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 $d$, $H(M, n) : \mathbb{Z} \to \mathbb{Z}$ the associated Hilbert function, and suppose that $r_1, \ldots, r_d$ 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 $\text{lcm}(\text{deg } r_1, \ldots, \text{deg } r_d)$.

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

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

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

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

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

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 $K[r_1, \ldots, r_d]$ (which is isomorphic to a polynomial ring over $K$). Therefore we may assume that $R = K[r_1, \ldots, r_d]$. Let $S$ be the subalgebra of $R$ generated by its homogeneous elements of degree $p = \text{lcm}(\text{deg } r_1, \ldots, \text{deg } r_d)$. Then it is not hard to see that $R$ is a finitely generated $S$-module. Therefore $M$ is a finitely generated $S$-module,
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

\[
M = M^0 \oplus \ldots \oplus M^{p-1}, \quad M^k = \bigoplus_{i \equiv_k (p)} M_i,
\]

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

\[
H(M, n) = P_k((n - k)/p), \quad n \equiv_k (p), \quad n \gg 0,
\]

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 quasi-polynomials

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 \[2\], we let the grade of \( Q \) denote the smallest integer \( \delta \geq -1 \) such that \( a_i(\lambda) \) 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 \( \pi \). Let \( I \) be the ideal of \( R \) generated by all homogeneous elements \( x \) of \( R \) such that \( \gcd(\deg x, \pi) = 1 \). Then

\[
\text{grade } Q < \dim M/IM.
\]

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 \( D(M) = \{p \in V(M), \dim A/p = \dim M\} = \{p_1, \ldots, p_r\} \). Clearly \( I \nsubseteq p_i \) for \( i = 1, \ldots, r \). By prime avoidance, we conclude that \( I \nsubseteq p_1 \cup \ldots \cup p_r \). By induction on \( r \), we show that

\[
S = \{x \in I, \; x \text{ homogeneous, } \gcd(\deg x, \pi) = 1\} \nsubseteq \bigcup_{i=1}^r p_i.
\]
This is clear for \( r = 1 \). For \( 1 \leq j \leq r \), we may assume by induction that

\[
S \not\subseteq \bigcup_{i=1, i \neq j}^{r} p_i.
\]

Assume that \( S \subset p_1 \cup \cdots \cup p_r \). Then for each \( j = 1, \ldots, r \) there is \( x_j \in S \) such that

\[
x_j \in p_j \setminus \bigcup_{i=1, i \neq j}^{r} p_i.
\]

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

\[
x_1 \in p_1 \setminus \bigcup_{i=2}^{r} p_i \quad \text{and} \quad x_2 \ldots x_r \in \bigcap_{i=2}^{r} p_i \setminus p_1 \quad \text{implies} \quad x \not\in \bigcup_{i=1}^{r} p_i,
\]

a contradiction.

Let \( x \in S \setminus (p_1 \cup \ldots \cup p_r) \). 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 \( \dim(0 : x)_M \leq \dim M - 1 \).

**Proof of Theorem** \( \Box \) We prove by induction on \( \dim M = d \) that \( \dim M/IM \leq \gamma \) implies \( a_j(\omega) \) constant for all \( j \geq \gamma \). This is clear if \( d \leq \gamma \) (then \( j \geq \gamma \) implies \( a_j(\omega) = 0 \)), 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 \( \dim M''/IM'' \leq \gamma \). 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. \( \Box \)

**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 \( \pi \) of \( Q \), then \( \text{grade} \, Q < \gamma \).

**Proof.** Let \( u = \deg Q \) and let us first compare the leading coefficients. We can assume \( \gamma \leq u \). 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 \( \pi \) is the period, we conclude that \( C = 0 \), and \( a_u(n) = a_u(n-g) \). But \( g \) is coprime to \( \pi \), and it follows that \( a_u \) is constant.

The descending induction being started, one argues as follows for the lower coefficients. Suppose that \( k \geq \gamma \). 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. \( \Box \)
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 $\delta$ the affine span of every $\delta$-dimensional face of $P$ contains a point with integer coordinates. Then $\text{grade } E_P < \delta$.

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

**References**


