

From Solutions of Systems of Polynomial Equations to Gröbner Bases

Kenneth Chu

`chu@math.utexas.edu`

Department of Mathematics

University of Texas at Austin

October 24, 2006

Abstract

Abstract

- Huygens' Principle for waves ...

Abstract

- Huygens' Principle for waves ...
- Gröbner bases as "simplification" tools of algebraic systems of equations.

Abstract

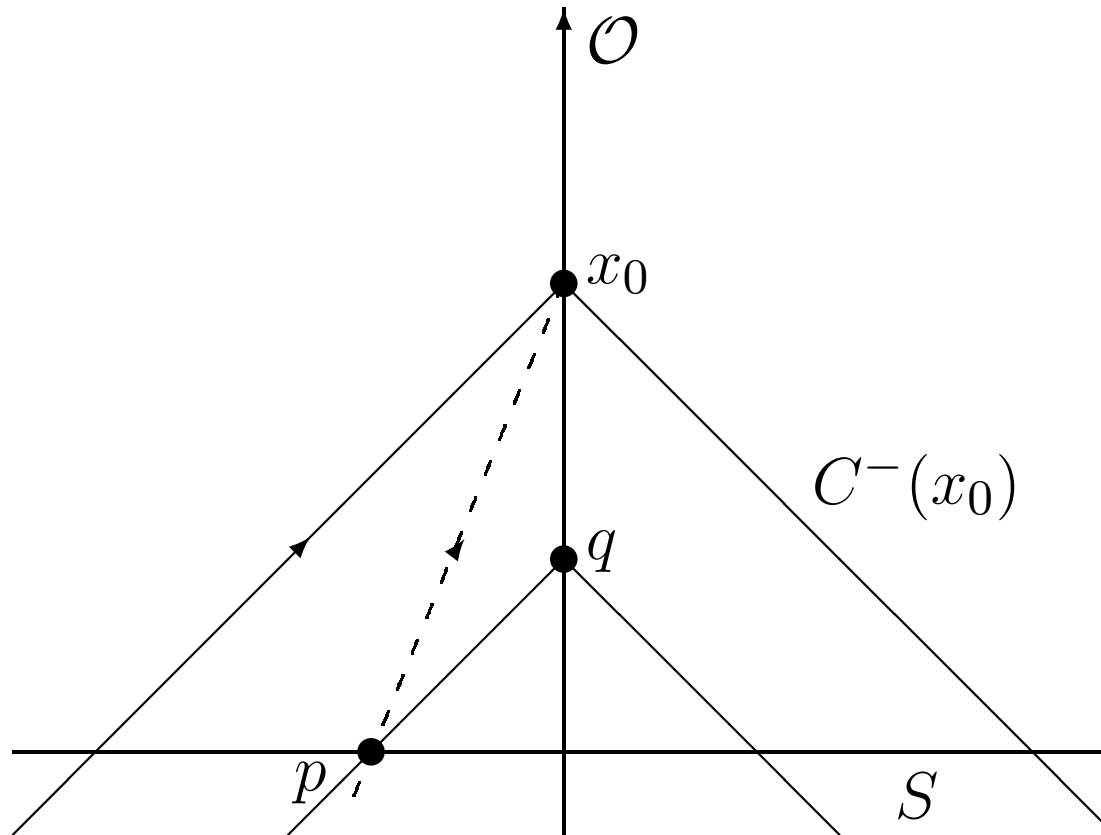
- Huygens' Principle for waves ...
- Gröbner bases as "simplification" tools of algebraic systems of equations.
- "Pathologies" of the Multivariate Division Algorithm (MDA)

Abstract

- Huygens' Principle for waves ...
- Gröbner bases as "simplification" tools of algebraic systems of equations.
- "Pathologies" of the Multivariate Division Algorithm (MDA)
- Gröbner bases as "cure" to MDA

Illustration of Huygens' Principle

Illustration of Huygens' Principle



The dash line indicates “ripples” from the event p on the Cauchy surface S to the event x_0 .

The Necessary Conditions

The Necessary Conditions

It can be shown that the validity of Huygens' Principle is equivalent to the vanishing of a certain quantity σ .

The Necessary Conditions

It can be shown that the validity of Huygens' Principle is equivalent to the vanishing of a certain quantity σ .

$$\sigma = 0 \text{ on } C_{-}^{\Omega}(x_0) \implies \text{TS}[\sigma; a_1 \dots a_m] = 0, \text{ for every integer } m \geq 0.$$

The Necessary Conditions

It can be shown that the validity of Huygens' Principle is equivalent to the vanishing of a certain quantity σ .

$$\sigma = 0 \text{ on } C_{-}^{\Omega}(x_0) \implies \text{TS}[\sigma;_{a_1 \dots a_m}] = 0, \text{ for every integer } m \geq 0.$$

The first few terms in the Taylor series of σ

$$(1 \text{ eqn}) \quad 0 = B - \frac{1}{2} A^k_{;k} - \frac{1}{4} A_k A^k + \frac{R}{6}$$

$$(4 \text{ eqns}) \quad 0 = H^k_{a;k}$$

$$(4^2 \text{ eqns}) \quad 0 = S_{abk}{}^k - \frac{1}{2} C^k_{ab}{}^l L_{kl} + 5 \left(H_{ak} H_b{}^k - \frac{1}{4} g_{ab} H_{kl} H^{kl} \right)$$

$$(4^3 \text{ eqns}) \quad 0 = 3S_{abk} H^k_c + C^k_{ab}{}^l H_{ck;l}$$

$$(4^4 \text{ eqns}) \quad 0 = \begin{cases} 3C_{kabl;m} C^k_{cd}{}^{lm} + 8C^k_{ab}{}^l S_{kld} + 40S_{ab}{}^k S_{cdk} \\ -8C^k_{ab}{}^l S_{klc;d} - 24C^k_{ab}{}^l S_{cdk;l} + 4C^k_{ab}{}^l C_l{}^m{}_{ck} L_{dm} \\ +12C^k_{ab}{}^l C^m_{cdl} L_{km} + 12H_{ka;b} H^k_d - 16H_{ka;b} H^k_{c;d} \\ -84H^k_a C_{kbcl} H^l_d - 18H_{ka} H^k_b L_{cd} \end{cases}$$

How would you solve this (System A)?

How would you solve this (System A)?

(for $\alpha, \tau, \bar{\alpha}, \bar{\tau}$)

$$2\alpha + 3\bar{\tau} + 2\bar{\alpha} + 3\tau = 0$$

$$27\bar{\tau}^2 + 12\bar{\alpha}\bar{\tau} + 4\alpha^2 - 40\alpha\bar{\alpha} + 24\alpha\bar{\tau} = 0$$

How would you solve this (System A)?

(for $\alpha, \tau, \bar{\alpha}, \bar{\tau}$)

$$2\alpha + 3\bar{\tau} + 2\bar{\alpha} + 3\tau = 0$$

$$27\bar{\tau}^2 + 12\bar{\alpha}\bar{\tau} + 4\alpha^2 - 40\alpha\bar{\alpha} + 24\alpha\bar{\tau} = 0$$

$$\begin{aligned} & -2188\bar{\alpha}\alpha\bar{\tau} + 6294\tau\alpha\bar{\tau} - 1584\tau\bar{\alpha}^2 \\ & + 1188\tau^2\bar{\alpha} - 7172\bar{\tau}\bar{\alpha}^2 - 5048\bar{\alpha}^2\alpha \\ & + 2824\alpha^2\bar{\tau} + 3465\bar{\tau}\tau^2 + 1278\alpha\bar{\tau}^2 \\ & - 1584\bar{\alpha}^3 - 1984\tau\bar{\alpha}\alpha - 3960\tau\bar{\alpha}\bar{\tau} \\ & + 904\alpha^3 + 2277\tau\bar{\tau}^2 - 5742\bar{\alpha}\bar{\tau}^2 \\ & + 608\bar{\alpha}\alpha^2 = 0 \end{aligned}$$

How would you solve this (System A)?

(for $\alpha, \tau, \bar{\alpha}, \bar{\tau}$)

$$2\alpha + 3\bar{\tau} + 2\bar{\alpha} + 3\tau = 0$$

$$27\bar{\tau}^2 + 12\bar{\alpha}\bar{\tau} + 4\alpha^2 - 40\alpha\bar{\alpha} + 24\alpha\bar{\tau} = 0$$

$$\begin{aligned} & -2188\bar{\alpha}\alpha\bar{\tau} + 6294\tau\alpha\bar{\tau} - 1584\tau\bar{\alpha}^2 \\ & + 1188\tau^2\bar{\alpha} - 7172\bar{\tau}\bar{\alpha}^2 - 5048\bar{\alpha}^2\alpha \\ & + 2824\alpha^2\bar{\tau} + 3465\bar{\tau}\tau^2 + 1278\alpha\bar{\tau}^2 \\ & - 1584\bar{\alpha}^3 - 1984\tau\bar{\alpha}\alpha - 3960\tau\bar{\alpha}\bar{\tau} \\ & + 904\alpha^3 + 2277\tau\bar{\tau}^2 - 5742\bar{\alpha}\bar{\tau}^2 \\ & + 608\bar{\alpha}\alpha^2 = 0 \end{aligned}$$

$$\begin{aligned} & 1396\bar{\alpha}\alpha\bar{\tau} + 1302\tau\alpha\bar{\tau} - 396\bar{\tau}\bar{\alpha}^2 \\ & + 1320\bar{\alpha}^2\alpha + 2248\alpha^2\bar{\tau} + 297\bar{\tau}\tau^2 \\ & + 4734\alpha\bar{\tau}^2 + 1320\tau\bar{\alpha}\alpha - 396\tau\bar{\alpha}\bar{\tau} \\ & - 3240\tau\alpha^2 - 990\alpha\tau^2 - 198\bar{\tau}^3 \\ & - 664\alpha^3 - 99\tau\bar{\tau}^2 - 66\bar{\alpha}\bar{\tau}^2 \\ & - 2512\bar{\alpha}\alpha^2 = 0 \end{aligned}$$

How about this (System B)?

How about this (System B)?

$$\bar{\alpha} = 0$$

$$2\alpha + 3\bar{\tau} = 0$$

$$\tau = 0$$

How about this (System B)?

$$\bar{\alpha} = 0$$

$$2\alpha + 3\bar{\tau} = 0$$

$$\tau = 0$$

Surprise! Surprise!

How about this (System B)?

$$\bar{\alpha} = 0$$

$$2\alpha + 3\bar{\tau} = 0$$

$$\tau = 0$$

Surprise! Surprise!

The previous two systems are “transformations” of each other via elementary algebraic manipulations (adding, subtracting equations, etc.)

How about this (System B)?

$$\bar{\alpha} = 0$$

$$2\alpha + 3\bar{\tau} = 0$$

$$\tau = 0$$

Surprise! Surprise!

The previous two systems are “transformations” of each other via elementary algebraic manipulations (adding, subtracting equations, etc.)

They therefore have **exactly** the same solutions.

I was desperate to know ...

I was desperate to know ...

How to “simplify” a system of polynomial equations

I was desperate to know ...

How to “simplify” a system of polynomial
equations

in a systematic fashion

I was desperate to know ...

How to “simplify” a system of polynomial equations

in a systematic fashion

so that the resulting system is “easy” to solve.

Commutative Algebra Trivia ...

Commutative Algebra Trivia ...

Given any subset $S \subseteq \mathbb{C}[x_1, \dots, x_n]$,

Commutative Algebra Trivia ...

Given any subset $S \subseteq \mathbb{C}[x_1, \dots, x_n]$, define

$$\langle S \rangle := \left\{ \sum_{i=1}^k f_i s_i \mid s_i \in S, f_i \in \mathbb{C}[x_1, \dots, x_n] \right\}.$$

Commutative Algebra Trivia ...

Given any subset $S \subseteq \mathbb{C}[x_1, \dots, x_n]$, define

$$\langle S \rangle := \left\{ \sum_{i=1}^k f_i s_i \mid s_i \in S, f_i \in \mathbb{C}[x_1, \dots, x_n] \right\}.$$

$\langle S \rangle$ is called the ideal of $\mathbb{C}[x_1, \dots, x_n]$
generated by the subset $S \subseteq \mathbb{C}[x_1, \dots, x_n]$.

Solutions of $S = \text{Solutions of } \langle S \rangle$

Solutions of $S = \text{Solutions of } \langle S \rangle$

We say that $(c_1, \dots, c_n) \in \mathbb{C}^n$ is a solution of S if

Solutions of $S = \text{Solutions of } \langle S \rangle$

We say that $(c_1, \dots, c_n) \in \mathbb{C}^n$ is a solution of S if

$$f(c_1, \dots, c_n) = 0,$$

Solutions of $S = \text{Solutions of } \langle S \rangle$

We say that $(c_1, \dots, c_n) \in \mathbb{C}^n$ is a solution of S if

$$f(c_1, \dots, c_n) = 0,$$

for all $f(x_1, \dots, x_n) \in S \subseteq \mathbb{C}[x_1, \dots, x_n]$.

Solutions of $S = \text{Solutions of } \langle S \rangle$

We say that $(c_1, \dots, c_n) \in \mathbb{C}^n$ is a solution of S if

$$f(c_1, \dots, c_n) = 0,$$

for all $f(x_1, \dots, x_n) \in S \subseteq \mathbb{C}[x_1, \dots, x_n]$.

Theorem $(c_1, \dots, c_n) \in \mathbb{C}^n$ is a solution of S if and only if it is a solution of $\langle S \rangle$.

Solutions of $S = \text{Solutions of } \langle S \rangle$

We say that $(c_1, \dots, c_n) \in \mathbb{C}^n$ is a solution of S if

$$f(c_1, \dots, c_n) = 0,$$

for all $f(x_1, \dots, x_n) \in S \subseteq \mathbb{C}[x_1, \dots, x_n]$.

Theorem $(c_1, \dots, c_n) \in \mathbb{C}^n$ is a solution of S if and only if it is a solution of $\langle S \rangle$.

Corollary Let $S, T \subseteq \mathbb{C}[x_1, \dots, x_n]$. If $\langle S \rangle = \langle T \rangle$, then S and T have the same solutions.

Key Observation

Key Observation

Corollary Let $S, T \subseteq \mathbb{C}[x_1, \dots, x_n]$. If $\langle S \rangle = \langle T \rangle$, then S and T have the same solutions.

Key Observation

Corollary Let $S, T \subseteq \mathbb{C}[x_1, \dots, x_n]$. If $\langle S \rangle = \langle T \rangle$, then S and T have the same solutions.

Thus, in order to find solutions of given a finite* set of polynomials $S = \{s_1, \dots, s_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$,

Key Observation

Corollary Let $S, T \subseteq \mathbb{C}[x_1, \dots, x_n]$. If $\langle S \rangle = \langle T \rangle$, then S and T have the same solutions.

Thus, in order to find solutions of given a finite* set of polynomials $S = \{s_1, \dots, s_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$, one can attempt to look for a set $G = \{g_1, \dots, g_m\}$,

Key Observation

Corollary Let $S, T \subseteq \mathbb{C}[x_1, \dots, x_n]$. If $\langle S \rangle = \langle T \rangle$, then S and T have the same solutions.

Thus, in order to find solutions of given a finite* set of polynomials $S = \{s_1, \dots, s_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$, one can attempt to look for a set $G = \{g_1, \dots, g_m\}$, with $\langle G \rangle = \langle S \rangle$,

Key Observation

Corollary Let $S, T \subseteq \mathbb{C}[x_1, \dots, x_n]$. If $\langle S \rangle = \langle T \rangle$, then S and T have the same solutions.

Thus, in order to find solutions of given a finite* set of polynomials $S = \{s_1, \dots, s_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$, one can attempt to look for a set $G = \{g_1, \dots, g_m\}$, with $\langle G \rangle = \langle S \rangle$, such that the solutions of G are easy to “eyeball.”

Key Observation

Corollary Let $S, T \subseteq \mathbb{C}[x_1, \dots, x_n]$. If $\langle S \rangle = \langle T \rangle$, then S and T have the same solutions.

Thus, in order to find solutions of given a finite* set of polynomials $S = \{s_1, \dots, s_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$, one can attempt to look for a set $G = \{g_1, \dots, g_m\}$, with $\langle G \rangle = \langle S \rangle$, such that the solutions of G are easy to “eyeball.”

For example,

$$\begin{array}{lcl} \bar{\alpha} & = & 0 \\ 2\alpha + 3\bar{\tau} & = & 0 \\ \tau & = & 0 \end{array} \quad \text{versus} \quad \begin{array}{l} 0 = 2\alpha + 3\bar{\tau} + 2\bar{\alpha} + 3\tau \\ 0 = 27\bar{\tau}^2 + 12\bar{\alpha}\bar{\tau} + 4\alpha^2 - 40\alpha\bar{\alpha} + 24\alpha\bar{\tau} \\ 0 = -2188\bar{\alpha}\alpha\bar{\tau} + 6294\tau\alpha\bar{\tau} + \dots \\ 0 = 1396\bar{\alpha}\alpha\bar{\tau} + 1302\tau\alpha\bar{\tau} + \dots \end{array}$$

* *Hilbert's Basis Thm: Every proper ideal of $\mathbb{C}[x_1, \dots, x_n]$ has a finite generating set.*

How I encountered Gröbner bases

For my Master's thesis, I needed to prove that System A (hideous) admits only the zero solution.

How I encountered Gröbner bases

For my Master's thesis, I needed to prove that System A (hideous) admits only the zero solution.

Of course, System A has an associated ideal

$$I \subseteq \mathbb{C}[x_1, \dots, x_n].$$

How I encountered Gröbner bases

For my Master's thesis, I needed to prove that System A (hideous) admits only the zero solution.

Of course, System A has an associated ideal

$$I \subseteq \mathbb{C}[x_1, \dots, x_n].$$

I found the Gröbner basis for I , which turned out to be $\{\bar{\alpha}, 2\alpha + 3\bar{\tau}, \tau\}$. This gives System B, which can be solved by inspection.

How I encountered Gröbner bases

For my Master's thesis, I needed to prove that System A (hideous) admits only the zero solution.

Of course, System A has an associated ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$.

I found the Gröbner basis for I , which turned out to be $\{\bar{\alpha}, 2\alpha + 3\bar{\tau}, \tau\}$. This gives System B, which can be solved by inspection.

Simplifying systems of polynomial equations is one application of Gröbner bases.

But, it actually was a FLUKE!

But, it actually was a **FLUKE!**

Gröbner bases are not designed to make solving polynomial equations easier.

But, it actually was a **FLUKE!**

Gröbner bases are not designed to make solving polynomial equations easier.

In fact, the Gröbner basis of an ideal of $I = \langle f_1, \dots, f_k \rangle \subseteq \mathbb{C}[x_1, \dots, x_n]$ is not necessarily “simpler” than the original given generating set (i.e. the system of equations) $\{f_1, \dots, f_k\}$.

Purpose of Gröbner Bases ???

Gröbner bases are about

Purpose of Gröbner Bases ???

Gröbner bases are about ...

well, it will take a few slides ...

Representing elements of $\mathbb{C}[x]/I$

Representing elements of $\mathbb{C}[x]/I$

Consider $\mathbb{C}[x]$ and an ideal $I = \langle g(x) \rangle \subseteq \mathbb{C}[x]$, with $0 \neq g(x) \in \mathbb{C}[x]$.

Representing elements of $\mathbb{C}[x]/I$

Consider $\mathbb{C}[x]$ and an ideal $I = \langle g(x) \rangle \subseteq \mathbb{C}[x]$, with $0 \neq g(x) \in \mathbb{C}[x]$. Let $\mathbb{C}[x_1, \dots, x_n]/I$ be the quotient ring.

Representing elements of $\mathbb{C}[x]/I$

Consider $\mathbb{C}[x]$ and an ideal $I = \langle g(x) \rangle \subseteq \mathbb{C}[x]$, with $0 \neq g(x) \in \mathbb{C}[x]$. Let $\mathbb{C}[x_1, \dots, x_n]/I$ be the quotient ring.

Every $f(x) \in \mathbb{C}[x]$ determines an element in $\mathbb{C}[x]/I$.

Representing elements of $\mathbb{C}[x]/I$

Consider $\mathbb{C}[x]$ and an ideal $I = \langle g(x) \rangle \subseteq \mathbb{C}[x]$, with $0 \neq g(x) \in \mathbb{C}[x]$. Let $\mathbb{C}[x_1, \dots, x_n]/I$ be the quotient ring.

Every $f(x) \in \mathbb{C}[x]$ determines an element in $\mathbb{C}[x]/I$.

The map $f(x) \mapsto f(x) + I$ is far from one-to-one.

Representing elements of $\mathbb{C}[x]/I$

Consider $\mathbb{C}[x]$ and an ideal $I = \langle g(x) \rangle \subseteq \mathbb{C}[x]$, with $0 \neq g(x) \in \mathbb{C}[x]$. Let $\mathbb{C}[x_1, \dots, x_n]/I$ be the quotient ring.

Every $f(x) \in \mathbb{C}[x]$ determines an element in $\mathbb{C}[x]/I$.

The map $f(x) \mapsto f(x) + I$ is far from one-to-one. Every other element $f(x) + g(x)h(x) \in f(x) + I$ also represents $f(x) + I$.

Representing elements of $\mathbb{C}[x]/I$

Consider $\mathbb{C}[x]$ and an ideal $I = \langle g(x) \rangle \subseteq \mathbb{C}[x]$, with $0 \neq g(x) \in \mathbb{C}[x]$. Let $\mathbb{C}[x_1, \dots, x_n]/I$ be the quotient ring.

Every $f(x) \in \mathbb{C}[x]$ determines an element in $\mathbb{C}[x]/I$.

The map $f(x) \mapsto f(x) + I$ is far from one-to-one. Every other element $f(x) + g(x)h(x) \in f(x) + I$ also represents $f(x) + I$.

However, every such equivalence class $f(x) + I$ has a **distinguished** representative!

Representing elements of $\mathbb{C}[x]/I$

Consider $\mathbb{C}[x]$ and an ideal $I = \langle g(x) \rangle \subseteq \mathbb{C}[x]$, with $0 \neq g(x) \in \mathbb{C}[x]$. Let $\mathbb{C}[x_1, \dots, x_n]/I$ be the quotient ring.

Every $f(x) \in \mathbb{C}[x]$ determines an element in $\mathbb{C}[x]/I$.

The map $f(x) \mapsto f(x) + I$ is far from one-to-one. Every other element $f(x) + g(x)h(x) \in f(x) + I$ also represents $f(x) + I$.

However, every such equivalence class $f(x) + I$ has a **distinguished** representative!

Recall: Division Algorithm.

The (Univariate) Division Algorithm

(a.k.a. Long Division)

The (Univariate) Division Algorithm

(a.k.a. Long Division)

Given $f(x), g(x) \in \mathbb{C}[x]$, with $g(x) \neq 0$, there exist **unique** $q(x), r(x) \in \mathbb{C}[x]$ such that

The (Univariate) Division Algorithm

(a.k.a. Long Division)

Given $f(x), g(x) \in \mathbb{C}[x]$, with $g(x) \neq 0$, there exist **unique** $q(x), r(x) \in \mathbb{C}[x]$ such that

$$f(x) = g(x) q(x) + r(x),$$

satisfying:

The (Univariate) Division Algorithm

(a.k.a. Long Division)

Given $f(x), g(x) \in \mathbb{C}[x]$, with $g(x) \neq 0$, there exist **unique** $q(x), r(x) \in \mathbb{C}[x]$ such that

$$f(x) = g(x) q(x) + r(x),$$

satisfying: either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

The (Univariate) Division Algorithm

(a.k.a. Long Division)

Given $f(x), g(x) \in \mathbb{C}[x]$, with $g(x) \neq 0$, there exist **unique** $q(x), r(x) \in \mathbb{C}[x]$ such that

$$f(x) = g(x)q(x) + r(x),$$

satisfying: either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

$f(x)$ is called the dividend. $g(x)$ the divisor. $q(x)$ the quotient. $r(x)$ the remainder.

The (Univariate) Division Algorithm

(a.k.a. Long Division)

Given $f(x), g(x) \in \mathbb{C}[x]$, with $g(x) \neq 0$, there exist **unique** $q(x), r(x) \in \mathbb{C}[x]$ such that

$$f(x) = g(x) q(x) + r(x),$$

satisfying: either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

$f(x)$ is called the dividend. $g(x)$ the divisor. $q(x)$ the quotient. $r(x)$ the remainder.

Since $f(x) - r(x) = g(x) q(x) \in I = \langle g(x) \rangle$,
 $r(x) \in f(x) + I \subseteq \mathbb{C}[x]/I$.

The (Univariate) Division Algorithm

(a.k.a. Long Division)

Given $f(x), g(x) \in \mathbb{C}[x]$, with $g(x) \neq 0$, there exist **unique** $q(x), r(x) \in \mathbb{C}[x]$ such that

$$f(x) = g(x)q(x) + r(x),$$

satisfying: either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

$f(x)$ is called the dividend. $g(x)$ the divisor. $q(x)$ the quotient. $r(x)$ the remainder.

Since $f(x) - r(x) = g(x)q(x) \in I = \langle g(x) \rangle$,
 $r(x) \in f(x) + I \subseteq \mathbb{C}[x]/I$.

$r(x)$ is the distinguished representative of $f(x) + I$.

What about $\mathbb{C}[x_1, \dots, x_n]$?

What about $\mathbb{C}[x_1, \dots, x_n]$?

Let $I \subset \mathbb{C}[x_1, \dots, x_n]$ be an ideal.

What about $\mathbb{C}[x_1, \dots, x_n]$?

Let $I \subset \mathbb{C}[x_1, \dots, x_n]$ be an ideal.

Let $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ and $f(x_1, \dots, x_n) + I$ denote the equivalence class in $\mathbb{C}[x_1, \dots, x_n]/I$ that contains f .

QUESTION: Does $f(x_1, \dots, x_n) + I$ have a “distinguished” representative?

Recall how we got the distinguished representative of $f(x) + I \in \mathbb{C}[x]$:

What about $\mathbb{C}[x_1, \dots, x_n]$?

Let $I \subset \mathbb{C}[x_1, \dots, x_n]$ be an ideal.

Let $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ and $f(x_1, \dots, x_n) + I$ denote the equivalence class in $\mathbb{C}[x_1, \dots, x_n]/I$ that contains f .

QUESTION: Does $f(x_1, \dots, x_n) + I$ have a “distinguished” representative?

Recall how we got the distinguished representative of $f(x) + I \in \mathbb{C}[x]$:

the (Univariate) Division Algorithm

What about $\mathbb{C}[x_1, \dots, x_n]$?

Let $I \subset \mathbb{C}[x_1, \dots, x_n]$ be an ideal.

Let $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ and $f(x_1, \dots, x_n) + I$ denote the equivalence class in $\mathbb{C}[x_1, \dots, x_n]/I$ that contains f .

QUESTION: Does $f(x_1, \dots, x_n) + I$ have a “distinguished” representative?

Recall how we got the distinguished representative of $f(x) + I \in \mathbb{C}[x]$:

the (Univariate) Division Algorithm

Can we mimic this for $\mathbb{C}[x_1, \dots, x_n]$?

Example The (Univariate) Division Algorithm in Action

$$\begin{array}{r|l} & x^3 + 1 \\ \hline x^2 + 1 & \\ \hline \end{array}$$

Example The (Univariate) Division Algorithm in Action

	x
$x^2 + 1$	$x^3 + 1$

Example The (Univariate) Division Algorithm in Action

	x
$x^2 + 1$	$x^3 + 1$
	$x^3 + x$

Example The (Univariate) Division Algorithm in Action

	x
$x^2 + 1$	$x^3 + 1$
	$x^3 + x$
	$-x + 1$

Example The (Univariate) Division Algorithm in Action

	x
$x^2 + 1$	$x^3 + 1$
	$x^3 + x$
	$-x + 1$

Thus,

$$x^3 + 1 = x(x^2 + 1) + (-x + 1).$$

Example Multivariate Division Algorithm (MDA)

$y^2 - 1$						remainder
$xy - 1$						
	x^2y	+	xy^2	+	y^2	

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$

$y^2 - 1$					remainder
$xy - 1$					
	x^2y	+	xy^2	+	y^2

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x ,

$y^2 - 1$					remainder
$xy - 1$					
	x^2y	+	xy^2	+	y^2

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)

$y^2 - 1$					remainder
$xy - 1$					
	x^2y	+	xy^2	+	y^2

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$					remainder
$xy - 1$					
	x^2y	+	xy^2	+	y^2

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$					remainder
$xy - 1$	x				
	x^2y	+	xy^2	+	y^2

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$					remainder
$xy - 1$	x				
	x^2y	+	xy^2	+	y^2
	x^2y	-	x		

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$		remainder
$xy - 1$	x	
	$x^2y + xy^2 + y^2$	
	$x^2y - x$	
	$xy^2 + x + y^2$	

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$	x					remainder	
$xy - 1$	x						
	x^2y	+	xy^2	+	y^2		
	x^2y	-	x				
			xy^2	+	x	+	y^2

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$	x				remainder
$xy - 1$	x				
	x^2y	+	xy^2	+	y^2
	x^2y	-	x		
			xy^2	+	x
			xy^2	-	x

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$	x					remainder	
$xy - 1$	x						
	x^2y	+	xy^2	+	y^2		
	x^2y	-	x				
			xy^2	+	x	+	y^2
			xy^2	-	x		
					$2x$	+	y^2

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$	x					remainder	
$xy - 1$	x						
	x^2y	+	xy^2	+	y^2		
	x^2y	-	x				
			xy^2	+	x	+	y^2
			xy^2	-	x		
					y^2		$2x$

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$	x	$+$	1		remainder		
$xy - 1$	x						
	x^2y	$+$	xy^2	$+$	y^2		
	x^2y	$-$	x				
			xy^2	$+$	x	$+$	y^2
			xy^2	$-$	x		
					y^2		$2x$

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$	x	$+$	1		remainder			
$xy - 1$	x							
	x^2y	$+$	xy^2	$+$	y^2			
	x^2y	$-$	x					
			xy^2	$+$	x	$+$	y^2	
			xy^2	$-$	x			
						y^2		$2x$
						y^2	$-$	1

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$	x	$+$	1		remainder		
$xy - 1$	x						
	x^2y	$+$	xy^2	$+$	y^2		
	x^2y	$-$	x				
			xy^2	$+$	x	$+$	y^2
			xy^2	$-$	x		
					y^2		$2x$
					y^2	$-$	1
							1

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$	x	$+$	1		remainder			
$xy - 1$	x							
	x^2y	$+$	xy^2	$+$	y^2			
	x^2y	$-$	x					
			xy^2	$+$	x	$+$	y^2	
			xy^2	$-$	x			
						y^2	$2x$	
						y^2	$-$	1
							$2x + 1$	

Example Multivariate Division Algorithm (MDA)

- Monomial ordering: Lexicographic ordering $y \prec x$
(i.e. first ascending degrees in x , then ascending degrees in y .)
- Ordering of divisors: $xy - 1 \prec y^2 - 1$

$y^2 - 1$	$x + 1$	remainder
$xy - 1$	x	
	$x^2y + xy^2 + y^2$	
	$x^2y - x$	
	$xy^2 + x + y^2$	
	$xy^2 - x$	
	y^2	$2x$
	$y^2 - 1$	
		$2x + 1$

So, $x^2y + xy^2 + y^2 = (x + 1)(y^2 - 1) + (x)(xy - 1) + (2x + 1)$.

The Multivariate Division Algorithm

The Multivariate Division Algorithm

INPUT:

The Multivariate Division Algorithm

INPUT:

Dividend: $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

The Multivariate Division Algorithm

INPUT:

Dividend: $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Divisors: $h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

The Multivariate Division Algorithm

INPUT:

Dividend: $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Divisors: $h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Ordering of h_1, \dots, h_k

The Multivariate Division Algorithm

INPUT:

Dividend: $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Divisors: $h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Ordering of h_1, \dots, h_k

A monomial ordering \mathcal{O}

The Multivariate Division Algorithm

INPUT:

Dividend: $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Divisors: $h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Ordering of h_1, \dots, h_k

A monomial ordering \mathcal{O}

OUTPUT:

The Multivariate Division Algorithm

INPUT:

Dividend: $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Divisors: $h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Ordering of h_1, \dots, h_k

A monomial ordering \mathcal{O}

OUTPUT:

Quotients: $q_1(x_1, \dots, x_n), \dots, q_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

The Multivariate Division Algorithm

INPUT:

Dividend: $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Divisors: $h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Ordering of h_1, \dots, h_k

A monomial ordering \mathcal{O}

OUTPUT:

Quotients: $q_1(x_1, \dots, x_n), \dots, q_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Remainder: $r(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ such that

The Multivariate Division Algorithm

INPUT:

Dividend: $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Divisors: $h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Ordering of h_1, \dots, h_k

A monomial ordering \mathcal{O}

OUTPUT:

Quotients: $q_1(x_1, \dots, x_n), \dots, q_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Remainder: $r(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ such that

$$f = \sum_{i=1}^k q_i h_i + r \text{ and}$$

The Multivariate Division Algorithm

INPUT:

Dividend: $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Divisors: $h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Ordering of h_1, \dots, h_k

A monomial ordering \mathcal{O}

OUTPUT:

Quotients: $q_1(x_1, \dots, x_n), \dots, q_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Remainder: $r(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ such that

$f = \sum_{i=1}^k q_i h_i + r$ and the \mathcal{O} -leading term of r is not divisible by the \mathcal{O} -leading term of any of the h_i .

The Multivariate Division Algorithm

INPUT:

Dividend: $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Divisors: $h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Ordering of h_1, \dots, h_k

A monomial ordering \mathcal{O}

OUTPUT:

Quotients: $q_1(x_1, \dots, x_n), \dots, q_k(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Remainder: $r(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ such that

$f = \sum_{i=1}^k q_i h_i + r$ and the \mathcal{O} -leading term of r is not divisible by the \mathcal{O} -leading term of any of the h_i .

Is r unique?

Back to our Earlier Question ...

Let $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ and $I = \langle h_1, \dots, h_k \rangle$.

QUESTION: Does $f(x_1, \dots, x_n) + I$ have a “distinguished” representative?

Back to our Earlier Question ...

Let $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ and $I = \langle h_1, \dots, h_k \rangle$.

QUESTION: Does $f(x_1, \dots, x_n) + I$ have a “distinguished” representative?

We can now use the Multivariate Division Algorithm to “divide” f

Back to our Earlier Question ...

Let $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ and $I = \langle h_1, \dots, h_k \rangle$.

QUESTION: Does $f(x_1, \dots, x_n) + I$ have a “distinguished” representative?

We can now use the Multivariate Division Algorithm to “divide” f by h_1, \dots, h_k

Back to our Earlier Question ...

Let $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ and $I = \langle h_1, \dots, h_k \rangle$.

QUESTION: Does $f(x_1, \dots, x_n) + I$ have a “distinguished” representative?

We can now use the Multivariate Division Algorithm to “divide” f by h_1, \dots, h_k to get a remainder r :

$$f - r = \sum_{i=1}^k q_i h_i \in I = \langle h_1, \dots, h_k \rangle.$$

Back to our Earlier Question ...

Let $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ and $I = \langle h_1, \dots, h_k \rangle$.

QUESTION: Does $f(x_1, \dots, x_n) + I$ have a “distinguished” representative?

We can now use the Multivariate Division Algorithm to “divide” f by h_1, \dots, h_k to get a remainder r :

$$f - r = \sum_{i=1}^k q_i h_i \in I = \langle h_1, \dots, h_k \rangle.$$

Is r “distinguished”?

No! — A Tragic Example

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$,

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$, we obtain:

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$, we obtain:

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Tragedy 1:

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$, we obtain:

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Tragedy 1: The remainder depends on the divisor ordering

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$, we obtain:

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Tragedy 1: The remainder depends on the divisor ordering (i.e. choice of generators for $\langle h_1, h_2 \rangle$),

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$, we obtain:

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Tragedy 1: The remainder depends on the divisor ordering (i.e. choice of generators for $\langle h_1, h_2 \rangle$, and even worse

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$, we obtain:

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Tragedy 1: The remainder depends on the divisor ordering (i.e. choice of generators for $\langle h_1, h_2 \rangle$, and even worse an ordering of them).

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$, we obtain:

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Tragedy 1: The remainder depends on the divisor ordering (i.e. choice of generators for $\langle h_1, h_2 \rangle$, and even worse an ordering of them). Hence it is NOT a distinguished element of $[xy^2 - x] \in \mathbb{C}[x, y]/\langle h_1, h_2 \rangle!$

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$, we obtain:

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Tragedy 1: The remainder depends on the divisor ordering (i.e. choice of generators for $\langle h_1, h_2 \rangle$, and even worse an ordering of them). Hence it is NOT a distinguished element of $[xy^2 - x] \in \mathbb{C}[x, y]/\langle h_1, h_2 \rangle!$

Tragedy 2:

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$, we obtain:

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Tragedy 1: The remainder depends on the divisor ordering (i.e. choice of generators for $\langle h_1, h_2 \rangle$, and even worse an ordering of them). Hence it is NOT a distinguished element of $[xy^2 - x] \in \mathbb{C}[x, y]/\langle h_1, h_2 \rangle$!

Tragedy 2: $xy^2 - x = x \cdot (y^2 - 1) \in I = \langle xy + 1, y^2 - 1 \rangle$, but

No! — A Tragic Example

Let $f(x, y) = xy^2 - x$, $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_1 > h_2$, we obtain:

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Using the Multivariate Division Algorithm, with monomial ordering $y \prec x$ and divisor ordering $h_2 > h_1$, we obtain:

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Tragedy 1: The remainder depends on the divisor ordering (i.e. choice of generators for $\langle h_1, h_2 \rangle$, and even worse an ordering of them). Hence it is NOT a distinguished element of $[xy^2 - x] \in \mathbb{C}[x, y]/\langle h_1, h_2 \rangle!$

Tragedy 2: $xy^2 - x = x \cdot (y^2 - 1) \in I = \langle xy + 1, y^2 - 1 \rangle$, but the first remainder is NOT even zero!

Pathology Report

Let $G := \{g_1, \dots, g_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$.

Pathology Report

Let $G := \{g_1, \dots, g_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$. Fix a monomial ordering.

Pathology Report

Let $G := \{g_1, \dots, g_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$. Fix a monomial ordering.

Given $f \in \mathbb{C}[x_1, \dots, x_n]$, let $\text{rem}(f, (g_1, \dots, g_k))$ be the remainder produced by the Multivariate Division Algorithm with the indicated order of the g_i 's.

Pathology Report

Let $G := \{g_1, \dots, g_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$. Fix a monomial ordering.

Given $f \in \mathbb{C}[x_1, \dots, x_n]$, let $\text{rem}(f, (g_1, \dots, g_k))$ be the remainder produced by the Multivariate Division Algorithm with the indicated order of the g_i 's.

• $f \in \langle g_1, \dots, g_k \rangle$ does **not** necessarily imply $\text{rem}(f, (g_1, \dots, g_k)) = 0$

Pathology Report

Let $G := \{g_1, \dots, g_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$. Fix a monomial ordering.

Given $f \in \mathbb{C}[x_1, \dots, x_n]$, let $\text{rem}(f, (g_1, \dots, g_k))$ be the remainder produced by the Multivariate Division Algorithm with the indicated order of the g_i 's.

- $f \in \langle g_1, \dots, g_k \rangle$ does **not** necessarily imply $\text{rem}(f, (g_1, \dots, g_k)) = 0$ (however, the converse is obviously true.)

Pathology Report

Let $G := \{g_1, \dots, g_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$. Fix a monomial ordering.

Given $f \in \mathbb{C}[x_1, \dots, x_n]$, let $\text{rem}(f, (g_1, \dots, g_k))$ be the remainder produced by the Multivariate Division Algorithm with the indicated order of the g_i 's.

- $f \in \langle g_1, \dots, g_k \rangle$ does **not** necessarily imply $\text{rem}(f, (g_1, \dots, g_k)) = 0$ (however, the converse is obviously true.)
- $\langle g_1, \dots, g_k \rangle = I = \langle h_1, \dots, h_r \rangle$ does **not** imply $\text{rem}(f, (g_1, \dots, g_k)) = \text{rem}(f, (h_1, \dots, h_r))$,

Pathology Report

Let $G := \{g_1, \dots, g_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$. Fix a monomial ordering.

Given $f \in \mathbb{C}[x_1, \dots, x_n]$, let $\text{rem}(f, (g_1, \dots, g_k))$ be the remainder produced by the Multivariate Division Algorithm with the indicated order of the g_i 's.

- $f \in \langle g_1, \dots, g_k \rangle$ does **not** necessarily imply $\text{rem}(f, (g_1, \dots, g_k)) = 0$ (however, the converse is obviously true.)
- $\langle g_1, \dots, g_k \rangle = I = \langle h_1, \dots, h_r \rangle$ does **not** imply $\text{rem}(f, (g_1, \dots, g_k)) = \text{rem}(f, (h_1, \dots, h_r))$, i.e. the representative of $f + I$ produced by the Multivariate Division Algorithm is non-unique if arbitrary generating sets of I are allowed as divisors in the Algorithm.

Pathology Report

Let $G := \{g_1, \dots, g_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$. Fix a monomial ordering.

Given $f \in \mathbb{C}[x_1, \dots, x_n]$, let $\text{rem}(f, (g_1, \dots, g_k))$ be the remainder produced by the Multivariate Division Algorithm with the indicated order of the g_i 's.

- $f \in \langle g_1, \dots, g_k \rangle$ does **not** necessarily imply $\text{rem}(f, (g_1, \dots, g_k)) = 0$ (however, the converse is obviously true.)
- $\langle g_1, \dots, g_k \rangle = I = \langle h_1, \dots, h_r \rangle$ does **not** imply $\text{rem}(f, (g_1, \dots, g_k)) = \text{rem}(f, (h_1, \dots, h_r))$, i.e. the representative of $f + I$ produced by the Multivariate Division Algorithm is non-unique if arbitrary generating sets of I are allowed as divisors in the Algorithm.
- $\text{rem}(f, (g_1, \dots, g_k))$ depends even on the ordering of the g_i 's.

Pathology Report

Let $G := \{g_1, \dots, g_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$. Fix a monomial ordering.

Given $f \in \mathbb{C}[x_1, \dots, x_n]$, let $\text{rem}(f, (g_1, \dots, g_k))$ be the remainder produced by the Multivariate Division Algorithm with the indicated order of the g_i 's.

- $f \in \langle g_1, \dots, g_k \rangle$ does **not** necessarily imply $\text{rem}(f, (g_1, \dots, g_k)) = 0$ (however, the converse is obviously true.)
- $\langle g_1, \dots, g_k \rangle = I = \langle h_1, \dots, h_r \rangle$ does **not** imply $\text{rem}(f, (g_1, \dots, g_k)) = \text{rem}(f, (h_1, \dots, h_r))$, i.e. the representative of $f + I$ produced by the Multivariate Division Algorithm is non-unique if arbitrary generating sets of I are allowed as divisors in the Algorithm.
- $\text{rem}(f, (g_1, \dots, g_k))$ depends even on the ordering of the g_i 's.

None of these occurs in the univariate case!

Pathology Report

Let $G := \{g_1, \dots, g_k\} \subseteq \mathbb{C}[x_1, \dots, x_n]$. Fix a monomial ordering.

Given $f \in \mathbb{C}[x_1, \dots, x_n]$, let $\text{rem}(f, (g_1, \dots, g_k))$ be the remainder produced by the Multivariate Division Algorithm with the indicated order of the g_i 's.

- $f \in \langle g_1, \dots, g_k \rangle$ does **not** necessarily imply $\text{rem}(f, (g_1, \dots, g_k)) = 0$ (however, the converse is obviously true.)
- $\langle g_1, \dots, g_k \rangle = I = \langle h_1, \dots, h_r \rangle$ does **not** imply $\text{rem}(f, (g_1, \dots, g_k)) = \text{rem}(f, (h_1, \dots, h_r))$, i.e. the representative of $f + I$ produced by the Multivariate Division Algorithm is non-unique if arbitrary generating sets of I are allowed as divisors in the Algorithm.
- $\text{rem}(f, (g_1, \dots, g_k))$ depends even on the ordering of the g_i 's.

None of these occurs in the univariate case!

Gröbner bases can be used to overcome these pathologies.

Definition of Gröbner Bases

Definition of Gröbner Bases

A Gröbner basis of an ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$ (w.r.t. a chosen monomial ordering) is a finite subset $G = \{g_1, \dots, g_k\}$ of I such that

$$\langle \text{Im}(g_1), \dots, \text{Im}(g_k) \rangle = \text{Lm}(I).$$

Definition of Gröbner Bases

A Gröbner basis of an ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$ (w.r.t. a chosen monomial ordering) is a finite subset $G = \{g_1, \dots, g_k\}$ of I such that

$$\langle \text{Im}(g_1), \dots, \text{Im}(g_k) \rangle = \text{Lm}(I).$$

For $f \in \mathbb{C}[x_1, \dots, x_n]$,

$\text{Im}(f) \quad := \quad$ leading monomial of f (w.r.t. chosen monomial ordering)

$\text{Lm}(I) \quad := \quad \langle \{ \text{Im}(f) \mid f \in I \} \rangle$, leading monomial ideal of I .

Definition of Gröbner Bases

A Gröbner basis of an ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$ (w.r.t. a chosen monomial ordering) is a finite subset $G = \{g_1, \dots, g_k\}$ of I such that

$$\langle \text{Im}(g_1), \dots, \text{Im}(g_k) \rangle = \text{Lm}(I).$$

For $f \in \mathbb{C}[x_1, \dots, x_n]$,

$\text{Im}(f) \quad := \quad$ leading monomial of f (w.r.t. chosen monomial ordering)

$\text{Lm}(I) \quad := \quad \langle \{ \text{Im}(f) \mid f \in I \} \rangle$, leading monomial ideal of I .

Suppose $I = \langle g_1, \dots, g_k \rangle$.

Definition of Gröbner Bases

A Gröbner basis of an ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$ (w.r.t. a chosen monomial ordering) is a finite subset $G = \{g_1, \dots, g_k\}$ of I such that

$$\langle \text{Im}(g_1), \dots, \text{Im}(g_k) \rangle = \text{Lm}(I).$$

For $f \in \mathbb{C}[x_1, \dots, x_n]$,

$\text{Im}(f) \quad := \quad$ leading monomial of f (w.r.t. chosen monomial ordering)

$\text{Lm}(I) \quad := \quad \langle \{ \text{Im}(f) \mid f \in I \} \rangle$, leading monomial ideal of I .

Suppose $I = \langle g_1, \dots, g_k \rangle$. Then $\text{Im}(g_i) \in \text{Lm}(I)$, for each $i = 1, \dots, k$.

Definition of Gröbner Bases

A Gröbner basis of an ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$ (w.r.t. a chosen monomial ordering) is a finite subset $G = \{g_1, \dots, g_k\}$ of I such that

$$\langle \text{Im}(g_1), \dots, \text{Im}(g_k) \rangle = \text{Lm}(I).$$

For $f \in \mathbb{C}[x_1, \dots, x_n]$,

$\text{Im}(f) \quad := \quad$ leading monomial of f (w.r.t. chosen monomial ordering)

$\text{Lm}(I) \quad := \quad \langle \{ \text{Im}(f) \mid f \in I \} \rangle$, leading monomial ideal of I .

Suppose $I = \langle g_1, \dots, g_k \rangle$. Then $\text{Im}(g_i) \in \text{Lm}(I)$, for each $i = 1, \dots, k$.

Hence, **in general**, we have

$$\langle \text{Im}(g_1), \dots, \text{Im}(g_k) \rangle \subseteq \text{Lm}(I).$$

Definition of Gröbner Bases

A Gröbner basis of an ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$ (w.r.t. a chosen monomial ordering) is a finite subset $G = \{g_1, \dots, g_k\}$ of I such that

$$\langle \text{Im}(g_1), \dots, \text{Im}(g_k) \rangle = \text{Lm}(I).$$

For $f \in \mathbb{C}[x_1, \dots, x_n]$,

$\text{Im}(f) \quad := \quad$ leading monomial of f (w.r.t. chosen monomial ordering)

$\text{Lm}(I) \quad := \quad \langle \{ \text{Im}(f) \mid f \in I \} \rangle$, leading monomial ideal of I .

Suppose $I = \langle g_1, \dots, g_k \rangle$. Then $\text{Im}(g_i) \in \text{Lm}(I)$, for each $i = 1, \dots, m$.

Hence, **in general**, we have

$$\langle \text{Im}(g_1), \dots, \text{Im}(g_k) \rangle \subseteq \text{Lm}(I).$$

That $G = \{g_1, \dots, g_k\}$ is a Gröbner basis precisely says that the inclusion above is in fact an equality.

Misc. Facts about Gröbner Bases

Misc. Facts about Gröbner Bases

Clearly, $\langle G \rangle = \langle \{g_1, \dots, g_k\} \rangle \subset I$, for every Gröbner basis $G \subset I$.

Misc. Facts about Gröbner Bases

Clearly, $\langle G \rangle = \langle \{g_1, \dots, g_k\} \rangle \subset I$, for every Gröbner basis $G \subset I$.

Gröbner bases are indeed “bases” (generating sets),

Misc. Facts about Gröbner Bases

Clearly, $\langle G \rangle = \langle \{g_1, \dots, g_k\} \rangle \subset I$, for every Gröbner basis $G \subset I$.

Gröbner bases are indeed “bases” (generating sets), i.e. if $G = \{g_1, \dots, g_k\}$ is a Gröbner basis of $I \subseteq \mathbb{C}[x_1, \dots, x_n]$,

Misc. Facts about Gröbner Bases

Clearly, $\langle G \rangle = \langle \{g_1, \dots, g_k\} \rangle \subset I$, for every Gröbner basis $G \subset I$.

Gröbner bases are indeed “bases” (generating sets), i.e. if $G = \{g_1, \dots, g_k\}$ is a Gröbner basis of $I \subseteq \mathbb{C}[x_1, \dots, x_n]$, then $I = \langle g_1, \dots, g_k \rangle$.

Misc. Facts about Gröbner Bases

Clearly, $\langle G \rangle = \langle \{g_1, \dots, g_k\} \rangle \subset I$, for every Gröbner basis $G \subset I$.

Gröbner bases are indeed “bases” (generating sets), i.e. if $G = \{g_1, \dots, g_k\}$ is a Gröbner basis of $I \subseteq \mathbb{C}[x_1, \dots, x_n]$, then $I = \langle g_1, \dots, g_k \rangle$.

Hilbert’s Basis Theorem (applied to $\text{Lm}(I)$) \implies Every ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$ admits Gröbner bases.

Example: A “Non-Gröbner” Basis

Recall from Tragic Example: we were dividing

$f(x, y) = xy^2 - x$ by $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

Example: A “Non-Gröbner” Basis

Recall from Tragic Example: we were dividing

$f(x, y) = xy^2 - x$ by $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

So the ideal we are looking at is $I = \langle xy + 1, y^2 - 1 \rangle$, and $\{xy + 1, y^2 - 1\}$ is a generating set for $I \subseteq \mathbb{C}[x, y]$.

Example: A “Non-Gröbner” Basis

Recall from Tragic Example: we were dividing

$f(x, y) = xy^2 - x$ by $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

So the ideal we are looking at is $I = \langle xy + 1, y^2 - 1 \rangle$, and $\{xy + 1, y^2 - 1\}$ is a generating set for $I \subseteq \mathbb{C}[x, y]$.

Note that $x + y = y \cdot (xy + 1) - x \cdot (y^2 - 1)$

Example: A “Non-Gröbner” Basis

Recall from Tragic Example: we were dividing

$f(x, y) = xy^2 - x$ by $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

So the ideal we are looking at is $I = \langle xy + 1, y^2 - 1 \rangle$, and $\{xy + 1, y^2 - 1\}$ is a generating set for $I \subseteq \mathbb{C}[x, y]$.

Note that $x + y = y \cdot (xy + 1) - x \cdot (y^2 - 1) \in I$.

Example: A “Non-Gröbner” Basis

Recall from Tragic Example: we were dividing

$f(x, y) = xy^2 - x$ by $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

So the ideal we are looking at is $I = \langle xy + 1, y^2 - 1 \rangle$, and $\{xy + 1, y^2 - 1\}$ is a generating set for $I \subseteq \mathbb{C}[x, y]$.

Note that $x + y = y \cdot (xy + 1) - x \cdot (y^2 - 1) \in I$.

And, $\text{Im}(x + y) = x$

Example: A “Non-Gröbner” Basis

Recall from Tragic Example: we were dividing

$f(x, y) = xy^2 - x$ by $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

So the ideal we are looking at is $I = \langle xy + 1, y^2 - 1 \rangle$, and $\{xy + 1, y^2 - 1\}$ is a generating set for $I \subseteq \mathbb{C}[x, y]$.

Note that $x + y = y \cdot (xy + 1) - x \cdot (y^2 - 1) \in I$.

And, $\text{Im}(x + y) = x \notin \langle xy, y^2 \rangle$

Example: A “Non-Gröbner” Basis

Recall from Tragic Example: we were dividing

$f(x, y) = xy^2 - x$ by $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

So the ideal we are looking at is $I = \langle xy + 1, y^2 - 1 \rangle$, and $\{xy + 1, y^2 - 1\}$ is a generating set for $I \subseteq \mathbb{C}[x, y]$.

Note that $x + y = y \cdot (xy + 1) - x \cdot (y^2 - 1) \in I$.

And, $\text{Im}(x + y) = x \notin \langle xy, y^2 \rangle = \langle \text{Im}(xy + 1), \text{Im}(y^2 - 1) \rangle$.

Example: A “Non-Gröbner” Basis

Recall from Tragic Example: we were dividing

$f(x, y) = xy^2 - x$ by $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

So the ideal we are looking at is $I = \langle xy + 1, y^2 - 1 \rangle$, and $\{xy + 1, y^2 - 1\}$ is a generating set for $I \subseteq \mathbb{C}[x, y]$.

Note that $x + y = y \cdot (xy + 1) - x \cdot (y^2 - 1) \in I$.

And, $\text{Im}(x + y) = x \notin \langle xy, y^2 \rangle = \langle \text{Im}(xy + 1), \text{Im}(y^2 - 1) \rangle$.

So, we have shown:

$$\langle \text{Im}(xy + 1), \text{Im}(y^2 - 1) \rangle \subsetneq \text{Lm}(I).$$

Example: A “Non-Gröbner” Basis

Recall from Tragic Example: we were dividing

$f(x, y) = xy^2 - x$ by $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

So the ideal we are looking at is $I = \langle xy + 1, y^2 - 1 \rangle$, and $\{xy + 1, y^2 - 1\}$ is a generating set for $I \subseteq \mathbb{C}[x, y]$.

Note that $x + y = y \cdot (xy + 1) - x \cdot (y^2 - 1) \in I$.

And, $\text{Im}(x + y) = x \notin \langle xy, y^2 \rangle = \langle \text{Im}(xy + 1), \text{Im}(y^2 - 1) \rangle$.

So, we have shown:

$$\langle \text{Im}(xy + 1), \text{Im}(y^2 - 1) \rangle \subsetneq \text{Lm}(I).$$

Hence $\{xy + 1, y^2 - 1\}$ is a generating set

Example: A “Non-Gröbner ” Basis

Recall from Tragic Example: we were dividing

$f(x, y) = xy^2 - x$ by $h_1(x, y) = xy + 1$ and $h_2(x, y) = y^2 - 1$ in $\mathbb{C}[x, y]$.

So the ideal we are looking at is $I = \langle xy + 1, y^2 - 1 \rangle$, and $\{xy + 1, y^2 - 1\}$ is a generating set for $I \subseteq \mathbb{C}[x, y]$.

Note that $x + y = y \cdot (xy + 1) - x \cdot (y^2 - 1) \in I$.

And, $\text{lm}(x + y) = x \notin \langle xy, y^2 \rangle = \langle \text{lm}(xy + 1), \text{lm}(y^2 - 1) \rangle$.

So, we have shown:

$$\langle \text{lm}(xy + 1), \text{lm}(y^2 - 1) \rangle \subsetneq \text{Lm}(I).$$

Hence $\{xy + 1, y^2 - 1\}$ is a generating set but NOT a Gröbner basis for I .

How Gröbner Bases Cure MDA

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Outline of Proof

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Outline of Proof First, note $\text{rem}(f, G) + I = f + I = \text{rem}(f, G') + I$.

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Outline of Proof First, note $\text{rem}(f, G) + I = f + I = \text{rem}(f, G') + I$.
Hence $\text{rem}(f, G) - \text{rem}(f, G') \in I$

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Outline of Proof First, note $\text{rem}(f, G) + I = f + I = \text{rem}(f, G') + I$. Hence $\text{rem}(f, G) - \text{rem}(f, G') \in I \implies \text{lm}(\text{rem}(f, G) - \text{rem}(f, G')) \in \text{Lm}(I)$.

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Outline of Proof First, note $\text{rem}(f, G) + I = f + I = \text{rem}(f, G') + I$. Hence $\text{rem}(f, G) - \text{rem}(f, G') \in I \implies \text{lm}(\text{rem}(f, G) - \text{rem}(f, G')) \in \text{Lm}(I)$.

Key Observation: No monomial in $\text{rem}(f, G)$ or $\text{rem}(f, G')$ belongs to $\text{Lm}(I)$, by the hypothesis that G and G' are Gröbner bases of I .

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Outline of Proof First, note $\text{rem}(f, G) + I = f + I = \text{rem}(f, G') + I$. Hence $\text{rem}(f, G) - \text{rem}(f, G') \in I \implies \text{lm}(\text{rem}(f, G) - \text{rem}(f, G')) \in \text{Lm}(I)$.

Key Observation: No monomial in $\text{rem}(f, G)$ or $\text{rem}(f, G')$ belongs to $\text{Lm}(I)$, by the hypothesis that G and G' are Gröbner bases of I . (Recall how the remainder in the Multivariate Division Algorithm is “assembled.”)

Aside: G Gröbner \Rightarrow Each monomial in $\text{rem}(f, G) \notin \text{Lm}(I)$

$y^2 - 1$	x	$+$	1			remainder		
$xy - 1$	x							
	x^2y	$+$	xy^2	$+$	y^2			
	x^2y	$-$	x					
			xy^2	$+$	x	$+$	y^2	
			xy^2	$-$	x			
					$2x$	$+$	y^2	
							$2x$	
						y^2	$-$	1
							1	$2x + 1$

Aside: G Gröbner \Rightarrow Each monomial in $\text{rem}(f, G) \notin \text{Lm}(I)$

$y^2 - 1$	x	$+$	1		remainder					
$xy - 1$	x									
	x^2y	$+$	xy^2	$+$	y^2					
	x^2y	$-$	x							
			xy^2	$+$	x	$+$	y^2			
			xy^2	$-$	x					
					$2x$	$+$	y^2		$2x$	
							y^2	$-$	1	
									1	$2x + 1$

The monomial x appears in the remainder because it is not divisible by y^2 or xy

Aside: G Gröbner \Rightarrow Each monomial in $\text{rem}(f, G) \notin \text{Lm}(I)$

$y^2 - 1$	x	$+$	1		remainder					
$xy - 1$	x									
	x^2y	$+$	xy^2	$+$	y^2					
	x^2y	$-$	x							
			xy^2	$+$	x	$+$	y^2			
			xy^2	$-$	x					
					$2x$	$+$	y^2		$2x$	
							y^2	$-$	1	
									1	$2x + 1$

The monomial x appears in the remainder because it is not divisible by y^2 or $xy \implies x \notin \langle y^2, xy \rangle \subset \text{Lm}(I)$.

Aside: G Gröbner \Rightarrow Each monomial in $\text{rem}(f, G) \notin \text{Lm}(I)$

$y^2 - 1$	x	$+$	1			remainder		
$xy - 1$	x							
	x^2y	$+$	xy^2	$+$	y^2			
	x^2y	$-$	x					
			xy^2	$+$	x	$+$	y^2	
			xy^2	$-$	x			
					$2x$	$+$	y^2	
							$2x$	
						y^2	$-$	1
							1	$2x + 1$

The monomial x appears in the remainder because it is not divisible by y^2 or $xy \implies x \notin \langle y^2, xy \rangle \subset \text{Lm}(I)$.

If $\{y^2 - 1, xy - 1\}$ **were** a Gröbner basis for $I = \langle y^2 - 1, xy - 1 \rangle$, then we would have $\langle y^2, xy \rangle = \langle \text{lm}(y^2 - 1), \text{lm}(xy - 1) \rangle = \text{Lm}(I)$.

Aside: G Gröbner \Rightarrow Each monomial in $\text{rem}(f, G) \notin \text{Lm}(I)$

$y^2 - 1$	x	$+$	1		remainder					
$xy - 1$	x									
	x^2y	$+$	xy^2	$+$	y^2					
	x^2y	$-$	x							
			xy^2	$+$	x	$+$	y^2			
			xy^2	$-$	x					
					$2x$	$+$	y^2		$2x$	
							y^2	$-$	1	
									1	$2x + 1$

The monomial x appears in the remainder because it is not divisible by y^2 or $xy \implies x \notin \langle y^2, xy \rangle \subset \text{Lm}(I)$.

If $\{y^2 - 1, xy - 1\}$ were a Gröbner basis for $I = \langle y^2 - 1, xy - 1 \rangle$, then we would have $\langle y^2, xy \rangle = \langle \text{lm}(y^2 - 1), \text{lm}(xy - 1) \rangle = \text{Lm}(I)$.

Hence $x \notin \text{Lm}(I)$,

Aside: G Gröbner \Rightarrow Each monomial in $\text{rem}(f, G) \notin \text{Lm}(I)$

$y^2 - 1$	x	$+$	1		remainder					
$xy - 1$	x									
	x^2y	$+$	xy^2	$+$	y^2					
	x^2y	$-$	x							
			xy^2	$+$	x	$+$	y^2			
			xy^2	$-$	x					
					$2x$	$+$	y^2	$2x$		
							y^2	$-$	1	
									1	$2x + 1$

The monomial x appears in the remainder because it is not divisible by y^2 or $xy \implies x \notin \langle y^2, xy \rangle \subset \text{Lm}(I)$.

If $\{y^2 - 1, xy - 1\}$ were a Gröbner basis for $I = \langle y^2 - 1, xy - 1 \rangle$, then we would have $\langle y^2, xy \rangle = \langle \text{lm}(y^2 - 1), \text{lm}(xy - 1) \rangle = \text{Lm}(I)$.

Hence $x \notin \text{Lm}(I)$, if $\{y^2 - 1, xy - 1\}$ were a Gröbner basis for I .

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Proof First, note $\text{rem}(f, G) + I = f + I = \text{rem}(f, G')$. Hence $\text{rem}(f, G) - \text{rem}(f, G') \in I \implies \text{lm}(\text{rem}(f, G) - \text{rem}(f, G')) \in \text{Lm}(I)$.

Key Observation: No monomial in $\text{rem}(f, G)$ or $\text{rem}(f, G')$ belongs to $\text{Lm}(I)$, by the hypothesis that G and G' are Gröbner bases of I . (Recall how the remainder in the Multivariate Division Algorithm is “assembled.”)

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Proof First, note $\text{rem}(f, G) + I = f + I = \text{rem}(f, G')$. Hence $\text{rem}(f, G) - \text{rem}(f, G') \in I \implies \text{lm}(\text{rem}(f, G) - \text{rem}(f, G')) \in \text{Lm}(I)$.

Key Observation: No monomial in $\text{rem}(f, G)$ or $\text{rem}(f, G')$ belongs to $\text{Lm}(I)$, by the hypothesis that G and G' are Gröbner bases of I . (Recall how the remainder in the Multivariate Division Algorithm is “assembled.”)

Now, suppose on the contrary that $\text{rem}(f, G) - \text{rem}(f, G') \neq 0$

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Proof First, note $\text{rem}(f, G) + I = f + I = \text{rem}(f, G')$. Hence $\text{rem}(f, G) - \text{rem}(f, G') \in I \implies \text{lm}(\text{rem}(f, G) - \text{rem}(f, G')) \in \text{Lm}(I)$.

Key Observation: No monomial in $\text{rem}(f, G)$ or $\text{rem}(f, G')$ belongs to $\text{Lm}(I)$, by the hypothesis that G and G' are Gröbner bases of I . (Recall how the remainder in the Multivariate Division Algorithm is “assembled.”)

Now, suppose on the contrary that $\text{rem}(f, G) - \text{rem}(f, G') \neq 0 \implies \text{lm}(\text{rem}(f, G) - \text{rem}(f, G')) \notin \text{Lm}(I)$

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Proof First, note $\text{rem}(f, G) + I = f + I = \text{rem}(f, G')$. Hence $\text{rem}(f, G) - \text{rem}(f, G') \in I \implies \text{lm}(\text{rem}(f, G) - \text{rem}(f, G')) \in \text{Lm}(I)$.

Key Observation: No monomial in $\text{rem}(f, G)$ or $\text{rem}(f, G')$ belongs to $\text{Lm}(I)$, by the hypothesis that G and G' are Gröbner bases of I . (Recall how the remainder in the Multivariate Division Algorithm is “assembled.”)

Now, suppose on the contrary that $\text{rem}(f, G) - \text{rem}(f, G') \neq 0 \implies \text{lm}(\text{rem}(f, G) - \text{rem}(f, G')) \notin \text{Lm}(I)$, contradiction. □

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Corollary

If $G = \{g_1, \dots, g_k\}$ is a Gröbner basis for $I = \langle g_1, \dots, g_k \rangle$, then for any $f \in \mathbb{C}[x_1, \dots, x_n]$,

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Corollary

If $G = \{g_1, \dots, g_k\}$ is a Gröbner basis for $I = \langle g_1, \dots, g_k \rangle$, then for any $f \in \mathbb{C}[x_1, \dots, x_n]$,

1) $f \in I \iff \text{rem}(f, G) = 0.$

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Corollary

If $G = \{g_1, \dots, g_k\}$ is a Gröbner basis for $I = \langle g_1, \dots, g_k \rangle$, then for any $f \in \mathbb{C}[x_1, \dots, x_n]$,

- 1) $f \in I \iff \text{rem}(f, G) = 0$.
- 2) $\text{rem}(f, G)$ no longer depends on the ordering of the g_i 's.

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Corollary

If $G = \{g_1, \dots, g_k\}$ is a Gröbner basis for $I = \langle g_1, \dots, g_k \rangle$, then for any $f \in \mathbb{C}[x_1, \dots, x_n]$,

- 1) $f \in I \iff \text{rem}(f, G) = 0$.
- 2) $\text{rem}(f, G)$ no longer depends on the ordering of the g_i 's.
- 3) The representative $\text{rem}(f, G)$ of $f + I$ is now “unique”

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Corollary

If $G = \{g_1, \dots, g_k\}$ is a Gröbner basis for $I = \langle g_1, \dots, g_k \rangle$, then for any $f \in \mathbb{C}[x_1, \dots, x_n]$,

- 1) $f \in I \iff \text{rem}(f, G) = 0$.
- 2) $\text{rem}(f, G)$ no longer depends on the ordering of the g_i 's.
- 3) The representative $\text{rem}(f, G)$ of $f + I$ is now “unique” as long as we invoke the Multivariate Division Algorithm with a Gröbner basis for I .

How Gröbner Bases Cure MDA

Theorem Let I be an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and let a monomial ordering be fixed. Then for any two Gröbner basis G, G' for I , we have:

$$\text{rem}(f, G) = \text{rem}(f, G'), \quad \text{for any } f \in \mathbb{C}[x_1, \dots, x_n].$$

Corollary

If $G = \{g_1, \dots, g_k\}$ is a Gröbner basis for $I = \langle g_1, \dots, g_k \rangle$, then for any $f \in \mathbb{C}[x_1, \dots, x_n]$,

- 1) $f \in I \iff \text{rem}(f, G) = 0$.
- 2) $\text{rem}(f, G)$ no longer depends on the ordering of the g_i 's.
- 3) The representative $\text{rem}(f, G)$ of $f + I$ is now “unique” as long as we invoke the Multivariate Division Algorithm with a Gröbner basis for I .

All previously mentioned pathologies are fixed!

Big Remaining Question ...

Let an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be given. Fix a monomial ordering.

Big Remaining Question ...

Let an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be given. Fix a monomial ordering.

We already know I possesses Gröbner bases (by applying Hilbert's Basis Theorem to $\text{Lm}(I)$).

Big Remaining Question ...

Let an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be given. Fix a monomial ordering.

We already know I possesses Gröbner bases (by applying Hilbert's Basis Theorem to $\text{Lm}(I)$).

- How to construct Gröbner bases for I ?

Big Remaining Question ...

Let an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be given. Fix a monomial ordering.

We already know I possesses Gröbner bases (by applying Hilbert's Basis Theorem to $\text{Lm}(I)$).

- How to construct Gröbner bases for I ?
- More practically: Suppose $I = \langle h_1, \dots, h_r \rangle$, can we construct Gröbner bases from the h_i 's?

Big Remaining Question ...

Let an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be given. Fix a monomial ordering.

We already know I possesses Gröbner bases (by applying Hilbert's Basis Theorem to $\text{Lm}(I)$).

- How to construct Gröbner bases for I ?
- More practically: Suppose $I = \langle h_1, \dots, h_r \rangle$, can we construct Gröbner bases from the h_i 's? In other words, can we obtain a Gröbner basis for I from a given generating set (basis) of I ?

Big Remaining Question ...

Let an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be given. Fix a monomial ordering.

We already know I possesses Gröbner bases (by applying Hilbert's Basis Theorem to $\text{Lm}(I)$).

- How to construct Gröbner bases for I ?
- More practically: Suppose $I = \langle h_1, \dots, h_r \rangle$, can we construct Gröbner bases from the h_i 's? In other words, can we obtain a Gröbner basis for I from a given generating set (basis) of I ?

Yes. Buchberger's Algorithm

Some Remarks

We will omit the details of Buchberger's algorithm.

Some Remarks

We will omit the details of Buchberger's algorithm.

Buchberger's algorithm is extremely computationally intensive. Modern computer algebra systems are necessary for the theory to be useful in practice.

Some Remarks

We will omit the details of Buchberger's algorithm.

Buchberger's algorithm is extremely computationally intensive. Modern computer algebra systems are necessary for the theory to be useful in practice.

There are modifications (improvements) of Buchberger's algorithm.

Some Remarks

We will omit the details of Buchberger's algorithm.

Buchberger's algorithm is extremely computationally intensive. Modern computer algebra systems are necessary for the theory to be useful in practice.

There are modifications (improvements) of Buchberger's algorithm.

I used a modified version of Buchberger's algorithm as a "simplification" tool. But I lucked in. There is no theoretical reason why a Gröbner basis should be any "simpler" than the generating set used to construct it. Gröbner bases are not by design "simplification" tools; they are designed to fix the defects of the Multivariate Division Algorithm.

Applications of Gröbner Bases

1) Membership of ideals of polynomial rings

Determine whether $f \in \mathbb{C}[x_1, \dots, x_n]$ belongs to an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$.

Applications of Gröbner Bases

1) Membership of ideals of polynomial rings

Determine whether $f \in \mathbb{C}[x_1, \dots, x_n]$ belongs to an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$.

2) Simplification/Solution of Systems of Polynomial Equations

Applications of Gröbner Bases

1) Membership of ideals of polynomial rings

Determine whether $f \in \mathbb{C}[x_1, \dots, x_n]$ belongs to an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$.

2) Simplification/Solution of Systems of Polynomial Equations

3) Implicitization

Suppose that the parametric equations

$$x_1 = f_1(t_1, \dots, t_m) \quad \dots \quad x_n = f_n(t_1, \dots, t_m),$$

*define an **algebraic variety** $V \subseteq \mathbb{C}^n$. Can we express V “implicitly”?*

Applications of Gröbner Bases

1) Membership of ideals of polynomial rings

Determine whether $f \in \mathbb{C}[x_1, \dots, x_n]$ belongs to an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$.

2) Simplification/Solution of Systems of Polynomial Equations

3) Implicitization

Suppose that the parametric equations

$$x_1 = f_1(t_1, \dots, t_m) \quad \dots \quad x_n = f_n(t_1, \dots, t_m),$$

*define an **algebraic variety** $V \subseteq \mathbb{C}^n$. Can we express V “implicitly”? i.e. Can we find polynomial equations in the x_i 's that define V ?*

Applications of Gröbner Bases

1) Membership of ideals of polynomial rings

Determine whether $f \in \mathbb{C}[x_1, \dots, x_n]$ belongs to an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$.

2) Simplification/Solution of Systems of Polynomial Equations

3) Implicitization

Suppose that the parametric equations

$$x_1 = f_1(t_1, \dots, t_m) \quad \dots \quad x_n = f_n(t_1, \dots, t_m),$$

*define an **algebraic variety** $V \subseteq \mathbb{C}^n$. Can we express V “implicitly”? i.e. Can we find polynomial equations in the x_i 's that define V ? Gröbner bases can be used to solve this problem.*

THE END