Challenges in Computational Algebraic Geometry

Computational Algebraic Geometry Workshop

David A. Cox

Department of Mathematics and Computer Science
Amherst College
dac@cs.amherst.edu

FoCM'08
20 June 2008

Challenges

There are many challenges facing Computational Algebraic Geometry:

- Practical: Do big problems using existing algorithms and hardware.
- Theoretical: Find better algorithms. Also understand the complexity of existing algorithms.

This Talk

I will discuss some *completely different* challenges facing Computational Algebraic Geometry.

Outline

Nature, 20 January 2000

A Synthetic Oscillatory Network of Transcriptional Regulators

Michael B. Elowitz & Stanislas Leibler

Departments of Molecular Biology and Physics, Princeton

Networks of interacting biomolecules carry out many essential functions in living cells, but the ‘design principles’ underlying the functioning of such intracellular networks remain poorly understood.

Here we present the design and construction of a synthetic network to implement a particular function. We used three transcriptional repressor systems to build an oscillating network, termed the repressilator, in *Escherichia coli*.

From “Box 1” of the Article

Three repressor-protein concentrations p_i and their corresponding mRNA concentrations m_i (i is *lacI*, *tetR*,*cI*) are treated as continuous dynamical variables.

The kinetics of the system are determined by six coupled first-order differential equations:

$$\begin{aligned} \frac{dm_i}{dt} &= -m_i + \frac{\alpha}{1+p_j^n} + \alpha_0 \\ \frac{dp_i}{dt} &= -\beta(p_i - m_i) \end{aligned}$$

for $i =$ *lacI*, *tetR*, *cI*, $j =$ *cI*, *lacI*, *tetR* and $n, \alpha, \alpha_0, \beta > 0$.

Question

What are the steady-state solutions?

Steady State Solutions

The steady state solutions are solutions of the system:

$$\begin{aligned} 0 &= -m_i + \frac{\alpha}{1+p_j^n} + \alpha_0 \\ 0 &= -\beta(p_i - m_i) \end{aligned}$$

Write the indices as $i = 1,2,3$, $j = 2,3,1$.

The System of Equations

$$\begin{aligned} 0 &= -p_1 + \tfrac{\alpha}{1+p_2^n} + \alpha_0 \\ 0 &= -p_2 + \tfrac{\alpha}{1+p_3^n} + \alpha_0 \\ 0 &= -p_3 + \tfrac{\alpha}{1+p_1^n} + \alpha_0 \end{aligned}$$

Real Solutions

Claim

Assume $\alpha, \alpha_0 > 0$.

- The equation
$$p = \frac{\alpha}{1+p^n} + \alpha_0$$
has a unique real solution, denoted p.
- The unique real solution of
$$\begin{aligned} 0 &= -p_1 + \tfrac{\alpha}{1+p_2^n} + \alpha_0 \\ 0 &= -p_2 + \tfrac{\alpha}{1+p_3^n} + \alpha_0 \\ 0 &= -p_3 + \tfrac{\alpha}{1+p_1^n} + \alpha_0 \end{aligned}$$
is given by $p_1 = p_2 = p_3 = p$.

Proof for $n = 2$

Set $p = p_1$, $a = \alpha$, $b = \alpha_0$ and eliminate p_2, p_3:

$$(p^3 - bp^2 + p - a - b)(1 + 2a^2 + a^4 + 5ab + 4a^3b + 3b^2 + 8a^2b^2 + 8ab^3 + a^3b^3 + 3b^4 + 3a^2b^4 + 3ab^5 + b^6 - ap - 2a^2bp - 2ab^2p - a^3b^2p - 2a^2b^3p - ab^4p + 3p^2 + 4a^2p^2 + 12abp^2 + 3a^3bp^2 + 9b^2p^2 + 12a^2b^2p^2 + 18ab^3p^2 + 9b^4p^2 + 3a^2b^4p^2 + 6ab^5p^2 + 3b^6p^2 - 2ap^3 + a^3p^3 - 2a^2bp^3 - 4ab^2p^3 - 2a^2b^3p^3 - 2ab^4p^3 + 3p^4 + 3a^2p^4 + 9abp^4 + 9b^2p^4 + 4a^2b^2p^4 + 12ab^3p^4 + 9b^4p^4 + 3ab^5p^4 + 3b^6p^4 - ap^5 - 2ab^2p^5 - ab^4p^5 + p^6 + a^2p^6 + 2abp^6 + 3b^2p^6 + 2ab^3p^6 + 3b^4p^6 + b^6p^6) = 0$$

The second factor is a polynomial H of degree 6 in p.

Small Discriminant Calculation

$p^3 - bp^2 + p - a - b$ has a unique real root when $a, b > 0$.

Proof for $n = 2$, Continued

Larger Discriminant Calculation

The polynomial H is positive when $p, a, b > 0$.

(Suggested by Fabrice Rouillier) The discriminant of H is

$$Disc(H, p) = a^{16}(a^2 + b^6 + 3b^2 + 3b^4 + 1 + 2ab + 2ab^3)P$$

where P is a sum (no subtractions) of monomials in a, b with a constant term 16384. The leading coefficient of H

$$a^2 + b^6 + 3b^2 + 3b^4 + 1 + 2ab + 2ab^3$$

is strictly positive when $a, b > 0$, so H has no root at infinity. So the number of real roots of H is constant when $a, b > 0$.

QED

Better Proof for all $n > 0$

(Suggested by André Galligo)

Key Point

If $\alpha, \alpha_0, n > 0$, then $p \mapsto \frac{\alpha}{1+p^n} + \alpha_0$ is strictly decreasing.

Assume

$$\begin{aligned} p_1 &= \frac{\alpha}{1+p_2^n} + \alpha_0 \\ p_2 &= \frac{\alpha}{1+p_3^n} + \alpha_0 \\ p_3 &= \frac{\alpha}{1+p_1^n} + \alpha_0 \end{aligned}$$

and suppose for example $p_2 < p_3$. Then

$$p_2 < p_3 \Rightarrow p_1 > p_2 \Rightarrow p_3 < p_1 \Rightarrow p_2 > p_3,$$

a contradiction. QED

From the “Methods” Section of the Article

Time-lapse microscopy was conducted on a Zeiss Axiovert 135TV microscope equipped with a 512 $\times$ 512-pixel cooled CCD camera (Princeton Instruments).

Bright-field (0.1 s) and epifluorescence (0.05–0.5 s) exposures were taken periodically (every 5 or 10 min). All light sources (standard 100 W Hg and halogen lamps) were shuttered between exposures.

A fast Fourier transform was applied to the temporal fluorescence signal from each analyzed cell lineage and divided by the transform of a decaying exponential with a time constant of 90 min, the measured lifetime of GFPaav.

More from “Box 1” of the Article

The system of differential equations has a unique steady state, which becomes unstable when

$$\frac{(\beta+1)^2}{\beta} < \frac{3X^2}{4+2X}$$

where

$$X = \frac{\alpha n p^{n-1}}{(1+p^n)^2}$$

and p is the solution to

$$p = \frac{\alpha}{1+p^n} + \alpha_0$$

No Justification Whatsoever!

This is all they say about uniqueness!

Challenge 1

Biology is using more and more mathematics, but their culture is very different. Hence:

- They describe the microscope and the types of lights.
- They mention the use of FFT to analyze the data.

But when it comes to a serious mathematical assertion, they say nothing! Here are unanswered questions:

- Did they know the proof just described?
- Why didn't they say "since $\frac{\alpha}{1+p^n} + \alpha_0$ is decreasing"?

Challenge 1

Users in other fields may have different traditions for dealing (or not dealing) with mathematics. How do we help them take the mathematics seriously?

What is a Computation?

A symbolic computation can take many forms:

- An algorithm (most general)
- A straight-line program (for large polynomials)
- An explicit formula (determinant or determinant of a complex)

I will illustrate this range of computations with the example of the classical multivariable resultant. As we will see, there are some challenges.

The Classical Multivariable Resulant

Let $F_0, \ldots, F_n \in \mathbb{C}[x_0, \ldots, x_n]$ be homogeneous polynomials of degrees $d_0, \ldots, d_n$.

Definition

The Resultant of $F_0, \ldots, F_n$, denoted

$$\mathrm{Res} = \mathrm{Res}_{d_0,\ldots,d_n}(F_0, \ldots, F_n)$$

is a polynomial in the coefficients of $F_0, \ldots, F_n$ with the property that

$$\mathrm{Res}(F_0, \ldots, F_n) = 0 \iff \begin{cases} F_0 = \cdots = F_n = 0 \\ \text{has a nontrivial solution} \end{cases}$$

Computing Resultants

$\mathrm{Res} = \mathrm{Res}_{d_0,\ldots,d_n}(F_0,\ldots,F_n)$ can be computed many ways:

- The Macaulay formula, which expresses Res as a quotient of two determinants.
- In some special cases, there are determinantal formulas for Res (Sylvester, Bézout, etc.).
- The Poisson formula, which expresses Res as a product of F_0 evaluated at the solutions of $F_1 = \cdots = F_n = 0$.
- The Cayley formula, which expresses Res as the determinant of a complex.

GCD of Maximal Minors

Here is another resultant formula. Let $d = \sum_{i=0}^{n} d_i - n$ and set $S = \mathbb{C}[x_0, \ldots, x_n]$. Then S_k denotes the vector space of homogeneous polynomials of degree k. Consider

$$\begin{array}{ccc} S_{d-d_0} \oplus \cdots \oplus S_{d-d_n} & \longrightarrow & S_d \\ (G_0, \ldots, G_n) & \longmapsto & G_0F_0 + \cdots + G_nF_n \end{array}$$

Theorem

Let M be matrix of this map with respect to the monomial bases. Regard the coefficients of the F_i as variables. Then

$$Res = \gcd\{\textit{maximal minors of } M\}.$$

Resultant Matrices

The matrix of the previous slide is called a resultant matrix by Elkadi and Mourrain. The resultant matrix, denoted ResMat, has some advantages over the resultant Res:

- ResMat requires no symbolic computation.
- For a specific choice of the F_i, Res = 0 $\iff$ ResMat does not have maximal rank.
- ResMat adapts well to approximate coefficients.

A Challenging Suggestion

This approach suggests that in certain situations, resultants should be replaced with resultant matrices.

A Very Different Formula

Let $A = (A_{ij})_{0 \le i,j \le n}$. Set $\widehat{F}_i = F_i(\frac{\partial}{\partial A_{i0}}, \dots, \frac{\partial}{\partial A_{in}})$ and define

$$\frac{T^k}{k} = d_0 \cdots d_n \sum_{k_0+\cdots+k_n=k} \prod_{i=0}^{n} \frac{\widehat{F}_i^{k_i}}{(d_i k_i)!} \frac{\operatorname{Tr} A^{d_0k_0+\cdots+d_nk_n}}{d_0k_0+\cdots+d_nk_n}\bigg|_{A=0}$$

Theorem (Morozov & Shakirov, 2008; Faá di Bruno, 1859)

$$\operatorname{Res}(x_0^{d_0} - F_0, \dots, x_n^{d_n} - F_n) = \exp\Big(-\sum_{k=0}^{\infty} \frac{T^k}{k}\Big)$$

This generalizes the classical formula

$$\det(I - A) = \exp\Big(-\sum_{k=0}^{\infty} \frac{\operatorname{Tr} A^k}{k}\Big)$$

(Thanks to Jean-Pierre Jouanolou for the 1859 reference.)

A Joint Paper

The multiplicity of computations presents another challenge, related to the way some mathematicians view computations.

For example, I wrote a paper with Laurent Busé and Carlos D'Andrea on implicitization of surfaces in $\mathbb{P}^3$. Like resultants, implicitization can be done many ways, including:

- Gröbner bases.
- Resultants.
- Moving surfaces (Sederberg, Chen, Goldman, etc.)

The first referee rejected the paper and wondered why we didn't use Gröbner bases to solve the problem!

Challenge 2

The multiplicity of computations leads to more challenges:

Challenge 2

- (Within the Computational Community)
  Can we be truly open to radically different ways of thinking about objects [resultants, for example] that we know and love?
- (Relating to the Larger Mathematical Community)
  How do we educate our fellow algebraic geometers and commutative algebraists about the importance of multiple approaches to computational problems?

Bad Algorithms

There are many bad algorithms.

Primality Testing

Test the primality of $n > 1$ in $\mathbb{Z}$ dividing n by all $1 < m < n$.

High complexity need not make an algorithm bad.

Buchberger Algorithm

Compute a Gröbner basis of $\langle f_1, \ldots, f_s \rangle \subseteq \mathbb{Q}[x_1, \ldots, x_n]$.

This algorithm is doubly exponential but incredibly useful.

On the other hand, there are some completely impractical algorithms that are nevertheless wonderful.

Here are three of my favorite bad algorithms.

An Algorithm of Kronecker

Irreducibility over $\mathbb{Q}$

Let $f \in \mathbb{Z}[x]$ have degree n and relatively prime coefficients. How do we tell if f is irreducible over $\mathbb{Q}$?

Create a finite list of polynomials g as follows:

- For $0 < d < n$ and factors a_i of $f(i)$, $i = 0, \ldots, d$, find $g \in \mathbb{Q}[x]$ with $\deg(g) \leq d$ and $g(i) = a_i$, $i = 0, \ldots, d$.
- Accept g if $\deg(g) = d$ and $g \in \mathbb{Z}[x]$; reject otherwise.

Theorem (Kronecker)

f is irreducible $\iff$ f is divisible by none of these g's.

This algorithm is dreadfully inefficient but still wonderful because it gives a constructive method for finding factors. It is not obvious such such a method exists.

Another Algorithm of Kronecker

Factoring over a Number Field

Let $f \in \mathbb{Q}[x]$ is irreducible and let $\mathbb{Q} \subseteq K$ be a number field. How do we factor f over K?

The previous algorithm requires a UFD (very rare for number fields) and, as noted by Hendrik Lenstra, finitely many units (only $\mathbb{Q}$ and imaginary quadratic fields). So how do we proceed?

First observe that there is an algorithm that works over K, namely the Euclidean Algorithm for $K[x]$.

In 1882, Kronecker combined factorization in $\mathbb{Q}[x]$ and the Euclidean Algorithm for $K[x]$ to give a factorization algorithm in $K[x]$.

Using Factorization over $\mathbb{Q}$

Let g be the minimal polynomial of a primitive element $\beta \in K$, so that $K = \mathbb{Q}(\beta) \simeq \mathbb{Q}[y]/\langle g(y)\rangle$. Then set

$$A = \mathbb{Q}[x,y]/\langle f(x), g(y)\rangle \simeq K[x]/\langle f(x)\rangle$$

and pick $t \in \mathbb{Q}$ such that $x + ty$ takes distinct values on the solutions of $f(x) = g(y) = 0$.

Let $M : A \to A$ be the linear map induced by multiplication by $x + ty$ and let

$$\mathrm{Char}_M(u) = \prod_{i=1}^{s} \Phi_i(u)$$

be the factorization of the characteristic polynomial of M into irreducible factors in $\mathbb{Q}[x]$.

Using the Euclidean Algorithm over K

Theorem (Kronecker)

The irreducible factors of f in $K[x]$, $K = \mathbb{Q}(\beta)$, are given by

$$gcd_{K[x]}(f(x), \Phi_i(x + t\beta))$$

- This algorithm for factoring f over $K[x]$ is bad because computing the characteristic polynomial involves evaluating a large determinant.
- This algorithm is wonderful because it shows how to factor in situations when unique factorization fails in $\mathscr{O}_K$.
- This algorithm is wonderful because it links factoring and the Euclidean algorithm.

Graphs Coloring and Sudoku

Let $G = (V, E)$ be a graph with vertices $V = \{1, \ldots, n\}$.

Definition

A *k*-coloring of G is a function from V to a set of k colors such that adjacent vertices have distinct colors.

Example

vertices = 81 squares

edges = links between:

- squares in same column
- squares in same row
- squares in same 3×3

Colors $= \{1, 2, \ldots, 9\}$

Goal: Extend the partial coloring to a full coloring.

				3	5			
	1		2			9		
7		6				2		
6			5				3	
2				4				9
	3				1			5
		3				4		8
		4			6		7	
			3	1				

Graph Ideal

Definition

The *k*-coloring ideal of G is the ideal $I_{G,k} \subseteq \mathbb{C}[x_i \mid i \in V]$ generated by:

$$\begin{aligned} \text{for all } i \in V: &\quad x_i^k - 1 \\ \text{for all } ij \in E: &\quad x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} \end{aligned}$$

Lemma

$\mathbf{V}(I_{G,k}) \subseteq \mathbb{C}^n$ consists of all k-colorings of G for the set of colors consisting of the k^{th} roots of unity

$$\mu_n = \{1,\ \zeta_k,\ \zeta_k^2,\ \ldots,\ \zeta_k^{k-1}\}, \quad \zeta_k = e^{2\pi i/k}$$

Uniquely k-Colorable Graphs

Definition

A graph G is uniquely k-colorable if it has a unique k-coloring up the permutation of the colors.

We start with a k-coloring of G that uses all k colors. Assume the k colors occur among the last k vertices. Then:

- Use variables $x_1, \ldots, x_{n-k}, y_1, \ldots, y_k$ with lex order

$$x_1 > \cdots > x_{n-k} > y_1 > \cdots > y_k$$

- Use these variables to label the vertices of G.

A Theorem

Consider the following n polynomials:

$$y_k^k - 1$$

$$h_j(y_j,\ldots,y_k) = \textstyle\sum_{\alpha_j+\cdots+\alpha_k=j} y_j^{\alpha_j}\cdots y_k^{\alpha_k}, \quad j = 1,\ldots,k-1$$

$$x_i - y_j, \quad \text{color}(x_i) = \text{color}(y_j),\ j \geq 1$$

Theorem (Hillar & Windfeldt, 2008)

The following are equivalent:

- *G is uniquely k-colorable.*
- *The n polynomials $g_1,\ldots,g_n$ listed above lie in $I_{G,k}$.*
- *$\{g_1,\ldots,g_n\}$ is a Gröbner basis for $I_{G,k}$.*

Solving the Sudoku

To solve this sudoku, use:

- 81 variables x_{ij}, $1 \leq i,j \leq 9$.
- Relabel the 9 variables for red squares as $y_1, \ldots, y_9$.
- The graph ideal $I_{G,9}$.
- The 9 polynomials $y_9{}^9 - 1$, $h_8(y_8, y_9), h_7(y_7, y_8, y_9)$, $h_6(y_6, y_7, y_8, y_9), \ldots,$ $h_1(y_1, \ldots, y_9) = y_1 + \cdots + y_9$.
- The 16 polynomials $x_{31} - y_7$, $x_{33} - y_6, x_{37} - y_2, \ldots$

				3	5			
	1		2			9		
7		6				2		
6			5				3	
2				4				9
	3				1			5
		3				4		8
		4			6		7	
			3	1				

Assuming a unique solution, the Gröbner basis of the ideal generated by these polynomials will contain $x_{11} - y_i$, etc. This will tell us how to fill in the blank squares!

Really Bad and Wonderful

This algorithm is a really bad way to solve sudoku puzzles. People have tried to implement it in *Magma*, *Mathematica*, etc., with no success—the 81 variables of a 9×9 sudoku make the complexity too great. (This method can work using various tricks, but these tricks are essentially the standard algorithm to solve sudoku.)

A Good Student Project

This can be done successfully for 4×4 sudoku puzzles.

This algorithm is wonderful in the way it links sukoku, graph coloring, and Gröbner bases. Such unexpected connections are part of the wonder and joy of mathematics.

Challenge 3

Cutting-edge algorithms are very important in computational algebraic geometry. But there are also bad algorithms that deserve to be celebrated:

- They can show us that something is possible.
- They can illustrate the links between different ideas.
- They can amuse and inspire us.

Challenge 3

Can we love these bad algorithms? Can we find more?

Thank you!