Algorithms for Zero-Dimensional Polynomial Systems

Hamid Rahkooy

INRIA-CNRS-LORIA, Nancy

12 June 2019

Motivation: Multi-Sequences

- Finding recurrence relations of a sequence is a classic problem
- Fibonacci Numbers: $1,\ 1,\ 2,\ 3,\ 5,\ \ldots$

$\rightsquigarrow$ $a_{n+2} - a_{n+1} - a_n = 0, \quad a_0 = a_1 = 1$

- **Multi-Sequences**

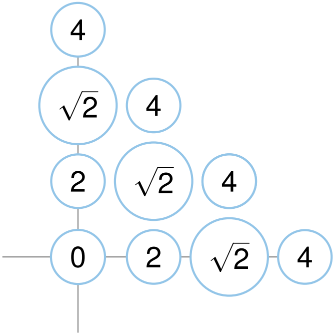
  $a_{00} = 0$

  $a_{10} = a_{01=2}$

  $a_{20} = a_{11} = a_{02} = \sqrt{2}$

  $a_{30} = a_{21} = a_{12} = a_{03} = 4$

  $\ldots$



$\rightsquigarrow$ A recurrence relation

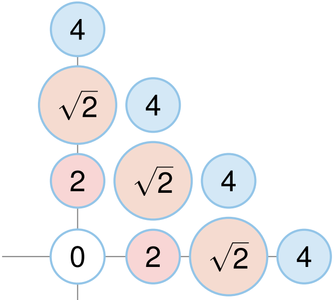
$a_{ii} - a_{jj} = 0, \ i \neq j$

An Algebraic Approach to Multi-Sequences

- An algebraic definition for the Fibonacci Sequence:
  $1 \to x^0,\ 1 \to x,\ 2 \to x^2,\ 3 \to x^3, \dots$

$\rightsquigarrow$ Recurrence Relation:
  $1+x = x^2,\ \ x+x^2 = x^3 = x(1+x+x^2),\ \ x^2(1+x+x^2),\ \ \dots$

- An algebraic definition of the multi-sequence:



- $x \to 2, y \to 2, x^2 \to \sqrt{2}, \dots$

$\rightsquigarrow$ Recurrence Relations:

- $x - y$
- $x(x-y), y(x-y)$
- $x^2(x-y), xy(x-y), y^2(x-y)$

Computing Recurrence Relations

- Naïve/First Algorithm

$$H = \begin{array}{c} \\ 1 \\ x \\ y \\ x^2 \\ xy \\ y^2 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x & y & x^2 & xy & y^2 \end{array} \\ \begin{pmatrix} 1 & 2 & 2 & 4 & 4 & 4 \\ 2 & 4 & 4 & 0 & 0 & 0 \\ 2 & 4 & 4 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array},$$

$\leadsto$ Kernel of H gives the recurrence relations

- More sophisticated: Use algebraic/geometric structure of the the set of recurrences and apply computer algebra

A geometric Problem

Problem. Given two "curves" in the plane, find their intersection.

- A Circle $f_1 = x^2 + (y-1)^2 - 1$
- A Line $f_2 = y^2$

$\rightsquigarrow$ *Intuitively*, the intersection is a *Double Point*

$\rightsquigarrow$ *Intuitively*, the **Dimension** of the intersection is zero.

Gröbner Bases, An Algebraic Solution

- **Ideal with Basis** $\{f_1, f_2\}$**, denoted by** $I = \langle f_1, f_2 \rangle$ is the set of all linear combinations of f_1 and f_2 (e.g., $x \cdot f_1 + (x^2y + y) \cdot f_2$)

⇝ the intersection of f_1, f_2, f_3 is the same as the intersection of f_1, f_2

⇝ An ideal can have different bases:

  - $I = \left\langle f_1 = x^2 + (y-1)^2 - 1, f_2 = y^2 \right\rangle$
  - $I = \langle f_1, f_1 + f_2 \rangle$
  - $I = \langle f_1, f_2, f_1 + f_2 \rangle$

⇝ **Gröbner Bases** are the "good" bases.

Gröbner Bases

- Let $I = \langle f_1 = x^2 + (y-1)^2 - 1, f_2 = y^2 \rangle$
  1. $\{f_1, f_2\}$ is a Gröbner basis for I
  2. $\{f_1, f_1 + f_2\}$ is NOT a Gröbner basis for I
  3. $\{f_1, f_2, f_1 + f_2\}$ is a Gröbner basis for I
- Gröbner Bases were discovered by Bruno Buchberger in 1965
- Gröbner Bases has a lot of properties

$\rightsquigarrow$ they are a generalization of **Gaussian Elimination**, e.g., see the **Triangular** basis in 1.

Quotient of an Ideal

- **Quotient of I, $\mathbb{C}[X]/I$,** is the set of all polynomials **modula** polynomials in I
- The quotient is a **Vector Space**

Theorem

$\dim(I) = 0$ *iff* $\dim(\mathbb{C}[X]/I)$ *is finite*

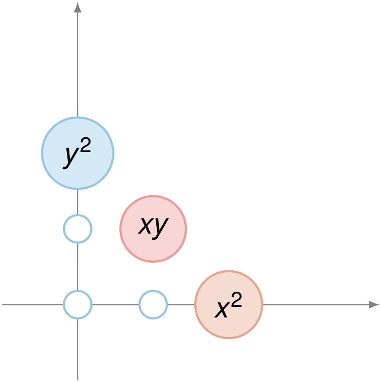
$\rightsquigarrow$ Linear algebra techniques can be used

- Finding a basis for the quotient was the PhD problem of Buchberger, given by Gröbner, which lead to the discovery of Gröbner Bases.

Quotient of Zero-Dimensional Ideals

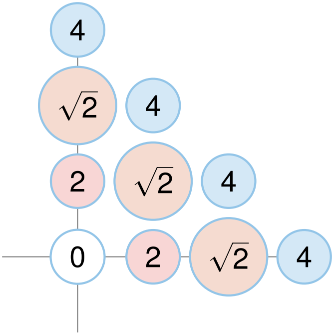
Theorem (Buchberger 1965)

One can obtain a basis for the quotient from a Gröbner basis.



- $x^2 + (y-1)^2 - 1$
- y^2
- xy

Gröbner basis of Multi-Sequences



- $x - y$
- $x(x - y), y(x - y)$
- $x^2(x - y), xy(x - y), y^2(x - y)$

$\rightsquigarrow$ Set of recurrence relations form an ideal $I = \langle x - y \rangle$

Problem. Find a Gröbner basis for the ideal of recurrences

- Multi-sequences $\longleftrightarrow$ **Dual** of the quotient of ideals

$\rightsquigarrow$ Dual of quotients: Well-known w/ fast algorithms

- Ideal of recurrences is $0-$dim iff the mult-sequence has a nice form
- Ideal of recurrences is orthogonal to the V.S. of sequences

Complexities

- n =: numb. of vars, s = numb. of given terms of the multi-sequence, $r = \dim(\mathbb{C}[x_1, \ldots, x_n]/I)$.
  Note. $s > r$

1965 [Berlekamp, Massey] The linear algebra algorithm for uni-variate case $O(s^3)$

1990 [Sakata] $O(s^3)$

1993 [Marinari, Möller, Mora] $O(nr^3)$, w/ strong assumptions

2016 [Berthomieu, Faugère] $O(s^3 + \text{smaller terms})$

2017 [Neiger, R., Schost] $O(nsBr^3)$, w/ B a certain bound to be pre-computed

2017 [Mourrain] $O(nsr^3)$

2019 [Mantzaflaris, R., Schost] $O(n(s-r)^3 + ns)$