Computational Algebra

11. Further directions

In this course, we studied the theory of Gröbner bases for ideals in polynomial rings. There are a number of ways in which the theory can be extended, leading to new applications.

(A) Gröbner bases for modules over polynomial rings.

(Computational Commutative Algebra 1 by Kreuzer and Robbiano)

Modules are to rings what vector spaces are to fields: if in the definition of a vector space we substitute the field of scalars with an arbitrary ring, we obtain the notion of a module. Ideals are a special case of modules over a ring, so one may wonder whether the theory of Gröbner bases can be extended to modules over a polynomial ring. One archetipical example is $(k[\underline{x}])^r$, whose elements are r-tuples of polynomials: for example,

$$\begin{pmatrix} 3x^2 + 2y \\ -x + 7xy \end{pmatrix} \in \left(k[x,y]\right)^2$$

If we denote by $e_1, \dots, e_r$ the standard basis of $(k[\underline{x}])^r$:

$$e_i := (0, \dots, 0, \overset{(i)}{1}, 0, \dots, 0)$$

then we define <u>terms</u> in $(k[\underline{x}])^r$ those elements of the form

$$t \cdot e_i \quad , \quad t \in \mathbb{T}$$

Every element in $(k[\underline{x}])^r$ can then decomposed as a sum of terms

$$\begin{pmatrix} 3x^2 + 2y \\ -x + 7xy \end{pmatrix} = 3x^2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 2y \begin{pmatrix} 1 \\ 0 \end{pmatrix} + (-1)x \begin{pmatrix} 0 \\ 1 \end{pmatrix} + 7xy \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Now, once we are given a term order $\leq$ on $\mathbb{T}$, we can extend it to an order on the terms of $(k[\underline{x}])^r$. We do so, so that

i. $s \cdot e_i \leq t \cdot e_j$ implies $(u \cdot s)\, e_i \leq (u \cdot t)\, e_j$

for all $s, t, u \in \mathbb{T}$

ii. $s \leq t$ and $i \leq j$ implies $s e_i \leq t e_j$

for all $s, t \in \mathbb{T}$.

Two possible ways to obtain an order on the terms of $(k[\underline{x}])^r$ starting from a term order on $\mathbb{T}$ are the so-called <u>position-over-</u>

term (POT) and the term-over-position orders:

POT: $s\cdot e_i \leq^{pot} t\cdot e_j \iff i<j$ or ($i=j$ and $s\leq t$)

TOP: $s\cdot e_i \leq^{top} t\cdot e_j \iff s<t$ or ($s=t$ and $i<j$)

Now, analogously as in the ideal setting, we can define leading terms, leading coefficients, and so reductions and S-polynomials. By extending carefilly these notions, one obtains the the module-analogue of Buchberger's Algorithm always terminates and provides a Gröbner basis in the module setting.

(B) Syzygies and homological algebra.

One of the most important modules that we can compute is the so-called syzygy module: given polynomials $f_1, \dots, f_r \in k[\underline{x}]$, a syzygy is a tuple $(g_1, \dots, g_r) \in (k[\underline{x}])^r$ such that

$$g_1 f_1 + \dots + g_r f_r = 0$$

Hence a syzygy is a generalization of a linear relation, which allows polynomial coefficients. One easily sees that syzygies form a submodule of $(k[\underline{x}])^r$ and that they are the kernel of the map

$$\begin{aligned} (k[\underline{x}])^r &\longrightarrow k[\underline{x}] \\ e_i &\longmapsto f_i \end{aligned}$$

which is a linear map of $k[\underline{x}]$-modules. The notion of syzygy can then defined starting from any finite set of module elements (if $m_1, \dots, m_s \in (k[\underline{x}])^r$, then a syzygy of $m_1, \dots, m_s$ is an element $(n_1, \dots, n_s) \in (k[\underline{x}])^s$ such that $n_1 m_1 + \dots + n_s m_s = 0$). The key result, from a computational point of view, is that an algorithm by Schreyer provides a Gröbner basis for the module of syzygies. This, then, allows one to compute, for example a so-called *finite free resolution* of an ideal, namely a sequence of maps

$$0 \longrightarrow F_m \xrightarrow{\varphi_m} F_{m-1} \xrightarrow{\varphi_{m-1}} \dots \longrightarrow F_1 \xrightarrow{\varphi_1} k[\underline{x}] \longrightarrow 0$$

where the image of φ_1 is the given ideal, and

$$\operatorname{im}(\varphi_i) = \ker(\varphi_{i-1}) \quad \forall i$$

Being able to determine such an object allows one to determine several properties of the ideal. Moreover, this opens the way to the computation of the Hom-modules, (modules of homomorphisms between modules), the Tor-modules, the Ext-modules, namely to the computation of homological quantities related to the ideal we started with.

(c) The F_5 algorithm.

The notion of syzygy plays a prominent role in the theory of Gröbner bases. In fact, it is possible to phrase the condition of being a Gröbner basis in terms of a special relation that has to hold between the modules of syzygies of the candidate Gröbner basis and of syzygies of the leading term ideal (namely, the condition is that every syzygy of the leading term ideal can be "lifted" to a syzygy of the candidate Gröbner basis). From this, it is rather easy to prove the correctness of Buchberger's Algorithm.

There is also another way how syzygies enter the theory of Gröbner bases and it is the fact that via the analysis of some simple syzygies of a tuple of polynomials we are able to understand beforehand when some S-polynomial will reduce to zero. From this observation, the algorithm F_5 by Faugere attaches a "signature" to the polynomials that should be reduced during the computation of a Gröbner basis, predicting which ones will reduce to zero and hence saving us from performing a useless reduction. This, unfortunately, does not always happen, but it happens often enough, namely for the following kind of input polynomials.

Def: a tuple $(r_1, \dots, r_s)$ of elements of a commutative ring R is called a regular sequence if r_1 is not a zero-divisor of R, $[r_2]$ is not a zero-divisor of $R/(r_1)$, $[r_3]$ is not a zero-divisor of $R/(r_1, r_2)$, and so on.

The result is that the algorithm F_5 avoids the computation of all useless zero reductions (i.e., predicts when an S-polynomial will reduce to zero before computing the reduction) when the input tuple of polynomials is a regular sequence.

(D) Hilbert functions.

Given a homogeneous ideal $I \subseteq k[\underline{x}]$, i.e., an ideal generated by homogeneous polynomials, we can define, for $d \in \mathbb{N}$,

$$I_d := \{\text{homogeneous polynomials of degree } d \text{ in } I\} \cup \{0\}$$

One then notices that, although I is infinite-dimensional as a k-vector space each I_d has finite dimension over k. Hence, one way to study the global information about I is to consider the function:

$$HF_I : \mathbb{N} \longrightarrow \mathbb{N}, \quad d \longmapsto \dim_k {}^{k[\underline{x}]_d}\!/\!_{I_d}$$

This function is called the <u>Hilbert function</u> of I.

The first important result about the Hilbert function is that it is eventually polynomial, namely there exists a polynomial

$HP_I \in \mathbb{Q}[t]$ such that there exists $\bar{d} \in \mathbb{N}$ with

$$HF_I(d) = HP_I(d) \quad \text{for all } d \geq \bar{d}$$

The polynomial HP_I is called the Hilbert polynomial of I, and it conveys several properties of the ideal. For example, if X is the projective variety determined by I (better: the projective scheme), then HP_I encodes the dimension of X (in the degree of HP_I), the degree of X (in the leading coefficient of HP_I), and the arithmetic genus of X (in the constant coefficient of HP_I). When the ideal I comes, instead, from a combinatorial origin (e.g., it is the Stanley-Reisner ideal of a simplicial complex), then the Hilbert function and polynomial encode combinatorial properties, too. Instead of dealing with infinitely many values of a function, we can "pack" them into a single object, namely, a formal power series; in this way we obtain the so-called Hilbert series.

$$HS_I := \sum_{d \in \mathbb{N}} HF_I(d) \cdot z^d$$

Once considered as a series, this piece of information can be maniputed sometimes in an easier way.

The main algorithmic result about Hilbert functions/polynomial/series is that the Hilbert function of a homogeneous ideal is equal to the Hilbert function of its leading term ideal, as long as we consider a term order that refines the total degree of monomials (for example DegLex or DegRevLex).

Example: consider the ideal

$$I = (-x^2 - yz + z^2, x^2 - yz - z^2) \subseteq \mathbb{Q}[x,y,z]$$

this ideal is the ideal encoding the intersection of two conics in projective space; we can write

$$I = (x^2 - yz - z^2, yz) = (x^2 - z^2, yz)$$

from Buchberger's criterion, we see that the latter two generators form a Gröbner basis of I with respect to DegLex; we hence have $LT_{DegLex}(I) = (x^2, yz)$

therefore $HF_I = HF_{(x^2, yz)}$

let us start computing the latter Hilbert function:

$$HF_{(x^2, yz)}(0) = \dim_{\mathbb{Q}} \mathbb{Q}[x,y,z]_0 / I_0 = 1$$

$$\dim_{\mathbb{Q}} \mathbb{Q}[x,y,z]_1 / I_1 = \dim_{\mathbb{Q}} \langle x,y,z\rangle / (0) = 3$$

$$\dim_{\mathbb{Q}} \mathbb{Q}[x,y,z]_2 / I_2 = \dim_{\mathbb{Q}} \langle x^2, y^2, z^2, xy, yz, xz\rangle / \langle x^2, yz\rangle = 4$$

$$\dim_{\mathbb{Q}} \mathbb{Q}[x,y,z]_3 / I_3 = ?$$

$$\mathbb{Q}[x,y,z]_3 = \langle x^3, y^3, z^3, x^2y, x^2z, xy^2, y^2z, xz^2, yz^2, xyz\rangle$$

$$I_3 = \langle x^3, x^2y, x^2z, xyz, y^2z, yz^2\rangle$$

hence $\dim_{\mathbb{Q}} \mathbb{Q}[x,y,z]_3 / I_3 = 4$ and one can see that from now on the Hilbert function will have the constant value 4; this encodes the fact that the two conics intersect in 4 points, which in turn is the degree of the ideal I; we see how the use of leading terms transforms the computation of the Hilbert function from an algebraic problem to a combinatorial one.

Hilbert functions are also related to finite free resolutions as briefly introduced before, since the Hilbert function can be "read" from a free resolution, however the latter has to be of a special kind in terms of the graded structure, namely it has to be a *graded free resolution*.

(E) Gröbner basis in a non-commutative setting.

It is possible to set up a similar theory to the one of Gröbner bases we studied in our course, that applies to non-commutative algebras. This comes with a cost, namely Buchberger's algorithm will not extend to an algorithm that always terminates.

The setting is the following: we start from a semigroup S with a well-ordering $\leq$ that is a semigroup ordering, i.e., such that

$$t_1 < t_2 \quad \text{implies} \quad l t_1 r < l t_2 r \quad \text{for all } l, r, t_1, t_2 \in S$$

Then we form the semigroup ring $k\langle S\rangle$ (which, as a k-vector space has S as basis, and the multiplication is obtained by extending by linearity the multiplication in S). The semigroup $\mathbb{N}^n$, for example, determines the semigroup ring $k[x_1, \dots, x_n]$ of usual polynomials; if for S we take the semigroup of words over a finite alphabeth of n letters (where multiplication is concatenation of words), then $k\langle S\rangle$ is the ring of non-commutative polynomials over those letters which is usually denoted $k\langle x_1, \dots, x_n\rangle$. The well-order on S allows one to write any element in $k\langle S\rangle$ as a unique ordered representation as a linear combination of elements of S:

$$f = \sum_{i=1}^{s} c_i t_i \quad \text{where } c_i \in k\setminus\{0\},\ t_i \in S$$
$$\text{and } t_1 > t_2 > \dots > t_s$$

In this way we can associate to f a leading term and a leading coefficient, as we did in the commutative case. Notice, for example, that if we consider S the free semigroup generated by n letters, i.e., the semigroup of words, then we can consider as in the commutative case the degrexlex order, where the "degree" of a word is given by the number of letters composing it. (with repetitions).

Now one can start defining the non-commutative analogues of leading term ideals and canonical forms for a two-sided ideal $I \subseteq k\langle S\rangle$. In this way one obtains the analogues of the notion of Gröbner bases, which allow one to decide whether an element in $k\langle S\rangle$ belongs to a given two-sided ideal. Here is now where the theory departs from the one in the commutative case since we face the problem of the undecidability of the word problem for the free non-commutative semigroup on n letters.