An algorithm for the Hilbert-Samuel function of a primary ideal

Teo Mora * and Maria Evelina Rossi **

Dipartimento di Matematica,
Via L.B. Alberti 4, 16132 Genova
Italy
E-mails: * rossim@dima.unige.it and **theomora@dima.unige.it †

1 Introduction

Let R be a noetherian local ring of dimension d, m its maximal ideal, $K = R/m$ the residue field. If I is an m-primary ideal, then $l_R(R/I)$ is finite, each I^n/I^{n+1} is naturally an R-module and the Hilbert-Samuel function of I is the numerical function

$$H_I(n) = l_R(I^n/I^{n+1}).$$

The Poincaré-Samuel series is its generating series

$$P_I(t) = \sum_{n\geq 0} H_I(n)\ t^n.$$

By the Hilbert-Serre Theorem, there exists a polynomial $\mathcal{P}_I(t) \in \mathbb{Q}[t]$ such that

$$P_I(t) = \mathcal{P}_I(t)/(1-t)^d,$$

where $\mathcal{P}_I(1) = e = e(I)$ the multiplicity of the m-primary ideal I.

† The first author thanks the GAGE, École Polytechnique, Palaiseau in Paris for hospitality and financial support during the preparation of this paper. The second author is partially supported by M.P.I. (Italy). The research is also partially supported by ESPRIT-BRA 6846 **PoSSo** and HCM Network EUROPROJ

Several algorithms exist for computing the Hilbert-Samuel function when I is the maximal ideal of R. Not a great deal is known about computational methods for a primary ideal. For an approach to the computation of Hilbert-Samuel functions of primary ideals, see [**17**].

The reason that pushed us to find a good procedure to compute the Hilbert-Samuel function of a primary ideal is the increasing interest concerning this topic in different fields. In the geometric case, the Hilbert-Samuel function of a m-primary ideal of a local ring can give a numerical measure of the singularity of the variety at a corresponding point. Moreover in these last years, many authors are working in interesting problems related to the Hilbert-Samuel function of a 0-dimensional scheme in the projective space. In this case the defining ideal is intersection of $\wp$-primary ideals with $\wp$ a prime ideal corresponding to a point in the associated reduced scheme (see for example [**6**], [**5**]). Also in [**15**] and [**16**] there are very interesting results and questions about the Hilbert-Samuel function of a primary ideal with respect to the maximal ideal of a d-dimensional local Cohen-Macaulay ring.

We think that to have an implemented procedure to compute the Hilbert-Samuel function also in the primary case could be useful; the algorithm we outline in this paper is already implicit in the computer algebra literature and is well within reach of most specialized systems for computations in algebraic geometry; we hope that making it explicit, will make it soon available in many of them. For the same reason, we conclude our paper with a practical guide for "computing it yourself".

2 The taming of the problem

Enter Problem

Let R be a local ring, m its maximal ideal, K the residue field and let I be an m-primary ideal. The direct sum $\bigoplus_{n=0}^{\infty} I^n/I^{n+1}$ is a naturally graded R/I-algebra, denoted $\mathrm{Gr}_I(R)$ and called the graded ring associated to the ideal I. Remark that $H_I(n) = l_R([Gr_I(R)]_n)$, that is the length of the homogeneous part of degree n of the graded ring.

Our aim is to compute explicitly the Hilbert-Samuel polynomial (or the Poincaré-Samuel series) of I and we need therefore to specialize our setting, in order to have sufficiently concrete data for the algorithms we are describing. All over the paper, therefore, the local ring R will be restricted to be the localization at a prime ideal of a finitely generated algebra over a field k. This restriction alone however is not sufficient, since all data must be represented in a form amenable to computations. The algorithms we are going to describe, in fact, will produce the answer we sought (the Hilbert-Samuel function of $I \subset R$) by manipulating the data described below.

So we assume to explicitly know:

1) an effective field k [(1)].

[(1)] Usually a finite extension of the rationals or of another prime field; if you are used to work with algebraically closed fields, you don't have to worry: the smallest field containing the definition

2) a polynomial ring $P := k[X_1, \ldots, X_n]$ over k
3) a finite system of generators $\{h_1, \ldots, h_t\}$ of an ideal $H \subset P$
4) a finite system of generators $\{f_1, \ldots, f_s\}$ of an ideal $J \subset P$.

We assume moreover that J is primary for a prime ideal $\wp$ of dimension d and we also need to explicitly know:

5) a finite system of generators $\{g_1, \ldots, g_r\}$ of $\wp$.

We then define $Q = P/H$, $\pi : P \longrightarrow Q$ the canonical projection, $R = Q_{\pi(\wp)}$, $m = \pi(\wp)R$, $I = \pi(J)R$. We also define $A = Q_{1+\pi(J)}$, $L = \pi(J)A$.

Example To make our assumptions clear, let us assume we want to compute the Hilbert function of $m^2 \subset R$, where R is the localization at a rational normal curve of the coordinate ring of a rational normal surface of $\mathbb{C}^3$.

To make the computation viable, we need to specify *which* rational nomal surface and curve we are thinking of. So we set:

1) $k = \mathbb{Q}$, the definition field of both the ideal of the rational normal curve and surface
2) $P = \mathbb{Q}[X_1, \ldots, X_3]$
3) $h_1 = X_1X_2 - X_3$, so that the ideal of the surface is $H = (h_1)$
4) the following polynomials

$$f_1 = g_1^2 = X_1^4 - 2X_2X_1^2 + X_2^2$$

$$f_2 = g_1g_2 = X_2X_1^3 - X_2^2X_1 - X_3X_1^2 + X_3X_2$$

$$f_3 = g_1g_3 = -X_2^2X_1^2 + X_3X_1^3 + X_2^3 - X_3X_2X_1$$

$$f_4 = g_2^2 = X_2^4 - 2X_3X_2^2X_1 + X_3^2X_1^2$$

$$f_5 = g_2g_3 = -X_2^3X_1 + X_3X_2X_1^2 + X_3X_2^2 - X_3^2X_1$$

$$f_6 = g_3^2 = X_2^4 - 2X_3X_2^2X_1 + X_3^2X_1^2$$

defining the $\wp$-primary ideal $J = \wp^2$, where $\wp$ has dimension 1

5) a finite system of generators for $\wp$, i.e. the following polynomials:

$$g_1 = X_1^2 - X_2 \quad g_2 = X_1X_2 - X_3 \quad g_3 = X_1X_3 - X_2^2$$

It should be clear that the problem is equivalent to computing the Hilbert-Samuel function of $m^2 \subset R$, where R is the localization at a rational normal curve of ring of the affine plane $\mathbb{C}^2$.

Computers are however dumb and cannot suspect that if you don't tell them. The setting here would be much more easy and the computations more feasible. One has to give:

1) $k = \mathbb{Q}$
2) $P = \mathbb{Q}[X_1, X_2]$
4) $f_1 = g_1^2 = X_1^4 - 2X_2X_1^2 + X_2^2$

---

fields of the ideals $H, J, \wp$ is a finite extension of the prime field. You compute over this field and then tensor (in your mind) with your algebraically closed field defining the $\wp$-primary ideal $J = \wp^2$, where $\wp$ is the rational normal curve generated by:

5) $g_1 = X_1^2 - X_2$

and the solution of the problem is then obviously $H_I(n) = 2\ \forall n$.

In fact we will use this simpler isomorphic case, to prove the correctness of all the computations we will perform on our example.

Enter Graal

We start by recalling the basic definitions related to standard and Gröbner bases for an ideal in a polynomial ring $P := k[X_1, \ldots, X_n]$.

Let $<$ be a semigroup ordering over the semigroup of power-products of P, i.e. the semigroup generated by $\{X_1, \ldots, X_n\}$. Each non-zero polynomial $f \in P$ can be uniquely written as an ordered combination of power-products $f = \sum c_i \tau_i$, with $c_i \in k \setminus \{0\}$, $\tau_1 > \tau_2 > \cdots$; τ_1 is then called the leading term of $f, \tau_1 = T(f)$. For an ideal $\mathcal{I}$, the leading term ideal $T(\mathcal{I})$ is the ideal generated by $\{T(f) : f \in \mathcal{I} \setminus \{0\}\}$.

A *standard basis* of $\mathcal{I}$ is a set $G \subset \mathcal{I}$ s.t. $\{T(g) : g \in G\}$ generates $T(\mathcal{I})$. If $<$ is a well-ordering then a standard basis is called a *Gröbner basis* of $\mathcal{I}$.

This notion is strictly related with the one of standard bases for L-adic topologies, or L-standard bases, which we recall now:
If A is a ring and $L \subset A$ is an ideal s.t. $\bigcap L^n = (0)$, then define the associated graded ring to be $Gr_L(A) = \bigoplus_{n=0}^{\infty} L^n/L^{n+1}$ [(2)] For each $a \in A \setminus \{0\}$, there is a well-defined $n = v_L(a)$ s.t. $a \in L^n, a \notin L^{n+1}$ and so a well-defined element $in_L(a) \in L^n/L^{n+1} \subset Gr_L(A)$, which is the residue class of a mod$L$. An L-standard basis of an ideal $\mathcal{I} \subset A$ is a set $G \subset \mathcal{I}$ s.t. $\{in_L(g) : g \in G\}$ generates $in_L(\mathcal{I}) = \{in_L(f) : f \in \mathcal{I}\}$.

Since the notion of associated graded ring is crucial for the solution of our problem, we must first of all give a "concrete" version of the notion; we start by remarking that $Gr_L(A)$ is a finitely generated graded A/L-algebra and, under the further assumption that A/L is a finitely generated graded k-algebra, then it is a finitely generated k-algebra too, i.e. the quotient of a suitably graded polynomial ring over k modulo a homogeneous ideal. If this ideal were known through a Gröbner basis, then the whole corpus of algorithmic commutative algebra could be used to derive information about $Gr_L(A)$ and therefore about the L-adic topology of A. This leads to the following:

Definition 1 *Let A is a ring and $L \subset A$ is an ideal s.t.*

- $\bigcap L^n = (0)$
- *A/L is a finitely generated algebra over a field k*

The Graal *of $L \subset A$ is the assignment of*

1) two sets of indeterminates $\{X_1, \ldots, X_n\}$, $\{T_1, \ldots, T_s\}$

2) a set of polynomials $G := \{p_1, \ldots, p_t\} \subset \mathcal{P} := k[X_1, \ldots, X_n, T_1, \ldots, T_s]$

s.t. grading $\mathcal{P}$ by setting $\deg(X_i) := 0, \deg(T_j) := 1$ and denoting $\mathcal{H}$ the ideal generated by $\{p_1, \ldots, p_t\}$, one has:

a) the p_i's are homogeneous, and therefore such is $\mathcal{H}$

b) G is a Gröbner basis of $\mathcal{H}$ for some ordering

c) $Gr_I(R) = \bigoplus_{d=0}^{\infty} L^d/L^{d+1} \simeq \mathcal{P}/\mathcal{H}$

---

(2) This of course generalizes the notion of associated graded ring we have given for a local ring R and an ideal I, which is primary for the maximal ideal.

Remark that the Graal of $I \subset R$ is *not* just the associated graded ring of I; it is an explicit representation of it, which is particularly suitable for computations, because it is given as the quotient of a polynomial ring by an ideal given through a Gröbner basis. Again, the point here is that the Graal can be computed, but of course, only if our setting is suitably restricted and a convenient representation of A and L is available.

We therefore assume to have data 1),2),3),4) as in the preceding section, i.e. to be given k, P, $\{h_1, \ldots, h_t\}$, $\{f_1, \ldots, f_s\}$, so that defining $H = (h_1, \ldots, h_t)$, $J = (f_1, \ldots, f_s)$, $Q = P/H$ and $\pi : P \longrightarrow Q$ the canonical projection, one has:

$$A = Q_{1+\pi(J)} \quad L = \pi(J)A.$$

Now we consider the polynomial ring $\mathcal{P} = k[X_1, \ldots, X_n, T_1, \ldots, T_s]$ and the ideal $\mathcal{T} = (T_1, \ldots, T_s)$ in it and we remark that $Gr_{\mathcal{T}}\mathcal{P}$ is $\mathcal{P}$ itself, graded by assigning $\deg(X_i) = 0$, $\deg(T_j) = 1$. We fix a semigroup ordering $<$ s.t.

- $\deg(\tau_1) > \deg(\tau_2)$ implies $\tau_1 < \tau_2$
- $X_i > 1 \ \forall i$

and we define $<_w$ to be the semigroup well-ordering s.t. $\tau_1 <_w \tau_2$ if and only if

- either $\deg(\tau_1) < \deg(\tau_2)$
- or $\deg(\tau_1) = \deg(\tau_2)$ and $\tau_1 > \tau_2$.

With these definitions and notation, then the Graal can be computed as follows [**14**]:

Theorem 1 *Let $\Im$ be the ideal generated by $\{h_1, \ldots, h_t, f_1 - T_1, \ldots, f_s - T_s\}$ and let G be a standard basis of it w.r.t. $<$. Then:*

1) $\{in_{\mathcal{T}}(g) : g \in G\}$ generates $\mathcal{H} := in_{\mathcal{T}}(\Im)$

2) $\{in_{\mathcal{T}}(g) : g \in G\}$ is a Gröbner basis of $\mathcal{H}$ w.r.t. $<_w$

3) $Gr_L(A) \simeq \mathcal{P}/\mathcal{H}$

Moreover:

4) $G \cap k[X_1, \ldots, X_n]$ is a Gröbner basis of $J + H \subset P$

Example (cont.) With the same notation the Graal of $L \subset A$ is the assignment of

$$\mathcal{P} = \mathbb{Q}[X_1, X_2, X_3, T_1, T_2, T_3, T_4, T_5, T_6]$$

and of the polynomials

$$X_3 - X_2X_1, T_4, T_2, T_5, T_3 - X_2T_1, T_6 - 2X_2X_1^2T_1 + X_1^4T_1, X_2^2 - 2X_2X_1^2 + X_1^4$$

which define the ideal $\mathcal{H}$ since

$$X_3 - X_2X_1, T_4, T_2, T_5, -T_3 + X_2T_1, T_6 - X_2^2T_1,$$

$$X_2^2 - 2X_2X_1^2 + X_1^4 - T_1, X_2^4 - 2X_3X_2^2X_1 + X_3^2X_1^2 - T_6, X_2^3 - X_3X_2X_1 - X_2^2X_1^2 + X_3X_1^3 - T_3$$

are a standard basis of $\Im$ (3)

(3) The computation above has been performed with an experimental implementation by A. Carbone of the Graal algorithm over CoCoA 1.5. If you are interested the computation took 0.15 secs. on a Mac Powerbook 180. The ordering we have chosen is quite complex to describe now (see however footnote 10); the leading terms are however the leftmost ones.

We can easily check the computation above on the equivalent version of the example, where $\mathcal{P} = \mathbb{Q}[X_1, X_2, T_1]$, $\Im = (X_2^2 - 2X_2X_1^2 + X_1^4 - T_1)$, so that $\mathcal{H} = (X_2^2 - 2X_2X_1^2 + X_1^4)$. The isomorphism between the two associated graded rings is an obvious projection.

The reader will have remarked that the Graal we are able to compute is not the one for which we wish to compute Hilbert functions. The former in fact is $Gr_L(A)$, where A is the localization of the coordinate ring Q at $1 + \pi(J)$ and $L = \pi(J)A$; the latter is $Gr_I(R)$ where R is the localization of Q at the prime $\pi(\wp)$, and $I = \pi(J)R$.

In [**14**] it is explained how to generalize Theorem 1 to compute $Gr_I(R)$ when I is the maximal ideal of Q. The same technique applies to this slightly more general case, where I is just primary, as we detail now.

First of all remark that if $\wp$ is maximal, then $R = A$: in fact, since $1+\pi(J) \subset Q \setminus \pi(\wp)$, $A \subset R$; conversely if $g \in Q$ is not in $\pi(\wp)$, then there are $f \in Q$, $h \in \wp$, s.t. $gf = 1 - h$; by nilpotency, there is ρ s.t. $h^\rho \in \pi(J)$ and then $gf(1 + h + \cdots h^{\rho-1}) = 1 - h^\rho$, proving the converse inclusion.

Then remark, that if $\wp$ is prime and not maximal, since we know a basis of $\wp$ we can obtain a Gröbner basis of it and so a maximal subset of variables which are algebraically independent mod$\wp$. After renumbering, let them be $X_1, \ldots, X_d$. Define then $P_0 = k(X_1, \ldots, X_d)[X_{d+1}, \ldots, X_n]$, H_0, J_0 the ideals in P_0 generated by the h_i's and the f_j's resp., $\wp_0 = \wp P_0$, $Q_0 = P_0/H_0$, $\pi_0 : P_0 \longrightarrow Q_0$ the canonical projection; then $R = (Q_0)_{\wp_0}$ and $I = \pi_0(J_0)(Q_0)_{\wp_0}$, so reducing effectively to the case in which $\wp$ is maximal.

To conclude, we have therefore an explicit method for computing the Graal of $I \subset R$, since a standard basis of $\Im$ can be computed (see sect. 4 for details).

Example (cont.) It is clear that X_1 is alg. ind. mod.$\wp$, so we have to change our setting to:

1) $k = \mathbb{Q}(X_1)$
2) $P = k[X_2, X_3]$
3) $h_1 = X_1X_2 - X_3$
4) the following generators of J_0

$$f_1 = g_1^2 = X_1^4 - 2X_2X_1^2 + X_2^2$$

$$f_2 = g_1g_2 = X_2X_1^3 - X_2^2X_1 - X_3X_1^2 + X_3X_2$$

$$f_4 = g_2^2 = X_2^4 - 2X_3X_2^2X_1 + X_3^2X_1^2$$

since $\wp_0$ is generated by

5) $g_1 = X_1^2 - X_2$, $g_2 = X_1X_2 - X_3$.

The Graal of $I \subset R$ is then the assignment of $\mathcal{P} = \mathbb{Q}(X_1)[X_2, X_3, T_1, T_2, T_4]$ and of the polynomials

$$X_3 - X_2X_1, T_4, T_2, X_2^2 - 2X_2X_1^2 + X_1^4$$

which define the ideal $\mathcal{H}$ since

$$X_3 - X_2X_1, T_4, T_2, X_2^2 - 2X_2X_1^2 + X_1^4 - T_1$$

is a standard basis of $\Im$.

Analogously, in the isomorphic version of the example, the setting becomes:

1) $k = \mathbb{Q}(X_1)$
2) $P = k[X_2, X_3]$
4) $f_1 = g_1^2 = X_1^4 - 2X_2X_1^2 + X_2^2$
5) $g_1 = X_1^2 - X_2$ and the Graal of $I \subset R$ is the assignment of $\mathcal{P} = \mathbb{Q}(X_1)[X_2, T_1]$ and $\mathcal{H} = (X_2^2 - 2X_2X_1^2 + X_1^4)$.

Enter Gröbner

Gröbner bases play an important rôle for the computation of (classical) Hilbert functions because of a well known theorem by Macaulay which states that, for a homogeneous ideal $\mathcal{I} \subset k[X_1, \ldots, X_n]$ there is a k-vector space isomorphism between corresponding homogeneous components of the graded rings $k[X_1, \ldots, X_n]/\mathcal{I}$ and $k[X_1, \ldots, X_n]/T(\mathcal{I})$. The computation of the Hilbert function of $k[X_1, \ldots, X_n]/\mathcal{I}$ is therefore reduced to the computation of the one of $k[X_1, \ldots, X_n]/T(\mathcal{I})$ and this in turn is reduced to counting the number of power-products of each degree, which are not in $T(\mathcal{I})$, a question for which very effective techniques have been produced in recent years.

For our setting, Gröbner bases play a similar rôle: the next section will be devoted to show that easy modifications to all the known algorithms allow to count the number of power-products of each degree, which are not in $T(\mathcal{H})$. This gives the Hilbert function of $\mathcal{P}/\mathcal{H}$ as a k-algebra, i.e. the function $H_{\mathcal{H}}(\bullet)$ such that $H_{\mathcal{H}}(d)$ counts the dimension of the k-vector space generated by the elements $\{f \in \mathcal{P}/\mathcal{H} : f \text{ homogeneous}, deg(f) = d\}$, which because of Theorem 1 is equal to $dim_k(I^d/I^{d+1})$.

Exit Problem

The only problem which is left is what is the relation between the Hilbert function $H_{\mathcal{H}}(\bullet)$ that we know how to compute and the Hilbert function $H_I(\bullet)$ that we want to compute.

This is a consequence of the following well-known fact (we recall that $K = R/m$):

Lemma 1 $H_{\mathcal{H}}(\bullet) = dim_k(K)H_I(\bullet)$

Proof: Denote by M the R-module I^d/I^{d+1}. Since I is a m-primary ideal, there exists an integer ρ such that $m^\rho M = 0$. Hence there is a finite chain of R-modules

$$M \supset mM \supset m^2M \supset \cdots \supset m^{\rho-1}M \supset m^\rho M = 0$$

Let $M_i := m^{i-1}M/m^iM$ for $i = 1 \ldots \rho$ and $l_R(N)$ be the length of the R-module N. If we consider the above chain we have $l_R(M) = \sum_i l_R(M_i)$. Now each M_i is a K-vector space and so it is easy to see that $l_R(M_i) = dim_K(M_i)$. It is clear that M_i is also a k-vector space and $dim_k(M) = \sum_i dim_k(M_i)$.

So finally one has:

$$H_{\mathcal{H}}(d) = dim_k(M) = \sum dim_k(M_i) = dim_k(K) \sum dim_K(M_i) =$$

$$= dim_k(K) \sum l_R(M_i) = dim_k(K) l_R(M) = dim_k(K) H_I(d)$$

proving the assertion. ▮

Of course, we must be able to compute also $dim_k(K)$, but this is the multiplicity of $\wp \subset P$, which we can obtain, e.g., by computing its Hilbert function with Gröbner basis techniques. [(4)].

Example (cont) The example we have given, once the Graal is known, is so trivial that it can be computed by hand. We have in fact to count the number of power-products of each degree which are not in the power-product ideal $(X_3, T_4, T_2, X_2^2) \subset \mathbb{Q}(X_1)[X_2, X_3, T_1, T_2, T_4]$ and there are of course 2 of them for each degree δ, namely $T_1^\delta, X_2 T_1^\delta$. Since $K = k = \mathbb{Q}(X_1)$ we are through. [(5)]

3 Double Poincaré series, or Much Ado About Nothing

As mentioned previously, all the known algorithms for Hilbert functions assume the polynomial ring to be graded in the natural way, so that each indeterminate has degree 1.

The only new thing here is that we have to compute the Hilbert function of a quotient of a polynomial ring $\mathcal{P} := k[X_1, \ldots, X_n, T_1, \ldots, T_s]$ where $\deg(T_i) = 1$ but $\deg(X_j) = 0$. The obvious solution is to consider $\mathcal{P}$ as bigraded by considering a second degree Δ s.t. $\Delta(T_i) = 0, \Delta(X_j) = 1$. The ideal $\mathcal{H}$ is not necessarily bihomogeneous, but the ideal $T(\mathcal{H})$ is such. So, if we define $H^{(2)}(d_1, d_2)$ to be the cardinality of the set of those terms $\tau \notin T(\mathcal{H})$ s.t. $\deg(\tau) = d_1, \Delta(\tau) = d_2$ and $P^{(2)}(t_1, t_2) = \sum H^{(2)}(d_1, d_2) t_1^{d_1} t_2^{d_2}$, one has that $H_{\mathcal{H}}(d) = \sum_{d_2} H^{(2)}(d, d_2)$ (the sum being finite since each X_i is nilpotent) and that $P_{\mathcal{H}}(t) := \sum_d H_{\mathcal{H}}(d) t^d = P^{(2)}(t, 1)$. Remark that $P^{(2)}(t_1, t_2) = \mathcal{P}^{(2)}(t_1, t_2)/(1-t_1)^n (1-t_2)^s$ for a polynomial $\mathcal{P}$.

It is then easy to modify all the known algorithms for Hilbert function computation so that they compute $H^{(2)}(d_1, d_2)$ and $P^{(2)}(t_1, t_2)$ for a monomial ideal.

Here is a fast review of the Hilbert function algorithms, where we denote by $\mathcal{M}$ a monomial ideal in $k[X_1, \ldots, X_n]$ with the usual graduation and by $H_{\mathcal{M}}(\bullet)$, $\mathcal{P}_{\mathcal{M}}(\bullet)$ its Hilbert function and the polynomial s.t. its Poincaré series is $\mathcal{P}_{\mathcal{M}}(t)/(1-t)^n$. To avoid cumbersome notation, we will identify $\mathcal{M}$ with the underlying set of power products. The algorithms will be described in a very sketchy form, referring to the original papers for a more detailed description, including essential improvements.

Möller-Mora algorithms

Denote by χ the characteristic function of $\mathcal{M}$, i.e. the function which to each power-product τ associates the value 1 if $\tau \notin \mathcal{M}$, the value 0 if $\tau \in \mathcal{M}$ and by μ the Moebius

---

(4) This is a second reason why we need the explicit knowledge of a system of generators of $\wp$, the first one being the need of extracting a maximal set of indipendent variables mod$\wp$.

(5) We could of course have chosen to invert X_2; then $K = k[X_1]/(X_1^2 - X_2)$, the power-product ideal would have been $(X_3, T_4, T_2, X_1^4) \subset \mathbb{Q}(X_2)[X_1, X_3, T_1, T_2, T_4]$, giving $H_{\mathcal{H}}(\delta) = 4, dim_k(K) = 2, H_I(\delta) = 2$.

inversion function of χ, i.e. the function s.t.

$$\chi(\tau) = \sum_{\omega|\tau} \mu(\omega) \quad \forall \tau$$

which is non-zero only for finitely many ω's. Then:

$$H_{\mathcal{M}}(\bullet) = \sum_{\tau} \mu(\tau) H_{\tau}(\bullet)$$

$$P_{\mathcal{M}}(\bullet) = \sum_{\tau} \mu(\tau) P_{\tau}(\bullet).$$

The papers [**11,12**] give different algorithms to compute the function μ; these algorithms are now obsolete but have been the first ones to have polynomial complexity in the number of generators of $\mathcal{M}$[6].

The reduction to the monomial case via Gröbner bases and Macaulay theorem and the use of Moebius function is already in [**4**].

Bayer-Stillman algorithm

Let $\mathcal{M}$ be generated by $\{\tau_1, \ldots, \tau_r\}$, $\mathcal{M}'$ be generated by $\{\tau_1, \ldots, \tau_{r-1}\}$ and let $\mathcal{M}'' = \mathcal{M}' : \tau_r$. Bayer-Stillman algorithm ([**1**]) computes $\mathcal{P}_{\mathcal{M}}(t)$ by the formula:

$$\mathcal{P}_{\mathcal{M}}(t) = \mathcal{P}_{\mathcal{M}'}(t) - t^{\deg(\tau_r)} \mathcal{P}_{\mathcal{M}''}(t)$$

using induction on the number of generators. Their paper contains also a discussion of multigraded Hilbert functions.

BCR algorithm

Bayer-Stillman algorithm works by recursion on the number of generators; an approach by recursion on the number of indeterminates was introduced in [**9**] and is at the basis of the algorithm in [**2**].

Choose a variable, say Y, and let $a_1, \ldots, a_s$ be an increasing sequence in $\mathbb{N}$, $\omega_{11}, \ldots, \omega_{1u_1}, \ldots, \omega_{s1}, \ldots, \omega_{su_s}$ be power products free of Y s.t. $\mathcal{M}$ is minimally generated by

$$\{Y^{a_1}\omega_{11}, \ldots, Y^{a_1}\omega_{1u_1}, \ldots, Y^{a_s}\omega_{s1}, \ldots, Y^{a_s}\omega_{su_s}\}$$

Denote $\mathcal{M}_j$ the ideal generated by $\omega_{11}, \ldots, \omega_{1u_1}, \ldots, \omega_{j1}, \ldots, \omega_{ju_j}$. Then:

$$\mathcal{P}_{\mathcal{M}}(t) = 1 + t^{a_1}(\mathcal{P}_{\mathcal{M}_1}(t) - 1) + \ldots + t^{a_s}(\mathcal{P}_{\mathcal{M}_s}(t) - 1)$$

and there is a straightforward but more complex formula for $H_{\mathcal{M}}(\bullet)$.

---

(6) A Hilbert function algorithm is necessarily exponential in the number of indeterminates, unless P=NP, since the subproblem of computing the dimension of a monomial ideal is NP-complete.

The paper [**2**] not only introduces the formula for $\mathcal{P}_{\mathcal{M}}$ ([**9**] uses only the formula for $H_{\mathcal{M}}$) but also devises an algorithm which makes an "optimal" choice for the "pivot" variable; as a consequence the algorithm in most instances has quadratic complexity [(7)] in the number of generators.

Hollman algorithm

Hollman algorithm ([**8**]) in a sense is a hybrid between Bayer-Stillman and BCR ([**2**]) algorithms; it recursively reduces the number of variables like BCR, but instead of using a decomposition, it applies division like Bayer-Stillman. It chooses a variable Y and makes use of the formula:

$$\mathcal{P}_{\mathcal{M}}(t) = \mathcal{P}_{\mathcal{M}'}(t) + t\mathcal{P}_{\mathcal{M}''}(t)$$

where $\mathcal{M}' = \mathcal{M} \cup (Y)$, $\mathcal{M}'' = \mathcal{M} : Y$.

The Divide-and-Conquer algorithm

The Divide-and-Conquer algorithm ([**3**]) selects, randomly but according to some well-defined strategy, a term τ and applies the formula:

$$\mathcal{P}_{\mathcal{M}}(t) = \mathcal{P}_{\mathcal{M}'}(t) + t^{\deg(\tau)}\mathcal{P}_{\mathcal{M}''}(t)$$

where $\mathcal{M}' = \mathcal{M} \cup (\tau)$, $\mathcal{M}'' = \mathcal{M} : \tau$.

Double Poincaré Series

The generalization of all these algorithms to a monomial ideal $\mathcal{M}$ in the ring $k[X_1, \dots, X_n, T_1, \dots, T_s]$, bigraded by deg and Δ as above, is straightforward.

All algorithms need the knowledge of the Hilbert function or of the Poincaré series of an ideal generated by a single power product τ. In the classical case, one has: $\mathcal{P}_\tau(t) = t^{\deg(\tau)}$; in the generalized case, one has: $\mathcal{P}^{(2)}_\tau(t) = t^{\deg(\tau)}t_1^{\Delta(\tau)}$. Similar formulas hold for Hilbert functions.

Then the formulas are to be straightforwardly changed to become:

$$\begin{aligned}
\mathcal{P}^{(2)}_{\mathcal{M}}(t,t_1) &= \mathcal{P}^{(2)}_{\mathcal{M}'}(t,t_1) - t^{\deg(\tau_r)}t_1^{\Delta(\tau_r)}\mathcal{P}^{(2)}_{\mathcal{M}''}(t,t_1) && \text{Bayer}-\text{Stillman}\\
\mathcal{P}^{(2)}_{\mathcal{M}}(t,t_1) &= 1 + u^{a_1}(\mathcal{P}^{(2)}_{\mathcal{M}_1}(t,t_1) - 1) + \ldots + u^{a_s}(\mathcal{P}^{(2)}_{\mathcal{M}_s}(t,t_1) - 1) && \text{BCR}\\
\mathcal{P}^{(2)}_{\mathcal{M}}(t,t_1) &= \mathcal{P}^{(2)}_{\mathcal{M}'}(t,t_1) + u\mathcal{P}_{\mathcal{M}''}(t,t_1) && \text{Hollman}\\
\mathcal{P}^{(2)}_{\mathcal{M}}(t,t_1) &= \mathcal{P}^{(2)}_{\mathcal{M}'}(t,t_1) + t^{\deg(\tau)}t_1^{\Delta(\tau)}\mathcal{P}^{(2)}_{\mathcal{M}''}(t) && \text{Divide}-\text{and}-\text{Conquer}
\end{aligned}$$

where, in the BCR and the Hollman formulas, $u = t$ if $Y = X_i$, $u = t_1$ if $Y = T_j$.

---

(7) as opposed to exponential in the number of indeterminates.

4 All's well that ends well: a practical guide to computation

This section aims to be a sort of "practical guide" for the interested readers who wish to really perform Hilbert function computations on their favourite specialized computer algebra system.

Some systems could support the algorithm we have described in its full generality, but surely all of them allow to compute it under some restrictions and perhaps by using "dirty tricks" to force them to do computations which they are not planned to do. We will describe here both what can be straightforwardly done with the systems and also the "dirty tricks"; the latter don't require any programming ability from the user, since they just require to suitably modify the input and interpreting the output of a computation.

Since all the systems support only the arithmetics of either a prime field or a rational function field on it, we will restrict ourselves to the case in which $k = \mathbb{Q}$ or $k = \mathbb{Z}_p$; in fact there are easy "dirty tricks" to force them to compute with algebraic extensions, but presenting them too, would have made the presentation even more complex than it is now.

Reducing to the case in which $\wp$ is maximal and computing its multiplicity

Recall that $\wp$ is given by a system of generators $g_1, \ldots, g_r$ in $k[X_1, \ldots, X_n]$ where $k = \mathbb{Q}$ or $k = \mathbb{Z}_p$ and remark that none of the system provides a test of primality for $\wp$, so it is your task to assure that $\wp$ is prime and J a $\wp$-primary ideal. All the systems allow to compute the multiplicity and the dimension of $\wp$ (the former gives you $\dim_k(K)$), but most system don't give a maximal set of independent variables too.

If the example doesn't involve too many variables, there is a painful way out, where all steps except the first must be performed by paper and pencil:

- compute a Gröbner basis of $\wp$ for any ordering and collect the power-products in $T(\wp)$
- take its radical, by substituting each occurrence of a power of a variable by the variable itself (e.g. substitute $X_1^2 X_2$ with $X_1 X_2$)
- find out, by paper and pencil, a maximal set of variables $X_{i_1}, \ldots, X_{i_d}$ s.t. no generator of the radical of $T(\wp)$ depends only on these variables; this is a maximal set of independent variables; their cardinality must be of course the same as the dimension of $\wp$, allowing easily to correct mistakes.

Computing the Graal

We can now assume $\wp$ to be maximal, but at the price of having enlarged k; so we need to modify somehow the description of our data, to make the rest of the presentation easier; we therefore assume to know:

1) a field $k = k_0(Z_1, \ldots, Z_d)$ where either $k_0 = \mathbb{Q}$ or $k_0 = \mathbb{Z}_p$
2) $P := k[X_1, \ldots, X_n]$
3) a finite system of generators $\{h_1, \ldots, h_t\}$ of an ideal $H \subset P$
4) a finite system of generators $\{f_1, \ldots, f_s\}$ of an ideal $J \subset P$ where J is primary for a *maximal* ideal $\wp$
5) a finite system of generators $\{g_1, \ldots, g_r\}$ of $\wp$.

In other words we have just made explicit the trascendence basis of k over its prime field. This, of course, because if your system doesn't compute with trascendental extensions, you will have to play dirty tricks with the Z_i's.

In principle, there are two efficient algorithms for computing the Graal of $L \subset A$:

- the first one uses a variant of Buchberger algorithm for computing Gröbner bases, the Tangent Cone Algorithm, which applies to orderings which are not well-orderings and so allows to compute standard bases of polynomial ideals; we refer to the tutorial [**13**] for a description. We have already seen that once a standard basis of $\Im$ is known for a suitable ordering, the Graal is obtained by selecting the initial forms of the basis elements
- under the assumption that a Gröbner basis of H is known (of course you can compute it and substitute it to the original basis of H in your data), a more efficient algorithm has been recently proposed in [**7**], where the application to Graal computation is explicitly described.

Remark that your favourite computer algorithm system either does not yet support the algorithm mentioned above, or does not allow to perform computations over a rational functional field k. However you are lucky since a standard basis computation can be always reduced via homogeneization to a Gröbner basis one as detailed in [**10**].

We will discuss how to do this and how to compute by "dirty tricks"over a rational function field k; we will discuss in different steps, by increasing weakness of the system:

a) First we assume that k is prime, and that your system while not supporting the algorithms above has a wide choice of orderings for Gröbner basis computation.

Then you can reduce the standard basis computation of $\Im$ to a Gröbner basis computation via homogeneization, as detailed in [**10**]. What you have to do is:

- adjoin a new variable U
- homogeneize w.r.t. U the elements in the input basis of $\Im$, i.e. the h_i and the $f_j - T_j$
- denoting $<$ the ordering on $k[\mathbf{X},\mathbf{T}]$ for which you want to compute the standard basis of $\Im$, define the following ordering $<_h$ on $k[U,\mathbf{X},\mathbf{T}]$ (the actual way of defining it and the set of orderings $<$ you can choose depend of course on the system):

    if m_1, m_2 are power products in $k[\mathbf{X},\mathbf{T}]$, then $U^{e_1}m_1 <_h U^{e_2}m_2$ if and only if either $\deg(U^{e_1}m_1) < \deg(U^{e_2}m_2)$ or $\deg(U^{e_1}m_1) = \deg(U^{e_2}m_2)$ and $m_1 < m_2$

  (here of course deg is the "usual" degree under which you have homogeneized)
- compute a Gröbner basis w.r.t. $<_h$ of the ideal generated by the homogeneizations of the h_i and the $f_j - T_j$ and dehomogeneize the result; what you get is a standard basis of $\Im$ w.r.t. $<$

b) Now we assume that k is a rational function field, and that your system has a wide choice of orderings for Gröbner basis computation. In this case you can reduce to the situation above, by considering your polynomials as elements of $k_0[\mathbf{Z},\mathbf{X},\mathbf{T}]$ and not of $k[\mathbf{X},\mathbf{T}]$, as follows:

- adjoin a new variable U
- homogeneize the elements h_i, $f_j - T_j \in k_0[\mathbf{Z},\mathbf{X},\mathbf{T}]$
- denoting $<$ the ordering on $k[\mathbf{X},\mathbf{T}]$ for which you want to compute the standard basis of $\Im$, choose an ordering $<_Z$ on $k_0[\mathbf{Z}]$ and define the following ordering $<_h$ on $k[U,\mathbf{X},\mathbf{T}]$:

    if m_1, m_2 are power products in $k[\mathbf{X},\mathbf{T}]$, t_1, t_2 are power products in $k_0[\mathbf{Z}]$ then $U^{e_1}t_1m_1 <_h U^{e_2}t_2m_2$ if and only if either $\deg(U^{e_1}t_1m_1) < \deg(U^{e_2}t_2m_2)$ or

$\deg(U^{e_1}t_1m_1) = \deg(U^{e_2}t_2m_2)$ and $m_1 < m_2$ or $\deg(U^{e_1}t_1m_1) = \deg(U^{e_2}t_2m_2)$, $m_1 = m_2$ and $t_1 <_Z t_2$

(this is probably not the optimal ordering to choose, but it is easy to describe)

- compute a Gröbner basis w.r.t. $<_h$ of the ideal generated by the homogeneizations of the h_i and the $f_j - T_j$ and dehomogeneize the result; what you get is still a standard basis of $\Im \subset k[\mathbf{X}, \mathbf{T}]$ w.r.t. $<$
- it has however many redundant elements; you are now interested in the leading power-products only; so extract the leading power-products of the standard basis elements; read them in $k_0(\mathbf{Z})[\mathbf{X}, \mathbf{T}]$, remove the redundant elements and you get a basis for the monomial ideal in $k[\mathbf{X}, \mathbf{T}]$ whose Hilbert function you need to compute.

c) Now we assume that your system supports only a few orderings; this will surely include the *degrevlex* ordering which is defined by:

$m_1 = U_1^{a_1} \cdots U_n^{a_n} < U_1^{b_1} \cdots U_n^{b_n} = m_2$ if and only if either $\deg(m_1) < \deg(m_2)$ or $\deg(m_1) = \deg(m_2)$ and there is j s.t. $a_i = b_i \ \forall i < j$, $a_j > b_j$

Remark that the ordering depends on a ordering $U_1 < \cdots < U_n$ of the variables. What you have to do is

- to adjoin three new homogeneization variables T_0, X_0, Z_0
- transform the polynomials h_i, $f_j - T_j$ so that they are multihomogeneous in

$$\{T_0, T_1, \ldots, T_s\}, \{X_0, X_1, \ldots, X_n\}, \{Z_0, Z_1, \ldots, Z_d\}$$

- compute a Gröbner basis of the ideal generated by the polynomials so obtained w.r.t. the degrevlex ordering induced by

$$T_1 < \cdots < T_s < T_0 < X_0 < X_1 < \cdots < X_n < Z_0 < Z_1 < \cdots < Z_d$$

- dehomogeneizing you get a standard basis of $\Im$
- extract the leading power-products of the standard basis elements; read them in $k_0(\mathbf{Z})[\mathbf{X}, \mathbf{T}]$, remove the redundant elements and you get a basis for the monomial ideal in $k[\mathbf{X}, \mathbf{T}]$ whose Hilbert function you need to compute.

Example (cont.) Let us apply this approach to compute the Graal in our example. After having renamed X_1 to Z_1, but without renumbering X_2, X_3 the homogeneization of the generating system of $\Im$ is:

$$Z_0X_3 - Z_1X_2, Z_0^4X_2^2T_0 - 2Z_1^2Z_0^2X_2X_0T_0 + Z_1^4X_0^2T_0 - Z_0^4X_0^2T_1,$$

$$Z_0^3X_3X_2T_0 - Z_1Z_0^2X_2^2T_0 - Z_1^2Z_0X_3X_0T_0 + Z_1^3X_2X_0T_0 - Z_0^3X_0^2T_2,$$

$$Z_0^3X_2^3T_0 - Z_1Z_0^2X_3X_2X_0T_0 - Z_1^2Z_0X_2^2X_0T_0 + Z_1^3X_3X_0^2T_0 - Z_0^3X_0^3T_3,$$

$$Z_0^2X_3^2T_0 - 2Z_1Z_0X_3X_2T_0 + Z_1^2X_2^2T_0 - Z_0^2X_0^2T_4,$$

$$Z_0^2X_3X_2^2T_0 - Z_1Z_0X_2^3T_0 - Z_1Z_0X_3^2X_0T_0 + Z_1^2X_3X_2X_0T_0 - Z_0^2X_0^3T_5,$$

$$Z_0^2X_2^4T_0 - 2Z_1Z_0X_3X_2^2X_0T_0 + Z_1^2X_3^2X_0^2T_0 - Z_0^2X_0^4T_6$$

A Gröbner basis computation returns the following polynomials

$$Z_0X_3 - Z_1X_2, Z_0^4X_2^2T_0 - 2Z_1^2Z_0^2X_2X_0T_0 + Z_1^4X_0^2T_0 - Z_0^4X_0^2T_1, Z_0^3X_0^2T_2, Z_0^2X_0^2T_4,$$

$$Z_0^2X_0^3T_5, Z_0^3X_0^4T_6 - Z_0^3X_2X_0^3T_3, Z_0^4X_0^3T_3 - Z_0^4X_2X_0^2T_1$$

which give the same standard basis we obtained before [10], and 50 more redundant polynomials [11]

Computing the Hilbert function

Here is the point where dirty tricks don't help anymore; while the modifications to the usual Hilbert function algorithm are easy, they must be done at program level.

References

[1] D. Bayer, M. Stillmann, *Computation of Hilbert Functions*, J. Symb. Comp. **14** (1992), 31–50.

[2] A. Bigatti, M. Caboara, L. Robbiano, *On the computation of Hilbert-Poincaré series*, J. AAECC **2** (1991), 21–33.

[3] A. Bigatti, P. Conti, L. Robbiano, C. Traverso, *A "Divide and Conquer" algorithm for Hilbert-Poincaré series, multiplicity and dimension of monomial ideals*, Proc. AAECC 10, Lect. Notes Comp. Sci. **673** (1993), Springer.

[4] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. Thesis, Innsbruck, (1965).

[5] M.P. Cavaliere, M.E. Rossi, G. Valla, *The strong Castelnuovo Lemma for zero dimensional schemes*, preprint.

[6] D. Eisenbud, J. Harris, *Finite projective schemes in linearly general position*, J. Appl. Geom. 1 (1991), 15–50.

[7] P. Gianni,T.Mora, L. Robbiano, C. Traverso, *Hilbert functions and Buchberger algorithm*, preprint.

[8] J. Hollman, J., *On the computation of the Hilbert series*, Latin 92, Saõ Paulo, Lect. Notes Comp. Sci. **583** (1992), Springer.

[9] M.V. Kondrat'eva, E.V. Pankrat'ev, *A recursive algorithm for the computation of Hilbert polynomial*, EUROCAL 87, Lect. Notes Comp. Sci. **382** (1989), Springer.

---

(10) In fact the degrevlex to $k_0[Z_1, X_2, X_3, T_1, \ldots, T_6]$ is the ordering we used before, so that you could check the result.

(11) There is in fact a price to pay for this roundabout computation; remark that the computation with CoCoA 1.5 took 13.35 secs., so approx. 90 times more than the direct computation by the Tangent Cone Algorithm

[10] D. Lazard, *Gröbner bases, Gaussian elimination and resolution of systems of polynomial equations*, EUROCAL 83, Lect. Notes. Comp. Sci. **162** (1983), Springer, 146–156.

[11] H.M. Möller, T. Mora, *The computation of the Hilbert function*, Proc.EUROCAL 83, Lect. Notes Comp. Sci. **162** (1983), Springer, 157–167

[12] H.M. Möller, T. Mora, *Computational aspects of reduction strategies to construct resolutions of monomial ideals*, AAECC2, Lect. Notes Comp. Sci. **228** (1986), Springer.

[13] T. Mora, G. Pfister, C. Traverso, *An introduction to the tangent cone algorithm*, in C. Hoffmann ed. *Issues in robotics and non-linear geometry*, JAI Press, Greenwich, Conn. (1992), 199–270.

[14] T. Mora, *La Queste del Saint Graal: a computational approach to local algebra*, Discrete Applied Math. **33** (1991), 161–190.

[15] J. Sally, *Hilbert coefficients and reduction number 2*, J. Alg. Geo. and Sing. **1** (1992), 325–333.

[16] J. Sally, *Ideals whose Hilbert function and Hilbert polynomial agree at n=1* , **157** (1993), 534–547.

[17] W. Spangher, *On the computation of Hilbert-Samuel series and multiplicity*, AAECC6, Lect. Notes Comp. Sci. **356** (1989), Springer, 407–414.