Lecture 13: Multivariate Polynomial Division Algorithm & Monomial Ideals

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

March 1, 2021

Overview

- Two Familiar Division Algorithms
- Generalization: Multivariate Multipolynomial Division
- Issues with the division algorithm
- Monomial Ideals & Dickson's Lemma
- Conclusion
- Acknowledgements

Division with remainder over $\mathbb{F}[x]$

- **Input:** two elements $a, b \in \mathbb{F}[x]$, with b non-zero
- **Output:** $q, r \in \mathbb{F}[x]$ such that $\deg(r) < \deg(b)$ and $a = q \cdot b + r$

Division with remainder over $\mathbb{F}[x]$

- **Input:** two elements $a, b \in \mathbb{F}[x]$, with b non-zero
- **Output:** $q, r \in \mathbb{F}[x]$ such that $\deg(r) < \deg(b)$ and $a = q \cdot b + r$
- Start with $r = a$, $q = 0$

Division with remainder over $\mathbb{F}[x]$

- **Input:** two elements $a, b \in \mathbb{F}[x]$, with b non-zero
- **Output:** $q, r \in \mathbb{F}[x]$ such that $\deg(r) < \deg(b)$ and $a = q \cdot b + r$
- Start with $r = a$, $q = 0$
- While $\deg(r) \geq \deg(b)$:
  - $q \leftarrow q + \cancel{x^{\deg(r)-\deg(b)}}$ $\quad + \dfrac{LC(r)}{LC(b)} \cdot x^{\deg(r)-\deg(b)}$
  - $\underbrace{r \leftarrow r - x^{\deg(r)-\deg(b)} \cdot \dfrac{LC(r)}{LC(b)} \cdot b}_{\text{reducing degree of remainder}}$

maintain $a = qb + r$

$$LT(r) = LC(r) \cdot x^{\deg(r)}$$

$$\frac{LC(r)}{LC(b)} x^{\deg(r) - \deg(b)} \cdot LC(b) \cdot x^{\deg(b)} = LC(r) \cdot x^{\deg(r)}$$

Division with remainder over $\mathbb{F}[x]$

- **Input:** two elements $a, b \in \mathbb{F}[x]$, with b non-zero
- **Output:** $q, r \in \mathbb{F}[x]$ such that $\deg(r) < \deg(b)$ and $a = q \cdot b + r$
- Start with $r = a$, $q = 0$
- While $\deg(r) \geq \deg(b)$:
  - $q \leftarrow q + x^{\deg(r)-\deg(b)}$
  - $r \leftarrow r - x^{\deg(r)-\deg(b)} \cdot \dfrac{LC(r)}{LC(b)} \cdot b$
- Analysis: we will perform at most $\deg(a) - \deg(b) + 1$ subtractions to r. Total time $(\deg(a) - \deg(b) + 1)(\deg(b) + 1)$.

Example

- $a(x) = x^3 + 2x^2 + x + 1,\ b(x) = 2x + 1$

$$r = \frac{7}{8}$$

$$q = \frac{x^2}{2} + \frac{3}{4}x + \frac{1}{8}$$

$$b = 2x+1 \;\Big|\; x^3 + 2x^2 + x + 1$$

$$x^3 + \frac{x^2}{2}$$

$$\frac{3}{2}x^2 + x + 1$$

$$\frac{3}{2}x^2 + \frac{3x}{4}$$

$$\frac{x}{4} + 1$$

$$\frac{x}{4} + \frac{1}{8}$$

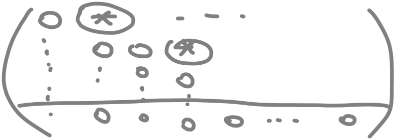
$$7/8$$

Solving Linear System - Gaussian Elimination

- **Input:** matrix $A \in \mathbb{F}^{n \times d}$, vector $b \in \mathbb{F}^{n}$
- **Output:** Is there a solution $y \in \mathbb{F}^{d}$ to $Ay = b$?

Solving Linear System - Gaussian Elimination

- **Input:** matrix $A \in \mathbb{F}^{n \times d}$, vector $b \in \mathbb{F}^n$
- **Output:** Is there a solution $y \in \mathbb{F}^d$ to $Ay = b$?
- Algorithm
  1. Put $C = \underbrace{\begin{pmatrix} A & b \end{pmatrix}}_{\mathbb{F}^{n \times (d+1)}}$ in reduced row-echelon form *we will focus on this*



Solving Linear System - Gaussian Elimination

- **Input:** matrix $A \in \mathbb{F}^{n \times d}$, vector $b \in \mathbb{F}^n$
- **Output:** Is there a solution $y \in \mathbb{F}^d$ to $Ay = b$?
- Algorithm
  1. Put $C = \begin{pmatrix} A & b \end{pmatrix}$ in reduced row-echelon form *we will focus on this*
  2. From bottom-up along rows of A, if the equation has a solution then set it properly

Solving Linear System - Gaussian Elimination

- **Input:** matrix $A \in \mathbb{F}^{n \times d}$, vector $b \in \mathbb{F}^n$
- **Output:** Is there a solution $y \in \mathbb{F}^d$ to $Ay = b$?
- Algorithm
  1. Put $C = \begin{pmatrix} A & b \end{pmatrix}$ in reduced row-echelon form *we will focus on this*
  2. From bottom-up along rows of A, if the equation has a solution then set it properly
  3. So long as there are no inconsistencies, we found a solution

Example

- $A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 2 & 3 & -1 \end{pmatrix}$ and $b = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$

$\exists\, y \in \mathbb{F}^3$ s.t. $Ay = b$ $\quad y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$

$$C = \left(\begin{array}{ccc|c} 1 & 0 & 1 & 3 \\ 1 & 1 & 0 & 1 \\ 2 & 3 & -1 & 0 \end{array}\right) \longrightarrow \begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 3 & -3 & -6 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{array}{l} \leftarrow \text{non-redundant} \\ \leftarrow \text{redundant} \end{array}$$

$\boxed{y_3 = t}$ $\quad y_2 - t = -2 \Rightarrow \boxed{y_2 = t - 2}$

$y_1 + t = 3 \Rightarrow y_1 = 3 - t$ $\quad \begin{pmatrix} 3-t \\ t-2 \\ t \end{pmatrix} \quad t \in \mathbb{F}$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 2 & 3 & -1 \end{pmatrix} \qquad b = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$$

$$\begin{aligned} \rightarrow f_1 \quad & y_1 + y_3 - 3 = 0 \\ \left\{ \begin{array}{l} f_2 \\ f_3 \end{array} \right. \quad & \begin{array}{l} y_1 + y_2 - 1 = 0 \\ y_1 + 3y_2 - y_3 = 0 \end{array} \end{aligned}$$

$$y_1 > y_2 > y_3$$

$$\underline{f_1}\ ,\ \underline{f_2 - f_1}\ ,\ \underbrace{f_3 - f_1 - 3(f_2 - f_1)}_{0}$$

Why Multivariate Multipolynomial Division?

- From last lecture, many algorithmic problems we really would like to solve:
  1. ideal membership problem
  2. solving polynomial equations
  3. implicitization problem
  4. finding irreducible components of algebraic set
  5. among others...

Why Multivariate Multipolynomial Division?

- From last lecture, many algorithmic problems we really would like to solve:
    1. ideal membership problem
    2. solving polynomial equations
    3. implicitization problem
    4. finding irreducible components of algebraic set
    5. among others...
- It turns out that a generalization of both algorithms above is fundamental to solve all the problems above!

Why Multivariate Multipolynomial Division?

- From last lecture, many algorithmic problems we really would like to solve:
  1. ideal membership problem
  2. solving polynomial equations
  3. implicitization problem
  4. finding irreducible components of algebraic set
  5. among others...
- It turns out that a generalization of both algorithms above is fundamental to solve all the problems above!
- Implicit in the seminal works of Hilbert and Gordan from 1890s!

Why Multivariate Multipolynomial Division?

- From last lecture, many algorithmic problems we really would like to solve:
  1. ideal membership problem
  2. solving polynomial equations
  3. implicitization problem
  4. finding irreducible components of algebraic set
  5. among others...
- It turns out that a generalization of both algorithms above is fundamental to solve all the problems above!
- Implicit in the seminal works of Hilbert and Gordan from 1890s!
- Complexity analyzed by Buchberger in 1960s!

Monomial Ordering

- In division algorithm over $\mathbb{F}[x]$, implicitly assumed $x \leq x^2 \leq x^3 \leq \cdots$ and that constants were "smaller than" any power of x

Monomial Ordering

- In division algorithm over $\mathbb{F}[x]$, implicitly assumed $x \leq x^2 \leq x^3 \leq \cdots$ and that constants were "smaller than" any power of x
- In our linear system solving algorithm, we implicitly assumed that $y_1 \geq y_2 \geq \cdots \geq y_d$

Monomial Ordering

- In division algorithm over $\mathbb{F}[x]$, implicitly assumed $x \leq x^2 \leq x^3 \leq \cdots$ and that constants were "smaller than" any power of x
- In our linear system solving algorithm, we implicitly assumed that $y_1 \geq y_2 \geq \cdots \geq y_d$
- Can we assume a similar ordering for monomials in $\mathbb{F}[x_1, \ldots, x_n]$? YES!

Monomial Ordering

- In division algorithm over $\mathbb{F}[x]$, implicitly assumed $x \leq x^2 \leq x^3 \leq \cdots$ and that constants were "smaller than" any power of x
- In our linear system solving algorithm, we implicitly assumed that $y_1 \geq y_2 \geq \cdots \geq y_d$
- Can we assume a similar ordering for monomials in $\mathbb{F}[x_1, \ldots, x_n]$? YES!
- Even to write a polynomial in a "humanly consistent way" we assume a monomial order (i.e., the ones we write first)
- Example: given two monomials $\mathbf{x^a}, \mathbf{x^b} \in \mathbb{F}[x_1, \ldots, x_n]$, we say

$$\mathbf{x^a} \succeq \mathbf{x^b} \;\text{ if }\; \mathbf{a} \geq \mathbf{b} \;\text{ in lexicographic order over }\; \mathbb{N}^n$$

$a \geq b$ if first index i s.t. $a_i \neq b_i$ we have $a_i > b_i$

<u>aa</u>rdvark > <u>ab</u>original $(2, \underline{1}, 3) > (2, \underline{0}, 100)$

Monomial Ordering

- In division algorithm over $\mathbb{F}[x]$, implicitly assumed $x \leq x^2 \leq x^3 \leq \cdots$ and that constants were "smaller than" any power of x
- In our linear system solving algorithm, we implicitly assumed that $y_1 \geq y_2 \geq \cdots \geq y_d$
- Can we assume a similar ordering for monomials in $\mathbb{F}[x_1, \ldots, x_n]$? YES!
- Even to write a polynomial in a "humanly consistent way" we assume a monomial order (i.e., the ones we write first)
- Example: given two monomials $\mathbf{x}^{\mathbf{a}}, \mathbf{x}^{\mathbf{b}} \in \mathbb{F}[x_1, \ldots, x_n]$, we say

$$\mathbf{x}^{\mathbf{a}} \succeq \mathbf{x}^{\mathbf{b}} \text{ if } \mathbf{a} \geq \mathbf{b} \text{ in lexicographic order over } \mathbb{N}^n$$

$LT(f) \cdot LT(g) = LT(f \cdot g)$

- In general a good monomial order has:
  1. *Total order*: any two elements can be compared
  2. *Transitive*: $\mathbf{x}^{\mathbf{a}} \succeq \mathbf{x}^{\mathbf{b}}$ and $\mathbf{x}^{\mathbf{b}} \succeq \mathbf{x}^{\mathbf{c}}$ then $\mathbf{x}^{\mathbf{a}} \succeq \mathbf{x}^{\mathbf{c}}$
  3. *Well-behaved under multiplication:* $\mathbf{x}^{\mathbf{a}} \succeq \mathbf{x}^{b} \Rightarrow \mathbf{x}^{\mathbf{a}+\mathbf{c}} \succeq \mathbf{x}^{\mathbf{b}+\mathbf{c}}$
  4. *Well-ordering*: every non-empty subset has a *smallest element*

(ensure that algorithms will terminate)

Leading Terms, Monomials, Coefficients

- Now we are ready to define special terms of polynomials

$$f(\mathbf{x}) = \sum_{\alpha} f_\alpha \cdot \mathbf{x}^\alpha$$

Leading Terms, Monomials, Coefficients

- Now we are ready to define special terms of polynomials

$$f(\mathbf{x}) = \sum_{\alpha} f_\alpha \cdot \mathbf{x}^\alpha$$

- The *support* of f

$$\operatorname{supp}(f) := \{\underline{\alpha \in \mathbb{N}^n} \mid \underline{f_\alpha \neq 0}\}$$

Leading Terms, Monomials, Coefficients

$f(x, y) = x^2 y + x y^{100} + x y^{99} + y^{200}$

- Now we are ready to define special terms of polynomials

$\succeq$ lex

$\text{mdeg}(f) = (2, 1)$

$$f(\mathbf{x}) = \sum_{\alpha} f_\alpha \cdot \mathbf{x}^\alpha$$

$\succeq$ graded lex

$\text{mdeg}(f) = y^{200}$

- The *support* of f

$$\text{supp}(f) := \{\alpha \in \mathbb{N}^n \mid f_\alpha \neq 0\}$$

- The *multidegree* of f is the maximum monomial in the support of f according to $\boxed{\succeq.}$ Termed $\text{mdeg}(f)$.
- The *leading monomial* of f is $LM(f) := \mathbf{x}^{\text{mdeg}(f)}$
- The *leading coefficient* of f is $LC(f) := f_{\text{mdeg}(f)}$
- The *leading term* of f is $LC(f) \cdot LM(f)$.

A Division Algorithm - a first attempt $\bar{x} = (x_1, \dots, x_n)$

- **Input:** polynomials $G, F_1, \dots, F_s \in \mathbb{F}[\mathbf{x}]$ and a monomial order $\succeq$
- **Output:** $\underline{Q_1, \dots, Q_s}, \underline{R} \in \mathbb{F}[\mathbf{x}]$ such that

$$G = F_1 \cdot Q_1 + \cdots + F_s \cdot Q_s + R$$

where $\mathrm{mdeg}(R) < \mathrm{mdeg}(F_i)$ for $i \in [s]$

A Division Algorithm - a first attempt

- **Input:** polynomials $G, F_1, \ldots, F_s \in \mathbb{F}[\mathbf{x}]$ and a monomial order $\succeq$
- **Output:** $Q_1, \ldots, Q_s, R \in \mathbb{F}[\mathbf{x}]$ such that

$$G = F_1 \cdot Q_1 + \cdots + F_s \cdot Q_s + R$$

  where $\text{mdeg}(R) < \text{mdeg}(F_i)$ for $i \in [s]$
- *Idea*: same as in one-variable case - cancel the leading term of G by using F_i

A Division Algorithm - a first attempt

- **Input:** polynomials $G, F_1, \ldots, F_s \in \mathbb{F}[\mathbf{x}]$ and a monomial order $\succeq$
- **Output:** $Q_1, \ldots, Q_s, R \in \mathbb{F}[\mathbf{x}]$ such that

$$G = F_1 \cdot Q_1 + \cdots + F_s \cdot Q_s + R$$

  where $\mathrm{mdeg}(R) < \mathrm{mdeg}(F_i)$ for $i \in [s]$
- *Idea*: same as in one-variable case - cancel the leading term of G by using F_i
- Example 1: $G = xy^2 + 1$, $F_1 = xy + 1$ and $F_2 = y + 1$

$Q_2 : -1$

$Q_1 : y$

$F_2 = \underline{y}+1$

$F_1 = \underline{xy}+1$

$r = 2$

$$\begin{array}{l} xy^2 + 1 \\ \hline xy^2 + y \\ \hline -y + 1 \\ -y - 1 \\ \hline 2 \; / 0 \end{array}$$

A Division Algorithm - a first attempt

- **Input:** polynomials $G, F_1, \ldots, F_s \in \mathbb{F}[\mathbf{x}]$ and a monomial order $\succeq$
- **Output:** $Q_1, \ldots, Q_s, R \in \mathbb{F}[\mathbf{x}]$ such that

$$G = F_1 \cdot Q_1 + \cdots + F_s \cdot Q_s + R$$

  where $\mathrm{mdeg}(R) < \mathrm{mdeg}(F_i)$ for $i \in [s]$
- *Idea*: same as in one-variable case - cancel the leading term of G by using F_i
- Example 1: $G = xy^2 + 1$, $F_1 = xy + 1$ and $F_2 = y + 1$
- Thus we have

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

A Division Algorithm - a first attempt

- **Input:** polynomials $G, F_1, \ldots, F_s \in \mathbb{F}[\mathbf{x}]$ and a monomial order $\succeq$
- **Output:** $Q_1, \ldots, Q_s, R \in \mathbb{F}[\mathbf{x}]$ such that

$$G = F_1 \cdot Q_1 + \cdots + F_s \cdot Q_s + R$$

where $\cancel{\mathrm{mdeg}(R) \prec \mathrm{mdeg}(F_i)}$ for $i \in [s]$ $\quad \mathrm{mdeg}(F_i) \nmid \alpha \quad \alpha \in \mathrm{supp}(R)$

- *Idea*: same as in one-variable case - cancel the leading term of G by using F_i
- Example 1: $G = xy^2 + 1$, $F_1 = xy + 1$ and $F_2 = y + 1$
- Thus we have

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

- Quotients are not unique:

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

$$x^2 y > x y^{100}$$

but $x y^{100} \nmid x^2 y$

problem for the division question that we posed

Division Algorithm - Subtlety

- The following subtlety comes because we have more than one variable
- Example 2: $G = x^2y + xy^2 + y^2$, $F_1 = xy - 1$ and $F_2 = y^2 - 1$ with lex order

$r = x + y + 1$

$Q_1 : x + y$

$Q_2 : 1$

$F_1 = xy - 1$

$F_2 = y^2 - 1$

$$
\begin{array}{l}
x^2y + xy^2 + y^2 \\
x^2y - x \\
\hline
xy^2 + x + y^2 \\
xy^2 - y \\
\hline
x + y^2 + y \\
\hline
y^2 + y \\
y^2 - 1 \qquad y + 1 \; / \; 0
\end{array}
$$

Division Algorithm - Subtlety

- The following subtlety comes because we have more than one variable
- Example 2: $G = x^2y + xy^2 + y^2$, $F_1 = xy - 1$ and $F_2 = y^2 - 1$ with lex order
- Thus we have

$$x^2y + xy^2 + y^2 = (x+y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + \underbrace{(x + y + 1)}_{r}$$

Division Algorithm - Subtlety

- The following subtlety comes because we have more than one variable
- Example 2: $G = x^2y + xy^2 + y^2$, $F_1 = xy - 1$ and $F_2 = y^2 - 1$ with lex order
- Thus we have

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

- So, instead of requiring that the leading term of remainder be smaller than leading term of divisors, better to require that *no monomial* of R is divisible by *any leading monomial* of the F_i's

A Division Algorithm - second attempt

- **Input:** polynomials $G, F_1, \ldots, F_s \in \mathbb{F}[\mathbf{x}]$
- **Output:** $Q_1, \ldots, Q_s, R \in \mathbb{F}[\mathbf{x}]$ such that

$$G = F_1 \cdot Q_1 + \cdots + F_s \cdot Q_s + R$$

no monomial of R be divisible by *any leading term* of the F_i's.
Furthermore if $F_i Q_i \neq 0$, we also want:

$$LM(G) \succeq LM(F_i Q_i)$$

A Division Algorithm - second attempt

- **Input:** polynomials $G, F_1, \ldots, F_s \in \mathbb{F}[\mathbf{x}]$
- **Output:** $Q_1, \ldots, Q_s, R \in \mathbb{F}[\mathbf{x}]$ such that

$$G = F_1 \cdot Q_1 + \cdots + F_s \cdot Q_s + R$$

no monomial of R be divisible by *any leading term* of the F_i's.
Furthermore if $F_i Q_i \neq 0$, we also want:

$$LM(G) \succeq LM(F_i Q_i)$$

- Algorithm:
  1. While $LM(G)$ is divisible by some $LM(F_i)$, divide appropriately (respecting the order preference of F_i's)
  2. If no $LM(F_i) \mid LM(G)$, add $LT(G)$ to the remainder and go back to step 1

A Division Algorithm - second attempt

- **Input:** polynomials $G, F_1, \ldots, F_s \in \mathbb{F}[\mathbf{x}]$
- **Output:** $Q_1, \ldots, Q_s, R \in \mathbb{F}[\mathbf{x}]$ such that

$$G = F_1 \cdot Q_1 + \cdots + F_s \cdot Q_s + R$$

no monomial of R be divisible by *any leading term* of the F_i's.
Furthermore if $F_i Q_i \neq 0$, we also want:

$$LM(G) \succeq LM(F_i Q_i)$$

- Algorithm:
  1. While $LM(G)$ is divisible by some $LM(F_i)$, divide appropriately (respecting the order preference of F_i's)
  2. If no $LM(F_i) \mid LM(G)$, add $LT(G)$ to the remainder and go back to step 1
- The algorithm above always terminates.

A Division Algorithm - second attempt

- **Input:** polynomials $G, F_1, \ldots, F_s \in \mathbb{F}[\mathbf{x}]$
- **Output:** $Q_1, \ldots, Q_s, R \in \mathbb{F}[\mathbf{x}]$ such that

$$G = F_1 \cdot Q_1 + \cdots + F_s \cdot Q_s + R$$

  no monomial of R be divisible by *any leading term* of the F_i's. Furthermore if $F_i Q_i \neq 0$, we also want:

$$LM(G) \succeq LM(F_i Q_i)$$

- Algorithm:
  1. While $LM(G)$ is divisible by some $LM(F_i)$, divide appropriately (respecting the order preference of F_i's)
  2. If no $LM(F_i) \mid LM(G)$, add $LT(G)$ to the remainder and go back to step 1
- The algorithm above always terminates.
- Proof is by well-ordering principle of the monomial order and fact that each step of division algorithm decreases leading term of G.

~~Pseudocode~~ Proof of termination

$G^{(0)}, G^{(1)}, G^{(2)}, \dots$

$LM(G^{(0)}) \succ LM(G^{(1)}) \succ LM(G^{(2)}) \succ \dots$

monomial ordering is a well ordering.

$S = \{LM(G^{(i)})\}$ must have a smallest element!

How does this generalize the two previous algorithms?

- Note that for univariate polynomials, the division algorithm works in the same way, if we consider the leading term of G one at a time

[1] This is more appropriate when checking if a linear form is in the span of a set of other linear forms

How does this generalize the two previous algorithms?

- Note that for univariate polynomials, the division algorithm works in the same way, if we consider the leading term of G one at a time
- For row-echelon form, note that it is exactly the division algorithm when the polynomials are linear[1]

[1] This is more appropriate when checking if a linear form is in the span of a set of other linear forms

Does it have the properties we want?

- What properties would we want from a division algorithm?
  1. remainder should be *uniquely determined*
  2. ordering shouldn't really matter (especially since we are trying to use it to solve ideal membership problem)
  3. univariate division algorithm solves ideal membership problem - so our division algorithm should also solve it

$$g \overset{?}{\in} (f_1, f_2)$$

$$(f_2, f_1)$$

$$g = f \cdot q + r \qquad g \in (f) \text{ iff } r = 0$$

Does it have the properties we want?

- What properties would we want from a division algorithm?
  1. remainder should be *uniquely determined*
  2. ordering shouldn't really matter (especially since we are trying to use it to solve ideal membership problem)
  3. univariate division algorithm solves ideal membership problem - so our division algorithm should also solve it
- Example 3: $G = x^2y + xy^2 + y^2$, $F_1 = y^2 - 1$ and $F_2 = xy - 1$ with lex order

same as example 2 with order reversed

$Q_1 : x + 1$

$Q_2 : x$

$F_1 = y^2 - 1$

$F_2 = xy - 1$

$$\begin{array}{l} x^2y + xy^2 + y^2 \\ \underline{x^2y - x} \\ xy^2 + x + y^2 \\ \underline{xy^2 - x} \end{array}$$

$r = 2x + 1$

$$\begin{array}{l} 2x + y^2 \\ \hline y^2 \\ \underline{y^2 - 1} \\ \cancel{1} \; 0 \end{array}$$

Does it have the properties we want?

- What properties would we want from a division algorithm?
  1. remainder should be *uniquely determined*
  2. ordering shouldn't really matter (especially since we are trying to use it to solve ideal membership problem)
  3. univariate division algorithm solves ideal membership problem - so our division algorithm should also solve it
- Example 3: $G = x^2y + xy^2 + y^2$, $F_1 = y^2 - 1$ and $F_2 = xy - 1$ with lex order
  same as example 2 with order reversed
- Note that remainder here is $2x + 1$, which is different from remainder in example 2: $(x + y + 1)$

Does it have the properties we want?

- What properties would we want from a division algorithm?
  1. remainder should be *uniquely determined*
  2. ordering shouldn't really matter (especially since we are trying to use it to solve ideal membership problem)
  3. univariate division algorithm solves ideal membership problem - so our division algorithm should also solve it
- Example 3: $G = x^2y + xy^2 + y^2$, $F_1 = y^2 - 1$ and $F_2 = xy - 1$ with lex order same as example 2 with order reversed
- Note that remainder here is $2x + 1$, which is different from remainder in example 2: $(x + y + 1)$
- Our division algorithm only gives *sufficient* condition for ideal membership problem: if G has zero remainder when divided by $(F_1, \ldots, F_s)$ then we know $G \in (F_1, \ldots, F_s)$

Does it have the properties we want?

- What properties would we want from a division algorithm?
  1. remainder should be *uniquely determined*
  2. ordering shouldn't really matter (especially since we are trying to use it to solve ideal membership problem)
  3. univariate division algorithm solves ideal membership problem - so our division algorithm should also solve it
- Example 3: $G = x^2y + xy^2 + y^2$, $F_1 = y^2 - 1$ and $F_2 = xy - 1$ with lex order   same as example 2 with order reversed
- Note that remainder here is $2x + 1$, which is different from remainder in example 2: $(x + y + 1)$
- Our division algorithm only gives *sufficient* condition for ideal membership problem: if G has zero remainder when divided by $(F_1, \ldots, F_s)$ then we know $G \in (F_1, \ldots, F_s)$
- Example 4: $G = xy^2 - x$, $F_1 = xy - 1$ and $F_2 = y^2 - 1$

Does it have the properties we want?

- What properties would we want from a division algorithm?
  1. remainder should be *uniquely determined*
  2. ordering shouldn't really matter (especially since we are trying to use it to solve ideal membership problem)
  3. univariate division algorithm solves ideal membership problem - so our division algorithm should also solve it
- Example 3: $G = x^2y + xy^2 + y^2$, $F_1 = y^2 - 1$ and $F_2 = xy - 1$ with lex order

  same as example 2 with order reversed
- Note that remainder here is $2x + 1$, which is different from remainder in example 2: $(x + y + 1)$
- Our division algorithm only gives *sufficient* condition for ideal membership problem: if G has zero remainder when divided by $(F_1, \ldots, F_s)$ then we know $G \in (F_1, \ldots, F_s)$
- Example 4: $G = xy^2 - x$, $F_1 = xy - 1$ and $F_2 = y^2 - 1$
- The "fix" for this division algorithm is to find a *good basis* for the ideal generated by $F_1, \ldots, F_s$ - the so-called Gröbner basis

Description of Ideals

- In the definition of algebraic sets, we used any family of polynomials $\mathcal{F}$ to define an algebraic set (or the ideal $I_{\mathcal{F}}$).

Question

Does every ideal of $\mathbb{F}[x_1, \ldots, x_n]$ have a finite description?

[2] Which was in fact first proved by Gordan.

Description of Ideals

- In the definition of algebraic sets, we used any family of polynomials $\mathcal{F}$ to define an algebraic set (or the ideal $I_{\mathcal{F}}$).

Question

Does every ideal of $\mathbb{F}[x_1, \ldots, x_n]$ have a finite description?

- Today we will address this question for *monomial ideals*. This will be done by Dickson's lemma[2]

[2] Which was in fact first proved by Gordan.

Description of Ideals

- In the definition of algebraic sets, we used any family of polynomials $\mathcal{F}$ to define an algebraic set (or the ideal $I_{\mathcal{F}}$).

Question

Does every ideal of $\mathbb{F}[x_1, \ldots, x_n]$ have a finite description?

- Today we will address this question for *monomial ideals*. This will be done by Dickson's lemma[2]
- A monomial ideal is any ideal generated by a family $\mathcal{F}$ of monomials (not necessarily a finite number of them)

[2] Which was in fact first proved by Gordan.

Description of Ideals

- In the definition of algebraic sets, we used any family of polynomials $\mathcal{F}$ to define an algebraic set (or the ideal $I_{\mathcal{F}}$).

Question

Does every ideal of $\mathbb{F}[x_1, \ldots, x_n]$ have a finite description?

- Today we will address this question for *monomial ideals*. This will be done by Dickson's lemma[2]
- A monomial ideal is any ideal generated by a family $\mathcal{F}$ of monomials (not necessarily a finite number of them)

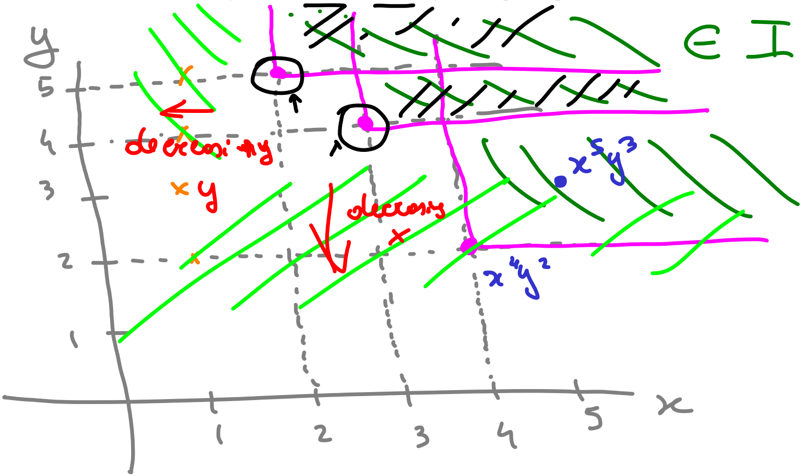
Theorem (Dickson's lemma)

Let $I = (\mathbf{x}^{\alpha} \mid \alpha \in \mathcal{F}) \subset \mathbb{F}[x_1, \ldots, x_n]$ be a monomial ideal. Then I can be written as $I = (\mathbf{x}^{\alpha(1)}, \ldots, \mathbf{x}^{\alpha(s)})$, where $\alpha(1), \ldots, \alpha(s) \in \mathcal{F}$

[2] Which was in fact first proved by Gordan.

Dickson's Lemma - picture & example

- Example: $I = (x^4y^2, x^3y^4, x^2y^5) \subset \mathbb{F}[x, y]$



Proof of Dickson's Lemma

- Induction on number of variables:

Proof of Dickson's Lemma

- Induction on number of variables:
  1. $n = 1$ then we know all monomial ideals are generated by x_1^α for some $\alpha \in \mathbb{N}$. If $\beta \in \mathcal{F}$ is its *smallest* element, then we have $I = (x_1^\beta)$

$\mathcal{F} = \{x_1^\alpha\}_\alpha$

$\alpha \in \mathcal{F}$ is $\alpha > \beta \Rightarrow x_1^\beta \mid x_1^\alpha$

$\Rightarrow x_1^\alpha \in (x_1^\beta) \Rightarrow I = (x_1^\beta)$

Proof of Dickson's Lemma

- Induction on number of variables:
  1. $n = 1$ then we know all monomial ideals are generated by x_1^α for some $\alpha \in \mathbb{N}$. If $\beta \in \mathcal{F}$ is its *smallest* element, then we have $I = (x_1^\beta)$
  2. Suppose $n \geq 1$ and theorem proved for n. Let us now prove it for $n + 1$ variables. Rewrite variables as $x_1, \ldots, x_n, y$.

Proof of Dickson's Lemma

- Induction on number of variables:
  1. $n = 1$ then we know all monomial ideals are generated by x_1^α for some $\alpha \in \mathbb{N}$. If $\beta \in \mathcal{F}$ is its *smallest* element, then we have $I = (x_1^\beta)$
  2. Suppose $n \geq 1$ and theorem proved for n. Let us now prove it for $n+1$ variables. Rewrite variables as $x_1, \ldots, x_n, y$.
  3. Let $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be the monomial ideal generated by $\mathbf{x}^\alpha$ such that $\mathbf{x}^\alpha \cdot y^m \in I$ for some $m \geq 0$.

$I = I_{\mathcal{F}}$ $\quad\quad J \subset \mathbb{F}[x_1, \ldots, x_n]$

Proof of Dickson's Lemma

- Induction on number of variables:
  1. $n = 1$ then we know all monomial ideals are generated by x_1^α for some $\alpha \in \mathbb{N}$. If $\beta \in \mathcal{F}$ is its *smallest* element, then we have $I = (x_1^\beta)$
  2. Suppose $n \geq 1$ and theorem proved for n. Let us now prove it for $n+1$ variables. Rewrite variables as $x_1, \ldots, x_n, y$.
  3. Let $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be the monomial ideal generated by $\mathbf{x}^\alpha$ such that $\mathbf{x}^\alpha \cdot y^m \in I$ for some $m \geq 0$.
  4. $\underbrace{J \text{ is finitely generated}}_{\text{by induction hypothesis}}$, say $J = (\mathbf{x}^{\alpha(1)}, \cdots, \mathbf{x}^{\alpha(s)})$

Proof of Dickson's Lemma

- Induction on number of variables:
  1. $n = 1$ then we know all monomial ideals are generated by x_1^α for some $\alpha \in \mathbb{N}$. If $\beta \in \mathcal{F}$ is its *smallest* element, then we have $I = (x_1^\beta)$
  2. Suppose $n \geq 1$ and theorem proved for n. Let us now prove it for $n+1$ variables. Rewrite variables as $x_1, \ldots, x_n, y$.
  3. Let $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be the monomial ideal generated by $\mathbf{x}^\alpha$ such that $\mathbf{x}^\alpha \cdot y^m \in I$ for some $m \geq 0$.
  4. J is finitely generated, say $J = (\mathbf{x}^{\alpha(1)}, \cdots, \mathbf{x}^{\alpha(s)})$
  5. Let $m_i \in \mathbb{N}$ be smallest integer such that $\mathbf{x}^{\alpha(i)} \cdot y^{m_i} \in I$, and let $\boxed{N := \max m_i.}$ And let $I_N := (\underline{\mathbf{x}^{\alpha(1)} \cdot y^{m_1}}, \ldots, \underline{\mathbf{x}^{\alpha(s)} \cdot y^{m_s}})$

Proof of Dickson's Lemma

- Induction on number of variables:
  1. $n = 1$ then we know all monomial ideals are generated by x_1^α for some $\alpha \in \mathbb{N}$. If $\beta \in \mathcal{F}$ is its *smallest* element, then we have $I = (x_1^\beta)$
  2. Suppose $n \geq 1$ and theorem proved for n. Let us now prove it for $n+1$ variables. Rewrite variables as $x_1, \ldots, x_n, y$.
  3. Let $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be the monomial ideal generated by $\mathbf{x}^\alpha$ such that $\mathbf{x}^\alpha \cdot y^m \in I$ for some $m \geq 0$.
  4. J is finitely generated, say $J = (\mathbf{x}^{\alpha(1)}, \cdots, \mathbf{x}^{\alpha(s)})$
  5. Let $m_i \in \mathbb{N}$ be smallest integer such that $\mathbf{x}^{\alpha(i)} \cdot y^{m_i} \in I$, and let $N := \max m_i$. And let $I_N := (\mathbf{x}^{\alpha(1)} \cdot y^{m_1}, \ldots, \mathbf{x}^{\alpha(s)} \cdot y^{m_s})$
  6. Any $\mathbf{x}^\beta y^m$ in I such that $m \geq N$ is in I_N.

$x^\beta y^m \in I \Rightarrow x^\beta \in J \Rightarrow x^\beta \in (x^{\alpha(i)})$

$m \geq N \Rightarrow y^N \mid y^m \Rightarrow y^{m_i} x^{\alpha(i)} \mid y^N x^{\alpha(i)}$

$y^N x^{\alpha(i)} \mid y^m x^\beta \Rightarrow x^\beta y^m \in I_N$

Proof of Dickson's Lemma

- Induction on number of variables:
  1. $n = 1$ then we know all monomial ideals are generated by x_1^α for some $\alpha \in \mathbb{N}$. If $\beta \in \mathcal{F}$ is its *smallest* element, then we have $I = (x_1^\beta)$
  2. Suppose $n \geq 1$ and theorem proved for n. Let us now prove it for $n+1$ variables. Rewrite variables as $x_1, \ldots, x_n, y$.
  3. Let $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be the monomial ideal generated by $\mathbf{x}^\alpha$ such that $\mathbf{x}^\alpha \cdot y^m \in I$ for some $m \geq 0$.
  4. J is finitely generated, say $J = (\mathbf{x}^{\alpha(1)}, \cdots, \mathbf{x}^{\alpha(s)})$
  5. Let $m_i \in \mathbb{N}$ be smallest integer such that $\mathbf{x}^{\alpha(i)} \cdot y^{m_i} \in I$, and let $N := \max m_i$. And let $I_N := (\mathbf{x}^{\alpha(1)} \cdot y^{m_1}, \ldots, \mathbf{x}^{\alpha(s)} \cdot y^{m_s})$
  6. Any $\mathbf{x}^\beta y^m$ in I such that $m \geq N$ is in I_N.
  7. For $0 \leq \ell < N$, let $J_\ell \subseteq \mathbb{F}[\mathbf{x}]$ be the monomial ideal defined by $\mathbf{x}^\alpha \in J_\ell \Leftrightarrow \mathbf{x}^\alpha y^\ell \in I$. Also $\underbrace{\text{finitely generated}}_{\text{by induction hypothesis}}$. $J_\ell = (\mathbf{x}^{\alpha_\ell(1)}, \ldots, \mathbf{x}^{\alpha_\ell(s_\ell)})$

deg(y) small

Proof of Dickson's Lemma

- Induction on number of variables:
  1. $n = 1$ then we know all monomial ideals are generated by x_1^{α} for some $\alpha \in \mathbb{N}$. If $\beta \in \mathcal{F}$ is its *smallest* element, then we have $I = (x_1^{\beta})$
  2. Suppose $n \geq 1$ and theorem proved for n. Let us now prove it for $n+1$ variables. Rewrite variables as $x_1, \ldots, x_n, y$.
  3. Let $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be the monomial ideal generated by $\mathbf{x}^{\alpha}$ such that $\mathbf{x}^{\alpha} \cdot y^m \in I$ for some $m \geq 0$.
  4. J is finitely generated, say $J = (\mathbf{x}^{\alpha(1)}, \cdots, \mathbf{x}^{\alpha(s)})$
  5. Let $m_i \in \mathbb{N}$ be smallest integer such that $\mathbf{x}^{\alpha(i)} \cdot y^{m_i} \in I$, and let $N := \max m_i$. And let $I_N := (\mathbf{x}^{\alpha(1)} \cdot y^{m_1}, \ldots, \mathbf{x}^{\alpha(s)} \cdot y^{m_s})$
  6. Any $\mathbf{x}^{\beta} y^m$ in I such that $m \geq N$ is in I_N.
  7. For $0 \leq \ell < N$, let $J_\ell \subseteq \mathbb{F}[\mathbf{x}]$ be the monomial ideal defined by $\mathbf{x}^{\alpha} \in J_\ell \Leftrightarrow \mathbf{x}^{\alpha} y^{\ell} \in I$. Also finitely generated. $J_\ell = (\mathbf{x}^{\alpha_\ell(1)}, \ldots, \mathbf{x}^{\alpha_\ell(s_\ell)})$
  8. Let $I_\ell := (\mathbf{x}^{\alpha_\ell(1)} \cdot y^{\ell}, \ldots, \mathbf{x}^{\alpha_\ell(s_\ell)} \cdot y^{\ell})$

Proof of Dickson's Lemma

- Induction on number of variables:
  1. $n = 1$ then we know all monomial ideals are generated by x_1^α for some $\alpha \in \mathbb{N}$. If $\beta \in \mathcal{F}$ is its *smallest* element, then we have $I = (x_1^\beta)$
  2. Suppose $n \geq 1$ and theorem proved for n. Let us now prove it for $n+1$ variables. Rewrite variables as $x_1, \ldots, x_n, y$.
  3. Let $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be the monomial ideal generated by $\mathbf{x}^\alpha$ such that $\mathbf{x}^\alpha \cdot y^m \in I$ for some $m \geq 0$.
  4. J is finitely generated, say $J = (\mathbf{x}^{\alpha(1)}, \cdots, \mathbf{x}^{\alpha(s)})$
  5. Let $m_i \in \mathbb{N}$ be smallest integer such that $\mathbf{x}^{\alpha(i)} \cdot y^{m_i} \in I$, and let $N := \max m_i$. And let $I_N := (\mathbf{x}^{\alpha(1)} \cdot y^{m_1}, \ldots, \mathbf{x}^{\alpha(s)} \cdot y^{m_s})$
  6. Any $\mathbf{x}^\beta y^m$ in I such that $m \geq N$ is in I_N.
  7. For $0 \leq \ell < N$, let $J_\ell \subseteq \mathbb{F}[\mathbf{x}]$ be the monomial ideal defined by $\mathbf{x}^\alpha \in J_\ell \Leftrightarrow \mathbf{x}^\alpha y^\ell \in I$. Also finitely generated. $J_\ell = (\mathbf{x}^{\alpha_\ell(1)}, \ldots, \mathbf{x}^{\alpha_\ell(s_\ell)})$
  8. Let $I_\ell := (\mathbf{x}^{\alpha_\ell(1)} \cdot y^\ell, \ldots, \mathbf{x}^{\alpha_\ell(s_\ell)} \cdot y^\ell)$
  9. Show that $I = I_0 + I_1 + \cdots + I_N$

$\supset$ each finitely generated

Proof of Dickson's lemma

$$I \subset \underbrace{I_0 + I_1 + \cdots + I_N}$$

$x^\beta y^m \in I$ if $m \geq N$ then $x^\beta y^m \in I_N$

suppose $m < N$

by definition $x^\beta \in J_m \Rightarrow \exists\, \alpha_m(i)$

s.t. $x^{\alpha_m(i)} \mid x^\beta$

$$x^{\alpha_m(i)} \cdot y^m \mid y^m x^\beta \Rightarrow x^\beta y^m \in I_m$$

$$\rotatebox{90}{$\in$}$$

$$I_m$$

$$\Rightarrow I \subset I_0 + \cdots + I_N \quad \blacksquare$$

Consequences of Dickson's lemma

- Dickson's lemma helps us decide if a monomial relation is a proper *monomial ordering*

Corollary (Monomial Order Criterion)

If $>$ is a relation on $\mathbb{N}^n$ satsifying

1. $>$ *is a total ordering on* $\mathbb{N}^n$
2. $\alpha > \beta$ *and* $\gamma \in \mathbb{N}^n$ *then* $\alpha + \gamma > \beta + \gamma$

behaves well under $\times$

Then $>$ is a well-ordering if, and only if, $\alpha \geq 0$ for all $\alpha \in \mathbb{N}^n$.

Consequences of Dickson's lemma

- Dickson's lemma helps us decide if a monomial relation is a proper *monomial ordering*

Corollary (Monomial Order Criterion)

If $>$ is a relation on $\mathbb{N}^n$ satsifying

1. $>$ *is a total ordering on* $\mathbb{N}^n$
2. $\alpha > \beta$ *and* $\gamma \in \mathbb{N}^n$ *then* $\alpha + \gamma > \beta + \gamma$

Then $>$ is a well-ordering if, and only if, $\alpha \geq 0$ for all $\alpha \in \mathbb{N}^n$.

- As we will see later in the course, this is great as different monomial orderings are used for different purposes.
  - elimination ordering (variant of lex order)
  - graded rev-lex order used in most ideal membership tasks

Consequences of Dickson's lemma

- Dickson's lemma helps us decide if a monomial relation is a proper *monomial ordering*

Corollary (Monomial Order Criterion)

If $>$ is a relation on $\mathbb{N}^n$ satsifying

1. *$>$ is a total ordering on $\mathbb{N}^n$*
2. *$\alpha > \beta$ and $\gamma \in \mathbb{N}^n$ then $\alpha + \gamma > \beta + \gamma$*

Then $>$ is a well-ordering if, and only if, $\alpha \geq 0$ for all $\alpha \in \mathbb{N}^n$.

- As we will see later in the course, this is great as different monomial orderings are used for different purposes.
  - elimination ordering
  - graded rev-lex order used in most ideal membership tasks
- From the set of bases for a monomial ideal, there is one which is better than others:

no redundant elements

A *minimal basis* of a monomial ideal is one where none of the generators is divisible by another generator.

- Two Familiar Division Algorithms
- Generalization: Multivariate Multipolynomial Division
- Issues with the division algorithm
- Monomial Ideals & Dickson's Lemma
- Conclusion
- Acknowledgements

Conclusion

- Today we learned about the division algorithm and Dickson's lemma
- Division algorithm generalizes univariate division algorithm and Gaussian elimination
- Division algorithm is not great - we will fix that by finding a good basis
- Dickson's lemma shows that monomial ideals are finitely generated
- Can use it to have easy criterion for checking monomial orderings
- Will use this lemma to prove Hilbert Basis Theorem

Acknowledgement

- Lecture based entirely on the book by CLO: Ideals, varieties and algorithms (see course webpage for a copy - or get online version through UW library)