Rational functions, Hilbert series, and forbidden subwords

J. Bell

Classical theory of Gröbner bases

- Let $A = \mathbb{C}[x_1, \ldots, x_d]/I$.

- We put a degree lexicographic (dlex) order on the monomials in $x_1, \ldots, x_d$ by declaring that

$$x_1 < x_2 < \cdots < x_d.$$

- For example, $x_1^3 > x_3x_2$ and $x_3x_2 > x_3x_1$.

- For each polynomial f, we let $\mathrm{in}(f)$ denote the dlex largest monomial in f with a nonzero coefficient.

- For example, $\mathrm{in}(x_1^3 + 3x_2x_3 + 7x_4) = x_1^3$.

- We let $\mathrm{in}(I)$ denote the ideal generated by all the $\mathrm{in}(f)$'s with $f \in I$.

Example: Consider $\mathbb{C}[x,y]/I$ with $x < y$, where $I = (x^3 - y, yx - 1)$.

Notice that $x^3, yx \in \text{in}(I)$. Also

$$x^2(yx - 1) - y(x^3 - y) = y^2 - x^2 \in I,$$

so $y^2 \in \text{in}(I)$.

The Gröbner basis algorithm terminates at this point and we see

$$\text{in}(I) = (x^3, y^2, yx).$$

In this example, we have

$$\text{in}(I) = (x^3, y^2, yx).$$

Notice that

$$\mathbb{C}[x, y]/(x^3, y^2, xy)$$

is 4-dimensional as a $\mathbb{C}$-vector space. It has as a basis the images of $1, x, x^2, xy$.

From this we can deduce that the images of $1, x, x^2, xy$ in $A = \mathbb{C}[x, y]/I$ for a basis for this algebra.

Notice that $\text{in}(I)$ is a *monomial ideal*; that is, it is generated by monomials.
Studying monomial ideals is much easier than studying ordinary ideals in a polynomial ring. Often one can use combinatorial methods.

For the purposes of this talk, any set of generators for I whose initial terms generate $\text{in}(I)$ will be called a *Gröbner basis* for I.

SOME APPLICATIONS OF GRÖBNER BASES

- A combinatorial proof of the Hilbert Basis theorem

- They can be used to compute Hilbert series and test if rings are Cohen-Macaulay

- Unexpected: They can be used to answer questions in graph theory

- Unexpected: They can be used to answer questions such as: How many squares on an infinite chess board can a knight reach in at most d moves?

How many squares can the knight reach in at most d moves.

Idea Take the subalgebra of $\mathbb{C}[x, y, x^{-1}, y^{-1}]$ generated by $x^2y, x^2y^{-1}, xy^2, xy^{-2}, x^{-1}y^2$
$x^{-1}y^{-2}, x^{-2}y, x^{-2}y^{-1}$.

We have a surjection from

$$\mathbb{C}[t_1, \ldots, t_8]$$

onto this subalgebra.

Finding a Gröbner basis for the kernel allows us to answer the question.

ANS: $1 + 4d + 7d^2$ for $d \geq 3$, 33 when $d = 2$, 8 when $d = 1$.

Hilbert series

Given a monomial algebra

$$A = \mathbb{C}[x_1, \ldots, x_d]/J$$

we let $f(n)$ denote the number of surviving monomials of degree n in A. Then

$$H(t) = \sum_{n=0}^{\infty} f(n)t^n$$

is called the *Hilbert Series* of A.

Example

$$A \;=\; \mathbb{C}[x, y]/(x^2).$$

Surviving words:

$$y^i, y^i x, i \geq 0.$$

Hence

$$H(t) = 1 + 2t + 2t^2 + \cdots = (1 + t)/(1 - t).$$

Gröbner bases can also be applied in the noncommutative setting.

We let $\mathbb{C}\{X_1, \ldots, X_k\}$ denote the ring of all "noncommutative polynomials" in $X_1, \ldots, X_k$ with coefficients in $\mathbb{C}$.

Notice that a degree lexicographic order still makes sense for words in $X_1, \ldots, X_k$ and so, just as before, we can define the initial ideal, $\mathrm{in}(I)$, of an ideal in $\mathbb{C}\{X_1, \ldots, X_k\}$.

BIG PROBLEM

The real problem with noncommutative Gröbner bases is that they need not be finite.

E.g., Let $I \subseteq \mathbb{C}\{x, y\}$ be the ideal generated by $y^2 - xy$ $(x < y)$.

Then $y^2 \in \mathrm{in}(I)$, but we're not done yet.

Notice

$$[y^2 - xy, y] = yxy - xy^2 \in I,$$

too.

Thus $yxy \in \mathrm{in}(I)$. By induction, one can show that

$$\mathrm{in}(I) = (yx^j y \mid j \geq 0),$$

which is not a finitely generated ideal.

Speaker's Opinion: That's not good.

Given a monomial algebra

$$A = \mathbb{C}\{X_1, \ldots, X_k\}/(W_1, W_2, \ldots)$$

we define the *Hilbert Series* of A to be the function

$$H(t) := \sum_{n=0}^{\infty} f(n) t^n,$$

where $f(n)$ is the number of words in $X_1, \ldots, X_k$ of length n which avoid $W_1, W_2, \ldots$.

In general, given an algebra

$$A = \mathbb{C}\{X_1, \ldots, X_k\}/I$$

we define its Hilbert series to be the Hilbert series of the monomial algebra

$$\mathbb{C}\{X_1, \ldots, X_k\}/\mathrm{in}(I).$$

Thus computation of Hilbert series reduces to the combinatorial problem of counding words on an alphabet which avoid a given set of words.

We call this the forbidden subwords problem.

How many words on the letters A, C, T, G of length n avoid the subword GAG?

Let $f(n)$ denote the number of such words. Let $g(n)$ denote the number of words of length n which begin with GAG and have no other occurrences of GAG.

First Observation: Take a word of length n which avoids GAG and add a letter at the beginning. Then either we have a word of length $n+1$ which avoids GAG, or we have a word of length $n+1$ which begins with GAG and has no other occurrences. Thus

$$4f(n) \;=\; f(n+1) + g(n+1).$$

Second Observation: If we take a word W of length n with no occurrences of GAG and add GAG at the beginning, then W will have exactly one occurrence of GAG unless W begins $AG\cdots$. From this we see

$$f(n) = g(n+3) + g(n+1).$$

Let's put these together:

$$4f(n) \;=\; f(n+1) + g(n+1)$$

and so

$$g(n+1) = 4f(n) - f(n+1).$$

Also

$$f(n) = g(n+3) + g(n+1).$$

Thus

$$f(n) = 4f(n+2) - f(n+3) + 4f(n) - f(n+1).$$

Hence

$$f(n+3) = 4f(n+2) - f(n+1) + 3f(n) \qquad \text{for } n > 0.$$

From here we can obtain asymptotic estimates.

In general, given a finite alphabet X and a finite list of forbidden subwords, the number of words on X of length n which avoid this list will satisfy a recurrence.

Algebraically, this can be thought of in terms of *monomial algebras*.

Given an alphabet $X = \{X_1, \ldots, X_k\}$ and words $W_1, \ldots, W_d$, the words on X which avoid $W_1, \ldots, W_d$ are in one-to-one correspondence with the monomials in $X_1, \ldots, X_k$ which have nonzero image in the ring

$$\mathbb{C}\{X_1, \ldots, X_k\}/(W_1, \ldots, W_d).$$

Notice that if

$$A = \mathbb{C}\{X_1, \ldots, X_k\}/(W_1, \ldots, W_d)$$

is a finitely presented monomial algebra, then the coefficients of its Hilbert series satisfy a recurrence. This says that its Hilbert series is the power series expansion of a rational function.

We are especially interested in the case that an algebra A has a rational Hilbert series. Many well-known classes of algebras have rational Hilbert series.

- A finitely generated commutative $\mathbb{C}$-algebra

- The enveloping algebra of a finite dimensional Lie algebra

- A finitely presented monomial algebra

- $\bigoplus \mathsf{H}^0(X, \mathcal{L}^{\otimes \sigma^{n-1}})$, X n.s. projective variety, $\mathcal{L}$ a very σ-ample invertible sheaf, σ an automorphism of X.

- The group algebra of an abelian-by-finite group

- graded algebras of finite global dimension

To understand the significance of a Hilbert series we must talk about growth of algebras.

Let A be an algebra and let $H(t)$ be its Hilbert series, with $f(n)$ denoting the coefficient of t^n in $H(t)$.

If $f(n) = \mathrm{O}(n^d)$ for some d, then we say that A has polynomially bounded growth.

If there is some $C > 1$ such that $f(n) > C^n$ for all sufficiently large n, we say that A has exponential growth.

Otherwise, we say A has intermediate growth.

But what is the significance of growth?

For a commutative algebra, A must have polynomially bounded growth. The smallest degree polynomial which bounds the growth is equal to the Krull dimension minus 1.

In the noncommutative setting, growth was first used by topologists when studying fundamental groups.

Theorem: If M is a compact Riemannian manifold with all sectional curvatures less than 0, then the group algebra of $\pi_1(M)$ has exponential growth.

Theorem: If M is a complete n-dimensional Riemannian manifold whose mean curvature tensor is everywhere positive semidefinite, then the group algebra of any finitely generated subroup of $\pi_1(M)$ has polynomially bounded growth (deg $\leq n$).

These theorems are due to Milnor.

Significance of Hilbert Series:

Hilbert Series tell us about the "growth" of an algebra. If the Hilbert series $H(t)$ of an algebra A is rational, then we have either:

- A has exponential growth; or
- A has polynomially bounded growth–in this case, the degree of the growth is given by the order of the pole at $t = 1$ in $H(t)$ minus 1.

GK DIMENSION

Given a finitely generated k-algebra A with Hilbert series

$$H(t) = f(0) + f(1)t + f(2)t^2 + \cdots$$

we define the GK dimension of A ($\mathrm{GKdim}(A)$) to be the infimum over all $\alpha \geq 0$ such that

$$f(0) + \cdots + f(n) < n^{\alpha - 1}$$

for all n sufficiently large.

If no such α exists, we take the GK dimension to be infinity.

For example, if $A = \mathbb{C}[x_1, \ldots, x_d]$, the Hilbert series can be seen to be

$$H(t) = 1/(1-t)^d.$$

The power series expansion of this is just

$$\sum_{n=0}^{\infty} \binom{n+d-1}{d-1} t^n.$$

Since $\binom{n+d-1}{d-1}$ is a polynomial in n of degree $d-1$, we conclude that

$$\mathsf{GKdim}(A) \;=\; d.$$

More generally, the GK dimension of a finitely generated commutative $\mathbb{C}$-algebra is the same as its Krull dimension.

- If A is finitely generated, then A has GK dimension 0 if and only if it is finite dimensional.

- There are no algebras of GK dimension strictly between 0 and 1 or strictly between 1 and 2

- For any real number $\alpha \geq 2$, there exists an algebra of GK dimension α.

- An algebra with a rational Hilbert series either has integer GK dimension or the GK dimension is infinite.

Around 1980, Martin Lorenz asked if a prime PI algebra must have a rational Hilbert series (for some set of generators and with some dlex order).

To answer this, we should probably say what a prime PI algebra is.

PI stands for "polynomial identity". This theory began with Amitsur and Kaplansky in the 50s and is now considered to be well-understood.

An algebra is said to be PI, if there is a nonzero, noncommutative polynomial

$$p(x_1, \ldots, x_d)$$

such that

$$p(a_1, \ldots, a_d) = 0$$

for all $a_1, \ldots, a_d \in A$.

A few examples.

Obvious one: If A is commutative then A is PI. (Take the polynomial $x_1x_2 - x_2x_1$.)

Less obvious one: Let A be the ring of 2×2 matrices over $\mathbb{C}$.

Then A satisfies the identity

$$x_1(x_2x_3 - x_3x_2)^2 - (x_2x_3 - x_3x_2)^2x_1 \;=\; 0.$$

Why? Use the Cayley-Hamilton theorem.

QUESTION: Does a PI algebra necessarily have a rational Hilbert series (with respect to some generating set and dlex order)?

ANSWER: NO! Constructions of Warfield show this is not the case. Let

$$I = (y)^3 + (yx^iy \mid i \text{ not a perfect square}).$$

Then $A = F\{x, y\}/I$ has GK dimension 2.5. Moreover the image of $(y)^3$ is (0) in A. Thus A satisfies $[t_1, t_2]^3$.

Problem: Warfield's construction shows that the nilpotent radical of an affine PI algebra is not in general well-behaved. Thus we restrict our consideration to the prime PI case.

Just for the record, a ring R is prime if whenever $xry = 0$ for all r in R, we must have either $x = 0$ or $y = 0$.

Even in this prime case, problems can arise. Stafford has shown that there exist PI algebras which have rational Hilbert series with respect to some dlex order, but which are not rational with respect to another. Thus some care has to be exercised in finding the right generating set and dlex order.

Recall we have the theorem:

Theorem: (Anick, Ufnarovskii) Let A be a finitely presented monomial algebra; i.e.,

$$A = F\{x_1, \ldots, x_n\}/(W_1, \ldots, W_m).$$

Then A has a rational Hilbert series. Moreover, if we let R denote the radius of convergence of the Hilbert series, we have the following cases:

- If $R < 1$, then A contains a copy of the free algebra on two generators;
- If $R = 1$, then A has integer GK dimension equal to the order of the pole at $t = 1$ in $H_A(t)$; or
- If $R > 1$, then $R = \infty$ and A is finite dimensional over F and $H_A(t)$ is a polynomial.

From this we see that if we can order our variables in some way so that the Gröbner basis algorithm terminates after a finite number of steps, then our algebra has a rational Hilbert series. There is a more general criterion which allows one to see if a monomial algebra has a rational Hilbert series. As an example, consider the algebra

$$F\{x, y\}/(yx^j y \mid j \geq 0).$$

Algebras with such an associated digraph are called *automata algebras*.

THEOREM: If A is an automata algebra, then A has a rational Hilbert series.

BACK TO PI RINGS!

The straightforward approach to showing that a finitely generated prime PI ring has a rational Hilbert series is the following.

- First take a central element $z \in A$ such that when z is inverted, the resulting ring A_z is a finite module over its center.

- By the Artin-Tate lemma the center of A_z is a finitely generated commutative ring and hence has rational Hilbert series.

- Use this Hilbert series and the fact that A_z is a finite module over its center to show that A_z has rational Hilbert series.

- Somehow "pullback" the information about A_z to A and show that it too has a rational Hilbert series.

How to get this to work: carefully pick the z which you are going to invert using Gröbner techniques. Once you have done this, you will have a lot of information about how it interacts with other elements of the algebra.

FACT: If A is a finitely generated prime PI algebra then $\mathsf{GKdim}(A) = d$ for some nonnegative integer d.

FACT: If A is an affine prime PI ring of GK dimension d, then

$$k[z_1, \ldots, z_d] \subseteq A.$$

Now what do we do? Notice that if we pick generators for our PI algebra A, say $x_1, \ldots, x_m$. Let V be the vector space spanned by these elements, 1, and by $z_1, \ldots, z_d$. Let W be the vector space spanned by $1, z_1, \ldots, z_d$. Then

$$\dim(W^n) = \binom{n+d}{d},$$

and

$$\dim(V^n) \le Cn^d$$

for some $C > 0$.

WHAT IS THE SIGNIFICANCE OF THIS FACT?

Example: Consider a word u in $x_1, \ldots, x_m$. As an example, look at $u = x_1x_2x_3$. Consider

$$x_1x_2x_3W^{n-3} + x_1x_2W^{n-2} + x_1W^{n-1} + W^n.$$

This space is contained in V^n.

If this set sum is direct, then it has dimension at least

$$\binom{n+d}{n} + \binom{n+d-1}{d} + \binom{n+d-2}{d} + \binom{n+d-3}{d}$$

$$\sim \ 4n^d/d! = \text{length}(u)n^d/d!.$$

Thus if u is long enough this sum cannot be direct. It follows that there is some N such that every word, u, of length N has an initial subword v such that there is a polynomial q_u with the property that

$$0 = vq_u(z_1, \ldots, z_d) + \text{lower lex. order terms.}$$

It follows that if we invert

$$z = \prod_{u \text{ of length } N} q_u,$$

then our algebra is a finite module over its center.

Having constructed this z, if we are careful in picking the right set of generators for our algebra, we see that it can be argued that A_z has a rational Hilbert series and that we can "pullback" and get that A has a rational Hilbert series.

CONJECTURES:

Is the result true for affine Noetherian PI rings (without the prime hypothesis)?

Are prime PI rings finitely presented?

THE END