PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 135, Number 5, May 2007, Pages 1305–1308
S 0002-9939(06)08834-4
Article electronically published on November 15, 2006

ON THE COEFFICIENTS OF HILBERT QUASIPOLYNOMIALS

WINFRIED BRUNS AND BOGDAN ICHIM

(Communicated by Bernd Ulrich)

ABSTRACT. The Hilbert function of a module over a positively graded algebra is of quasi-polynomial type (Hilbert–Serre). We derive an upper bound for its grade, i.e. the index from which on its coefficients are constant. As an application, we give a purely algebraic proof of an old combinatorial result (due to Ehrhart, McMullen and Stanley).

1. Hilbert quasipolynomials

Let K be a field, and R a positively graded K-algebra, that is, $R = \bigoplus_{i\geq 0} R_i$ where $R_0 = K$ and R is finitely generated over K. We do not assume R to be generated in degree 1—the generators may be of arbitrarily high degree. The following theorem of Hilbert–Serre describes the Hilbert functions of finitely generated graded R-modules M.

Theorem 1. *Let $M = \bigoplus_{i\in\mathbb{Z}} M_i$ be a finitely generated graded R-module of dimension d, $H(M, \_) : \mathbb{Z} \to \mathbb{Z}$ the associated Hilbert function, and suppose that $r_1, \dots, r_d$ is a homogeneous system of parameters for M.*

Then there is a quasi-polynomial Q_M of degree $d-1$, such that $H(M, n) = Q_M(n)$ for $n \gg 0$. Moreover, the period of Q_M divides $\operatorname{lcm}(\deg r_1, \dots, \deg r_d)$.

The terminology concerning quasipolynomials is explained as follows: a function $Q : \mathbb{Z} \to \mathbb{C}$ is called a *quasipolynomial* of *degree* u if

$$Q(n) = a_u(n)n^u + a_{u-1}(n)n^{u-1} + \dots + a_1(n)n + a_0(n),$$

where $a_i : \mathbb{Z} \to \mathbb{C}$ is a periodic function for $i = 0, \dots, u$, and $a_u \neq 0$. The *period* of Q is the smallest positive integer π such that

$$a_i(n + m\pi) = a_i(n)$$

for all $n, m \in \mathbb{Z}$ and $i = 0, \dots, u$.

For the reader's convenience, we include a short proof the Hilbert–Serre theorem, or rather its reduction to the classical theorem of Hilbert. By definition of homogeneous system of parameters, M is a finitely generated module over $K[r_1, \dots, r_d]$ (which is isomorphic to a polynomial ring over K). Therefore we may assume that $R = K[r_1, \dots, r_d]$. Let S be the subalgebra of R generated by its homogeneous elements of degree $p = \operatorname{lcm}(\deg r_1, \dots, \deg r_d)$. Then it is not hard to see that R is a finitely generated S-module. Therefore M is a finitely generated S-module,

Received by the editors December 22, 2005.
2000 *Mathematics Subject Classification.* Primary 13A02.
Key words and phrases. Hilbert quasi-polynomial, Ehrhart quasi-polynomial.

too, and $\dim_S M = \dim_R M$. As a last reduction step, we can replace R by S and assume that R is generated by its elements of degree p.

Then we have the decomposition

$$M = M^0 \oplus \ldots \oplus M^{p-1}, \qquad M^k = \bigoplus_{i \equiv k\ (p)} M_i,$$

into finitely generated R-modules, and $\dim M = \max_k \dim M^k$.

Let us consider a single module M^k. Then we can normalize the degrees in R dividing them by p and re-grade M^k by giving degree $(i-k)/p$ to the elements of its degree i component in the original grading, $i \equiv k\ (p)$. By Hilbert's theorem, the Hilbert function of M^k re-graded is given by a true polynomial $P_k(n)$ for $n \gg 0$.

Returning to M we obtain

$$H(M,n) = P_k((n-k)/p), \qquad n \equiv k\ (p),\ n \gg 0,$$

and this proves the theorem.

It is clear that any improvement of the theorem depends on the "coherence" of the modules M^k. The reduction in the proof above forgets the original module structure to a large extent. Clearly, in the extreme case in which R is generated by its degree p elements, M is just a direct sum of the independent modules M^k. But if the M^k are sufficiently related, then one can say more on Q_M.

2. The grade of Hilbert quasipolynomials

It is a natural question to ask how close Q_M is to being a true polynomial. The next theorem, which is the main result of this paper, provides an answer. Following Ehrhart [E], we let the *grade* of Q denote the smallest integer $\delta \geq -1$ such that $a_i(\_)$ is constant for all $i > \delta$.

Theorem 2. *Let $M = \bigoplus_{i \in \mathbb{Z}} M_i$ be a finitely generated graded R-module of dimension d, and*

$$Q(n) = a_{d-1}(n)n^{d-1} + a_{d-2}(n)n^{d-2} + \ldots + a_1(n)n + a_0(n)$$

its Hilbert quasi-polynomial with period π. Let I be the ideal of R generated by all homogeneous elements x of R such that $\gcd(\deg x, \pi) = 1$. *Then*

$$\operatorname{grade} Q < \dim M/IM.$$

The theorem will be proved by an induction based on the following lemma, in which, as usual, $(0:x)_M = \{u \in M : xu = 0\}$.

Lemma 3. *With the notation of the theorem, if* $\dim M/IM < \dim M$, *then there is a homogeneous $x \in I$ with* $\gcd(\deg x, \pi) = 1$, *such that*

(a) $\dim M/xM = \dim M - 1$,
(b) $\dim(0:x)_M \leq \dim M - 1$.

Proof. Let $D(M) = \{\mathfrak{p} \in V(M), \dim A/\mathfrak{p} = \dim M\} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Clearly $I \not\subset \mathfrak{p}_i$ for $i = 1, \ldots, r$. By prime avoidance, we conclude that $I \not\subset \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$. By induction on r, we show that

$$S = \{x \in I,\ x \text{ homogeneous},\ \gcd(\deg x, \pi) = 1\} \not\subset \bigcup_{i=1}^{r} \mathfrak{p}_i.$$

This is clear for $r = 1$. For $1 \le j \le r$, we may assume by induction that

$$S \not\subset \bigcup_{i=1, i\neq j}^{r} \mathfrak{p}_i.$$

Assume that $S \subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$. Then for each $j = 1, \dots, r$ there is $x_j \in S$ such that

$$x_j \in \mathfrak{p}_j \setminus \big(\bigcup_{i=1, i\neq j}^{r} \mathfrak{p}_i \big).$$

Let $\deg x_1 = \alpha$ and $\deg x_2 \dots x_r = \beta$. Then $x = x_1^{\operatorname{lcm}(\alpha,\beta)/\alpha} + (x_2 \dots x_r)^{\operatorname{lcm}(\alpha,\beta)/\beta} \in S$, since it is homogeneous, and $\gcd(\operatorname{lcm}(\alpha,\beta),\pi) = 1$. Now

$$x_1 \in \mathfrak{p}_1 \setminus \big(\bigcup_{i=2}^{r} \mathfrak{p}_i\big) \quad \text{and} \quad x_2 \dots x_r \in \big(\bigcap_{i=2}^{r} \mathfrak{p}_i\big) \setminus \mathfrak{p}_1 \quad \text{implies} \quad x \notin \bigcup_{i=1}^{r} \mathfrak{p}_i,$$

a contradiction.

Let $x \in S \setminus (\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r)$. Then $\dim M/xM = \dim M - 1$. Moreover every prime ideal in the support of $(0 : x)_M$ is in the support of M/xM. Thus $\dim (0 : x)_M \le \dim M - 1$. □

Proof of Theorem 2. We prove by induction on $\dim M = d$ that $\dim M/IM \le \gamma$ implies $a_j(\_)$ constant for all $j \ge \gamma$. This is clear if $d \le \gamma$ (then $j \ge \gamma$ implies $a_j(\_) = 0$), so we may assume $d > \gamma$. Let x be as in the lemma, and $g = \deg x$.

Set $M' = M/xM$ and $M'' = (0 : x)_M$. Then $M'/IM' \cong M/IM$ and certainly $\dim M''/IM'' \le \gamma$. Since $\dim M', \dim M'' < \dim M$, we may assume by induction that $H(M/xM, n)$ and $H((0 : x)_M, n)$, $n \gg 0$, are quasipolynomials of grade $< \gamma$.

The exact sequence

$$0 \longrightarrow (0 : x)_M(-g) \longrightarrow M(-g) \xrightarrow{\ x\ } M \longrightarrow M/xM \longrightarrow 0$$

gives the equation

$$H(M, n) - H(M, n - g) = H(M/xM, n) - H((0 : x)_M, n - g).$$

For a quasipolynomial Q it is easy to see that $Q(n - g)$ has the same grade as Q. Therefore the right-hand side in the previous equation is a quasipolynomial of grade $< \gamma$ for $n \gg 0$, and so this holds for the left-hand side, too. So it remains only to apply the following lemma. □

Lemma 4. *Let $Q(n) = \sum a_k(n) n^k$ be a quasipolynomial. If $Q(n) - Q(n - g)$ is of grade $< \gamma$ for some g coprime to the period π of Q, then* $\operatorname{grade} Q < \gamma$.

Proof. Let $u = \deg Q$ and let us first compare the leading coefficients. We can assume $\gamma \le u$. Then one has $a_u(n) - a_u(n - g) = C$ for some constant C and all n, and so $a_u(n) - a_u(n - \pi g) = \pi C$. Since π is the period, we conclude that $C = 0$, and $a_u(n) = a_u(n - g)$. But g is coprime to π, and it follows that a_u is constant.

The descending induction being started, one argues as follows for the lower coefficients. Suppose that $k \ge \gamma$. Then $a_k(n) - a_k(n - g)$ is a polynomial in the coefficients a_j for $j > k$ and g. Since the higher coefficients are constant by induction, it follows that $a_k(n) - a_k(n - g)$ is constant, too, and the rest of the argument is as above. □

3. An application to rational polytopes

In this section we shall give a purely algebraic proof of an old theorem, which was conjectured by Ehrhart ([E], p. 53), and proved independently by McMullen (see [M]) and Stanley ([S], Theorem 2.8).

Theorem 5. *Let P be a d-dimensional rational convex polytope in $\mathbb{R}^m$, and let the Ehrhart quasi-polynomial of P be*

$$E_P(n) = a_d(n)n^d + a_{d-1}(n)n^{d-1} + \ldots + a_1(n)n + a_0(n).$$

Suppose that for some δ the affine span of every δ-dimensional face of P contains a point with integer coordinates. Then $\operatorname{grade} E_P < \delta$.

Proof. We choose a field K and let R be the Ehrhart ring of P. It is the vector subspace of $K[X_1^{\pm 1}, \ldots, X_m^{\pm 1}, T]$ spanned by all Laurent monomials $X^a T^n = X_1^{a_1} \ldots X_m^{a_m} T^n$ where $a = (a_1, \ldots, a_m) \in nP$, $n \in \mathbb{Z}$, $n \geq 0$. By Gordan's lemma it follows easily that R is a finitely generated, positively graded K-algebra, where we use the exponent of T as the degree of a monomial. The Ehrhart function of P is just the Hilbert function of R. (See Chapter 6 of [BH] for more information.)

Let π be the period of E_P, and F a δ-dimensional face of P. Since the affine span of F contains a point with integer coordinates, nF contains a point with integer coordinates for all $n \gg 0$. We chose n big enough so that nF contains a point m_F with integer coordinates for every δ-dimensional face F, and $\gcd(n, \pi) = 1$.

Now let $J \subset R$ be the ideal generated by the monomials $X^{m_F} T^n$. If $\dim R/J \leq \delta$, then we are done by Theorem 2 because the ideal I in Theorem 2 contains J.

Since J is a monomial ideal, $\operatorname{Ass}_R R/J$ consists of monomial prime ideals. In particular, $\operatorname{Min}_R R/J$ consists of monomial prime ideals. By theorem 6.1.7 of [BH], for each $\mathfrak{p} \in \operatorname{Min}_R R/J$, there is a face $G_\mathfrak{p}$ of P, such that $\mathfrak{p}$ is generated by all monomials outside the cone associated with $G_\mathfrak{p}$. One has $\dim R/\mathfrak{p} = \dim G_\mathfrak{p} + 1$. Since $J \subset \mathfrak{p}$, it follows that $\dim G_\mathfrak{p} \leq \delta - 1$. So $\dim R/J = \max\{\dim R/\mathfrak{p}, \mathfrak{p} \in \operatorname{Min}_R R/J\} \leq (\delta - 1) + 1 = \delta$. □

References

[BH] W. Bruns and J. Herzog. *Cohen-Macaulay Rings*. Rev. ed. Cambridge University Press, 1998.

[E] E. Ehrhart. *Polynômes arithmétiques et Méthode des Polyèdres en Combinatoire*. International Series of Numerical Mathematics. **35**, Birkhäuser Verlag, 1977. MR0432556 (55:5544)

[M] P. McMullen. *Lattice invariant valuations on rational polytopes*. Arch. Math. **31** (1978/79), 509–516. MR0526617 (80d:52011)

[S] R. Stanley. *Decompositions of rational convex polytopes*. Ann. Discr. Math. **6** (1980), 333–342. MR0593545 (82a:52007)

FB Mathematik/Informatik, Universität Osnabrück, 49069 Osnabrück, Germany
E-mail address: winfried@math.uos.de

FB Mathematik/Informatik, Universität Osnabrück, 49069 Osnabrück, Germany; and Institute of Mathematics, C.P. 1-764, 70700 Bucharest, Romania
E-mail address: bogdan.ichim@math.uos.de; bogdan.ichim@imar.ro