{\mathrm{HK}}(\mathfrak{a}+\mu R)$ do not depend on the characteristic of the field K, and so the same is true for $s(R)$. $\square$

Remark 6. Let $(R, \mathfrak{m}, K)$ be a local or graded ring of characteristic $p > 0$, and let $\eta \in E_R(K)$ be a generator of the socle of the injective hull of K. In [12] Watanabe and Yoshida define the minimal relative Hilbert–Kunz multiplicity of R to be

$$m_{\mathrm{HK}}(R) = \liminf_{e\to\infty} \frac{\ell(R/\mathrm{ann}_R(F^e(\eta)))}{p^{de}},$$

where $d = \dim R$. They compute $m_{\mathrm{HK}}(R)$ in the case R is the Segre product of polynomial rings [12, Theorem 5.8]. Their work is closely related to our computation of $s(R)$ in the example below.

3. Examples

Example 7. Let K be a perfect field of positive characteristic, and consider integers $r, s \geqslant 2$. Let R be the Segre product of the polynomial rings $K[x_1, \dots, x_r]$ and $K[y_1, \dots, y_s]$, i.e., R is subring of $A = K[x_1, \dots, x_r, y_1, \dots, y_s]$ generated over K be the monomials $x_i y_j$ for $1 \leqslant i \leqslant r$ and $1 \leqslant j \leqslant s$. It is well-known that R is isomorphic to the determinantal ring obtained by killing the size two minors of an $r \times s$ matrix of indeterminates, and that the dimension of the ring R is $d = r + s - 1$. Lemma 4 enables us to compute not just the F-signature $s(R)$, but also a closed-form expression for the numbers a_q.

The rings $R \subseteq A$ satisfy the hypotheses of Lemma 4, and so

$$a_q = \ell\left(\frac{R}{\mathfrak{m}_A^{[q]} \cap R}\right) = \ell\left(\frac{K[x_1,\ldots,x_r]}{(x_1^q,\ldots,x_r^q)} \# \frac{K[y_1,\ldots,y_s]}{(y_1^q,\ldots,y_s^q)}\right),$$

where # denotes the Segre product. The Hilbert–Poincaré series of these rings are

$$\mathrm{Hilb}\left(\frac{K[x_1,\ldots,x_r]}{(x_1^q,\ldots,x_r^q)}, u\right) = \frac{(1-u^q)^r}{(1-u)^r}, \quad \mathrm{Hilb}\left(\frac{K[y_1,\ldots,y_s]}{(y_1^q,\ldots,y_s^q)}, v\right) = \frac{(1-v^q)^s}{(1-v)^s}$$

and so a_q is the sum of the coefficients of $u^i v^i$ in the polynomial

$$\frac{(1-u^q)^r}{(1-u)^r}\frac{(1-v^q)^s}{(1-v)^s} \in \mathbb{Z}[u,v].$$

Therefore a_q equals the constant term of the Laurent polynomial

$$\frac{(1-u^q)^r}{(1-u)^r}\frac{(1-u)^{-q})^s}{(1-u^{-1})^s} = \frac{u^s(1-u^q)^{r+s}}{u^{sq}(1-u)^{r+s}} \in \mathbb{Z}[u,u^{-1}],$$

and hence the coefficient of $u^{s(q-1)}$ in

$$\frac{(1-u^q)^{r+s}}{(1-u)^{r+s}} = \left[\sum_{i=0}^{r+s}(-1)^i\binom{r+s}{i}u^{iq}\right]\left[\sum_{n\geqslant 0}\binom{d+n}{d}u^n\right].$$

Consequently we get

$$\begin{aligned} a_q &= \sum_{i=0}^{s}(-1)^i\binom{r+s}{i}\binom{d+s(q-1)-iq}{d} \\ &= \sum_{i=0}^{s}(-1)^i\binom{d+1}{i}\binom{q(s-i)+d-s}{d}, \end{aligned}$$

where we follow the convention that $\binom{m}{n} = 0$ unless $0 \leqslant n \leqslant m$. This shows that the F-signature of R is

$$s(R) = \lim_{q\to\infty}\frac{a_q}{q^d} = \frac{1}{d!}\sum_{i=0}^{s}(-1)^i\binom{d+1}{i}(s-i)^d.$$

We point out that $s(R) = A(d,s)/d!$ where the numbers

$$A(d,s) = \sum_{i=0}^{s}(-1)^i\binom{d+1}{i}(s-i)^d$$

are the *Eulerian numbers*, i.e., the number of permutations of d objects with $s-1$ *descents*; more precisely, $A(d,s)$ is the number of permutations $\pi = a_1a_2\cdots a_d \in S_d$ whose *descent set*

$$D(\pi) = \{i : a_i > a_{i+1}\}$$

has cardinality $s-1$, see [10, Section 1.3]. These numbers satisfy the recursion

$$A(d,s)=sA(d-1,s)+(d-s+1)A(d-1,s-1) \quad \text{where } A(1,1)=1.$$

Example 8. Let K be a perfect field of positive characteristic. For integers $n \geqslant 1$ and $d \geqslant 2$, let R be the nth Veronese subring of the polynomial ring $A=K[x_1,\dots,x_d]$, i.e., R is subring of A which is generated, as a K-algebra, by the monomials of degree n. In the case $d=2$ and $p \nmid n$, the F-signature of R is $s(R)=1/n$, as worked out in [7, Example 17].

It is readily seen that the rings $R \subseteq A$ satisfy the hypotheses of Lemma 4, and therefore

$$a_q=\ell\left(\frac{R}{\mathfrak{m}_A^{[q]}\cap R}\right).$$

Consequently a_q equals the sum of the coefficients of $1, t^n, t^{2n}, \dots$ in

$$\operatorname{Hilb}\left(\frac{K[x_1,\dots,x_d]}{(x_1^q,\dots,x_d^q)}, t\right)=\frac{(1-t^q)^d}{(1-t)^d}=(1+t+t^2+\cdots+t^{q-1})^d.$$

Let $f(m)$ be the sum of the coefficients of powers of t^n in

$$(1+t+t^2+\cdots+t^{m-1})^d.$$

A routine computation using, for example, induction on d, gives us $f(n)=n^{d-1}$, and it follows that

$$f(kn)=k^d f(n)=k^d n^{d-1}.$$

To obtain bounds for $a_q=f(q)$, choose integers k_i with $k_1 n \leqslant q \leqslant k_2 n$ where $0 \leqslant |q-k_i n| \leqslant n-1$. Then $f(k_1 n) \leqslant f(q) \leqslant f(k_2 n)$, and hence

$$\left(\frac{q-n+1}{n}\right)^d n^{d-1} \leqslant k_1^d n^{d-1} \leqslant a_q \leqslant k_2^d n^{d-1} \leqslant \left(\frac{q+n-1}{n}\right)^d n^{d-1}.$$

Consequently,

$$a_q=\frac{q^d}{n}+O(q^{d-1}),$$

and $s(R)=1/n$.

Acknowledgements

I would like to thank Ezra Miller for several useful discussions.

References

[1] I.M. Aberbach, F. Enescu, When does the F-signature exist? preprint.

[2] I.M. Aberbach, G.J. Leuschke, The F-signature and strong F-regularity, Math. Res. Lett. 10 (2003) 51–56.
[3] M. Hochster, Rings of invariants of tori, Cohen–Macaulay rings generated by monomials, and polytopes, Ann. of Math. 96 (2) (1972) 318–337.
[4] M. Hochster, Contracted ideals from integral extensions of regular rings, Nagoya Math. J. 51 (1973) 25–43.
[5] M. Hochster, Big Cohen–Macaulay modules and algebras and embeddability in rings of Witt vectors, Conference on Commutative Algebra—1975 Queen's Univ., Kingston, Ont., 1975, pp. 106–195. Queen's Papers on Pure and Applied Math., No. 42, Queen's Univ., Kingston, Ont., 1975.
[6] M. Hochster, C. Huneke, Tight closure, invariant theory, and the Briançon-Skoda theorem, J. Amer. Math. Soc. 3 (1990) 31–116.
[7] C. Huneke, G.J. Leuschke, Two theorems about maximal Cohen–Macaulay modules, Math. Ann. 324 (2002) 391–404.
[8] P. Monsky, The Hilbert–Kunz function, Math. Ann. 263 (1983) 43–49.
[9] K.E. Smith, M. Van den Bergh, Simplicity of rings of differential operators in prime characteristic, Proc. London Math. Soc. 75 (3) (1997) 32–62.
[10] R. Stanley, Enumerative Combinatorics, Vol. I, Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1986.
[11] K.-i. Watanabe, Hilbert–Kunz multiplicity of toric rings, Proc. Inst. Natural Sci., Nihon Univ. 35 (2000) 173–177.
[12] K.-i. Watanabe, K.-i. Yoshida, Minimal relative Hilbert–Kunz multiplicity, Illinois J. Math. 428 (2004) 273–294.
[13] Y. Yao, Observations on the F-signature of local rings of characteristic p, preprint.