CoCoA at Work

Lorenzo Robbiano

University of Genoa, Italy

Computational Commutative Algebra,
MSRI at Berkeley, USA,
March 13 – 15, 2003

ABSTRACT

In this talk I will present three different situations where the *hard work* of CoCoA proved to be essential. In a sort of *crescendo* they are shown in order of increasing difficulty.

- The first case is the huge computation which led to the proof that certain strange univariate polynomials with sparse squares are minimal (rating: **easy**).
- The second topic relates to the computation underlying the full solution of a famous inverse problem in Statistics (rating: **moderately difficult**).
- Finally, I will discuss some preliminary experimental results about generic initial ideals which are still being investigated (rating: **quite difficult**, at least for me).

CoCoA 5 (New project. First official presentation at **COCOA VIII** (Cadiz (Spain) 2 – 7 June 2003)

*The new meaning of a "*CoCoA *Bug".*

Papers, books, software, and news are available at
`http://cocoa.dima.unige.it`

INDEX

1) Sparse Squares

For further details see

J. Abbott: *Sparse Squares of Polynomials*,
Mathematics of Computation (2000) p. 407–413

and the book

M. Kreuzer, L. Robbiano: *Computational Commutative Algebra 1*,
Springer, 2000, p. 261–263 (*Tutorial 42: Strange Polynomials*)

Here you see an **easy** CoCoA session.

```
Use Q[x];
F:= x^12 + 2x^11 - 2x^10 + 4x^9 - 10x^8 + 50x^7 - 128x^6 - 506x^5 +
    506x^4 - 1012x^3 + 2530x^2 - 12650x - 31625;
Len(F);    F^2; Len(F^2);
13
-------------------------------
x^24 + 4x^23 + 44x^19 - 1804x^17 - 9764x^13 - 176402x^12 + 144716x^11 -
3508604x^7 + 24482304x^6 + 14081980x^5 + 800112500x + 1000140625
-------------------------------
12
```

Therefore the polynomial

$$F = x^{12} + 2\,x^{11} - 2\,x^{10} + 4\,x^{9} - 10\,x^{8} + 50\,x^{7} - 128\,x^{6} - 506\,x^{5} + 506\,x^{4} - 1012\,x^{3} + 2530\,x^{2} - 12650\,x - 31625$$

is such that

$$F^2 = x^{24} + 4\,x^{23} + 44\,x^{19} - 1804\,x^{17} - 9764\,x^{13} - 176402\,x^{12} + 144716\,x^{11} - 3508604\,x^{7} + 24482304\,x^{6} + 14081980\,x^{5} + 800112500\,x + 1000140625$$

is "shorter"

After several clever reductions of the problem, it was necessary to compute (with CoCoA) about $150,000$ Gröbner bases, to conclude that F is the **smallest** among the polynomials with rational coefficients, such that the square has fewer power products in its support.

2) Border Bases and Design of Experiments.

For further details see

M. Caboara, L. Robbiano: *Families of Estimable Terms*, Proceedings of ISSAC 2001, (London, Ontario, Canada, July '01, (New York, N.Y.), B. Mourrain, Ed. 56–63, 2001

L. Robbiano: *Zero-Dimensional Ideals*, or, *The inestimable Value of Estimable Terms*, Proceedings of the Academy Colloquium (2001), Constructive Algebra and Systems Theory. To appear

Design of Experiments (DoE) is a branch of Statistics.
Let us see one (very sketchy) example.

EXAMPLE (Chemical Plant)

A problem arises at the filtration stage in a chemical plant.

In similar plants the filtration cycle takes $\sim 40\ min.$

In this plant the filtration cycle takes $\sim 80\ min.$

WHY ?

SEVEN potential causes are considered:

water supply, raw material, level of temperature, rate of addition of caustic soda, ...

A total set of experiments (points) would be

$$2^7 = 128$$

It is practically impossible to carry out all those experiments.

Too expensive and too time consuming.

Complete designs D are too big. We need SUBSETS.

They are called FRACTIONS

$$F \subset D$$

Question 1: Are there "good" confounding equations for F?

Question 2: How do we compute them?

Question 3: How do we connect defining ideals with models?

Answer 1: The defining ideal, a Gröbner basis, an indicator function (separator).

Answer 2: The Buchberger-Möller Algorithm.

Answer 3:

Let $F \subset D$ and let $s = |F|$. Then

$$\dim(K[x_1, \ldots, x_n]/I(F)) = s$$

So, let $\{t_1, \ldots, t_s\}$ be power products such that their classes form a K-basis of the quotient ring, and let

$$y = f(x) = \sum_{i=1}^{s} \lambda_i t_i$$

be a polynomial function on F. By estimating the t_i's at F, we get an $s \times s$ "evaluation matrix", which is INVERTIBLE. This means that by evaluating y at the points of F we can

IDENTIFY the MODEL

Question 4: How do we get monomial bases?

Answer 4: Use Gröbner bases.

BUT

Gröbner bases are not enough!

Let D be the 3^2 complete design. It has 9 points and canonical basis $\{1,\ x,\ y,\ x^2,\ xy,\ y^2,\ x^2y,\ xy^2,\ x^2y^2\}$.

Example: Five Points.

Let $D \subset F$ be the following fraction

$$D = \{(0,0),\ (0,-1),\ (1,0),\ (1,1),\ (-1,1)\}$$

and consider the tuple $\mathcal{O} = (1,\ x,\ y,\ x^2,\ y^2)$.

It is immediate to check that the determinant of the evaluation matrix is -4, hence $\overline{\mathcal{O}}$ is a basis of $P/I(F)$,

BUT

$$f = x^2 + xy - x - \frac{1}{2}y^2 - \frac{1}{2}y \ \in\ I(F)$$

and for every term ordering σ, we see that

either $\mathrm{LT}_\sigma(f) = x^2$ or $\mathrm{LT}_\sigma(f) = y^2$.

A fundamental problem.

Now we concentrate on a very important problem.

Let D be a full factorial design, and let $\mathcal{O} \subset \mathcal{O}(D)$ be a complete set of estimable terms. What are the fractions F of D such that $\overline{\mathcal{O}}$ is a basis of $P/I(D)$ as a K-vector space?

We know already that Gröbner bases are not enough!
A new tool is needed

The notion of a Border basis.

Definition 1 Let O be a non-empty set of power products such that whenever $t'|t$ for some $t \in O$ then $t' \in O$. Then O is called a **complete set of estimable terms**.

Theorem Let $\mathcal{O} = (t_1, \ldots, t_\mu)$ be such that $O = \{t_1, \ldots, t_\mu\}$ is a complete set of estimable terms, and let $b_1, \ldots, b_\nu$ be power products such that $\mathcal{O}^+ = (b_1, \ldots, b_\nu)$. Let $\mathcal{G} = (g_1, \ldots, g_\nu)$ be a tuple of non-zero polynomials marked by $\mathcal{O}^+$, such that $\mathrm{Supp}(b_j - g_j) \subseteq O$ for $i = 1, \ldots, \nu$, and let I be the ideal generated by $\mathcal{G}$.

The following conditions are equivalent

a) The set $\overline{O} = (\bar{t}_1, \ldots, \bar{t}_\mu)$ is a basis of P/I as a K-vector space.

b) The matrices $\mathcal{M}_1, \ldots, \mathcal{M}_n$ associated to (G, O^+) are pairwise commuting.

In that case, $\mathcal{G}$ is called a **border basis** of I with respect to $\mathcal{O}$.

Let $\mathcal{D}$ be the full 3^2 factorial design whose canonical polynomials are $f_1 = x^3 - x$ and $f_2 = y^3 - y$. In this case $O(\mathcal{D}) = \{1, x, y, x^2, xy, y^2, x^2y, xy^2\}$. Let $O = \{1, x, y, x^2, y^2\} \subset O(\mathcal{D})$. It is a complete set of estimable terms, and we get the equality $O^+ = \{x^3, y^3, xy, x^2y, xy^2\}$

PROBLEM: Find all the fractions $\mathcal{F}$ of $\mathcal{D}$ such that O is a basis of the K-vector space $P/I(\mathcal{F})$.

We introduce new independent indeterminates

$$a_{11}, \ldots, a_{15},\ a_{21}, \ldots, a_{25},\ a_{31}, \ldots, a_{35}$$

and construct the polynomials

$$\begin{aligned} g_1 &= xy \quad + a_{11} + a_{12}x + a_{13}y + a_{14}x^2 + a_{15}y^2 \\ g_2 &= x^2y + a_{21} + a_{22}x + a_{23}y + a_{24}x^2 + a_{25}y^2 \\ g_3 &= xy^2 + a_{31} + a_{32}x + a_{33}y + a_{34}x^2 + a_{35}y^2 \end{aligned}$$

in $K[A][x, y]$. We mark them by xy, x^2y and xy^2 respectively.

The matrices associated to (G, O^+) are

$$\mathcal{M}_x = \begin{pmatrix} 0 & 0 & -a_{11} & 0 & -a_{31} \\ 1 & 0 & -a_{12} & 1 & -a_{32} \\ 0 & 0 & -a_{13} & 0 & -a_{33} \\ 0 & 1 & -a_{14} & 0 & -a_{34} \\ 0 & 0 & -a_{15} & 0 & -a_{35} \end{pmatrix} \quad \mathcal{M}_y = \begin{pmatrix} 0 & -a_{11} & 0 & -a_{21} & 0 \\ 0 & -a_{12} & 0 & -a_{22} & 0 \\ 1 & -a_{13} & 0 & -a_{23} & 1 \\ 0 & -a_{14} & 0 & -a_{24} & 0 \\ 0 & -a_{15} & 1 & -a_{25} & 0 \end{pmatrix}$$

We force $\mathcal{M}_x$ and $\mathcal{M}_y$ to commute by imposing

$\mathcal{M}x\mathcal{M}y - \mathcal{M}y\mathcal{M}x = 0$, and get 20 **equations in the** a_{ij}.

A computation carried out with CoCoA shows that $\mathcal{I}(O)$ is zero-dimensional, radical and its multiplicity is 81.

In conclusion, out of the $126 = \binom{9}{5}$ **five-tuples of points in** $\mathcal{D}$**, there are** 81 **five-tuples which solve the problem.**

One of the solutions of $\mathcal{I}(O)$ is the point $p \in \mathbb{Q}^{15}$ whose coordinates are

$$\begin{array}{llllll} a_{11} = 0 & a_{12} = -1 & a_{13} = -\frac{1}{2} & a_{14} = 1 & a_{15} = -\frac{1}{2} \\ a_{21} = 0 & a_{22} = \ \ 0 & a_{23} = -\frac{1}{2} & a_{24} = 0 & a_{25} = -\frac{1}{2} \\ a_{31} = 0 & a_{32} = -1 & a_{33} = -\frac{1}{2} & a_{34} = 1 & a_{35} = -\frac{1}{2} \end{array}$$

By substituting those values in $G \subset \mathbb{Q}(A)[x, y]$ we have the border basis $G_p \subset \mathbb{Q}[x, y]$.

The fraction $\mathcal{F}_p$ of $\mathcal{D}$ defined by G_p is

$$\{(0,0), (0,-1), (1,0), (1,1), (-1,1)\}$$

This is the Example of the Five Points introduced before.

It is possible to show that out of the 81 five-tuples which solve the problem, only 45 can be found using Gröbner Bases.

3) Generic Initial Ideals and Sections.

For further details see

A.M. Bigatti, A. Conca, L. Robbiano: *Generic Initial Ideals and Distractions*, In preparation

The keywords here are Generic Initial Ideals, Distractions, and Hyperplane Sections.

Let me recall some facts.

Theorem (Galligo-Bayer-Stillman)
Let K be an infinite field, let σ be a term ordering on $\mathbb{T}^n$, and let I be a homogeneous ideal in P. For a generic element $g \in \mathrm{GL}(n, K)$, we have

a) The ideal $\mathrm{in}_\sigma(g(I))$ is constant.

b) The ideal $\mathrm{in}_\sigma(g(I))$ is Borel-fixed.

Proposition (Borel and Strongly Stable Ideals)
Let K be a field, and let I be a monomial ideal in the polynomial ring $K[x_1, \ldots, x_n]$. Consider the following conditions.

a) The ideal I is Borel-fixed

b) The ideal I is strongly stable

Then b) $\Rightarrow$ a). Moreover, if $\operatorname{char}(K) = 0$ they are equivalent.

Proposition (Strongly Stable Ideals and Gins)
Let K be a field, and let I be a strongly stable monomial ideal in the polynomial ring $K[x_1, \ldots, x_n]$. Then

$$\operatorname{gin}_\sigma(I) = I$$

Theorem (Gins and Hyperplane Sections)
Let I be a homogeneous ideal in P, let $h \in P_1$ be a generic linear form, let $i \in \{1, \ldots, n\}$, and let σ be a term ordering of x_i-DegRev type. Then we have the equality

$$\operatorname{gin}_{\sigma_i}(I_h) = (\operatorname{gin}_\sigma(I))_{x_i}$$

of ideals in $K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$.

QUESTION

For **ideals of distractions** and term orderings of x_i-DegRev type, is it true that

$$\operatorname{gin}_{\sigma_i}(I_{x_i}) = (\operatorname{gin}_\sigma(I))_{x_i}$$

The reason we thought it was true was a combination of **intuition** and some CoCoA **experimental evidence**.

BUT

The answer is **NO**. The turning point happened when CoCoA finished the following session.

WARNING

CoCoA examples involving computations of generic initial ideals have probability of being correct equal to $100\% - \varepsilon$, where ε is as small as you wish... but not equal to 0.

```
M := Mat([[1,1,1,1],[0,0,0,-1],[1,0,0,0],[0,1,0,0]]);
Use Q[x,y,z,w], Ord(M);
   I := Ideal(x^5, x^4y, x^4z, x^3y^2, x^2y^3 );
   G1:= GinSect(Subst(HDistraction(I), w,
                    Randomized(DensePoly(1)-w)));
   G2:= GinSect(Subst(HDistraction(I), w, 0)); G1=G2;
 FALSE
 -------------------------------
   G1;G2;
 Ideal(x^5, x^4y, x^4z, x^3y^2, x^3yz, x^3z^3, x^2y^5)
 -------------------------------
 Ideal(x^5, x^4y, x^4z, x^3y^2, x^2y^3)
 -------------------------------
```

So what is true?

CoCoA gave a great many examples where the above equality was true, if we used **`DegRevLex`**. Finally, we were able to prove the following:

Theorem *Let I be a strongly stable monomial ideal in the polynomial ring P, and let $\mathcal{L}$ be a distraction matrix. Then*

$$\mathrm{gin}_{\mathrm{drl}}(D_{\mathcal{L}}(I)) = I$$

The hypotheses are very tight, since for instance the theorem cannot be generalized to orderings of x_n-DegRev type, nor can it be generalized to stable ideals, ...

```
Use S::=Z/(32003)[x[1..4]];

G:=[x[3]^2x[4]^2, x[2]^3]; I:=Stable(G); Gin1:=Gin(MNDistraction(I));
GinI:=Gin(I); GinI=Gin1;

FALSE
Res(S/GinI); Res(S/Gin1);
0 --> S^4(-7) --> S^18(-6) --> S^3(-4)(+)S^24(-5) --> S^4(-3)(+)S^10(-4) --> S
-------------------------------
0 --> S^4(-7) --> S^18(-6) --> S^3(-4)(+)S^24(-5) --> S^4(-3)(+)S^10(-4) --> S
-------------------------------
I;
Ideal(x[1]^2x[3]^2, x[1]x[2]x[3]^2, x[2]^2x[3]^2, x[1]x[3]^3,
x[2]x[3]^3, x[3]^4, x[1]x[3]^2x[4], x[2]x[3]^2x[4], x[3]^3x[4],
x[3]^2x[4]^2, x[1]^3, x[1]^2x[2], x[1]x[2]^2, x[2]^3)
-------------------------------


GinI;
Ideal(x[1]^3, x[1]^2x[2], x[1]x[2]^2, x[2]^3, x[1]^2x[3]^2,
x[1]x[2]x[3]^2, x[2]^2x[3]^2, x[1]^2x[3]x[4], x[1]x[3]^3, x[2]x[3]^3,
x[1]x[2]x[3]x[4], x[3]^4, x[1]x[3]^2x[4], x[1]^2x[4]^2)
-------------------------------
Gin1;
Ideal(x[1]^3, x[1]^2x[2], x[1]x[2]^2, x[2]^3, x[1]^2x[3]^2,
x[1]x[2]x[3]^2, x[2]^2x[3]^2, x[1]^2x[3]x[4], x[1]x[3]^3, x[2]x[3]^3,
x[1]x[2]x[3]x[4], x[3]^4,  x[2]^2x[3]x[4], x[1]^2x[4]^2)
-------------------------------
```

Several corollaries follow, a lot of material is under investigation. Let me show one.

Corollary *Let I be a zero-dimensional strongly stable monomial ideal in P, and let $\mathcal{L}$ be a distraction matrix which is radical for I, and whose entries are in $K[x_1, \ldots, x_n, x_{n+1}]$.*

Then $D_{\mathcal{L}}(I)$ is the ideal of a finite set of rational points in $\mathbb{P}^n_K$ such that $\operatorname{gin}_{\mathrm{drl}}(D_{\mathcal{L}}(I)) = I$.

This is not the end
or the beginning of the end,
but it is the end of the beginning.

(Sir Winston Churchill)