

# Computing syzygies with Gröbner bases

Steven V Sam

July 2, 2008

## 1 Motivation.

The aim of this article is to motivate the inclusion of Gröbner bases in algebraic geometry via the computation of syzygies. In particular, we will discuss Gröbner bases for finite modules over polynomial rings, and mention how this tool can be used to compute minimal free resolutions of graded finite modules. We won't prove any results. Instead, we refer the reader to the references at the end for proofs.

This article was written as a final project for the program on computational algebraic geometry at the University of Utah during June 16 to July 3, 2008.

We begin with an example from [BM].

### 1.1 The example of the twisted cubic in $\mathbf{P}^3$ .

We work in projective space  $\mathbf{P}^3$  over a field  $k$ , and let  $S = k[w, x, y, z]$  be the homogeneous coordinate ring of  $\mathbf{P}^3$ . Define polynomials  $f_1 = w^2 - xy$ ,  $f_2 = wy - xz$ , and  $f_3 = wz - y^2$ ; the homogeneous ideal  $I = (f_1, f_2, f_3)$  defines a twisted cubic curve  $X \subset \mathbf{P}^3$ . Note also that  $X$  has a parameterization  $(r, s) \mapsto (r^2s, r^3, rs^2, s^3)$ . We would somehow like to be able to deform  $I$  to some monomial ideal  $J$ , motivated by the fact that computations are much easier to perform for monomial ideals, and with the hopes that such computations could be used to obtain information about our original ideal  $I$ .

We define an action of  $k^\times$  on the monomials of  $S$  of degree  $< 4$  by

$$t \cdot w^a x^b y^c z^d = t^{-(16a+4b+c)} w^a x^b y^c z^d.$$

On a polynomial  $p$  with degree  $< 4$ , we get an operation by having  $k^\times$  act on the monomials of  $p$ , and then “clear denominators” for  $t$ . In our case, this means the following:

$$f_1 \mapsto w^2 - t^{27}xy =: g_1, \quad f_2 \mapsto wy - t^{13}xz =: g_2, \quad f_3 \mapsto wz - t^{14}y^2 =: g_3.$$

If we evaluate these polynomials at  $t = 0$ , we end up with monomials. This will in general happen: what we are really doing is picking out the “biggest” monomial of our polynomial under the lexicographic ordering given by  $w > x > y > z$ . Motivated by this, we will call the above operation in, and write  $\text{in}(p)$  for the largest monomial of  $p$ .

Now comes the next point: what sorts of information can be extracted from the monomial ideal  $(\text{in}(f_1), \text{in}(f_2), \text{in}(f_3)) = (w^2, wy, wz)$ ? First, let us examine the geometry of this process. First, define  $I_t = (w^2 - t^{27}xy, wy - t^{13}xz, wz - t^{14}y^2)$ . The map  $k[t] \rightarrow S[t]/I_t$  defines a map  $\varphi: X_t \rightarrow \mathbf{A}^1$  where  $X_t = \text{Proj } S[t]/I_t$  is the closed subscheme of  $\mathbf{P}^4$  defined by  $I_t$ . The preimage of 1 under  $\varphi$  is our original twisted cubic curve  $X_1 = X$ , and the preimage of  $s \neq 0$  under  $\varphi$  is a curve  $X_s$  isomorphic to  $X$ . We are interested in the structure of  $X_0$ , which should correspond to a monomial ideal. One first guess might be that  $X_0$  is defined by the ideal  $(w^2, wy, wz)$ , but this will turn out to be wrong.

## 1.2 Flat families.

To understand the picture better, we recall that a **family of schemes** is the fibers of a morphism  $f: X \rightarrow Y$ , and that we call the family **flat** if  $f$  is a flat morphism. One of the key points of flat morphisms is the following characterization:

**Theorem 1** ([Har, III.9.9]). *Let  $T$  be an integral Noetherian scheme, and  $X \subseteq \mathbf{P}_T^n$  a closed subscheme. For each  $t \in T$ , let  $P_t$  be the Hilbert polynomial of the fiber  $X_t = X \times_T \text{Spec } k(t)$  when considered as a closed subscheme of  $\mathbf{P}_{k(t)}^n$ , where  $k(t) = \mathcal{O}_{T,t}/\mathfrak{m}_{T,t}$  denotes the residue field of  $t \in T$ . Then  $X$  is flat over  $T$  if and only if  $P_t$  is independent of  $t$ .*

In our example, we take  $T = \mathbf{A}^1$ , and consider  $X$  as a closed subscheme of  $\mathbf{P}_T^4 = \mathbf{P}_k^4 \times_{\text{Spec } k} \mathbf{A}_k^1$ . Evaluating  $t = s$ , the Hilbert polynomial of  $S/I_s$  is  $P(d) = 3d + 1$  for  $s \neq 0$ . But the Hilbert polynomial of  $S/(w^2, wy, wz)$  is  $z^2 + \frac{3}{2}z + 2$ , which is not even of the same degree. This should come as no surprise: the ideal  $(w^2, wy, wz)$  defines a closed subscheme of dimension 2.

As we shall explain in the next section, the main issue here is that with respect to our ordering  $w > x > y > z$ , the set  $\{f_1, f_2, f_3\}$  is not a Gröbner basis of  $I$ . It turns out that the ideal that cuts out  $X_0$  is  $(w^2, wy, wz, xz^2)$ .

## 2 Gröbner Bases.

### 2.1 More of the twisted cubic curve.

We will continue our discussion of the twisted cubic curve  $X$  of the previous section here and examine what might be going wrong. Consider the monomials  $m_1 = w^2$ ,  $m_2 = wy$ ,  $m_3 = wz$ . The module of syzygies, or relations, on the  $m_i$  are generated by

$$\begin{aligned} ym_1 - wm_2 &= 0 \\ zm_1 - wm_3 &= 0 \\ zm_2 - ym_3 &= 0. \end{aligned}$$

If we substitute  $g_i$  for  $m_i$ , we see that

$$yg_1 - wg_2 = t^{13}xg_3,$$

and

$$zg_1 - wg_3 = t^{14}yg_2,$$

are lifts to syzygies of the  $g_i$ , but

$$zg_2 - yg_3 = -t^{13}xz^2 + t^{14}y^3,$$

and the right-hand side is not generated by the  $g_i$ , so does not lift to a syzygy. The solution is to throw in  $g_4 = xz^2 + ty^3$ , which is in the ideal  $(g_1, g_2, g_3)$ , but now when we repeat the process with the new set of (redundant) generators, all of the pairwise syzygies of the leading monomials will lift to syzygies of the  $g_i$ . This also explains why the special fiber  $X_0$  of the previous section needed more generators.

## 2.2 Gröbner bases for modules.

All of the following information and more can be found in [Eis95, Chapter 15]. First, some notation. When we write  $x^a$ , this will be shorthand for the monomial  $x_1^{a_1} \cdots x_n^{a_n}$ . Let  $F$  be a finite free  $S$ -module with basis  $\{e_1, \dots, e_r\}$ . A **monomial** in  $F$  is an element of the form  $m = x^a e_i$  for some  $i$ , and a **term** is an element of the form  $cx^a e_i$  for  $c \in k$ . A **monomial submodule** is one generated by monomials. We can recover our original notion of monomials by taking  $F = S$  and  $\{e_i\} = \{1\}$ . If  $m$  and  $n$  are monomials of  $S$ , we say that a term  $cm e_i$  **divides**  $dne_j$  if  $i = j$  and  $m$  divides  $n$  in the usual sense, and define the **quotient**  $cm e_i / dne_j$  to be  $cm/dn \in S$ .

A **monomial order** on  $F$  is a total order  $>$  on the monomials of  $F$  such that if  $m_1, m_2$  are monomials of  $F$  and  $n$  is a monomial of  $S$  of positive degree, then  $m_1 > m_2$  implies that  $nm_1 > nm_2 > m_2$ . For terms,  $cm_1 > dm_2$  if  $m_1 > m_2$  (this is just notation and does not define an ordering). Given a monomial order  $>$  on  $F$ , and  $f \in F$ , we will define  $\text{in}_>(f)$  (the **initial term** of  $f$ ) to be the largest term of  $f$ . If  $M$  is a submodule of  $F$ , we will write  $\text{in}_>(M)$  to be the submodule generated by  $\{\text{in}_>(f) \mid f \in M\}$ . Also, if  $\{g_1, \dots, g_t\}$  is a generating set for  $M$  such that  $\{\text{in}_>(g_1), \dots, \text{in}_>(g_t)\}$  generates  $\text{in}_>(M)$ , then we will call  $\{g_1, \dots, g_t\}$  a **Gröbner basis** with respect to  $>$ .

## 2.3 A division algorithm.

Now we describe an algorithm which will be a fundamental step in computing a Gröbner basis of a submodule. As usual, let  $S = k[x_1, \dots, x_n]$  and let  $F$  be a free finite  $S$ -module with basis  $\{e_i\}$ , and some monomial order  $>$ .

Pick  $f, g_1, \dots, g_t \in F$ . Our goal is to develop a standard form

$$f = \sum m_u g_{s_u} + f'$$

for  $f$  with respect to  $g_1, \dots, g_t$ . We do so by induction. Suppose that the indices  $s_1, \dots, s_p$  and  $m_1, \dots, m_p$  have been chosen. Set

$$f'_p := f - \sum_{u=1}^p m_u g_{s_u}.$$

If  $f'_p \neq 0$ , and  $m$  is the maximal term of  $f'_p$  with respect to  $>$  which is divisible by some  $\text{in}_>(g_i)$ , then suppose that  $i$  is minimal with respect to this property, and set

$$\begin{aligned} s_{p+1} &:= i, \\ m_{p+1} &:= m / \text{in}_>(g_i). \end{aligned}$$

We repeat this process as long as  $f'_p \neq 0$  and some  $\text{in}_>(g_i)$  divides a monomial of  $f'_p$ . The element  $f'$  is the last  $f'_p$  produced from this algorithm.

This algorithm terminates in a finite amount of time because at each step, the maximal term of  $f'_p$  divisible by some  $\text{in}_>(g_i)$  decreases at each step, and one can show that monomial orders are well-orderings.

## 2.4 Buchberger's criterion and algorithm.

Now we will show how one can use the division algorithm to compute a Gröbner basis of a module. We first define some notation that will be used for the rest of the section.

Let  $F$  be a free module over  $S$  with basis  $\{e_1, \dots, e_r\}$  and let  $>$  be a monomial order on  $F$ . Pick nonzero elements  $g_1, \dots, g_t$  of  $F$ . Let  $\bigoplus S\varepsilon_i$  be a free module with basis  $\{\varepsilon_1, \dots, \varepsilon_t\}$  corresponding to the elements  $g_1, \dots, g_t$ , and define a map

$$\varphi: \bigoplus S\varepsilon_i \rightarrow F, \quad \varepsilon_i \mapsto g_i.$$

If  $\text{in}_>(g_i)$  and  $\text{in}_>(g_j)$  involve the same basis element of  $F$ , i.e.,  $\text{in}_>(g_i) = x^a e_\ell$  and  $\text{in}_>(g_j) = x^b e_\ell$  for some  $\ell$ , then define

$$m_{ij} := \text{in}_>(g_i) / \gcd(\text{in}_>(g_i), \text{in}_>(g_j))$$

where  $\gcd$  denotes the largest term which divides both  $\text{in}_>(g_i)$  and  $\text{in}_>(g_j)$ . Also define

$$\sigma_{ij} := m_{ji}\varepsilon_i - m_{ij}\varepsilon_j.$$

Using the division algorithm, we have standard expressions

$$m_{ji}g_i - m_{ij}g_j = \sum f_u^{(ij)} g_u + h_{ij}$$

for  $m_{ji}g_i - m_{ij}g_j$  with respect to  $g_1, \dots, g_t$ . If  $\text{in}_>(g_i)$  and  $\text{in}_>(g_j)$  do not involve the same basis element of  $F$ , then define  $h_{ij} = 0$  in this case.

The important theorem is the following:

**Theorem 2** (Buchberger's criterion). *The elements  $g_1, \dots, g_t$  form a Gröbner basis if and only if  $h_{ij} = 0$  for all  $i$  and  $j$ .*

For a proof, see [Eis95, Theorem 15.8].

This gives a nice algorithm for computing a Gröbner basis of a submodule  $M$  of  $F$ . Namely, suppose we are given a set of generators  $\{g_1, \dots, g_t\}$  of  $M$ . Then we compute the  $h_{ij}$  as above. If they are all 0, then Theorem 2 says that  $\{g_1, \dots, g_t\}$  is a Gröbner basis. Otherwise, pick some  $h_{ij} \neq 0$ , and repeat the process with the set of generators  $\{g_1, \dots, g_t, h_{ij}\}$ . This process is guaranteed to terminate because it generates a strictly increasing chain of submodules consisting of initial terms.

## 2.5 Computing syzygies.

It turns out that Buchberger's algorithm provides more data than meets the eye. Using the notation from the previous section, let  $\{g_1, \dots, g_t\}$  be a Gröbner basis of  $M$ . Then set

$$\tau_{ij} := m_{ji}\varepsilon_i - m_{ij}\varepsilon_j - \sum_u f_u^{(ij)} \varepsilon_u.$$

By Theorem 2 we know that  $\varphi(\tau_{ij}) = 0$ . We will define a monomial order  $>'$  on  $\bigoplus_{j=1}^t S\varepsilon_j$  by setting  $m\varepsilon_u >' n\varepsilon_v$  if and only if

1.  $\text{in}_>(mg_u) > \text{in}_>(ng_v)$  with respect to the ordering  $>$  on  $F$ , or
2.  $\text{in}_>(mg_u) = \text{in}_>(ng_v)$  (up to a scalar multiple) and  $u < v$ .

The next theorem allows us to compute syzygies of modules:

**Theorem 3** (Schreyer [Sch]). *With the notation above, the  $\tau_{ij}$  are a Gröbner basis for  $\bigoplus_{j=1}^t S\varepsilon_j$  with respect to the ordering  $>'$ .*

For a proof, see [Eis95, Theorem 15.10].

### 3 Application to Minimal Free Resolutions.

We end with an application to the computation of minimal free resolutions of finite graded  $S$ -modules. First, we define what a minimal free resolution is. Let  $(\mathbf{F}, \mathbf{d})$  be a complex

$$\mathbf{F} : \dots \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \xrightarrow{d_{i-1}} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \longrightarrow 0.$$

We say that  $(\mathbf{F}, \mathbf{d})$  is a **resolution** of  $F_0$  if  $\text{image } d_{i+1} = \ker d_i$  for all  $i$ , and  $(\mathbf{F}, \mathbf{d})$  is a **free resolution** if each  $F_i$  is a free  $S$ -module. A free resolution is **minimal** if for each  $i$ , a basis of  $F_{i-1}$  maps onto a minimal set of generators for  $\text{coker } d_i$  under the quotient map.

The case of interest is when  $F_0$  is a graded module. In this case, we are concerned with graded resolutions. This means simply that each  $d_i$  is a degree 0 map. Note that a degree  $a$  map  $M \rightarrow N$  can always be made a degree 0 map by replacing  $M$  with  $M(-a)$ , where  $M(-a)$  is defined by  $M(-a)_i = M_{i-a}$  for all  $d$  (here the subscript refers to the graded part with that degree). The following theorem states that graded minimal free resolutions are unique up to isomorphism.

**Theorem 4.** *Let  $M$  a finite graded  $S$ -module. If  $\mathbf{F}$  and  $\mathbf{G}$  are minimal graded free resolutions of  $M$ , then there exists a graded isomorphism of complexes  $\mathbf{F} \rightarrow \mathbf{G}$  which is the identity map on  $M$ .*

Another useful fact is that minimal resolutions have finite length. Define the **length** of a resolution  $(\mathbf{F}, \mathbf{d})$  to be the largest  $i$  such that  $F_i \neq 0$  but  $F_{i+1} = 0$ .

**Theorem 5** (Hilbert syzygy theorem). *Let  $M$  a finite graded  $S$ -module. Then there exists a graded free resolution of  $M$  consisting of finite  $S$ -modules of length at most  $n$ .*

Proofs of the above two theorems can be found in [Eis95, Theorem 20.2] and [Eis95, Corollary 19.7], respectively.

Combining all of the above, we now have an algorithm for computing the minimal free resolution of a finite  $S$ -module  $M$ . Suppose we are given a set of generators and relations for  $M$ . The first step is to find a minimal generating set  $\{g_1, \dots, g_t\}$  for  $M$  with relations  $\{r_1, \dots, r_s\}$ . Then we define  $F_1 = \bigoplus_{i=1}^t S\varepsilon_i(-a_i)$ , where  $\deg g_i = a_i$ , and  $d_1: F_1 \rightarrow M$  by  $\varepsilon_i \mapsto g_i$ . Since we know the generators, we have a generating set  $\{g'_1, \dots, g'_{t'}\}$  for the kernel of  $d_1$ . We then set  $F_2 = \bigoplus_{i=1}^{t'} S\varepsilon'_i(-a'_i)$ , where  $\deg g'_i = a'_i$ , and define  $d_2: F_2 \rightarrow F_1$  by  $\varepsilon'_i \mapsto g'_i$ . Theorem 3 then gives a method of computing a generating set for  $\ker d_2$  by computing a Gröbner basis for  $\ker d_1$  (which we can do for submodules of free modules). We can then define  $F_3$ , etc. We continue in this way until eventually  $\ker d_i = 0$  for some  $i$ , which is guaranteed by Theorem 5. The resulting resolution will be minimal because we chose minimal generating sets at each step.

### 4 Further Comments.

As mentioned earlier, much more reading on Gröbner bases can be found in [Eis95, Chapter 15] along with some programming projects and future directions.

An implementation of Gröbner bases and computation of minimal free resolutions of  $S$ -modules can be found in the program Macaulay 2 [M2]. A more thorough discussion of syzygies and their connections with algebraic geometry can be found in the book [Eis05].

Improvements to the algorithm presented above for computing the minimal free resolution of a graded module can be found in [LSS].

The minimal free resolution  $(\mathbf{F}, \mathbf{d})$  of a finite graded  $S$ -module  $M$  has an associated **Betti table**  $(\beta_{ij})$ , where  $\beta_{ij}$  is defined as the number of generators of degree  $i$  in  $F_j$ . From Theorem 4, we know that these numbers are an invariant of  $M$ . The papers [ES] and [BS] make great progress toward a classification of the possible tables  $(\beta_{ij})$  that can arise from a module.

## References

- [BM] Dave Bayer and David Mumford, What Can Be Computed in Algebraic Geometry?, *Computational algebraic geometry and commutative algebra* (Cortona, 1991), 1–48 Sympos. Math., XXXIV, Cambridge Univ. Press, Cambridge, 1993.
- [BS] Mats Boij and Jonas Söderberg, Betti numbers of graded modules and the multiplicity conjecture in the non-Cohen–Macaulay case, preprint, [arXiv:0803.1645](https://arxiv.org/abs/0803.1645).
- [Eis95] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Math. **150**, Springer–Verlag, New York, 1995.
- [Eis05] David Eisenbud, *The Geometry of Syzygies: A Second Course in Algebraic Geometry and Commutative Algebra*, Graduate Texts in Math. **229**, Springer–Verlag, New York, 2005.
- [ES] David Eisenbud and Frank-Olaf Schreyer, Betti numbers of graded modules and cohomology of vector bundles, to appear in *J. Amer. Math. Soc.*, [arXiv:0712.1843](https://arxiv.org/abs/0712.1843).
- [M2] Daniel R. Grayson and Michael E. Stillman, *Macaulay 2, a software system for research in algebraic geometry*, available at <http://www.math.uiuc.edu/Macaulay2/>.
- [Har] Robin Hartshorne, *Algebraic Geometry*, Graduate Texts in Math. **52**, Springer–Verlag, New York, 1977.
- [LSS] Ricardo La Scala and Michael Stillman, Strategies for computing minimal free resolutions, *J. Symbolic Computation*, vol. 26, issue 4, (1998), 409–431.
- [Sch] Frank-Olaf Schreyer, *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass’schen Divisionssatz*. Diplom Thesis, University of Hamburg, Germany.

Steven V Sam  
Department of Mathematics  
Massachusetts Institute of Technology  
Cambridge, MA 02139  
[ssam@math.mit.edu](mailto:ssam@math.mit.edu)  
<http://math.mit.edu/~ssam/>