Gröbner bases, formal languages, and applications

Steven Sam

University of California, Berkeley

September 20, 2014

See also: "Directions in Commutative Algebra: Past, Present, Future II", 4:30pm - 5:15pm

Theme of the talk:

- Reduction of algebraic problems to combinatorial problems
- Combinatorial tools: Gröbner bases and formal languages

Examples:

- **Hilbert basis theorem** (Let $\mathbf{k}$ be a field. Every ideal in $A = \mathbf{k}[x_1, \ldots, x_n]$ is finitely generated.)
  follows from
  Dixon's lemma (The poset $\mathbf{Z}^n_{\geq 0}$ under termwise comparison contains no infinite antichains.)
- "Finitely generated A-modules have rational Hilbert series"
  follows from
  "Every regular language has a rational generating function"
  (A stronger statement can be made in this case, but let's minimize technicalities)

Let's sketch this now...

A **term order** is an ordering of monomials in $\mathbf{k}[x_1, \ldots, x_n]$ so that

- no infinite descending chains
- $m < m'$ implies $nm < nm'$

For $f \in \mathbf{k}[x_1, \ldots, x_n]$ define $\mathrm{init}(f)$ to be its maximal monomial and for an ideal I, let $\mathrm{init}(I)$ be the $\mathbf{k}$-span of $\mathrm{init}(f)$ for $f \in I$.

Basic properties:

- A generating set for $\mathrm{init}(I)$ gives one for I
- For I homogeneous, I and $\mathrm{init}(I)$ have same Hilbert series

So we have reduced problem to monomial ideals

- If I is a monomial ideal with infinite generating set $m_1, m_2, \dots$ so that no m_i divides any other m_j, then their exponents would be an infinite antichain in $\mathbf{Z}^n_{\geq 0}$; now use Dixon's lemma
- A degree d monomial in n variables can be encoded as a sequence of "stars and bars" with $n-1$ "bars" and d "stars", e.g., $x_2^3 x_3^2 x_5 \leftrightarrow | * * * | * * || *$
  This is a regular language on the alphabet $\{*, |\}$, i.e., can be encoded as the set of walks in a weighted graph, so has a rational generating function

Want to apply this strategy to other algebraic structures to get analogues of Hilbert basis theorem and rationality of Hilbert series.

The modules $M = \bigoplus_{i \geq 0} M_i$ will be $\mathbf{Z}_{\geq 0}$-graded vector spaces together with collections of operations $M_i \to M_j$ which may depend on i and j.

So there is an intuitive notion of submodules, finite generation, and Hilbert series.

This is most cleanly packaged as follows: $\mathcal{C}$ is a category whose isomorphism classes are given by nonnegative integers and M is a functor from $\mathcal{C}$ to $\mathbf{k}$-vector spaces. Then M_i will be the value of M evaluated on the isoclass corresponding to i.

Call them $\mathcal{C}$-**modules**.

Some examples:

- $\mathcal{C} = \mathbf{FI}$ is the category of finite sets and injective maps. So there is one operation $M_i \to M_j$ for each injection $[i] \to [j]$.
- $\mathcal{C} = \mathbf{FS}^{\mathrm{op}}$ is the *opposite* of the category of finite sets and surjective maps. So there is one operation $M_i \to M_j$ for each surjection $[j] \to [i]$.
- $\mathcal{C} = \mathbf{VI}(\mathbf{F}_q)$ is the category of finite-dimensional $\mathbf{F}_q$-vector spaces and injective linear maps. So there is one operation $M_i \to M_j$ for each injection $\mathbf{F}_q^i \to \mathbf{F}_q^j$.
- G-sets, weighted sets, colored injections, symplectic vector spaces, etc.

All of these can be analyzed with generalizations of Gröbner bases using the strategy we just outlined.

For each i, there is a "free" $\mathcal{C}$-module $P(i)$ with

$$P(i)_j = \mathbf{k}[\mathrm{Hom}_{\mathcal{C}}(i,j)].$$

Intuitively, $P(i)_j$ is the set of all operations that get you from M_i to M_j, so for any choice of element $x \in M_i$ one can define a map $P(i) \to M$.

These spaces have distinguished bases, which we should think of as monomials.

(Technically, we can't define term orders because of the existence of finite-order invertible operators: e.g., if $g^2 = 1$ then $g < 1$ would imply $1 < g$ and vice versa. This can be fixed, but I won't go into it.)

Let's focus on one example. Let $\mathcal{C} = \mathbf{FS}^{\mathrm{op}}$ be the opposite of the category of finite sets and surjective maps.

Theorem (Sam–Snowden)

Let M be a finitely generated $\mathcal{C}$-module.

- *Every submodule of M is also finitely generated.*
- *The Hilbert series $\sum_{i \geq 0} \dim_{\mathbf{k}}(M_i) t^i$ is a rational function in t.*

We finish with two applications of this in topology and algebraic geometry.

Lannes–Schwartz artinian conjecture

Let $\mathcal{C} = \mathrm{Vec}(\mathbf{F}_q)$ be the category of finite-dimensional $\mathbf{F}_q$-vector spaces and $\mathbf{k} = \mathbf{F}_q$.

Theorem (Putman, Sam, Snowden)

Submodules of finitely generated $\mathcal{C}$-modules are finitely generated.

This follows from the previous result and also from joint work with Andy Putman.

This was conjectured by Jean Lannes and Lionel Schwartz. Their interest comes from a connection of these modules with unstable modules over the Steenrod algebra.

Let $\mathbf{P}(V)$ be the projectivization of a vector space V.
The Segre embedding is the map

$$\begin{aligned} \mathbf{P}(V_1) \times \cdots \times \mathbf{P}(V_n) &\to \mathbf{P}(V_1 \otimes \cdots \otimes V_n) \\ ([v_1], \ldots, [v_n]) &\mapsto [v_1 \otimes \cdots \otimes v_n]. \end{aligned}$$

Three ways to get equations that vanish on the image:

1. Reduce from n to $n-1$ by considering the composition

$$\begin{aligned} \mathbf{P}(V_1) \times \cdots \times \mathbf{P}(V_{n-1}) \times \mathbf{P}(V_n) &\to \mathbf{P}(V_1) \times \cdots \times \mathbf{P}(V_{n-1} \otimes V_n) \\ &\to \mathbf{P}(V_1 \otimes \cdots \otimes V_n) \end{aligned}$$

2. Permute factors
3. Use linear maps $V_i \to V_i'$.

These operations also extend to other things like higher syzygies (call this Tor_i)

This was formalized by Snowden in the notion of a Δ-module.
See my 4:30 talk for more details.

But 1. and 2. are similar to the operations given by $\mathcal{C} = \mathbf{FS}^{\mathrm{op}}$.
This can made rigorous; intuitively the result is:

Theorem (Sam–Snowden)

For each i, there is a finite list of Segre embeddings whose Tor_i groups allow one to build all others under operations 1., 2., and 3.

This was previously shown by Snowden when $\mathbf{k}$ is a field of characteristic 0 using specialized representation theory.

The combinatorial (Gröbner) approach ends up being simpler and more general.

A question

I didn't elaborate on this point, but the connection to formal languages comes from the fact that the morphisms/operations can always be encoded in a "linear way" so that they form a regular language.

There are some more examples of categories $\mathcal{C}$ that we'd like to consider where the morphisms don't have a linear structure, but rather some kind of graphical structure.

Example: The objects of $\mathcal{C}$ are ordered finite sets $[0], [1], [2], \dots$. A morphism $[i] \to [j]$ is an increasing function $f\colon [i] \to [j]$ together with a perfect matching on $[j] \setminus f([i])$.

Is there some notion of "graphical language" which could encode things like this? I expect that well-behaved graphical languages have D-finite generating functions.