Boundedness questions for polynomials in many variables

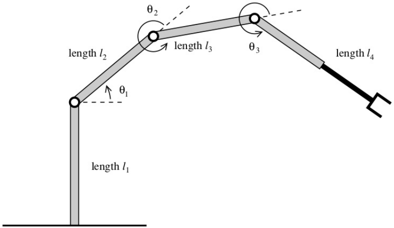
Daniel Erman (Wisconsin)
Steven Sam (UCSD)
Andrew Snowden (Michigan)

March 8, 2021: Wisconsin Logic Seminar

Solving polynomial equations

One of the most fundamental problems in algebra is to solve systems of polynomial equations. This example involves a robot arm:

$$
\begin{aligned}
a &= \ell_3(cd - st) + \ell_2 c \\
b &= \ell_4(ct + ds) + \ell_2 s \\
0 &= c^2 + s^2 - 1 \\
0 &= d^2 + t^2 - 1
\end{aligned}
$$



Naive definition: The **complexity** of a system of polynomial equations is the amount of time it would take a computer to determine the solutions of the system.

Question

Can we better understand the complexity of systems of polynomial equations?

Hilbert's Landmark Theorems (1890s)

In a fixed number of variables, complexity is always bounded in various senses.

Throughout: $S = \mathbb{C}[x_1, \ldots, x_n]$ is the ring of polynomials.

- **Hilbert Basis Theorem**: S is noetherian (i.e. every ideal in S is finitely generated).
- **Hilbert Syzygy Theorem**: every S-module has a free resolution (I'll discuss this in a moment. . .) of length $\leq n$.

Question

Are there interesting analogues of these results as $n \to \infty$?

Question

How complicated can r polynomials $f_1, \ldots, f_r$ of degree $\leq d$ become as $n \to \infty$?

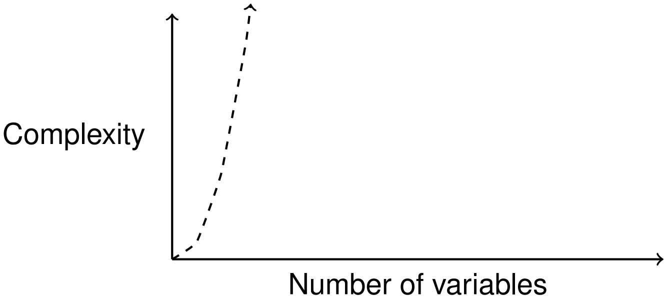
E.g: How complicated can 4 cubic polynomials in $100,000$ variables be?

Cartoon view of complexity

Question

How does complexity of polynomials grow as the number of variables increases?

Expectation: things should get MUCH MUCH more complicated.



Details: as $n \to \infty$, we fix the number of polynomials that we are considering, and the degrees of those polynomials. (We also need a more precise notion of "complexity".)

Measuring Complexity via Syzygies

Definition

A **syzygy** is a relation among the columns of a matrix.

Start with the matrix $[x^2, xy, y^2]$. We have a relation:

$$y \cdot [x^2] - x \cdot [xy] + 0 \cdot [y^2] = [0]$$

Minimal syzygies of $[x^2, xy, y^2] \longleftrightarrow$ the columns of $\begin{bmatrix} y & 0 \\ -x & y \\ 0 & -x \end{bmatrix}$

Key point: Taking syzygies turns a matrix M_1 into an new matrix M_2:

$$M_1 = [x^2, xy, y^2] \qquad \text{yields} \qquad M_2 = \begin{bmatrix} y & 0 \\ -x & y \\ 0 & -x \end{bmatrix}$$

Projective Dimension

Taking syzygies turns a matrix M_1 into a new matrix M_2. Iterating yields a **free resolution**:

$$F_0 \xleftarrow{M_1} F_1 \xleftarrow{M_2} F_2 \xleftarrow{M_3} F_3 \longleftarrow \cdots$$

Metaphor: Free resolutions are like Taylor series; both express a potentially complicated object (a module or a function) in terms of simpler objects (free modules or polynomials).

Definition

For a set of polynomials $f_1, \ldots, f_r$, we define $\mathrm{pdim}(f_1, \ldots, f_r)$ as the minimal p such that there is a free resolution of the form:

$$S^1 \xleftarrow{[f_1, f_2, \cdots f_r]} S^r \xleftarrow{M_2} F_2 \xleftarrow{M_3} \cdots \xleftarrow{M_p} F_p \longleftarrow 0\,.$$

Theorem (Hilbert Syzygy Theorem, 1890)

For any S-module M, $\mathrm{pdim}(M) \leq n$.

Key point: pdim measures the complexity of polynomials (in a meaningful way).

What happens to Hilbert's Theorems as $n \to \infty$?

At first pass, nothing good seems to happen! Over $\mathbb{C}[x_1, x_2, \ldots]$:

- **Basis Theorem fails**: Some ideals require infinitely many generators.
- **Syzygy Theorem fails**: Ideals can have arbitrarily large pdim.

At first pass: no analogous bounds on complexity as $n \to \infty$.

But what if we make the question more specific:

Question

Let f_1, f_2, f_3, f_4 be cubic polynomials in 10^{10} variables. Hilbert's Syzygy Theorem says $\operatorname{pdim}(f_1, \ldots, f_4) \le 10^{10}$. Can we do better?

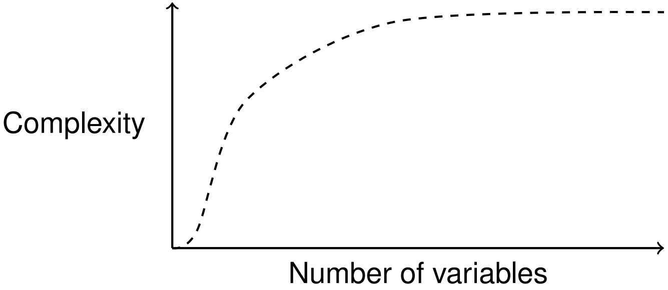
Stillman's Conjecture

Stillman's Conjecture (Proven by Ananyan–Hochster 2015)

Let $f_1, \ldots, f_r$ be polynomials of degree $\leq d$. One can bound $\mathrm{pdim}(f_1, \ldots, f_r)$ solely in terms of r and d (i.e. the bound is independent of the number of variables).

This is a version of Hilbert's Syzygy Theorem as $n \to \infty$.

The cartoon to have in your head:



How should we study polynomials as $n \to \infty$?

This was a real mystery, which is why Stillman's Question was open for 20 years.

Main issue: no algebraic techniques for studying polynomials as $n \to \infty$.

A counterexample to Stillman's Conjecture would be:

- A sequence of polynomials $f_{1,(n)}, \ldots, f_{r,(n)} \in \mathbb{C}[x_1, \ldots, x_n]$ where $\mathrm{deg}(f_{i,(n)}) \leq d$ for all $1 \leq i \leq r$ and $n \leq \infty$. And where $\mathrm{pdim}(f_{1,(n)}, \ldots, f_{r,(n)}) \to \infty$ as $n \to \infty$.

Can't study individual collections of polynomials. Need a framework where sequences of polynomials as $n \to \infty$ make sense.

This leads fairly naturally to an **ultraproduct** framework.

From products to ultraproducts

Example

$\prod_{n\in\mathbb{N}}\mathbb{C}$ is not itself a field. For instance if $(a_n) = (1, 0, 1, 0, 1, 0, \dots)$ and $(b_n) = (0, 1, 0, 1, 0, 1, 0, \dots)$ then $(a_n)(b_n) = 0$ but neither (a_n) nor (b_n) is zero.

Same idea works if $\mathbb{N} = V \cup W$ and $a_n = 0 \;\; \forall n \in V$ and $b_n = 0 \;\; \forall n \in W$.

Idea: force things to be 0 via an equivalence relation. Fix a non-principal ultrafilter $\mathcal{U} \subseteq 2^{\mathcal{I}}$.

In the ultraproduct $\prod_{n\in\mathbb{N}}\mathbb{C}/\sim$, we have $(a_n) = 0 \iff \exists V \in \mathcal{U}$ where $a_n = 0 \forall n \in V$.

Properties of ultrafilters will ensure that this is a field:

- For any $S \subseteq \mathbb{N}$ either V or its complement is in $\mathcal{U}$.
- If $V \in \mathcal{U}$ then any set containing V is also in $\mathcal{U}$.
- If $V, W \in \mathcal{U}$ then so is $V \cap W$.

Ultraproduct ring

Definition

Let $\mathcal{U}$ be a non-principal ultrafilter on $\mathbb{N}$. Let $\mathbf{R}$ be the ultraproduct of $(\mathbb{C}[x_1, \dots, x_n])_{n \in \mathbb{N}}$ with respect to $\mathcal{U}$ (in the category of graded rings).

A degree d element of $\mathbf{R}$ is a sequence $f_{(n)} \in \mathbb{C}[x_1, \dots, x_n]$ of degree d elements (mod $\sim$).

Example

The sequence $(x_1^2 + x_2^2 + \cdots + x_n^2)$ as $n \to \infty$ is an element of $\mathbf{R}$.

Good news: this provides the framework we want. A counterexample to Stillman's Conjecture would be a sequence $f_{1,(n)}, \dots, f_{r,(n)} \in \mathbb{C}[x_1, \dots, x_n]$ of degree $\leq d$ polynomials where $\mathrm{pdim} \to \infty$ as $n \to \infty$. This determines $\mathbf{f}_1, \dots, \mathbf{f}_r \in \mathbf{R}$ of degree $\leq d$.

Bad news: the ring $\mathbf{R}$ looks awful! Very non-noetherian. As a $\mathbb{C}$-algebra, it requires an uncountable number of generators in each degree d. Very far from Hilbert's framework.

Main result

Actually, it's all good news! The ring **R** is as well-behaved as we could've dreamed:

Theorem (Erman-Sam-Snowden, 2018)

The ultraproduct ring **R** *is isomorphic to a polynomial ring* $K[\mathcal{Z}]$ *where* K *is the ultrapower of* $\mathbb{C}$ *and where* $\mathcal{Z}$ *is a collection of variables of uncountable cardinality.*

Upshot: let $f_{1,(n)}, \ldots, f_{r,(n)}$ a sequence of polynomials in $\mathbb{C}[x_1, \ldots, x_n]$ as $n \to \infty$. Write $\mathbf{f}_1, \ldots, \mathbf{f}_r$ for the corresponding elements in **R**.

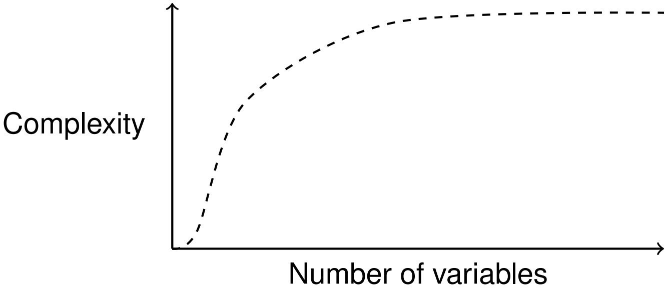
- Invariants play well with the sequences. E.g. there is some $V \in \mathcal{U}$ where

$$\mathrm{pdim}(f_{1,n}, \ldots, f_{r,n}) = \mathrm{pdim}(\mathbf{f}_1, \ldots, \mathbf{f}_r) \qquad \text{for all } n \in V.$$

- Any question $\mathbf{f}_1, \ldots, \mathbf{f}_r \in \mathbf{R}$ references only finitely many elements $z_1, \ldots, z_N$ of $\mathcal{Z}$
- The extension $K[z_1, \ldots, z_N] \to K[\mathcal{Z}]$ is very well behaved. (Faithfully flat.)
- So it suffices to answer the question for $\mathbf{f}_1, \ldots, \mathbf{f}_r \in K[z_1, \ldots, z_N]$.
- Now, Hilbert's result **do apply** and we get everything we would ever want.

Back to complexity

- We wanted to study r polynomials $f_1, \ldots, f_r$ of degree $\leq d$ in n variables as $n \to \infty$.
- The ultraproduct **R** provides a framework for doing this.
- Good algebraic properties of **R** give global bounds on the complexity of sequences $f_{1,(n)}, \ldots, f_{r,(n)}$.
- These in turn yield complexity bounds on $f_1, \ldots, f_r$ which are independent of n.



What next?

1. What properties pass formally from the ultraproduct to the sequence? We want theorems like: $(\mathbf{f}_1, \ldots, \mathbf{f}_r)$ is a prime idea of $\mathbf{R}$ if and only if there exists $V \in \mathfrak{U}$ where $(f_{1,(n)}, \ldots, f_{r,(n)})$ is a prime ideal of $\mathbb{C}[x_1, \ldots, x_n]$ for all $n \in V$.
2. Is there a meta reason why the ultraproduct of “nice objects” (e.g. polynomial rings) should be another “nice object”?
3. The ultraproduct allows limits of individual ring elements. But algebra tends to be more interested in taking ideals or modules or varieties as the atomic objects. Do ultraproducts (or other constructions) make sense in this setting?
4. Local rings: What properties does the ultraproduct of $\mathbb{C}[[x_1, \ldots, x_n]]$ have?