Lecture 14: Gröbner Bases and Buchberger's Algorithm

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

March 1, 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 $(F_1, \dots, F_s)$ then we know $G \in (F_1, \dots, F_s)$
- 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 $x^2 \in (f_1, f_2)$

$$-f_1 y + f_2 \cdot x = \cancel{x^3y} - \cancel{2xy^2} + x^2 - \cancel{x^3y} + \cancel{2xy^2}$$

$$= x^2$$

$f_1 = x^3 - 2xy$

$f_2 = x^2y - 2y^2 + x$

$g = x^2$

lex

$q_1 \quad 0$

$q_2 \quad 0$

$g = f_1 \cdot 0 + f_2 \cdot 0 + x^2$

$= f_2 \cdot 0 + f_1 \cdot 0 + x^2$

$$\begin{array}{l|l} x^3 - 2xy & \\ x^2y - 2y^2 + x & x^2 \\ \hline \end{array}$$

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

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

- 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 $LT(I)$

Moto: no leading monomial left behind

$$LT(I) := \{ LT(f) \mid f \in I \}$$

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

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 $LT(I)$

$$f_1 = x^3 - 2xy \qquad f_2 = x^2y - 2y^2 + x$$

$$\underset{\underset{x^2}{\Downarrow}}{\boxed{LM((f_1, f_2))}} \underset{\supset}{\neq} \boxed{(LT(f_1), LT(f_2))} \qquad x^2 \in (f_1, f_2)$$

$$\underbrace{(LT(f_1), LT(f_2))}_{(x^3,\, x^2y)}$$

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

Hilbert Basis theorem: $\mathbb{F}[x_1, \ldots, x_n]$ all ideals are 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

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 $g_1, \ldots, g_s \in \underline{I}$ such that $\underline{LM(I)} = (\underline{LM(g_1)}, \ldots, \underline{LM(g_s)})$

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

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

    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!

$f \in I \qquad (g_1, \dots, g_s)$

$\Longrightarrow \mathrm{LT}(f) \in (\underline{\mathrm{LM}(g_1)}, \dots, \underline{\mathrm{LM}(g_s)})$ (*)

$\Longrightarrow \exists\ h_1, \dots, h_s$ s.t.

division algorithm

$\boxed{f - h_1 g_1 - h_2 g_2 - \dots - h_s g_s} \in I$

and $\mathrm{LT}(f - h_1 g_1 - h_2 g_2 - \dots - h_s g_s)$

$< \mathrm{LT}(f)$

$\Longrightarrow$ (by (*)) we will never add to remainder

$\Longrightarrow$ when division algorithm terminates must have 0 remainder.

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 monomial 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 $f = g + r$
- Division algorithm gives existence of r
- Uniqueness comes from fact that if r, r' are remainders, then $r - r' \in I \Rightarrow r = r'$ by division algorithm

$f = g + r$
$= g' + r'$

$\underline{r - r'} = \underline{g' - g} \in I$

$\Rightarrow$ division

G 0 remainder.

[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?

(1) recognize when basis is Gröbner basis?

(2) can we construct one?

[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

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

S-polynomials they "cancel" the leading terms of f, g

$f_1 = x^3 - 2xy \quad f_2 = x^2y - 2y^2 + x$

$LCM(x^3, x^2y) = x^3y$

$$\frac{x^3y}{1 \cdot x^3} f_1 - \frac{x^3y}{x^2y} \cdot f_2 = y f_1 - x f_2 = x^2$$

[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

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

- 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.

$LCM(x^3y^2, x^4y) = x^4y^2$

$$\frac{x^4y^2}{1 \cdot x^3y^2} f - \frac{x^4y^2}{3 \cdot x^4y} g =$$

$$= x(\cancel{x^3y^2} - x^2y^3) - \frac{y}{3}(\cancel{3x^4y} + y^2) = -x^3y^3 - \frac{y^3}{3}$$

---

[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

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

- 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 $\mathrm{mdeg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\mathrm{mdeg}(p_1 + \cdots + p_s) < \delta$, 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 $i, j \in [s]$

leading term got cancelled.

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 $\text{mdeg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\text{mdeg}(p_1 + \cdots + p_s) < \delta$, 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 $c_i \cdot \mathbf{x}^\delta = LT(p_i)$

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 $\text{mdeg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\text{mdeg}(p_1 + \cdots + p_s) < \delta$, 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. $\text{mdeg}(p_1 + \cdots + p_s) < \delta \Rightarrow \underline{c_1 + \cdots + c_s = 0}$

$$(p_1 + \cdots + p_s)_\delta = c_1 x^\delta + c_2 x^\delta + \cdots + c_s x^\delta = 0$$

$$\Rightarrow \boxed{c_1 + c_2 + \cdots + c_s = 0}$$

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 $\text{mdeg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\text{mdeg}(p_1 + \cdots + p_s) < \delta$, 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. $\text{mdeg}(p_1 + \cdots + p_s) < \delta \Rightarrow c_1 + \cdots + c_s = 0$
  3. Since p_i, p_j have same leading monomial

$LCM(x^\delta, x^\delta) = x^\delta$

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

$$S(p_i, p_j) = \frac{x^\delta}{\underbrace{LT(p_i)}_{c_i x^\delta}} p_i - \frac{x^\delta}{\underbrace{LT(p_j)}_{c_j x^\delta}} \cdot p_j$$

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 $\text{mdeg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\text{mdeg}(p_1 + \cdots + p_s) < \delta$, 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. $\text{mdeg}(p_1 + \cdots + p_s) < \delta \Rightarrow \boxed{c_1 + \cdots + c_s = 0}$
  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)

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

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

$$-\frac{c_s}{c_s}$$

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 $\mathrm{mdeg}(p_i) = \delta \in \mathbb{N}^n$ for all $i \in [s]$ such that $\mathrm{mdeg}(p_1 + \cdots + p_s) < \delta$, 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. $\mathrm{mdeg}(p_1 + \cdots + p_s) < \delta \Rightarrow c_1 + \cdots + c_s = 0$
  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)
  $$\sum_{i=1}^{s-1} c_i \cdot \underline{S(p_i, p_s)} = p_1 + \cdots + p_s$$
  5. note that $\underline{\mathrm{mdeg}(S(p_i, p_j))} < \underline{\delta}$ mdegree decreasing!

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.

$I \quad (f_1, \ldots, f_s)$

$S(f_i, f_j)$ divide by $\langle f_1, \ldots, f_s \rangle$

using division algorithm

if all remainders are zero

then $\{f_1, \ldots, f_s\}$ is Gröbner basis.

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.

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 $\underline{f \in I}$, we have that

$$\underline{LT(f)} \in (\underline{LT(g_1), \ldots, LT(g_s)}) = LM(I)$$

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)

$$f = \underline{g_1} h_1 + \cdots + g_s h_s$$

in the most efficient way

where $\underline{\mathrm{mdeg}(f)} \leq \max_i(\mathrm{mdeg}(g_i h_i))$

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)

$$\boxed{f = g_1 h_1 + \cdots g_s h_s}$$

  where $\mathrm{mdeg}(f) \leq \max_i(\mathrm{mdeg}(g_i h_i))$
- 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 $\mathrm{mdeg}(f) \leq \max_i(\mathrm{mdeg}(g_i h_i))$

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

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

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

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

- 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)

mdeg(f) = x^γ

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

$x^\gamma \leq LM(g_s h_s)$

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

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

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

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

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

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

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

$$\underbrace{\mathrm{mdeg}(f)}_{x^{\gamma}} = \underbrace{\mathrm{mdeg}(g_i h_i)}_{x^{\gamma_i} x^{\nu_i}} \Rightarrow LM(f) \in (LM(g_1), \ldots, LM(g_s))$$

$\gamma = \gamma_i + \nu_i \Rightarrow x^{\gamma_i} \mid x^{\gamma}$

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

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

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

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

- So need to see what happens when $\boxed{\delta > \mathrm{mdeg}(f)}$

Proof of Buchberger's Criterion

- We are now in case: $\mathrm{mdeg}(f) < \delta$
- 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

$\overline{f}^G = 0$ f divided by $\langle g_1, \dots, g_s \rangle$ has zero remainder.

[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: $\text{mdeg}(f) < \delta$
- 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:

[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: $\mathrm{mdeg}(f) < \delta$
- 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:
- $\mathrm{mdeg}(f) < \delta \Rightarrow$ component of multi-degree δ must vanish

$$\boxed{\mathrm{mdeg}(g_i h_i) = \delta}$$

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

$$f = \underbrace{[g_1 h_1 + \cdots + g_s h_s]_\delta}_{LT(h_1)LT(g_1) + \cdots + LT(g_s)LT(h_s)} + \sum_{\gamma < \delta} [g_1 h_1 + \cdots + g_s h_s]_\gamma$$

$$= \underbrace{LT(h_1) g_1 + \cdots + LT(h_s) \cdot g_s}_{\text{each Polynomial has mdeg} = \delta} + \underbrace{\sum_{i=1}^{s} \overbrace{(h_i - LT(h_i))}^{< LT(h_i)} g_i}_{\mathrm{mdeg} < \delta}$$

[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: $\text{mdeg}(f) < \delta$
- 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:
- $\text{mdeg}(f) < \delta \Rightarrow$ component of multi-degree δ must vanish
- Now we use our lemma over $\underline{LT(h_1) \cdot g_1 + \cdots + LT(h_s) \cdot g_s}$ to decrease its multi-degree via S-polynomials

$LT(h_i) g_i = p_i \qquad \text{mdeg}(p_i) = \delta$

[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: $\text{mdeg}(f) < \delta$
- 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:
- $\text{mdeg}(f) < \delta \Rightarrow$ 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

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

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: $\text{mdeg}(f) < \delta$
- 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:
- $\text{mdeg}(f) < \delta \Rightarrow$ 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

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

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

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

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

Proof of Buchberger's Criterion

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

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

Proof of Buchberger's Criterion

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

$$\text{mdeg}(A_i g_i) \le \text{mdeg}(S(g_i, g_j))$$

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

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

$$B_k = x^{\delta - \gamma_{ij}} \cdot A_k$$

Proof of Buchberger's Criterion

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

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

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

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

mdeg(S(pi,pj)) < δ

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

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

=

by property of S-polynomials

mdeg(Aigi)

Proof of Buchberger's Criterion

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

$$\text{mdeg}(A_i g_i) \le \text{mdeg}(S(g_i, g_j))$$

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

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

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

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

by property of S-polynomials

- By our S-polynomial lemma, we have

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

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

Proof of Buchberger's Criterion

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

$$\|$$

$$f = \underbrace{\sum c_i g_i}_{\text{mdeg} < \delta} + \underbrace{\text{sum of stuff mdeg} < \delta}_{\sum E_i g_i}$$

contradicts minimality of δ

Example: twisted cubic

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

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

Buchberger's criterion

[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!

[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]

$S^G \neq 0$

$\Rightarrow$ remainder of S by G S^G

$LM(S^G) \notin (LM(f_1), \ldots, LM(f_s))$

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

$$(LM(f_1), \dots, LM(f_s)) \not\ni LM(S^G)$$

$$\Rightarrow (LM(f_1), \dots, LM(f_s)) \subsetneq (LM(f_1), \dots, LM(f_s), LM(S^G))$$

every time we add a new S-polynomial we are strictly increasing the monomial ideal

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 $(LT(G) \setminus \{p\})$

$G = \{p_1, \ldots, p_s\}$

$p_i \longleftrightarrow \frac{p_i}{LC(p_i)}$

$LC(p_i) = \underline{1}$

$p_i^{G \setminus p_i}$

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

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

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 $x_1 > \ldots > x_n$

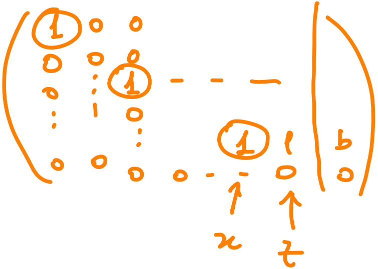
Applications of Groebner Bases

- 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:



$$\boxed{x = b - t}$$

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: $I = (x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z)$

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

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

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

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

  - 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 :)~~

could be great final project

(references there)

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)