

Principles of Solving Minimal Problems

T o m a s P a j d l a

The Art of Solving Minimal Problems

ICCV 2015 Tutorial

cmp.felk.cvut.cz/iccv-2015-minimal



Czech Technical University Prague

Center for Machine Perception



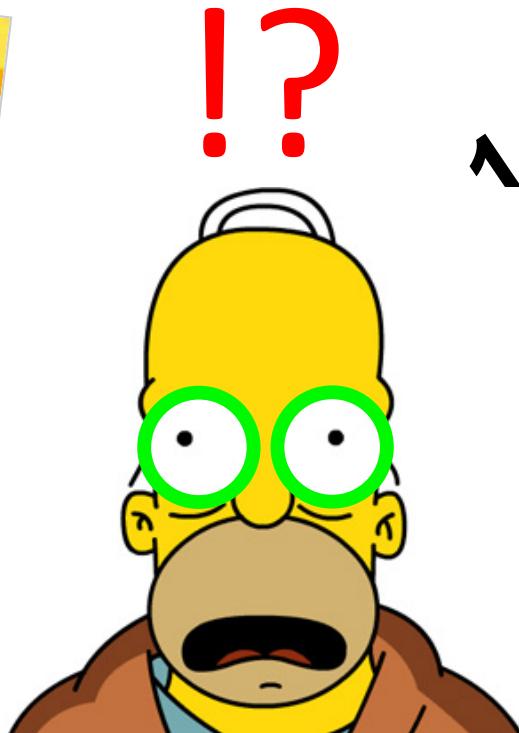
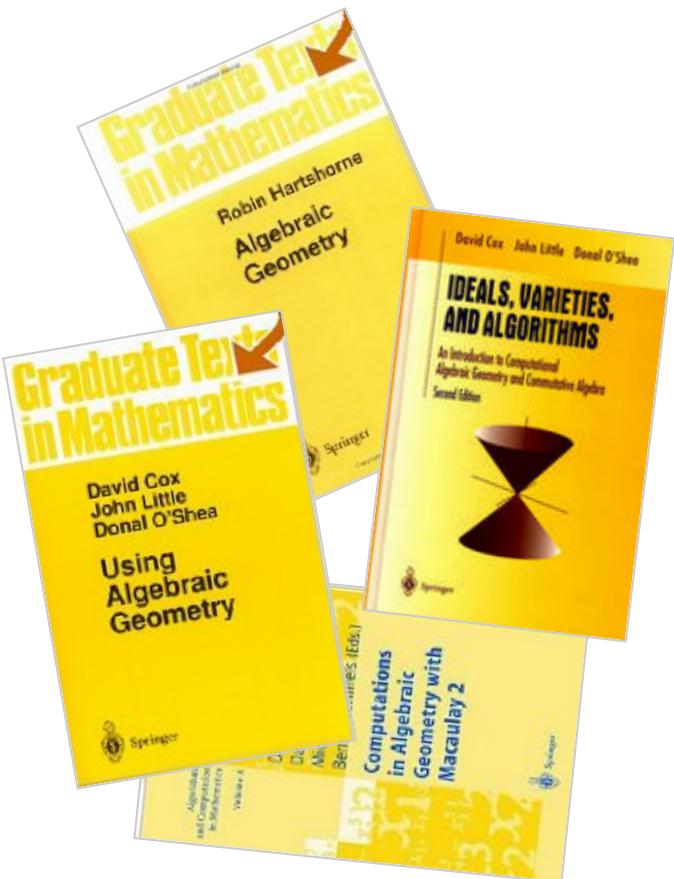
SOLVING MINIMAL PROBLEMS

Minimal problem:

use as few data as to generate a system of algebraic equations with a finite number of solutions

1. Problem formulation → algebraic equations
2. Solving algebraic equations

SOLVING ALGEBRAIC EQUATIONS

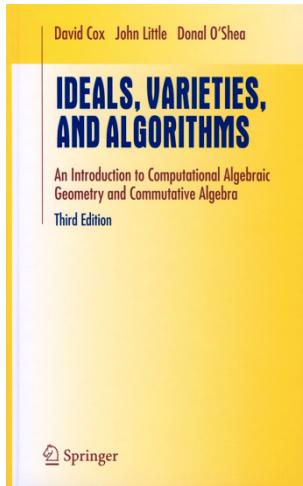


Quotient ring
 $1+1=?$
action matrix
ideal
 $xy^2+7y+..$
field



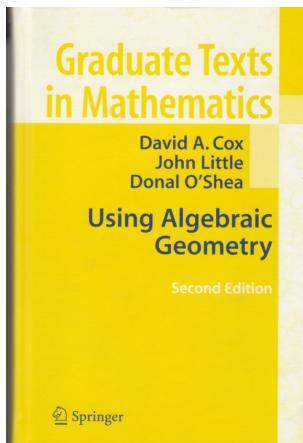
LOOKS AS “the MATHEMATICS” !!!
LET’S TAKE AN ENGINEERING APPROACH

LITERATURE



Mathematics

1. [Cox et al. Ideal Varieties and Algorithm. Springer 2015.](#)
(An Introduction to Algebraic Geometry ... New edition!)
2. [Cox et al. Using Algebraic Geometry. Springer 1998.](#)
(More advanced Algebraic Geometry)
3. F. Kubler, P. Renner, K. Schmedders.
[Computing All Solutions to Polynomial Equations in Economics](#)
(Very lightweight intro to polynomial system solving).



Minimal problem papers
cmp.felk.cvut.cz/minimal

S I N G L E U N K N O W N → E I G E N V A L U E S

1 equation, 1 variable → companion matrix → eigenvalues

$$f(x) = x^3 + 4x^2 + x - 6 = -6 + 1x + 4x^2 + 1x^3$$

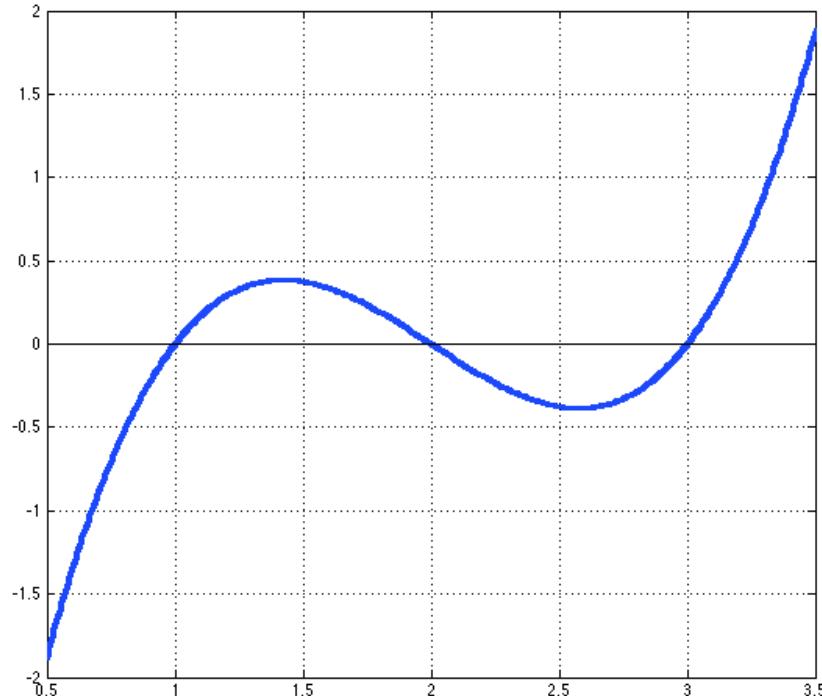
$$M_x = \begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & -1 \\ 0 & 1 & -4 \end{bmatrix}$$

... a simple rule

```
>> e=eig(M_x)
```

$$e = \begin{bmatrix} 1 \\ -2 \\ -3 \end{bmatrix} \quad x_1 = 1, x_2 = -2, x_3 = -3$$

Towards the MULTIPLICATION MATRIX M_x



a polynomial

$$\begin{aligned}f(x) &= (x - 1)(x - 2)(x - 3) \\&= x^3 - 6x^2 + 11x - 6\end{aligned}$$

with roots

$$x_1 = 1, x_2 = 2, x_3 = 3$$

i.e.

$$f(x) : f(x_1) = f(x_2) = f(x_3) = 0$$

REMAINDERS are a linear space

$r(x) = h(x) \bmod f(x)$... remainder on division by $f(x)$

$$h(x) = q(x) f(x) + r(x)$$

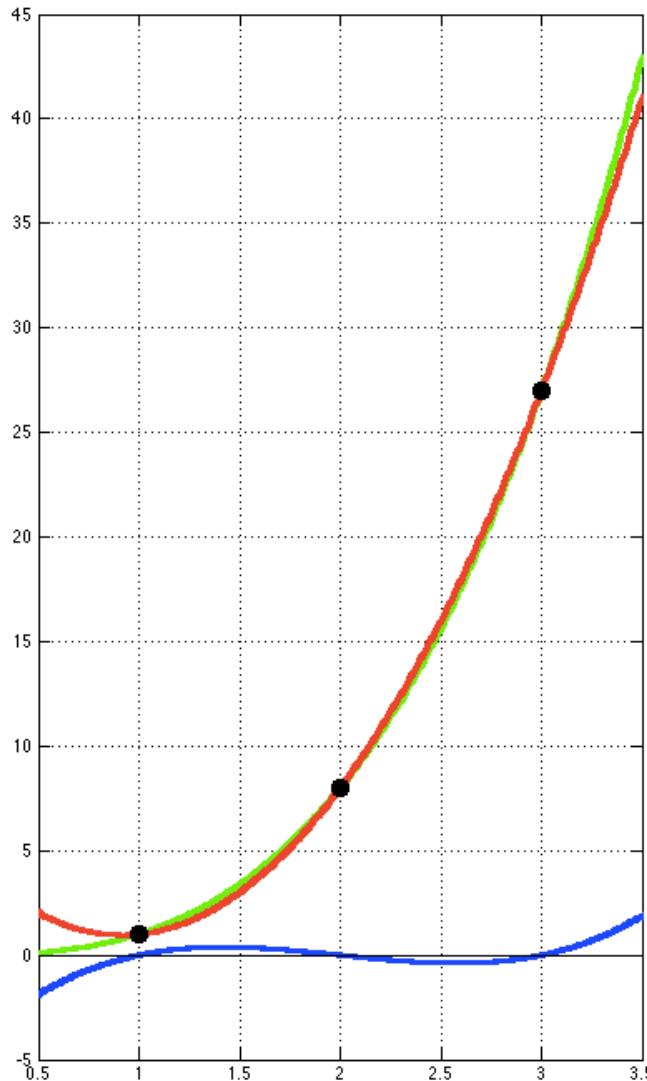
such that $\deg r(x) < \deg f(x)$ or $r(x) = 0$

- remainders have low degrees
- can be represented by finite vectors

e.g. for $f(x) = x^3 - 6x^2 + 11x - 6$ \deg of $r(x)$ is smaller than 3:

$$r(x) = a_2 x^2 + a_1 x + a_0 \equiv \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} \in \mathbb{R}^3$$

REMAINDERS evaluate



Evaluate a general polynomial $h(x)$ on
roots of $f(x)$: $x_1 = 1, x_2 = 2, x_3 = 3$
using the the remainder $r(x)$

$$\begin{aligned} h(x_i) &= q(x_i) f(x_i) + r(x_i) \\ &= q(x_i) 0 + r(x_i) = r(x_i) \end{aligned}$$

$$h(x_i) = r(x_i) \quad i = 1, 2, 3$$

Example

$$\underline{h(x) = x^3} \quad \underline{f(x) = x^3 - 6x^2 + 11x - 6}$$

$$h(x) = 1 f(x) + (6x^2 - 11x + 6)$$

$$\underline{r(x) = 6x^2 - 11x + 6}$$

MAPPING by MULTIPLICATION

Consider a mapping \mathbb{M} of polynomials to polynomials generated by multiplication by x

$$h(x) \rightarrow x h(x)$$

It generates a mapping on reminders on division by $f(x)$

$$h(x) \bmod f(x) \xrightarrow{\mathbb{M}} (x h(x)) \bmod f(x)$$

$$a_2 x^2 + a_1 x + a_0 \rightarrow b_2 x^2 + b_1 x + b_0$$

... can be seen as a mapping in the linear space of vectors of coefficients

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} \xrightarrow{\mathbb{M}} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} \dots \quad \mathbb{M}: \mathbb{R}^3 \rightarrow \mathbb{R}^3$$

... IS LINEAR

$$M: \mathbb{R}^3 \rightarrow \mathbb{R}^3 \quad h(x) \bmod f(x) \xrightarrow{M} (x \ h(x)) \bmod f(x)$$

is a LINEAR MAPPING! ... can be represented by a matrix

Example $f(x) = x^3 - 6x^2 + 11x - 6$

$$\begin{aligned} M(1) &= x \cdot 1 = x & \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \xrightarrow{M} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, & \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \xrightarrow{M} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, & \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \xrightarrow{M} \begin{bmatrix} 6 \\ -11 \\ 6 \end{bmatrix} \\ M(x) &= x \cdot x = x^2 & & & \\ M(x^2) &= x^3 \bmod f(x) & & & \\ &= 6x^2 - 11x + 6 & \begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & -11 \\ 0 & 1 & 6 \end{bmatrix} &= \begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & -11 \\ 0 & 1 & 6 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{aligned}$$

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} \xrightarrow{M} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix}$$

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} = M_x \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix}$$

FINIS CORONAT OPUS

Putting it all together

Evaluate reminder

and its image

$$\begin{array}{c} r(x_i) = a_2x_i^2 + a_1x_i + a_0 \\ \downarrow \\ x_ir(x_i) = b_2x_i^2 + b_1x_i + b_0 \\ \leftarrow \\ (x_ia_2)x_i^2 + (x_ia_1)x_i + (x_ia_0) = b_2x_i^2 + b_1x_i + b_0 \end{array}$$

For all generic
roots \rightarrow
• use monic
• use LA

$$x_i \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} x_ia_0 \\ x_ia_1 \\ x_ia_2 \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} = M_x \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix}$$

$$M_x a = x_i a$$

Roots of $f(x)$ are eigenvalues of M_x

SOLVING ALGEBRAIC EQUATIONS & GB

→ generalize remainder on division to
m equations & n vars

$$h(x, y, \dots) = q_1(x, y, \dots) f_1(x, y, \dots) + q_2(x, y, \dots) f_2(x, y, \dots) + \dots + r(x, y, \dots)$$

← divisors → remainder

For general $f_i(x, y, \dots)$ remainder $r(x, y, \dots)$ not well defined
... depends on the ordering of divisors!

→ Groebner basis ... divisors for which remainder well defined
→ does not depend on the ordering of divisors

SOLVING ALGEBRAIC EQUATIONS & GB

Linear equations are algebraic equations

linear equations

$$\begin{aligned} 4x + 8y + 7z &= 0 \\ 6x + 3y + 2z &= 0 \\ 7x + 7y + 1z &= 0 \end{aligned}$$

Gaussian elimination

$$\left[\begin{array}{ccc|c} 4 & 8 & 7 & x \\ 6 & 3 & 2 & y \\ 7 & 7 & 1 & z \end{array} \right] = 0$$

$$\left[\begin{array}{ccc|c} 4 & 8 & 7 & x \\ 0 & 36 & 34 & y \\ 0 & 0 & -167 & z \end{array} \right] = 0 \quad \xrightarrow{\hspace{10em}} \quad \begin{aligned} 4x + 8y + 7z &= 0 \\ 36y + 34z &= 0 \\ 167z &= 0 \end{aligned}$$

Groebner basis

SOLVING ALGEBRAIC EQUATIONS & GB

m equations, n variables (an example for m = 2 & n = 2)

$$\begin{aligned} 0 &= 25xy - 20y - 15x + 12 \\ 0 &= y^2 + x^2 - 1 \end{aligned}$$

→ Groebner basis

(polynomials with the same solutions but **easy** to solve
lexicographical ordering of monomials)

$$\begin{aligned} f_1 \rightarrow 0 &= 25xy - 20y - 15x + 12 \\ f_2 \rightarrow 0 &= y^2 + x^2 - 1 \\ 0 &= 125y^3 - 75y^2 + 27 - 45y \quad \leftarrow \text{how to get it ?} \\ &= (-5x - 4)f_1 + (125y - 75)f_2 \end{aligned}$$

... a polynomial combination of f_1, f_2

MATRIX FORM OF POLYNOMIALS (F4 - Like Approach)

$$f_1 = 25xy - 20y - 15x + 12$$

$$f_2 = y^2 + x^2 - 1$$

$$f_3 = (-5x - 4)f_1 + (125y - 75)f_2$$

$$\begin{aligned} f_1 &\rightarrow \begin{bmatrix} 0 & 25 & -15 & 0 & -20 & 12 \end{bmatrix} \begin{bmatrix} x^2 \\ xy \\ x \\ y^2 \\ y \\ 1 \end{bmatrix} \\ f_2 &\rightarrow \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & -1 \end{bmatrix} \end{aligned}$$

ADDING MULTIPLES

$$f_1 = 25xy - 20y - 15x + 12$$

$$f_2 = y^2 + x^2 - 1$$

$$f_3 = (-5x - 4)f_1 + (125y - 75)f_2 = a \boxed{x f_1} + b \boxed{y f_2} + c$$



$$\begin{array}{l}
 f_1 \rightarrow \left[\begin{array}{ccccccc|c} 0 & 0 & -25 & -15 & 0 & 0 & -20 & 12 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & -1 \end{array} \right] \begin{matrix} \boxed{x^2 y} \\ x^2 \\ x y \\ x \end{matrix} \\
 f_2 \rightarrow \left[\begin{array}{ccccccc|c} 0 & 1 & 0 & 0 & 0 & 1 & 0 & -1 \end{array} \right] \begin{matrix} x^2 \\ x y \\ x \end{matrix} \\
 x f_1 \rightarrow \left[\begin{array}{ccccccc|c} 25 & -15 & -20 & 12 & 0 & 0 & 0 & 0 \end{array} \right] \begin{matrix} x y \\ x \\ x \end{matrix} \\
 y f_2 \rightarrow \left[\begin{array}{ccccccc|c} 1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \end{array} \right] \begin{matrix} y^3 \\ y^2 \\ y \\ 1 \end{matrix}
 \end{array}$$

GAUSSIAN ELIMINATION

$$f_1 = 25xy - 20y - 15x + 12$$

$$f_2 = y^2 + x^2 - 1$$

$$\begin{aligned} f_3 &= (-5x - 4)f_1 + (125y - 75)f_2 = axf_1 + byf_2 + c \\ &= 125y^3 - 75y^2 - 45y + 27 \end{aligned}$$

$$\left[\begin{array}{cccc|cccc|c} 5 & -3 & -4 & \frac{12}{5} & 0 & 0 & 0 & 0 & x^2y \\ 0 & 5 & 0 & 0 & 0 & 5 & 0 & -5 & x^2 \\ 0 & 0 & 125 & -75 & 0 & 0 & -100 & 60 & xy \\ 0 & 0 & 0 & 0 & 125 & -75 & -45 & 27 & x \end{array} \right] \quad \begin{matrix} y^3 \\ y^2 \\ y \\ 1 \end{matrix}$$

Gaussian elimination

SOLVING POLYNOMIAL EQUATIONS BY CONSTRUCTING GROEBNER BASIS

A generalization of the Gaussian elimination

multiplication by scalars



multiplication by scalars & variables

PRACTICAL CASES – (10 eqns, 10 vars, deg 3)

m equations, n variables

$$f_1(x, y) = 25xy - 15x - 20y + 12$$

$$f_2(x, y) = x^2 + y^2 - 1$$

⋮

→ Groebner basis → generalized
(e.g. in grevlex ordering) companion
matrix (multiplication in $\mathbb{Q}[x_1, \dots]/I(f_1, \dots)$)

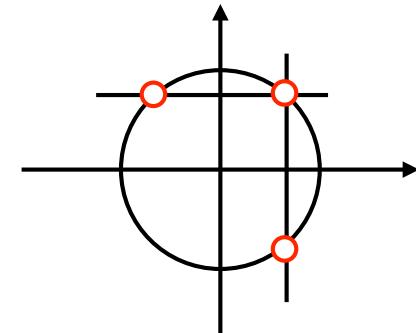
$$\mathbb{M}_{x+y} = \begin{bmatrix} 0 & 125 & 0 & 125 \\ -60 & 100 & 125 & 75 \\ -63 & 45 & 175 & 45 \\ 65 & 100 & -125 & 75 \end{bmatrix}$$

SOLVING ALGEBRAIC EQUATIONS

m equations, n variables

$$f_1(x, y) = 25xy - 15x - 20y + 12$$

$$f_2(x, y) = x^2 + y^2 - 1$$



→ Groebner basis → generalized companion matrix → eigenvectors

$$v \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ -\frac{4}{5} & \frac{4}{5} & \frac{4}{5} & \frac{4}{5} \\ \frac{3}{5} & -\frac{3}{5} & \frac{3}{5} & \frac{3}{5} \\ \frac{16}{25} & \frac{16}{25} & \frac{16}{25} & \frac{16}{25} \end{bmatrix}$$

$$\begin{aligned} x_1 &= -\frac{4}{5}, & y_1 &= \frac{3}{5} \\ x_2 &= \frac{4}{5}, & y_2 &= -\frac{3}{5} \\ x_3 &= \frac{4}{5}, & y_3 &= \frac{3}{5} \end{aligned}$$

THE DIFFICULT PART

Equations → Groebner basis



no simple rule:

1. NP-complete in m, n (~ 3-coloring of graphs)
(takes very long time to compute)
2. EXPSPACE-complete problem
(needs huge space to remember intermediate results)

HISTORY



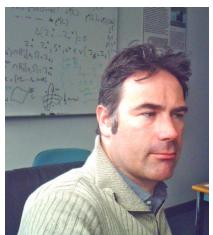
- 1888 David Hilbert: Finiteness theorem
Every ideal has a finite generating set



- 1965 Bruno Buchberger: Groebner bases
*Computational procedure for solving systems
of polynomial equations*
(Extremely simple: 20 lines of Maple code!)



- 1998 Hans Stetter: Multiplication matrix
A stable numerical procedure via eigenvectors



- 1999 Jean-Charles Faugere: F4 algorithm
An efficient computational tool for cryptography

GB COMPUTATION ALGORITHMS

1. “Standard” (Hironaka 1964) and Groebner (Burchberger 1965) bases
2. 1965: Buchberger’s algorithm
 - a generalization of the Gauss-Jordan elimination
 - extremely simple: 7 (+ 13 for the rem division) lines of code
 - not efficient
 - not good for numerical approximations
3. 1999 (2005): F4 (F5) algorithm (J.-C. Faugere)
 - more efficient, more robust, more complex

COMPUTING GB MAY BE VERY HARD

Example:

4 polynomials, 3 variables, degree ≤ 6 , small integer coeffs

$$f_1 = 8x^2y^2 + 5xy^3 + 3x^3z + x^2yz$$

$$f_2 = x^5 + 2y^3z^2 + 13y^2z^3 + 5yz^4$$

$$f_3 = 8x^3 + 12y^3 + xz^2 + 3$$

$$f_4 = 7x^2y^4 + 18xy^3z^2 + y^3z^3$$

have extremely simple Groebner basis

$$g_1 = x$$

$$g_2 = y^3 + \frac{1}{4}$$

$$g_3 = z^2$$

HOWEVER

when computed by the Buchberger's algorithm over the rational numbers w.r.t. the grevlex ordering $x > y > z$,
the following polynomial appears during the computation:

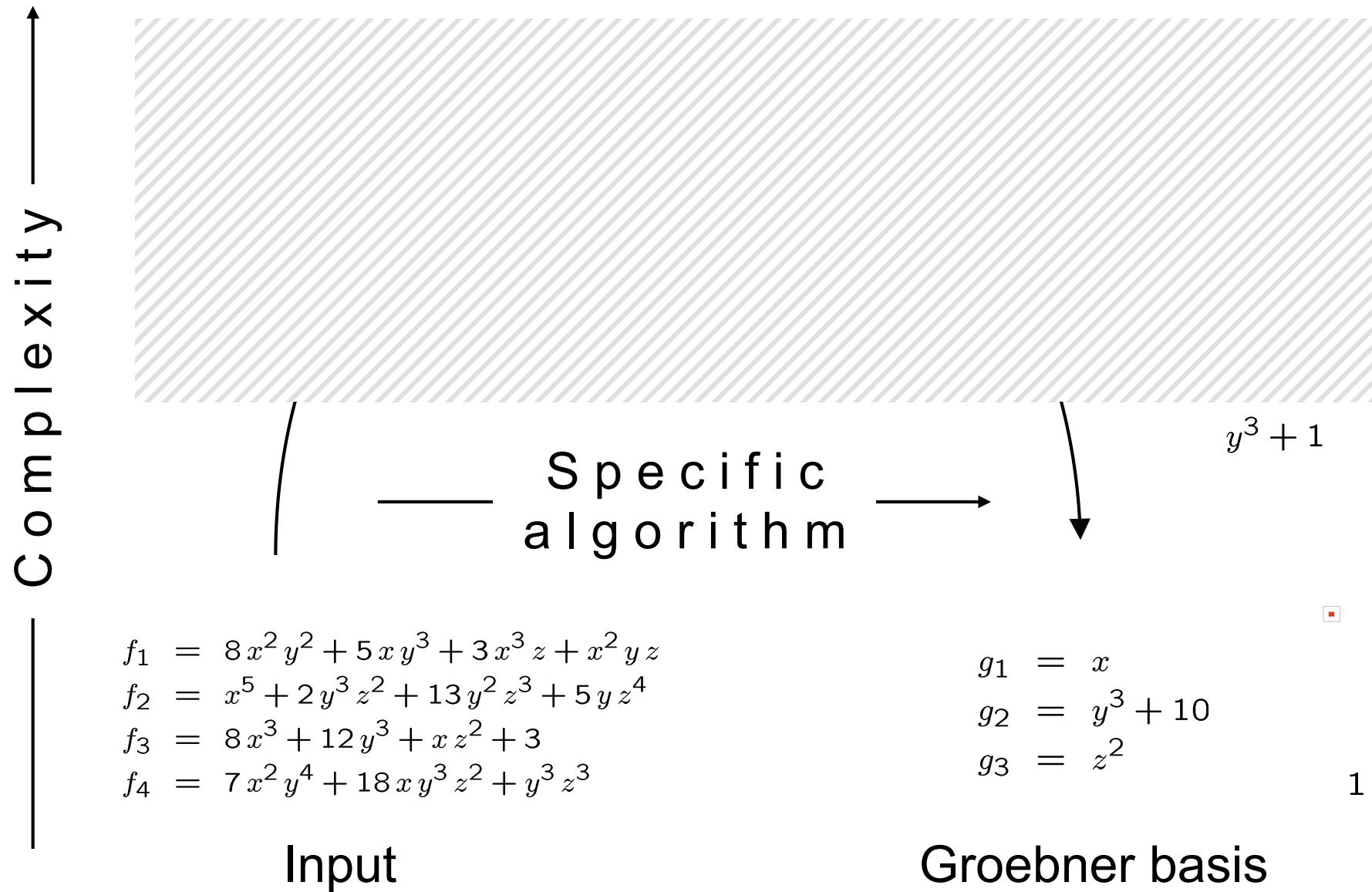
$$y^3 - 1735906504290451290764747182\dots$$



$\sim 80,000$ digits

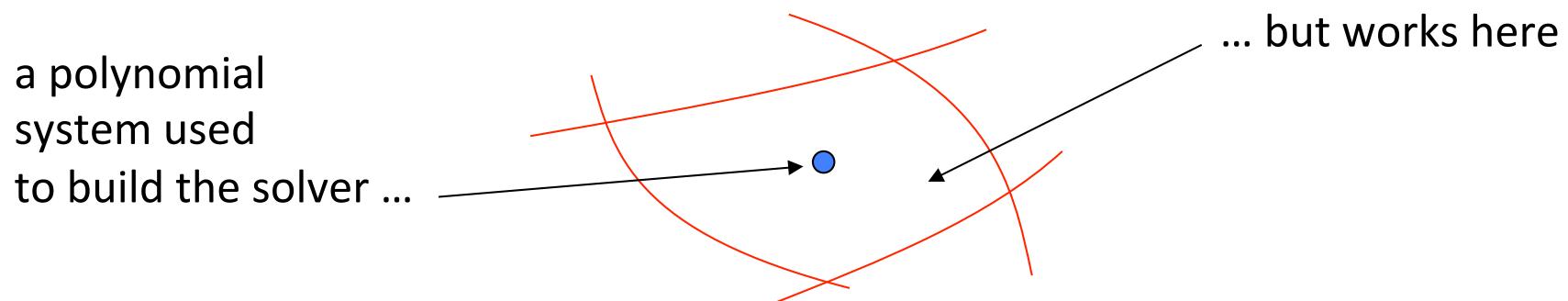
W H Y ?

General algorithms can construct all GBs but often generate many complicated polynomials



SPECIFIC GB CONSTRUCTION ALG'S

1. Find a short path towards the GB which is independent from the actual coefficients, implement it efficiently
 - Solver is made out a single concrete system and then used on other systems
 - This works around generic solutions



2. Use floating-point arithmetics to do the manipulations to avoid huge coefficients.

COMPUTATION

Macaulay2 program over the rational field \mathbb{Q}

```
R = QQ[x,y,z, MonomialOrder=>GRevLex];  
I = ideal(8*x^2*y^2 + 5*x*y^3 + 3*x^3*z + x^2*y*z,  
          x^5 + 2*y^3*z^2 + 13*y^2*z^3 + 5*y*z^4,  
          8*x^3 + 12*y^3 + x*z^2 + 3,  
          7*x^2*y^4 + 18*x*y^3*z^2 + y^3*z^3)  
G = gens gb I
```

will run very long.

The problem is in remembering very long coefficients.

COMPUTATION

Macaulay2 program over the finite field $\mathbb{Z}/13$

```
R = ZZ/13[x,y,z, MonomialOrder=>GRevLex];  
I = ideal(8*x^2*y^2 + 5*x*y^3 + 3*x^3*z + x^2*y*z,  
          x^5 + 2*y^3*z^2 + 13*y^2*z^3 + 5*y*z^4,  
          8*x^3 + 12*y^3 + x*z^2 + 3,  
          7*x^2*y^4 + 18*x*y^3*z^2 + y^3*z^3)  
G = gens gb I
```

returns a very similar basis in a fraction of second

$$\begin{array}{lcl} g_1 & = & x \\ g_2 & = & y^3 + 10 \\ g_3 & = & z^2 \end{array} \quad \left(\begin{array}{lcl} g_1 & = & x \\ g_2 & = & y^3 + \frac{1}{4} \\ g_3 & = & z^2 \end{array} \right)$$

SHORT PATH TO GB

1. Use a computer algebra system (Macaulay2) to compute the Groebner basis in a finite field (fast!) for random coefficients and remember the path:

```
R = ZZ/P[x,y,z, MonomialOrder=>GRevLex];
```



“lucky” prime number (always exists)

try $P = 1, 2, 3, 5, 7, \dots, 30011, 30013, 30029, \dots$

until the result stabilizes (always does)

2. Remember the “path of construction” and hard-code it.

FLOATING POINT ARITHMETICS

Strictly speaking, polynomial manipulations must be done in exact arithmetics

$$f_1 = 25xy + 25x + 12$$

$$f_2 = x^2y + x^2 + 3$$

$$\begin{aligned} xf_1 - 25f_2 &= x(\cancel{25xy} + \cancel{25x} + 12) - 25(\cancel{x^2y} + \cancel{x^2} + 3) \\ &= 12x - 75 \end{aligned}$$

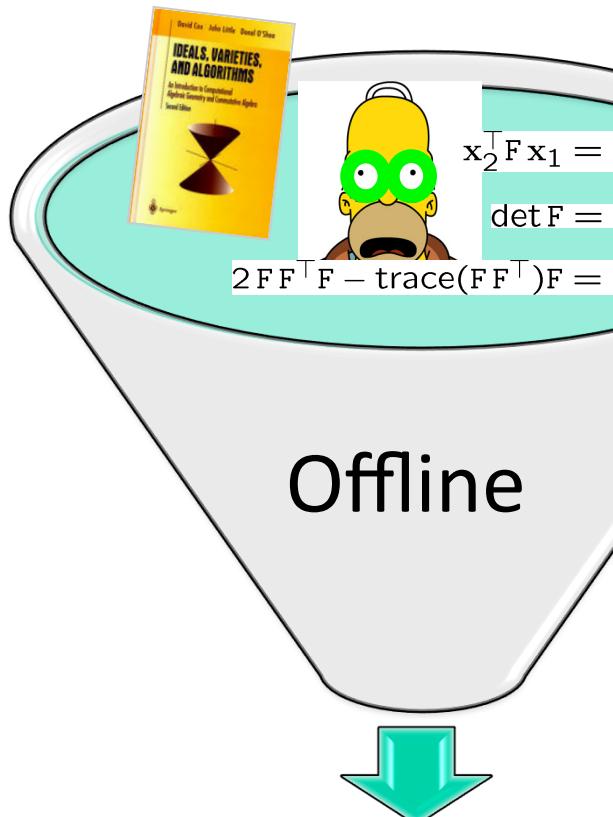
Double canceling

may fail when rounding occurs

in floating point arithmetics

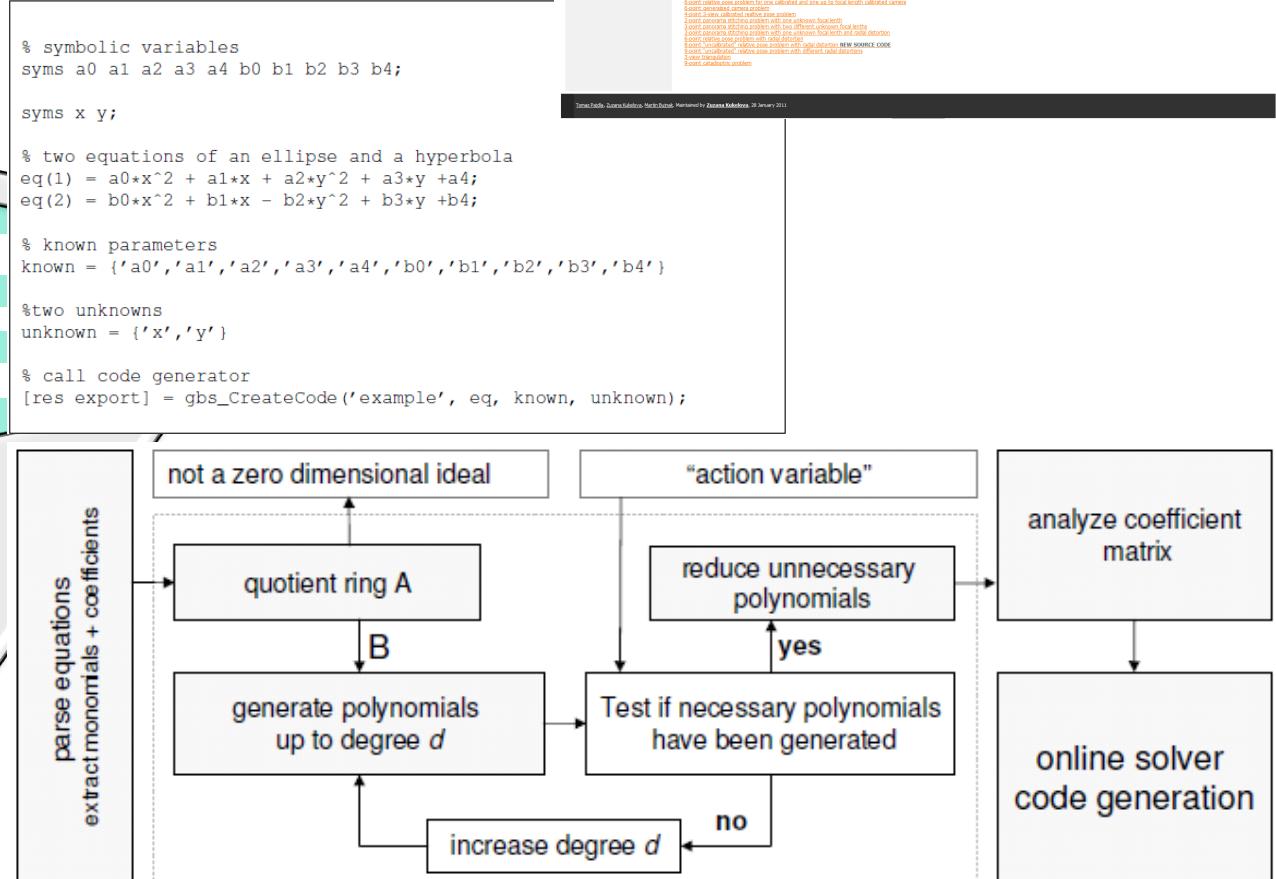
SOLVER GENERATOR

Z. Kukelova, M. Bujnak, T. Pajdla,
Automatic Generator of Minimal Problems
 ECCV 2008



Offline

Online solver



Principles of Solving Minimal Problems

T o m a s P a j d l a

The Art of Solving Minimal Problems
ICCV 2015 Tutorial



Czech Technical University Prague

Center for Machine Perception



SINGLE UNKNOWN → EIGENVALUES

Roots may be (often are) complex

1. Often, due to relaxing originally semi-algebraic problem, (i.e. including inequalities or only interest in real solutions) to an algebraic problem.
2. Sometimes many more complex than real solutions
→ waste of effort on computing them

Remedy

1. Use bracketing to look for real roots only
 - + Easy to stop as soon as sufficient accuracy reached

STURM Theorem

1. A polynomial $f(z) = 0$ in a single variable z

2. $g(z) = \frac{f(z)}{\gcd(f(z), f'(z))}$ has no multiple roots!

3. Sturm sequence

$$g_0(z) = g(z)$$

$$g_1(z) = g'(z)$$

$$g_2(z) = -\text{rem}(g_0(z), g_1(z))$$

$$g_3(z) = -\text{rem}(g_1(z), g_2(z))$$

⋮

$$g_n(z) = \text{constant}$$

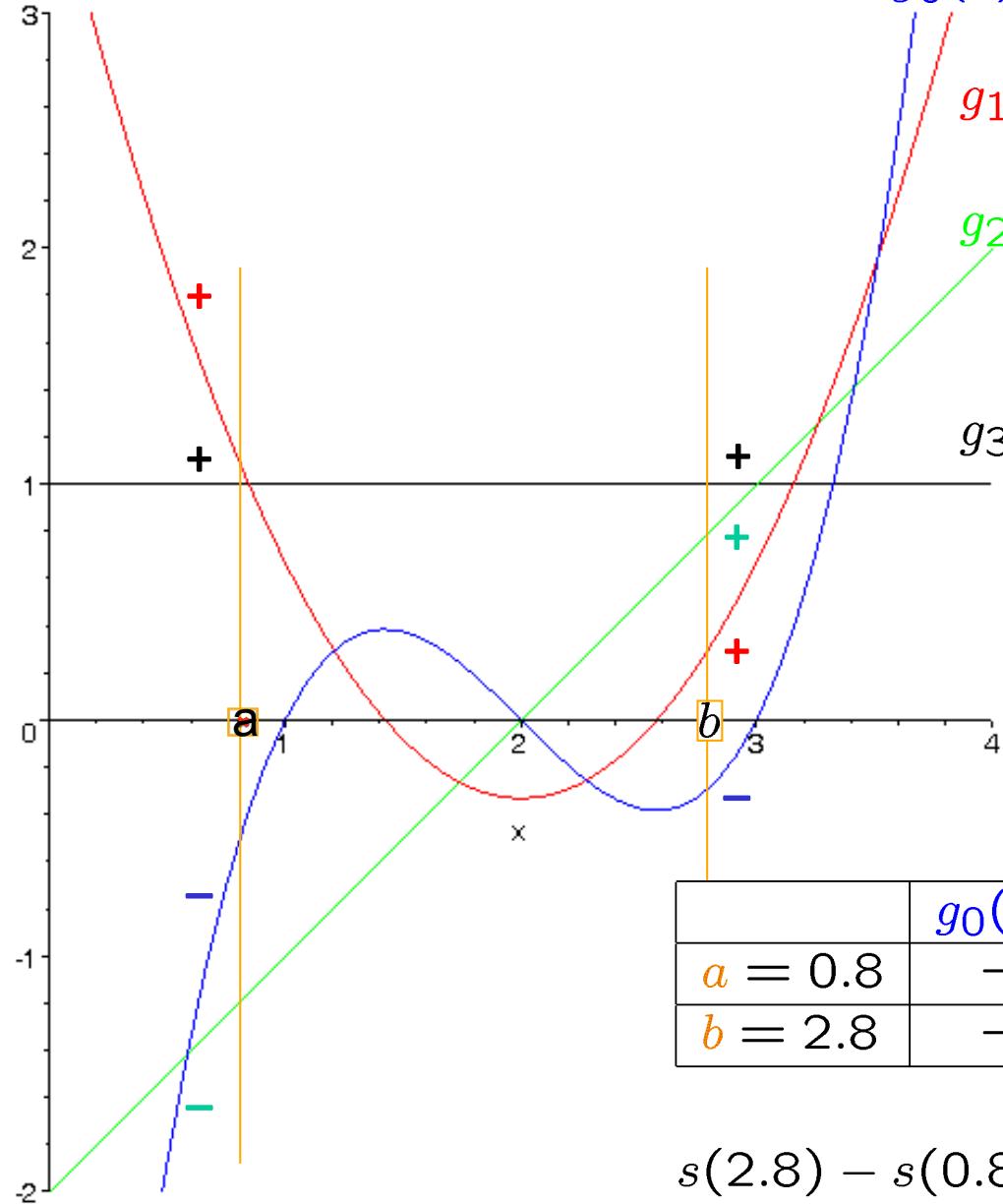
STURM Theorem

Theorem [Sturm]

- $(a, b]$... an interval in \mathbb{R}
 - s_a ... the number of sign changes in $g_0(a), g_1(a), \dots, g_n(a)$
 - s_b ... the number of sign changes in $g_0(b), g_1(b), \dots, g_n(b)$
- \Rightarrow the number of real roots in $(a, b] = s_b - s_a$

If there are roots in an interval ... split it ... test again

STURM Theorem



$$g_0(z) = f(z) = (z-1)(z-2)(z-3)$$

$$g_1(z) = f'(z) = z^2 - 4z + \frac{11}{3}$$

$$g_2(z) = -\text{rem}(g_0(z), g_1(z)) = z - 2$$

$$g_3(z) = -\text{rem}(g_1(z), g_2(z)) = 1$$

	$g_0(z)$	$g_1(z)$	$g_2(z)$	$g_3(z)$	$s(z)$
$a = 0.8$	-	+	-	+	3
$b = 2.8$	-	+	+	+	1

$$s(2.8) - s(0.8) = 3 - 1 = 2$$

S T U R M T h e o r e m

- + only real roots are computed
 - + search only roots with meaningful values
 - + precision can be controlled
- Often faster for many computer vision problems

S T U R M T h e o r e m

- + only real roots are computed
 - + search only roots with meaningful values
 - + precision can be controlled
- Often faster for many computer vision problems

Principles of Solving Minimal Problems

T o m a s P a j d l a

The Art of Solving Minimal Problems
ICCV 2015 Tutorial



Czech Technical University Prague

Center for Machine Perception

