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 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*
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 \( x^2 \in (f_1, f_2) \)

\[
- f_1y + f_2 \cdot x = x^3y - 2xy^2 + x^2 - x^3y + 2xy^2
\]

\[
= x^2
\]
\[ f_1 = x^3 - 2xy \]
\[ f_2 = x^2y - 2y^2 + x \]
\[ g = x^2 \]

\[ g = f_1 \cdot 0 + f_2 \cdot 0 + x^2 \]

\[ g = f_2 \cdot 0 + f_1 \cdot 0 + x^2 \]
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 \( I \subseteq \mathbb{F}[x] \) 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 \( LT(I) \)

\[ \mathbf{x} = (x_1, \ldots, x_n) \]

**Note:** 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 $I \subseteq \mathbb{F}[x]$ 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 \textit{finitely generated}
Ideal of Leading Terms & Hilbert Basis Theorem

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

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

$LM((f_1, f_2)) \neq (LT(f_1), LT(f_2))$

$x^2 \in (f_1, f_2)$

$(x^3, x^2y)$
Ideal of Leading Terms & Hilbert Basis Theorem

- Given ideal $I \subseteq \mathbb{F}[x]$ 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 $I \subseteq \mathbb{F}[x]$ 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 \( I \subseteq \mathbb{F}[x] \) 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 \textit{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 \textit{strictly contained} in \( LT(I) \)

- Now we are ready to prove Hilbert’s basis theorem:
  - Let \( I \subseteq \mathbb{F}[x] \) be an ideal
  - By Dickson’s lemma, \( LM(I) \) is finitely generated
Ideal of Leading Terms & Hilbert Basis Theorem

Given ideal \( I \subseteq \mathbb{F}[x] \) 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 \( I \subseteq \mathbb{F}[x] \) be an ideal
- By Dickson’s lemma, \( LM(I) \) is finitely generated
- Let \( g_1, \ldots, g_s \in I \) such that \( LM(I) = (LM(g_1), \ldots, LM(g_s)) \)

\[(g_1, \ldots, g_s) \subseteq I\]
Ideal of Leading Terms & Hilbert Basis Theorem

Given ideal \( I \subseteq \mathbb{F}[x] \) 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 \textit{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 \textit{strictly contained} in \( LT(I) \)

Now we are ready to prove Hilbert’s basis theorem:

- Let \( I \subseteq \mathbb{F}[x] \) 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!
\[ f \in I \quad (g_1, \ldots, g_n) \]

\[ \Rightarrow \quad \text{LT}(f) \in (\text{LM}(g_1), \ldots, \text{LM}(g_n)) \quad (\star) \]

\[ \Rightarrow \quad \exists \ h_1, \ldots, h_n \text{ s.t.} \]

\[ \text{division algorithm} \]

\[ \frac{f - h_1 g_1 - h_2 g_2 - \cdots - h_n g_n}{(f - h_1 g_1 - h_2 g_2 - \cdots - h_n g_n)} \in I \]

and \[ \text{LT} (f - h_1 g_1 - h_2 g_2 - \cdots - h_n g_n) \leq \text{LT}(f) \]

\[ \Rightarrow (\text{by (\star)}) \text{ we will never add to remainder} \]

\[ \Rightarrow \text{ when division algorithm terminates must have 0 remainders} . \]
- Problems with Division Algorithm & Hilbert Basis Theorem

- Gröbner Basis

- Buchberger’s Algorithm

- Conclusion

- Acknowledgements
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 $LM(I)$.

$\textit{no leading monomial left behind}$

---

$^1$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 $f \in \mathbb{F}[x]$ there is a unique $r \in \mathbb{F}[x]$ 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 Groebner basis for $I$, then given $f \in \mathbb{F}[x]$ there is a unique $r \in \mathbb{F}[x]$ 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* $\text{LM}(I)$

**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 Groebner basis for $I$, then given $f \in \mathbb{F}[x]$ there is a unique $r \in \mathbb{F}[x]$ with the following properties:
  1. no term of $r$ is divisible by any $\text{LM}(g_i)$
  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

\(^1\)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:** given two polynomials \( f, g \in \mathbb{F}[x] \), let \( x^\gamma = LCM(LM(f), LM(g)) \). Then, the S-polynomial of \( f, g \) is

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

S-polynomials they "cancel" the leading terms of \( f, g \):

\[
S(f, g) = x^3y - \frac{x^3y}{y} \cdot \frac{1}{y} = x^2
\]

\( \text{LCM}(x^3, x^2y) = x^3y \)

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:**

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

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

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

\[
LCM(x^3y^2, x^4y) = x^4y^2
\]

\[
f = \frac{x^4y^2}{x^4y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = -x^3y^3 - \frac{y^3}{3}
\]

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

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

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

- S-polynomials are designed to produce cancellations of leading terms.

---

2This name is a shortening for “syzygy polynomials” since they are syzygies over the monomial ideal.
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 \( i, j \in [s] \).
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 $c_i = \text{LC}(p_i)$, so $c_i \cdot x^\delta = \text{LT}(p_i)$
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 $c_i = \text{LC}(p_i)$, so $c_i \cdot x^\delta = \text{LT}(p_i)$
2. $\text{mdeg}(p_1 + \cdots + p_s) < \delta \Rightarrow c_1 + \cdots + c_s = 0$

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

$\Rightarrow \left[ c_1 + c_2 + \cdots + c_s = 0 \right]$
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 $c_i = \text{LC}(p_i)$, so $c_i \cdot x^\delta = \text{LT}(p_i)$
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

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

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

$$S(p_i, p_j) = \frac{x^\delta}{\text{LT}(p_i)} \cdot p_i - \frac{x^\delta}{\text{LT}(p_j)} \cdot p_j$$
How Cancellation Happens: \( S \)-polynomial lemma

- Next lemma shows that every cancellation of leading terms amongst polynomials of same degree happen \textit{because of} \( S \)-polynomial

\textbf{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 \( c_i = \text{LC}(p_i) \), so \( c_i \cdot x^\delta = \text{LT}(p_i) \)
2. \( \text{mdeg}(p_1 + \cdots + p_s) < \delta \Rightarrow \sum_{i=1}^{s} c_i = 0 \)
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)

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

\[
\sum_{i=1}^{\Delta - 1} c_i \left( \frac{1}{c_i} p_i - \frac{1}{c_\Delta} p_\Delta \right) = \sum_{i=1}^{\Delta - 1} p_i - p_\Delta \frac{c_i + \cdots + c_{\Delta-1}}{c_\Delta}
\]
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 $c_i = \text{LC}(p_i)$, so $c_i \cdot x^\delta = \text{LT}(p_i)$
  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

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

4. Thus, by using (2)

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

5. note that $\text{mdeg}(S(p_i, p_j)) < \delta$ mdegree decreasing!
Buchberger’s Criterion

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

Let \( I \subseteq \mathbb{F}[x] \) 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.

\[
\begin{align*}
I & \subseteq \mathbb{F}[x] \\
S(g_i, g_j) \text{ divide by } & <f_1, \ldots, f_s> \\
\text{using division algorithm} & \\
\text{if all remainders are zero} & \text{ then } \{f_1, \ldots, f_s\} \text{ is Gröbner basis.}
\end{align*}
\]
Buchberger’s Criterion

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

  Let $I \subseteq \mathbb{F}[x]$ 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 $I \subseteq \mathbb{F}[x]$ 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

$$\text{LT}(f) \in (\text{LT}(g_1), \ldots, \text{LT}(g_s)) = \text{LM}(I)$$
Buchberger’s Criterion

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

Let \( I \subseteq \mathbb{F}[x] \) 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)

\[
f = g_1h_1 + \cdots + g_sh_s
\]

where \( \text{mdeg}(f) \leq \max_i(\text{mdeg}(g_ih_i)) \)
Buchberger’s Criterion

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

  Let $I \subseteq \mathbb{F}[x]$ 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 $\text{mdeg}(f) \leq \max_i(\text{mdeg}(g_i h_i))$

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

- Take representation of \textit{lowest multidegree}, that is, one for which

\[ \delta := \max_i (\text{mdeg}(g_i h_i)) \text{ is minimum} \]
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 $\text{mdeg}(f) \leq \max_i(\text{mdeg}(g_i h_i))$

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

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

  is minimum

- Such minimum $\delta$ 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)

\[
mdeg(f) = x^r \quad f = g_1h_1 + \cdots + g_sh_s
\]

where \( mdeg(f) \leq \max_i(mdeg(g_ih_i)) \)

- Take representation of lowest multidegree, that is, one for which \( \delta := \max_i(mdeg(g_ih_i)) \) is minimum

- Such minimum \( \delta \) exists by the well-ordering of monomial order

- In particular, \( mdeg(f) \leq \delta \)
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 \( \text{mdeg}(f) \leq \max_i (\text{mdeg}(g_i h_i)) \)

- Take representation of \textit{lowest multidegree}, that is, one for which

\[
\delta := \max_i (\text{mdeg}(g_i h_i)) \text{ is minimum}
\]

- Such minimum \( \delta \) exists by the well-ordering of monomial order

- In particular, \( \text{mdeg}(f) \leq \delta \)

- If \( \text{mdeg}(f) = \delta \), then there is some \( i \in [s] \) such that

\[
\text{mdeg}(f) = \text{mdeg}(g_i h_i) \Rightarrow \text{LM}(f) \in (\text{LM}(g_1), \ldots, \text{LM}(g_s))
\]
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 \( \text{mdeg}(f) \leq \max_i (\text{mdeg}(g_i h_i)) \)

- Take representation of \textit{lowest multidegree}, that is, one for which

\[
\delta := \max_i (\text{mdeg}(g_i h_i)) \text{ is minimum}
\]

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

\[
\text{mdeg}(f) = \text{mdeg}(g_i h_i) \Rightarrow \text{LM}(f) \in (\text{LM}(g_1), \ldots, \text{LM}(g_s))
\]

- So need to see what happens when \( \delta > \text{mdeg}(f) \)
Proof of Buchberger’s Criterion

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

\[ f^G = 0 \quad \text{if divided by } \langle g_1, \ldots, g_s \rangle \text{ has zero remainder.} \]

---

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 \( S(g_i, g_j)^G = 0 \) to obtain another expression of \( f \in I \) with smaller \( \delta \)
- Let’s isolate part of highest multi-degree:

\[ \text{This is a short-hand notation to say that the division by } G \text{ is zero} \]
Proof of Buchberger’s Criterion

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

\[
\begin{align*}
    f &= g_i h_1 + \ldots + g_0 h_0 \\
    f &= \left[ g_i h_1 + \ldots + g_0 h_0 \right]_\delta + \sum_{\delta < \delta} \left[ g_i h_1 + \ldots + g_0 h_0 \right]_\delta \\
    &= \text{LT}(h_1) \text{LT}(g_i) + \ldots + \text{LT}(g_0) \text{LT}(h_0) \\
    &= \text{LT}(h_1) g_i + \ldots + \text{LT}(h_0) g_0 + \sum_{i = 1}^{\delta} \left( h_i - \text{LT}(h_i) \right) g_i
\end{align*}
\]

\( \text{mdeg} < \delta \)

\( ^3 \)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 \( S(g_i, g_j)^G = 0^3 \) to obtain another expression of \( f \in I \) with smaller \( \delta \)
- Let’s isolate part of highest multi-degree:
- \( \text{mdeg}(f) < \delta \Rightarrow \) component of multi-degree \( \delta \) 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

\[
LT(h_i) \cdot g_i = p_i \quad \text{mdeg}(p_i) = \delta
\]

\(^3\)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 \( S(g_i, g_j)^G = 0 \) to obtain another expression of \( f \in I \) with smaller \( \delta \)
- Let’s isolate part of highest multi-degree:
  \( \text{mdeg}(f) < \delta \Rightarrow \) component of multi-degree \( \delta \) 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

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

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: \( \text{mdeg}(f) < \delta \)
- In this case we will use the fact that \( S(g_i, g_j)^G = 0 \) to obtain another expression of \( f \in I \) with smaller \( \delta \)
- Let’s isolate part of highest multi-degree:
- \( \text{mdeg}(f) < \delta \Rightarrow \) component of multi-degree \( \delta \) 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

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

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

- \( S(g_i, g_j)^G = 0 \Rightarrow S(g_i, g_j) = A_1g_1 + \cdots + A_sg_s \)

\[
\text{mdeg}(A_i g_i) \leq \text{mdeg}(S(g_i, g_j))
\]

\(^3\) This is a short-hand notation to say that the division by \( G \) is zero
Proof of Buchberger’s Criterion

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

\[ \text{mdeg}(A_i g_i) \leq \text{mdeg}(S(g_i, g_j)) \]
Proof of Buchberger’s Criterion

- $S(g_i, g_j)^G = 0 \Rightarrow S(g_i, g_j) = A_1 g_1 + \cdots + A_s g_s$
  \[
  \text{mdeg}(A_i g_i) \leq \text{mdeg}(S(g_i, g_j))
  \]

- Multiplying above by $x^{\delta - \gamma_{ij}}$
  \[
  S(p_i, p_j) = x^{\delta - \gamma_{ij}} \cdot S(g_i, g_j) = B_1 g_1 + \cdots + B_s g_s
  \]
  \[
  B_k = x^{\delta - \gamma_{ij}} \cdot A_n
  \]
Proof of Buchberger’s Criterion

- \( S(g_i, g_j)^G = 0 \Rightarrow S(g_i, g_j) = A_1 g_1 + \cdots + A_s g_s \)
  \[ \text{mdeg}(A_i g_i) \leq \text{mdeg}(S(g_i, g_j)) \]

- Multiplying above by \( x^{\delta - \gamma_{ij}} \)
  \[ S(p_i, p_j) = x^{\delta - \gamma_{ij}} \cdot S(g_i, g_j) = B_1 g_1 + \cdots + B_s g_s \]

- When \( B_i g_i \neq 0 \) by the first bullet
  \[ \text{mdeg}(B_i g_i) \leq \text{mdeg}(x^{\delta - \gamma_{ij}} \cdot S(g_i, g_j)) < \delta \]
  by property of \( S \)-polynomials

- by property of \( S \)-polynomials
Proof of Buchberger’s Criterion

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

\[ \text{mdeg}(A_i g_i) \leq \text{mdeg}(S(g_i, g_j)) \]

- Multiplying above by \( x^{\delta - \gamma_{ij}} \)

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

- When \( B_i g_i \neq 0 \) by the first bullet

\[ \text{mdeg}(B_i g_i) \leq \text{mdeg}(x^{\delta - \gamma_{ij}} \cdot S(g_i, g_j)) < \delta \]

by property of S-polynomials

- By our S-polynomial lemma, we have

\[ \sum_{i=1}^{s} \text{LT}(h_i) \cdot g_i = \sum_{i \neq j} a_{ij} \cdot S(p_i, p_j) = C_1 g_1 + \cdots + C_s g_s \]

where \( \text{mdeg}(C_i g_i) < \delta \)
Proof of Buchberger’s Criterion

\[ f = \sum \text{LT}(h_i) g_i \underbrace{\text{mod}_\delta}_\text{I}\ ] + \sum \text{stuff of mod}_\delta < \delta \]

\[ f = \sum c_i g_i \underbrace{\text{mod}_\delta}_\text{mddeg} < \delta \]

contradicts

\[ \sum \mathbb{E} : g_i \underbrace{\text{minimality of } \delta}_\text{sum of stuff of mod}_\delta < \delta \]
Example: twisted cubic

- Let $G = \{y - x^2, z - x^3\}$ with monomial order $y > z > x$
Problems with Division Algorithm & Hilbert Basis Theorem

Gröbner Basis

Buchberger’s Algorithm

Conclusion

Acknowledgements
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 \( I \)

\[^4\text{Or the ascending chain condition on the monomial ideal } LT(I), \text{ for the fancy language ones}\]
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 \( I \)
  - Set \( G = \{f_1, \ldots, f_s\} \)

---

\[^4\text{Or the ascending chain condition on the monomial ideal } LT(I), \text{ for the fancy language ones} \]
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 $G$

---

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!\(^4\)

---

\(^4\)Or the ascending chain condition on the monomial ideal \( LT(I) \), for the fancy language ones
\( (\text{LM}(d_1), \ldots, \text{LM}(f_0)) \neq \text{LM}(S^G) \)

\[ \Rightarrow (\text{LM}(d_1), \ldots, \text{LM}(f_0)) \subsetneq (\text{LM}(d_1), \ldots, \text{LM}(f_0), \text{LM}(g)) \]

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
Reduction Grobner Basis

Of all Grobner bases for an ideal \( I \), one is special. What makes it special are the following:

- \( \text{LC}(p) = 1 \) for all \( p \in G \)
- For all \( p \in G \), no monomial of \( p \) lies in \( (\text{LT}(G) \setminus \{p\}) \)

\[ G = \{ p_1, \ldots, p_n \} \]

\[ \text{LC}(p_i) = 1 \]

\[ p_i \in G \setminus \{ p_i \} \]
Of all Grobner bases for an ideal $I$, one is special. What makes it special are the following:

- $\text{LC}(p) = 1$ for all $p \in G$
- For all $p \in G$, no monomial of $p$ lies in $(\text{LT}(G) \setminus \{p\})$

These are so-called \textit{reduced Groebner bases}
Reduced Groebner Basis

Of all Groebner 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

\[
f \in I \iff f^G = 0
\]
Applications of Groebner Bases

- **Solution to Ideal Membership Problem:**
  
  Given $f, I$, simply compute Groebner basis $G$ of $I$ and
  
  \[ f \in I \iff f^G = 0 \]

- **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
  
  \[
  f \in I \iff f^G = 0
  \]

- **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

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

• 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
  
  \[
  f \in I \iff f^G = 0
  \]

- **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

  \[
  f \in I \iff f^G = 0
  \]

- 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

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

  *Univariate in \( z \)
Applications of Groebner Bases

- **Solution to *Ideal Membership Problem***:
  
  Given \( f, I \), simply compute Groebner basis \( G \) of \( I \) and
  
  \[
  f \in I \iff f^G = 0
  \]

- **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
    
    \[
    G = \{x - z, y - 2z^2, z^4 + (1/2)z^2 - 1/4\}
    \]
  
  - \( z \) 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
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 (reference 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)