# Comprehensive Gröbner Bases and their Applications

Marek Rychlik

Department of Mathematics
University of Arizona

February 3, 2009

Outline

## Software

- *Maxima Gröbner package*, distributed with the *Maxima* open source CAS, based on *DOE MACSYMA*, the grand daddy of all CAS.
- *CGBLisp*, a standalone CAS for calculations with Gröbner and Comprehensive Gröbner bases.
- The development versions can be obtained from my development site: http://marekrychlik.com

## Software

- *Maxima Gröbner package*, distributed with the *Maxima* open source CAS, based on *DOE MACSYMA*, the grand daddy of all CAS.
- *CGBLisp*, a standalone CAS for calculations with Gröbner and Comprehensive Gröbner bases.
- The development versions can be obtained from my development site: http://marekrychlik.com

## Software

- *Maxima Gröbner package*, distributed with the *Maxima* open source CAS, based on *DOE MACSYMA*, the grand daddy of all CAS.
- *CGBLisp*, a standalone CAS for calculations with Gröbner and Comprehensive Gröbner bases.
- The development versions can be obtained from my development site: http://marekrychlik.com

## Gröbner Basis dictionary

- Variables: $\mathbf{x} = (x_1, x_2, \ldots, x_n)$
- A *computable ring k*, i.e. a ring in which all structure operations can be performed constructively.
- Rings $\mathbb{Z}, \mathbb{Q}, \bar{\mathbb{Q}} \subset \mathbb{C}, \mathbb{Z}_p$ are all computable rings.
- A finite algebraic extension of a computable ring is also computable.
- The ring of real numbers $\mathbb{R}$ is not computable.

## Gröbner Basis dictionary

- Variables: $\mathbf{x} = (x_1, x_2, \ldots, x_n)$
- A *computable ring* $k$, i.e. a ring in which all structure operations can be performed constructively.
- Rings $\mathbb{Z}, \mathbb{Q}, \bar{\mathbb{Q}} \subset \mathbb{C}, \mathbb{Z}_p$ are all computable rings.
- A finite algebraic extension of a computable ring is also computable.
- The ring of real numbers $\mathbb{R}$ is not computable.

## Gröbner Basis dictionary

- Variables: $\mathbf{x} = (x_1, x_2, \ldots, x_n)$
- A *computable ring* $k$, i.e. a ring in which all structure operations can be performed constructively.
- Rings $\mathbb{Z}, \mathbb{Q}, \bar{\mathbb{Q}} \subset \mathbb{C}, \mathbb{Z}_p$ are all computable rings.
- A finite algebraic extension of a computable ring is also computable.
- The ring of real numbers $\mathbb{R}$ is not computable.

Gröbner Basis dictionary

- Variables: $\mathbf{x} = (x_1, x_2, \ldots, x_n)$
- A *computable ring k*, i.e. a ring in which all structure operations can be performed constructively.
- Rings $\mathbb{Z}, \mathbb{Q}, \bar{\mathbb{Q}} \subset \mathbb{C}, \mathbb{Z}_p$ are all computable rings.
- A finite algebraic extension of a computable ring is also computable.
- The ring of real numbers $\mathbb{R}$ is not computable.

Gröbner Basis dictionary

- Variables: $\mathbf{x} = (x_1, x_2, \ldots, x_n)$
- A *computable ring k*, i.e. a ring in which all structure operations can be performed constructively.
- Rings $\mathbb{Z}, \mathbb{Q}, \bar{\mathbb{Q}} \subset \mathbb{C}, \mathbb{Z}_p$ are all computable rings.
- A finite algebraic extension of a computable ring is also computable.
- The ring of real numbers $\mathbb{R}$ is not computable.

## Gröbner Basis dictionary

- Polynomial ring: $R = k[\mathbf{x}]$.
- A finitely generated ideal:

$$I = \mathrm{Id}(F) = \left\{ \sum_{j=1}^{s} a_j f_j : a_j \in R \right\}$$

  where $F = \{f_1, f_2, \ldots, f_n\} \subseteq k[\mathbf{x}]$ is a set of generators.
- Variety: $V(F) = \bigcap_{f \in F} f^{-1}(0)$

## Gröbner Basis dictionary

- Polynomial ring: $R = k[\mathbf{x}]$.
- A finitely generated ideal:

$$I = \mathrm{Id}(F) = \left\{ \sum_{j=1}^{s} a_j f_j : a_j \in R \right\}$$

  where $F = \{f_1, f_2, \ldots, f_n\} \subseteq k[\mathbf{x}]$ is a set of generators.
- Variety: $V(F) = \bigcap_{f \in F} f^{-1}(0)$

## Gröbner Basis dictionary

- Polynomial ring: $R = k[\mathbf{x}]$.
- A finitely generated ideal:

$$I = \mathrm{Id}(F) = \left\{ \sum_{j=1}^{s} a_j f_j : a_j \in R \right\}$$

  where $F = \{f_1, f_2, \ldots, f_n\} \subseteq k[\mathbf{x}]$ is a set of generators.
- Variety: $V(F) = \bigcap_{f \in F} f^{-1}(0)$

## Radical ideal

### Definition

If $I \subset R$ is an ideal then the *radical ideal* of $I$ is defined as follows;

$$\sqrt{I} = \{f \in R : \exists n \geq 0 \; f^n \in I\}$$

## Monomial and term ordering

- A *monomial* is

$$\mathbf{x}^{\alpha} = \prod_{i=1}^{n} x_i^{\alpha_i}$$

  where $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a multi-index.
- The *degree* of $\mathbf{x}^{\alpha}$ is

$$|\alpha| = \sum_{i=1}^{n} \alpha_j.$$

## Monomial and term ordering

### Definition

Monomial ordering $\succ$ is *admissible* if:

- $\succ$ is *total*;
- *compatible with multiplication:*

$$\forall \alpha, \beta, \gamma \; \mathbf{x}^{\alpha} \succ \mathbf{x}^{\beta} \Rightarrow \mathbf{x}^{\alpha}\mathbf{x}^{\gamma} \succ \mathbf{x}^{\beta}\mathbf{x}^{\gamma};$$

- $\succ$ is a *well-ordering*: every decreasing sequence has smallest element.

## The lexicographic order

- The variables are ordered: $x_1 \succ x_2 \succ \ldots \succ x_n$.
- If $\mathbf{x}^\alpha$ and $\mathbf{x}^\beta$ are two monomials then $\mathbf{x}^\alpha \succ \mathbf{x}^\beta$ is defined as follows: Let $k \in \{1, 2, 3, \ldots, n\}$ be the unique number such that
  - For $j = 1, 2, \ldots, k$ we have $\alpha_j = \beta_j$.
  - Either $k = n$ or $\alpha_{k+1} \neq \beta_{k+1}$.

  Then $\mathbf{x}^\alpha \succ \mathbf{x}^\beta$ if $k < n$ and $\alpha_{k+1} > \beta_{k+1}$.

Standard admissible monomial orders

- Lexicographic (*lex*)

**Definition**

An admissible order is called *graded* if a monomial with a larger degree succeeds a monomial with a smaller degree.

- Graded lexicographic (*grlex*); ties broken by lexicographic order.
- Graded reverse lexicographic (*grevlex*); ties broken by the reverse lexicographic order, i.e. if $\mathbf{x}^\alpha \prec_{lex} \mathbf{x}^\beta$ and $|\alpha| = |\beta|$ then $\mathbf{x}^\alpha \succ_{grlex} \mathbf{x}^\beta$.

## Leading monomials, terms and coefficients

- Let us write a polynomial $f$ as

$$f = \sum_{m \in M(f)} a(m)m$$

where $m$ is a monomial, $M(f)$ is a finite set of monomials of $f$, and $a(m)$ is its coefficient at $m$.

$LM(f)$ Leading monomial, largest according to the monomial order in effect.

$LC(f)$ Leading coefficient.

$LT(f)$ Leading term.

- Identity:

$$LT(f) = LC(f) \cdot LM(f)$$

# Division algorithm

**Input**: $f_1, f_2, \ldots, f_s, f \in k[\mathbf{x}]$
**Output**: $a_1, a_2, \ldots, a_s, r \in k[\mathbf{x}]$ such that
$f = a_1 f_1 + a_2 f_2 + \ldots + a_s f_s + r$
and for $i = 1, 2, \ldots, s$ we have $LM(f_i) \not| LM(r)$.

**for** $i := 1$ **to** s **do**
  $a_i := 0$
$p := f$
**while** $p \neq 0$ **do**
  $i := 1$
  $flag :=$ **false**
  **while** $i \leq s$ **and** $flag =$ **false do**
    **if** $LT(f_i) | LT(p)$ **then**
      $a_i := a_i + LT(p)/LT(f_i)$
      $p := p - (LT(p)/LT(f_i))f_i$
      $flag :=$ **true**
    **else**
      $i := i + 1$
  **if** $flag =$ **false** then
    $r := r + LT(p)$
    $p := p - LT(p)$

## Ideal Membership Problem and the division algorithm

### Problem

*Let the variable ordering be* $x \prec y \prec z$ *and the monomial ordering be* lex. *Let* $f = \underline{z^3} - y^4$, $f_1 = \underline{y^2} - x^3$, *and* $f_2 = \underline{z} - x^2$. *Is* $f$ *in the ideal* $\mathrm{Id}(\{f_1, f_2\})$?

# Ideal Membership Problem and the division algorithm

$$
\begin{array}{lll}
 & a_1 : -y^2 - x^3 & \\
 & a_2 : z^2 + x^2 z + x^4 & \\
f_1 : y^2 - x^3 & & \\
f_2 : z - x^2 & f : \underline{z^3} - y^4 & \\
(f_2, z^2) & z^3 - x^2 z^2 & \\
 & \hline & \\
 & \quad -y^4 + \underline{x^2 z^2} & \\
(f_2, x^2 z) & \quad x^2 z^2 - x^4 z & \\
 & \quad \hline & \\
 & \quad\quad -y^4 + \underline{x^4 z} & \\
(f_2, x^4) & \quad\quad x^4 z - x^6 & \\
 & \quad\quad \hline & \\
 & \quad\quad\quad -\underline{y^4} + x^6 & \\
(f_1, -y^2) & \quad\quad\quad -y^4 + x^3 y^2 & \\
 & \quad\quad\quad \hline & \\
 & \quad\quad\quad\quad x^6 - \underline{x^3 y^2} & \\
(f_1, -x^3) & \quad\quad\quad\quad -x^3 y^2 + x^6 & \\
 & \quad\quad\quad\quad \hline & \\
 & \quad\quad\quad\quad\quad 0 &
\end{array}
$$

Note: The leading terms have been underlined.

Ideal Membership Problem and the division algorithm
Thus

$$f = (-y^2 - x^3)(y^2 - x^3) + (z^2 + x^2 z + x^4)(z - x^2)$$

and $f \in I$.
We note that the division algorithm always produces quotients $a_i$ with the property

$$LT(a_i f_i) \preceq LT(f).$$

Why Gröbner Bases?

- The division algorithm by a random set of polynomials $F$ may yield a remainder $r \neq 0$ even if $f \in I$.
- This problem does not occur if $F$ is a *Gröbner basis*.

Why Gröbner Bases?

- The division algorithm by a random set of polynomials $F$ may yield a remainder $r \neq 0$ even if $f \in I$.
- This problem does not occur if $F$ is a *Gröbner basis*.

## Notation

- Let $F \subseteq k[\mathbf{x}]$ be an arbitrary (finite or infinite) set of polynomials.
- The *leading monomial set* of $F$ is defined as

$$LM(F) = \{LM(f) : f \in F\}.$$

- The *leading term set* of $F$ is defined as

$$LT(F) = \{LT(f) : f \in F\}$$

- If $F$ is a polynomial ideal then so is $LM(F)$. Moreover, if $F$ is an arbitrary set then

$$\mathrm{Id}(LM(F)) = LM(\mathrm{Id}(F)).$$

## Notation

- Let $F \subseteq k[\mathbf{x}]$ be an arbitrary (finite or infinite) set of polynomials.
- The *leading monomial set* of $F$ is defined as

$$LM(F) = \{LM(f) : f \in F\}.$$

- The *leading term set* of $F$ is defined as

$$LT(F) = \{LT(f) : f \in F\}$$

- If $F$ is a polynomial ideal then so is $LM(F)$. Moreover, if $F$ is an arbitrary set then

$$\mathrm{Id}(LM(F)) = LM(\mathrm{Id}(F)).$$

## Notation

- Let $F \subseteq k[\mathbf{x}]$ be an arbitrary (finite or infinite) set of polynomials.
- The *leading monomial set* of $F$ is defined as

$$LM(F) = \{LM(f) : f \in F\}.$$

- The *leading term set* of $F$ is defined as

$$LT(F) = \{LT(f) : f \in F\}$$

- If $F$ is a polynomial ideal then so is $LM(F)$. Moreover, if $F$ is an arbitrary set then

$$\mathrm{Id}(LM(F)) = LM(\mathrm{Id}(F)).$$

## Notation

- Let $F \subseteq k[\mathbf{x}]$ be an arbitrary (finite or infinite) set of polynomials.
- The *leading monomial set* of $F$ is defined as

$$LM(F) = \{LM(f) : f \in F\}.$$

- The *leading term set* of $F$ is defined as

$$LT(F) = \{LT(f) : f \in F\}$$

- If $F$ is a polynomial ideal then so is $LM(F)$. Moreover, if $F$ is an arbitrary set then

$$\mathrm{Id}(LM(F)) = LM(\mathrm{Id}(F)).$$

Precise definition of Gröbner Bases

## Definition

A Gröbner basis is a set of polynomials $G$ such that

$$LM(G) = LM(\mathrm{Id}(G))$$

Equivalently, if $f \in \mathrm{Id}(G)$ then $LM(f)$ is divisible by $LM(g)$ for some $g \in G$.

Some properties of Gröbner Bases

- The *Hilbert basis theorem* implies that every polynomial ideal has a *finite* Gröbner basis.
- Gröbner bases can be algorithmically constructed using *Buchberger algorithm* or its versions.
- The recent algorithms of Faugère are reported to perform better, but they are not freely available.

## The S-polynomial (syzygy-polynomial)

### Definition

Let $f$ and $g$ be two polynomials in $k[\mathbf{x}]$. The *syzygy polynomial* of $f$ and $g$ is defined as follows: Let $\mathbf{t} = LCM(LT(f), LT(g))$. Then

$$S(f,g) = \frac{\mathbf{t}}{LT(f)} f - \frac{\mathbf{t}}{LT(g)} g. \tag{1}$$

The above definition may differ from one in texts which emphasize the case when $k$ is a field: let $\mathbf{x}^\gamma = LCM(LM(f), LM(g))$. Then

$$\tilde{S}(f,g) = \frac{\mathbf{x}^\gamma}{LT(f)} f - \frac{\mathbf{x}^\gamma}{LT(g)} g. \tag{2}$$

Since for many applications $k$ itself is a polynomial ring, and thus not a field, we choose to work with the first definition.

## Buchberger Criterion

### Theorem

*A subset $G \subseteq k[\mathbf{x}]$ is a Gröbner basis (of the ideal $\mathrm{Id}(G)$ it generates) iff for every $f, g \in G$ we have*

$$S(f,g) \xrightarrow[G]{} 0$$

*i.e. the remainder of division of $S(f,g)$ by $G$ is $0$.*

## An Example of Buchberger criterion

### Problem

*Let* $V = \{(t^2, t^3, t^4) : t \in k\}$. *Show that* $I = I(V) = \mathrm{Id}(\{y^2 - x^3, z - x^2\})$.

The solution amounts to showing that $G = \{g_1, g_2\}$ where $g_1 = y^2 - x^3$ and $g_2 = z - x^2$, is a Gröbner basis of this ideal with variable ordering $x \prec y \prec z$ and lex ordering. This can be verified using Buchberger criterion.

$$S(g_1, g_2) = z(y^2 - x^3) - y^2(z - x^2) = -x^3 z + x^2 y^2$$

# An Example of Buchberger criterion

## Problem

*Let* $V = \{(t^2, t^3, t^4) : t \in k\}$. *Show that* $I = I(V) = \mathrm{Id}(\{y^2 - x^3, z - x^2\})$.

The division algorithm yields 0:

$$\begin{array}{ll} & a_1 : x^2 \\ & a_2 : -x^3 \\ & \\ y^2 - x^3 & -x^3 z + x^2 y^2 \\ z - x^2 & -x^3 z + x^5 \\ & \hline \\ & x^2 y^2 - x^5 \\ & x^2 y^2 - x^5 \\ & \hline \\ & 0 \end{array}$$

## An Example of Buchberger criterion

### Problem

*Let* $V = \{(t^2, t^3, t^4) : t \in k\}$. *Show that* $I = I(V) = \mathrm{Id}(\{y^2 - x^3, z - x^2\})$.

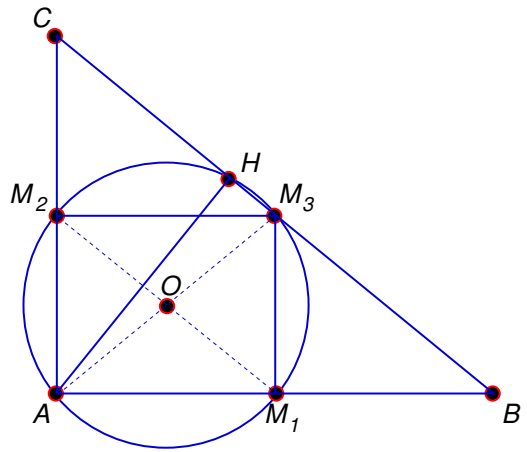
We complete the proof of $I = \mathrm{Id}(V)$ by considering $f \in I(V)$. We write it as $f = a_1 f_1 + a_2 f_2 + r$, where $r \in I(V)$ as well. But $r = a(x) + yb(x)$ because no term of $r$ is divisible by $z$ or $y^2$. But the substitution $x = t^2, y = t^3$ yields $a(t^2) + t^3 b(t^2)$. Thus $a(t^2) \equiv 0$ and $b(t^2) \equiv 0$ (even-odd powers). Hence $a = b = 0$. Also $\sqrt{I} = I$ because an ideal of a variety is always radical ($k$ *does not have to be an algebraically closed field* for this argument to work).

Buchberger algorithm

In the following algorithm $NormalForm(S, G)$ denotes the remainder part of the output of the division algorithm of $S$ by $G$.

**Input**: $F = (f_1, f_2, \ldots, f_s)$ where $f_i \in k[\mathbf{x}]$
**Output**: a Gröbner basis $G = (g_1, g_2, \ldots, g_t)$ of $\mathrm{Id}(F)$
$G := F$
**repeat**
$G' := G$
**for each pair** $\{p, q\}$, $p \neq q$, **in** $G$ **do**
$S := NormalForm(S(p, q), G)$
**if** $S \neq 0$ **then** $G' := G' \cup \{S\}$
**until** $G = G'$

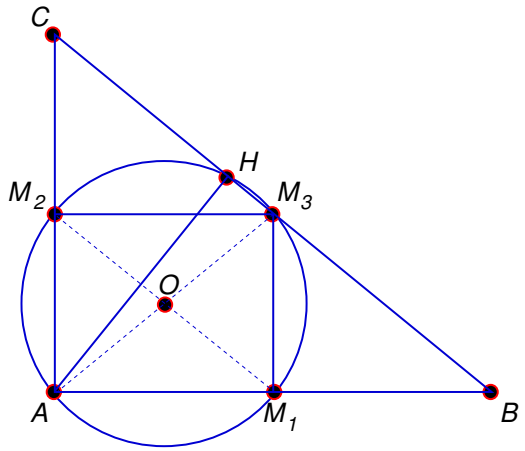
# Apollonius Circle Theorem




## Theorem

*(Apollonius Circle Theorem) If ABC is a triangle, $M_1$, $M_2$, $M_3$ are the centers of the sides and H is the foot of the altitude drawn from A then, $M_1$, $M_2$, $M_3$ and H lie on one circle.*

# Apollonius Circle Theorem

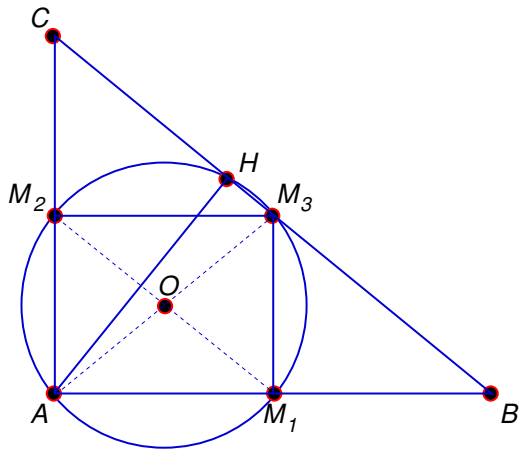



Let $A = (0, 0)$, $B = (u_1, 0)$ and $C = (0, u_2)$. Thus,

$$\begin{aligned} M_1 &= (\frac{u_1}{2}, 0), \\ M_2 &= (0, \frac{u_2}{2}), \\ M_3 &= (\frac{u_1}{2}, \frac{u_2}{2}) \end{aligned}$$

are the midpoints of the sides. Let $H = (x_1, x_2)$.

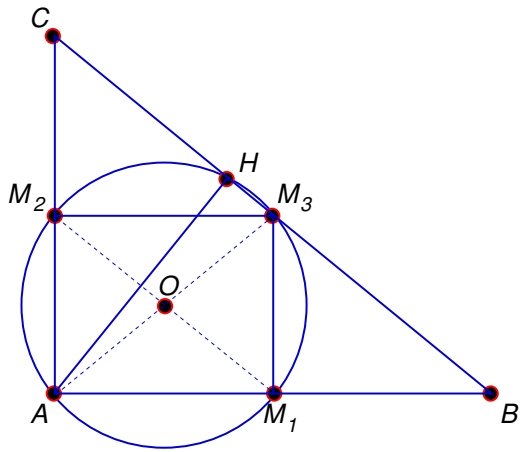
# Apollonius Circle Theorem




$AM_1M_3M_2$ is a rectangle, so the circle containing $A, M_1, M_2, M_3$ is

$$(x_1 - u_1/4)^2 + (x_2 - u_2/4)^2 = (u_1/4)^2 + (u_2/4)^2.$$

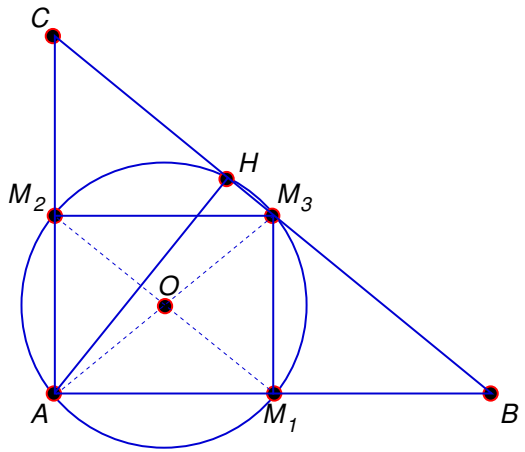
# Apollonius Circle Theorem




The conditions on $H$ are:

1. $AH \perp BC$;
2. $B, C, H$ are collinear.

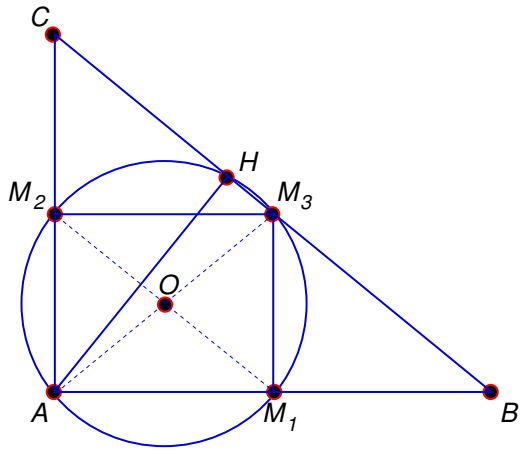
# Apollonius Circle Theorem




The condition $AH \perp BC$ translates into

$$f_1 = (x_1, x_2).(u_1, -u_2) = 0.$$

# Apollonius Circle Theorem




The condition that $B, C, H$ are collinear translates into vanishing of the determinant:

$$f_2 = \begin{vmatrix} u_1 & 0 & 1 \\ 0 & u_2 & 1 \\ x_1 & x_2 & 1 \end{vmatrix} = 0$$

## An algebraic fomulation of Apollonius Circle Theorem

- The expanded polynomials are:

$$\begin{aligned} f_1 &= x_1 u_1 - x_2 u_2, \\ f_2 &= -x_1 u_2 - u_1 x_2 + u_1 u_2 \\ f &= (x_1 - u_1/4)^2 + (x_2 - u_2/4)^2 - (u_1/4)^2 - (u_2/4)^2 \\ &= x_2^2 - u_2 x_2/2 + x_1^2 - u_1 x_1/2. \end{aligned}$$

- Apollonius Circle Theorem admits the following reformulation:

$$\forall u_1 > 0, u_2 > 0 \; (f_1 = 0 \wedge f_2 = 0) \Rightarrow f = 0$$

- We can see the need to replace the above statement by one without the quantifiers.

## "Follows strictly" Definition

**Definition**

A polynomial $f \in S$ *follows strictly* from $f_1, \ldots, f_s \in k[\mathbf{u}, \mathbf{x}]$ if

$$f \in \mathrm{Id}(V(f_1, \ldots, f_s)).$$

- It is worth noting that this definition does not distinguish between parameters and variables.

## Properties

- Over algebraically closed fields, for any set of polynomials $F$:
$$\mathrm{Id}(V(F)) = \sqrt{\mathrm{Id}(F)}.$$
- If $k$ is algebraically closed then $f$ follows strictly from $F$ iff
$$f \in \sqrt{\mathrm{Id}(\{f_1, f_2, \ldots, f_s\})}.$$
- If $k = \mathbb{R}$ then we have no simple algebraic criterion; however, if if $f$ follows strictly over $\mathbb{C}$ then it follows strictly over $\mathbb{R}$.
- Hardly any classical geometry theorem translated into the language of algebra leads to a true algebraic statement; this is due to exceptional parameters.

## Properties

- Over algebraically closed fields, for any set of polynomials $F$:
$$\mathrm{Id}(V(F)) = \sqrt{\mathrm{Id}(F)}.$$
- If $k$ is algebraically closed then $f$ follows strictly from $F$ iff
$$f \in \sqrt{\mathrm{Id}(\{f_1, f_2, \ldots, f_s\})}.$$
- If $k = \mathbb{R}$ then we have no simple algebraic criterion; however, if if $f$ follows strictly over $\mathbb{C}$ then it follows strictly over $\mathbb{R}$.
- Hardly any classical geometry theorem translated into the language of algebra leads to a true algebraic statement; this is due to exceptional parameters.

## Properties

- Over algebraically closed fields, for any set of polynomials $F$:
$$\mathrm{Id}(V(F)) = \sqrt{\mathrm{Id}(F)}.$$
- If $k$ is algebraically closed then $f$ follows strictly from $F$ iff
$$f \in \sqrt{\mathrm{Id}(\{f_1, f_2, \ldots, f_s\})}.$$
- If $k = \mathbb{R}$ then we have no simple algebraic criterion; however, if if $f$ follows strictly over $\mathbb{C}$ then it follows strictly over $\mathbb{R}$.
- Hardly any classical geometry theorem translated into the language of algebra leads to a true algebraic statement; this is due to exceptional parameters.

## Properties

- Over algebraically closed fields, for any set of polynomials $F$:
$$\mathrm{Id}(V(F)) = \sqrt{\mathrm{Id}(F)}.$$
- If $k$ is algebraically closed then $f$ follows strictly from $F$ iff
$$f \in \sqrt{\mathrm{Id}(\{f_1, f_2, \ldots, f_s\})}.$$
- If $k = \mathbb{R}$ then we have no simple algebraic criterion; however, if if $f$ follows strictly over $\mathbb{C}$ then it follows strictly over $\mathbb{R}$.
- Hardly any classical geometry theorem translated into the language of algebra leads to a true algebraic statement; this is due to exceptional parameters.

# Apollonius Circle Theorem and "follows strictly"

$$\begin{aligned} f_1 &= x_1 u_1 - x_2 u_2, \\ f_2 &= -x_1 u_2 - u_1 x_2 + u_1 u_2 \\ f &= (x_1 - u_1/4)^2 + (x_2 - u_2/4)^2 - (u_1/4)^2 - (u_2/4)^2 \\ &= x_2^2 - u_2 x_2/2 + x_1^2 - u_1 x_1/2. \end{aligned}$$

- We claim that $f$ does not follow strictly from $f_1$ and $f_2$. To see it, we observe that
  1. if $(\mathbf{u}, \mathbf{x}) \in V(\{u_1, u_2\})$ then $(\mathbf{u}, \mathbf{x}) \in V(\{f_1, f_2\})$;
  2. thus, $V(\{u_1, u_2\})$ is a subset of $V(\{f_1, f_2\})$;
  3. this means that when $u_1 = u_2 = 0$, $(x_1, x_2)$ are arbitrary.
- Hence, $f$ does not have to vanish.

## Apollonius Circle Theorem and "follows strictly"

$$\begin{aligned} f_1 &= x_1 u_1 - x_2 u_2, \\ f_2 &= -x_1 u_2 - u_1 x_2 + u_1 u_2 \\ f &= (x_1 - u_1/4)^2 + (x_2 - u_2/4)^2 - (u_1/4)^2 - (u_2/4)^2 \\ &= x_2^2 - u_2 x_2/2 + x_1^2 - u_1 x_1/2. \end{aligned}$$

- We claim that $f$ does not follow strictly from $f_1$ and $f_2$. To see it, we observe that
  1. if $(\mathbf{u}, \mathbf{x}) \in V(\{u_1, u_2\})$ then $(\mathbf{u}, \mathbf{x}) \in V(\{f_1, f_2\})$;
  2. thus, $V(\{u_1, u_2\})$ is a subset of $V(\{f_1, f_2\})$;
  3. this means that when $u_1 = u_2 = 0$, $(x_1, x_2)$ are arbitrary.
- Hence, $f$ does not have to vanish.

## Apollonius Circle Theorem and "follows strictly"

$$\begin{aligned} f_1 &= x_1 u_1 - x_2 u_2, \\ f_2 &= -x_1 u_2 - u_1 x_2 + u_1 u_2 \\ f &= (x_1 - u_1/4)^2 + (x_2 - u_2/4)^2 - (u_1/4)^2 - (u_2/4)^2 \\ &= x_2^2 - u_2 x_2/2 + x_1^2 - u_1 x_1/2. \end{aligned}$$

- We claim that $f$ does not follow strictly from $f_1$ and $f_2$. To see it, we observe that
  1. if $(\mathbf{u}, \mathbf{x}) \in V(\{u_1, u_2\})$ then $(\mathbf{u}, \mathbf{x}) \in V(\{f_1, f_2\})$;
  2. thus, $V(\{u_1, u_2\})$ is a subset of $V(\{f_1, f_2\})$;
  3. this means that when $u_1 = u_2 = 0$, $(x_1, x_2)$ are arbitrary.
- Hence, $f$ does not have to vanish.

## Apollonius Circle Theorem and "follows strictly"

$$\begin{aligned} f_1 &= x_1 u_1 - x_2 u_2, \\ f_2 &= -x_1 u_2 - u_1 x_2 + u_1 u_2 \\ f &= (x_1 - u_1/4)^2 + (x_2 - u_2/4)^2 - (u_1/4)^2 - (u_2/4)^2 \\ &= x_2^2 - u_2 x_2/2 + x_1^2 - u_1 x_1/2. \end{aligned}$$

- We claim that $f$ does not follow strictly from $f_1$ and $f_2$. To see it, we observe that
  1. if $(\mathbf{u}, \mathbf{x}) \in V(\{u_1, u_2\})$ then $(\mathbf{u}, \mathbf{x}) \in V(\{f_1, f_2\})$;
  2. thus, $V(\{u_1, u_2\})$ is a subset of $V(\{f_1, f_2\})$;
  3. this means that when $u_1 = u_2 = 0$, $(x_1, x_2)$ are arbitrary.
- Hence, $f$ does not have to vanish.

## Apollonius Circle Theorem and "follows strictly"

$$\begin{aligned} f_1 &= x_1 u_1 - x_2 u_2, \\ f_2 &= -x_1 u_2 - u_1 x_2 + u_1 u_2 \\ f &= (x_1 - u_1/4)^2 + (x_2 - u_2/4)^2 - (u_1/4)^2 - (u_2/4)^2 \\ &= x_2^2 - u_2 x_2/2 + x_1^2 - u_1 x_1/2. \end{aligned}$$

- We claim that $f$ does not follow strictly from $f_1$ and $f_2$. To see it, we observe that
  1. if $(\mathbf{u}, \mathbf{x}) \in V(\{u_1, u_2\})$ then $(\mathbf{u}, \mathbf{x}) \in V(\{f_1, f_2\})$;
  2. thus, $V(\{u_1, u_2\})$ is a subset of $V(\{f_1, f_2\})$;
  3. this means that when $u_1 = u_2 = 0$, $(x_1, x_2)$ are arbitrary.
- Hence, $f$ does not have to vanish.

## Apollonius Circle Theorem and "follows strictly"

$$\begin{aligned} f_1 &= x_1 u_1 - x_2 u_2, \\ f_2 &= -x_1 u_2 - u_1 x_2 + u_1 u_2 \\ f &= (x_1 - u_1/4)^2 + (x_2 - u_2/4)^2 - (u_1/4)^2 - (u_2/4)^2 \\ &= x_2^2 - u_2 x_2/2 + x_1^2 - u_1 x_1/2. \end{aligned}$$

- We claim that $f$ does not follow strictly from $f_1$ and $f_2$. To see it, we observe that
  1. if $(\mathbf{u}, \mathbf{x}) \in V(\{u_1, u_2\})$ then $(\mathbf{u}, \mathbf{x}) \in V(\{f_1, f_2\})$;
  2. thus, $V(\{u_1, u_2\})$ is a subset of $V(\{f_1, f_2\})$;
  3. this means that when $u_1 = u_2 = 0$, $(x_1, x_2)$ are arbitrary.
- Hence, $f$ does not have to vanish.

## Equivalent correct reformulations

$$\begin{aligned}
\forall u_1, u_2 \quad & \big(f_1 = 0 \wedge f_2 = 0 \wedge (u_1 \neq 0 \vee u_2 \neq 0)\big) \Rightarrow f = 0 \\
\forall u_1, u_2 \quad & \big(f_1 = 0 \wedge f_2 = 0 \wedge (u_1 u_2 \neq 0)\big) \Rightarrow f = 0 \\
\forall u_1, u_2 \quad & \big(f_1 = 0 \wedge f_2 = 0\big) \Rightarrow \big(f = 0 \vee u_1 u_2 = 0\big) \\
\forall u_1, u_2 \quad & \big(f_1 = 0 \wedge f_2 = 0\big) \Rightarrow u_1 u_2 f = 0
\end{aligned}$$

## Quantifier-free versions:

$$\begin{aligned}
u_1 u_2 f &\in I(V(\{f_1, f_2\})) \\
u_1 u_2 f &\in \sqrt{\mathrm{Id}(\{f_1, f_2\})} \quad (k \text{ algebraically closed})
\end{aligned}$$

The saturation ideal

**Definition**

Given two ideals $I, J \subseteq k[\mathbf{x}]$, the *saturation ideal* is defined as follows:

$$I : J^{\infty} = \{f \in k[\mathbf{x}] : \ \exists g \in J \, \exists n \geq 0 \ g^n f \in I\}$$

## Calculating Gröbner Basis of the saturation ideal

Gröbner basis of the saturation ideal can be computed in these steps:

1. Let $I = \mathrm{Id}(\{f_1, f_2, \ldots, f_s\})$ and $G = \mathrm{Id}(\{g_1, g_2, \ldots, g_r\}$.
2. We form the set

$$F' = F \cup \{1 - t_1 g_1 - \ldots - t_r g_r\}$$

   where $t_1, t_2, \ldots, t_r$ are new variables.
3. We compute the Gröbner basis $H'$ of $\mathrm{Id}(F')$ with respect to a monomial order order in which all monomials containing $t$'s precede all monomials that do not depend on $t$'s.
4. The subset $H \subseteq H'$ of those polynomials which do not depend on $t$'s is a Gröbner basis of $I : J^{\infty}$.

## Calculating Gröbner Basis of the saturation ideal

Gröbner basis of the saturation ideal can be computed in these steps:

1. Let $I = \mathrm{Id}(\{f_1, f_2, \ldots, f_s\})$ and $G = \mathrm{Id}(\{g_1, g_2, \ldots, g_r\}$.
2. We form the set

$$F' = F \cup \{1 - t_1 g_1 - \ldots - t_r g_r\}$$

   where $t_1, t_2, \ldots, t_r$ are new variables.
3. We compute the Gröbner basis $H'$ of $\mathrm{Id}(F')$ with respect to a monomial order order in which all monomials containing $t$'s precede all monomials that do not depend on $t$'s.
4. The subset $H \subseteq H'$ of those polynomials which do not depend on $t$'s is a Gröbner basis of $I : J^{\infty}$.

## Calculating Gröbner Basis of the saturation ideal

Gröbner basis of the saturation ideal can be computed in these steps:

1. Let $I = \mathrm{Id}(\{f_1, f_2, \ldots, f_s\})$ and $G = \mathrm{Id}(\{g_1, g_2, \ldots, g_r\}$.
2. We form the set

$$F' = F \cup \{1 - t_1 g_1 - \ldots - t_r g_r\}$$

   where $t_1, t_2, \ldots, t_r$ are new variables.
3. We compute the Gröbner basis $H'$ of $\mathrm{Id}(F')$ with respect to a monomial order order in which all monomials containing $t$'s precede all monomials that do not depend on $t$'s.
4. The subset $H \subseteq H'$ of those polynomials which do not depend on $t$'s is a Gröbner basis of $I : J^{\infty}$.

## Calculating Gröbner Basis of the saturation ideal

Gröbner basis of the saturation ideal can be computed in these steps:

1. Let $I = \mathrm{Id}(\{f_1, f_2, \ldots, f_s\})$ and $G = \mathrm{Id}(\{g_1, g_2, \ldots, g_r\}$.
2. We form the set

$$F' = F \cup \{1 - t_1 g_1 - \ldots - t_r g_r\}$$

   where $t_1, t_2, \ldots, t_r$ are new variables.
3. We compute the Gröbner basis $H'$ of $\mathrm{Id}(F')$ with respect to a monomial order order in which all monomials containing $t$'s precede all monomials that do not depend on $t$'s.
4. The subset $H \subseteq H'$ of those polynomials which do not depend on $t$'s is a Gröbner basis of $I : J^{\infty}$.

## Quantifier Elimination

- Many problems can be formulated as

$$\forall \mathbf{x} \in k^n \qquad (f_1(\mathbf{x}) = 0 \wedge f_2(\mathbf{x}) = 0 \wedge \ldots \wedge f_p(\mathbf{x}) = 0) \\ \Rightarrow (g_1(\mathbf{x} = 0) \vee g_2(\mathbf{x}) = 0 \vee \ldots \vee g_q(\mathbf{x}) = 0)\,.$$

**Theorem**

*When $k$ is algebraically closed, the above statement is equivalent to*

$$1 \in I : J^\infty.$$

*where $I = \mathrm{Id}(\{f_1, f_2, \ldots, f_p\})$ and $J = \mathrm{Id}(\{g_1, g_2, \ldots, g_q\})$.*

## Quantifier Elimination

- Many problems can be formulated as

$$\forall \mathbf{x} \in k^n \qquad (f_1(\mathbf{x}) = 0 \wedge f_2(\mathbf{x}) = 0 \wedge \ldots \wedge f_p(\mathbf{x}) = 0) \\ \Rightarrow (g_1(\mathbf{x} = 0) \vee g_2(\mathbf{x}) = 0 \vee \ldots \vee g_q(\mathbf{x}) = 0)\,.$$

**Theorem**

*When $k$ is algebraically closed, the above statement is equivalent to*

$$1 \in I : J^{\infty}.$$

*where $I = \mathrm{Id}(\{f_1, f_2, \ldots, f_p\})$ and $J = \mathrm{Id}(\{g_1, g_2, \ldots, g_q\})$.*

Testing radical ideal membership — “Rabinowitz trick”

**Theorem**

*The following statements are equivalent:*

$$f \in \sqrt{I} \iff 1 \in I : f^{\infty}$$

*In other words, $f$ belongs to the radical ideal of $I$ iff the saturation ideal $I : f^{\infty}$ is trivial.*

## *CGBlisp* calculations

```
;; An automatic proof of the Apollonius Circle Theorem
;; Encoding by hand
(setf vars '(x1 x2))
(setf params '(u1 u2))
(setf allvars (append vars params))
(setf hypotheses "[x1*u1-x2*u2, -x1*u2-u1*x2+u1*u2]")
(setf conclusions  "[2*x2^2-u2*x2+2*x1^2-u1*x1,u1,u2]")
;; Saturation test
(string-ideal-polysaturation
        hypotheses conclusions allvars)
```

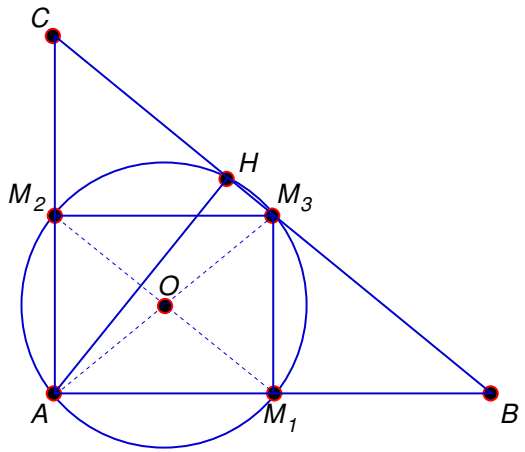
## Calculations using *CGBlisp* package

```
USER(16): (load "../examples/apollonius0" :print 5)
; Loading ../examples/apollonius0.lisp
(X1 X2)
(U1 U2)
(X1 X2 U1 U2)
"[x1*u1-x2*u2, -x1*u2-u1*x2+u1*u2]"
"[2*x2^2-u2*x2+2*x1^2-u1*x1,u1,u2]"
[ 1 ]
NIL
T
```

# A fully automated proof with *CGBLisp*

```
;; Prove Apollonius Circle Theorem:
(prove-theorem
 ;; If
 (
  (perpendicular A B A C) ; AB _|_ AC
  (midpoint B C M)        ; M is the midpoint of BC
  (midpoint A M O)        ; O is the midpoint of AM
  (collinear B H C)       ; H lies on BC
  (perpendicular A H B C) ; AH _|_ BC
  )
 ;; Then
 (
  (equidistant M O H O)   ; MO = HO
  ;; Or
  (identical-points B C)  ; B = C
  )
 )
```

# Apollonius Circle Theorem figure



# The Comprehensive Gröbner Basis framework

- Variables are split into *main variables* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and *parameters* $\mathbf{u} = (u_1, u_2, \ldots, u_l)$.
- Polynomials with parameters: $S = k[\mathbf{u}, \mathbf{x}]$

**Definition**

If $F \subseteq S$ and $\mathbf{a} \in k^l$ then *the specialization (or specification)* $F_{\mathbf{m}} \subseteq R = k[\mathbf{x}]$ is the result of substituting $\mathbf{u} = \mathbf{a}$ into $F$.

- 
- If $G \subseteq S$ is a Gröbner basis then $G_{\mathbf{a}} \subseteq R$ *is not* a Gröbner basis in general.
- It is true that

$$\mathrm{Id}(F_{\mathbf{a}}) = \mathrm{Id}(F)_{\mathbf{a}}$$

# The Comprehensive Gröbner Basis framework

- Variables are split into *main variables* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and *parameters* $\mathbf{u} = (u_1, u_2, \ldots, u_l)$.
- Polynomials with parameters: $S = k[\mathbf{u}, \mathbf{x}]$

**Definition**

If $F \subseteq S$ and $\mathbf{a} \in k^l$ then *the specialization (or specification)* $F_{\mathbf{m}} \subseteq R = k[\mathbf{x}]$ is the result of substituting $\mathbf{u} = \mathbf{a}$ into $F$.

- 
- If $G \subseteq S$ is a Gröbner basis then $G_{\mathbf{a}} \subseteq R$ *is not* a Gröbner basis in general.
- It is true that

$$\mathrm{Id}(F_{\mathbf{a}}) = \mathrm{Id}(F)_{\mathbf{a}}$$

## The Comprehensive Gröbner Basis framework

- Variables are split into *main variables* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and *parameters* $\mathbf{u} = (u_1, u_2, \ldots, u_l)$.
- Polynomials with parameters: $S = k[\mathbf{u}, \mathbf{x}]$

### Definition

If $F \subseteq S$ and $\mathbf{a} \in k^l$ then *the specialization (or specification)* $F_{\mathbf{m}} \subseteq R = k[\mathbf{x}]$ is the result of substituting $\mathbf{u} = \mathbf{a}$ into $F$.

- If $G \subseteq S$ is a Gröbner basis then $G_{\mathbf{a}} \subseteq R$ *is not* a Gröbner basis in general.
- It is true that

$$\mathrm{Id}(F_{\mathbf{a}}) = \mathrm{Id}(F)_{\mathbf{a}}$$

## The Comprehensive Gröbner Basis framework

- Variables are split into *main variables* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and *parameters* $\mathbf{u} = (u_1, u_2, \ldots, u_l)$.
- Polynomials with parameters: $S = k[\mathbf{u}, \mathbf{x}]$

### Definition

If $F \subseteq S$ and $\mathbf{a} \in k^l$ then *the specialization (or specification)* $F_{\mathbf{m}} \subseteq R = k[\mathbf{x}]$ is the result of substituting $\mathbf{u} = \mathbf{a}$ into $F$.

- If $G \subseteq S$ is a Gröbner basis then $G_{\mathbf{a}} \subseteq R$ *is not* a Gröbner basis in general.
- It is true that

$$\mathrm{Id}(F_{\mathbf{a}}) = \mathrm{Id}(F)_{\mathbf{a}}$$

## The Comprehensive Gröbner Basis framework

- Variables are split into *main variables* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and *parameters* $\mathbf{u} = (u_1, u_2, \ldots, u_l)$.
- Polynomials with parameters: $S = k[\mathbf{u}, \mathbf{x}]$

### Definition

If $F \subseteq S$ and $\mathbf{a} \in k^l$ then *the specialization (or specification)* $F_{\mathbf{m}} \subseteq R = k[\mathbf{x}]$ is the result of substituting $\mathbf{u} = \mathbf{a}$ into $F$.

- If $G \subseteq S$ is a Gröbner basis then $G_{\mathbf{a}} \subseteq R$ *is not* a Gröbner basis in general.
- It is true that

$$\mathrm{Id}(F_{\mathbf{a}}) = \mathrm{Id}(F)_{\mathbf{a}}$$

## Comprehensive Gröbner Basis definition

### Definition

A subset $G \subseteq k[\mathbf{u}, \mathbf{x}]$ is called a Comprehensive Groöbner Basis (CGB) if for every parameter $\mathbf{a} \in k^l$ $G_{\mathbf{a}}$ is a Gröbner Basis.

## Comprehensive Gröbner Basis definition

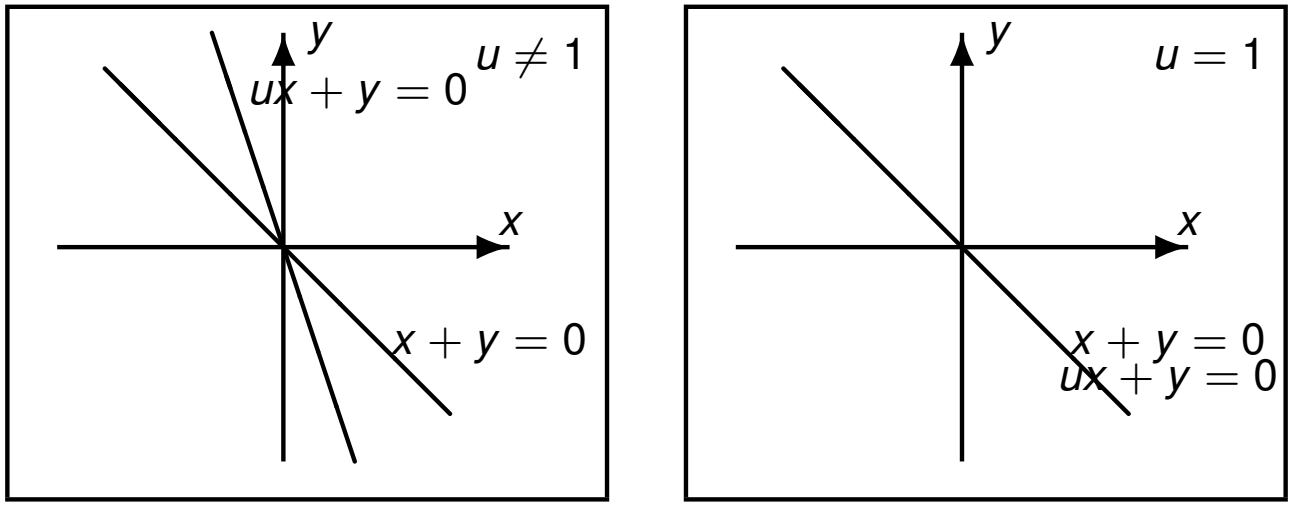
### Definition

A subset $G \subseteq k[\mathbf{u}, \mathbf{x}]$ is called a Comprehensive Groöbner Basis (CGB) if for every parameter $\mathbf{a} \in k^l$ $G_{\mathbf{a}}$ is a Gröbner Basis.

### Theorem

*(Weispfenning, 1990) Every ideal $I \subseteq k[\mathbf{u}, \mathbf{x}]$ has a CGB.*

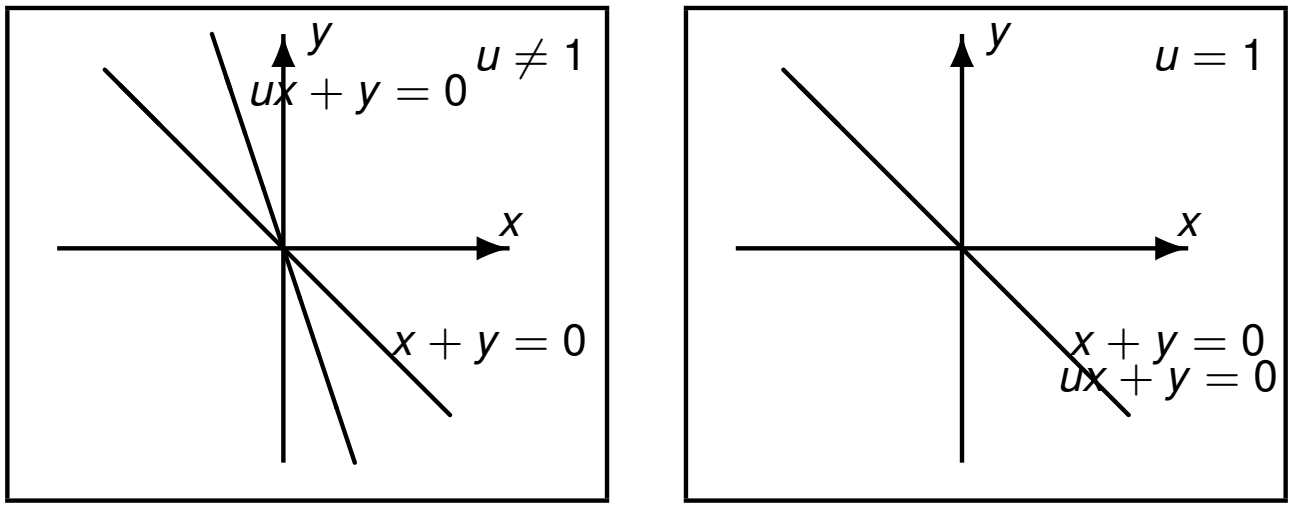
# The toy example




## Problem

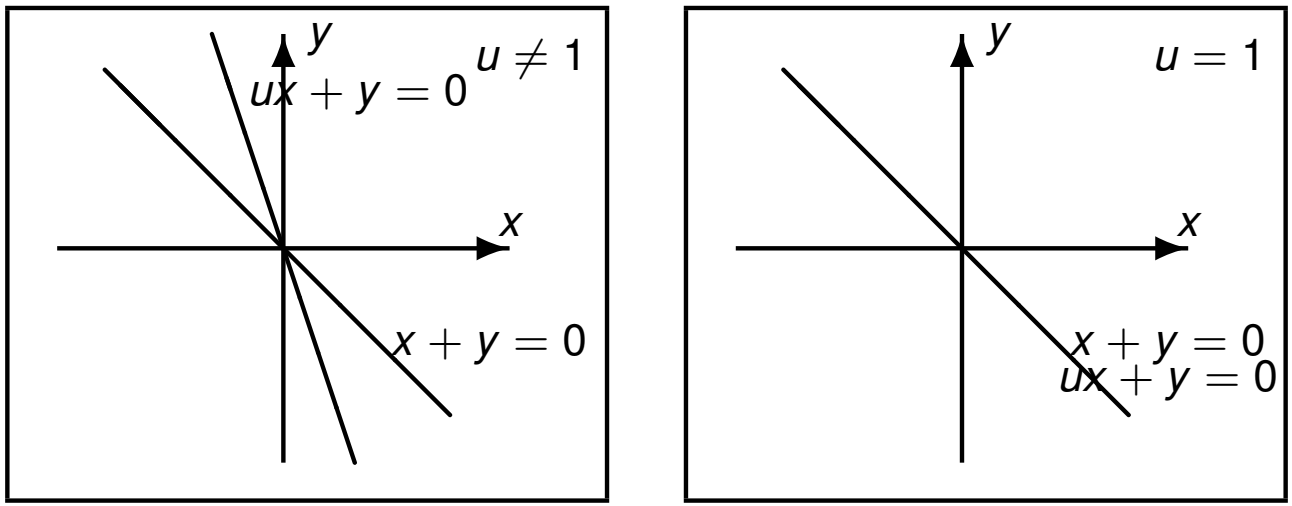
*(Toy problem in CGB) What is the dimension of the intersection of two lines* $x + y = 0$ *and* $ux + y = 0$ *as function of the parameter* $u$*?*

# The toy example



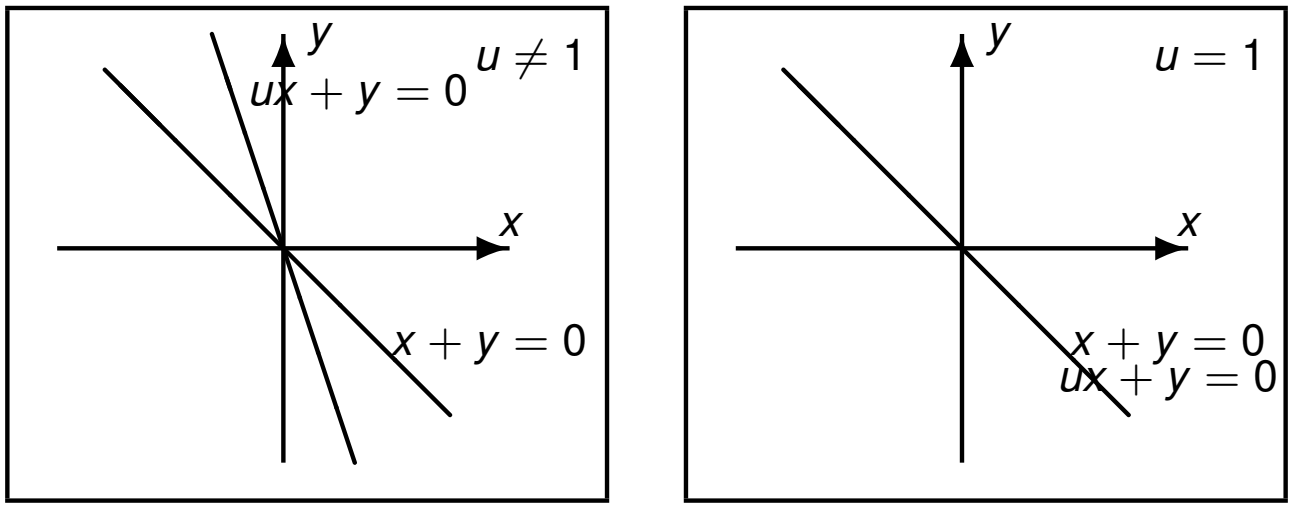

- Let $F = \{x + y, ux + y\} \subset k[u, x, y]$
- Let us first find the Gröbner basis as a function of the parameter ($x \succ y \succ z$, the monomial order is *lex*).
- We run into a problem: we are not able to determine what the $LM(ux + y)$ is.
- We need to branch the computation.

# The toy example



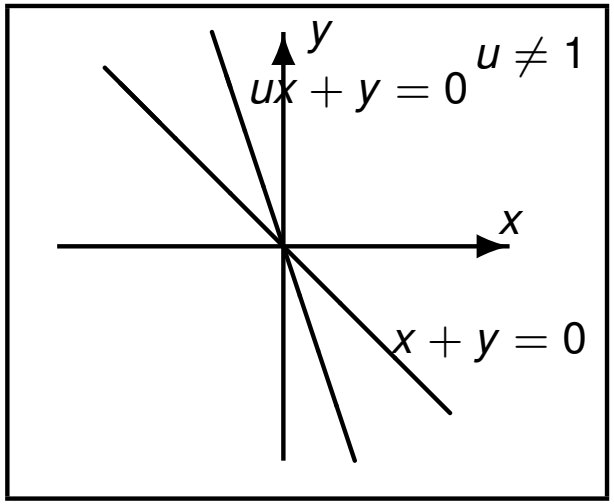

- Let $F = \{x + y, ux + y\} \subset k[u, x, y]$
- Let us first find the Gröbner basis as a function of the parameter ($x \succ y \succ z$, the monomial order is *lex*).
- We run into a problem: we are not able to determine what the $LM(ux + y)$ is.
- We need to branch the computation.

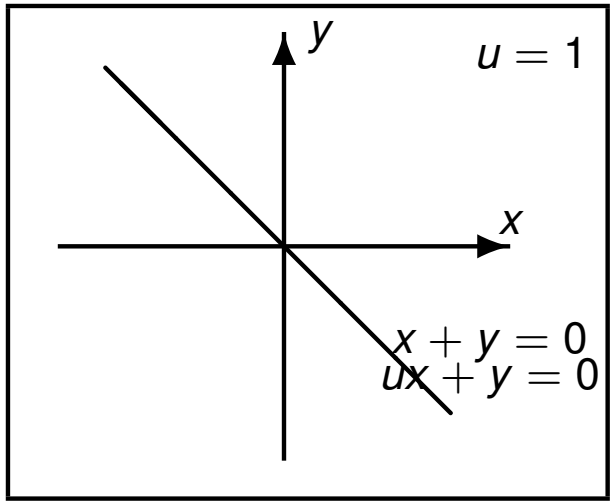
# The toy example




- Let $F = \{x + y, ux + y\} \subset k[u, x, y]$
- Let us first find the Gröbner basis as a function of the parameter ($x \succ y \succ z$, the monomial order is *lex*).
- We run into a problem: we are not able to determine what the $LM(ux + y)$ is.
- We need to branch the computation.

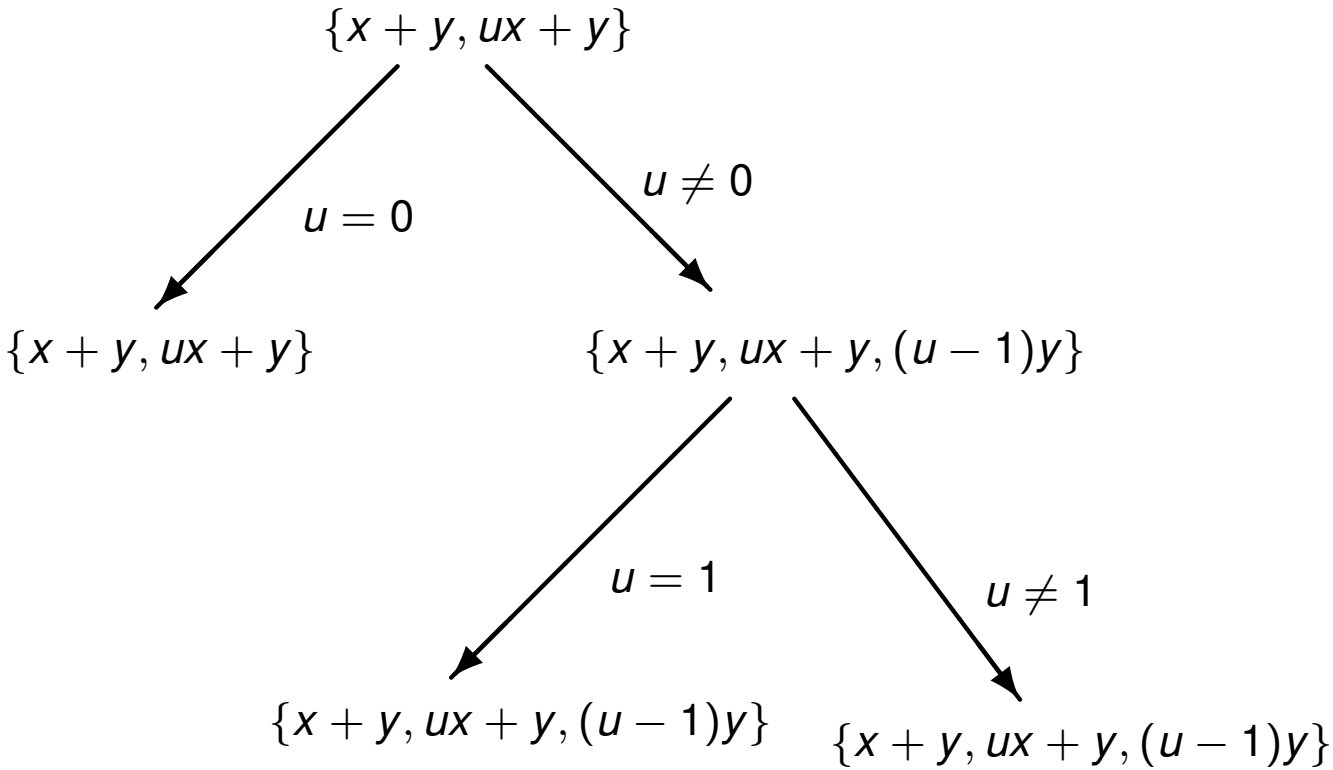
# The toy example




- Let $F = \{x + y, ux + y\} \subset k[u, x, y]$
- Let us first find the Gröbner basis as a function of the parameter ($x \succ y \succ z$, the monomial order is *lex*).
- We run into a problem: we are not able to determine what the $LM(ux + y)$ is.
- We need to branch the computation.

# The tree generated by the CGB algorithm



The solution of a parametric problem

- The *Comprehensive Gröbner System* (CGS) is an object derived from the algorithmically constructed tree previously considered.
- For the toy example,

$$\begin{aligned}
&\{\ (\ \{\ u = 0\ \},\quad \{\ x + y,\ ux + y\ \}\ ),\\
&(\ \{\ u \neq 0, u = 1\ \},\quad \{\ ux + y,\ (u-1)y\}\ ),\\
&(\ \{\ u \neq 0, u \neq 1\ \},\quad \{\ ux + y,\ (u-1)y\}\ )\ \}.
\end{aligned}$$

The solution of a parametric problem

- The *Comprehensive Gröbner System* (CGS) is an object derived from the algorithmically constructed tree previously considered.
- For the toy example,

$$\begin{aligned} &\{ (\{ u = 0 \}, && \{ x + y, ux + y \}), \\ &(\{ u \neq 0, u = 1 \}, && \{ ux + y, (u-1)y \}), \\ &(\{ u \neq 0, u \neq 1 \}, && \{ ux + y, (u-1)y \}) \}. \end{aligned}$$

## Comprehensive Gröbner System Definition

- A *Comprehensive Gröbner System* consists of pairs.
- The first element is a *condition*, i.e. a set of equations *(green list)* and inequations *(red list)* obtained by walking down from the root of the tree to the leaf.
- The second element of each pair is a Gröbner basis under any specialization satisfying the condition (leaf of the tree).

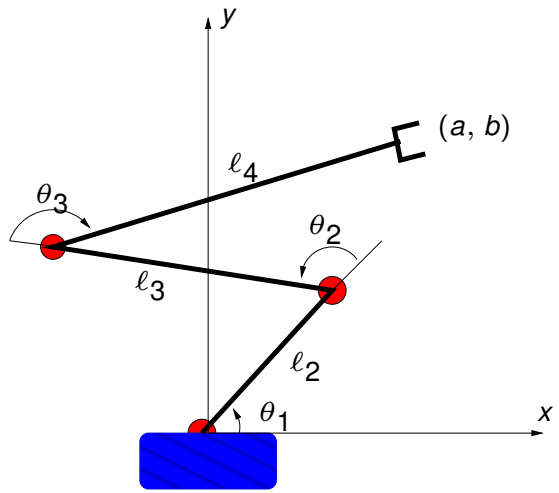
## Comprehensive Gröbner System Definition

- A *Comprehensive Gröbner System* consists of pairs.
- The first element is a *condition*, i.e. a set of equations *(green list)* and inequations *(red list)* obtained by walking down from the root of the tree to the leaf.
- The second element of each pair is a Gröbner basis under any specialization satisfying the condition (leaf of the tree).

Comprehensive Gröbner System Definition

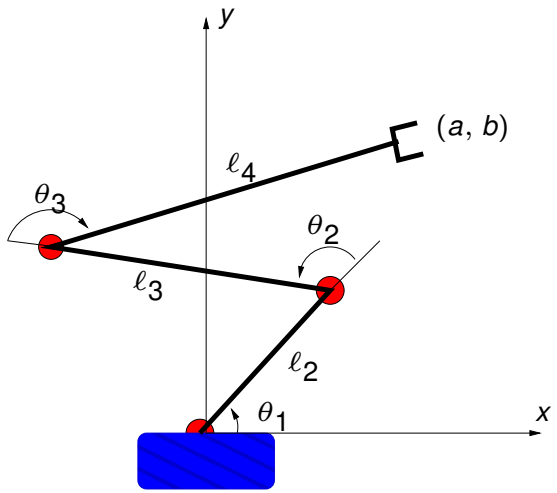
- A *Comprehensive Gröbner System* consists of pairs.
- The first element is a *condition*, i.e. a set of equations *(green list)* and inequations *(red list)* obtained by walking down from the root of the tree to the leaf.
- The second element of each pair is a Gröbner basis under any specialization satisfying the condition (leaf of the tree).

# Mathematical robotics



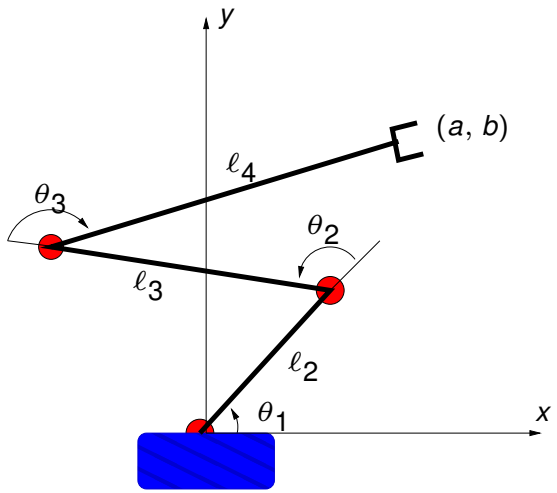

- Joint space: $\mathcal{J} = \{(\theta_1, \theta_2, \ldots, \theta_m)\}$
- Configuration space: $\mathcal{C} = \{(a, b)\}$
- Joint map: $f : \mathcal{J} \to \mathcal{C}$
- *Kinematic singularity:* when joint is moving with infinite velocity while the grasper is moving with finite velocity.

# Mathematical robotics



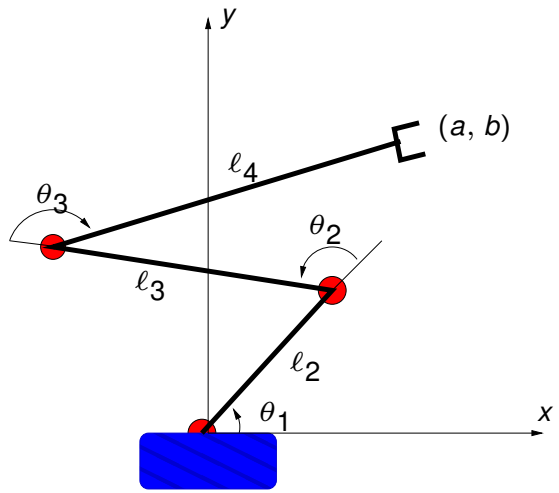

- Joint space: $\mathcal{J} = \{(\theta_1, \theta_2, \ldots, \theta_m)\}$
- Configuration space: $\mathcal{C} = \{(a, b)\}$
- Joint map: $f : \mathcal{J} \to \mathcal{C}$
- *Kinematic singularity:* when joint is moving with infinite velocity while the grasper is moving with finite velocity.

# Mathematical robotics




- Joint space: $\mathcal{J} = \{(\theta_1, \theta_2, \ldots, \theta_m)\}$
- Configuration space: $\mathcal{C} = \{(a, b)\}$
- Joint map: $f : \mathcal{J} \to \mathcal{C}$
- *Kinematic singularity:* when joint is moving with infinite velocity while the grasper is moving with finite velocity.

# Mathematical robotics




- Joint space: $\mathcal{J} = \{(\theta_1, \theta_2, \ldots, \theta_m)\}$
- Configuration space: $\mathcal{C} = \{(a, b)\}$
- Joint map: $f : \mathcal{J} \to \mathcal{C}$
- *Kinematic singularity:* when joint is moving with infinite velocity while the grasper is moving with finite velocity.

Dimension analysis of the joint map

**Problem**

*Determine the dimensions of the varieties $f^{-1}(c)$ for all points $c$ for the two-arm robot with $l_2 = l_3 = 1$.*

## Calculating Gröbner System with *CGBLisp*

```
;;For the robot with arms of length 1, determine the
;;dimensions of f^{-1}(c) for all c=(a,b)
(STRING-GROBNER-SYSTEM
"[a-l3*c1*c2+l3*s1*s2-l2*c1, b-l3*c1*s2-l3*c2*s1-l2*s1,
c1^2+s1^2-1, c2^2+s2^2-1]"
'(C2 S2 C1 S1)
'(A B L2 L3)
:COVER '(("[l2-1,l3-1]" "[]"))
:MAIN-ORDER #'grevlex>
:PARAMETER-ORDER #'lex>
)
```

## Notes

- The settings $l_2 = l_3 = 1$ are included as part of the green list instead of modifying the equations
- The main variable order is set to *grevlex*.
- The order must be a graded order in order to calculate the dimension.

Notes

- The settings $l_2 = l_3 = 1$ are included as part of the green list instead of modifying the equations
- The main variable order is set to *grevlex*.
- The order must be a graded order in order to calculate the dimension.

Notes

- The settings $l_2 = l_3 = 1$ are included as part of the green list instead of modifying the equations
- The main variable order is set to *grevlex*.
- The order must be a graded order in order to calculate the dimension.

## A theorem on dimension

**Theorem**

*If a graded monomial order is used then:*

$$dim(V(I)) = dim(V(LM(I))).$$

- If $I$ is a monomial ideal then the variety $V(I)$ is a union of coordinate hyperplanes.
- The dimension $dim(V(I))$ can be easily computed.

## A theorem on dimension

**Theorem**

*If a graded monomial order is used then:*

$$dim(V(I)) = dim(V(LM(I))).$$

- If $I$ is a monomial ideal then the variety $V(I)$ is a union of coordinate hyperplanes.
- The dimension $dim(V(I))$ can be easily computed.

## A theorem on dimension

**Theorem**

*If a graded monomial order is used then:*

$$dim(V(I)) = dim(V(LM(I))).$$

- If $I$ is a monomial ideal then the variety $V(I)$ is a union of coordinate hyperplanes.
- The dimension $dim(V(I))$ can be easily computed.

## Output of *CGBLisp* - Case 1

```
--------------------CASE 1--------------------
Condition:
Green list: [L2-1,L3-1]
Red list: [A,A^2+B^2]
Basis: [(-2*A)*S2+(-2*A^2-2*B^2)*S1+(A^2*B+B^3),
(-2)*C2+(A^2+B^2-2),(2*A)*C1+(2*B)*S1+(-A^2-B^2),
(4*A^2+4*B^2)*S1^2+(-4*A^2*B-4*B^3)*S1+
(A^4+2*A^2*B^2-4*A^2+B^4)]
```

## Output of CGBLisp - Case 2

```
--------------------CASE 2--------------------
Condition:
Green list: [L2-1,L3-1,A^2+B^2]
Red list: [B^2,A]
Basis: [(32*B^4)]
```

## Output of CGBLisp - Case 3

```
--------------------CASE 3--------------------
Condition:
Green list: [L2-1,L3-1,A]
Red list: [B]
Basis: [(4*B^2)*C1^2+(B^4-4*B^2),
(2*B)*S2+(-2*B^2)*C1,(-2)*C2+(B^2-2),
(2*B)*S1+(-B^2)]
```

## Output of CGBLisp - Case 4

```
--------------------CASE 4--------------------
Condition:
Green list: [L2-1,L3-1,A,B]
Red list: []
Basis: [(1)*C1^2+(1)*S1^2+(-1),(1)*S2,(1)*C2+(1)]
```

Dimension of the kinematic singularity

- The dimension ccan be calculated automatically, but we can do it by hand easily as well.
- The following table contains the necessary information:

| Case # | $LM(I)$ | dimension |
|---|---|---|
| 1 | $\mathrm{Id}(\{s_2, c_2, c_1, s_1^2\})$ | 0 |
| 2 | $\mathrm{Id}(\{1\})$ | -1 |
| 3 | $\mathrm{Id}(\{c_1^2, s_2, c_2, s_1\})$ | 0 |
| 4 | $\mathrm{Id}(\{c_1^2, s_2, c_2\})$ | 1 |

## Analysis based on a Gröbner system

- When $a, b \neq 0$ (CASE 1) and $a^2 + b^2 = 0$ (non-geometric condition) then there are no solutions; the points (a, $\pm ia$) cannot be reached by the robot.
- When $a, b = 0$ (CASE 4), we have a kinematic singularity. The variety $f^{-1}(0,0)$ is 1-dimensional. The joint variety $\mathcal{J}$ is 2-dimensional and the configuration variety is 2-dimensional as well. Thus, for non-singular values $(a, b)$ the dimension of $f^{-1}(a, b)$ will be

$$dim(\mathcal{C}) - dim(\mathcal{J}) = 0.$$

The variety $f^{-1}(0,0)$ in CASE 4 can be determined easily:

$$c_2 = -1,\ s_2 = 0,\ s_1 \text{ is arbitrary.}$$

## Analysis based on a Gröbner system

- When $a, b \neq 0$ (CASE 1) and $a^2 + b^2 = 0$ (non-geometric condition) then there are no solutions; the points (a, $\pm ia$) cannot be reached by the robot.
- When $a, b = 0$ (CASE 4), we have a kinematic singularity. The variety $f^{-1}(0,0)$ is 1-dimensional. The joint variety $\mathcal{J}$ is 2-dimensional and the configuration variety is 2-dimensional as well. Thus, for non-singular values $(a, b)$ the dimension of $f^{-1}(a, b)$ will be

$$dim(\mathcal{C}) - dim(\mathcal{J}) = 0.$$

The variety $f^{-1}(0,0)$ in CASE 4 can be determined easily:

$$c_2 = -1, \ s_2 = 0, \ s_1 \text{ is arbitrary.}$$

## Into the future

- Study papers of Faugère to get to the forefront of current research on GB, especially the F4 and F5 algorithms.
- Akiro Suzuki described an algorithm for CGB which uses only standard GB and a clever choice of slack variables.
- Kuranishi-Cartan theory studies mildly non-commutative rings, when some “variables” are differential operators. Interesting applications to PDE are on the horizon. Study G. Reid, Ping Lin, A. Wittkopf and W.M. Seiler.

Into the future

- Study papers of Faugère to get to the forefront of current research on GB, especially the F4 and F5 algorithms.
- Akiro Suzuki described an algorithm for CGB which uses only standard GB and a clever choice of slack variables.
- Kuranishi-Cartan theory studies mildly non-commutative rings, when some “variables” are differential operators. Interesting applications to PDE are on the horizon. Study G. Reid, Ping Lin, A. Wittkopf and W.M. Seiler.

Into the future

- Study papers of Faugère to get to the forefront of current research on GB, especially the F4 and F5 algorithms.
- Akiro Suzuki described an algorithm for CGB which uses only standard GB and a clever choice of slack variables.
- Kuranishi-Cartan theory studies mildly non-commutative rings, when some “variables” are differential operators. Interesting applications to PDE are on the horizon. Study G. Reid, Ping Lin, A. Wittkopf and W.M. Seiler.