Journal of Algebra **247**, 104–133 (2002)
doi:10.1006/jabr.2001.9020, available online at http://www.idealibrary.com on IDEAL®

Lengths of Tors Determined by Killing Powers of Ideals in a Local Ring

J. Bruce Fields

University of Michigan, Ann Arbor, Michigan
E-mail: bfields@umich.edu

Communicated by Craig Huneke

Received February 12, 2001

Given a local ring R and n ideals whose sum is primary to the maximal ideal of R, one may define a function which takes an n-tuple of exponents $(a_1, \ldots, a_n)$ to the length of $\operatorname{Tor}_k(R/I_1, \ldots, R/I_n)$. These functions are shown to have rational generating functions in certain cases.

In this paper we investigate functions

$$f_k = \operatorname{length}\left(\operatorname{Tor}_k^R\left(M_1/I_1^{a_1}M_1, \ldots, M_n/I_n^{a_n}M_n\right)\right),$$

where R is a (noetherian) local ring, M_i is a finitely generated R-module and I_i an ideal of R, for $1 \leq i \leq n$, and $I_1 + \cdots + I_n + \operatorname{Ann} M_1 + \cdots + \operatorname{Ann} M_n$ is primary to the maximal ideal of R.

Special cases of these functions are interesting in their own right; see, for example, the discussion below of Hilbert–Kunz functions. It is also hoped that a better understanding of these functions may lead to insights into the theory of intersection multiplicities; for example, it seems reasonable to attempt to calculate the intersection multiplicity of varieties defined by ideals I_1 and I_2 using only properties of the function

$$f_0(a_1, a_2) = \operatorname{length}\left(R/\left(I_1^{a_1} + I_2^{a_2}\right)\right),$$

although this has not yet proved possible. We are, however, able to establish certain properties of the functions f_k in some generality. In

0021-8693/02 $35.00

particular, they are shown to have rational generating functions in the following cases:

(1) $n = 2$, $M_1 = M_2 = R$, $k \geq 2$; or

(2) $n = 2$, $M_1 = M_2 = R$, k is arbitrary, R is regular, and

$$\bigoplus_{a_1, a_2 \geq 0} (I_1^{a_1} \cap I_2^{a_2}) t_1^{a_1} t_2^{a_2} \subset R[t_1, t_2]$$

is a finitely generated R-algebra; or

(3) n is arbitrary, $M_1 = \cdots = M_n = R$, $k = 0$, $R = K[[x_1, \ldots, x_d]]$ (K any field), and $I_1, \ldots, I_n$ are generated by monomials.

1. BASIC DEFINITIONS

All rings are commutative, and local rings are in addition assumed to be Noetherian.

Definition 1.1. Given n modules $M_1, \ldots, M_n$ over a ring R, define the R-module $\operatorname{Tor}_k^R(M_1, \ldots, M_n)$ by

(1) choosing a projective resolution

$$\cdots \to P_{i,3} \to P_{i,2} \to P_{i,1} \to P_{i,0} \to M_i \to 0$$

for each M_i,

(2) tensoring together all of these projective resolutions (with the modules M_i removed) and taking the total complex,

$$\cdots \to \bigoplus_{\substack{(i_1, \ldots, i_n) \\ \sum_j i_j = 2}} P_{1, i_1} \otimes \cdots \otimes P_{n, i_n} \to \bigoplus_{\substack{(i_1, \ldots, i_n) \\ \sum_j i_j = 1}} P_{1, i_1} \otimes \cdots \otimes P_{n, i_n}$$
$$\to P_{1,0} \otimes \cdots \otimes P_{n,0} \to 0,$$

and

(3) taking the kth homology of this complex.

This defines a functor, covariant in each of the n variables, which specializes for $n = 2$ to the usual Tor. It shares most of the basic properties with the usual 2-variable Tor; for example.

(1) A short exact sequence in any of the variables gives the usual long exact sequence.

(2) Any element of R that kills one of the M_i also kills $\operatorname{Tor}_k(M_1, \ldots, M_n)$.

(3) $\operatorname{Tor}_0^R(M_1, \dots, M_n) = M_1 \otimes_R \cdots \otimes_R M_n$.

(4) If all but one of the M_i is flat, then $\operatorname{Tor}_k(M_1, \dots, M_n) = 0$ for all $k > 0$.

(5) If the M_i are all finitely generated over R, so is $\operatorname{Tor}_i(M_1, \dots, M_n)$.

DEFINITION 1.2. Let R be a Noetherian ring, let n be a positive integer, let $M_1, \dots, M_n$ be finitely generated R-modules, and let $I_1, \dots, I_n$ be ideals of R. Let $J = I_1 + \cdots + I_n + \operatorname{Ann}_R(M_1) + \cdots + \operatorname{Ann}_R(M_n)$, and assume that R/J has finite length. For k a non-negative integer, define

$$f_k(a_1, \dots, a_n) = \operatorname{length}\left(\operatorname{Tor}_k\left(M_1/I_1^{a_1}M_1, \dots, M_n/I_n b^{a_n} M_n\right)\right).$$

Note that the modules $\operatorname{Tor}_k(M_1/I_1^{a_1}M_1, \dots, M_n/I_n^{a_n}M_n)$ do have finite length, since they are finitely generated modules that are killed by the ideal $J' = I_1^{a_1} + \cdots + I_n^{a_n} + \operatorname{Ann} M_1 + \cdots + \operatorname{Ann} M_n$, and hence are finitely generated modules over R/J', which has finite length. (This is because J' has the same radical as the ideal J above, and R/J is assumed to be finite length.)

In this paper, the ring R will always be local, and the modules $M_1, \dots, M_n$ will almost always be equal to R.

We conclude this section with some examples.

(1) If $n = 1$, then f_0 is the usual Hilbert function and is eventually a polynomial of degree $d = \dim R$.

(2) In [2, 3], Brown studies f_0 in the case $n = 2$ and $M = R$; he calls this function the Hilbert function of I_1 and I_2. In [2], he gives sufficient conditions for f_0 to be eventually polynomial (in other words, for there to exist (b_1, b_2) such that $f_0(a_1, a_2)$ agrees with a polynomial for all $(a_1, a_2) \geq (b_1, b_2)$). In [3], he considers the case where f_0 is eventually a polynomial in a_1, a_2, and $\min(a_1, a_2)$. Both papers also provide several examples of such functions, including examples which show that f_0 is not necessarily eventually a polynomial in a_1, a_2, and $\min(a_1, a_2)$. He also provides counterexamples to a more general conjecture that f_0 is eventually polynomial on regions bordered by parallel lines.

(3) If $M_1 = \cdots = M_N = M$, $I_1, \dots, I_n$ are all principal ideals, and R has characteristic p, for $p > 0$ a prime, then the function $\mathrm{HK}_{M,I}\colon a \mapsto f_0(p^a, \dots, p^a)$ is called the Hilbert–Kunz function on M of the ideal $I = I_1 + \cdots + I_n$. The more standard definition is in terms of bracket powers,

$$I^{[p^e]} = \left(\{ i^{p^e} | i \in I \}\right).$$

With this notation, $\mathrm{HK}_{M,I}(a) = \text{length}(M/I^{[p^e]}M)$. Because R has characteristic p, $I^{[p^e]} = I_1^{p^e} + \cdots + I_n^{p^e}$, which shows that $\mathrm{HK}_{M,I}$ is dependent only on I and not on the choice of $I_1, \ldots, I_n$.

Monsky has shown [15] that this function has the form

$$e_{\mathrm{HK}}(M, I)\, p^{da} + O\big(p^{a(d-1)}\big),$$

where $d = \dim M$ and $e_{\mathrm{HK}}(M, I)$ is a positive real constant. The constant $e_{\mathrm{HK}}(R, m)$ may be written $e_{\mathrm{HK}}(R)$, and $\mathrm{HK}_{R,m}$ may be written HK_R and called just the Hilbert–Kunz function of R.

It is not even known in general whether $\mathrm{e}_{\mathrm{HK}}(R)$ is rational. However, many results have been proved in particular cases; see [4, 6, 10, 15–18, 22].

The Hilbert–Kunz function also has an important connection with the theory of tight closure. If $I \subset J$ are m-primary ideals of R, then $I^* = J^*$ if and only if $e_{\mathrm{HK}}(R, I) = \mathrm{e}_{\mathrm{HK}}(R, J)$. This statement is true when R is a complete local domain, and in somewhat more generality. (See [13, Theorem 8-17], or see the more thorough discussion in [12].)

(4) In [7], Contessa considers the generalization of the previous situation to the case of arbitrary k. She is able to use results about the higher Tors to determine the form of Hilbert–Kunz functions of modules over regular rings of dimension at most two.

2. QUASIPOLYNOMIAL FUNCTIONS

Given an $\mathbb{N}^n$-graded module M having finite length in each graded piece, there is a natural notion of a Hilbert function $\mathbb{N}^n \to \mathbb{N}$ given by

$$(a_1, \ldots, a_n) \mapsto \text{length}\big(M_{(a_1, \ldots, a_n)}\big).$$

For $n = 1$ this is the usual Hilbert function. We will see that certain $\mathbb{N}^n$-graded algebraic objects (including, for example, finitely generated modules over finitely generated algebras over fields) have Hilbert functions which have rational generating functions. In fact, these Hilbert functions are *quasipolynomial*, a stronger condition. This fact will be used to prove that in some cases the functions f_k are also quasipolynomial.

Most of the results of this section are known, though not perhaps in the form we need them; see, for example, [14].

Most of the functions considered here are defined on $\mathbb{N}^n$. However, it will be convenient to identify such functions with functions defined on all of $\mathbb{Z}^n$ that are zero for elements of $\mathbb{Z}^n$ not in $\mathbb{N}^n$.

DEFINITION 2.1. Given linearly independent vectors $\alpha_1, \ldots, \alpha_e \in \mathbb{N}^n$, say that a function $f\colon \mathbb{N}^n \to \mathbb{Z}$ is *periodic with respect to* $\alpha_1, \ldots, \alpha_e$ if the function $\alpha \mapsto f(\alpha + \gamma) - f(\alpha)$ is identically zero on $\mathbb{N}^n$, for any $\gamma \in \mathbb{N}\alpha_1 + \cdots + \mathbb{N}\alpha_e$.

DEFINITION 2.2. Given $\beta \in \mathbb{N}^n$ and linearly independent vectors $\alpha_1, \ldots, \alpha_e \in \mathbb{N}^n$, the *cone with vertex β generated by $\alpha_1, \ldots, \alpha_e$* is

$$C_{\beta, \alpha_1, \ldots, \alpha_e} = \beta + \mathbb{R}_{\geq 0}\alpha_1 + \cdots + \mathbb{R}_{\geq 0}\alpha_e \subset \mathbb{R}^n_{\geq 0}.$$

Given $x = (x_1, \ldots, x_n)$ and $a = (a_1, \ldots, a_n)$, x^a will be used in the following as a shorthand for $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$.

DEFINITION 2.3. Let $\alpha_1, \ldots, \alpha_e \in \mathbb{N}^n$ be linearly independent vectors in $\mathbb{R}^n$, and let β be another element of $\mathbb{N}^n$. Let $C = C_{\beta, \alpha_1, \ldots, \alpha_e}$ be the cone with vertex β generated by $\alpha_1, \ldots, \alpha_e$. Call f: $\mathbb{N}^n \to \mathbb{Z}$ *simple quasipolynomial of polynomial degree d on $\beta, \alpha_1, \ldots, \alpha_e$* if $f(x) = 0$ for $x \notin C$ and

$$f(x) = \sum_{\alpha \in \mathbb{N}^n} c_\alpha(x) x^\alpha$$

for $x \in C$, where each c_α, considered as a function of x, is periodic with respect to $\alpha_1, \ldots, \alpha_e$ and is identically zero for all $\alpha = (a_1, \ldots, a_n)$ such that $\Sigma a_i > d$, and where there exists an α satisfying $\Sigma a_i = d$ such that $c_\alpha(x)$, as a function of x, is not identically zero.

If $\beta = 0$, $e = n$, and $\alpha_1, \ldots, \alpha_e \in \mathbb{N}^n$ are generators of the lattice $\mathbb{Z}^n$, then the functions $c_\alpha(x)$ do not depend on x, and the simple quasipolynomials of polynomial degree d on β, $\alpha_1, \ldots, \alpha_e$ are exactly the integer-valued polynomials of degree d on $\mathbb{N}^n$.

We use the term "polynomial degree" and not just "degree" because there is also a second notion of degree:

DEFINITION 2.4. The *cumulative degree* of a simple quasipolynomial of polynomial degree d on β, $\alpha_1, \ldots, \alpha_e$ is $d + e$.

The cumulative degree will turn out to be the more useful number for our purposes. It will also be convenient to allow simple quasipolynomial functions of cumulative degree 0, defined as follows.

DEFINITION 2.5. A function f: $\mathbb{N}^n \to \mathbb{Z}$ is *simple quasipolynomial of cumulative degree* 0 if it is nonzero on at most a single element of $\mathbb{N}^n$.

LEMMA 2.6. *If f_1 and f_2 are both simple quasipolynomial functions on β, $\alpha, \ldots, \alpha_e$, of cumulative degree d_1 and d_2, respectively, then $f_1 + f_2$ is also simple quasipolynomial on β, $\alpha_1, \ldots, \alpha_e$, of cumulative degree at most* $\max(d_1, d_2)$.

Proof. The proof is immediate from the definition of a simple quasipolynomial function. ∎

DEFINITION 2.7. Given a function $f\colon \mathbb{N}^n \to \mathbb{Z}$, recall that the *generating function of* f is the power series $F \in \mathbb{Z}[x_1, \dots, x_n]$ defined by

$$F(x) = \sum_{\alpha \in \mathbb{N}^n} f(\alpha) x^{\alpha}.$$

LEMMA 2.8. *Let $F(x_1, \dots, x_n)$ be the generating function of $f\colon \mathbb{N}^n \to \mathbb{Z}$, fix ($\beta \in \mathbb{N}^n$, and fix a linearly independent set of vectors $\alpha_1, \dots, \alpha_e \in \mathbb{N}^n$. Suppose*

$$F(x_1, \dots, x_n) = \frac{1}{\prod_{j=1}^{e} (1 - x^{\alpha_j})^{d_j}}$$

with $\sum_{j=1}^{e} d_j = d$. Then f is the simple quasipolynomial function of cumulative degree d given by

$$f(a_1, \dots, a_n) = \begin{cases} \prod_j \binom{d_j - 1 + m_j}{m_j} & \text{if } (a_1, \dots, a_n) = \sum_j m_j \alpha_j, \\ 0 & \text{otherwise}. \end{cases}$$

Proof. Given $\alpha \in \mathbb{N}^n$, there is at most one way of writing α as an $\mathbb{N}$-linear combination of $\alpha_1, \dots, \alpha_e$. This means that the coefficient of x^{α} in F is nonzero if and only if α can be written as the $\mathbb{N}$-linear combination of $\alpha_1, \dots, \alpha_e$. If α is such an exponent, write $\alpha = \sum m_j \alpha_j$. Then the coefficient of x^{α} in F is the product of the coefficients of $x^{m_j \alpha_j}$ in $1/(1 - x^{\alpha_j})^{d_j}$, and it is easy to verify that these coefficients are just the binomial coefficients given in the description of f above. ∎

DEFINITION 2.9. Given a polynomial $P(x_1, \dots, x_n)$, define $\operatorname{Supp} P$, the support of P, to be the set of all $\alpha \in \mathbb{N}^n$ such that the coefficient of x^{α} in P is nonzero.

DEFINITION 2.10. Given linearly independent vectors $\alpha_1, \dots, \alpha_e \in \mathbb{N}^n$ and another vector $\beta \in \mathbb{N}^n$, let

$$\Pi_{\beta, \alpha_1, \dots, \alpha_e} = \left\{ \alpha \in \mathbb{N}^n \,\middle|\, \alpha = \beta + \sum_i m_i \alpha_i, 0 \le m_i < 1 \right\}.$$

Given any $\alpha \in C_{\beta, \alpha_1, \dots, \alpha_e} \cap \mathbb{N}^n$, there is a unique representative of α modulo $\alpha_1, \dots, \alpha_e$ in $\Pi_{\beta, \alpha_1, \dots, \alpha_e}$; in the following, we use $\overline{\alpha}$ to denote that unique representative.

LEMMA 2.11. *Let $F(x_1, \dots, x_n)$ be the generating function of $f\colon \mathbb{N}^n \to \mathbb{Z}$, fix $\beta \in \mathbb{N}^n$, and fix a linearly independent set of vectors $\alpha_1, \dots, \alpha_e \in \mathbb{N}^n$. Suppose*

$$F(x_1, \dots, x_n) = \frac{P}{\prod_{j=1}^{e} (1 - x^{\alpha_j})^{d_j}}$$

with $\sum_{j=1}^{e} d_j = d$ *and* $\operatorname{Supp} P \subset \Pi = \Pi_{\beta, \alpha_1, \dots, \alpha_e}$. *Write* $P = \sum_{\alpha \in \Pi} c_\alpha x^\alpha$, *with each* $c_\alpha \in \mathbb{Z}$ *a constant. Then f is the simple quasipolynomial function of cumulative degree d given by*

$$f(\alpha) = \prod_j c_{\bar{\alpha}} \binom{d_j - 1 + m_j}{m_j} \qquad \left(\text{where } \alpha = \bar{\alpha} + \sum_j m_j \alpha_j\right).$$

Proof. The generating function F can be written as the sum of the fractions

$$\frac{c_\alpha x^\alpha}{\prod_{j=1}^{e} (1 - x^{\alpha_j})^{d_j}}.$$

The result then follows from the previous lemma. ∎

LEMMA 2.12. *Fix* $\beta \in \mathbb{N}^n$, *and fix linearly independent vectors* $\alpha_1, \dots, \alpha_e \in \mathbb{N}^n$. *Then functions of the form*

$$F(x_1, \dots, x_n) = \frac{x^\alpha}{\prod_{j=1}^{e} (1 - x^{\alpha_j})^{d_j}}$$

with $\alpha \in \Pi = \Pi_{\beta, \alpha_1, \dots, \alpha_e}$, *and* $\sum_{j=1}^{e} d_j \le d$, *form a* $\mathbb{Z}$*-basis for the generating functions of the simple quasipolynomial functions of cumulative degree at most d on* $\beta, \alpha_1, \dots, \alpha_e$.

Proof. This is a consequence of the previous lemma and of the fact that the functions

$$(a_1, \dots, a_e) \mapsto \prod_j \binom{d_j - 1 + a_j}{a_j},$$

with $\sum (d_j - 1)$ at most d, form a basis over $\mathbb{Z}$ for the polynomials of degree at most d. (See, e.g., Theorem 11.1.12 of [5].) ∎

It will prove useful (in particular, in Theorem 2.25) to know something about the restriction of a simple quasipolynomial function to a smaller cone with different generators.

LEMMA 2.13. *Let* f_1 *be simple quasipolynomial on* $\beta, \alpha_1, \dots, \alpha_e$ *of cumulative degree d. Pick* $\beta' \in \mathbb{N}^n$ *and linearly independent* $\alpha_1', \dots, \alpha_{e'}'$ *such that*

$$C' = C_{\beta', \alpha_1', \dots, \alpha_{e'}'} \subseteq C = C_{\beta, \alpha_1, \dots, \alpha_e}.$$

Define a new function f' such that $f'(\alpha) = \alpha$ for $\alpha \in C'$ and $f'(\alpha) = 0$ for $\alpha' \in C'$. Then there exist positive integers m_i such that f' is simple quasipolynomial of cumulative degree at most d on β', $m_1\alpha'_1, \dots, m_{e'}\alpha'_{e'}$.

Proof. For each α'_i, choose m_i such that $m_i\alpha'_i \in \mathbb{N}\alpha_1 + \cdots + \mathbb{N}\alpha_e$. Since f is simple quasipolynomial, we know that

$$f(x) = \sum_{\alpha \in \mathbb{N}^n} c_\alpha(x)x^\alpha$$

for $x \in C$, where c_α is periodic with respect to $\alpha_1, \dots, \alpha_e$ and is identically zero for all $\alpha = (a_1, \dots, a_n)$ such that $\Sigma a_i > d - e$. Since the c_α's are periodic with respect to $\alpha_1, \dots, \alpha_e$, they are also periodic with respect to $m_1\alpha'_1, \dots, m_{e'}\alpha_{e'}$. Therefore f' is also simple quasipolynomial. The bound on the degrees of the terms x^α bounds the polynomial degree of f' above by $d - e$. The cumulative degree of f' is therefore at most $d - e + e' \leq d$. ∎

The next definition, and the following theorem, make it possible to reduce the proofs of theorems about quasipolynomial functions defined on $\mathbb{N}^n$ to the $n = 1$ case.

DEFINITION 2.14. Given a function f $\mathbb{N}^n \to \mathbb{N}$, define a new function f^* by

$$f^*(a) = \sum_{a_1 + \cdots + a_n = a} f(a_1, \dots, a_n).$$

THEOREM 2.15. *If f: $\mathbb{N}^n \to \mathbb{N}$ is simple quasipolynomial of cumulative degree d, then f^*: $\mathbb{N} \to \mathbb{N}$ is also simple quasipolynomial of cumulative degree d.*

Proof. Write F for the generating function associated with f, and write F^* for the generating function associated with f^*. Then $F^*(y) = F(y, \dots, y)$. By Lemma 2.12, F has the form

$$\frac{P(x)}{\prod_{j=1}^{e}(1 - x^{\alpha_j})^{d_j}},$$

so by substituting $(y, \dots, y)$ for $(x_1, \dots, x_n) = x$, we see that F^* has the form

$$\frac{P'(y)}{\prod_{j=1}^{e}(1 - y^{a_j})^{d_j}},$$

where by a_j we mean the sum of the coordinates of the vector α_j. By Lemma 2.12 again, this is the generating function of a quasipolynomial function of cumulative degree at most d, so f^* must be quasipolynomial of cumulative degree at most d.

It remains only to show that the cumulative degree of f^* is not less than d. Let C, β, $\alpha_1, \ldots, \alpha_e$, and the functions c_α be as in the definition of a simple quasipolynomial function (Definition 2.3). Without loss of generality we may assume that $\beta = 0$. Let $\Lambda^* = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_e$, and let $\Lambda^+ = \mathbb{N}\alpha_1 + \cdots + \mathbb{N}\alpha_e$. We can also assume without loss of generality that $c_\alpha(x) = 0$ for any $x \notin \Lambda^+$. Since $c_\alpha(x)$ is periodic with respect to $\alpha_1, \ldots, \alpha_e$, f may now be written in the form

$$f(x) = \begin{cases} \sum_\alpha c_\alpha x^\alpha & \text{for } x \in \Lambda^+ \\ 0 & \text{for } x \notin \Lambda^+, \end{cases}$$

where the c_α's are constants not depending on x. Write $p(x)$ for the polynomial function $p(x) = \sum_\alpha c_\alpha x^\alpha$. Then

$$\begin{aligned} f^*(a) &= \sum_{a_1 + \cdots + a_n = a} f(a_1, \ldots, a_n) \\ &= \sum_{\substack{a_1 + \cdots + a_n = a \\ (a_1, \ldots, a_n) \in \Lambda^+}} p(a_1, \ldots, a_n). \end{aligned}$$

Since f has cumulative degree d, p is a polynomial of degree $d - e$. To prove that f^* has cumulative degree at least d, it will suffice to show that f^* is bounded below by a polynomial of degree $d - 1$. Let p_{d-e} be the $d - e$ degree part of p, and let $f_{d-e} = p_{d-e}|_{\Lambda^+}$ be the corresponding polynomial degree $d - e$ part of f. It will suffice to show that $(f_{d-e})^*$ is bounded below by a polynomial of degree $d - 1$.

If $p_{d-e}(a_1, \ldots, a_n)$ were negative for some $(a_1, \ldots, a_n) \in \Lambda^+$, then the polynomial function

$$\begin{aligned} a \mapsto p(aa_1, \ldots, aa_n) &= p_{d-e}(aa_1, \ldots, aa_n) + \text{lower order terms} \\ &= p_{d-e}(a_1, \ldots, a_n) a^d + \text{lower order terms} \end{aligned}$$

would have a negative leading term, and p would eventually take on negative values. In particular, since multiples of $(a_1, \ldots, a_n)$ are also contained in Λ^+, p would take on negative values on Λ^+. But this does not happen, so p_{d-e} must be nonnegative on Λ^+. It also cannot be the case that p_{d-e} is identically zero on Λ^+. So p_{d-e} must be positive for some $\beta = (b_1, \ldots, b_n) \in \Lambda^+$.

Let $\pi\colon \mathbb{R}^n \to \mathbb{R}$ be the mapping defined by $\pi(a_1, \dots, a_n) = \sum_i a_i$, and write $b = \pi(\beta)$. The subset of $\pi^{-1}(b)$ on which p_{d-e} is zero is a proper algebraic subset of $\pi^{-1}(b)$, so one can find a positive real number c and an $(n-1)$-dimensional disk $\Delta \subset \pi^{-1}(b)$ contained in the $\mathbb{R}^+$-span of $\alpha_1, \dots, \alpha_e$ such that $p_{d-e}(\alpha) \geq c$ for any $\alpha \in \Delta$. Note that any positive a and any $\alpha \in \Delta$, $p_{d-e}(a\alpha) = a^{d-e} p_{d-e}(\alpha) \geq c a^{d-e}$, so $p_{d-e}(\alpha) \geq c a^{d-e}$ for any $\alpha \in a\Delta$.

Now for any $a \in \mathbb{N}$,

$$\begin{aligned}
(f_{d-e})^*(a) &= \sum_{\alpha \in \pi^{-1}(a) \cap \Lambda^+} p_{d-e}(\alpha) \\
&\geq \sum_{\alpha \in (\frac{a}{b}\Delta) \cap \Lambda^+} p_{d-e}(\alpha) \\
&\geq \sum_{\alpha \in (\frac{a}{b}\Delta) \cap \Lambda^+} c\left(\frac{a}{b}\right)^{d-e} \\
&= \#\left(\left(\frac{a}{b}\Delta\right) \cap \Lambda^+\right) c\left(\frac{a}{b}\right)^{d-e},
\end{aligned}$$

where the notation $\#((\frac{a}{b}\Delta) \cap \Lambda^+)$ is used to denote the number of members of the set $(\frac{a}{b}\Delta) \cap \Lambda^+$.

Therefore it suffices to show that the cardinality of the set $(a\Delta) \cap \Lambda^+$ is bounded below by a polynomial in a of degree $e-1$.

Note that the intersection of $a\Delta$ with the $\mathbb{Q}_{\geq 0}$-span of the α_i's is dense in $a\Delta$. Therefore we can choose linearly independent $\alpha_1', \dots, \alpha_e'$ in $a\Delta$ such that each α_i' is a linear combination of the α_i's with coefficients in $\mathbb{Q}_{\geq 0}$. Clear denominators, letting $m \in \mathbb{N}$ be such that $m\alpha_i' \in \Lambda^+$ for all i, and write α_i'' for $m\alpha_i'$. Then $\alpha_1'', \dots, \alpha_e'' \in m\Delta \cap \Lambda^+$, and the $\alpha_1'', \dots, \alpha_e''$ are linearly independent. Write Λ''^+ for the set of $\mathbb{N}$-linear combinations of the α_i''. Then clearly $(ma\Delta) \cap \Lambda''^+ \subset (ma\Delta) \cap \Lambda^+$ for any a, so it suffices to prove that $(ma\Delta) \cap \Lambda''^+$ is a polynomial of degree $e-1$ in a.

Finally, $(ma\Delta) \cap \Lambda''^+$ is exactly the set $\{\sum_i a_i \alpha_i \mid \sum_i a_i = a\}$, and the cardinality of this set is $\binom{e-1+a}{a}$, a polynomial of degree $e-1$. ∎

DEFINITION 2.16. A function $f\colon \mathbb{N}^n \to \mathbb{Z}$ is *quasipolynomial of degree d* if it can be written as a finite sum of simple quasipolynomial functions of cumulative degree at most d, and it cannot be written as a finite sum of simple quasipolynomial functions of cumulative degree less than d.

Sometimes we will say that a function $f\colon \mathbb{N}^n \to \mathbb{Z}$ is *quasipolynomial on* $\alpha_1, \dots, \alpha_e \in \mathbb{N}^n$; by this we mean that f can be written as a finite sum of simple quasipolynomial functions on subsets of $\alpha_1, \dots, \alpha_e$.

Note that this definition does not agree with the definition of the term quasipolynomial given, for example, in 4.4 of [25].

It is obvious from this definition that simple quasipolynomial functions of cumulative degree d are also quasipolynomial functions of degree d.

LEMMA 2.17. *If $f_1\colon \mathbb{N}^n \to \mathbb{Z}$ and $f_2\colon \mathbb{N}^n \to \mathbb{Z}$ are quasipolynomial, of degrees d_1 and d_2 respectively, then $f_1 + f_2$ is quasipolynomial of degree at most* $\max(d_1, d_2)$. *Also, if $d_1 \neq d_2$, then the degree of $f_1 + f_2$ is exactly* $\max(d_1, d_2)$.

Proof. Immediate from the definition. ∎

The following lemmas provide a few examples of quasipolynomial functions.

LEMMA 2.18. *If $f(\alpha)$ is zero for all but finitely many values of α, then f is quasipolynomial of degree* 0.

Proof. The proof follows immediately from the definition of a simple quasipolynomial of degree 0. ∎

LEMMA 2.19. *A function $f\colon \mathbb{N} \to \mathbb{Z}$ is quasipolynomial on* 1 (*in other words, is the sum of simple quasipolynomial functions on β,* 1 *for various β's*) *of degree d iff it is eventually polynomial of degree $d - 1$.*

Proof. A simple quasipolynomial function $f(\alpha)$ on β, 1 is a function that is zero for $\alpha < \beta$ and that agrees for $\alpha \geq \beta$ with a polynomial with coefficients that are periodic with respect to 1 and therefore are constant. Such a function is clearly eventually polynomial, as is the sum of such functions.

For the converse, let f' be the polynomial function that f eventually agrees with. A polynomial of degree $d - 1$ is simple quasipolynomial of degree d. The difference between f and f' is then nonzero for only finitely many values of $\mathbb{N}$ and is accounted for by the previous lemma. ∎

Let $\epsilon_1, \dots, \epsilon_n \in \mathbb{N}^n$ be the standard basis for $\mathbb{N}^n$, so that ϵ_i is the vector having a one in the ith coordinate and zeros elsewhere.

In the following, wherever we write $\alpha \geq \beta$, for $\alpha = (a_1, \dots, a_n)$ and $\beta = (b_1, \dots, b_n)$, we mean that $a_i \geq b_i$ for all $i \in (1, 2, \dots, n)$

LEMMA 2.20. *If a function $f\colon \mathbb{N}^n \to \mathbb{Z}$ is quasipolynomial on $\epsilon_1, \dots, \epsilon_n$ of degree d then there exists $\alpha' \in \mathbb{N}^n$ such that $f(\alpha)$ agrees with a polynomial of degree $d - n$ for all $\alpha \geq \alpha'$.* (*Here we take a polynomial of negative degree to be identically zero.*)

Proof. A simple quasipolynomial function on a proper subset of $e_1, \dots, e_n$ is easily seen to be eventually zero, whereas a simple quasipolynomial function on $\epsilon_1, \dots, \epsilon_n$ agrees eventually with a polynomial with constant coefficients, as in the previous proof. The sum of such functions is, therefore, eventually a polynomial, and the statement about the degree follows from the definition of cumulative degree. ▮

The converse to this theorem is false; for example, if f has non-polynomial behavior on along a line extending parallel to one of the coordinate axes, then f is not quasipolynomial, even though there may exist an α' such that if(α) agrees with a polynomial for all $\alpha \geq \alpha'$.

LEMMA 2.21. *The product of two quasipolynomial functions in distinct sets of variables is quasipolynomial of degree equal to the sum of the degrees of the two quasipolynomial functions.*

Proof. Let $f(x_1, \dots, x_m)$ and $g(y_1, \dots, y_n)$ be the two functions. Let $f = f_1 + \cdots + f_r$, with each f_i simple quasipolynomial, and with f_1 having degree equal to the degree of f. Choose $g_1, \dots, g_s$ similarly. Then

$$fg = \sum_{i,j} f_i g_j,$$

so it is clear that fg is quasipolynomial if the product of two simple quasipolynomial functions is simple quasipolynomial. If, in addition, such products have degrees equal to the sums of the degrees of their factors, then the statement about degrees will also be proved, since $f_1 g_1$ would then have the correct degree, with all the other products having equal or lesser degrees. Thus we may assume without loss of generality that f and g are simple quasipolynomial. Write $F(x_1, \dots, x_m)$ and $G(y_1, \dots, y_n)$ for the generating functions of f and g, respectively. The generating function of fg is just FG and, by Lemma 2.12, FG is the generating function of a simple quasipolynomial function of the correct degree. ▮

Theorem 2.24 will demonstrate that quasipolynomial functions have a very simple characterization in terms of generating functions. Some preliminary lemmas will be required before the proof of this fact.

LEMMA 2.22. *Let $F(x_1, \dots, x_n)$ be the generating function of $f\colon \mathbb{N}^n \to \mathbb{Z}$. Assume*

$$F(x_1, \dots, x_n) = \frac{P(x_1, \dots, x_n)}{\prod_{j=1}^{e} (1 - x^{\alpha_j})^{d_j}}$$

with $\alpha_1, \dots, \alpha_d \in \mathbb{N}^n$ vectors that are linearly independent in $\mathbb{R}^n$ and P a polynomial. Then f is quasipolynomial of cumulative degree at most $\sum_{j=1}^{e} d_j$.

Proof. The function F is the sum of fractions of the form

$$\frac{x^{\gamma}}{\prod_{j=1}^{e}(1-x^{\alpha_j})^{d_j}}.$$

Each of these is the generating function of a simple quasipolynomial function of degree d, by Lemma 2.12. ▮

LEMMA 2.23. *Let $F(x)$ be a rational function in $\mathbb{N}(x_1,\dots,x_n)$ of the form*

$$F(x) = \frac{P(x)}{\prod_{j=1}^{e}(1-x^{\alpha_j})^{d_j}},$$

with $P(x) \in \mathbb{N}[k_1,\dots,k_n]$, $\alpha_j \in \mathbb{N}^n$, and $d_j \in \mathbb{N}$. If the α_j's are linearly dependent, then $F(x)$ can be rewritten in the form

$$F(x) = \sum_i \frac{P_i(x)}{\prod_{j=1}^{e}(1-x^{\alpha_{i,j}})^{d_{i,j}}},$$

for some $\alpha_{i,j} \in \mathbb{N}^n$, $P_i \in \mathbb{N}[x_1,\dots,x_n]$, and $d_{i,j}, e_i \in \mathbb{N}$, such that each e_i is strictly less than e.

Proof. Choose a linear dependence relation among the α_j's. By clearing denominators and renumbering the α_j's if necessary, this relation can be written

$$m_1\alpha_1 + \cdots + m_k\alpha_k = m_{k+1}\alpha_{k+1} + \cdots + m_e\alpha_e,$$

where each m_k is a nonnegative integer. Write γ for the element of $\mathbb{N}^n$ that both sides of this equation are equal to. Let $d = 1 + \sum_{j=1}^{k}(d_j - 1)$, and let $d' = 1 + \sum_{j=k+1}^{e}(d_j - 1)$. Since

$$(1-x^{m_j\alpha_j}) = (1-x^{\alpha_j})(1 + x^{\alpha_j} + x^{2\alpha_j} + \cdots + x^{(m_j-1)\alpha_j}),$$

F can be rewritten in the form

$$\frac{P'(x)}{\prod_{j=1}^{e}(1-x^{m_j\alpha_j})^{d_j}},$$

with P' a new polynomial. Next write

$$F(x) = \frac{P'(1-x^{\gamma})^{d+d'}}{(1-x^{\gamma})^{d+d'}\prod_{j=1}^{e}(1-x^{m_j\alpha_j})^{d_j}}, \tag{2.1}$$

and note that

$$(1 - x^{\gamma}) = (1 - x^{\sum_{i=1}^{k}(m_i\alpha_i)}) = (1 - x^{m_1\alpha_1})x^{\sum_{i=2}^{k}(m_i\alpha_i)} + (1 - x^{m_2\alpha_2})x^{\sum_{i=3}^{k}(m_i\alpha_i)} + \cdots + (1 - x^{m_{k-1}\alpha_{k-1}})x^{m_k\alpha_k} + (1 - x^{m_k\alpha_k}),$$

which shows that $(1 - x^{\gamma})$ is contained in the ideal generated by $(1 - x^{m_1}), \dots, (1 - x^{m_k})$. Similarly, $(1 - x^{\gamma})$ is also contained in the ideal generated by $(1 - x^{m_{k+1}}), \dots, (1 - x^{m_e})$. This fact, together with our choice of d and d', allows us to rewrite $(1 - x^{\gamma})^{d+d'}$ as the sum of terms each of which is contained one of both $(1 - x^{m_i})^{d_i}$ for $1 \le i \le k$ and $(1 - x^{m_i})^{d_i}$ for $k < i \le e$ as factors. Finally we are able to write F in the desired form by expanding the numerator of Eq. (2.1), breaking up the fraction into a sum of fractions, and canceling these factors. ▮

THEOREM 2.24. *Let $F(x_1, \dots, x_n)$ be the generating function of f: $\mathbb{N}^n \to \mathbb{Z}$. Then f is quasipolynomial iff F can be written in the form*

$$F(x) = \frac{P(x)}{\prod_{j=1}^{e}(1 - x^{\alpha_j})^{m_j}}.$$

Proof. If F is in the given form, then we can use repeated applications of the previous lemma to rewrite F as the sum of terms each of which is in the form specified in Lemma 2.22. Thus f is the sum of quasipolynomial functions and must itself be quasipolynomial.

Conversely, if f is quasipolynomial, then f can be written as the sum of simple quasipolynomial functions. The form of the generating function of each of these simple quasipolynomial functions is given by Lemma 2.12, and the sum of such functions can clearly be written in the form required. ▮

THEOREM 2.25. *Let f: $\mathbb{N}^n \to \mathbb{N}$ be quasipolynomial of degree d. Then*

$$f^*(a) = \sum_{a_1 + \cdots + a_n = a} f(a_1, \dots, a_n)$$

is also quasipolynomial of degree d.

Proof. If f is quasipolynomial, and $F(x_1, \dots, x_n)$ is its generating function, then the generating function of f^* is $F^*(x, \dots, x)$. The fact that f^* is quasipolynomial then follows immediately from Theorem 2.24. It is also clear from this theorem that the degree of f^* is at most d. The only remaining difficulty is to show that the degree cannot be less than d.

There must exist β, $\alpha_1, \dots, \alpha_e$ such that f restricted to $C_{\beta, \alpha_1, \dots, \alpha_e}$ is simple quasipolynomial of cumulative degree d. If not, then we could cover $\mathbb{N}^n$ by cones in such a way that on each cone f was simple quasipolynomial (using Theorem 2.13) and had degree less than d. This would express f as the sum of simple quasipolynomial functions of cumulative degree less than d, contradicting the fact that f has degree d.

Let f' be the restriction of f to $C_{\beta, \alpha_1, \dots, \alpha_e}$. Then $f'(\alpha) \le f(\alpha)$ for all $\alpha \in \mathbb{N}^n$, so $f'^*(a) \le f^*(a)$ for all $a \in \mathbb{N}$. By Theorem 2.15, f'^* has degree d; it follows immediately from the definition of simple quasipolynomial that f^* must have degree at least d. ▮

LEMMA 2.26. *If f, g: $\mathbb{N}^n \to \mathbb{N}$ are quasipolynomial and $f(\alpha) \le g(\alpha)$ for all $\alpha \in \mathbb{N}^n$, then* $\deg f \le \deg g$.

Proof. The previous theorem allows us to reduce to the case $n = 1$. A quasipolynomial function of degree 1 is eventually equal to a polynomial with periodic coefficients, and the result is trivial for such functions. ▮

Our eventual goal is to show that the Hilbert functions of certain $\mathbb{N}^n$-graded algebraic objects are quasipolynomial functions. The next theorem will allow us to make arguments that use induction on the degree of those algebraic objects.

THEOREM 2.27. *Let f: $\mathbb{N}^n \to \mathbb{Z}$, g: $\mathbb{N}^n \to \mathbb{Z}$, and $\beta \in \mathbb{N}^n$ be such that $f(\alpha + \beta) - f(\alpha) = g(\alpha)$. If g is quasipolynomial, then so is f. In addition, if f: $\mathbb{N}^n \to \mathbb{N}$, so all the values of f are nonnegative, then the degree of f is one greater than that of g.*

Proof. Let F and G be the generating functions of f and g, respectively. The relation $f(\alpha + \beta) - f(\alpha) = g(\alpha)$ is equivalent to the relation $F = G(1 - x^{\beta})$. It is clear, then, that F is the generating function of a quasipolynomial function if G is. It remains to show that the degree increases by one when the values of f are known to be nonnegative.

Let b be the sum of the coordinates of the vector β. Then

$$F^* = \frac{G^*}{1 - x^b},$$

where F^* and G^* are the generating functions associated with, respectively, f^* and g^*. Thus by the previous theorem and by Theorem 2.25 we can assume without loss of generality that $n = 1$.

It is not hard to see that in the case $n = 1$ a quasipolynomial function g agrees eventually with a polynomial with periodic coefficients. Such a function is eventually bounded below by a function with generating function of the form

$$\frac{c}{(1-x^N)^d},$$

where c a positive real number and d is the degree of g. Therefore f is bounded below by a function with generating function

$$\frac{c}{(1-x^N)^d(1-x^b)},$$

and it follows that f has degree $d+1$. ∎

3. $\mathbb{N}^n$-GRADED ALGEBRAS AND MODULES

The quasipolynomial functions introduced in the previous section are useful because they occur as the Hilbert functions of certain $\mathbb{N}^n$-graded algebraic objects.

THEOREM 3.1. *Let S be an $\mathbb{N}^n$-graded algebra such that S_0 is Artin and S is finitely generated as an algebra over S_0. Let M be a finitely generated, $\mathbb{N}^n$-graded S-module of dimension d. Then the Hilbert function $f(\alpha) = \operatorname{length}(M_\alpha)$ is quasipolynomial of degree d.*

Proof. The proof will be by induction on d. If $d = 0$ then M has finite length, and length (M_α) is zero for all but finitely many α, so f is quasipolynomial of degree 0.

Now assume that $d > 0$ and that the theorem is proved for all smaller d. Because the sum of quasipolynomial functions is quasipolynomial, we can take a primary filtration of M and assume without loss of generality that M is P-primary for some $P \in \operatorname{Spec}(S)$.

We can map an $\mathbb{N}^n$-graded polynomial ring onto S and work over the polynomial ring instead of over S. So we may as well assume S is polynomial; say $S = S_0[s_1, \dots, s_e]$, with $\deg(s_i) = \alpha_i \in \mathbb{N}^n$.

Since $d = \dim M > 0$, there must be some s_i not contained in P; otherwise M would have finite length. That s_i must be a non-zero divisor on M. This means that the sequence

$$0 \to M \xrightarrow{s_i} M \to \frac{M}{s_i M} \to 0$$

is exact, so

$$\text{length}(M_\alpha) - \text{length}(M_{\alpha-\alpha_i}) = \text{length}\left(\left(\frac{M}{s_i M}\right)_\alpha\right)$$

$$f(\alpha) - f(\alpha - \alpha_i) = f_{M/s_i M}(\alpha).$$

Since s_i is a non-zero divisor on M, M/s_iM has dimension $d-1$. Therefore, by the induction assumption, M/s_iM is quasipolynomial of degree $d-1$, and, by Theorem 2.27, f_M is quasipolynomial of degree d. ∎

It should be clear from the proof that if $s_1, \dots, s_e$ are generators of S of degrees $\alpha_1, \dots, \alpha_e$, then the generating function of the Hilbert function can be written as a rational function with denominator $\prod_i (1 - x^{\alpha_i})$.

A few examples might be helpful.

(1) If M is a finitely generated module over an $\mathbb{N}$-graded algebra S that is generated by elements of degree 1, then the Hilbert function f_M is quasipolynomial on $\{1\}$ and hence is eventually polynomial, as expected.

(2) If M is a finitely generated module over an $\mathbb{N}^2$-graded algebra S, and if every algebra-generator of S over S_0 has degree $(0,1)$ or $(1,0)$, then S is quasipolynomial of degree $d = \dim S$ on $(0,1)$ and $(1,0)$. By Theorem 2.20, there exists a β such that, for all $\alpha \geq \beta$, $f_S(\alpha)$ is equal to a polynomial of degree at most $d-2$. Thus we obtain Theorem 2 of [1], that Hilbert functions of bigraded modules are eventually polynomial of degree at most $(\dim M) - 2$. More results about these functions can be found in [26].

(3) More generally, let M be a finitely generated module over an $\mathbb{N}^n$-graded algebra S, and assume every algebra-generator of S over S_0 has degree e_i, where e_i is the vector in $\mathbb{N}^n$ that is one in the ith position but zero elsewhere. Again, there is a β such that $f_M(\alpha)$ agrees with a polynomial of degree at most $d - n$ for all $\alpha \geq \beta$. (See [11], where it is also shown that all the highest degree monomials of this polynomial have nonnegative coefficients.)

(4) If $M = S = k[s_1, \dots, s_e]$, and if the degree of s_i is α_i, then the generating function of the Hilbert function f_S is

$$\frac{1}{\prod_i (1 - x^{\alpha_i})}$$

and f_S is quasipolynomial of degree d. Also for the twisted module $M(-\alpha)$ (recall that $M(\alpha)_\beta = M_{-\alpha+\beta}$), the corresponding generating function is

$$\frac{x^\alpha}{\prod_i (1 - x^{\alpha_i})}.$$

It is not hard to see that any quasipolynomial function with a generating function of the form

$$\frac{P(x)}{\prod_i (1 - x^{\alpha_i})}$$

such that $P(x)$ has nonnegative coefficients can be written as the sum of such functions. Direct sums of modules have Hilbert functions that are the sums of the Hilbert functions of the individual modules. In this way, any quasipolynomial function of this form can be realized as the Hilbert function of some finitely generated module over such an S. In fact, this identifies exactly the set of all functions that arise as the Hilbert functions of $\mathbb{N}^n$-graded modules.

THEOREM 3.2. *Let S be an $\mathbb{N}^n$-graded, finitely generated, algebra over a local ring R with maximal ideal m, and let T be an $\mathbb{N}^n$-graded, finitely generated, S-algebra. Assume that $S_0 = T_0 = R$. Let N and M be finitely-generated $\mathbb{N}^n$-graded modules over T and S, respectively, with $N \supset M$, and suppose that for every element of N there is a power of m multiplying that element into M. Then $f_{N/M}$: $\alpha \to \operatorname{length}((N/M)_\alpha)$ is quasipolynomial of degree at most* $\dim(T/(\operatorname{Ann}_T N))$.

Proof. We can filter N/M by N/TM and TM/M. The quotient N/TM is a T-module, not just an S-module. Also, N/TM is a finitely generated T-module, and since every element of N is multiplied into M (and hence into TM) by a power of m, it follows that there exists an n such that m^n kills every element of N/TM. Therefore N/TM can be thought of as a module over T/m^nT. This module now satisfies the conditions of the previous theorem, so the Hilbert function of N/TM is quasipolynomial. Since $\operatorname{Ann}_T N/TM \supset \operatorname{Ann}_T N$, this function is in addition quasipolynomial of degree at most $\dim N$.

It remains only to show that TM/M has a quasipolynomial Hilbert function of degree at most $\dim N$. So assume $N = TM$. Suppose that T is generated over S by r generators, so $T = S[t_1, \dots, t_r]$. Suppose that r is at least 2, and that the theorem has already been proved for smaller values of r. Apply the theorem with $S[t_1]$ replacing S and $S[t_1]M$ replacing M, and with T and N as before. It is clear that the hypotheses of the theorem are still satisfied, and T is generated over $S[t_1]M$ by $r - 1$ elements, so by assumption the Hilbert function of $N/S[t_1]M$ is quasipolynomial. Similarly, apply the theorem with S and M as before, but T replaced by $S[t_1]$ and N by $S[t_1]M$, and the conclusion is that $S[t_1]M/M$ also has a quasipolynomial Hilbert function. The Hilbert function of N/M is the sum of the Hilbert functions of $N/S[t_1]M$ and $S[t_1]M/M$, and sum of two quasipolynomial functions is quasipolynomial, so the result follows by induction if only we can deal with the case $r = 1$.

So assume $N = S[t]M$ (where $t = t_1$). Construct the S-module

$$N' = \bigoplus_{i=0}^{\infty} \frac{t^{i+1}M + t^iM + \cdots + tM + M}{t^iM + t^{i-1}M + \cdots + tM + M}.$$

This module has the same Hilbert series as N/M; to see this, note that the quotient modules that we are summing are just successive quotients of modules in the filtration

$$\frac{M}{M} \subset \frac{tM + M}{M} \supseteqq \frac{t^2M + tM + M}{M} \subset \cdots,$$

and note that

$$\bigcup_{i=0}^{\infty} \frac{t^iM + t^{i-1}M + \cdots + M}{M} = \frac{N}{M},$$

thanks to our assumption that $N = TM = S[t]M$.

Note also that $t(t^iM + \cdots + M) \subset (t^{i+1}M + \cdots + M)$, so multiplication by t induces a well-defined surjection

$$\frac{t^iM + \cdots + M}{t^{i-1}M + \cdots + M} \to \frac{t^{i+1}M + \cdots M}{t^iM + \cdots + M},$$

and this in turn induces a well-defined map $N^i \to N'$. Thus multiplication by t makes sense on N', making N' a T-module as well as an S-module.

Let $m_1, \dots, m_k$ be a set of generators for M as a module over S. Write $\overline{tm_1}, \dots, \overline{tm_k}$ for the images of these generators in tM/M. An arbitrary element of

$$\frac{t^{i+1}M + t^iM + \cdots + tM + M}{t^iM + t^{i-1}M + \cdots + tM + M}$$

can be written $t^i \sum_j s_j \overline{tm_j}$, with $s_j \in S$. An arbitrary element of N' can be written as a finite sum of such elements, so it follows that N' is generated over T by $\overline{m}_1, \dots, \overline{m}_k$, and hence that N' is finitely generated over T.

Any element of N' is killed by a power of m because N' is a direct sum of subquotients of N/M, which has the property that any element is killed by a power of m. Since N' is a T-module, it must also be the case that any element of N' is killed by a power of mT. Because N' is finitely generated, it follows that N' is killed by some fixed power of mT and hence is a finitely generated module over $T/(mT)^j$ for some j. The fact that N', and hence N/M, has a quasipolynomial Hilbert function follows now from the previous theorem. Note also that $\operatorname{Ann}_T N' \supset \operatorname{Ann}_T N$, so dim $N' \leq$ dim N, and N/M has a quasipolynomial Hilbert function of degree at most dim N. ∎

4. RESULTS ABOUT $\mathrm{Tor}_k(R/I_1^{a_1}, R/I_2^{a_2})$ FOR $k \geq 2$

Now we apply the results of the previous section to the problem of describing the functions

$$f_k(a_1, \dots, a_n) = \mathrm{length}\big(\mathrm{Tor}_k(M_1/I_1^{a_1}M_1, \dots, M_n/I_n^{a_n}M_n)\big)$$

in the case $n = 2$, $M_1 = M_2 = R$, $k \geq 2$.

Let I be any ideal of a ring R, and let M be an R-module. The short exact sequence $0 \to I \to R \to R/I \to 0$ gives rise to a long exact sequence

(4.1)

$$\begin{array}{cclclclcl}
\cdots & \to & \mathrm{Tor}_k(I, M) & \to & 0 & \to & \mathrm{Tor}_k(R/I, M) & \to & \\
 & \to & \mathrm{Tor}_{k-1}(I, M) & \to & 0 & \to & \mathrm{Tor}_{k-1}(R/I, M) & \to & \cdots \\
\cdots & \to & \mathrm{Tor}_0(I, M) & \to & M & \to & M/IM & \to & 0,
\end{array}$$

which yields an isomorphism $\mathrm{Tor}_k(R/I, M) \cong \mathrm{Tor}_{k-1}(I, M)$ for $i \geq 2$ and an injection $\mathrm{Tor}_1(R/I, M) \to \mathrm{Tor}_0(I, M)$.

If I_1 and I_2 are two ideals of R, then $\mathrm{Tor}_k(R/I_1, R/I_2) \cong \mathrm{Tor}_{k-2}(I_1, I_2)$ for $k \geq 3$, by two applications of the above isomorphisms. Since direct sums commute with Tor, there is also an isomorphism

$$\bigoplus_{a_1, a_2 \geq 0} \mathrm{Tor}_k^R(R/I_1^{a_1}, R/I_2^{a_2}) \cong \mathrm{Tor}_{k-2}^R\left(\bigoplus_{a_1 \geq 0} I_1^{a_1}, \bigoplus_{a_2 \geq 0} I_2^{a_2}\right)$$

for $k \geq 3$. Let t_1 and t_2 be indeterminates; then we can replace $\oplus_{a_i \geq 0} I_i^{a_i}$ by the algebra $R[I_i t] = \oplus_{a_i \geq 0} I_i^{a_i} t^{a_i}$. This allows us to impose the structure of an algebra on $\oplus_{a_1, a_2 \geq 0} \mathrm{Tor}_k^R(R/I_1^{a_1}, R/I_2^{a_2})$.

LEMMA 4.1. *Let I_1 and I_2 be ideals of a ring R. Let $S_i = R[I, t_i] = \oplus_{a_i \geq 0} I_i^{a_i} t_i^{a_i}$. Then the R-modules*

$$\bigoplus_{a_1, a_2 \geq 0} \mathrm{Tor}_k^R(R/I_1^{a_1}, R/I_2^{a_2})$$

can be given the structure of $\mathbb{N}^2$-graded, finitely generated $S_1 \otimes_R S_2$-modules, for $k \geq 2$.

Proof. For $k > 2$, we know that this direct sum is isomorphic to $\mathrm{Tor}_{k-2}^R(S_1, S_2)$. Let $r_{i,1}, \dots, r_{i,m_i}$ generate I_i. Let $T_1 = R[x_{1,1}, \dots, x_{1,m_1}]$

and $T_2 = R[x_{2,1}, \dots, x_{2,m_2}]$ be polynomial rings, and map T_i onto S_i by mapping $x_{i,j}$ onto $r_{i,j}t_i$. This makes S_i into a T_i-module. Choose a resolution of S_i by finitely generated projective T_i-modules,

$$\cdots \to P_{i,1} \to P_{i,0} \to S_i.$$

Since T_i is a free R-module, this resolution is also a resolution for S_i over R. Therefore $\operatorname{Tor}_k^R(S_1, S_2)$ is the homology of the total complex

$$\cdots \to P_{1,1} \otimes_R P_{2,0} \oplus P_{1,0} \otimes_R P_{2,1} \to P_{1,0} \otimes_R P_{1,0} \to 0.$$

The R-modules in this complex are easily seen to also be finitely generated $T_1 \otimes_R T_2$-modules, and the maps $T_1 \otimes T_2$-maps. Therefore the homology modules $\operatorname{Tor}_k^R(S_1, S_2)$ are also finitely generated modules over $T_1 \otimes T_2$. In addition, note that these modules must be killed by the kernels of the maps $T_i \to S_i$; thus, each $\operatorname{Tor}_k^R(S_1, S_2)$ is also a finitely generated $S_1 \otimes S_2$-module.

For $k = 2$, apply direct sums to the end of the long exact sequence of Eq. (4.1) above to get

$$0 \to \bigoplus_{a_1, a_2 \geq 0} \operatorname{Tor}_2^R(R/I_1^{a_1}, R/I_2^{a_2}) \to R[I_1t_1] \otimes_R R[I_2t_2]$$
$$\to R[I_1t_1] \otimes_R R[t_2].$$

The map $R[I_1t_2] \otimes_R R[I_2t_2] \to R[I_1t_1] \otimes_R R[t_2]$ is clearly a map of $S_1 \otimes_R S_2$-modules, so the kernel is an $S_1 \otimes_R S_2$-module. ∎

THEOREM 4.2. *Let I_1 and I_2 be ideals of a local ring (R, m) of dimension d such that $I_1 + I_2$ is m-primary. Then for $k \geq 2$ the function*

$$f_k(a_1, a_2) = \operatorname{length}\big(\operatorname{Tor}_k(R/I_1^{a_1}, R/I_2^{a_2})\big)$$

is quasipolynomial of degree at most $2d$.

Proof. Fix $k \geq 2$. Then $\oplus_{a_1, a_2} \operatorname{Tor}_k(R/I_1^{a_1}, R/I_2^{a_2})$ is isomorphic to (or, in the case of $k = 2$, is at least a submodule of) $\operatorname{Tor}_{k-2}(S_1, S_2)$. Since $I_1 + I_2$ is m-primary, $I_1^{a_1} + I_2^{a_2}$ is also m-primary, so some power of m is contained in $I_1^{a_1} + I_2^{a_2}$ and some power of m kills $\operatorname{Tor}_k(R/I_1^{a_1}, R/I_2^{a_2})$. Therefore every graded piece of $\operatorname{Tor}_{k-2}(S_1, S_2)$ is killed by a power of m. By the previous lemma, $\operatorname{Tor}_{k-2}(S_1, S_2)$ is a finitely generated $S_1 \otimes S_2$-module. It follows that every element of $\operatorname{Tor}_{k-2}(S_1, S_2)$ is also killed by a power of $m(S_1 \otimes S_2)$ and, in fact, that a fixed power $m^N(S_1 \otimes S_2)$ kills every element of the module. Therefore $\operatorname{Tor}_{k-2}(S_1, S_2)$ is actually a module over $(R/m^N) \otimes_R (S_1 \otimes S_2)$.

Thus the module $\oplus_{a_1, a_2} \operatorname{Tor}_k(R/I_1^{a_1}, R/I_2^{a_2})$ is isomorphic, by an isomorphism that preserves the grading, to a finitely generated, bigraded module over $(R/m^N) \otimes_R (S_1 \otimes S_2)$. This makes f_k the Hilbert function of a finitely generated bigraded module over the bigraded ring $(R/m^N) \otimes_R (S_1 \otimes S_2)$. By Theorem 3.1 this Hilbert function is quasipolynomial of degree equal to the dimension of the ring. So it remains only to calculate the dimension of $(R/m^N) \otimes_R (S_1 \otimes S_2)$. The ideal $m(S_1 \otimes S_2)$ is nilpotent, so the ring $(R/m) \otimes_R (S_1 \otimes S_2)$ has the same dimension, and

$$(R/m) \otimes_R (S_1 \otimes S_2) \cong ((R/m) \otimes_R S_1) \otimes_{R/m} ((R/m) \otimes_R S_2).$$

The dimension of $(R/m) \otimes_R S_i = (R/m) \otimes_R R[I_i t]$ is the analytic spread of I_i, which is at most d. The claimed result follows. ∎

The module $\operatorname{Tor}_k(S_1, S_2)$ whose Hilbert function we calculate in the above proof is a module over an algebra all of whose multidegrees are either $(0, 1)$ or $(1, 0)$. By the second example of the previous section, such a function is eventually polynomial of degree at most 2 less than the dimension of the module. Therefore

COROLLARY 4.3. *Let I_1 and I_2 be ideals of a local ring (R, m) such that $I_1 + I_2$ is m-primary. Then there exists a $(b_1, b_2) \in \mathbb{N}^2$ such that, for $k \geq 2$ and $(a_1, a_2) \geq (b_1, b_2)$, the function*

$$f_k(a_1, a_2) = \operatorname{length}(\operatorname{Tor}_k(R/I_1^{a_1}, R/I_2^{a_2}))$$

is polynomial of degree at most $2d - 2$.

Note that it is possible that the Tor modules could have dimension less than the sums of the analytic spreads of the two ideals; for example, if I_1 and I_2 are generated by disjoint parts of a system of parameters, then the higher Tor's are all zero. However, I know of no examples showing that nonzero polynomials of smaller degree may occur.

5. $\operatorname{Tor}_1(R/I_1^{a_1}, R/I_2^{a_2})$

The next goal is to establish some results about the functions f_1 and f_0. As far as we know, the following may be true.

CONJECTURE 5.1. *Let I_1 and I_2 be ideals of a local ring (R, m) such that $I_1 + I_2$ is m-primary. Then the function*

$$f_1(a_1, a_2) = \operatorname{length}(\operatorname{Tor}_1(R/I_1^{a_1}, R/I_2^{a_2}))$$

is quasipolynomial of degree at most $\dim R + 2$.

However, all we know now is this:

THEOREM 5.2. *Let I_1 and I_2 be ideals of a local ring (R, m) such that $I_1 + I_2$ is m-primary, and such that the R-algebra*

$$T = \bigoplus_{a_1, a_2} (I_1^{a_1} \cap I_2^{a_2}) x_1^{a_1} x_2^{a_2} \subset R[x_1, x_2]$$

is finitely generated as an algebra over R. Then the function

$$f(a_1, a_2) = \text{length}(\text{Tor}_1(R/I_1^{a_1}, R/I_2^{a_2}))$$

is quasipolynomial of degree at most $\dim R + 2$.

Proof. Let T be the doubly graded R-algebra described above. By assumption it is finitely generated. Let S be the doubly graded R algebra

$$S = R[I_1 x_1, I_2 x_2] = \bigoplus_{a_1, a_2} I_1^{a_1} I_2^{a_2} x_1^{a_1} x_2^{a_2}.$$

Since $S \subset T$, T is also an S-algebra. Now observe that

$$T/S = \bigoplus_{a_1, a_2} \frac{I_1^{a_1} \cap I_2^{a_2}}{I_1^{a_1} I_2^{a_2}} x_1^{a_1} x_2^{a_2}$$

and recall that $\text{Tor}_1^R(R/I_1^{a_1}, R/I_2^{a_2}) = (I_1^{a_1} \cap I_2^{a_2})/I_1^{a_1} I_2^{a_2}$. Apply Theorem 3.2, with $N = T$, $M = S$, and the conclusion follows; all that remains is to calculate the upper bound on the dimension of R.

Let $M \subset T$ be the ideal generated by m and by $(I_1^{a_1} \cap I_2^{a_2}) x_1^{a_1} x_2^{a_2}$, for all a_1, a_2 satisfying $a_1 + a_2 \geq 1$. Clearly M is maximal, with $T/M \cong R/m$. Also, $\dim T = \text{height } M$. Let P be a minimal prime such that $\dim T/P = \dim T$, and let $p = P \cap R$. Apply the dimension formula to get

$$\begin{aligned} \dim T + 0 &= \text{height } M + \text{tr.deg}_{R/mR} T/MT \\ &\leq \text{height}(m_R(R/p)) + \text{tr.deg}_{R/p} T \\ &\leq \dim R + 2 \end{aligned}$$

DEFINITION 5.3. Given a pair (I_1, I_2) of ideals of the local ring (R, m), call the algebra $\oplus_{a_1, a_2} (I_1^{a_1} \cap I_2^{a_2}) x_1^{a_1} x_2^{a_2}$ the *intersection algebra* of I_1 and I_2. If this algebra is finitely generated over R, we will say that I_1 and I_2 have *finite intersection algebra*.

The previous theorem can now be restated as follows.

COROLLARY 5.4. *If I_1 and I_2, ideals of the local ring (R, m), have finite intersection algebra, then the function*

$$f(a_1, a_2) = \text{length}(\text{Tor}_1(R/I_1^{a_1}, R/I_2^{a_2}))$$

is quasipolynomial of degree at most $\dim R + 2$.

Note that there are examples of ideals I_1, I_2 in local rings (R, m) that do not have finite intersection algebras. Such examples can be constructed from examples existing in the literature of non-finitely generated symbolic power algebras. (See [9, 20, 21].

In particular, given an ideal $P \subset R$ such that the algebra

$$R \oplus P^{(1)} \oplus P^{(2)} \oplus \cdots$$

is not finitely generated, it is possible to find a $f \in R$ such that the ideals (f) and P do not have finite intersection algebra. To do this, choose f so that $(P^a : f^a) = P^{(a)}$, for all a.

LEMMA 5.5. *If R regular and $P \subset R$ prime, then there exists $f \in R$ such that $(P^a : f^a) = P^{(a)}$ for all a.*

Proof. Since R is a regular local ring, so is R_P. The associated graded ring of a regular local ring is a polynomial ring, so, in particular, $\mathrm{gr}_{PR_P}(R_P) = (R - P)^{-1}\,\mathrm{gr}_P(R)$ is a domain. Let I be the kernel of the natural map $\mathrm{gr}_P(R) \to (R - P)^{-1}\,\mathrm{gr}_P(R)$. Then $(R - P)^{-1}I = 0$, and, since I is finitely generated, there exists $f \in R - P$ such that $fI = 0$. (We are implicitly identifying elements in R with their images in $\mathrm{gr}_P(R)$ via the natural map $R \to R/P \subset \mathrm{gr}_P(R)$.) This means that $fg \in P^{n+1}$ for any element g of P^n which can be multiplied into P^{n+1} by an element of $R - P$. More generally, any element $g \in P^n$ which can be multiplied into P^{n+m} by an element of $R - P$ satisfies $f^m g \in P^{n+m}$. The result follows. ∎

LEMMA 5.6. *If f and P are chosen as suggested above, then the intersection algebra $\bigoplus_{a_1, a_2 \geq 0}(P^{a_1} \cap (f^{a_2}))x_1^{a_1}x_2^{a_2}$ is not finitely generated.*

Proof. We will prove the contrapositive. Assume that the intersection algebra is finitely generated. Note that $(P^{a_1} : f^{a_2})f^{a_2} = P^{a_1} \cap (f^{a_2})$, so the algebra can be rewritten as $\bigoplus(P^{a_1} : f^{a_2})x_1^{a_1}(x_2 f)^{a_2}$. Map this to the symbolic power algebra $\bigoplus_a P^{(a)}x^a$ by mapping tf to 1. This is an ungraded ring homomorphism. So the symbolic power is finitely generated, since it can be written as a homomorphic image of the intersection algebra, which we assumed to be finitely generated. ∎

The examples in the papers cited above give rise in this way to a number of quite concrete examples of pairs of ideals with non-finite intersection algebras. Studying the functions f_1 that arise in such examples would be an interesting subject for further research.

6. $\mathrm{Tor}_0(R/I_1^{a_1}, R/I_2^{a_2})$

Throughout this section, (R, m) is a regular local ring of dimension d.

Let I_1 and I_2 be ideals of R such that $I_1 + I_2$ is m-primary, and let $f_\chi(a_1, a_2)$ be the Euler characteristic

$$f_\chi(a_1, a_2) = \chi(R/I_1^{a_1}, R/I_2^{a_2}) = \sum_k (-1)^k \operatorname{length}(\operatorname{Tor}_k^R(R/I_1^{a_1}, R/I_2^{a_2})).$$

This sum is well defined because the Tor's are all zero for $k > \dim R$, and because the condition that $I_1 + I_2$ be m-primary forces all of the Tor_k's to have finite length. The function χ is biadditive (so, for example, $\chi(M \oplus N, P) = \chi(M, P) + \chi(N, P)$) because each of the Tor_k's are. Also, $\chi(M, N)$ is zero whenever M and N are such that $\dim(M) + \dim(N) < d$ (see [8, 19]). And if length $(M \otimes N) < \infty$, as is the case when $M = R/I^{a_1}$ and $N = R/I^{a_2}$, then $\dim(M) + \dim(N) \leq d$ (see [23]).

THEOREM 6.1. *For large a_1 and a_2, $f_\chi(a_1, a_2)$ is either identically zero or is eventually a polynomial of degree d.*

Proof. Fix a_1 and a_2 and let $P_{u,1}, \dots, P_{u,s_u}$ be the primes associated to $I_u^{a_u}$. For $u = 1$ and $u = 2$, choose filtrations of $R/I_u^{a_u}$ by prime cyclic modules, and let $p_{u,i}$ be the number of times that $R/P_{u,i}$ occurs in the corresponding filtration. Then by biadditivity,

$$\chi(R/I_1^{a_1}, R/I_2^{a_2}) = \sum_{i \leq s_1, j \leq s_2} p_{1,i} p_{2,j} \chi(R/P_{1,i} R/P_{2,j}).$$

Assume that the $P_{u,i}$'s are ordered so that $P_{u,1}, \dots, P_{u,s'_u}$ have the least height of any of the $P_{u,i}$'s, and let e_u be this minimal height. Since each $P_{u,i}$ contains $I_u^{a_u}$, we know that $P_{1,i} + P_{2,j}$ is m-primary for any i and j. Therefore $e_1 + e_2 \geq d$. This means that if $i > s'_1$ or $j > s'_2$ then $\operatorname{height}(P_{1,i}) + \operatorname{height}(P_{2,j}) > e_1 + e_2 \geq d$, so $\chi(R/P_{1,i} R/P_{2,j}) = 0$. Therefore

$$\chi\left(\frac{R}{I_1^{a_1}}, \frac{R}{I_2^{a_2}}\right) = \sum_{i \leq s'_1, j \leq s'_2} p_{1,i} p_{2,j} \chi\left(\frac{R}{P_{1,i}}, \frac{R}{P_{2,j}}\right).$$

Note that $p_{u,i}$ is independent of the choice of filtration; in fact, $p_{u,i}$ is just the length of $R_{P_{u,i}}/I_u^{a_u} R_{P_{u,i}}$. Also, the ideals $P_{u,1}, \dots, P_{u,s'_u}$ are also the associated primes of minimal height of any power of I_u. So, for any a_1 and a_2,

$$\begin{aligned} f_\chi(a_1, a_2) &= \chi\left(\frac{R}{I_1^{a_1}}, \frac{R}{I_2^{a_2}}\right) \\ &= \sum_{i \leq s'_1, j \leq s'_2} \operatorname{length}\left(\frac{R_{P_{1,i}}}{I_1^{a_1} R_{P_{1,i}}}\right) \operatorname{length}\left(\frac{R_{P_{2,j}}}{I_2^{a_2} R_{P_{2,j}}}\right) \chi\left(\frac{R}{P_{1,i}}, \frac{R}{P_{2,j}}\right). \end{aligned}$$

Since I_u is primary to the maximal ideal of $R_{P_{u,i}}$, the functions

$$a_u \mapsto \text{length}\left(\frac{R_{P_{u,i}}}{I_u^{a_u} R_{P_{u,i}}}\right)$$

as just Hilbert functions and are eventually polynomial of degree e_u. Therefore, the function $f_\chi(a_1, a_2)$ is polynomial of degree d for sufficiently large a_1 and a_1, if $e_1 + e_2 = d$, and is identically zero if $e_1 + e_2 > d$, since in that case all of the $\chi(R/P_{1,i}, R/P_{2,j})$'s are zero. ▮

We can also describe f_χ as follows.

THEOREM 6.2. *$f_\chi(a_1, a_2)$ is either identically zero or quasipolynomial of degree $d + 2$.*

Proof. By the proof of the previous theorem, $f_\chi(a_1, a_2)$ is the sum of terms of the form $cg_1(a_1)g_2(a_2)$, where g_1 and g_2 are eventually polynomial and c is a nonnegative integer. By Lemma 2.17, the sum of quasipolynomial functions is quasipolynomial of degree equal to the maximum of the degrees of the summands. So it suffices to show that each such summand is either identically zero or is quasipolynomial of degree $d + 2$. By Lemma 2.19, g_1 and g_2 are each quasipolynomial of degree $e_1 + 1$ and $e_2 + 1$ (where e_1 and e_2 are as in the proof of the previous theorem). So Lemma 2.21 says that $cg_1(a_1)g_2(a_2)$ is a quasipolynomial function of a_1 and a_2 of degree $e_1 + e_2 + 2 = d + 2$, as long as c is nonzero. ▮

THEOREM 6.3. *If I_1 and I_2 have finite intersection algebra, then the function*

$$f_0(a_1, a_2) = \text{length}\left(\frac{R}{I_1^{a_1} + I_2^{a_2}}\right)$$

is quasipolynomial of degree $\dim R + 2$.

Proof. By the previous theorems, we already know that f_i is quasipolynomial for $i > 0$, and we know that the alternating sum $\chi = f_0 - f_1 + f_2 + \cdots$ is quasipolynomial. Since $f_0 = \chi + f_1 - f_2 + \cdots$, and since the f_i's are eventually zero, this expresses f_0 as a finite sum of quasipolynomial functions. Thus f_0 is quasipolynomial. It remains to calculate the degree, but this is done in the following lemma. ▮

LEMMA 6.4. *If the function*

$$f_0(a_1, a_2) = \text{length}\left(\frac{R}{I_1^{a_1} + I_2^{a_2}}\right)$$

is quasipolynomial, then its degree is $\dim R + 2$.

Proof. Both I_1 and I_2 are contained in m, so $I_1^{a_1} + I_2^{a_2} \subset m^{\min(a_1, a_2)}$. Therefore f_0 is bounded below by, for example, the function given by

$$f(a_1, a_2) = \begin{cases} \operatorname{length}\left(R/m^{(a_1+a_2)/3}\right) & \text{if } 1/2 \le a_1/a_2 \le 2 \\ 0 & \text{otherwise.} \end{cases}$$

Since length (R/m^{a_1}) is eventually polynomial of degree d, this function is quasipolynomial of degree $d + 2$. So f_0 is bounded below by a quasipolynomial function of degree $d + 2$.

Since $I_1 + I_2$ is m-primary, there exists N such that $m^N \subset I_1 + I_2$. It follows that $m^{N(a_1+a_2)} \subset I_1^{a_1} + I_2^{a_2}$, so

$$f_0(a_1, a_2) \le \operatorname{length}\left(R/m^{N(a_1+a_2)}\right).$$

Therefore $f_0(a_1, a_2)$ can also be bounded above by a polynomial of degree d, and hence by a quasipolynomial function of degree $d + 2$.

The result now follows from Lemma 2.26. ∎

7. MONOMIAL IDEALS

Let K be a field, let $R = K[[x_1, \dots, x_d]]$, and let $I_1, \dots, I_n$ be ideals of R generated by monomials.

The monomials of R correspond to elements of $(\mathbb{Z}_{\ge 0})^d \subset \mathbb{R}^d$, under a map "log" which takes a monomial x^α to the integer vector α determined by its exponents. Similarly, monomial ideals correspond to subsets of $\mathbb{R}^d$; write $\log I$ for the discrete subset of $\mathbb{R}^d$ corresponding to the exponents of the monomials contained in I.

THEOREM 7.1. *If $I_1, \dots, I_n$ are monomial ideals in $R = K[[x_1, \dots, x_d]]$ satisfying $\sqrt{I_1 + \cdots + I_n} = (x_1, \dots, x_n)$, then*

$$f_0(a_1, \dots, a_n) = \operatorname{length}\left(\frac{R}{I_1^{a_1} + \cdots + I_n^{a_n}}\right)$$

is quasipolynomial of degree $d + n$.

Proof. The length $f_0(a_1, \dots, a_n)$ is equal to the cardinality of $\log(R) \setminus \log(I_1^{a_1} + \cdots + I_n^{a_n})$. Pick N such that $m^N \subset I_1 + \cdots + I_n$. Given $(a_1, \dots, a_n) \in \mathbb{Z}^n$, note that

$$m^{N(a_1+ \cdots + a_n)} \subset I_1^{a_1} + \cdots + I_n^{a_n}. \tag{7.1}$$

Write $\#(A)$ to mean the cardinality of a set A. The function $(a_1, \dots, a_n) \mapsto \#\log(R) \setminus \log(m^{N(a_1+ \cdots + a_n)})$ is clearly quasipolynomial, so it suffices to show that the function

$$(a_1, \dots, a_n) \mapsto \#\left(\log(I_1^{a_1} + \cdots + I_n^{a_n}) \setminus \log(m^{N(a_1+ \cdots + a_n)})\right) \tag{7.2}$$

is quasipolynomial. Let $(x^{\beta_{i,1}}, \dots, x^{\beta_{i,k_i}})$ be a set of generators for I_i. The set $S_\alpha = \log(I_1^{a_1} + \cdots + I_n^{a_n}) \setminus \log(m^{N(a_1 + \cdots + a_n)})$ (where $\alpha = (a_1, \dots, a_n)$) can be defined as the set of all $\gamma = (g_1, \dots, g_d)$ satisfying the $\mathbb{Z}$-linear inequalities;

$$
\begin{array}{ccc}
\gamma & \geq & \sum_{i,j} d_{i,j}\beta_{i,j} \\
\sum_j d_{1,j} & = & l_1 a_1 \\
 & \vdots & \\
\sum_j d_{n,j} & = & l_n a_n \\
\sum_i l_i & = & 1 \\
\sum_i g_i & < & N(a_1 + \cdots + a_n)
\end{array}
$$

for some $l_i, d_{i,j} \in \mathbb{N}$.

The next-to-last equation is equivalent to the requirement that $l_{i'} = 1$ for a single i', and that $l_i = 0$ for all $i \neq i'$. Together with the previous n equations, this implies that $\sum_j d_{i',j} = a_{i'}$ for some i', and that $d_{i,j} = 0$ for any $i \neq i'$. The first equation then degenerates to the statement that there exists an i' such that $\gamma \geq \sum_{i',j} d_{i',j}\beta_{i',j}$ for some $d_{i',j}$ with $\sum_j d_{i',j} = a_{i'}$. This in turn is true iff $x^\gamma \in I_{i'}^{a_{i'}}$ for some i'. A monomial x^γ is contained in a sum of monomial ideals iff it is contained in one of the ideals, so we see that γ satisfies all but the last of the equations above iff $x^\gamma \in I_1^{a_1} + \cdots + I_n^{a_n}$. Finally, the last equation imposes the requirement that x^γ not be contained in $m^{N(a_1, \dots, a_n)}$.

We can introduce auxiliary variables $\epsilon = (e_1, \dots, e_d) \in \mathbb{N}^d$ and $f \in \mathbb{N}$ and rewrite these inequalities as equalities:

$$
\begin{array}{rcl}
-\gamma + \sum_{i,j} \beta_{i,j} d_{i,j} + \epsilon & = & 0 \\
-l_1 a_1 + \sum_j d_{1,j} & = & 0 \\
 & \vdots & \\
-l_n a_n + \sum_j d_{n,j} & = & 0 \\
-1 + \sum_i l_i & = & 0 \\
-\sum_i N a_i + \sum_i g_i + f + 1 & = & 0.
\end{array}
$$

A solution to these equations is an element of $\mathbb{N}^{2n+\sum_i k_i+2d+1}$ of the form

$$(a_1,\ldots,a_n,I_1,\ldots,l_n,d_{1,1},\ldots,d_{n,k_n},e_1,\ldots,e_d,f,g_1,\ldots,g_d).$$

Let $T \subset \mathbb{N}^{2n+\sum_i k_i+2d+1}$ be the set of all such solutions. For brevity's sake, we will write $(\alpha, \lambda, \delta, \epsilon, f, \gamma)$ for a typical element of T.

By a fundamental theorem of integer programming (see, e.g., Section I.3 of [24]), T is a finitely generated monoid, and the monoid algebra $A = K[T]$ is Noetherian. Make A an $\mathbb{N}^n$-graded algebra by giving the element $(\alpha, \lambda, \delta, \epsilon, f, \gamma)$ degree α. Form the ideal I generated by all elements $(\alpha, \lambda, \delta, \epsilon, f, \gamma) - (\alpha', \lambda', \delta', \epsilon', f', \gamma')$ satisfying $\alpha = \alpha'$ and $\gamma = \gamma'$. This ideal is homogeneous, so the algebra A/I is also $\mathbb{N}^n$-graded. Given a degree $\alpha' \in \mathbb{N}^d$, the degree-α' part of A/I has a K-basis consisting of elements of the form $(\alpha, \lambda, \delta, \epsilon, f, \gamma) + I$ satisfying $\alpha \equiv \alpha'$. Such a K-basis can be put in one-to-one correspondence with the elements of S_α, with $(\alpha,\lambda, \delta, \epsilon, f, \gamma) + I$ mapping to $\gamma \in S_\alpha$. Therefore the function f_0 is the Hilbert function of A/I and is quasipolynomial by Theorem 3.1. The degree bound follows by the same argument used in Lemma 6.4. ▮

In the case $n = 2$, where there are only two ideals I_1 and I_2, we know already that the functions f_χ and f_k for $k \geq 2$ are quasipolynomial.

COROLLARY 7.2. *If I_1, I_2 are monomial ideals in $R = K[[x_1,\ldots,x_d]]$, then*

$$f_k(a_1,a_2) = \text{length}\left(\operatorname{Tor}_k\left(\frac{R}{I_1^{a_1}}, \frac{R}{I_2^{a_2}}\right)\right)$$

is a quasipolynomial function for all $k \geq 0$.

REFERENCES

1. P. B. Bhattacharya, The Hilbert function of two ideals, *Proc. Cambridge Philos. Soc.* **53** (1957), 568–575.
2. W. C. Brown, Hilbert functions for two ideals, *J. Algebra*, to appear.
3. W. C. Braun, "Hilbert Functions for Two Ideals *ii*," preprint.
4. R.-O. Buchweitz and Q. Chen, Hilbert–Kunz functions of cubic curves and surfaces, *J. Algebra* **197** (1997), 246–267.
5. P.-J. Cahen and J.-L. Chabert, "Integer-Valued Polynomials," Amer. Math. Soc., Providence, 1997.
6. A. Conca, Hilbert–Kunz function of monomial ideals and binomial hypersurfaces, *Manuscripta Math.* **90**, No. 3 (1996), 287–300.
7. M. Contessa, On the Hilbert–Kunz function and Koszul homology, *J. Algebra* **175** (1995), 757–766.
8. H. Gillet and C. Soulé, *K*-théorie et nullité des multiplicités d'intersection, *C. R. Acad. Sci. Paris Ser. I Math.* **300**, No. 3 (1985), 71–74.

9. S. Goto, K. Nishida, and K. Watanabe, Non-Cohen–Macaulay symbolic blow-ups for space monomial curves and counterexamples to Cowsik's question, *Proc. Amer. Math. Soc.* **120**, No. 2 (1994), 383–392.
10. C. Han and P. Monsky, Some surprising Hilbert–Kunz functions, *Math. Z.* **214**, No. 1 (1993), 119–135.
11. M. Herrmann, E. Hyry, J. Ribbe, and Z. Tang, Reduction numbers and multiplicities of multigraded structures, *J. Algebra* **197** (1997), 311–341.
12. M. Hochster, Tight closure in equal characteristic, big Cohen–Macaulay algebras, and solid closure, *in* "Commutative Algebra: Syzygies, Multiplicities, and Birational Algebra (South Hadley, MA, 1992)," pp. 173–196, Amer. Math. Soc., Providence, 1994.
13. M. Hochster and C. Huneke, Tight closure, invariant theory, and the Briançon–Skoda theorem, *J. Amer. Math. Soc.* **3**, No. 1 (1990), 31–116.
14. A. G. Khovanskiĭ, Sums of finite sets, orbits of commutative semigroups and Hilbert functions, Funktsional. Anal. i Prilozhen. **29** (1995), No. 2, 36–50, 95.
15. P. Monsky, The Hilbert–Kunz function, *Math. Ann.* **263**, No. 1 (1983), 43–49.
16. P. Monsky, The Hilbert–Kunz function of a characteristic 2 cubic, *J. Algebra* **197** (1997), 268–277.
17. P. Monsky, Hilbert–Kunz functions in a family: Line-S_4 quartics, *J. Algebra* **208** (1998), 359–371.
18. P. Monsky, Hilbert–Kunz functions in a family: Point-S_4 quartics, *J. Algebra* **208** (1998), 343–358.
19. P. Roberts, The vanishing of intersection multiplicities of perfect complexes, *Bull. Amer. Math. Soc.* (*N.S.*) **13**, No. 2 (1985), 127–130.
20. P. Roberts, An infinitely generated symbolic blow-up in a power series ring and a new counterexample to Hilbert's fourteenth problem, *J. Algebra* **132** (1990), 461–473.
21. P. C. Roberts, A prime ideal in a polynomial ring whose symbolic blow-up is not Noetherian, *Proc. Amer. Math. Soc.* **94**, No. 4 (1985), 589–592.
22. G. Seibert, The Hilbert–Kunz function of rings of finite Cohen–Macaulay type, *Arch. Math.* (*Basel*) **69**, No. 4 (1997), 286–296.
23. J.-P. Serre, "Algèbre locale. Multiplicités," Springer-Verlag, Berlin, 1965; Cours au Collège de France, 1957–1958, rédigé par Pierre Gabriel, 2nd ed., 1965; Lecture Notes in Mathematics, 11.
24. R. P. Stanley, "Combinatorics and Commutative Algebra," 2nd ed., Birkhäuser, Boston, 1996.
25. R. P. Stanley, "Enumerative Combinatorics," Vol. 1, Cambridge Univ. Press, Cambridge, UK, 1997, with a foreword by Gian-Carlo Rota, corrected reprint of the 1986 original.
26. J. K. Verma, D. Katz, and S. Mandal, Hilbert functions of bigraded algebras, *in* "Commutative Algebra (Trieste, 1992)," pp. 291–302, World Scientific, River Edge, NJ, 1994.