

HOW TO COMPUTE HILBERT POLYNOMIALS

Shuchao Bi
January, 2009

ABSTRACT. In this write-up, I present an algorithm to compute Hilbert polynomials for homogeneous ideals in polynomial rings.

1. REDUCTION TO MONOMIAL IDEALS

Through this write-up, let's write S for the graded ring $k[x_1, \dots, x_r]$ over a field k .

Definition 1. For a homogeneous ideal $I \subset S$, define the Hilbert function of I as

$$H_I(n) = \dim_k(S/I)_n, \text{ for any natural number } n$$

where $(S/I)_n$ denote the degree n part of S/I .

Proposition 1. Let $I \subset S$ be a homogeneous ideal and $\text{in}(I)$ be the initial ideal of I respect to some monomial order $>$. Then I has the same Hilbert function as the monomial ideal $\text{in}(I)$.

Proof. Write $\text{LM}(f)$ and $\text{LT}(f)$ for leading monomial and leading term). Our goal is to show $\dim I_s = \dim \text{in}(I)_s$. If this is true, then Hilbert function $H_I(s) = \dim(S/I)_s = \dim S_s - \dim I_s = \dim S_s - \dim \text{in}(I)_s = \dim(S/\text{in}(I))_s = H_{\text{in}(I)}(s)$.

As $\{\text{LM}(f) : f \in I_s\}$ is a finite set and I is a homogeneous ideal, we can choose $f_1, \dots, f_m \in I_s$ such that

$$\{\text{LM}(f) : f \in I_s\} = \{\text{LM}(f_1), \dots, \text{LM}(f_m)\}.$$

We can further assume that all $\text{LM}(f_i)$ s are all distinct and

$$\text{LM}(f_1) > \text{LM}(f_2) > \dots > \text{LM}(f_m).$$

The key idea of this proof is to show that f_i s form a vector basis for I_s while $\text{LM}(f_i)$ s form a vector basis for $\text{in}(I)_s$.

Suppose there exist $a_i \in k$ such that

$$a_1 f_1 + \dots + a_m f_m = 0,$$

let a_i be the first a_j to be nonzero. Then $\text{LT}(a_1 f_1 + \dots + a_m f_m) = a_i \text{LM}(f_i) \neq 0$, contradiction. That implies f_i s are linearly independent. $\text{LM}(f_i)$ s are linear independent for the exact same reason.

If f_i s do not span I_s , choose one $f \in I_s$ not in the span with minimal leading monomial respect to $>$. $LT(f) = aLM(f_i)$ for some $a \in k$ and i . Take $g = f - af_i$, g is not in the span either but with smaller leading monomial, contradiction.

Noting $LM(f)_i \in in(I)_s$, it remains to prove that $LM(f)_i$ s span $in(I)_s$. For every $f \in in(I)$ which is homogeneous of degree s . By Lemma 2 below, every term of f lies in $in(I)$. So f is a k -linear combination of degree s monomials which also lie in I . It suffices to show every monomial of f is in that span. So assume f is a monomial, f lies in $in(I)$ by Lemma below $f = x^a in(g)$ for some monomial x^a and $g \in I$. (Here assume we know that $in(I)$ can be generated by finite elements of form $in(f)$ for some $f \in I$, see next section for a proof.) $x^a g$ still lies in I and $f = in(x^a g)$, let h be the degree s homogeneous part of $x^a g$, h still lies in I since I is homogeneous and $f = in(x^a g) = in(h)$. But we know $in(h) = in(f_i)$ for some i , we are done. \square

Lemma 1. A monomial x^b lies in a monomial ideal $(x^{a_1}, \dots, x^{a_t})$ iff x^b is divisible by some x^{a_i} .

Proof. Suppose

$$x^b = h_1 x^{a_1} + h_2 x^{a_2} + \dots + h_t x^{a_t} \text{ for } h_i \in S.$$

Take leading term of both sides, we can assume h_i s are terms. So all nonzero $h_i x^{a_i}$ s involve the same monomial, namely x^b , i.e., x^b is divisible by that x^{a_i} . \square

Lemma 2. A polynomial f lies in a monomial ideal iff every term of f lies in that monomial ideal.

Proof. Suppose f lie in an monomial ideal $I = (x^{a_1}, \dots, x^{a_t})$. It suffices to show the leading term of f is in I . Suppose

$$f = h_1 x^{a_1} + h_2 x^{a_2} + \dots + h_t x^{a_t} \text{ for } h_i \in S.$$

Take leading term of both sides, we see

$$LT(f) = m_1 x^{a_1} + m_2 x^{a_2} + \dots + m_t x^{a_t} \text{ for monomial } m_i \in S. \square$$

2. COMPUTING THE INITIAL IDEAL: BUCHBERGER'S ALGORITHM

In section 1, we reduce the problem of computing the Hilbert polynomial of a homogeneous ideal I to computing the Hilbert polynomial of a monomial ideal $in(I)$. So the first problem is how to find $in(I)$, i.e. given a set of generators of I , how to find a set of generators of $in(I)$, this is where the great idea of Gröbner basis comes in.

Definition 2. A Gröbner basis of an ideal $I \subset S$ is a finite set of elements $\{g_1, \dots, g_m\}$ in I such that $\{LT(g_1), \dots, LT(g_m)\}$ generate $\text{in}(I)$.

Lemma 3. There exist a Gröbner basis for any ideal I . Furthermore, any Gröbner basis $\{g_1, \dots, g_m\}$ of I generate I .

Proof. The existence is essentially a consequence of Hilbert basis theorem or equivalently Dickson's lemma. Choose a set of generators $\{g_1, \dots, g_m\}$ of I , if $\{LT(g_1), \dots, LT(g_m)\}$ do not generate $\text{in}(I)$. There exists $f \in I$, such that $LT(f)$ is not in $(LT(g_1), \dots, LT(g_m))$, i.e., $(LT(g_1), \dots, LT(g_m))$ is strictly bigger than $(LT(g_1), \dots, LT(g_m), LT(f))$. If there is no (finite) Gröbner basis for I , we could construct an infinite ascending chain, contradicts to the Hilbert basis theorem.

For the second statement, suppose the opposite, i.e., $I \neq (g_1, \dots, g_m)$. Choose a f not in (g_1, \dots, g_m) and with smallest leading term. Then $LT(f) \in \text{in}(I)$, so

$$LT(f) = h_1 LT(g_1) + \dots + h_m LT(g_m), \quad \text{for some monomials } h_i \in S.$$

Let $f' = f - h_1 g_1 + \dots + h_m g_m$, then f' has leading term strictly smaller than f , contradicts to our choice of f . \square

We will see a constructive proof of existence in a minute.

Division Algorithm

Proposition 2. For any given set of polynomials $\{g_1, \dots, g_m\}$ and f , f can be written as

$$f = h_1 g_1 + \dots + h_m g_m + r$$

with any term of r not divisible by any $LM(g_i)$. If $\{g_1, \dots, g_m\}$ is a Gröbner basis for $I = (g_1, \dots, g_m)$, then r is unique. We call r the remainder of f respect to g_i s.

Proof. The existence is the following division algorithm.

Input: g_1, \dots, g_m, f

Output: h_1, \dots, h_m, r such that

$$f = h_1 g_1 + \dots + h_m g_m + r$$

with h_i in S and any term of r not divisible by any $LM(g_i)$.

$h_1 := 0, \dots, h_m := 0, p := f$

WHILE $p \neq 0$ DO

$i := 1$

 divisionoccured := false

 WHILE $i \leq m$ AND divisionoccured = false DO

 IF $LT(g_i)$ divides $LT(p)$ THEN

```

       $h_i := h_i + \text{LT}(p)/\text{LT}(g_i)$ 
       $p := p - (\text{LT}(p)/\text{LT}(g_i))g_i$ 
      divisionoccured = true
    ELSE  $i := i + 1$ 
  IF divisionoccured = false THEN
     $r := r + \text{LT}(p)$ 
     $p := p - \text{LT}(p)$ 

```

Note, after each step, no matter division occurs or not, the leading monomial of p get smaller. So the algorithm terminates after finite steps.

For the uniqueness, suppose $f = g + r = g' + r'$ with $g, g' \in I$ and no terms of r and r' can be divisible by any $\text{LT}(g_i)$. $r - r' = g' - g \in I$, if $r - r'$ is not zero, $\text{LT}(r - r') \in \text{in}(I)$ which is generated by $\text{LM}(g_1), \dots, \text{LM}(g_m)$. By Lemma 1 in section 1 $\text{LT}(r - r')$ is divisible by some $\text{LM}(g_i)$, contradicts to the fact that no terms of r and r' can be divisible by any $\text{LT}(g_i)$. \square

Definition 3. For any two polynomial f and g , definite the S-polynomial of them as

$$S(f, g) = \frac{\text{LCM}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)} f - \frac{\text{LCM}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)} g$$

where LCM stands for least common multiple.

Proposition 3. (Buchberger's Criterion) $G = \{g_1, \dots, g_m\}$ is a Gröbner basis for $I = (g_1, \dots, g_m)$ iff for every pair $i \neq j$ the remainder of $S(g_i, g_j)$ respect to $\{g_1, \dots, g_m\}$ is zero.

Proof. " \Rightarrow ": If G is a Gröbner basis. Let r_{ij} denote the remainder of $S(g_i, g_j)$, r_{ij} lies in I as $S(g_i, g_j)$ does. If $r_{ij} \neq 0$, $\text{LT}(r_{ij})$ lies in $\text{in}(I)$ which is generated by $\{\text{LT}(g_1), \dots, \text{LT}(g_m)\}$, so by Lemma 1, $\text{LT}(r_{ij})$ is divisible by some $\text{LT}(g_i)$, contradicts to the definition of remainder.

" \Leftarrow ": This part of proof (which can be found in both references) is omitted. \square

Now let's answer the question at the beginning of this section. Given $I = (f_1, \dots, f_s)$ we want a set of generators of $\text{in}(I)$. This is given by the Buchberger's Algorithm.

Input $F = \{f_1, \dots, f_s\}$

Output a Gröbner basis $G = \{g_1, \dots, g_t\}$ for $I = (f_1, \dots, f_s)$ with F subset G

$G := F$

REPEAT

$G' = G$

FOR each pair $p \neq q$ in G' DO
 $S := \overline{S(p, q)}_{G'}$ (remainder of $S(p, q)$ w.r.t G')
IF $S \neq 0$ THEN $G := G \cup \{S\}$
UNTIL $G = G'$

The only nontrivial part of this algorithm is to how that this algorithm terminates after finite step. Now let $\text{in}(G)$ be the monomial ideal generated by leading terms of elements in set G . After each step if $G \neq G'$, there are some nonzero remainder r w.r.t G' added to G , then $\text{LT}(r)$ is not in $\text{in}(G')$, so $\text{in}(G)$ strictly contains $\text{in}(G')$, by the Hilbert Basis Theorem, this process terminates after finite steps. Note this is also a constructive proof of existence of Gröbner basis. \square

3. HILBERT-POINCARÉ SERIES FOR MONOMIAL IDEALS

For computation purpose, it turns out to be convenient to work with the generating function of Hilbert functions.

Definition 4. For a homogeneous ideal $I \subset S$, define the Hilbert-Poincaré series $HS_I(t)$ of I to be the generating function of $H_I(n)$, more explicitly,

$$HS_I(t) = H_I(0) + H_I(1)t + H_I(2)t^2 + H_I(3)t^3 + \dots$$

Proposition 4. For any homogeneous ideal $I \subset S = k[x_1, \dots, x_r]$,

$$HS_I(t) = \frac{Q(t)}{(1-t)^r} \text{ for some } Q(t) \in \mathbb{Z}[t].$$

Proof. We prove this by induction on the number of variables r in S .

$$0 \rightarrow \frac{(I:x_1)}{I}(-1) \rightarrow \frac{S}{I}(-1) \xrightarrow{x_1} \frac{S}{I} \rightarrow \frac{S}{(I,x_1)} \rightarrow 0.$$

Similar to the proof of Lemma 4 below, from this exact sequence, we get

$$HS_I(t) - tHS_I(t) = HS_{(I,x_1)}(t) - tHS_{\frac{(I:x_1)}{I}}.$$

Note, x_1 acts as zero both on $\frac{(I:x_1)}{I}$ and $\frac{S}{(I,x_1)}$, so they are actually $S/x_1 = k[x_2, \dots, x_r]$ modules. By induction hypothesis, there exist $Q_1(t)$ and $Q_2(t) \in \mathbb{Z}[t]$ such that

$$HS_{(I,x_1)}(t) = \frac{Q_1(t)}{(1-t)^{r-1}} \text{ and } HS_{\frac{(I:x_1)}{I}} = \frac{Q_2(t)}{(1-t)^{r-1}}.$$

That implies

$$HS_I(t) = \frac{Q_1(t) - tQ_2(t)}{(1-t)^r}. \quad \square$$

Now we have

$$HS_I(t) = \frac{Q(t)}{(1-t)^r} \text{ for some } Q(t) \in \mathbb{Z}[t].$$

Suppose degree $Q(t) = d$ and

$$Q(t) = a_0 + a_1t + \dots + a_d t^d \text{ with } a_i \in \mathbb{Z}$$

For $n \geq d$, the coefficient of t^n in

$$HS_I(t) = \frac{Q(t)}{(1-t)^r} = (a_0 + a_1t + \dots + a_d t^d) \left(\sum_{i=0}^{\infty} \binom{r-1+i}{r-1} t^i \right)$$

is

$$a_0 \binom{r-1+n}{r-1} + a_1 \binom{r-1+n-1}{r-1} + \dots + a_d \binom{r-1+n-d}{r-1}.$$

This can be written as a polynomial in n when $n \geq d$, replace n by a variable t in that polynomial, denote the new polynomial by $P_I(t)$, called the Hilbert polynomial of I . For $n \geq d$, $P_I(n) = H_I(n)$, so the Hilbert polynomial is well-defined. Note the above argument shows us how to get Hilbert polynomials from Hilbert-Poincaré series.

Lemma 4. Let f be a homogeneous polynomial of degree $d \in S$, we have

$$HS_I(t) = HS_{(I,f)}(t) + t^d HS_{(I:f)}.$$

Proof. From the following exact sequence

$$0 \rightarrow \frac{S}{(I:f)}(-d) \rightarrow \frac{S}{(I)} \rightarrow \frac{S}{(I,f)} \rightarrow 0$$

we get for $n \geq d$

$$H_I(n) = H_{(I,f)}(n) + H_{(I:f)}(n-d).$$

that implies

$$HS_I(t) = HS_{(I,f)}(t) + t^d HS_{(I:f)}. \quad \square$$

Algorithm for Computing Hilbert-Poincaré Series for Monomial Ideals

Input: $I = (m_1, \dots, m_k)$, m_i monomials in $S = k[x_1, \dots, x_r]$.

Output: A polynomial $Q(t)$ in $\mathbb{Z}[t]$ such that $Q(t)/(1-t)^r$ is the Hilbert-Poincaré series of S/I .

Choose $S = \{x^{a_1}, \dots, x^{a_s}\} \subset \{m_1, \dots, m_k\}$ to be the minimal set of monomial generators of I ;
 If $S = 0$ then return 1;
 If $S = 1$ then return 0;
 If all elements of S have degree 1 then return $(1 - t)^s$;
 Else
 Choose one i such that $\deg(x^{a_i}) > 1$ and $1 \leq k \leq r$ s.t. $x_k | x^{a_i}$;
 Return $(\text{HilbertPoincaré}(I, x_k)) + t(\text{HilbertPoincaré}(I : x_k))$.

Note that (I, x_k) and $(I : x_k)$ are still monomial ideals (see the lemma below). The cardinality of the minimal sets of generators of ideals (I, x_k) and $(I : x_k)$ are less than or equal to that of I , and the sums of the degrees of monomials in these minimal sets of generators are strictly less than that of I , so by induction we know the Hilbert-Poincaré series of them. \square

Lemma 5. For a monomial x^b ,

$$((x^{a_1}, \dots, x^{a_t}) : x^b) = \left(\frac{x^{a_1}}{\text{GCD}(x^{a_1}, x^b)}, \dots, \frac{x^{a_t}}{\text{GCD}(x^{a_t}, x^b)} \right).$$

Proof. The " \supset " part is trivial. For the " \subset " part. Suppose $fx^b \in I = (x^{a_1}, \dots, x^{a_t})$, by Lemma 2 every term of fx^b is in I , so we can assume f is a term. By Lemma 1, fx^b is divisible by some x^{a_i} . Suppose $fx^b = x^{a_i}p$ for some term p , then $x^{a_i}p$ is a common multiple of x^{a_i} and x^b , so we can write

$$fx^b = x^{a_i}p = \frac{x^{a_i}x^b}{\text{GCD}(x^{a_i}, x^b)}p'$$

for some term p' . Cancel x^b from both sides, we get

$$f = \frac{x^{a_i}}{\text{GCD}(x^{a_i}, x^b)}p'.$$

That implies f is in the righthand side. \square

4. EXAMPLES

5. COMPUTING DIMENSIONS

REFERENCES

- D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms.
- D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Chapter 15.

G. Greuel, G. Pfister, A Singular Introduction to Commutative Algebra.