# Algebraic and Semi-Algebraic Reasoning For Formal Methods

Lecture 3 - Gröbner Bases and Nullstellensatz

Sriram Sankaranarayanan

# So far

- Ideals: $I \subseteq K[x_1, \dots, x_n]$
  - $p_1, p_2 \in I \;\Rightarrow\; p_1 + p_2 \in I$.
  - $p \in I,\ q \in \mathbb{R}[\vec{x}],\ pq \in I$.
- Varieties: Set of all points defined by common zeros of polynomials.

# Ideal Membership Testing

- **Input** Generators of an ideal $\langle p_1, \ldots, p_m \rangle$, $p \in K[\vec{x}]$
- **Output** $p \in I$?

# Monomial Ordering

- We will impose a ordering relation over monomials.
- For a single variable, this is easy:

$$x^0 \prec x^1 \prec x^2 \prec \cdots \prec x^n \prec \cdots$$

- What about multiple variables?

Requirements:

- $\prec$ is a total order over monomials.
- $p \prec q$ implies forall $w, \;\; pw \prec qw$.
- $\prec$ is well order: every non-empty set has a least element.

# Monomial ordering

- We can view it as an order between monomials $\vec{x}^{\alpha}$.
- Alternatively, ordering over $\mathbb{N}^n$.

$$\vec{x}^{\alpha_1} \prec \vec{x}^{\alpha_2} \ \Rightarrow \ \alpha_1 \prec \alpha_2$$

# Lexicographic Ordering

- Fix a rank among variables $x_1 > x_2 > \cdots > x_n$.
- Write each monomial as a vector $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.
  - Variables arranged in decreasing rank.
- Use lexicographic comparison:

$$(\vec{\alpha} \prec \vec{\beta}) \text{ iff } \alpha_1 = \beta_1, \cdots, \alpha_{i-1} = \beta_{i-1},\ \alpha_i < \beta_i$$

- Take $x > y$.

# Lexicographic Ordering

- Fix a rank among variables $x_1 > x_2 > \cdots > x_n$.
- Write each monomial as a vector $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.
  - Variables arranged in decreasing rank.
- Use lexicographic comparison:

$$(\vec{\alpha} \prec \vec{\beta}) \text{ iff } \alpha_1 = \beta_1, \cdots, \alpha_{i-1} = \beta_{i-1},\ \alpha_i < \beta_i$$

- Take $x > y$.
- $xy^{100} \prec x^2y^{10}$

# Lexicographic Ordering

- Fix a rank among variables $x_1 > x_2 > \cdots > x_n$.
- Write each monomial as a vector $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.
  - Variables arranged in decreasing rank.
- Use lexicographic comparison:

$$(\vec{\alpha} \prec \vec{\beta}) \text{ iff } \alpha_1 = \beta_1, \cdots, \alpha_{i-1} = \beta_{i-1},\ \alpha_i < \beta_i$$

- Take $x > y$.
- $xy^{100} \prec x^2y^{10}$
- $xy^2 \prec xy^4$

# Graded Lexicographic Ordering

$$\vec{\alpha} \prec \vec{\beta} \text{ iff}$$

- Either $|\vec{\alpha}|_1 < |\vec{\beta}|_1$, OR

# Graded Lexicographic Ordering

$$\vec{\alpha} \prec \vec{\beta} \text{ iff}$$

- Either $|\vec{\alpha}|_1 < |\vec{\beta}|_1$, OR
- $|\vec{\alpha}|_1 = |\vec{\beta}|_1 \ \wedge \ \vec{\alpha} \prec_{\text{lex}} \vec{\beta}$.

# Graded Lexicographic Ordering

$$\vec{\alpha} \prec \vec{\beta} \text{ iff}$$

- Either $|\vec{\alpha}|_1 < |\vec{\beta}|_1$, OR
- $|\vec{\alpha}|_1 = |\vec{\beta}|_1 \ \wedge \ \vec{\alpha} \prec_{\text{lex}} \vec{\beta}$.

- Take $x > y$.

# Graded Lexicographic Ordering

$$\vec{\alpha} \prec \vec{\beta} \text{ iff}$$

- Either $|\vec{\alpha}|_1 < |\vec{\beta}|_1$, OR
- $|\vec{\alpha}|_1 = |\vec{\beta}|_1 \ \wedge \ \vec{\alpha} \prec_{\text{lex}} \vec{\beta}$.

- Take $x > y$.
- $x^2y^{10} \prec xy^{15}$

# Graded Lexicographic Ordering

$$\vec{\alpha} \prec \vec{\beta} \text{ iff}$$

- Either $|\vec{\alpha}|_1 < |\vec{\beta}|_1$, OR
- $|\vec{\alpha}|_1 = |\vec{\beta}|_1 \ \wedge \ \vec{\alpha} \prec_{\mathsf{lex}} \vec{\beta}$.

- Take $x > y$.
- $x^2y^{10} \prec xy^{15}$
- $xy^2 \prec xy^4$

# Graded Lexicographic Ordering

$$\vec{\alpha} \prec \vec{\beta} \text{ iff}$$

- Either $|\vec{\alpha}|_1 < |\vec{\beta}|_1$, OR
- $|\vec{\alpha}|_1 = |\vec{\beta}|_1 \ \wedge \ \vec{\alpha} \prec_{\mathsf{lex}} \vec{\beta}$.

- Take $x > y$.
- $x^2y^{10} \prec xy^{15}$
- $xy^2 \prec xy^4$
- $y^3 \prec xy^2 \prec x^2y \prec x^3$

# Leading Term and Monomial

Let $\prec$ be a monomial oder and $p$ be a polynomial.

- $LT(p)$ : the term in $p$

$$p = 2xy + y^2 + 3x^2 + y^3$$

- Take $\prec$ to be lexicographic order with $x > y$.
- $LT(p) = 3x^2$, $LM(p) = x^2$.
- How does the answer change if we used graded lex ordering?

# Leading Term and Monomial

Let $\prec$ be a monomial oder and $p$ be a polynomial.

- $LT(p)$ : the term in $p$
  - $c_\alpha x^\alpha$, wherein $\alpha$ is the greatest among all monomials in the $\prec$ ordering.

$$p = 2xy + y^2 + 3x^2 + y^3$$

- Take $\prec$ to be lexicographic order with $x > y$.
- $LT(p) = 3x^2$, $LM(p) = x^2$.
- How does the answer change if we used graded lex ordering?

# Leading Term and Monomial

Let $\prec$ be a monomial oder and $p$ be a polynomial.

- $LT(p)$ : the term in $p$
  - $c_\alpha x^\alpha$, wherein $\alpha$ is the greatest among all monomials in the $\prec$ ordering.
- $LM(p)$ : the monomial in $p$

$$p = 2xy + y^2 + 3x^2 + y^3$$

- Take $\prec$ to be lexicographic order with $x > y$.
- $LT(p) = 3x^2$, $LM(p) = x^2$.
- How does the answer change if we used graded lex ordering?

# Leading Term and Monomial

Let $\prec$ be a monomial oder and $p$ be a polynomial.

- $LT(p)$ : the term in $p$
  - $c_\alpha x^\alpha$, wherein $\alpha$ is the greatest among all monomials in the $\prec$ ordering.
- $LM(p)$ : the monomial in $p$
  - $x^\alpha$, wherein $\alpha$ is the greatest among all monomials in the $\prec$ ordering.

$$p = 2xy + y^2 + 3x^2 + y^3$$

- Take $\prec$ to be lexicographic order with $x > y$.
- $LT(p) = 3x^2$, $LM(p) = x^2$.
- How does the answer change if we used graded lex ordering?

# Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:

# Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:
  - $p = p - 3x^2(x - 2) = 4x^2 + 5$

# Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:
  - $p = p - 3x^2(x - 2) = 4x^2 + 5$
  - $q = q + 3x^2$

## Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:
    - $p = p - 3x^2(x - 2) = 4x^2 + 5$
    - $q = q + 3x^2$
- Multiply dividend by $4x$ and subtract.

# Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:
  - $p = p - 3x^2(x - 2) = 4x^2 + 5$
  - $q = q + 3x^2$
- Multiply dividend by $4x$ and subtract.
  - $p = p - 4x(x - 2) = 8x + 5$

# Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:
  - $p = p - 3x^2(x - 2) = 4x^2 + 5$
  - $q = q + 3x^2$
- Multiply dividend by $4x$ and subtract.
  - $p = p - 4x(x - 2) = 8x + 5$
  - $q = q + 4x = 3x^2 + 4x$

# Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:
  - $p = p - 3x^2(x - 2) = 4x^2 + 5$
  - $q = q + 3x^2$
- Multiply dividend by $4x$ and subtract.
  - $p = p - 4x(x - 2) = 8x + 5$
  - $q = q + 4x = 3x^2 + 4x$
- Multiply div. by 8 and subtract.

# Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:
  - $p = p - 3x^2(x - 2) = 4x^2 + 5$
  - $q = q + 3x^2$
- Multiply dividend by $4x$ and subtract.
  - $p = p - 4x(x - 2) = 8x + 5$
  - $q = q + 4x = 3x^2 + 4x$
- Multiply div. by 8 and subtract.
  - $p = p - 8(x - 2) = 21$

# Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:
  - $p = p - 3x^2(x - 2) = 4x^2 + 5$
  - $q = q + 3x^2$
- Multiply dividend by $4x$ and subtract.
  - $p = p - 4x(x - 2) = 8x + 5$
  - $q = q + 4x = 3x^2 + 4x$
- Multiply div. by 8 and subtract.
  - $p = p - 8(x - 2) = 21$
  - $q = q + 8 = 3x^2 + 4x + 8.$

# Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:
  - $p = p - 3x^2(x - 2) = 4x^2 + 5$
  - $q = q + 3x^2$
- Multiply dividend by $4x$ and subtract.
  - $p = p - 4x(x - 2) = 8x + 5$
  - $q = q + 4x = 3x^2 + 4x$
- Multiply div. by 8 and subtract.
  - $p = p - 8(x - 2) = 21$
  - $q = q + 8 = 3x^2 + 4x + 8.$
- No more division possible.

# Univariate Polynomial Division

$$(3x^3 - 2x^2 + 5) \div (x - 2)?$$

- $p = (3x^3 - 2x^2 + 5), q = 0.$
- First multiply dividend by $3x^2$ and subtract:
  - $p = p - 3x^2(x - 2) = 4x^2 + 5$
  - $q = q + 3x^2$
- Multiply dividend by $4x$ and subtract.
  - $p = p - 4x(x - 2) = 8x + 5$
  - $q = q + 4x = 3x^2 + 4x$
- Multiply div. by 8 and subtract.
  - $p = p - 8(x - 2) = 21$
  - $q = q + 8 = 3x^2 + 4x + 8.$
- No more division possible.
  - $q = 3x^2 + 4x + 8$, $r = 8.$

# Univariate Division

Let $f, g \in K[x]$ for field $K$.

- We can write $f = qg + r$,
- $\deg(r) < \deg(g)$.

```
divide (f : K[x], g : K[x])
  p := f
  q := 0
  while (LT(g) divides LT(p) ):
      p := p - (LT(p)/LT(g)) g
      q := q + LT(p)/LT(g)
  r := p
```

# Multivariate Division

Divide $f$ : $2x^2y + 6y^2 + 4xy - 2x$ by

- $g_1 : (y - 2)$ and
- $g_2 : (x^2 + 3y)$.

- $f_1 = f - 2y(x^2 + 3y) = 4xy - 2x$

# Multivariate Division

Divide $f$ : $2x^2y + 6y^2 + 4xy - 2x$ by

- $g_1 : (y - 2)$ and
- $g_2 : (x^2 + 3y)$.

- $f_1 = f - 2y(x^2 + 3y) = 4xy - 2x$
- $f_2 = f_1 - 4x(y - 2) = 6x$.

# Multivariate Division

Divide $f:\ 2x^2y + 6y^2 + 4xy - 2x$ by

- $g_1 : (y-2)$ and
- $g_2 : (x^2+3y)$.

- $f_1 = f - 2y(x^2+3y) = 4xy - 2x$
- $f_2 = f_1 - 4x(y-2) = 6x$.
- No more divisions possible.

# Multivariate Division

Divide $f: \ 2x^2y + 6y^2 + 4xy - 2x$ by

- $g_1 : (y - 2)$ and
- $g_2 : (x^2 + 3y)$.

- $f_1 = f - 2y(x^2 + 3y) = 4xy - 2x$
- $f_2 = f_1 - 4x(y - 2) = 6x$.
- No more divisions possible.
- $f = 2yg_1 + 4xg_2 + 6x$.

# Rewriting System

$$f \xrightarrow{g_i} f'$$

- Choose a term $t$ in $f$.
  - $LT(g_i)$ must divide $t$.
- $f' = f - \frac{t}{LT(g_i)}\ g_i$
- Gets rid of $t$, replacing it with smaller terms.

$f$ : $2x^2y + 6y^2 + 4xy - 2x$

- $f \xrightarrow{x^2+3y} (2x^2y + 6y^2 + 4xy - 2x) - 2y(x^2 + 3y) = 4xy - 2x$.
- $$\begin{aligned} f \xrightarrow{y-2} & \ (2x^2y + 6y^2 + 4xy - 2x) - 2x^2(y-2) \\ & = 4x^2 + 6y^2 + 4xy - 2x \end{aligned}$$

# Rewriting System

Polynomial division: $f$ with $g_1, \ldots, g_m$.

- $f \xrightarrow{g_1} f_1 \xrightarrow{g_2} f_2 \cdots \xrightarrow{g_i} \cdots f_m$.

# Rewriting System

Polynomial division: $f$ with $g_1, \dots, g_m$.

- $f \xrightarrow{g_1} f_1 \xrightarrow{g_2} f_2 \cdots \xrightarrow{g_i} \cdots f_m$.
- Terminating? Yes, how do we prove it?

# Rewriting System

Polynomial division: $f$ with $g_1, \dots, g_m$.

- $f \xrightarrow{g_1} f_1 \xrightarrow{g_2} f_2 \cdots \xrightarrow{g_i} \cdots f_m$.
- Terminating? Yes, how do we prove it?
- Confluent? (i.e, unique normal form?)

# Rewriting System

Polynomial division: $f$ with $g_1, \dots, g_m$.

- $f \xrightarrow{g_1} f_1 \xrightarrow{g_2} f_2 \cdots \xrightarrow{g_i} \cdots f_m$.
- Terminating? Yes, how do we prove it?
- Confluent? (i.e, unique normal form?)
    - Not necessarily.

# Multivariate Division

- Result is not unique
- It depends on the order in which we divide.

# Multivariate Division (cont.)

Divide $f$ by $g_1, \ldots, g_m$ (in $K[x_1, \ldots, x_n]$):

- Fix monomial order $\prec$.

# Multivariate Division (cont.)

Divide $f$ by $g_1, \dots, g_m$ (in $K[x_1, \dots, x_n]$):

- Fix monomial order $\prec$.
- Initialize $p = f, q_1 = 0, \dots, q_m = 0, r = 0$.

# Multivariate Division (cont.)

Divide $f$ by $g_1, \ldots, g_m$ (in $K[x_1, \ldots, x_n]$):

- Fix monomial order $\prec$.
- Initialize $p = f, q_1 = 0, \ldots, q_m = 0, r = 0$.
- While $p \neq 0$:

# Multivariate Division (cont.)

Divide $f$ by $g_1, \dots, g_m$ (in $K[x_1, \dots, x_n]$):

- Fix monomial order $\prec$.
- Initialize $p = f, q_1 = 0, \dots, q_m = 0, r = 0$.
- While $p \neq 0$:
  - if $\exists i, LT(g_i) \mid LT(p)$ then:

# Multivariate Division (cont.)

Divide $f$ by $g_1, \dots, g_m$ (in $K[x_1, \dots, x_n]$):

- Fix monomial order $\prec$.
- Initialize $p = f, q_1 = 0, \dots, q_m = 0, r = 0$.
- While $p \neq 0$:
  - if $\exists i, LT(g_i) \mid LT(p)$ then:
    - $p := p - (LT(p)/LT(g_i))g_i$

# Multivariate Division (cont.)

Divide $f$ by $g_1, \ldots, g_m$ (in $K[x_1, \ldots, x_n]$):

- Fix monomial order $\prec$.
- Initialize $p = f, q_1 = 0, \ldots, q_m = 0, r = 0$.
- While $p \neq 0$:
  - if $\exists i, LT(g_i) \mid LT(p)$ then:
    - $p := p - (LT(p)/LT(g_i))g_i$
    - $q_i := q_i + LT(p)/LT(g_i)$

# Multivariate Division (cont.)

Divide $f$ by $g_1, \dots, g_m$ (in $K[x_1, \dots, x_n]$):

- Fix monomial order $\prec$.
- Initialize $p = f, q_1 = 0, \dots, q_m = 0, r = 0$.
- While $p \neq 0$:
  - if $\exists i, LT(g_i) \mid LT(p)$ then:
    - $p := p - (LT(p)/LT(g_i))g_i$
    - $q_i := q_i + LT(p)/LT(g_i)$
  - else:

# Multivariate Division (cont.)

Divide $f$ by $g_1, \dots, g_m$ (in $K[x_1, \dots, x_n]$):

- Fix monomial order $\prec$.
- Initialize $p = f, q_1 = 0, \dots, q_m = 0, r = 0$.
- While $p \neq 0$:
  - if $\exists i, LT(g_i) \mid LT(p)$ then:
    - $p := p - (LT(p)/LT(g_i))g_i$
    - $q_i := q_i + LT(p)/LT(g_i)$
  - else:
    - $p := p - LT(p)$

# Multivariate Division (cont.)

Divide $f$ by $g_1, \ldots, g_m$ (in $K[x_1, \ldots, x_n]$):

- Fix monomial order $\prec$.
- Initialize $p = f, q_1 = 0, \ldots, q_m = 0, r = 0$.
- While $p \neq 0$:
  - if $\exists i, LT(g_i) \mid LT(p)$ then:
    - $p := p - (LT(p)/LT(g_i))g_i$
    - $q_i := q_i + LT(p)/LT(g_i)$
  - else:
    - $p := p - LT(p)$
    - $r := r + LT(p)$

# Multivariate Division (cont.)

Divide $f$ by $g_1, \dots, g_m$ (in $K[x_1, \dots, x_n]$):

- Fix monomial order $\prec$.
- Initialize $p = f, q_1 = 0, \dots, q_m = 0, r = 0$.
- While $p \neq 0$:
  - if $\exists i, LT(g_i) \mid LT(p)$ then:
    - $p := p - (LT(p)/LT(g_i))g_i$
    - $q_i := q_i + LT(p)/LT(g_i)$
  - else:
    - $p := p - LT(p)$
    - $r := r + LT(p)$
- return $q_1, \dots, q_m, r$

# Reminder Properties

Divide $f$ by $g_1, \dots, g_m$ (in $K[x_1, \dots, x_n]$):

$$f = q_1 g_1 + \cdots + q_m g_m + r$$

What can we say about $q_i, r$?

- No term in $r$ is divisible by $LT(g_i)$ for any $i$.

# Reminder Properties

Divide $f$ by $g_1, \dots, g_m$ (in $K[x_1, \dots, x_n]$):

$$f = q_1 g_1 + \cdots + q_m g_m + r$$

What can we say about $q_i, r$?

- No term in $r$ is divisible by $LT(g_i)$ for any $i$.
- If $q_i g_i \neq 0$, then $LT(q_i g_i) \preceq LT(f)$.

# Reminder Properties

Divide $f$ by $g_1, \ldots, g_m$ (in $K[x_1, \ldots, x_n]$):

$$f = q_1 g_1 + \cdots + q_m g_m + r$$

What can we say about $q_i, r$?

- No term in $r$ is divisible by $LT(g_i)$ for any $i$.
- If $q_i g_i \neq 0$, then $LT(q_i g_i) \preceq LT(f)$.
  - Let's call this **no higher degree cancellation** property.

# Ideal Membership Problem

**Input** $\langle g_1, \dots, g_m \rangle, \ f \in k[x_1, \dots, x_n]$.

**Output** $f \in \langle g_1, \dots, g_m \rangle$.

- Perform a polynomial division $f$ with $g_1, \dots, g_m$.

$$f = q_1 g_1 + \cdots + q_m g_m + r$$

**Claim** If $r = 0$ then $f \in \langle g_1, \dots, g_m \rangle$.

Q: Does the converse hold?

# Ideal Membership vs Poly. Div.

Take $I = \langle xy^2 - x - y, x^2y - x - y \rangle$.

- Let $\prec$ be graded lex ordering.
- $y^2 - x^2 \in I$ since
  $(y^2 - x^2) = x \times (xy^2 - x - y) - y \times (x^2y - x - y)$.

# Ideal Membership vs Poly. Div.

Take $I = \langle xy^2 - x - y, x^2y - x - y\rangle$.

- Let $\prec$ be graded lex ordering.
- $y^2 - x^2 \in I$ since $(y^2 - x^2) = x \times (xy^2 - x - y) - y \times (x^2y - x - y)$.
- Reminder upon dividing $y^2 - x^2$ w.r.t $xy^2 - x - y, x^2y - x - y$?

# Ideal Membership vs Poly. Div.

Take $I = \langle xy^2 - x - y, x^2y - x - y \rangle$.

- Let $\prec$ be graded lex ordering.
- $y^2 - x^2 \in I$ since
  $(y^2 - x^2) = x \times (xy^2 - x - y) - y \times (x^2y - x - y)$.
- Reminder upon dividing $y^2 - x^2$ w.r.t
  $xy^2 - x - y, x^2y - x - y$?
  - Answer $r = y^2 - x^2$.

# Ideal Membership vs Poly. Div.

Take $I = \langle xy^2 - x - y, x^2y - x - y \rangle$.

- Let $\prec$ be graded lex ordering.
- $y^2 - x^2 \in I$ since $(y^2 - x^2) = x \times (xy^2 - x - y) - y \times (x^2y - x - y)$.
- Reminder upon dividing $y^2 - x^2$ w.r.t $xy^2 - x - y, x^2y - x - y$?
    - Answer $r = y^2 - x^2$.
- Issue : Proving membership of $y^2 - x^2$ requires *higher degree term cancellation*.

# Ideal Membership vs Poly. Div.

Take $I = \langle xy^2 - x - y, x^2y - x - y \rangle$.

- Let $\prec$ be graded lex ordering.
- $y^2 - x^2 \in I$ since
  $(y^2 - x^2) = x \times (xy^2 - x - y) - y \times (x^2y - x - y)$.
- Reminder upon dividing $y^2 - x^2$ w.r.t
  $xy^2 - x - y, x^2y - x - y$?
    - Answer $r = y^2 - x^2$.
- Issue : Proving membership of $y^2 - x^2$ requires *higher degree term cancellation*.
- However, remember polynomial division has the **no higher degree cancellation** property.

## Gröbner Basis

- Formulated by Büchberger in 1965: Named after his PhD advisor Wolfgang Gröbner!

# Gröbner Basis

- Formulated by Büchberger in 1965: Named after his PhD advisor Wolfgang Gröbner!
- Es un gran ganga!

# Gröbner Basis

- Formulated by Büchberger in 1965: Named after his PhD advisor Wolfgang Gröbner!
- Es un gran ganga!
- We are given an ideal $I = \langle g_1, \ldots, g_m \rangle$.

# Gröbner Basis

- Formulated by Büchberger in 1965: Named after his PhD advisor Wolfgang Gröbner!
- Es un gran ganga!
- We are given an ideal $I = \langle g_1, \dots, g_m \rangle$.
- Polynomial division is unable to test for membership.

# Gröbner Basis

- Formulated by Büchberger in 1965: Named after his PhD advisor Wolfgang Gröbner!
- Es un gran ganga!
- We are given an ideal $I = \langle g_1, \dots, g_m \rangle$.
- Polynomial division is unable to test for membership.
    - Due to *higher degree cancellation* problem.

# Gröbner Basis

- Formulated by Büchberger in 1965: Named after his PhD advisor Wolfgang Gröbner!
- Es un gran ganga!
- We are given an ideal $I = \langle g_1, \dots, g_m \rangle$.
- Polynomial division is unable to test for membership.
  - Due to *higher degree cancellation* problem.
- Compute a different basis $\langle p_1, \dots, p_K \rangle \equiv \langle g_1, \dots, g_m \rangle$.

# Gröbner Basis

- Formulated by Büchberger in 1965: Named after his PhD advisor Wolfgang Gröbner!
- Es un gran ganga!
- We are given an ideal $I = \langle g_1, \ldots, g_m \rangle$.
- Polynomial division is unable to test for membership.
  - Due to *higher degree cancellation* problem.
- Compute a different basis $\langle p_1, \ldots, p_K \rangle \equiv \langle g_1, \ldots, g_m \rangle$.
  - Generates the same ideal.

# Gröbner Basis

- Formulated by Büchberger in 1965: Named after his PhD advisor Wolfgang Gröbner!
- Es un gran ganga!
- We are given an ideal $I = \langle g_1, \dots, g_m \rangle$.
- Polynomial division is unable to test for membership.
  - Due to *higher degree cancellation* problem.
- Compute a different basis $\langle p_1, \dots, p_K \rangle \equiv \langle g_1, \dots, g_m \rangle$.
  - Generates the same ideal.
- **Guarantee:** $f \in I$ if and only if polynomial division of $f$ w.r.t $p_1, \dots, p_K$ yields remainder $0$.

# Gröbner Basis and Büchberger's Algorithm

# Finitely Generated Ideals

Definition of Ideal:

- $I \subseteq K[x_1, \dots, x_n]$,
- Closed under addition:
  - $f_1, f_2 \in I \;\Rightarrow\; f_1 + f_2 \in I$.
- Closed under multiplication with any element:
  - $f \in I, g \in K[\vec{x}] \;\Rightarrow\; gf \in I$.

- $\langle g_1, \dots, g_m \rangle = \{\sum_{i=1}^{m} \lambda_i g_i \mid \lambda_i \in K[\vec{x}]\}$.

# Finitely Generated Ideals

Definition of Ideal:

- $I \subseteq K[x_1, \dots, x_n]$,
- Closed under addition:
  - $f_1, f_2 \in I \;\Rightarrow\; f_1 + f_2 \in I$.
- Closed under multiplication with any element:
  - $f \in I, g \in K[\vec{x}] \;\Rightarrow\; gf \in I$.
- $\langle g_1, \dots, g_m \rangle = \{\sum_{i=1}^{m} \lambda_i g_i \mid \lambda_i \in K[\vec{x}]\}$.
- Can any ideal $I$ be written as $I = \langle g_1, \dots, g_l \rangle$ for a finite $l$?

# Finitely Generated Ideals

Definition of Ideal:

- $I \subseteq K[x_1, \ldots, x_n]$,
- Closed under addition:
  - $f_1, f_2 \in I \;\Rightarrow\; f_1 + f_2 \in I$.
- Closed under multiplication with any element:
  - $f \in I, g \in K[\vec{x}] \;\Rightarrow\; gf \in I$.

- $\langle g_1, \ldots, g_m \rangle = \{\sum_{i=1}^{m} \lambda_i g_i \mid \lambda_i \in K[\vec{x}]\}$.

- Can any ideal $I$ be written as $I = \langle g_1, \ldots, g_l \rangle$ for a finite $l$?

  - Si se puede!

# Finitely Generated Ideals

Definition of Ideal:

- $I \subseteq K[x_1, \dots, x_n]$,
- Closed under addition:
  - $f_1, f_2 \in I \;\Rightarrow\; f_1 + f_2 \in I$.
- Closed under multiplication with any element:
  - $f \in I, g \in K[\vec{x}] \;\Rightarrow\; gf \in I$.
- $\langle g_1, \dots, g_m \rangle = \{\sum_{i=1}^{m} \lambda_i g_i \mid \lambda_i \in K[\vec{x}]\}$.
- Can any ideal $I$ be written as $I = \langle g_1, \dots, g_l \rangle$ for a finite $l$?
  - Si se puede!
  - Hilbert's finite basis theorem.

# Hilbert's Finite Basis Theorem

*Hilbert, David (1890). "Über die Theorie der algebraischen Formen". Mathematische Annalen. 36 (4): 473–534.*

Any ideal $I$ over $K[x_1, \dots, x_n]$, where $K$ is a field, can be written $I = \langle g_1, \dots, g_m \rangle$ for a finite set of generators.

**Corollary:** Any increasing chain of ideals converges:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots I_N \subseteq \cdots$$

- $\exists j \geq 1$ such that $I_j = I_{j+1} = \cdots$.
- Modern terminology $K[x_1, \dots, x_n]$ is a *Noetherian Ring*.

# Proof of Hilbert's Finite Basis Theorem

- Consider the set of all leading terms of $I$.
    - $J = \{LT(p) \mid p \in I\}$.
    - Consider the ideal generated by $J$.

*Example:* $I = \{x^2, x^2y, 2x^3, \frac{1}{2}x^2y^2 + x^2 + x^2y, \cdots\}$

- $LT(I) = \{x^2, x^2y, x^3, \frac{1}{2}x^2y^2, \cdots\}$

# Proof of Hilbert's Finite Basis Theorem

- Consider the set of all leading terms of $I$.
  - $J = \{LT(p) \mid p \in I\}$.
  - Consider the ideal generated by $J$.

*Example:* $I = \{x^2, x^2y, 2x^3, \frac{1}{2}x^2y^2 + x^2 + x^2y, \cdots\}$

- $LT(I) = \{x^2, x^2y, x^3, \frac{1}{2}x^2y^2, \cdots\}$
- Since $K$ is a field, the coefficients can be set to $1$.

# Proof of Hilbert's Finite Basis Theorem

- Consider the set of all leading terms of $I$.
  - $J = \{LT(p) \mid p \in I\}$.
  - Consider the ideal generated by $J$.

*Example:* $I = \{x^2, x^2y, 2x^3, \frac{1}{2}x^2y^2 + x^2 + x^2y, \cdots\}$

- $LT(I) = \{x^2, x^2y, x^3, \frac{1}{2}x^2y^2, \cdots\}$
- Since $K$ is a field, the coefficients can be set to $1$.
- Monomial ideal: ideal generated by a set of monomials.

# Dickson's Lemma

- Every monomial ideal is finitely generated.
- TODO: include a nice picture visualizing this.
  - Monomial ideals as a subset of points in $\mathbb{N}^n$.
  - Closed under addition.

# Proof of Hilbert's Finite Basis Theorem

- Consider the set of all leading terms of $I$.

# Proof of Hilbert's Finite Basis Theorem

- Consider the set of all leading terms of $I$.
  - $J = \{LT(p) \mid p \in I\}$.

# Proof of Hilbert's Finite Basis Theorem

- Consider the set of all leading terms of $I$.
  - $J = \{LT(p) \mid p \in I\}$.
  - Consider the ideal generated by $J$.

## Proof of Hilbert's Finite Basis Theorem

- Consider the set of all leading terms of $I$.
  - $J = \{LT(p) \mid p \in I\}$.
  - Consider the ideal generated by $J$.
  - **Dickson's Lemma** $J$ is finitely generated.

$$\langle J \rangle = \langle m_1, \ldots, m_k \rangle$$

# Proof of Hilbert's Finite Basis Theorem

- Consider the set of all leading terms of $I$.
  - $J = \{LT(p) \mid p \in I\}$.
  - Consider the ideal generated by $J$.
  - **Dickson's Lemma** $J$ is finitely generated.

$$\langle J \rangle = \langle m_1, \dots, m_k \rangle$$

- Consider the basis $g_1, \dots, g_k \in I$ such that $LT(g_i) = m_i$.

# Proof of Hilbert's Finite Basis Theorem

- Consider the set of all leading terms of $I$.
  - $J = \{LT(p) \mid p \in I\}$.
  - Consider the ideal generated by $J$.
  - **Dickson's Lemma** $J$ is finitely generated.

$$\langle J \rangle = \langle m_1, \dots, m_k \rangle$$

- Consider the basis $g_1, \dots, g_k \in I$ such that $LT(g_i) = m_i$.
- Claim: $I = \langle g_1, \dots, g_k \rangle$

# Proof (Continued)

Claim: $I = \langle g_1, \dots, g_k \rangle$

- $\langle g_1, \dots, g_k \rangle \subseteq I$, since $g_1, \dots, g_k \in I$.

# Proof (Continued)

Claim: $I = \langle g_1, \dots, g_k \rangle$

- $\langle g_1, \dots, g_k \rangle \subseteq I$, since $g_1, \dots, g_k \in I$.
- To prove: $I \subseteq \langle g_1, \dots, g_k \rangle$.

## Proof (Continued)

Claim: $I = \langle g_1, \dots, g_k \rangle$

- $\langle g_1, \dots, g_k \rangle \subseteq I$, since $g_1, \dots, g_k \in I$.
- To prove: $I \subseteq \langle g_1, \dots, g_k \rangle$.
    - Contradiction: let $p \in I$ but $p \notin \langle g_1, \dots, g_k \rangle$.

# Proof (Continued)

Claim: $I = \langle g_1, \dots, g_k \rangle$

- $\langle g_1, \dots, g_k \rangle \subseteq I$, since $g_1, \dots, g_k \in I$.
- To prove: $I \subseteq \langle g_1, \dots, g_k \rangle$.
    - Contradiction: let $p \in I$ but $p \notin \langle g_1, \dots, g_k \rangle$.
    - Consider polynomial division of $p$ w.r.t $g_1, \dots, g_k$.

# Proof (Continued)

Claim: $I = \langle g_1, \dots, g_k \rangle$

- $\langle g_1, \dots, g_k \rangle \subseteq I$, since $g_1, \dots, g_k \in I$.
- To prove: $I \subseteq \langle g_1, \dots, g_k \rangle$.
  - Contradiction: let $p \in I$ but $p \notin \langle g_1, \dots, g_k \rangle$.
  - Consider polynomial division of $p$ w.r.t $g_1, \dots, g_k$.
  - $p = \sum_{i=1}^{k} q_i g_i + r$, where $r \neq 0$.

# Proof (Continued)

Claim: $I = \langle g_1, \dots, g_k \rangle$

- $\langle g_1, \dots, g_k \rangle \subseteq I$, since $g_1, \dots, g_k \in I$.
- To prove: $I \subseteq \langle g_1, \dots, g_k \rangle$.
    - Contradiction: let $p \in I$ but $p \notin \langle g_1, \dots, g_k \rangle$.
    - Consider polynomial division of $p$ w.r.t $g_1, \dots, g_k$.
    - $p = \sum_{i=1}^{k} q_i g_i + r$, where $r \neq 0$.
    - $r = \left(p - \sum_{i=1}^{k} q_i g_i\right) \in I$.

# Proof (Continued)

Claim: $I = \langle g_1, \dots, g_k \rangle$

- $\langle g_1, \dots, g_k \rangle \subseteq I$, since $g_1, \dots, g_k \in I$.
- To prove: $I \subseteq \langle g_1, \dots, g_k \rangle$.
  - Contradiction: let $p \in I$ but $p \notin \langle g_1, \dots, g_k \rangle$.
  - Consider polynomial division of $p$ w.r.t $g_1, \dots, g_k$.
  - $p = \sum_{i=1}^{k} q_i g_i + r$, where $r \neq 0$.
  - $r = \left(p - \sum_{i=1}^{k} q_i g_i\right) \in I$.
  - However, $LT(r)$ is not divisible by $LT(g_i)$.

# Proof (Continued)

Claim: $I = \langle g_1, \dots, g_k \rangle$

- $\langle g_1, \dots, g_k \rangle \subseteq I$, since $g_1, \dots, g_k \in I$.
- To prove: $I \subseteq \langle g_1, \dots, g_k \rangle$.
  - Contradiction: let $p \in I$ but $p \notin \langle g_1, \dots, g_k \rangle$.
  - Consider polynomial division of $p$ w.r.t $g_1, \dots, g_k$.
  - $p = \sum_{i=1}^{k} q_i g_i + r$, where $r \neq 0$.
  - $r = \left(p - \sum_{i=1}^{k} q_i g_i\right) \in I$.
  - However, $LT(r)$ is not divisible by $LT(g_i)$.
  - $r \notin I$.

# Proof (Continued)

Claim: $I = \langle g_1, \dots, g_k \rangle$

- $\langle g_1, \dots, g_k \rangle \subseteq I$, since $g_1, \dots, g_k \in I$.
- To prove: $I \subseteq \langle g_1, \dots, g_k \rangle$.
  - Contradiction: let $p \in I$ but $p \notin \langle g_1, \dots, g_k \rangle$.
  - Consider polynomial division of $p$ w.r.t $g_1, \dots, g_k$.
  - $p = \sum_{i=1}^{k} q_i g_i + r$, where $r \neq 0$.
  - $r = \left(p - \sum_{i=1}^{k} q_i g_i\right) \in I$.
  - However, $LT(r)$ is not divisible by $LT(g_i)$.
  - $r \notin I$.
  - Contradiction!

# Gröbner Basis

Consider ideal $I \subseteq K[x_1, \dots, x_n]$.

Let $G = \langle g_1, \dots, g_m \rangle$ such that

$$\langle LT(g_1), \dots, LT(g_m) \rangle = \langle LT(I) \rangle$$

- $G$ appeared in the proof of Hibert's theorem.

# Gröbner Basis

Consider ideal $I \subseteq K[x_1, \dots, x_n]$.

Let $G = \langle g_1, \dots, g_m \rangle$ such that

$$\langle LT(g_1), \dots, LT(g_m) \rangle = \langle LT(I) \rangle$$

- $G$ appeared in the proof of Hibert's theorem.
- Let $p \in I$, consider $r$ reminder of $p$ divided by $g_1, \dots, g_m$.

# Gröbner Basis

Consider ideal $I \subseteq K[x_1, \dots, x_n]$.

Let $G = \langle g_1, \dots, g_m \rangle$ such that

$$\langle LT(g_1), \dots, LT(g_m) \rangle = \langle LT(I) \rangle$$

- $G$ appeared in the proof of Hibert's theorem.
- Let $p \in I$, consider $r$ reminder of $p$ divided by $g_1, \dots, g_m$.
    - **Claim:** $r = 0$.

# Gröbner Basis

Consider ideal $I \subseteq K[x_1, \dots, x_n]$.

Let $G = \langle g_1, \dots, g_m \rangle$ such that

$$\langle LT(g_1), \dots, LT(g_m) \rangle = \langle LT(I) \rangle$$

- $G$ appeared in the proof of Hibert's theorem.
- Let $p \in I$, consider $r$ reminder of $p$ divided by $g_1, \dots, g_m$.
  - **Claim:** $r = 0$.
- Contradiction: $r = (p - \sum_{i=1}^{m} q_i g_i) \in I$.

# Gröbner Basis

Consider ideal $I \subseteq K[x_1, \ldots, x_n]$.

Let $G = \langle g_1, \ldots, g_m \rangle$ such that

$$\langle LT(g_1), \ldots, LT(g_m) \rangle = \langle LT(I) \rangle$$

- $G$ appeared in the proof of Hibert's theorem.
- Let $p \in I$, consider $r$ reminder of $p$ divided by $g_1, \ldots, g_m$.
  - **Claim:** $r = 0$.
- Contradiction: $r = (p - \sum_{i=1}^{m} q_i g_i) \in I$.
  - However, $LT(r)$ is not divisible by $LT(g_i)$.

# Gröbner Basis

Consider ideal $I \subseteq K[x_1, \dots, x_n]$.

Let $G = \langle g_1, \dots, g_m \rangle$ such that

$$\langle LT(g_1), \dots, LT(g_m) \rangle = \langle LT(I) \rangle$$

- $G$ appeared in the proof of Hibert's theorem.
- Let $p \in I$, consider $r$ reminder of $p$ divided by $g_1, \dots, g_m$.
    - **Claim:** $r = 0$.
- Contradiction: $r = (p - \sum_{i=1}^{m} q_i g_i) \in I$.
    - However, $LT(r)$ is not divisible by $LT(g_i)$.
    - $r \in I$, $LT(r) \in LT(I)$ but $LT(r) \notin \langle LT(g_1), \dots, LT(g_m) \rangle$.

# Gröbner Basis

Consider ideal $I \subseteq K[x_1, \dots, x_n]$.

Let $G = \langle g_1, \dots, g_m \rangle$ such that

$$\langle LT(g_1), \dots, LT(g_m) \rangle = \langle LT(I) \rangle$$

- $G$ appeared in the proof of Hibert's theorem.
- Let $p \in I$, consider $r$ reminder of $p$ divided by $g_1, \dots, g_m$.
  - **Claim:** $r = 0$.
- Contradiction: $r = (p - \sum_{i=1}^{m} q_i g_i) \in I$.
  - However, $LT(r)$ is not divisible by $LT(g_i)$.
  - $r \in I$, $LT(r) \in LT(I)$ but $LT(r) \notin \langle LT(g_1), \dots, LT(g_m) \rangle$.
  - Contradiction!

# Gröbner Basis

Consider ideal $I \subseteq K[x_1, \ldots, x_n]$.

Let $G = \langle g_1, \ldots, g_m \rangle$ such that

$$\langle LT(g_1), \ldots, LT(g_m) \rangle = \langle LT(I) \rangle$$

- $G$ appeared in the proof of Hibert's theorem.
- Let $p \in I$, consider $r$ reminder of $p$ divided by $g_1, \ldots, g_m$.
  - **Claim:** $r = 0$.
- Contradiction: $r = (p - \sum_{i=1}^{m} q_i g_i) \in I$.
  - However, $LT(r)$ is not divisible by $LT(g_i)$.
  - $r \in I$, $LT(r) \in LT(I)$ but $LT(r) \notin \langle LT(g_1), \ldots, LT(g_m) \rangle$.
  - Contradiction!
- $G$ is called a Gröbner basis of $I$.

# S-Polynomials

Take two polynomials $g_1, g_2$.

$$S(g_1, g_2) = \frac{L(g_1, g_2)}{LT(g_1)} g_1 - \frac{L(g_1, g_2)}{LT(g_2)} g_2$$

- $L(g_1, g_2)$ is the smallest degree monomial divisible by both $LT(g_1)$ and $LT(g_2)$.
- $LT(g_1) = a_1 x^{\alpha_1}, LT(g_2) = a_2 x^{\alpha_2}$.
  - $L(g_1, g_2) = x^{\max(\alpha_1, \alpha_2)}$.
- Forces cancellation of the leading terms.

- $g_1 = xy^2 - x - y, g_2 = x^2y - x - y$.

- $g_1 = xy^2 - x - y, g_2 = x^2y - x - y$.
- $L(g_1, g_2) = x^2y^2$.

- $g_1 = xy^2 - x - y, g_2 = x^2y - x - y$.
- $L(g_1, g_2) = x^2y^2$.
- $S(g_1, g_2) = \frac{x^2y^2}{xy^2}(g_1) - \frac{x^2y^2}{x^2y}(g_2)$

- $g_1 = xy^2 - x - y, g_2 = x^2y - x - y$.
- $L(g_1, g_2) = x^2y^2$.
- $S(g_1, g_2) = \frac{x^2y^2}{xy^2}(g_1) - \frac{x^2y^2}{x^2y}(g_2)$
    - $= x^2y^2 - x^2 - xy - x^2y^2 + xy + y^2$

- $g_1 = xy^2 - x - y, g_2 = x^2y - x - y$.
- $L(g_1, g_2) = x^2y^2$.
- $S(g_1, g_2) = \frac{x^2y^2}{xy^2}(g_1) - \frac{x^2y^2}{x^2y}(g_2)$
  - $= x^2y^2 - x^2 - xy - x^2y^2 + xy + y^2$
  - $= y^2 - x^2$.

# S-Polynomials (cont)

- S-polynomials capture the result of cancellation:

## S-Polynomials (cont)

- S-polynomials capture the result of cancellation:
- Suppose $LM(p_i) = \vec{x}^{\delta}$ for $i = 1, \dots, m$.

# S-Polynomials (cont)

- S-polynomials capture the result of cancellation:
- Suppose $LM(p_i) = \vec{x}^{\delta}$ for $i = 1, \dots, m$.
- However, $LM(\sum_{i=1}^{m} p_i) \prec \vec{x}^{\delta}$,

# S-Polynomials (cont)

- S-polynomials capture the result of cancellation:
- Suppose $LM(p_i) = \vec{x}^\delta$ for $i = 1, \ldots, m$.
- However, $LM(\sum_{i=1}^m p_i) \prec \vec{x}^\delta$,
  - It follows that $\sum_{i=1}^m p_i = \sum_{i=1}^m \sum_{j>i} c_{i,j} S(p_i, p_j)$, for some $c_{i,j} \in K$.

# Büchberger's Criterion

A basis $I = \langle g_1, \dots, g_m \rangle$ is a Gröbner basis if and only if

- For every $g_i, g_j,\ (i \neq j)$, reminder of $S(g_i, g_j)$ upon division by $g_1, \dots, g_m$ is $0$.
- Previously, $I = \langle xy^2 - x - y, x^2y - x - y \rangle$, not a Gröbner basis.
- $x^2 - y^2 \in I$ but reminder of $x^2 - y^2$ is non-zero.
- However, $I = \langle y^3 - x - y, x^2 - y^2, xy^2 - x - y \rangle$ is a Gröbner basis.

```python
import sympy as sp
from sympy.abc import x, y

F = [x * y**2  -x - y , x**2*y -x -y]
G = sp.Groebner(F, x, y, order='grlex',domain='C')
print(G)
```

Result: $\langle y^3 - x - y, x^2 - y^2, xy^2 - x - y \rangle$.

- $S(x^2 - y^2, xy^2 - x - y) = y^4 - x^2 - xy$
  - $= y \times (y^3 - x - y) + 1 \times (x^2 - y^2) + 0.$
  - Reminder is zero $\checkmark$.
- $S(y^3 - x - y, x^2 - y^2) = y^5 - x^3 - x^2 y$
  - $= y^2(y^3 - x - y) - (x + y)(x^2 - y^2) + 0.$
  - Reminder is zero $\checkmark$.

# Büchberger's Algorithm

- An algorithm for constructing Gröbner basis.
  - Input $I = \langle g_1, \ldots, g_m \rangle$
    - Monomial order $\prec$.
  - Output $\langle f_1, \ldots, f_K \rangle$ - Gröbner basis for $I$.

- $I_0 = \langle g_1, \ldots, g_m \rangle$.

# Büchberger's Algorithm

- An algorithm for constructing Gröbner basis.
  - Input $I = \langle g_1, \dots, g_m \rangle$
    - Monomial order $\prec$.
  - Output $\langle f_1, \dots, f_K \rangle$ - Gröbner basis for $I$.
- $I_0 = \langle g_1, \dots, g_m \rangle$.
- Let $I_j = \langle p_1, \dots, p_l \rangle$.

# Büchberger's Algorithm

- An algorithm for constructing Gröbner basis.
  - Input $I = \langle g_1, \dots, g_m \rangle$
    - Monomial order $\prec$.
  - Output $\langle f_1, \dots, f_K \rangle$ - Gröbner basis for $I$.
- $I_0 = \langle g_1, \dots, g_m \rangle$.
- Let $I_j = \langle p_1, \dots, p_l \rangle$.
- Check if current basis is Gröbner.

## Büchberger's Algorithm

- An algorithm for constructing Gröbner basis.
  - Input $I = \langle g_1, \dots, g_m \rangle$
    - Monomial order $\prec$.
  - Output $\langle f_1, \dots, f_K \rangle$ - Gröbner basis for $I$.

- $I_0 = \langle g_1, \dots, g_m \rangle$.

- Let $I_j = \langle p_1, \dots, p_l \rangle$.

- Check if current basis is Gröbner.

  - Compute $S(p_i, p_j)$ for each $i \neq j$.

## Büchberger's Algorithm

- An algorithm for constructing Gröbner basis.
    - Input $I = \langle g_1, \dots, g_m \rangle$
        - Monomial order $\prec$.
    - Output $\langle f_1, \dots, f_K \rangle$ - Gröbner basis for $I$.
- $I_0 = \langle g_1, \dots, g_m \rangle$.
- Let $I_j = \langle p_1, \dots, p_l \rangle$.
- Check if current basis is Gröbner.
    - Compute $S(p_i, p_j)$ for each $i \neq j$.
    - Compute reminder of $S(p_i, p_j)$ wrt $p_1, \dots, p_l$.

# Büchberger's Algorithm

- An algorithm for constructing Gröbner basis.
  - Input $I = \langle g_1, \ldots, g_m \rangle$
    - Monomial order $\prec$.
  - Output $\langle f_1, \ldots, f_K \rangle$ - Gröbner basis for $I$.
- $I_0 = \langle g_1, \ldots, g_m \rangle$.
- Let $I_j = \langle p_1, \ldots, p_l \rangle$.
- Check if current basis is Gröbner.
  - Compute $S(p_i, p_j)$ for each $i \neq j$.
  - Compute reminder of $S(p_i, p_j)$ wrt $p_1, \ldots, p_l$.
  - $I_{j+1} = \langle p_1, \ldots, p_l, r_{i,j} \rangle$.

# Büchberger's Algorithm

- An algorithm for constructing Gröbner basis.
  - Input $I = \langle g_1, \dots, g_m \rangle$
    - Monomial order $\prec$.
  - Output $\langle f_1, \dots, f_K \rangle$ - Gröbner basis for $I$.
- $I_0 = \langle g_1, \dots, g_m \rangle$.
- Let $I_j = \langle p_1, \dots, p_l \rangle$.
- Check if current basis is Gröbner.
  - Compute $S(p_i, p_j)$ for each $i \neq j$.
  - Compute reminder of $S(p_i, p_j)$ wrt $p_1, \dots, p_l$.
  - $I_{j+1} = \langle p_1, \dots, p_l, r_{i,j} \rangle$.
- If all S-polynomials leave a reminder of $0$, then we have a Gröbner basis.

# Büchberger's Algorithm

- An algorithm for constructing Gröbner basis.
  - Input $I = \langle g_1, \dots, g_m \rangle$
    - Monomial order $\prec$.
  - Output $\langle f_1, \dots, f_K \rangle$ - Gröbner basis for $I$.
- $I_0 = \langle g_1, \dots, g_m \rangle$.
- Let $I_j = \langle p_1, \dots, p_l \rangle$.
- Check if current basis is Gröbner.
  - Compute $S(p_i, p_j)$ for each $i \neq j$.
  - Compute reminder of $S(p_i, p_j)$ wrt $p_1, \dots, p_l$.
  - $I_{j+1} = \langle p_1, \dots, p_l, r_{i,j} \rangle$.
- If all S-polynomials leave a reminder of $0$, then we have a Gröbner basis.
- Termination?

# Complexity of Gröbner Basis

- Ideal membership is known to be EXPSPACE-complete.
  - Ernst Mayr, Journal of Complexity, 1997.
- Gröbner basis can be quite expensive.
  - Bound on the degree of polynomials is very high.
  - See Thomas Dube, SIAM J. of Comp. 1990.
- Büchberger Algorithm complexity bounded in EXPSPACE (?).

# Gröbner Basis

- Expensive computation in the worst case.
  - Best algorithms include Faguere's F5 algorithm.
- It is implemented in most computer algebra systems.
- Ideas to speed up:
  - Dynamically alter the monomial ordering on the fly.
  - Avoid unnecessary S-polynomial reductions.
  - ...

## Weak Nullstellensatz

- Let $p_1 = 0, \dots, p_m = 0$ represent an inconsistent set of polynomial inequalities.
- $1 \in \langle p_1, \dots, p_m \rangle$.

**Corollary** (Reduced) Gröbner basis must be $\langle 1 \rangle$.

# Nullstellensatz

$$p_1 = 0, \dots, p_m = 0 \vDash p = 0$$

Hilbert's Nullstellensatz:

$$p^r \in \langle p_1, \dots, p_m \rangle$$

- Rabinowitsch trick:
    - Compute Grobner basis of $\langle p_1, \dots, p_n, (1 - yp) \rangle$
    - **Claim:** Entailment holds iff $1 \in \langle p_1, \dots, p_n, (1 - yp) \rangle$

# Rabinowitsch Trick

- $p^r \in \langle p_1, \dots, p_m \rangle$ for some $r \in \mathbb{N}$
- $1 \in \langle p_1, \dots, p_n, (1 - yp) \rangle$

**Proof** See chapter 3 of book/during lecture.

## Operations on Varieties

- Algebraic Variety $V$
  - Representation: Gröbner basis of the ideal $\mathsf{Id}(V)$.
- Intersection of varieties:
- $V_1 \cap V_2$ – Groebner$(G_1 \cup G_2)$
- Union of varieties:
  - $V_1 \cup V_2 - G_1 \otimes G_2$.

- Inclusion Checking: $V_1 \subseteq V_2$
  - Check that every generator in $G_1$ belongs to $\langle G_2 \rangle$
- Image computation:
  - Assertion: $\varphi : g_1(\vec{x}) = 0 \;\wedge\; \cdots \;\wedge\; g_m(\vec{x}) = 0$
  - Transition relation $\rho :\; p_1(\vec{x}, \vec{x}') = 0 \;\wedge\; \cdots\; p_m(\vec{x}, \vec{x}') = 0.$
  - Post-Condition: $(\exists\, \vec{x})\; \varphi[\vec{x}] \wedge\; \rho[\vec{x}, \vec{x}']$

# Elimination Theory

Let $I : \langle p_1, \dots, p_m \rangle$ be an ideal in $K[x_1, \dots, x_n, y_1, \dots, y_m]$.

- Compute Gröbner basis $G$ under an *elimination order*

# Elimination Theory

Let $I : \langle p_1, \dots, p_m \rangle$ be an ideal in $K[x_1, \dots, x_n, y_1, \dots, y_m]$.

- Compute Gröbner basis $G$ under an *elimination order*
  - Eg., lexicographic ordering: $x_1 > \cdots > x_n > y_1 > \cdots > y_m$

# Elimination Theory

Let $I : \langle p_1, \ldots, p_m \rangle$ be an ideal in $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$.

- Compute Gröbner basis $G$ under an *elimination order*
  - Eg., lexicographic ordering: $x_1 > \cdots > x_n > y_1 > \cdots > y_m$
- Take all polynomials involving $y_1, \ldots, y_m$:

# Elimination Theory

Let $I : \langle p_1, \dots, p_m \rangle$ be an ideal in $K[x_1, \dots, x_n, y_1, \dots, y_m]$.

- Compute Gröbner basis $G$ under an *elimination order*
  - Eg., lexicographic ordering: $x_1 > \cdots > x_n > y_1 > \cdots > y_m$
- Take all polynomials involving $y_1, \dots, y_m$:
  - $\widehat{G} = G \cap K[y_1, \dots, y_m]$

# Elimination Theory

Let $I : \langle p_1, \dots, p_m \rangle$ be an ideal in $K[x_1, \dots, x_n, y_1, \dots, y_m]$.

- Compute Gröbner basis $G$ under an *elimination order*
  - Eg., lexicographic ordering: $x_1 > \cdots > x_n > y_1 > \cdots > y_m$
- Take all polynomials involving $y_1, \dots, y_m$:
  - $\widehat{G} = G \cap K[y_1, \dots, y_m]$
- Claim: $I \cap K[y_1, \dots, y_m] = \langle \widehat{G} \rangle$.

## Next Session

- Tuesday the 15th.
- Will try to show some calculations for programs and differential equations.
- Move on to talking about inequalities/semi-algebraic sets.