Mathematical Principles in Visual Computing: Solving Polynomial Systems Prof. Friedrich Fraundorfer SS2021

Slides by Vincent Lepetit

May 19, 2021

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

# 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





# Solving Polynomial Systems

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

 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

▲□▶ ▲□▶ ▲ □▶ ▲ □▶ □ のへぐ

### A Polynomial System

Let consider the following polynomial system:

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

(ロ)、(型)、(E)、(E)、(E)、(O)へ(C)

#### A Polynomial System

Let consider the following polynomial system:

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

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

Hint: try to remove x from the first equation

#### A Polynomial System

Let consider the following polynomial system:

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

Hint: try to remove x from the first equation Replace  $L_1$  by  $L_1 - 2L_2$ :

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

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

Hint: try to remove x from the second equation:



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

Hint: try to remove x from the second equation: Adding  $y^2L_2 - L_3$ :

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

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

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

Hint: try to remove y from the first equation



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

Hint: try to remove  $\boldsymbol{y}$  from the first equation

Add  $zL'_1 - L_4$ :

$$\begin{array}{ccccc} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array} \begin{cases} y^2 - 4z + z^2 + 5 &= & 0 \\ x^2 + z + z^2 &= & 0 \\ x^2 y^2 + y^2 z^2 - 2 &= & 0 \\ y^2 z + 2 &= & 0 \\ 5z - 4z^2 + z^3 - 2 &= & 0 \end{array}$$

(ロ)、(型)、(E)、(E)、(E)、(O)へ(C)

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

$$\begin{array}{ccccc} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array} \begin{cases} y^2 - 4z + z^2 + 5 &= & 0 \\ x^2 + z + z^2 &= & 0 \\ x^2 y^2 + y^2 z^2 - 2 &= & 0 \\ y^2 z + 2 &= & 0 \\ 5z - 4z^2 + z^3 - 2 &= & 0 \end{array}$$

◆□▶ ◆□▶ ◆ 臣▶ ◆ 臣▶ ○ 臣 ○ の Q @

Hint:  $L_5$  is a polynomial in z only

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

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.

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

closed form up to degree 4;

- closed form up to degree 4;
- for higher degrees:
  - ► the companion matrix method: The companion matrix of p(z) = z<sup>n</sup> + a<sub>n-1</sub>z<sup>n-1</sup> + ... + a<sub>1</sub>z + a<sub>0</sub> is

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

.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

- closed form up to degree 4;
- for higher degrees:
  - ► the companion matrix method: The companion matrix of p(z) = z<sup>n</sup> + a<sub>n-1</sub>z<sup>n-1</sup> + ... + a<sub>1</sub>z + a<sub>0</sub> 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(zI - C) of C).

- closed form up to degree 4;
- ► for higher degrees:
  - ► the companion matrix method: The companion matrix of p(z) = z<sup>n</sup> + a<sub>n-1</sub>z<sup>n-1</sup> + ... + a<sub>1</sub>z + a<sub>0</sub> 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(zI - C) of C).

Sturm's bracketing method (slightly less stable but much faster).

#### Two Gröbner bases

$$\begin{array}{cccc} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array} \begin{pmatrix} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2 y^2 + y^2 z^2 - 2 & = & 0 \\ y^2 z + 2 & = & 0 \\ 5z - 4z^2 + z^3 - 2 & = & 0 \end{array}$$

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

◆□▶ ◆□▶ ◆ 臣▶ ◆ 臣▶ ○ 臣 ○ の Q @

is a Gröbner basis.

#### Two Gröbner bases

$$\begin{array}{cccc} L_1' \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{array} \begin{pmatrix} y^2 - 4z + z^2 + 5 & = & 0 \\ x^2 + z + z^2 & = & 0 \\ x^2 y^2 + y^2 z^2 - 2 & = & 0 \\ y^2 z + 2 & = & 0 \\ 5z - 4z^2 + z^3 - 2 & = & 0 \end{array}$$

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

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

$$\begin{cases} g_1(x_1,...,x_n) &= 0 \\ & \dots \\ g_t(x_1,...,x_n) &= 0 \end{cases}$$

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

$$\begin{cases} g_1(x_1,\ldots,x_n) &= 0\\ \dots\\ g_t(x_1,\ldots,x_n) &= 0 \end{cases}$$

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.

We can create new equations from:

Inear combinations of existing equations.

◆□▶ ◆□▶ ◆ 臣▶ ◆ 臣▶ ○ 臣 ○ の Q @

We can create new equations from:

 linear combinations of existing equations. In particular, we can use the Gauss-Jordan elimination algorithm to simplify the system.

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

We can create new equations from:

Inear combinations of existing equations. In particular, we can use the Gauss-Jordan elimination algorithm to simplify the system. For example, we can write the system:

$$\left\{ \begin{array}{rrrr} 2x^2 + xy + y^2 + 1 & = & 0 \\ x^2 - xy + 2y^2 - 1 & = & 0 \end{array} \right. \label{eq:2.1}$$

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

in matrix form:

We can create new equations from:

Inear combinations of existing equations. In particular, we can use the Gauss-Jordan elimination algorithm to simplify the system. For example, we can write the system:

$$\left\{ \begin{array}{rrrr} 2x^2 + xy + y^2 + 1 & = & 0 \\ x^2 - xy + 2y^2 - 1 & = & 0 \end{array} \right. \label{eq:2.1}$$

in matrix form:

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

We can create new equations from:

Inear combinations of existing equations. In particular, we can use the Gauss-Jordan elimination algorithm to simplify the system. For example, we can write the system:

$$\left\{ \begin{array}{rrrr} 2x^2 + xy + y^2 + 1 & = & 0 \\ x^2 - xy + 2y^2 - 1 & = & 0 \end{array} \right. \label{eq:2.1}$$

in matrix form:

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

After Gauss-Jordan elimination:

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

We can create new equations from:

- Inear combinations of existing equations.
- algebraic combinations of existing equations.

We can create new equations from:

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

#### Monomials

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

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ● ●

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

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

▲□▶▲□▶▲≡▶▲≡▶ ≡ めぬる

with

•  $a_{\alpha}$  the **coefficient** of the monomial  $\mathbf{x}^{\alpha}$ .

#### Polynomials

**Definition.** A polynomial f in  $x_1, \ldots, x_n$  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

- $a_{\alpha}$  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.

Notations:  $k[x_1, \ldots, x_n]$ 

**Notation.** The set of all polynomials in  $x_1, \ldots, x_n$  with coefficients in k is denoted  $k[x_1, \ldots, x_n]$ .
**Notation.** The set of all polynomials in  $x_1, \ldots, x_n$  with coefficients in k is denoted  $k[x_1, \ldots, x_n]$ .

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

k[x] is the set of polynomials in one variable:  $x^2-x \in k[x]$  ,  $x^3+4x \in k[x].$ 

**Notation.** The set of all polynomials in  $x_1, \ldots, x_n$  with coefficients in k is denoted  $k[x_1, \ldots, x_n]$ .

k[x] is the set of polynomials in one variable:  $x^2-x \in k[x],$   $x^3+4x \in k[x].$ 

k[x,y] is the set of polynomials in two variables:  $x^2-y \in k[x,y],$   $x^3+2xy+y^2 \in k[x,y].$ 

# Definition - Leading Term LT(f)

**Definition.** Given a nonzero polynomial  $f \in k[x]$ , let

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m \,$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

where  $a_i \in k$  and  $a_0 \neq 0$ .

# Definition - Leading Term LT(f)

**Definition.** Given a nonzero polynomial  $f \in k[x]$ , let

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m \,$$

where  $a_i \in k$  and  $a_0 \neq 0$ .

 $a_0 x^m$  is called the *leading term* of f.

# Definition - Leading Term LT(f)

**Definition.** Given a nonzero polynomial  $f \in k[x]$ , let

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m \,$$

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

where  $a_i \in k$  and  $a_0 \neq 0$ .

 $a_0 x^m$  is called the *leading term* of f.

We will write  $LT(f) = a_0 x^m$ .

# Dividing Multivariate Polynomials?

Is there a division for polynomials in several variables?

# Dividing Multivariate Polynomials?

Is there a division for polynomials in several variables?

The answer is yes, but we need to decide which term of a polynomial is the leading term.

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

Is there a division for polynomials in several variables?

The answer is yes, but we need to decide which term of a polynomial is the leading term.

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

For example, what is the leading term of  $x^2 + xy + y^2$ ?

Is there a division for polynomials in several variables?

The answer is yes, but we need to decide which term of a polynomial is the leading term.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

For example, what is the leading term of  $x^2 + xy + y^2$ ?

To decide, we will define a monomial order.

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

A monomial order is any relation on the set of monomials  $x^{\alpha}$  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;

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

A monomial order is any relation on the set of monomials  $x^{\alpha}$  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:

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

 $\begin{array}{ll} 1. > \mbox{is a total (linear) ordering relation:} \\ \mbox{there is only one possible to order in increasing order under} > \\ \mbox{a set of monomials;} \end{array}$ 

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

2. > is compatible with multiplication:  
if 
$$x^{\alpha} > x^{\beta}$$
 and  $x^{\gamma}$  is any monomial, then  
 $x^{\alpha}x^{\gamma} = x^{\alpha+\gamma} > x^{\beta}x^{\gamma} = x^{\beta+\gamma}$ ;

A monomial order is any relation on the set of monomials  $x^{\alpha}$  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  $x^{\gamma}$  is any monomial, then  $x^{\alpha}x^{\gamma} = x^{\alpha+\gamma} > x^{\beta}x^{\gamma} = x^{\beta+\gamma}$ ;
- 3. > is a well-ordering:

A monomial order is any relation on the set of monomials  $x^{\alpha}$  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  $x^{\gamma}$  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 >.

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

A monomial order is any relation on the set of monomials  $x^{\alpha}$  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  $x^{\gamma}$  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:

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

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

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

# 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.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

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

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

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

**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.

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

**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.

$$\begin{split} &x^2yz^3>_{lex}x^2z^4 \quad \text{or} \quad x^2z^4>_{lex}x^2yz^3 \ ? \\ &\to x^2yz^3>_{lex}x^2z^4 \ \text{because} \ (2,1,3)-(2,0,4)=(0,\mathbf{1},-1) \end{split}$$

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

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

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

 $\blacktriangleright \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$ , or if



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

• 
$$\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$$
, or if

•  $\sum_{i=1}^{n} \alpha_{i} = \sum_{i=1}^{n} \beta_{i}$  and in the difference  $\alpha - \beta$ , the *rightmost* nonzero entry is *negative*.

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

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

$$\blacktriangleright \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$$
, or if

•  $\sum_{i=1}^{n} \alpha_{i} = \sum_{i=1}^{n} \beta_{i}$  and in the difference  $\alpha - \beta$ , the *rightmost* nonzero entry is *negative*.

Under this order  $>_{grevlex}$ :

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

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

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

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

$$\blacktriangleright \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$$
, or if

•  $\sum_{i=1}^{n} \alpha_{i} = \sum_{i=1}^{n} \beta_{i}$  and in the difference  $\alpha - \beta$ , the *rightmost* nonzero entry is *negative*.

Under this order  $>_{grevlex}$ :

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

$$x^2y^2z^2>_{grevlex}xy^4z$$
 or  $xy^4z>_{grevlex}x^2y^2z^2$ ?  
 $\rightarrow xy^4z>_{grevlex}x^2y^2z^2$  because  $1+4+1=2+2+2$  and

▲□▶▲□▶▲□▶▲□▶ = のへの

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

$$\blacktriangleright \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$$
, or if

•  $\sum_{i=1}^{n} \alpha_{i} = \sum_{i=1}^{n} \beta_{i}$  and in the difference  $\alpha - \beta$ , the *rightmost* nonzero entry is *negative*.

Under this order  $>_{grevlex}$ :

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

$$\begin{array}{ll} x^2y^2z^2 >_{grevlex} xy^4z & \text{or} & xy^4z >_{grevlex} x^2y^2z^2 \end{array} ? \\ \rightarrow xy^4z >_{grevlex} x^2y^2z^2 \text{ because } 1+4+1=2+2+2 \text{ and} \\ (1,4,1)-(2,2,2)=(-1,2,-1) \end{array}$$

ション・ 山田・ 山田・ 山田・ 山田・

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

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

◆□ ▶ ◆□ ▶ ◆三 ▶ ◆□ ▶ ◆□ ▶

#### Why Several Orders?

Computing Gröbner bases with  $>_{grevlex}$  is usually more efficient.

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

Computing Gröbner bases with  $>_{grevlex}$  is usually more efficient. Computing Gröbner bases with  $>_{lex}$  yields a polynomial system that can be easily solved.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

#### Cool If

- $\blacktriangleright$  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.

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

#### Cool If

- we use the monomial order ><sub>lex</sub> 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  $\left\langle x^2-y^2+1,\;xy-1\right\rangle$  is  $\left\langle y^4-y^2-1,\;x-y^3+y\right\rangle.$ 

#### Cool If

- we use the monomial order ><sub>lex</sub> 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

$$\begin{cases} x^2 - y^2 + 1 &= 0\\ xy - 1 &= 0 \end{cases}$$

has the same solutions as the system:

$$\begin{cases} y^4 - y^2 + -1 &= 0\\ x - y^3 + y &= 0 \end{cases}$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

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



#### 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

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

## Algorithms to Compute a Gröbner basis

First algorithm to compute a Gröbner basis: the Buchberger algorithm.

More recent algorithms are more efficient (F4 and F5 algorithms by Faugère).

In (Kukelova, 2008):

- 1. Start with  $d \leftarrow 1$ ;
- 2. Multiply each equation of the current system by every possible monomial of degree *d*;

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

- 3. Simplify the system with Gauss-Jordan elimination;
- 4. If not a Gröbner basis, set  $d \leftarrow d+1$ , and iterate from 1.

#### Computation Steps for (Stewenius, 2005)



Sac

- Unfortunately, computation of Gröbner bases under the lexicographic ordering ( $>_{lex}$ ) is often intractable for real problems.
- Using the graded reverse lexicographical ordering (  $>_{grevlex}$  ) usually yields more tractable computations.

Unfortunately, the resulting polynomial system is not necessarily easy to solve.

Fortunately, other properties of Gröbner bases can be used to find the solutions.

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

 $>_{lex}$  versus  $>_{grevlex}$ : Example

Computing a Gröbner basis for

$$\begin{cases} d_1^2 + Ad_1d_2 + d_2^2 - F^2 &= 0\\ d_1^2 + Bd_1d_3 + d_3^2 - F^2 &= 0\\ d_2^2 + Cd_2d_3 + d_3^2 - G^2 &= 0\\ d_2^2 + Dd_2d_4 + d_4^2 - F^2 &= 0\\ d_3^2 + Ed_3d_4 + d_4^2 - F^2 &= 0 \end{cases}$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

under  $>_{grevlex}$ : less than a second (but 130 polynomials in a 96Kb text file).

under  $>_{lex}$ : more than a week

### Further Reading and References I

- M. Byröd, K. Josephson, and K. Åström. Fast and Stable Polynomial Equation Solving and its Application to Computer Vision. 2009.
- D.A. Cox, J.B. Little, and D. O'Shea. Using Algebraic Geometry. Springer, 2005.
- D.A. Cox, J.B. Little, and D. O'Shea. Ideals, Varieties, and Algorithms. Springer, 2007.
- Z. Kukelova, M. Bujnak, and T. Pajdla.
  Automatic Generator of Minimal Problem Solvers.
  In European Conference on Computer Vision, 2008.

# Further Reading and References II

Z. Kukelova, M. Bujnak, and T. Pajdla. Polynomial Eigenvalue Solutions to Minimal Problems in Computer Vision.

*IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2012.

H. Li and R. Hartley.

Five-Point Motion Estimation Made Easy. In International Conference on Pattern Recognition, 2006.

D. Nister.

An Efficient Solution to the Five-Point Relative Pose Problem. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2004.

H. Stewénius, F. Schaffalitzky, and D. Nistér. How Hard Is Three-View Triangulation Really? In International Conference on Computer Vision, 2005.