New Algorithms for Decomposing Algebraic Sets

Rafael Mohr

joint with Christian Eder, Pierre Lairez and Mohab Safey El Din

DRN + EFI Conference

13.06.2024

Rheinland-Pfälzische Technische Universität Kaiserslautern Landau

Introduction

Let $\mathbb{K}$ be a field, $R := \mathbb{K}[x_1, \ldots, x_n]$, $\overline{\mathbb{K}}$ algebraic closure.
$f_1, \ldots, f_r \in R$, $X := V(f_1, \ldots, f_r) := \{f_1 = f_2 = \cdots = f_r = 0\} \subset \overline{\mathbb{K}}^n$ *algebraic set.*

Let $\mathbb{K}$ be a field, $R := \mathbb{K}[x_1, \ldots, x_n]$, $\overline{\mathbb{K}}$ algebraic closure.
$f_1, \ldots, f_r \in R$, $X := V(f_1, \ldots, f_r) := \{f_1 = f_2 = \cdots = f_r = 0\} \subset \overline{\mathbb{K}}^n$ *algebraic set.*

Theorem

X can be written uniquely

$$X = \bigcup_{i=1}^{r} X_i$$

with each X_i a $\mathbb{K}$-*irreducible* algebraic set (X_i *irreducible components*).

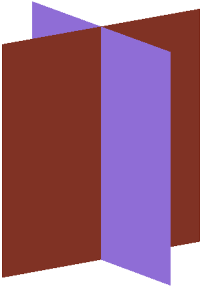
Let $\mathbb{K}$ be a field, $R := \mathbb{K}[x_1, \ldots, x_n]$, $\overline{\mathbb{K}}$ algebraic closure.
$f_1, \ldots, f_r \in R$, $X := V(f_1, \ldots, f_r) := \{f_1 = f_2 = \cdots = f_r = 0\} \subset \overline{\mathbb{K}}^n$ *algebraic set.*

Theorem

X can be written uniquely

$$X = \bigcup_{i=1}^{r} X_i$$

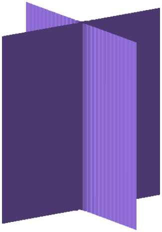
with each X_i a $\mathbb{K}$-*irreducible* algebraic set (X_i *irreducible components*).



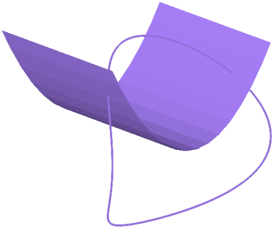
$X = V(xy) = V(x) \cup V(y)$

Definition

$X \subset \overline{\mathbb{K}}^n$ equidimensional if all irreducible components of X have the same dimension.



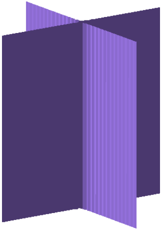
equidimensional



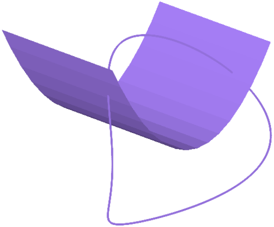
not equidimensional

Definition

$X \subset \overline{\mathbb{K}}^n$ equidimensional if all irreducible components of X have the same dimension.



equidimensional



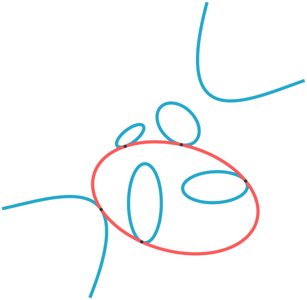
not equidimensional

Given X as $X = V(f_1, \ldots, f_r)$ with $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_n]$,

compute a representation $X = \bigcup_{i=1}^{m} X_i$, each X_i equidimensional.

Steiner problem: How many conics are tangent to 5 general conics?

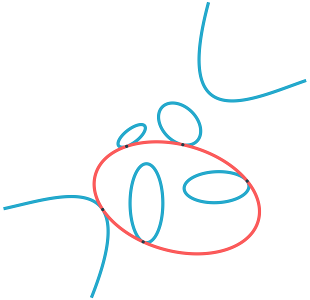
Steiner problem: How many conics are tangent to 5 general conics?



conic: cut out by polynomial of degree 2 in 2 variables

`juliahomotopycontinuation.org/3264/`

Steiner problem: How many conics are tangent to 5 general conics?



juliahomotopycontinuation.org/3264/

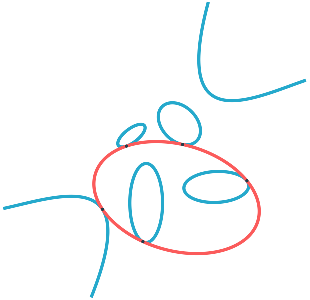
conic: cut out by polynomial of degree 2 in 2 variables

Tangency conditions via Jacobian criterion

$\Downarrow$

Polynomial System S in 5 equations, 5 variables

Steiner problem: How many conics are tangent to 5 general conics?



juliahomotopycontinuation.org/3264/

conic: cut out by polynomial of degree 2 in 2 variables

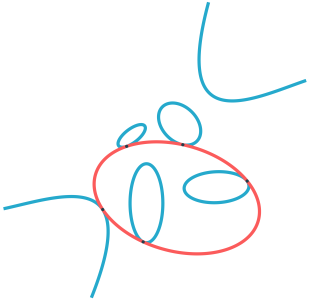
Tangency conditions via Jacobian criterion

$\Downarrow$

Polynomial System S in 5 equations, 5 variables

We expect $V(S)$ to have finitely many solutions.

Steiner problem: How many conics are tangent to 5 general conics?



juliahomotopycontinuation.org/3264/

conic: cut out by polynomial of degree 2 in 2 variables

Tangency conditions via Jacobian criterion

$\Downarrow$

Polynomial System S in 5 equations, 5 variables

We expect $V(S)$ to have finitely many solutions.

Problem: $V(S)$ has 2-dimensional component corresponding to squares of linear forms! $\rightsquigarrow$ degenerate solutions

Will work with an ideal $I \subset R$ s.t. $V(I) = X$.

Will work with an ideal $I \subset R$ s.t. $V(I) = X$.

Let $\prec$ be a *monomial order* on R.

Will work with an ideal $I \subset R$ s.t. $V(I) = X$.

Let $\prec$ be a *monomial order* on R.

$\rightsquigarrow$ notion of *leading monomial* $\operatorname{lm}(f)$ for each $f \in R$.

Will work with an ideal $I \subset R$ s.t. $V(I) = X$.

Let $\prec$ be a *monomial order* on R.

$\rightsquigarrow$ notion of *leading monomial* $\mathrm{lm}(f)$ for each $f \in R$.

Main algorithmic tool:

Definition

Gröbner basis G of ideal I w.r.t $\prec$:

Finite set $G \subset I$ s.t.

$$\langle \mathrm{lm}(G) \rangle = \mathrm{lm}(I).$$

Will work with an ideal $I \subset R$ s.t. $V(I) = X$.

Let $\prec$ be a *monomial order* on R.

$\rightsquigarrow$ notion of *leading monomial* $\mathrm{lm}(f)$ for each $f \in R$.

Main algorithmic tool:

Definition

Gröbner basis G of ideal I w.r.t $\prec$:

Finite set $G \subset I$ s.t.

$$\langle \mathrm{lm}(G) \rangle = \mathrm{lm}(I).$$

$\Downarrow$

Ideal membership via polynomial long division

Will work with an ideal $I \subset R$ s.t. $V(I) = X$.

Let $\prec$ be a *monomial order* on R.

$\rightsquigarrow$ notion of *leading monomial* $\operatorname{lm}(f)$ for each $f \in R$.

Main algorithmic tool:

Definition

Gröbner basis G of ideal I w.r.t $\prec$:

Finite set $G \subset I$ s.t.

$$\langle \operatorname{lm}(G) \rangle = \operatorname{lm}(I).$$

$$\Downarrow$$

Ideal membership via polynomial long division

triangular sets (e.g. Hubert 2003) and geometric resolutions (e.g. Giusti, Lecerf, and Salvy 2001)...

The Incremental Strategy

To decompose $V(f_1, \ldots, f_r)$:

To decompose $V(f_1, \dots, f_r)$:

$$\boxed{V(f_1)} \xrightarrow{\text{Dec. } V(f_1, f_2)} \boxed{V(f_1, f_2) = \bigcup_i X_i} \xrightarrow{\text{Dec. each } X_i \cap V(f_3)} \boxed{V(f_1, f_2, f_3) = \bigcup_i \bigcup_j X_{ij}}$$

To decompose $V(f_1, \ldots, f_r)$:

$$\boxed{V(f_1)} \xrightarrow{\text{Dec. } V(f_1, f_2)} \boxed{V(f_1, f_2) = \bigcup_i X_i} \xrightarrow{\text{Dec. each } X_i \cap V(f_3)} \boxed{V(f_1, f_2, f_3) = \bigcup_i \bigcup_j X_{ij}}$$

To decompose $V(f_1, \ldots, f_r)$:

$$\boxed{V(f_1)} \xrightarrow{\text{Dec. } V(f_1, f_2)} \boxed{V(f_1, f_2) = \bigcup_i X_i} \xrightarrow{\text{Dec. each } X_i \cap V(f_3)} \boxed{V(f_1, f_2, f_3) = \bigcup_i \bigcup_j X_{ij}}$$

To decompose $V(f_1, \ldots, f_r)$:

$$\boxed{V(f_1)} \xrightarrow{\text{Dec. } V(f_1, f_2)} \boxed{V(f_1, f_2) = \bigcup_i X_i} \xrightarrow{\text{Dec. each } X_i \cap V(f_3)} \boxed{V(f_1, f_2, f_3) = \bigcup_i \bigcup_j X_{ij}}$$

Have reduced to:

Given X equidimensional, $f \in \mathbb{K}[x_1, \ldots, x_n]$

Compute equidimensional decomposition of $X \cap V(f)$

To decompose $V(f_1, \dots, f_r)$:

$$\boxed{V(f_1)} \xrightarrow{\text{Dec. } V(f_1, f_2)} \boxed{V(f_1, f_2) = \bigcup_i X_i} \xrightarrow{\text{Dec. each } X_i \cap V(f_3)} \boxed{V(f_1, f_2, f_3) = \bigcup_i \bigcup_j X_{ij}}$$

Have reduced to:

Given X equidimensional, $f \in \mathbb{K}[x_1, \dots, x_n]$

Compute equidimensional decomposition of $X \cap V(f)$

Frequently used in other algorithms, e.g. (Lecerf 2003), (Moroz 2008), (Duff, Leykin, and Rodriguez 2022)...

$X \subset \overline{\mathbb{K}}^n$ equidimensional, $f \in \mathbb{K}[x_1, \ldots, x_n]$.

$X \subset \overline{\mathbb{K}}^n$ equidimensional, $f \in \mathbb{K}[x_1, \ldots, x_n]$.

$$Y \text{ irreducible component of } X \Rightarrow \begin{cases} f|_Y = 0 \textbf{ or} \\ f|_Y \text{ generically } \neq 0 \end{cases}$$

$X \subset \overline{\mathbb{K}}^n$ equidimensional, $f \in \mathbb{K}[x_1, \ldots, x_n]$.

$$Y \text{ irreducible component of } X \Rightarrow \begin{cases} f|_Y = 0 \textbf{ or} \\ f|_Y \text{ generically } \neq 0 \end{cases}$$

Example

$X = V(xy, xz, yz), f = x(x-1)$.

$X \subset \overline{\mathbb{K}}^n$ equidimensional, $f \in \mathbb{K}[x_1, \ldots, x_n]$.

Y irreducible component of $X \Rightarrow \begin{cases} f|_Y = 0 \text{ **or** } \\ f|_Y \text{ generically } \neq 0 \end{cases}$

Example

$X = V(xy, xz, yz), f = x(x-1)$.

X	$X_1 = V(x, y)$	$X_2 = V(x, z)$	$X_3 = V(y, z)$
	$f = 0$	$f = 0$	$f \neq 0$

$X \subset \overline{\mathbb{K}}^n$ equidimensional, $f \in \mathbb{K}[x_1, \ldots, x_n]$.

$$Y \text{ irreducible component of } X \Rightarrow \begin{cases} f|_Y = 0 \textbf{ or} \\ f|_Y \text{ generically } \neq 0 \end{cases}$$

Example

$X = V(xy, xz, yz), f = x(x-1)$.

X	$X_1 = V(x, y)$	$X_2 = V(x, z)$	$X_3 = V(y, z)$
	$f = 0$	$f = 0$	$f \neq 0$

$$X \cap V(f) = \underbrace{[V(x, y) \cup V(x, z)]}_{\text{dim=1}} \cup \underbrace{[V(y, z, x(x-1))]}_{\text{dim=0}}$$

$X \subset \overline{\mathbb{K}}^n$ equidimensional, $f \in \mathbb{K}[x_1, \ldots, x_n]$.

$$Y \text{ irreducible component of } X \Longrightarrow \begin{cases} f|_Y = 0 \textbf{ or} \\ f|_Y \text{ generically } \neq 0 \end{cases}$$

Example

$X = V(xy, xz, yz), f = x(x-1)$.

X	$X_1 = V(x, y)$	$X_2 = V(x, z)$	$X_3 = V(y, z)$
	$f = 0$	$f = 0$	$f \neq 0$

Definition

Regular Intersection: $f|_Y \neq 0$ for every irred. component Y of X.

Regular Sequence: $f_1, \ldots, f_r$ s.t. f_i regular over $V(f_1, \ldots, f_{i-1})$ $\forall i$.

$$I(X) := \{f \in R \mid f|_X = 0\}.$$

Lemma

f intersects X regularly

$$\Updownarrow$$

For every g with $gf \in I(X)$ (syzygy cofactor) we have $g \in I(X)$

$I(X) := \{f \in R \mid f|_X = 0\}.$

Lemma

f intersects X regularly

$$\Updownarrow$$

For every g with $gf \in I(X)$ (syzygy cofactor) we have $g \in I(X)$

$X = V(xy, xz, yz), f = x(x-1),$

$$I(X) := \{f \in R \mid f|_X = 0\}.$$

Lemma

f intersects X regularly

$$\Updownarrow$$

For every g with $gf \in I(X)$ (syzygy cofactor) we have $g \in I(X)$

$X = V(xy, xz, yz), f = x(x-1), g = y$:

$$gf \in \langle xy, xz, yz \rangle \text{ but } g \notin \langle xy, xz, yz \rangle.$$

$I(X) := \{f \in R \mid f|_X = 0\}.$

Lemma

f intersects X regularly

$$\Updownarrow$$

For every g with $gf \in I(X)$ (syzygy cofactor) we have $g \in I(X)$

$X = V(xy, xz, yz), f = x(x-1), g = y$:

$$gf \in \langle xy, xz, yz \rangle \text{ but } g \notin \langle xy, xz, yz \rangle.$$

Algorithmic Principle:

Using Gröbner basis computations,

find g with $gf \in I(X)$, $g \notin I(X)$

$$\Downarrow$$

Use g to modify X

Computing the Nondegenerate Locus

Algorithm 1

Let $f_1, \ldots, f_c \in R$ with $c \leq n$, the number of variables. Given $I := \langle f_1, \ldots, f_c \rangle$,

compute

Let $f_1, \ldots, f_c \in R$ with $c \leq n$, the number of variables. Given $I := \langle f_1, \ldots, f_c \rangle$,

compute

Definition

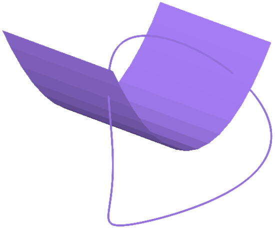
Nondegenerate locus: union of components of codimension c of $V(I)$.

Let $f_1, \ldots, f_c \in R$ with $c \leq n$, the number of variables. Given $I := \langle f_1, \ldots, f_c \rangle$,

compute

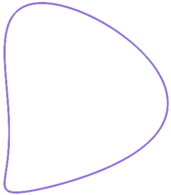
Definition

Nondegenerate locus: union of components of codimension c of $V(I)$.



$V(x^2z^2 + x^2y - z^3 - x^2 - yz + z, x^4 - x^2y - x^2z + yz)$

Nondegenerate Locus $\longrightarrow$



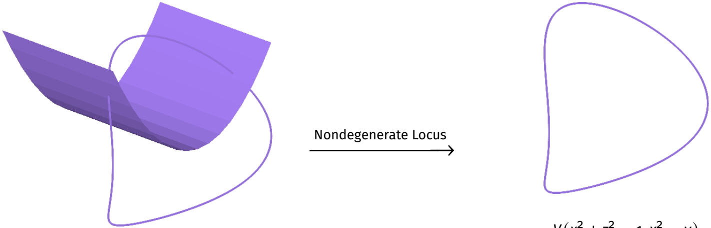
$V(x^2 + z^2 - 1, x^2 - y)$

Let $f_1, \ldots, f_c \in R$ with $c \leq n$, the number of variables. Given $I := \langle f_1, \ldots, f_c \rangle$,

compute

Definition

Nondegenerate locus: union of components of codimension c of $V(I)$.



$V(x^2 + z^2 - 1, x^2 - y)$

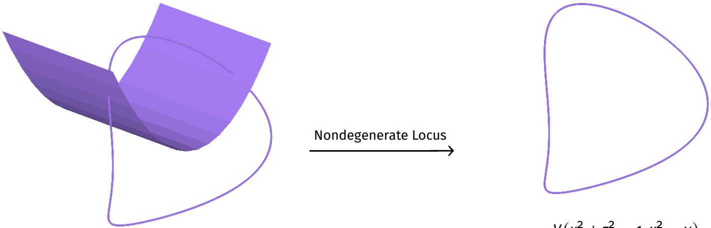
$V(x^2z^2 + x^2y - z^3 - x^2 - yz + z, x^4 - x^2y - x^2z + yz)$

In Steiner example: Nondegenerate Locus gives tangent conics!

Let $f_1, \ldots, f_c \in R$ with $c \leq n$, the number of variables. Given $I := \langle f_1, \ldots, f_c \rangle$, compute

Definition

Nondegenerate locus: union of components of codimension c of $V(I)$.



$V(x^2z^2 + x^2y - z^3 - x^2 - yz + z, x^4 - x^2y - x^2z + yz)$

$V(x^2 + z^2 - 1, x^2 - y)$

In Steiner example: Nondegenerate Locus gives tangent conics!

Note: $f_1, \ldots, f_c$ regular sequence $\Rightarrow \mathrm{ndeg}(V(f_1, \ldots, f_c)) = V(f_1, \ldots, f_c)$

Incremental step: Suppose $f_1, \ldots, f_k$ regular sequence, so that for $X = V(f_1, \ldots, f_k)$

$$\operatorname{ndeg}(X) = X.$$

Incremental step: Suppose $f_1, \ldots, f_k$ regular sequence, so that for $X = V(f_1, \ldots, f_k)$

$$\mathrm{ndeg}(X) = X.$$

Want to compute

$$\mathrm{ndeg}(X \cap V(f_{k+1}))$$

Incremental step: Suppose $f_1, \ldots, f_k$ regular sequence, so that for $X = V(f_1, \ldots, f_k)$

$$\mathrm{ndeg}(X) = X.$$

Want to compute

$$\mathrm{ndeg}(X \cap V(f_{k+1}))$$

Idea: Change X to $X \setminus V(h)$ s.t. all g with $gf \in I(X)$ lie in $I(X \setminus V(h))$.

Incremental step: Suppose $f_1, \ldots, f_k$ regular sequence, so that for $X = V(f_1, \ldots, f_k)$

$$\mathrm{ndeg}(X) = X.$$

Want to compute

$$\mathrm{ndeg}(X \cap V(f_{k+1}))$$

Example

$X = V(xy), f_2 = xz.$

Incremental step: Suppose $f_1, \ldots, f_k$ regular sequence, so that for $X = V(f_1, \ldots, f_k)$

$$\mathrm{ndeg}(X) = X.$$

Want to compute

$$\mathrm{ndeg}(X \cap V(f_{k+1}))$$

Example

$X = V(xy), f_2 = xz.$

$yf_2 \in I(X)$

Incremental step: Suppose $f_1, \ldots, f_k$ regular sequence, so that for

$X = V(f_1, \ldots, f_k)$

$$\mathrm{ndeg}(X) = X.$$

Want to compute

$$\mathrm{ndeg}(X \cap V(f_{k+1}))$$

Example

$X = V(xy), f_2 = xz.$

$yf_2 \in I(X)$ ⟶ $xy \in I(X)$

Incremental step: Suppose $f_1, \ldots, f_k$ regular sequence, so that for $X = V(f_1, \ldots, f_k)$

$$\mathrm{ndeg}(X) = X.$$

Want to compute

$$\mathrm{ndeg}(X \cap V(f_{k+1}))$$

Example

$X = V(xy), f_2 = xz.$

$yf_2 \in I(X)$ → $xy \in I(X)$

↓ $g \notin I(X)$ but $g \in I(X \setminus V(x))$

$$\mathrm{ndeg}(X \cap V(f_2)) = \overline{X \setminus V(x) \cap V(f_2)} = V(y, z)$$

Incremental step: Suppose $f_1, \ldots, f_k$ regular sequence, so that for

$X = V(f_1, \ldots, f_k)$

$$\operatorname{ndeg}(X) = X.$$

Want to compute

$$\operatorname{ndeg}(X \cap V(f_{k+1}))$$

Example

$X = V(xy), f_2 = xz.$

Compute y and x using Gröbner basis computations!

$yf_2 \in I(X)$ → $xy \in I(X)$

↓ $g \notin I(X)$ but $g \in I(X \setminus V(x))$

$$\operatorname{ndeg}(X \cap V(f_2)) = \overline{X \setminus V(x) \cap V(f_2)} = V(y, z)$$

Hot to compute Gröbner bases?

Fix: Polynomial Ring $R := \mathbb{K}[x_1, \ldots, x_n], f_1, \ldots, f_c \in R, I := \langle f_1, \ldots, f_c \rangle$.

Want: A Gröbner basis for I (w.r.t. some monomial ordering).

Hot to compute Gröbner bases?

Fix: Polynomial Ring $R := \mathbb{K}[x_1, \ldots, x_n]$, $f_1, \ldots, f_c \in R$, $I := \langle f_1, \ldots, f_c \rangle$.

Want: A Gröbner basis for I (w.r.t. some monomial ordering).

Buchberger's criterion (Buchberger 1965):

Theorem

G is a Gröbner basis for I iff for every $g_1, g_2 \in G$, the *S-polynomial*

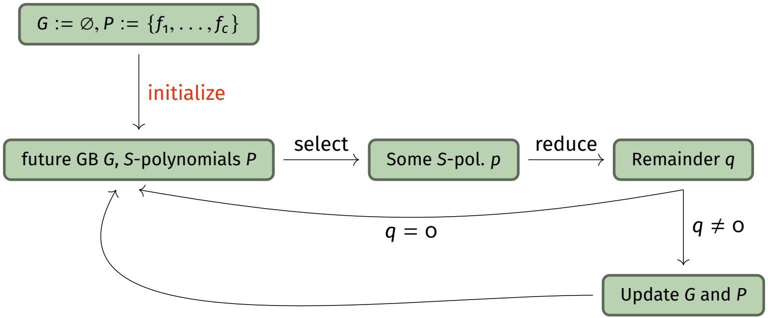
$$\frac{\operatorname{lcm}(\operatorname{lm}(g_1), \operatorname{lm}(g_2))}{\operatorname{lm}(g_1)} g_1 - \frac{\operatorname{lcm}(\operatorname{lm}(g_1), \operatorname{lm}(g_2))}{\operatorname{lm}(g_2)} g_2$$

reduces to zero by G via polynomial long division.

Hot to compute Gröbner bases?

Fix: Polynomial Ring $R := \mathbb{K}[x_1, \ldots, x_n]$, $f_1, \ldots, f_c \in R$, $I := \langle f_1, \ldots, f_c \rangle$.

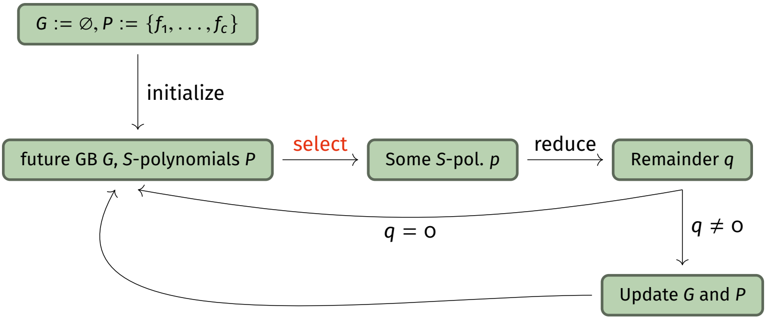
Want: A Gröbner basis for I (w.r.t. some monomial ordering).



Hot to compute Gröbner bases?

Fix: Polynomial Ring $R := \mathbb{K}[x_1, \ldots, x_n]$, $f_1, \ldots, f_c \in R$, $I := \langle f_1, \ldots, f_c \rangle$.

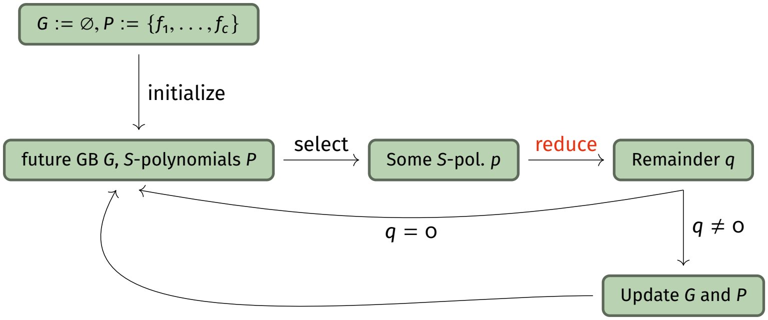
Want: A Gröbner basis for I (w.r.t. some monomial ordering).



Hot to compute Gröbner bases?

Fix: Polynomial Ring $R := \mathbb{K}[x_1, \ldots, x_n]$, $f_1, \ldots, f_c \in R$, $I := \langle f_1, \ldots, f_c \rangle$.

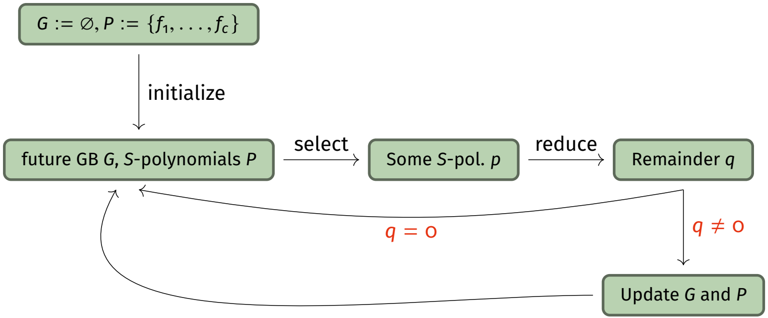
Want: A Gröbner basis for I (w.r.t. some monomial ordering).



Hot to compute Gröbner bases?

Fix: Polynomial Ring $R := \mathbb{K}[x_1, \ldots, x_n], f_1, \ldots, f_c \in R, I := \langle f_1, \ldots, f_c \rangle$.

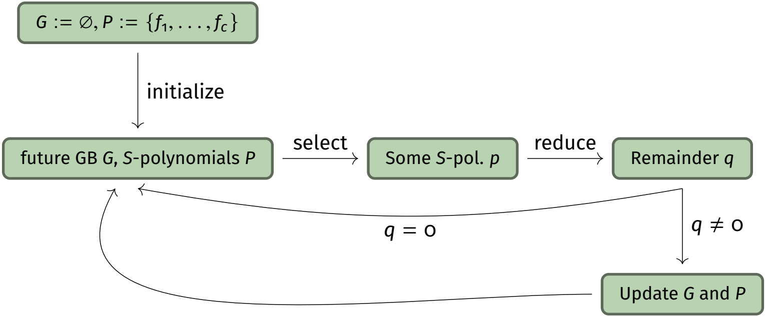
Want: A Gröbner basis for I (w.r.t. some monomial ordering).



Hot to compute Gröbner bases?

Fix: Polynomial Ring $R := \mathbb{K}[x_1, \ldots, x_n]$, $f_1, \ldots, f_c \in R$, $I := \langle f_1, \ldots, f_c \rangle$.

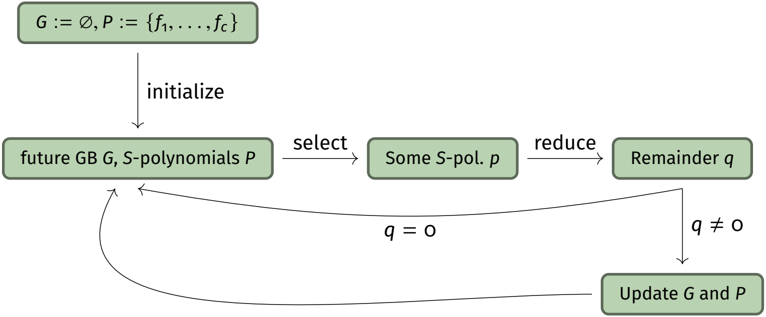
Want: A Gröbner basis for I (w.r.t. some monomial ordering).



Hot to compute Gröbner bases?

Fix: Polynomial Ring $R := \mathbb{K}[x_1, \ldots, x_n]$, $f_1, \ldots, f_c \in R$, $I := \langle f_1, \ldots, f_c \rangle$.

Want: A Gröbner basis for I (w.r.t. some monomial ordering).



Think of every S-polynomial as ug_i, g_i ith element in G, u monomial

$\rightsquigarrow$ computational history

Signature-based computations à la (J. C. Faugère 2002; Gao, Guan, and Volny IV 2010; Eder and J.-C. Faugère 2017):

Signature-based computations à la (J. C. Faugère 2002; Gao, Guan, and Volny IV 2010; Eder and J.-C. Faugère 2017):

1. Given GB for $I(X)$ compute GB for $I(X) + \langle f_{k+1} \rangle$

Signature-based computations à la (J. C. Faugère 2002; Gao, Guan, and Volny IV 2010; Eder and J.-C. Faugère 2017):

1. Given GB for $I(X)$ compute GB for $I(X) + \langle f_{k+1} \rangle$

$$\Downarrow$$

Every S-pol. equal to $g f_{k+1} \bmod I(X)$ for some $g \in R$. Signature: Tuple $(\mathrm{lm}(g), f_{k+1})$

Signature-based computations à la (J. C. Faugère 2002; Gao, Guan, and Volny IV 2010; Eder and J.-C. Faugère 2017):

1. Given GB for $I(X)$ compute GB for $I(X) + \langle f_{k+1} \rangle$

$$\Downarrow$$

Every S-pol. equal to gf_{k+1} mod $I(X)$ for some $g \in R$. Signature: Tuple $(\mathrm{lm}(g), f_{k+1})$

2. Only allow reductions that do *not* change $\mathrm{lm}(g)$

Signature-based computations à la (J. C. Faugère 2002; Gao, Guan, and Volny IV 2010; Eder and J.-C. Faugère 2017):

1. Given GB for $I(X)$ compute GB for $I(X) + \langle f_{k+1} \rangle$

$$\Downarrow$$

Every S-pol. equal to gf_{k+1} mod $I(X)$ for some $g \in R$. Signature: Tuple $(\text{lm}(g), f_{k+1})$

2. Only allow reductions that do *not* change $\text{lm}(g)$

3. Select S-polynomials by order of increasing $\text{lm}(g)$

Signature-based computations à la (J. C. Faugère 2002; Gao, Guan, and Volny IV 2010; Eder and J.-C. Faugère 2017):

1. Given GB for $I(X)$ compute GB for $I(X) + \langle f_{k+1} \rangle$

$\Downarrow$

Every S-pol. equal to $g f_{k+1} \bmod I(X)$ for some $g \in R$. Signature: Tuple $(\operatorname{lm}(g), f_{k+1})$

2. Only allow reductions that do *not* change $\operatorname{lm}(g)$

3. Select S-polynomials by order of increasing $\operatorname{lm}(g)$

Theorem

Result of reducing an S-polynomial depends *only* on its signature $(\operatorname{lm}(g), f_{k+1})$.

Koszul Criterion – An S-pol. with signature $(\mathrm{lm}(g), f_{k+1})$ reduces to zero if $\mathrm{lm}(g) \in \mathrm{lm}(I(X))$.

Koszul Criterion – An S-pol. with signature $(\mathrm{lm}(g), f_{k+1})$ reduces to zero if $\mathrm{lm}(g) \in \mathrm{lm}(I(X))$.

in sGB algorithm:

Zero reduction with cofactor $g \Longrightarrow gf_{k+1} \in I(X)$ but $g \notin I(X)$

$$\Downarrow$$

Furnishes nondegenerate locus computations as before!

Koszul Criterion – An S-pol. with signature $(\mathrm{lm}(g), f_{k+1})$ reduces to zero if $\mathrm{lm}(g) \in \mathrm{lm}(I(X))$.

in sGB algorithm:

Zero reduction with cofactor $g \Longrightarrow gf_{k+1} \in I(X)$ but $g \notin I(X)$

$\Downarrow$

Furnishes nondegenerate locus computations as before!

Algorithm with Black box GB usage

Koszul Criterion – An S-pol. with signature $(\mathrm{lm}(g), f_{k+1})$ reduces to zero if $\mathrm{lm}(g) \in \mathrm{lm}(I(X))$.

in sGB algorithm:

Zero reduction with cofactor $g \Longrightarrow g f_{k+1} \in I(X)$ but $g \notin I(X)$

$\Downarrow$

Furnishes nondegenerate locus computations as before!

Algorithm with Black box GB usage $\rightsquigarrow$ Dedicated GB algorithm

	Our Algorithm	●	●	●
Sing(2,8)	0.68s	23m	∞	∞
Sing(2,10)	2.9s	∞	∞	∞
Sos(2,6,4)	169s	∞	∞	∞
Steiner	42m	∞	∞	∞

Computed in characteristic 65521 on Intel Xeon Gold 6244.
● Elimination method in Singular, see e.g. (Decker, Greuel, and Pfister 1999).
● Regular Chains library in Maple, see e.g. (Kalkbrener 1993; Lemaire, Maza, and Xie 2005).
● Homological method in Macaulay2 presented in (Eisenbud, Huneke, and W. Vasconcelos 1992) plus Saturation.

Reference: Eder, Lairez, Mohr, and El Din 2023,
A Signature-based Algorithm to Compute the Nondegenerate Locus of a Polynomial System

	Our Algorithm	●	●	●
Sing(2,8)	0.68s	23m	∞	∞
Sing(2,10)	2.9s	∞	∞	∞
Sos(2,6,4)	169s	∞	∞	∞
Steiner	42m	∞	∞	∞

	sGB	Our Algorithm	Ratio	GB in Maple	●	Ratio
Sing(2,10)	1.9s	2.9s	1.5	0.11s	1.642s	15
Sos(2,6,4)	148s	160s	1.08	0.172s	22.7s	132
Sos(2,7,4)	3m	30m	10	0.433s	1h	8314
Sos(2,7,5)	25m	20h	48	2.294s	>359h	>564366

Computed in characteristic 65521 on Intel Xeon Gold 6244.
● Elimination method in Singular, see e.g. (Decker, Greuel, and Pfister 1999).
● Regular Chains library in Maple, see e.g. (Kalkbrener 1993; Lemaire, Maza, and Xie 2005).
● Homological method in Macaulay2 presented in (Eisenbud, Huneke, and W. Vasconcelos 1992) plus Saturation.
● "Naive" implementation of nondegenerate locus algorithm in Maple.

Reference: Eder, Lairez, Mohr, and El Din 2023,
A Signature-based Algorithm to Compute the Nondegenerate Locus of a Polynomial System

Computing Equidimensional Decompositions

Algorithm 2

This time: Compute full equidimensional decomposition of given $V(f_1, \ldots, f_r)$ with incremental strategy.

$$\Downarrow$$

Have to solve:

Given X equidimensional, $f \in \mathbb{K}[x_1, \ldots, x_n]$

Compute equidimensional decomposition of $X \cap V(f)$

After decomposing $X \cap V(f)$ another equation coming in!

After decomposing $X \cap V(f)$ another equation coming in!

$\Longrightarrow$ Philosophy: Split $X \cap V(f)$

As much as possible, as irredundantly as possible

After decomposing $X \cap V(f)$ another equation coming in!

$\Longrightarrow$ Philosophy: Split $X \cap V(f)$

As much as possible, as irredundantly as possible

$\Downarrow$

Components of lower degree while avoiding exponential blow up!

Incremental step: Again suppose we have function

$$\text{syzcof}(X, f)\text{: returns } g \text{ s.t. } gf \in I(X),\ g \notin I(X)$$

Incremental step: Again suppose we have function

$$\mathrm{syzcof}(X, f)\text{: returns } g \text{ s.t. } gf \in I(X),\ g \notin I(X)$$

Example

$X = V(xy, xz, yz), f = x(x-1), g := \mathrm{syzcof}(X, f) = y$

Incremental step: Again suppose we have function

$$\text{syzcof}(X, f)\text{: returns } g \text{ s.t. } gf \in I(X), g \notin I(X)$$

Example

$X = V(xy, xz, yz), f = x(x-1), g := \text{syzcof}(X, f) = y$

X	$V(x,y)$	$V(x,z)$	$V(y,z)$
	$f = 0$	$f = 0$	$f \neq 0$
	$g = 0$	$g \neq 0$	$g = 0$

Incremental step: Again suppose we have function

$$\mathrm{syzcof}(X, f)\text{: returns } g \text{ s.t. } gf \in I(X),\ g \notin I(X)$$

Example

$X = V(xy, xz, yz), f = x(x-1), g := \mathrm{syzcof}(X, f) = y$

X	$V(x,y)$	$V(x,z)$	$V(y,z)$
	$f = 0$	$f = 0$	$f \neq 0$
	$g = 0$	$g \neq 0$	$g = 0$

Incremental step: Again suppose we have function

$$\text{syzcof}(X, f)\text{: returns } g \text{ s.t. } gf \in I(X),\ g \notin I(X)$$

Example

$X = V(xy, xz, yz), f = x(x-1), g := \text{syzcof}(X, f) = y$

X	$V(x,y)$	$V(x,z)$	$V(y,z)$
	$f = 0$	$f = 0$	$f \neq 0$
	$g = 0$	$g \neq 0$	$g = 0$

Set $X_1 := \overline{X \setminus V(g)} = V(x, z)$. Then

$f = 0$ on X_1!

Incremental step: Again suppose we have function

$$\text{syzcof}(X, f)\text{: returns } g \text{ s.t. } gf \in I(X),\, g \notin I(X)$$

Example

$X = V(xy, xz, yz), f = x(x-1), g := \text{syzcof}(X, f) = y$

X	$V(x,y)$	$V(x,z)$	$V(y,z)$
	$f = 0$	$f = 0$	$f \neq 0$
	$g = 0$	$g \neq 0$	$g = 0$

Set $X_1 := \overline{X \setminus V(g)} = V(x, z)$. Then

$f = 0$ on X_1!

$$\Downarrow$$

$$X \cap V(f) = X_1 \cup \underbrace{[(X \setminus X_1) \cap V(f)]}_{\text{split with same approach!}}$$

Incremental step: Again suppose we have function

$$\operatorname{syzcof}(X, f)\text{: returns } g \text{ s.t. } gf \in I(X),\ g \notin I(X)$$

Example

$X = V(xy, xz, yz), f = x(x-1), g := \operatorname{syzcof}(X, f) = y$

X	$V(x,y)$	$V(x,z)$	$V(y,z)$
	$f = 0$	$f = 0$	$f \neq 0$
	$g = 0$	$g \neq 0$	$g = 0$

Set $X_1 := \overline{X \setminus V(g)} = V(x, z)$. Then

$f = 0$ on X_1!

$\Downarrow$

$$X \cap V(f) = X_1 \cup \underbrace{[(X \setminus X_1) \cap V(f)]}_{\text{split with same approach!}}$$

⚠ Splitting a lot via recursion

⚠ Irredundancy via disjointness (and no fake components!)

Algorithm: intersect

if $X \cap V(f)$ equidimensional **then**

  return $X \cap V(f)$

else

  $g \leftarrow \mathrm{syzcof}(X, f)$

  $X_1 \leftarrow \overline{X \setminus V(g)}$

  return $X_1 \cup \mathrm{intersect}(\mathrm{remove}(X, X_1), f)$

end if

Algorithm: intersect

if $X \cap V(f)$ equidimensional **then**
    return $X \cap V(f)$
else
    $g \leftarrow \text{syzcof}(X, f)$
    $X_1 \leftarrow \overline{X \setminus V(g)}$
    return $X_1 \cup \text{intersect}(\text{remove}(X, X_1), f)$
end if

Decompose further $X \setminus X_1$!

Algorithm: intersect

if $X \cap V(f)$ equidimensional **then**
  return $X \cap V(f)$
else
  $g \leftarrow \text{syzcof}(X, f)$
  $X_1 \leftarrow X \setminus V(g)$
  return $X_1 \cup \text{intersect}(\text{remove}(X, X_1), f)$
end if

Decompose further $X \setminus X_1$!

Algorithm: remove

Write $X_1 = V(h_1, \ldots, h_r)$
$X_1' \leftarrow V(h_2, \ldots, h_r)$
return $X \setminus V(h_1) \cup \text{intersect}(\text{remove}(X, X_1'), h_1)$

Algorithm: intersect

if $X \cap V(f)$ equidimensional **then**
  return $X \cap V(f)$
else
  $g \leftarrow \underline{\mathrm{syzcof}(X, f)}$
  $X_1 \leftarrow X \setminus V(g)$
  return $X_1 \cup \mathrm{intersect}(\mathrm{remove}(X, X_1), f)$
end if

Decompose further $X \setminus X_1$!

Algorithm: remove

Write $X_1 = V(h_1, \ldots, h_r)$
$X_1' \leftarrow V(h_2, \ldots, h_r)$
return $X \setminus V(h_1) \cup \mathrm{intersect}(\mathrm{remove}(X, X_1'), h_1)$

$$X \setminus X_1 = X \setminus V(h_1) \sqcup \left[(X \setminus X_1') \cap V(h_1)\right]$$

Algorithm: intersect

if $X \cap V(f)$ equidimensional **then**
    return $X \cap V(f)$
else
    $g \leftarrow \text{syzcof}(X, f)$
    $X_1 \leftarrow X \setminus V(g)$
    return $X_1 \cup \text{intersect}(\text{remove}(X, X_1), f)$
end if

Decompose further $X \setminus X_1$!

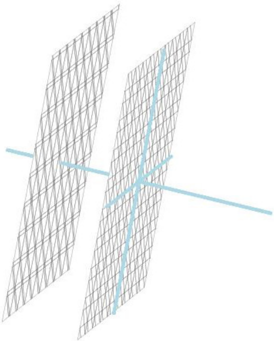
mutually recursive algorithms for decomposition of $X \cap V(f)$ and $X \setminus X_1$!

Algorithm: remove

Write $X_1 = V(h_1, \ldots, h_r)$
$X_1' \leftarrow V(h_2, \ldots, h_r)$
return $X \setminus V(h_1) \cup \text{intersect}(\text{remove}(X, X_1'), h_1)$

$$X \setminus X_1 = X \setminus V(h_1) \sqcup \left[(X \setminus X_1') \cap V(h_1)\right]$$

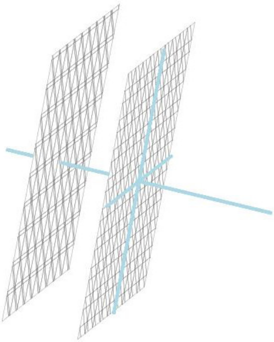
$\text{intersect}(X, f)$
$\text{syzcof}(X, f) = y$



$X = V(xy, xz, yz), f = x(x-1)$

$\text{intersect}(X, f)$
$\text{syzcof}(X, f) = y$

$X_1 = \overline{X \setminus V(y)}$
$= V(x, z)$



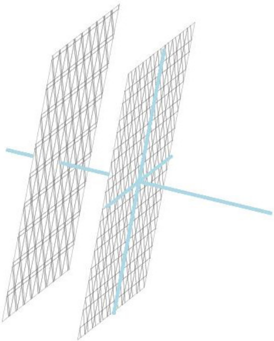
$X = V(xy, xz, yz), f = x(x-1)$

$\text{intersect}(X, f)$

$\text{syzcof}(X, f) = y$

$$X_1 = \overline{X \setminus V(y)} = V(x, z)$$

$\text{remove}(X, V(x, z))$



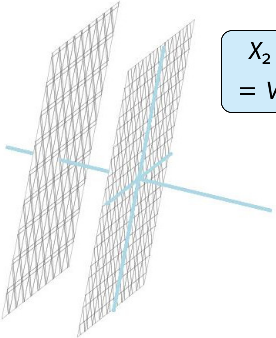
$X = V(xy, xz, yz), f = x(x - 1)$

$$\text{intersect}(X, f)$$
$$\text{syzcof}(X, f) = y$$

$$X_1 = \overline{X \setminus V(y)} = V(x, z)$$

$$\text{remove}(X, V(x, z))$$

$$X_2 = X \setminus V(x) = V(y, z) \setminus V(x)$$



$X = V(xy, xz, yz), f = x(x-1)$

$\text{intersect}(X, f)$

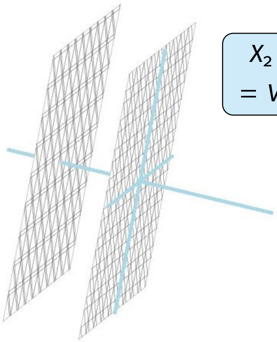
$\text{syzcof}(X, f) = y$

$X_1 = \overline{X \setminus V(y)} = V(x, z)$

$\text{remove}(X, V(x, z))$

$X_2 = X \setminus V(x) = V(y, z) \setminus V(x)$

$X_3 = X \setminus V(z) = V(x, y) \setminus V(z)$



$X = V(xy, xz, yz), f = x(x-1)$

intersect(X, f)
syzcof$(X, f) = y$

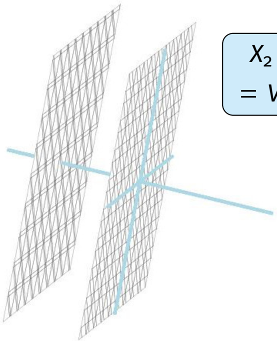
$X_1 = \overline{X \setminus V(y)}$
$= V(x, z)$

remove$(X, V(x, z))$

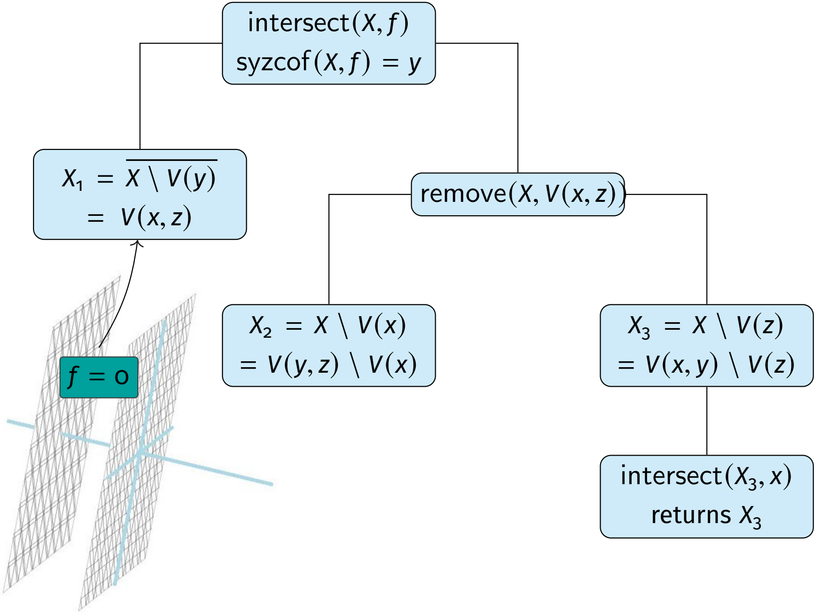
$X_2 = X \setminus V(x)$
$= V(y, z) \setminus V(x)$

$X_3 = X \setminus V(z)$
$= V(x, y) \setminus V(z)$

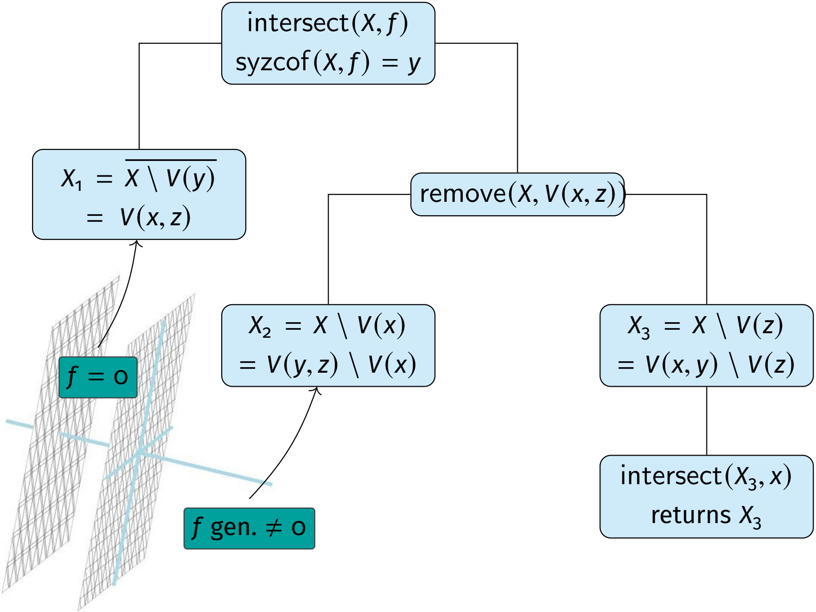
intersect(X_3, x)
returns X_3



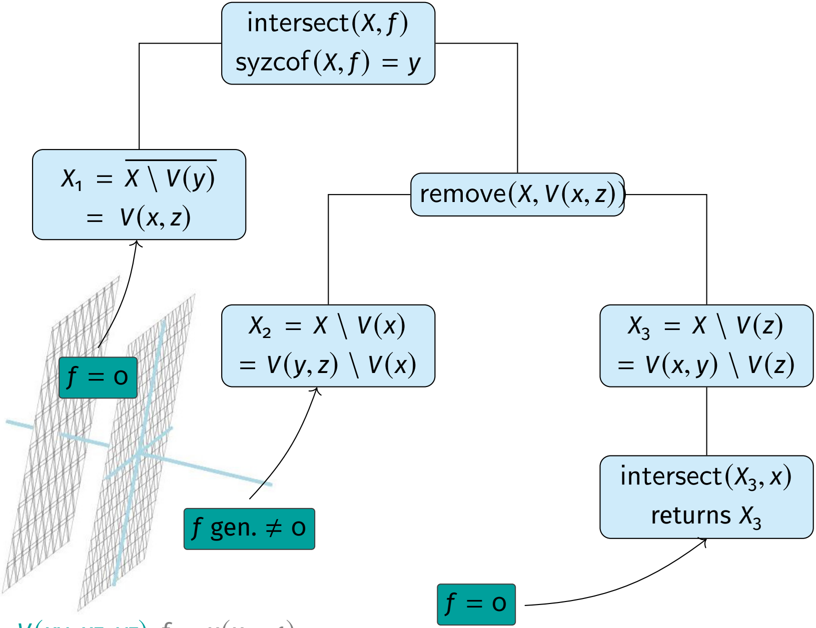
$X = V(xy, xz, yz), f = x(x - 1)$



$X = V(xy, xz, yz), f = x(x-1)$



$X = V(xy, xz, yz), f = x(x-1)$



$X = V(xy, xz, yz), f = x(x-1)$

intersect(X, f)

syzcof$(X, f) = y$

$X_1 = \overline{X \setminus V(y)}$

$= V(x, z)$

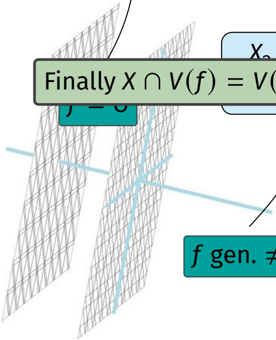
remove$(X, V(x, z))$

$X_2 = X \setminus V(x)$

$X_3 = X \setminus V(z)$

(z)

Finally $X \cap V(f) = V(x, z) \sqcup V(x, y) \setminus V(z) \sqcup V(y, z, x - 1) \setminus V(x)$



f gen. $\neq 0$

intersect(X_3, x)

returns X_3

$f = 0$

$X = V(xy, xz, yz), f = x(x - 1)$

“Naive” data structure:

- (F, h) modelling $X := V(F) \setminus V(h)$ ($F \subset \mathbb{K}[\mathbf{x}]$ finite, $h \in \mathbb{K}[\mathbf{x}]$).
- Gröbner basis of $I := (\langle F \rangle : g^{\infty})$ (satisfies $\sqrt{I} = I(X)$).

"Naive" data structure:

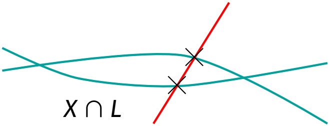
- (F, h) modelling $X := V(F) \setminus V(h)$ ($F \subset \mathbb{K}[\mathbf{x}]$ finite, $h \in \mathbb{K}[\mathbf{x}]$).
- Gröbner basis of $I := (\langle F \rangle : g^{\infty})$ (satisfies $\sqrt{I} = I(X)$).

$X \cap V(f)$ *already equidimensional* if

$f|_X = 0$ or $f \neq 0$ generically on X

"Naive" data structure:

- (F, h) modelling $X := V(F) \setminus V(h)$ ($F \subset \mathbb{K}[\mathbf{x}]$ finite, $h \in \mathbb{K}[\mathbf{x}]$).
- Gröbner basis of $I := (\langle F \rangle : g^{\infty})$ (satisfies $\sqrt{I} = I(X)$).



$X \cap V(f)$ *already equidimensional* if

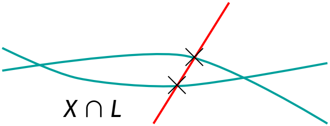
$f|_X = 0$ or $f \neq 0$ generically on $X \Leftrightarrow$

this happens at randomly selected

points on X

“Naive” data structure:

- (F, h) modelling $X := V(F) \setminus V(h)$ ($F \subset \mathbb{K}[\mathbf{x}]$ finite, $h \in \mathbb{K}[\mathbf{x}]$).
- Gröbner basis of $I := (\langle F \rangle : g^{\infty})$ (satisfies $\sqrt{I} = I(X)$).



L general affine subspace of complementary dimension

$X \cap V(f)$ *already equidimensional* if

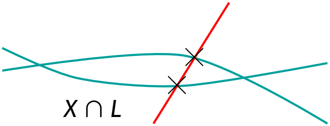
$f|_X = 0$ or $f \neq 0$ generically on X

$f\|_X = 0$ or gen. $\neq 0$ iff $f\|_{X \cap L} = 0$ or gen. $\neq 0$

$\Longrightarrow$ Avoid knowing a GB of I!

“Naive” data structure:

- (F, h) modelling $X := V(F) \setminus V(h)$ ($F \subset \mathbb{K}[\mathbf{x}]$ finite, $h \in \mathbb{K}[\mathbf{x}]$).
- Gröbner basis of $I := (\langle F \rangle : g^{\infty})$ (satisfies $\sqrt{I} = I(X)$).



L general affine subspace of complementary dimension

$X \cap V(f)$ *already equidimensional* if

$f|_X = 0$ or $f \neq 0$ generically on X

$f|_X = 0$ or gen. $\neq 0$ iff
$f|_{X \cap L} = 0$ or gen. $\neq 0$

$\Longrightarrow$ Avoid knowing a GB of I!

$X \cap L$ called *lifting fiber* or *witness set*
(Lecerf 2003; Sommese, Verschelde, and Wampler 2005)

	nb. comps.	Our Algorithm	●	●	●	●
Cyclic(8)	6	381.20	∞	∞	∞	∞
KdV		∞	352.61	∞	∞	7108.56
Leykin-1	13	2.63	4.38	640.52	∞	1.37
C1	4	128.84	∞	∞	∞	∞
PS(12)	2	51.21	∞	∞	∞	2060.03
Sing(10)	2	0.36	∞	∞	∞	∞
SOS(6,4)	2	4.83	∞	∞	∞	∞
SOS(6,5)	2	13.72	∞	∞	∞	∞
Steiner	2	869.79	∞	∞	∞	∞
sys2161	33	7.54	28.76	∞	∞	7.57
sys2880	50	4.27	144.30	1.80	3.44	4.00

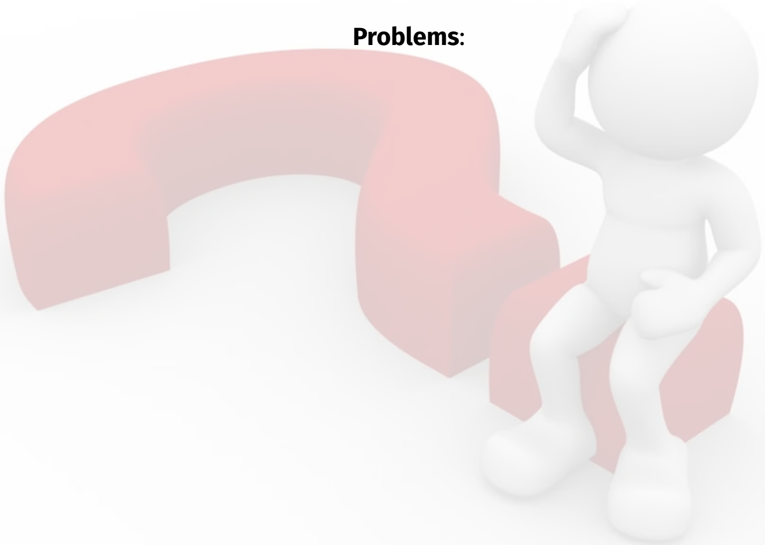
Computed in characteristic 65521 on Intel Xeon Gold 6244.
● Elimination method in Singular, see e.g. (Decker, Greuel, and Pfister 1999).
● Regular Chains library in Maple, see e.g. (Kalkbrener 1993; Lemaire, Maza, and Xie 2005).
● Homological method in Oscar presented in (Eisenbud, Huneke, and W. Vasconcelos 1992).
● Prime decomposition in Magma.

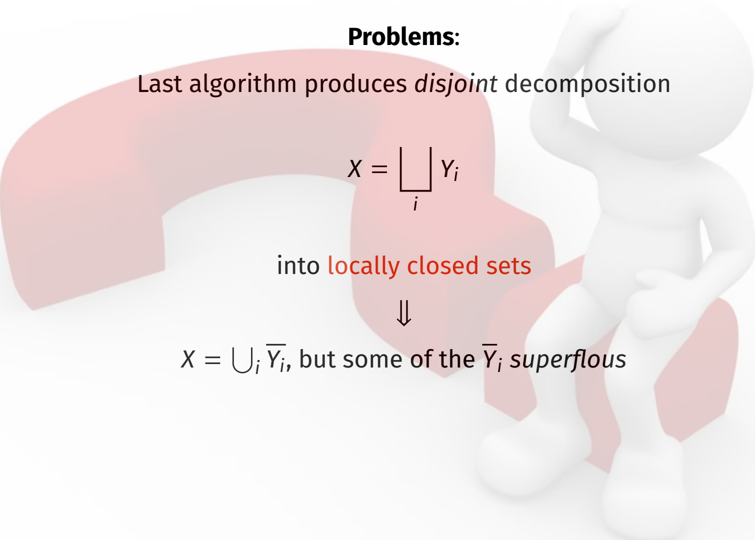
Reference: Eder, Lairez, Mohr, and Safey El Din 2023,
A Direttissimo Algorithm for Equidimensional Decomposition

A Non-Incremental Algorithm

Algorithm 3

Problems:





Problems:

Last algorithm produces *disjoint* decomposition

$$X = \bigsqcup_i Y_i$$

into locally closed sets

$$\Downarrow$$

$X = \bigcup_i \overline{Y_i}$, but some of the $\overline{Y}_i$ *superflous*

Problems:

Incremental structure $\rightsquigarrow$ computations tend to be hard "in the middle"

$\cong$

complexity bounds for Gröbner bases

(Bardet, J.-C. Faugère, and Salvy 2015; Hashemi and Seiler 2017)

Definition

$f_1, \ldots, f_c$ regular sequence iff for every i and every g with $gf_i \in \langle f_1, \ldots, f_{i-1} \rangle$ we have $g \in \langle f_1, \ldots, f_{i-1} \rangle$.

Definition

$f_1, \ldots, f_c$ regular sequence iff for every i and every g with $gf_i \in \langle f_1, \ldots, f_{i-1} \rangle$ we have $g \in \langle f_1, \ldots, f_{i-1} \rangle$.

vs. (W. V. Vasconcelos 1967), if $f_1, \ldots, f_c$ homogeneous

Theorem

$f_1, \ldots, f_c$ regular sequence iff for every i and every g with $gf_i \in \langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c \rangle$ we have $g \in \langle f_1, \ldots, f_c \rangle$.

Definition

$f_1, \ldots, f_c$ regular sequence iff for every i and every g with $gf_i \in \langle f_1, \ldots, f_{i-1} \rangle$ we have $g \in \langle f_1, \ldots, f_{i-1} \rangle$.

vs. (W. V. Vasconcelos 1967), if $f_1, \ldots, f_c$ homogeneous

Theorem

$f_1, \ldots, f_c$ regular sequence iff for every i and every g with $gf_i \in \langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c \rangle$ we have $g \in \langle f_1, \ldots, f_c \rangle$.

$$\Downarrow$$

Non-incremental regularity criterion

$$X = V(f_1, \ldots, f_c)$$

This time suppose we have function

$$\text{syzcof}(X)\text{: returns } g, i \text{ s.t. } gf_i \in \langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c \rangle, g \notin I(X)$$

$\rightsquigarrow$ done with signature-based computations

$$X = V(f_1, \ldots, f_c)$$

This time suppose we have function

$$\text{syzcof}(X)\text{: returns } g, i \text{ s.t. } gf_i \in \langle f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_c \rangle, g \notin I(X)$$

$\rightsquigarrow$ done with signature-based computations

$$X = V(f_1, \dots, f_c)$$

$$X_1 := V(f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_c) \setminus V(g) \qquad X_2 = V(f_1, \dots, f_c, g) \setminus X_1$$

This time suppose we have function

$$\text{syzcof}(X)\text{: returns } g, i \text{ s.t. } gf_i \in \langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c \rangle, g \notin I(X)$$

$\rightsquigarrow$ done with signature-based computations

$$X = V(f_1, \ldots, f_c)$$

$$X_1 := V(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c) \setminus V(g) \qquad X_2 = V(f_1, \ldots, f_c, g) \setminus X_1$$

Proceed recursively | Proceed recursively

This time suppose we have function

$$\text{syzcof}(X)\text{: returns } g, i \text{ s.t. } gf_i \in \langle f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_c \rangle,\ g \notin I(X)$$

$\rightsquigarrow$ done with signature-based computations

codim $\leq c$

$$X = V(f_1, \dots, f_c)$$

$$X_1 := V(f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_c) \setminus V(g)$$

Proceed recursively

$$X_2 = V(f_1, \dots, f_c, g) \setminus X_1$$

Proceed recursively

This time suppose we have function

$$\text{syzcof}(X)\text{: returns } g, i \text{ s.t. } gf_i \in \langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c \rangle, g \notin I(X)$$

$\rightsquigarrow$ done with signature-based computations

codim $\leq c$

$X = V(f_1, \ldots, f_c)$

codim $\leq c - 1$

$X_1 := V(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c) \setminus V(g)$

$X_2 = V(f_1, \ldots, f_c, g) \setminus X_1$

Proceed recursively

Proceed recursively

This time suppose we have function

$$\text{syzcof}(X)\text{: returns } g, i \text{ s.t. } gf_i \in \langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c \rangle, g \notin I(X)$$

$\rightsquigarrow$ done with signature-based computations

codim $\leq c$

$X = V(f_1, \ldots, f_c)$

codim $\leq c - 1$

$X_1 := V(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c) \setminus V(g)$

Proceed recursively

codim $\leq c$

$X_2 = V(f_1, \ldots, f_c, g) \setminus X_1$

Proceed recursively

This time suppose we have function

$$\text{syzcof}(X)\text{: returns } g, i \text{ s.t. } gf_i \in \langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c \rangle, g \notin I(X)$$

$\rightsquigarrow$ done with signature-based computations

codim $\leq c$

$X = V(f_1, \ldots, f_c)$

codim $\leq c - 1$

$X_1 := V(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_c) \setminus V(g)$

Proceed recursively

codim $\leq c$

$X_2 = V(f_1, \ldots, f_c, g) \setminus X_1$

Proceed recursively

Termination: when codim bound is matched

This time suppose we have function

$$\text{syzcof}(X)\text{: returns } g, i \text{ s.t. } gf_i \in \langle f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_c \rangle, g \notin I(X)$$

$\rightsquigarrow$ done with signature-based computations

codim $\leq c$

$X = V(f_1, \dots, f_c)$

codim $\leq c - 1$

$X_1 := V(f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_c) \setminus V(g)$

Proceed recursively

codim $\leq c$

$X_2 = V(f_1, \dots, f_c, g) \setminus X_1$

Proceed recursively

Termination: when codim bound is matched

X alg. set, $X_1 := V(h_1, \ldots, h_s)$. Define

$$\mathrm{hull}(X, h_1) := X \setminus \overline{X \setminus V(h_1)}$$

X alg. set, $X_1 := V(h_1, \ldots, h_s)$. Define

$$\mathrm{hull}(X, h_1) := X \setminus \overline{X \setminus V(h_1)}$$

Then

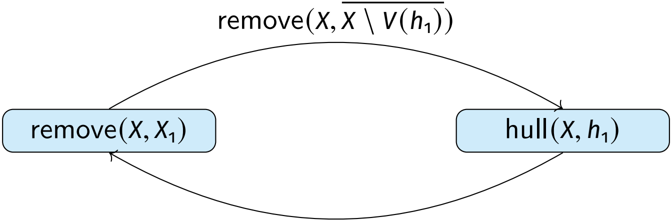
$$\overline{X \setminus X_1} = \overline{X \setminus V(h_1)} \sqcup \overline{\mathrm{hull}(X \setminus V(h_2, \ldots, h_s), h_1)}$$

X alg. set, $X_1 := V(h_1, \ldots, h_s)$. Define

$$\mathrm{hull}(X, h_1) := X \setminus \overline{X \setminus V(h_1)}$$

Then

$$\overline{X \setminus X_1} = \overline{X \setminus V(h_1)} \sqcup \overline{\mathrm{hull}(X \setminus V(h_2, \ldots, h_s), h_1)}$$

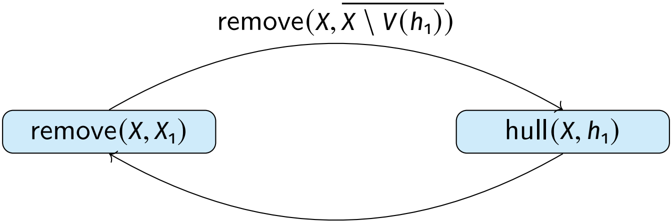


X alg. set, $X_1 := V(h_1, \ldots, h_s)$. Define

$$\mathrm{hull}(X, h_1) := X \setminus \overline{X \setminus V(h_1)}$$

Then

$$\overline{X \setminus X_1} = \overline{X \setminus V(h_1)} \sqcup \overline{\mathrm{hull}(X \setminus V(h_2, \ldots, h_s), h_1)}$$



Output has no redundancies

	Non-Incremental Algorithm	Incremental Algorithm
Cyclic(8)	∞	381.2
PS(14)	248.2	3128.3
PS(16)	13666.2	∞
SOS(7,5)	112.2	∞
Steiner	404.9	870.0
sys2161	26.2	7.54
ED(3,4)	30.7	294.1
ED(3,5)	828.1	∞

Computed in characteristic 65521 on Intel Xeon Gold 6244.
Reference: Preprint to come!

Other strategy: (Berthomieu, Mohr 2024), Computing Generic Fibers of Polynomial Ideals using FGLM and Hensel Lifting

	Non-Incremental Algorithm	Incremental Algorithm
Cyclic(8)	∞	381.2
PS(14)	248.2	3128.3
PS(16)	13666.2	∞
SOS(7,5)	112.2	∞
Steiner	404.9	870.0
sys2161	26.2	7.54
ED(3,4)	30.7	294.1
ED(3,5)	828.1	∞

Computed in characteristic 65521 on Intel Xeon Gold 6244.
Reference: Preprint to come!

Other strategy: (Berthomieu, Mohr 2024), Computing Generic Fibers of Polynomial Ideals using FGLM and Hensel Lifting

Thank you!