Lecture 8: Gröbner Bases and Buchberger's Algorithm

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

February 3, 2021

Overview

- Problems with Division Algorithm & Hilbert Basis Theorem
- Gröbner Basis
- Buchberger's Algorithm
- Conclusion
- Acknowledgements

Issues with Division Algorithm

- 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

Issues with Division Algorithm

- 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
- 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 $G \in (F_1, \ldots, F_s)$

Issues with Division Algorithm

- What properties would we want from a division algorithm?
  1. remainder should be *uniquely determined*
  2. ordering <u>shouldn't really matter</u> (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
- 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 $G \in (F_1, \ldots, F_s)$
- The main problem is due to the fact that for some generators of an ideal, we are *missing important leading monomials*

Issues with Division Algorithm

- 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
- 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 $G \in (F_1, \ldots, F_s)$
- The main problem is due to the fact that for some generators of an ideal, we are *missing important leading monomials*
- Example: $f_1 = x^3 - 2xy$ and $f_2 = x^2y - 2y^2 + x$ and $x^2 \in (f_1, f_2)$

grlex

$$\underbrace{y \cdot f_1 - x f_2}_{\in (f_1, f_2)} = x^3y - 2xy^2 - x^3y - 2xy^2 - x^2 = -x^2$$

Issues with Division Algorithm

- 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
- 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 $G \in (F_1, \ldots, F_s)$
- The main problem is due to the fact that for some generators of an ideal, we are *missing important leading monomials*
- Example: $f_1 = x^3 - 2xy$ and $f_2 = x^2y - 2y^2 + x$ and $x^2 \in (f_1, f_2)$
- 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

Issues with Division Algorithm

- 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
- 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 $G \in (F_1, \ldots, F_s)$
- The main problem is due to the fact that for some generators of an ideal, we are *missing important leading monomials*
- Example: $f_1 = x^3 - 2xy$ and $f_2 = x^2y - 2y^2 + x$ and $x^2 \in (f_1, f_2)$
- 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
- **Property:** a Gröbner basis is one which contains all the *important leading monomials*

Ideal of Leading Terms & Hilbert Basis Theorem

- Given ideal $I \subseteq \mathbb{F}[\mathbf{x}]$ and a monomial ordering $>$, let:
  1. $LT(I)$ be the set of all leading terms of nonzero elements of I
  2. $LM(I)$ be the monomial ideal generated by $LT(I)$

set monomials

$$LM(I) = (LT(I))$$

Ideal of Leading Terms & Hilbert Basis Theorem

- Given ideal $I \subseteq \mathbb{F}[\mathbf{x}]$ and a monomial ordering $>$, let:
  1. $LT(I)$ be the set of all leading terms of nonzero elements of I
  2. $LM(I)$ be the monomial ideal generated by $LT(I)$
- By Dickson's lemma, we know that $LM(I)$ is *finitely generated*

Ideal of Leading Terms & Hilbert Basis Theorem

- Given ideal $I \subseteq \mathbb{F}[\mathbf{x}]$ and a monomial ordering $>$, let:
  1. $LT(I)$ be the set of all leading terms of nonzero elements of I
  2. $LM(I)$ be the monomial ideal generated by $LT(I)$
- By Dickson's lemma, we know that $LM(I)$ is *finitely generated*
- By previous slide, we also know that given a generating set for I, it could be the case that the leading terms of the generators are *strictly contained* in $LT(I)$

$\underline{f_1 = x^3} + \cdots \qquad \underline{f_2 = x^2} y + \cdots$

$\underline{x^2}$

$LM(f_1) = x^3 \quad LM(f_2) = x^2 y$

$LM(I) \supset \{x^3, x^2 y, \underline{x^2}\} \not\subseteq (x^3, x^2 y)$

Ideal of Leading Terms & Hilbert Basis Theorem

- Given ideal $I \subseteq \mathbb{F}[\mathbf{x}]$ and a monomial ordering $>$, let:
  1. $LT(I)$ be the set of all leading terms of nonzero elements of I
  2. $LM(I)$ be the monomial ideal generated by $LT(I)$
- By Dickson's lemma, we know that $LM(I)$ is *finitely generated*
- By previous slide, we also know that given a generating set for I, it could be the case that the leading terms of the generators are *strictly contained* in $LT(I)$
- Now we are ready to prove Hilbert's basis theorem:
  - Let $I \subseteq \mathbb{F}[\mathbf{x}]$ be an ideal

$\overline{x} = (x_1, \ldots, x_n)$

Ideal of Leading Terms & Hilbert Basis Theorem

- Given ideal $I \subseteq \mathbb{F}[\mathbf{x}]$ and a monomial ordering $>$, let:
  1. $LT(I)$ be the set of all leading terms of nonzero elements of I
  2. $LM(I)$ be the monomial ideal generated by $LT(I)$
- By Dickson's lemma, we know that $LM(I)$ is *finitely generated*
- By previous slide, we also know that given a generating set for I, it could be the case that the leading terms of the generators are *strictly contained* in $LT(I)$
- Now we are ready to prove Hilbert's basis theorem:
  - Let $I \subseteq \mathbb{F}[\mathbf{x}]$ be an ideal
  - By Dickson's lemma, $LM(I)$ is finitely generated

Ideal of Leading Terms & Hilbert Basis Theorem

- Given ideal $I \subseteq \mathbb{F}[\mathbf{x}]$ and a monomial ordering $>$, let:
  1. $LT(I)$ be the set of all leading terms of nonzero elements of I
  2. $LM(I)$ be the monomial ideal generated by $LT(I)$
- By Dickson's lemma, we know that $LM(I)$ is *finitely generated*
- By previous slide, we also know that given a generating set for I, it could be the case that the leading terms of the generators are *strictly contained* in $LT(I)$
- Now we are ready to prove Hilbert's basis theorem:
  - Let $I \subseteq \mathbb{F}[\mathbf{x}]$ be an ideal
  - By Dickson's lemma, $LM(I)$ is finitely generated
  - Let $g_1, \ldots, g_s \in I$ such that $\underline{LM(I)} = (\underline{LM(g_1)}, \ldots, \underline{LM(g_s)})$

$(g_1, \ldots, g_s) \subseteq I$

$\supseteq$

Ideal of Leading Terms & Hilbert Basis Theorem

- Given ideal $I \subseteq \mathbb{F}[\mathbf{x}]$ and a monomial ordering $>$, let:
  1. $LT(I)$ be the set of all leading terms of nonzero elements of I
  2. $LM(I)$ be the monomial ideal generated by $LT(I)$
- By Dickson's lemma, we know that $LM(I)$ is *finitely generated*
- By previous slide, we also know that given a generating set for I, it could be the case that the leading terms of the generators are *strictly contained* in $LT(I)$
- Now we are ready to prove Hilbert's basis theorem:
  - Let $I \subseteq \mathbb{F}[\mathbf{x}]$ be an ideal
  - By Dickson's lemma, $LM(I)$ is finitely generated
  - Let $g_1, \ldots, g_s \in I$ such that $LM(I) = (LM(g_1), \ldots, LM(g_s))$
  - The division algorithm from last lecture shows that $I \subseteq (g_1, \ldots, g_s)$

$f \in I \Longrightarrow$

Note that for any $f \in I$ we have that
$$LM(f) \in LM(I) = (LM(g_1), \ldots, LM(g_s)).$$

  - So long as f is nonzero and in I we will be able to divide, and remainder will be zero. Since the division algorithm always terminates, we will end up with remainder zero!

$f \in I \Rightarrow f \bmod (g_1, \ldots, g_s) = 0.$

$(g_1, \dots, g_s)$

$$(LM(g_1), \dots, LM(g_s)) = LM(I)$$

$$f \in I \Rightarrow LT(f) \in LM(I)$$

$$\Rightarrow \exists\, i \in [s] \text{ s.t. } LT(f) = c\,\bar{x}^{\gamma} \cdot LM(g_i)$$

$$\bar{x}^{\alpha} = \sum_{i=1}^{s} \bar{x}^{\beta_i} \cdot \underline{\bar{x}^{\delta_i}} \cdot \overset{\in \mathbb{F}}{c_i}$$

$\beta_i + \delta_i \neq \alpha \Rightarrow c_i$'s will cancel

Gröbner Basis

- From the proof of Hilbert Basis Theorem, we saw the *existence* of a very special generating set of our ideal.
- The main property of the special generating set was that the *leading monomials of generating set generate the ideal* $LM(I)$

No leading term left behind.

[1] This was also independently discovered by Hironaka, who termed these bases "standard bases" and used them for ideals in power series rings

Gröbner Basis

- From the proof of Hilbert Basis Theorem, we saw the *existence* of a very special generating set of our ideal.
- The main property of the special generating set was that the *leading monomials of generating set generate the ideal* $LM(I)$
- **Definition:** A Gröbner basis of an ideal is a generating set which has the property above.[1]

[1] This was also independently discovered by Hironaka, who termed these bases "standard bases" and used them for ideals in power series rings

Gröbner Basis

- From the proof of Hilbert Basis Theorem, we saw the *existence* of a very special generating set of our ideal.
- The main property of the special generating set was that the *leading monomials of generating set generate the ideal* $LM(I)$
- **Definition:** A Gröbner basis of an ideal is a generating set which has the property above.[1]
- A first property of Groebner Bases is *uniqueness of remainder* in the division algorithm. More precisely: if $G = \{g_1, \ldots, g_s\}$ is a Gorebner basis for I, then given $f \in \mathbb{F}[\mathbf{x}]$ there is a unique $r \in \mathbb{F}[\mathbf{x}]$ with the following properties:
    1. no term of r is divisible by any $LM(g_i)$
    2. there is $g \in I$ such that $f = g + r$

[1] This was also independently discovered by Hironaka, who termed these bases "standard bases" and used them for ideals in power series rings

Gröbner Basis

- From the proof of Hilbert Basis Theorem, we saw the *existence* of a very special generating set of our ideal.
- The main property of the special generating set was that the *leading monomials of generating set generate the ideal* $LM(I)$
- **Definition:** A Gröbner basis of an ideal is a generating set which has the property above.[1]
- A first property of Groebner Bases is *uniqueness of remainder* in the division algorithm. More precisely: if $G = \{g_1, \ldots, g_s\}$ is a Gorebner basis for I, then given $f \in \mathbb{F}[\mathbf{x}]$ there is a unique $r \in \mathbb{F}[\mathbf{x}]$ with the following properties:
    1. no term of r is divisible by any $LM(g_i)$
    2. there is $g \in I$ such that $f = g + r$
- Division algorithm gives existence of r

[1] This was also independently discovered by Hironaka, who termed these bases "standard bases" and used them for ideals in power series rings

Gröbner Basis

- From the proof of Hilbert Basis Theorem, we saw the *existence* of a very special generating set of our ideal.
- The main property of the special generating set was that the *leading monomials of generating set generate the ideal* $LM(I)$
- **Definition:** A Gröbner basis of an ideal is a generating set which has the property above.[1]
- A first property of Groebner Bases is *uniqueness of remainder* in the division algorithm. More precisely: if $G = \{g_1, \ldots, g_s\}$ is a Gorebner basis for I, then given $f \in \mathbb{F}[\mathbf{x}]$ there is a unique $r \in \mathbb{F}[\mathbf{x}]$ with the following properties:
  1. no term of r is divisible by any $LM(g_i)$
  2. there is $g \in I$ such that $f = g + r$

$f = g + r$

$= g' + r'$

- Division algorithm gives existence of r

$r - r' = g' - g \in I$

- Uniqueness comes from fact that if r, r' are remainders, then $r - r' \in I \Rightarrow r = r'$ by division algorithm

$(r - r')^G = 0$

$= r - r'$

[1] This was also independently discovered by Hironaka, who termed these bases "standard bases" and used them for ideals in power series rings

Algorithmic Questions Around Groebner Bases

- Now that we know how important Groebner bases are, two questions come to mind:
  1. When do we know that a basis is a Groebner Basis?
  2. Given an ideal, how can we construct a Groebner basis of this ideal?

[2] This name is a shortening for "syzygy polynomials" since they are syzygies over the monomial ideal.

Algorithmic Questions Around Groebner Bases

- Now that we know how important Groebner bases are, two questions come to mind:
  1. When do we know that a basis is a Groebner Basis?
  2. Given an ideal, how can we construct a Groebner basis of this ideal?
- To deal with the first question, we have the following definition:

S-polynomial:[2] given two polynomials $f, g \in \mathbb{F}[\mathbf{x}]$, let $\mathbf{x}^\gamma = LCM(\underline{LM(f)}, \underline{LM(g)})$. Then, the S-polynomial of f, g is

$$S(f,g) := \frac{\mathbf{x}^\gamma}{LT(f)} \cdot f - \frac{\mathbf{x}^\gamma}{LT(g)} \cdot g$$

[2] This name is a shortening for "syzygy polynomials" since they are syzygies over the monomial ideal.

Algorithmic Questions Around Groebner Bases

- Now that we know how important Groebner bases are, two questions come to mind:
  1. When do we know that a basis is a Groebner Basis?
  2. Given an ideal, how can we construct a Groebner basis of this ideal?
- To deal with the first question, we have the following definition:

S-polynomial:[2] given two polynomials $f, g \in \mathbb{F}[\mathbf{x}]$, let $\mathbf{x}^\gamma = LCM(LM(f), LM(g))$. Then, the S-polynomial of f, g is

"Cancelling the leading term"

$$S(f,g) := \frac{\mathbf{x}^\gamma}{LT(f)} \cdot f - \frac{\mathbf{x}^\gamma}{LT(g)} \cdot g$$

- Example: $f = \underline{x^3y^2} - x^2y^3$ and $g = \underline{3x^4y} + y^2$ in $\mathbb{Q}[\mathbf{x}]$ with the graded lexicographic order.

$\gamma = (4,2) \quad x^4y^2 = \bar{x}^\gamma$

$$S(f,g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = (\cancel{x^4y^2} - x^3y^3) - (\cancel{x^4y^2} + y^3/3)$$

$$= -x^3y^3 - y^3/3$$

[2] This name is a shortening for "syzygy polynomials" since they are syzygies over the monomial ideal.

Algorithmic Questions Around Groebner Bases

- Now that we know how important Groebner bases are, two questions come to mind:
  1. When do we know that a basis is a Groebner Basis?
  2. Given an ideal, how can we construct a Groebner basis of this ideal?
- To deal with the first question, we have the following definition:

  S-polynomial:[2] given two polynomials $f, g \in \mathbb{F}[\mathbf{x}]$, let $\mathbf{x}^\gamma = LCM(LM(f), LM(g))$. Then, the S-polynomial of f, g is

$$S(f,g) := \underbrace{\frac{\mathbf{x}^\gamma}{LT(f)} \cdot f}_{} - \underbrace{\frac{\mathbf{x}^\gamma}{LT(g)} \cdot g}_{}$$

- Example: $f = x^3y^2 - x^2y^3$ and $g = 3x^4y + y^2$ in $\mathbb{Q}[\mathbf{x}]$ with the graded lexicographic order.
- S-polynomials are designed to produce cancellations of leading terms.

[2]This name is a shortening for "syzygy polynomials" since they are syzygies over the monomial ideal.

How Cancellation Happens: S-polynomial lemma

- Next lemma shows that every cancellation of leading terms amongst polynomials of same degree happen *because of S-polynomial*
- **Lemma:** If we have a sum $p_1 + \cdots + p_s$ where $\text{multideg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\text{multideg}(p_1 + \cdots + p_s) < \delta$, then $p_1 + \cdots + p_s$ is a linear combination, with coefficients in $\mathbb{F}$, of the S-polynomials $S(p_i, p_j)$, where $i, j \in [s]$

some cancellation happened (of leading term)

Any cancellation of leading monomials can be derived by S- polynomials

How Cancellation Happens: S-polynomial lemma

- Next lemma shows that every cancellation of leading terms amongst polynomials of same degree happen *because of S-polynomial*
- **Lemma:** If we have a sum $p_1 + \cdots + p_s$ where $\text{multideg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\text{multideg}(p_1 + \cdots + p_s) < \delta$, then $p_1 + \cdots + p_s$ is a linear combination, with coefficients in $\mathbb{F}$, of the S-polynomials $S(p_i, p_j)$, where $i, j \in [s]$
  1. Let $c_i = LC(p_i)$, so $\underline{c_i} \cdot \underline{\mathbf{x}^\delta} = \underline{LT(p_i)}$ $c_i \neq 0$

How Cancellation Happens: S-polynomial lemma

- Next lemma shows that every cancellation of leading terms amongst polynomials of same degree happen *because of S-polynomial*
- **Lemma:** If we have a sum $p_1 + \cdots + p_s$ where $\text{multideg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\text{multideg}(p_1 + \cdots + p_s) < \delta$, then $p_1 + \cdots + p_s$ is a linear combination, with coefficients in $\mathbb{F}$, of the S-polynomials $S(p_i, p_j)$, where $i, j \in [s]$
  1. Let $c_i = LC(p_i)$, so $c_i \cdot \mathbf{x}^\delta = LT(p_i)$
  2. $\text{multideg}(p_1 + \cdots + p_s) < \delta \Rightarrow c_1 + \cdots + c_s = 0$

$$(p_1 + \cdots + p_s)_\delta = \sum_{i=1}^{s} c_i$$

How Cancellation Happens: S-polynomial lemma

- Next lemma shows that every cancellation of leading terms amongst polynomials of same degree happen *because of S-polynomial*
- **Lemma:** If we have a sum $p_1 + \cdots + p_s$ where $\text{multideg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\text{multideg}(p_1 + \cdots + p_s) < \delta$, then $p_1 + \cdots + p_s$ is a linear combination, with coefficients in $\mathbb{F}$, of the S-polynomials $S(p_i, p_j)$, where $i, j \in [s]$
  1. Let $c_i = LC(p_i)$, so $c_i \cdot \mathbf{x}^\delta = LT(p_i)$
  2. $\text{multideg}(p_1 + \cdots + p_s) < \delta \Rightarrow c_1 + \cdots + c_s = 0$
  3. Since p_i, p_j have same leading monomial

$$S(p_i, p_j) = \frac{1}{c_i} p_i - \frac{1}{c_j} p_j$$

$$\bar{x}^\gamma = \bar{x}^\delta = LCM(\bar{x}^\delta, \bar{x}^\delta)$$

$$S(p_i, p_j) = \frac{\bar{x}^\delta}{c_i \bar{x}^\delta} p_i - \frac{\bar{x}^\delta}{c_j \bar{x}^\delta} p_j$$

How Cancellation Happens: S-polynomial lemma

- Next lemma shows that every cancellation of leading terms amongst polynomials of same degree happen *because of S-polynomial*
- **Lemma:** If we have a sum $p_1 + \cdots + p_s$ where $\text{multideg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\text{multideg}(p_1 + \cdots + p_s) < \delta$, then $p_1 + \cdots + p_s$ is a linear combination, with coefficients in $\mathbb{F}$, of the S-polynomials $S(p_i, p_j)$, where $i, j \in [s]$
  1. Let $c_i = LC(p_i)$, so $c_i \cdot \mathbf{x}^\delta = LT(p_i)$
  2. $\text{multideg}(p_1 + \cdots + p_s) < \delta \Rightarrow \underline{c_1 + \cdots + c_s = 0}$
  3. Since p_i, p_j have same leading monomial

$$S(p_i, p_j) = \frac{1}{c_i} p_i - \frac{1}{c_j} p_j$$

  4. Thus, by using (2)

$$\sum_{i=1}^{s-1} c_i \cdot \underline{S(p_i, p_s)} = p_1 + \cdots + p_s \quad -c_s$$

$$\sum_{i=1}^{s-1} c_i \left(\frac{1}{c_i} p_i - \frac{1}{c_s} p_s \right) = p_1 + \cdots + p_{s-1} - \frac{\overbrace{(c_1 + \cdots + c_{s-1})}^{-c_s}}{c_s} p_s$$

How Cancellation Happens: S-polynomial lemma

- Next lemma shows that every cancellation of leading terms amongst polynomials of same degree happen *because of S-polynomial*
- **Lemma:** If we have a sum $p_1 + \cdots + p_s$ where $\text{multideg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\text{multideg}(p_1 + \cdots + p_s) < \delta$, then $p_1 + \cdots + p_s$ is a linear combination, with coefficients in $\mathbb{F}$, of the S-polynomials $S(p_i, p_j)$, where $i, j \in [s]$
  1. Let $c_i = LC(p_i)$, so $c_i \cdot \mathbf{x}^\delta = LT(p_i)$
  2. $\text{multideg}(p_1 + \cdots + p_s) < \delta \Rightarrow c_1 + \cdots + c_s = 0$
  3. Since p_i, p_j have same leading monomial

$$S(p_i, p_j) = \frac{1}{c_i} p_i - \frac{1}{c_j} p_j$$

  4. Thus, by using (2) more efficient

using poly's of lower multidegree

$$\sum_{i=1}^{s-1} c_i \cdot S(p_i, p_s) = p_1 + \cdots + p_s$$

  5. note that $\text{multideg}(S(p_i, p_j)) < \delta$

Buchberger's Criterion

- Now that we are acquainted with S-polynomials and how cancellations happen, we can state Buchberger's criterion:

  Let $I \subseteq \mathbb{F}[\mathbf{x}]$ be an ideal. Then a basis $G = \{g_1, \ldots, g_s\}$ of I is a Groebner basis of I if, and only if, for all pairs $i \neq j$, the remainder on division of $\underline{S(g_i, g_j)}$ by G is zero.

Buchberger's Criterion

- Now that we are acquainted with S-polynomials and how cancellations happen, we can state Buchberger's criterion:

  Let $I \subseteq \mathbb{F}[\mathbf{x}]$ be an ideal. Then a basis $G = \{g_1, \ldots, g_s\}$ of I is a Groebner basis of I if, and only if, for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G is zero.

- $(\Rightarrow)$ if G is a Groebner basis, then $S(g_i, g_j) \in I \Rightarrow$ remainder of division by G is zero by previous slides.

$LM(S(g_i, g_i)) \in LM(I) = (LM(g_1), \ldots, LM(g_s))$

Buchberger's Criterion

- Now that we are acquainted with S-polynomials and how cancellations happen, we can state Buchberger's criterion:

  Let $I \subseteq \mathbb{F}[\mathbf{x}]$ be an ideal. Then a basis $G = \{g_1, \ldots, g_s\}$ of I is a Groebner basis of I if, and only if, for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G is zero.

- $(\Rightarrow)$ if G is a Groebner basis, then $S(g_i, g_j) \in I \Rightarrow$ remainder of division by G is zero by previous slides.
- $(\Leftarrow)$ need to prove that for any $f \in I$, we have that

$$LT(f) \in (LT(g_1), \ldots, LT(g_s))$$

if $\overline{S(g_i, g_j)}^G = 0 \quad \forall\, i \neq j$

then G Gröbner basis

$(LM(I) \subset (LM(g_1), \ldots, LM(g_s)))$

Buchberger's Criterion

- Now that we are acquainted with S-polynomials and how cancellations happen, we can state Buchberger's criterion:

  Let $I \subseteq \mathbb{F}[\mathbf{x}]$ be an ideal. Then a basis $G = \{g_1, \ldots, g_s\}$ of I is a Groebner basis of I if, and only if, for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G is zero.

- $(\Rightarrow)$ if G is a Groebner basis, then $S(g_i, g_j) \in I \Rightarrow$ remainder of division by G is zero by previous slides.
- $(\Leftarrow)$ need to prove that for any $f \in I$, we have that

$$LT(f) \in (LT(g_1), \ldots, LT(g_s))$$

- $f \in I = (g_1, \ldots, g_s)$ (as G is a generating set)

$$f = g_1 h_1 + \cdots + g_s h_s$$

where $\text{multideg}(f) \leq \max_i(\text{multideg}(g_i h_i))$

Buchberger's Criterion

- Now that we are acquainted with S-polynomials and how cancellations happen, we can state Buchberger's criterion:

  Let $I \subseteq \mathbb{F}[\mathbf{x}]$ be an ideal. Then a basis $G = \{g_1, \ldots, g_s\}$ of I is a Groebner basis of I if, and only if, for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G is zero.

- $(\Rightarrow)$ if G is a Groebner basis, then $S(g_i, g_j) \in I \Rightarrow$ remainder of division by G is zero by previous slides.
- $(\Leftarrow)$ need to prove that for any $f \in I$, we have that

$$LT(f) \in (LT(g_1), \ldots, LT(g_s))$$

- $f \in I = (g_1, \ldots, g_s)$ (as G is a generating set)

$$f = g_1 h_1 + \cdots g_s h_s$$

  where $\text{multideg}(f) \leq \max_i(\text{multideg}(g_i h_i))$
- Strategy: let's pick *most efficient representation* of f

Proof of Buchberger's Criterion

- $f \in I = (g_1, \ldots, g_s)$ (as G is a generating set)

$$f = g_1 h_1 + \cdots + g_s h_s$$

where $\text{multideg}(f) \le \max_i(\text{multideg}(g_i h_i))$

- Take representation of *lowest multidegree*, that is, one for which

$$\delta := \max_i(\text{multideg}(g_i h_i)) \quad \text{is minimum}$$

Proof of Buchberger's Criterion

- $f \in I = (g_1, \ldots, g_s)$ (as G is a generating set)

$$f = g_1 h_1 + \cdots g_s h_s$$

  where $\text{multideg}(f) \leq \max_i(\text{multideg}(g_i h_i))$
- Take representation of *lowest miltidegree*, that is, one for which

$$\delta := \max_i(\text{multideg}(g_i h_i)) \quad \text{is minimum}$$

- Such minimum δ exists by the well-ordering of monomial order

Proof of Buchberger's Criterion

- $f \in I = (g_1, \ldots, g_s)$ (as G is a generating set)

$$f = g_1 h_1 + \cdots g_s h_s$$

where $\text{multideg}(f) \leq \max_i(\text{multideg}(g_i h_i))$

- Take representation of *lowest miltidegree*, that is, one for which

$$\delta := \max_i(\text{multideg}(g_i h_i)) \quad \text{is minimum}$$

- Such minimum δ exists by the well-ordering of monomial order
- In particular, $\text{multideg}(f) \leq \delta$

Proof of Buchberger's Criterion

- $f \in I = (g_1, \ldots, g_s)$ (as G is a generating set)

$$f = g_1 h_1 + \cdots g_s h_s$$

where $\text{multideg}(f) \leq \max_i(\text{multideg}(g_i h_i))$

- Take representation of *lowest miltidegree*, that is, one for which

$$\delta := \max_i(\text{multideg}(g_i h_i)) \quad \text{is minimum}$$

- Such minimum δ exists by the well-ordering of monomial order
- In particular, $\text{multideg}(f) \leq \delta$
- If $\text{multideg}(f) = \delta$, then there is some $i \in [s]$ such that

$$\text{multideg}(f) = \text{multideg}(g_i h_i) \Rightarrow LM(f) \in (LM(g_1), \ldots, LM(g_s))$$

$\Longrightarrow$ LM(f) divisible by LM(g_i)

Proof of Buchberger's Criterion

- $f \in I = (g_1, \dots, g_s)$ (as G is a generating set)

$$f = g_1 h_1 + \cdots g_s h_s$$

  where $\text{multideg}(f) \leq \max_i(\text{multideg}(g_i h_i))$
- Take representation of *lowest miltidegree*, that is, one for which

$$\delta := \max_i(\text{multideg}(g_i h_i)) \quad \text{is minimum}$$

- Such minimum δ exists by the well-ordering of monomial order
- In particular, $\text{multideg}(f) \leq \delta$
- If $\text{multideg}(f) = \delta$, then there is some $i \in [s]$ such that

$$\text{multideg}(f) = \text{multideg}(g_i h_i) \Rightarrow LM(f) \in (LM(g_1), \dots, LM(g_s))$$

- So need to see what happens when $\delta > \text{multideg}(f)$

Proof of Buchberger's Criterion

- We are now in case: $\text{multideg}(f) < \delta$
- In this case we will use the fact that $\overline{S(g_i, g_j)}^G = 0$[3] to obtain another expression of $f \in I$ with smaller δ

[3] This is a short-hand notation to say that the division by G is zero

Proof of Buchberger's Criterion

- We are now in case: $\text{multideg}(f) < \delta$
- In this case we will use the fact that $\overline{S(g_i, g_j)}^G = 0$[3] to obtain another expression of $f \in I$ with smaller δ
- Let's isolate part of highest multi-degree:

$$f = \sum_{i=1}^{s} g_i h_i$$

$$= \underbrace{\sum_{i:\, \text{multideg}(h_i g_i)=\delta} LT(h_i) \cdot g_i}_{\text{highest multideg}} + \underbrace{\sum_{i:\, \text{multideg}(h_i g_i)=\delta} (h_i - LT(h_i)) g_i + \sum}_{\text{rest multideg} < \delta}$$

[3] This is a short-hand notation to say that the division by G is zero

Proof of Buchberger's Criterion

- We are now in case: $\text{multideg}(f) < \delta$
- In this case we will use the fact that $S(g_i, g_j)^G = 0$[3] to obtain another expression of $f \in I$ with smaller δ
- Let's isolate part of highest multi-degree:
- $\text{multideg}(f) < \delta \Rightarrow$ component of multi-degree δ must vanish

[3] This is a short-hand notation to say that the division by G is zero

Proof of Buchberger's Criterion

- We are now in case: $\text{multideg}(f) < \delta$
- In this case we will use the fact that $\overline{S(g_i, g_j)}^G = 0$[3] to obtain another expression of $f \in I$ with smaller δ
- Let's isolate part of highest multi-degree:
- $\text{multideg}(f) < \delta \Rightarrow$ component of multi-degree δ must vanish
- Now we use our lemma over $LT(h_1) \cdot g_1 + \cdots + LT(h_s) \cdot g_s$ to decrease its multi-degree via S-polynomials

[3] This is a short-hand notation to say that the division by G is zero

Proof of Buchberger's Criterion

- We are now in case: $\text{multideg}(f) < \delta$
- In this case we will use the fact that $\overline{S(g_i, g_j)}^G = 0$[3] to obtain another expression of $f \in I$ with smaller δ
- Let's isolate part of highest multi-degree:
- $\text{multideg}(f) < \delta \Rightarrow$ component of multi-degree δ must vanish
- Now we use our lemma over $LT(h_1) \cdot g_1 + \cdots + LT(h_s) \cdot g_s$ to decrease its multi-degree via S-polynomials
- Let $p_i = \underline{LT(h_i)} \cdot \underline{g_i}$. From your homework, we know

$$S(p_i, p_j) = \mathbf{x}^{\delta - \gamma_{ij}} \cdot S(g_i, g_j)$$

where $\gamma_{ij} = LCM(LM(g_i), LM(g_j))$

[3] This is a short-hand notation to say that the division by G is zero

Proof of Buchberger's Criterion

- We are now in case: $\text{multideg}(f) < \delta$
- In this case we will use the fact that $S(g_i, g_j)^G = 0$[3] to obtain another expression of $f \in I$ with smaller δ
- Let's isolate part of highest multi-degree:
- $\text{multideg}(f) < \delta \Rightarrow$ component of multi-degree δ must vanish
- Now we use our lemma over $LT(h_1) \cdot g_1 + \cdots + LT(h_s) \cdot g_s$ to decrease its multi-degree via S-polynomials
- Let $p_i = LT(h_i) \cdot g_i$. From your homework, we know

$$S(p_i, p_j) = \mathbf{x}^{\delta - \gamma_{ij}} \cdot S(g_i, g_j)$$

  where $\gamma_{ij} = LCM(LM(g_i), LM(g_j))$
- $\underline{S(g_i, g_j)^G = 0} \Rightarrow \underline{S(g_i, g_j)} = A_1 g_1 + \cdots + A_s g_s$

$$\underline{\text{multideg}(A_i g_i)} \leq \underline{\text{multideg}(S(g_i, g_j))}$$

by division algorithm

[3] This is a short-hand notation to say that the division by G is zero

Proof of Buchberger's Criterion

- $\overline{S(g_i, g_j)}^G = 0 \Rightarrow S(g_i, g_j) = A_1 g_1 + \cdots + A_s g_s$

$$\mathrm{multideg}(A_i g_i) \leq \mathrm{multideg}(S(g_i, g_j))$$

Proof of Buchberger's Criterion

- $\overline{S(g_i, g_j)}^G = 0 \Rightarrow S(g_i, g_j) = A_1 g_1 + \cdots + A_s g_s$

$$\text{multideg}(A_i g_i) \leq \text{multideg}(S(g_i, g_j))$$

- Multiplying above by $\mathbf{x}^{\delta - \gamma_{ij}}$

$$\underline{S(p_i, p_j)} = \mathbf{x}^{\delta - \gamma_{ij}} \cdot S(g_i, g_j) = B_1 g_1 + \cdots + B_s g_s$$

Proof of Buchberger's Criterion

- $\overline{S(g_i, g_j)}^G = 0 \Rightarrow S(g_i, g_j) = A_1 g_1 + \cdots + A_s g_s$

$$\text{multideg}(A_i g_i) \leq \text{multideg}(S(g_i, g_j))$$

- Multiplying above by $\mathbf{x}^{\delta - \gamma_{ij}}$

$$S(p_i, p_j) = \mathbf{x}^{\delta - \gamma_{ij}} \cdot S(g_i, g_j) = B_1 g_1 + \cdots + B_s g_s$$

- When $B_i g_i \neq 0$ by the first bullet

S-polynomials

$$\underline{\text{multideg}(B_i g_i)} \overset{\text{division algo}}{\leq} \underline{\text{multideg}(\mathbf{x}^{\delta - \gamma_{ij}} \cdot S(g_i, g_j))} < \delta$$

by property of S-polynomials

$$\text{multideg}(p_1 + \cdots + p_s) < \delta$$

$$\Rightarrow \text{multideg}\,(S(p_i, p_j)) < \delta$$

Proof of Buchberger's Criterion

- $S(g_i, g_j)^G = 0 \Rightarrow S(g_i, g_j) = A_1 g_1 + \cdots + A_s g_s$

$$\text{multideg}(A_i g_i) \leq \text{multideg}(S(g_i, g_j))$$

- Multiplying above by $\mathbf{x}^{\delta - \gamma_{ij}}$

$$S(p_i, p_j) = \mathbf{x}^{\delta - \gamma_{ij}} \cdot S(g_i, g_j) = \underline{B_1 g_1 + \cdots + B_s g_s}$$

- When $B_i g_i \neq 0$ by the first bullet

$$\underline{\text{multideg}(B_i g_i)} \leq \text{multideg}(\mathbf{x}^{\delta - \gamma_{ij}} \cdot S(g_i, g_j)) \underline{< \delta}$$

by property of S-polynomials

- By our S-polynomial lemma, we have

$$\sum_{i=1} p_i = \underbrace{\sum_{i=1}^{s} LT(h_i) \cdot g_i}_{< \delta} = \sum_{i \neq j} a_{ij} \cdot \underline{S(p_i, p_j)} = \underline{C_1 g_1 + \cdots + C_s g_s}$$

$$C_i g_i = \underbrace{\sum a_{ij} B_i g_i}_{< \delta}$$

where $\underline{\text{multideg}(C_i g_i) < \delta}$

Proof of Buchberger's Criterion

$$f = \underbrace{\sum LT(h_i)\, g_i} + \underbrace{\text{stuff of multideg} < \delta}$$

$$= \underbrace{\sum_{i=1}^{s} B_i g_i}_{\text{proved multideg} < \delta} + \underbrace{(\ \ldots\ )}_{\sum F_i g_i}$$

$$= \sum_{i=1}^{s} \underbrace{H_i g_i}_{\text{multideg} < \delta}$$

contradiction.

Example: twisted cubic

- Let $G = \{y - x^2, z - x^3\}$ with monomial order $\underline{y > z > x}$

$$S(y-x^2,\ z-x^3) = \frac{yz}{y}(y-x^2) - \frac{yz}{z}(z-x^3)$$

$$= yz - zx^2 - yz + yx^3 = yx^3 - zx^2$$

$q_1 \quad x^3$

$q_2 \quad -x^2$

$\rightarrow y - x^2$

$\rightarrow z - x^3$

$$\begin{array}{l} yx^3 - zx^2 \\ \underline{yx^3 - x^5} \\ -zx^2 + x^5 \\ -zx^2 + x^5 = 0 \end{array}$$

$r = 0$

$\therefore$ G is Gröbner basis

Buchberger's Algorithm

- From Buchberger's criterion, we can devise a natural algorithm to compute Groebner bases:
- **Input:** $I = (f_1, \ldots, f_s)$
- **Output:** Groebner basis G for I

[4] Or the ascending chain condition on the monomial ideal $LT(I)$, for the fancy language ones

Buchberger's Algorithm

- From Buchberger's criterion, we can devise a natural algorithm to compute Groebner bases:
- **Input:** $I = (f_1, \ldots, f_s)$
- **Output:** Groebner basis G for I
  1. Set $G = \{f_1, \ldots, f_s\}$

[4] Or the ascending chain condition on the monomial ideal $LT(I)$, for the fancy language ones

Buchberger's Algorithm

- From Buchberger's criterion, we can devise a natural algorithm to compute Groebner bases:
- **Input:** $I = (f_1, \ldots, f_s)$
- **Output:** Groebner basis G for I
  1. Set $G = \{f_1, \ldots, f_s\}$
  2. While there is $S_{ij} := S(f_i, f_j)$ such that

     $$S_{ij}^G \neq 0$$

     add S_{ij}^{G} to G
  3. Once all $S_{ij}^G = 0$ then return G

[4] Or the ascending chain condition on the monomial ideal $LT(I)$, for the fancy language ones

Buchberger's Algorithm

- From Buchberger's criterion, we can devise a natural algorithm to compute Groebner bases:
- **Input:** $I = (f_1, \ldots, f_s)$
- **Output:** Groebner basis G for I
  1. Set $G = \{f_1, \ldots, f_s\}$
  2. While there is $S_{ij} := S(f_i, f_j)$ such that
  $$S_{ij}^{G} \neq 0$$
  add S_{ij}^{G} to G
  3. Once all $S_{ij}^{G} = 0$ then return G
- Buchberger's criterion shows that this algorithm always returns a Groebner basis!

---

[4] Or the ascending chain condition on the monomial ideal $LT(I)$, for the fancy language ones

Buchberger's Algorithm

- From Buchberger's criterion, we can devise a natural algorithm to compute Groebner bases:

$(LM(f_1), \ldots, LM(f_s)) = J_t$

- **Input:** $I = (f_1, \ldots, f_s)$
- **Output:** Groebner basis G for I

$LM(S_{ij}^G) \in J_t$

1. Set $G = \{f_1, \ldots, f_s\}$
2. While there is $S_{ij} := S(f_i, f_j)$ such that

$J_{t+1} = J_t + (LM(S_{ij}^G))$

$$\boxed{S_{ij}^G \neq 0}$$

$J_t \subset J_{t+1} \subset \cdots$

add S_{ij}^G to G

3. Once all $S_{ij}^G = 0$ then return G

has to stabilize

- Buchberger's criterion shows that this algorithm always returns a Groebner basis!
- Algorithm will terminate because of Dickson's lemma![4]

every time we add S_{ij}^G we are adding a new element to $LM(I)$

[4]Or the ascending chain condition on the monomial ideal $LT(I)$, for the fancy language ones

Buchberger's Algorithm

- From Buchberger's criterion, we can devise a natural algorithm to compute Groebner bases:
- **Input:** $I = (f_1, \ldots, f_s)$
- **Output:** Groebner basis G for I
  1. Set $G = \{f_1, \ldots, f_s\}$
  2. While there is $S_{ij} := S(f_i, f_j)$ such that
  $$S_{ij}^G \neq 0$$
  add S_{ij} to G
  3. Once all $S_{ij}^G = 0$ then return G
- Buchberger's criterion shows that this algorithm always returns a Groebner basis!
- Algorithm will terminate because of Dickson's lemma![4]
- Thus, computing Groebner basis is *decidable*!

[4] Or the ascending chain condition on the monomial ideal $LT(I)$, for the fancy language ones

Reduced Groebner Basis

- Of all Grobener bases for an ideal I, one is special. What makes it special are the following:
  - $LC(p) = 1$ for all $p \in G$
  - For all $p \in G$, no monomial of p lies in $(LT(G) \setminus \{p\})$

$\{g_1, \ldots, g_s\} \longrightarrow \{g_i^{G \setminus \{g_i\}}\}$

$LC(g_i) = 1$

Reduced Groebner Basis

- Of all Grobener bases for an ideal I, one is special. What makes it special are the following:
  - $LC(p) = 1$ for all $p \in G$
  - For all $p \in G$, no monomial of p lies in $(LT(G) \setminus \{p\})$
- These are so-called **reduced Groebner bases**

Reduced Groebner Basis

- Of all Grobener bases for an ideal I, one is special. What makes it special are the following:
    - $LC(p) = 1$ for all $p \in G$
    - For all $p \in G$, no monomial of p lies in $(LT(G) \setminus \{p\})$
- These are so-called **reduced Groebner bases**
- Practice problem: prove that a reduced Groebner basis is *unique*.

Reduced Groebner Basis

- Of all Grobener bases for an ideal I, one is special. What makes it special are the following:
    - $LC(p) = 1$ for all $p \in G$
    - For all $p \in G$, no monomial of p lies in $(LT(G) \setminus \{p\})$
- These are so-called **reduced Groebner bases**
- Practice problem: prove that a reduced Groebner basis is *unique*.
- Why would we want uniqueness?
    - used to test whether two ideals are the same ideal!
    - nice "canonical" basis for the ideal (w.r.t. monomial ordering)

Applications of Groebner Bases

- Solution to *Ideal Membership Problem*:

  Given f, I, simply compute Groebner basis G of I and

$$f \in I \Leftrightarrow \overline{f}^{G} = 0$$

Applications of Groebner Bases

- Solution to *Ideal Membership Problem*:

  Given f, I, simply compute Groebner basis G of I and

$$f \in I \Leftrightarrow f^G = 0$$

- Solving *system of polynomial equations*:
  - Now this is just like doing Gaussian Elimination!

Applications of Groebner Bases

- Solution to *Ideal Membership Problem*:

  Given f, I, simply compute Groebner basis G of I and

  $$f \in I \Leftrightarrow f^G = 0$$

- Solving *system of polynomial equations*:
  - Now this is just like doing Gaussian Elimination!
  - Compute Groebner basis using lex order $x_1 > \ldots > x_n$

Applications of Groebner Bases

- Solution to *Ideal Membership Problem*:

  Given f, I, simply compute Groebner basis G of I and

$$f \in I \Leftrightarrow f^G = 0$$

- Solving *system of polynomial equations*:
  - Now this is just like doing Gaussian Elimination!
  - Compute Groebner basis using lex order $x_1 > \ldots > x_n$
  - Solve the system just like you would solve a linear system:

Applications of Groebner Bases

- Solution to *Ideal Membership Problem*:

  Given f, I, simply compute Groebner basis G of I and

$$f \in I \Leftrightarrow f^G = 0$$

- Solving *system of polynomial equations*:
  - Now this is just like doing Gaussian Elimination!
  - Compute Groebner basis using lex order $x_1 > \ldots > x_n$
  - Solve the system just like you would solve a linear system:
  - Example: $I = (x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z)$

$$x^2 + y^2 + z^2 = 1$$

$$x^2 + z^2 - y = 0$$

$$x = z$$

Applications of Groebner Bases

- Solution to *Ideal Membership Problem*:

  Given f, I, simply compute Groebner basis G of I and

$$f \in I \Leftrightarrow f^G = 0$$

- Solving *system of polynomial equations*:
  - Now this is just like doing Gaussian Elimination!
  - Compute Groebner basis using lex order $x_1 > \ldots > x_n$
  - Solve the system just like you would solve a linear system:
  - Example: $I = (x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z)$
  - Groebner basis for the above ideal (x > y > z)

$$G = \{\underbrace{x - z}_{x}, \underbrace{y - 2z^2}_{y}, \underbrace{z^4 + (1/2)z^2 - 1/4}\}$$

get the roots

$z = \alpha_1, \alpha_2, \alpha_3, \alpha_4$

Applications of Groebner Bases

- Solution to *Ideal Membership Problem*:

  Given f, I, simply compute Groebner basis G of I and

$$f \in I \Leftrightarrow f^G = 0$$

- Solving *system of polynomial equations*:
  - Now this is just like doing Gaussian Elimination!
  - Compute Groebner basis using lex order $x_1 > \ldots > x_n$
  - Solve the system just like you would solve a linear system:
  - Example: $I = (x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z)$
  - Groebner basis for the above ideal

$V(I) = 4$ pts

$$G = \{x - z, y - 2z^2, \underline{z^4 + (1/2)z^2 - 1/4}\}$$

  - z is determined by last equation
  - propagate solution by "going up" the other equations!

- Problems with Division Algorithm & Hilbert Basis Theorem
- Gröbner Basis
- Buchberger's Algorithm
- Conclusion
- Acknowledgements

Conclusion

- Today we learned about Groebner bases and their main property
- This “fixes” all the problems that we had with our division algorithm
- Proved Hilbert Basis Theorem
- Proved Buchberger’s criterion, which allows us to test whether a basis is a Groebner basis
- Proved decidability of finding Groebner basis for any ideal
- Used Groebner bases to solve *ideal membership problem* and *system of polynomial equations*
- If anyone would like to present the refinement on Buchberger’s Algorithms from CLO 2.10, I can give bonus homework points :)

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)