Mathematical Principles in Visual Computing: Solving Polynomial Systems

Prof. Friedrich Fraundorfer

SS2024

Slides by Vincent Lepetit and Friedrich Fraundorfer

April 23, 2024

Polynomial Systems in Computer Vision

Many Computer Vision problems can be solved by finding the roots of a polynomial system:

- camera pose estimation from point correspondences;
- camera relative motion estimation from point correspondences;
- image distortion calibration;
- point triangulation;
- ...

Solving Polynomial Systems

- no general method;
- several mathematical tools exist. For a given problem, a tool can be more adapted than the others.

Gröbner Bases

- introduced in 1965 by Bruno Buchberger (now at the Johannes Kepler University in Linz) in his Ph.D. thesis (named after his advisor Wolfgang Gröbner) to study sets of polynomials

A Polynomial System

Let consider the following polynomial system:

$$\begin{array}{l} L_1 \\ L_2 \\ L_3 \end{array} \begin{cases} 2x^2 + y^2 - 2z + 3z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \end{cases}$$

Hint: try to remove x from the first equation

Replace L_1 by $L_1 - 2L_2$:

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \end{array} \begin{cases} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \end{cases}$$

A Real Polynomial System (continued)

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \end{array} \begin{cases} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \end{cases}$$

Hint: try to remove x from the second equation:

Adding $y^2 L_2 - L_3$:

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \end{array} \begin{cases} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \\ y^2z + 2 & = & 0 \end{cases}$$

A Real Polynomial System (continued)

$$
\begin{array}{l}
L_1' \\
L_2 \\
L_3 \\
L_4
\end{array}
\left\{
\begin{array}{rcl}
y^2 - 4z + z^2 + 5 & = & 0 \\
x^2 + z + z^2 & = & 0 \\
x^2y^2 + y^2z^2 - 2 & = & 0 \\
y^2z + 2 & = & 0
\end{array}
\right.
$$

Hint: try to remove y from the first equation

Add $zL_1' - L_4$:

$$
\begin{array}{l}
L_1' \\
L_2 \\
L_3 \\
L_4 \\
L_5
\end{array}
\left\{
\begin{array}{rcl}
y^2 - 4z + z^2 + 5 & = & 0 \\
x^2 + z + z^2 & = & 0 \\
x^2y^2 + y^2z^2 - 2 & = & 0 \\
y^2z + 2 & = & 0 \\
5z - 4z^2 + z^3 - 2 & = & 0
\end{array}
\right.
$$

A Real Polynomial System (continued)

$$
\begin{array}{l}
L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5
\end{array}
\left\{
\begin{array}{rcl}
y^2 - 4z + z^2 + 5 & = & 0 \\
x^2 + z + z^2 & = & 0 \\
x^2y^2 + y^2z^2 - 2 & = & 0 \\
y^2z + 2 & = & 0 \\
5z - 4z^2 + z^3 - 2 & = & 0
\end{array}
\right.
$$

Hint: L_5 is a polynomial in z only

$5z - 4z^2 + z^3 - 2 = (z-1)^2(z-2)$

Each possible value for z gives a new polynomial system in x and y only.

Solving a Univariate Polynomial

- closed form up to degree 4;
- for higher degrees:
  - the companion matrix method: The *companion matrix* of $p(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$ is

$$\mathbf{C} = \begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & 0 & & -a_2 \\ & & \ddots & & \vdots \\ & & & 1 & -a_{n-1} \end{bmatrix}.$$

    Its eigenvalues are the roots of $p(z)$ (because $p(z)$ is the characteristic polynomial $\det(z\mathbf{I} - \mathbf{C})$ of $\mathbf{C}$).
  - Sturm's bracketing method (slightly less stable but much faster).

Two Gröbner bases

$$\begin{array}{l} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array} \left\{ \begin{array}{rcl} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2y^2 + y^2z^2 - 2 & = & 0 \\ y^2z + 2 & = & 0 \\ 5z - 4z^2 + z^3 - 2 & = & 0 \end{array} \right.$$

$$\left\{ y^2 - 4z + z^2 + 5, x^2 + z + z^2, x^2y^2 + y^2z^2 - 2, y^2z + 2, 5z - 4z^2 + z^3 - 2 \right\}$$

is a Gröbner basis.

$$\left\{ y^2 - 4z + z^2 + 5, x^2 + z + z^2, 5z - 4z^2 + z^3 - 2 \right\}$$

is also a Gröbner basis.

A Gröbner basis is a set of polynomials $\{g_1, \ldots, g_t\}$, such that the system

$$\left\{ \begin{array}{rcl} g_1(x_1, \ldots, x_n) & = & 0 \\ & \ldots & \\ g_t(x_1, \ldots, x_n) & = & 0 \end{array} \right.$$

has the same solutions as the original one,

but with some specific properties that make the new system easier to solve than the original one, OR AT LEAST USEFUL to solve the original one.

Tools

We can create new equations from:

- linear combinations of existing equations. Gauss-Jordan elimination algorithm to simplify the system.

$$\left\{ \begin{array}{rcl} 2x^2 + xy + y^2 + 1 & = & 0 \\ x^2 - xy + 2y^2 - 1 & = & 0 \end{array} \right.$$

  in matrix form:

$$\begin{bmatrix} 2 & 1 & 1 & 1 \\ 1 & -1 & 2 & -1 \end{bmatrix} \begin{bmatrix} x^2 \\ xy \\ y^2 \\ 1 \end{bmatrix} = 0\,.$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 1 \end{bmatrix} \begin{bmatrix} x^2 \\ xy \\ y^2 \\ 1 \end{bmatrix} = 0\,.$$

- *algebraic* combinations of existing equations.

Tools

We can create new equations from:

- linear combinations of existing equations.
- *algebraic* combinations of existing equations.
- the remainder of polynomial divisions (used by Buchberger's algorithm).

Monomials

Definition. A **monomial** in $x_1, \ldots, x_n$ is a product of the form:

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots \cdot x_n^{\alpha_n},$$

where all the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers, sometimes noted $\mathbf{x}^\alpha$ with $\alpha = (\alpha_1, \ldots, \alpha_n)$.

Examples: x, x^2, x^2y, x^2yz^3

Polynomials

Definition. A **polynomial** f in $x_1, \dots, x_n$ with coefficients in a field k is a finite linear combination with coefficients in k of monomials. A polynomial is written in the form

$$f = \sum_{\alpha} a_\alpha \mathbf{x}^\alpha, \quad a_\alpha \in k$$

with

- a_α the **coefficient** of the monomial $\mathbf{x}^\alpha$.
- If $a_\alpha \neq 0$, then we call $a_\alpha \mathbf{x}^\alpha$ a **term** of f.

Monomial Order

A monomial order is any relation on the set of monomials x^α in $k[x_1, \ldots, x_n]$ satisfying:

1. $>$ is a total (linear) ordering relation:
   there is only one possible to order in increasing order under $>$ a set of monomials;
2. $>$ is compatible with multiplication:
   if $x^\alpha > x^\beta$ and x^γ is any monomial, then
   $x^\alpha x^\gamma = x^{\alpha+\gamma} > x^\beta x^\gamma = x^{\beta+\gamma}$;
3. $>$ is a well-ordering:
   every nonempty set of monomials has a smallest element under $>$.

Monomial Order on $k[x]$

The only monomial order on $k[x]$ is the degree order, given by:

$$\ldots > x^{n+1} > x^n > \ldots > x^2 > x > 1.$$

Monomial Orders on $k[x_1, \ldots, x_n]$

For polynomials in several variables, there are many choices of monomial orders.

Let's first define an order on the variables: $x_1 > x_2 > \ldots > x_n$ (this is not a monomial order), and $x > y > z$.

Monomial Orders on $k[x_1, \ldots, x_n]$ - the Lexicographic Order $>_{lex}$

Definition. The lexicographic order: analogous to the ordering of words in a dictionary.

For example, under this order $>_{lex}$:

$$x^2 >_{lex} xy^2 >_{lex} xy >_{lex} x >_{lex} y$$

Formal definition: $x^\alpha >_{lex} x^\beta$ if in the difference $\alpha - \beta$ (which belongs to $\mathbb{Z}^n$), the leftmost nonzero entry is positive.

$x^2yz^3 >_{lex} x^2z^4$ or $x^2z^4 >_{lex} x^2yz^3$?

$\rightarrow x^2yz^3 >_{lex} x^2z^4$ because $(2,1,3) - (2,0,4) = (0,\mathbf{1},-1)$

Monomial Orders on $k[x_1, \ldots, x_n]$ - the Graded Reverse Lexicographic Order $>_{grevlex}$

Let x^α and x^β be monomials in $k[x_1, \ldots, x_n]$. $x^\alpha >_{grevlex} x^\beta$ if:

- $\sum_i^n \alpha_i > \sum_i^n \beta_i$, or if
- $\sum_i^n \alpha_i = \sum_i^n \beta_i$ and in the difference $\alpha - \beta$, the *rightmost* nonzero entry is *negative*.

Under this order $>_{grevlex}$:

$$xy^2 >_{grevlex} x^2 >_{grevlex} xy >_{grevlex} x >_{grevlex} y$$

$x^2y^2z^2 >_{grevlex} xy^4z \quad$ or $\quad xy^4z >_{grevlex} x^2y^2z^2$?

$\rightarrow xy^4z >_{grevlex} x^2y^2z^2$ because $1+4+1 = 2+2+2$ and $(1,4,1) - (2,2,2) = (-1, 2, \mathbf{-1})$

Monomial Orders

$$x^3y^2z >_{lex} x^2y^6z^8$$

$$x^2y^6z^8 >_{grevlex} x^3y^2z$$

$$x^2y^2z^2 >_{lex} xy^4z$$

$$xy^4z >_{grevlex} x^2y^2z^2$$

Important property

If

- we use the monomial order $>_{lex}$ to compute a Gröbner basis and
- the solution set is finite,

then a univariate polynomial (in the last variable) is in the basis.

For example, the Gröbner basis for $\langle x^2 - y^2 + 1,\ xy - 1 \rangle$ is $\langle y^4 - y^2 - 1,\ x - y^3 + y \rangle$.

The system

$$\left\{ \begin{array}{rcl} x^2 - y^2 + 1 & = & 0 \\ xy - 1 & = & 0 \end{array} \right.$$

has the same solutions as the system:

$$\left\{ \begin{array}{rcl} y^4 - y^2 - 1 & = & 0 \\ x - y^3 + y & = & 0 \end{array} \right.$$

but the latter is much simpler to solve.

A More Ugly Example

A Gröbner basis for

$$\begin{cases} x^2 - 2xz + 5 & = & 0 \\ xy^2 + yz + 1 & = & 0 \\ 3y^2 - 8xz & = & 0 \end{cases}$$

under $>_{lex}$ is

$$\{-81 + 4320z - 86400z^2 + 766272z^3 - 2513488z^4 - 295680z^5 - 242496z^6 + 61440z^8, -2472389942760 + 1450790919y + 98722479369600z - 1312504296363936z^2 + 5756399991700688z^3 + 711670127441280z^4 + 549519027506496z^5 - 10326680985600z^6 - 139421921341440z^7, 6503592729600 + 1450790919x - 257416379643438z + 3400639490020320z^2 - 14857079919551480z^3 - 1835782187164800z^4 - 1418473727285760z^5 + 26347944960000z^6 + 359882180198400z^7\}$$