Gröbner Bases

1. S-polynomials
   - eliminating the leading term
   - Buchberger's criterion and algorithm
2. Wavelet Design
   - construct wavelet filters
3. Proof of the Buchberger Criterion
   - two lemmas
   - proof of the Buchberger criterion
   - termination and elimination

MCS 563 Lecture 6
Analytic Symbolic Computation
Jan Verschelde, 24 January 2011

Gröbner Bases

S-polynomials

to eliminate the leading term

The leading term of a polynomial f is denoted by $\mathrm{LT}(f)$.

Any term is the product of a coefficient and a monomial, the leading monomial of is denoted by $\mathrm{LM}(f)$.

$\mathrm{LCM}(\mathbf{x}^\mathbf{a}, \mathbf{x}^\mathbf{a})$ is the least common multiple of $\mathbf{x}^\mathbf{a}$ and $\mathbf{x}^\mathbf{b}$.

To eliminate the leading term of two nonzero polynomials p and q, we compute an S-polynomial (S = Subtraction):

$$S(p,q) = \frac{\mathrm{LCM}(\mathrm{LM}(p),\mathrm{LM}(q))}{\mathrm{LT}(p)} \cdot p - \frac{\mathrm{LCM}(\mathrm{LM}(p),\mathrm{LM}(q))}{\mathrm{LT}(q)} \cdot q.$$

If p and q belong to the same ideal I, then $S(p,q) \in I$.

S-polynomials

to eliminate the leading term

The leading term of a polynomial f is denoted by $\mathrm{LT}(f)$.

Any term is the product of a coefficient and a monomial, the leading monomial of is denoted by $\mathrm{LM}(f)$.

$\mathrm{LCM}(\mathbf{x}^\mathbf{a}, \mathbf{x}^\mathbf{a})$ is the least common multiple of $\mathbf{x}^\mathbf{a}$ and $\mathbf{x}^\mathbf{b}$.

To eliminate the leading term of two nonzero polynomials p and q, we compute an S-polynomial ($S =$ Subtraction):

$$S(p,q) = \frac{\mathrm{LCM}(\mathrm{LM}(p), \mathrm{LM}(q))}{\mathrm{LT}(p)} \cdot p - \frac{\mathrm{LCM}(\mathrm{LM}(p), \mathrm{LM}(q))}{\mathrm{LT}(q)} \cdot q.$$

If p and q belong to the same ideal I, then $S(p,q) \in I$.

an example

Applying

$$S(p,q) = \frac{\mathrm{LCM}(\mathrm{LM}(p),\mathrm{LM}(q))}{\mathrm{LT}(p)} \cdot p - \frac{\mathrm{LCM}(\mathrm{LM}(p),\mathrm{LM}(q))}{\mathrm{LT}(q)} \cdot q$$

to $p = xy + 1$ and $q = y^2 - 1$ using $>_{\mathrm{lex}}$ leads to

$$\begin{aligned} S(p,q) &= \frac{\mathrm{LCM}(xy,y^2)}{xy}(xy+1) - \frac{\mathrm{LCM}(xy,y^2)}{y^2}(y^2-1) \\ &= y(xy+1) - x(y^2-1), \text{ as } \mathrm{LCM}(xy,y^2) = xy^2 \\ &= x + y \end{aligned}$$

We used p and q to define an ideal I for which the result of the division algorithm depended on the order.

With $S(p,q) \in I$ we add leading terms to the basis for I.

an example

Applying

$$S(p,q) = \frac{\mathrm{LCM}(\mathrm{LM}(p),\mathrm{LM}(q))}{\mathrm{LT}(p)} \cdot p - \frac{\mathrm{LCM}(\mathrm{LM}(p),\mathrm{LM}(q))}{\mathrm{LT}(q)} \cdot q$$

to $p = xy + 1$ and $q = y^2 - 1$ using $>_{\mathrm{lex}}$ leads to

$$\begin{aligned} S(p,q) &= \frac{\mathrm{LCM}(xy,y^2)}{xy}(xy+1) - \frac{\mathrm{LCM}(xy,y^2)}{y^2}(y^2-1) \\ &= y(xy+1) - x(y^2-1), \text{ as } \mathrm{LCM}(xy,y^2) = xy^2 \\ &= x + y \end{aligned}$$

We used p and q to define an ideal I for which the result of the division algorithm depended on the order.

With $S(p,q) \in I$ we add leading terms to the basis for I.

an example

Applying

$$S(p,q) = \frac{\mathrm{LCM}(\mathrm{LM}(p),\mathrm{LM}(q))}{\mathrm{LT}(p)} \cdot p - \frac{\mathrm{LCM}(\mathrm{LM}(p),\mathrm{LM}(q))}{\mathrm{LT}(q)} \cdot q$$

to $p = xy + 1$ and $q = y^2 - 1$ using $>_{\mathrm{lex}}$ leads to

$$\begin{aligned} S(p,q) &= \frac{\mathrm{LCM}(xy,y^2)}{xy}(xy+1) - \frac{\mathrm{LCM}(xy,y^2)}{y^2}(y^2-1) \\ &= y(xy+1) - x(y^2-1), \text{ as } \mathrm{LCM}(xy,y^2) = xy^2 \\ &= x + y \end{aligned}$$

We used p and q to define an ideal I for which the result of the division algorithm depended on the order.

With $S(p,q) \in I$ we add leading terms to the basis for I.

Gröbner Bases

1. S-polynomials
    - eliminating the leading term
    - Buchberger's criterion and algorithm
2. Wavelet Design
    - construct wavelet filters
3. Proof of the Buchberger Criterion
    - two lemmas
    - proof of the Buchberger criterion
    - termination and elimination

a Gröbner basis for an ideal

A set of polynomials g is a Gröbner basis for an ideal I if

1. $I = \langle g \rangle$ and
2. the leading terms of g generate the ideal of leading terms of the polynomials in I, i.e.: $\langle \mathrm{LT}(g) \rangle = \langle \mathrm{LT}(I) \rangle$.

Theorem (Buchberger's criterion)

A set $g = \{g_1, g_2, \ldots, g_s\}$ is a Gröbner basis if and only if for all pairs g_i and g_j, $i \neq j$, the remainder of the division of $S(g_i, g_j)$ by g equals zero.

This criterion leads to an algorithm for a Gröbner basis.

a Gröbner basis for an ideal

A set of polynomials g is a Gröbner basis for an ideal I if

1. $I = \langle g \rangle$ and
2. the leading terms of g generate the ideal of leading terms of the polynomials in I, i.e.: $\langle \mathrm{LT}(g) \rangle = \langle \mathrm{LT}(I) \rangle$.

Theorem (Buchberger's criterion)

A set $g = \{g_1, g_2, \ldots, g_s\}$ is a Gröbner basis if and only if for all pairs g_i and g_j, $i \neq j$, the remainder of the division of $S(g_i, g_j)$ by g equals zero.

This criterion leads to an algorithm for a Gröbner basis.

the Buchberger algorithm

The Buchberger algorithm to compute a Gröbner basis:

Input: $f = \{f_1, f_2, \dots, f_N\}$, $I = \langle f \rangle$.
Output: $g = \{g_1, g_2, \dots, g_s\}$, $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g) \rangle$.

```
$g := f$;
repeat
    h := g;
    for each pair $(p, q)$, $p \neq q$, $p, q \in g$ do
        $S := S(p, q)$;
        $r :=$ remainder of $S$ after division by $g$;
        if $r \neq 0$
         then $g := g \cup \{S\}$;
        end if;
    end for;
until $g = h$.
```

the Buchberger algorithm

The Buchberger algorithm to compute a Gröbner basis:

Input: $f = \{f_1, f_2, \ldots, f_N\}$, $I = \langle f \rangle$.
Output: $g = \{g_1, g_2, \ldots, g_s\}$, $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g) \rangle$.

```
$g := f$;
repeat
   h := g;
   for each pair $(p, q)$, $p \neq q$, $p, q \in g$ do
      $S := S(p, q)$;
      $r :=$ remainder of $S$ after division by $g$;
      if $r \neq 0$
       then $g := g \cup \{S\}$;
      end if;
   end for;
until $g = h$.
```

the Buchberger algorithm

The Buchberger algorithm to compute a Gröbner basis:

Input: $f = \{f_1, f_2, \ldots, f_N\}$, $I = \langle f \rangle$.
Output: $g = \{g_1, g_2, \ldots, g_s\}$, $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g) \rangle$.

```
$g := f$;
repeat
  h := g;
  for each pair $(p, q)$, $p \neq q$, $p, q \in g$ do
    $S := S(p, q)$;
    $r :=$ remainder of $S$ after division by $g$;
    if $r \neq 0$
     then $g := g \cup \{S\}$;
    end if;
  end for;
until $g = h$.
```

using Macaulay 2

```
$ M2
Macaulay2, version 1.3.1
with packages: ConwayPolynomials, Elimination, Inte
               PrimaryDecomposition, ReesAlgebra, S

i1 : R = QQ[x,y,MonomialOrder => Lex];

i2 : I = ideal(x^2 + 1,x*y - 1);

o2 : Ideal of R

i3 : G = gens gb I

o3 = | y2+1 x+y |
```

We see that $\{y^2 + 1, x + y\}$ is a Gröbner basis for the ideal $\langle x^2 + 1, xy - 1\rangle$ with the lexicographical order.

some more Gröbner basics

Buchberger's algorithm generalizes Euclid's algorithm for the GCD and row reduction for linear systems.

With a Gröbner bases, the division algorithm solves the ideal membership problem.

A Gröbner basis g is called reduced if

1. the leading coefficient of every polynomial in g is 1; and
2. for all $p \in g$, no monomial of p lies in $\langle \mathrm{LT}(g \setminus \{p\}) \rangle$.

Fixing a monomial order,
any nonzero ideal has a unique reduced Gröbner basis.

some more Gröbner basics

Buchberger's algorithm generalizes Euclid's algorithm for the GCD and row reduction for linear systems.

With a Gröbner bases, the division algorithm solves the ideal membership problem.

A Gröbner basis g is called reduced if

1. the leading coefficient of every polynomial in g is 1; and
2. for all $p \in g$, no monomial of p lies in $\langle \mathrm{LT}(g \setminus \{p\}) \rangle$.

Fixing a monomial order,
any nonzero ideal has a unique reduced Gröbner basis.

Gröbner Bases

1. S-polynomials
   - eliminating the leading term
   - Buchberger's criterion and algorithm
2. Wavelet Design
   - construct wavelet filters
3. Proof of the Buchberger Criterion
   - two lemmas
   - proof of the Buchberger criterion
   - termination and elimination

filtering a signal

A filter with input $\{x_n\}$ and output $\{y_n\}$ is completely determined by $\{h_n\}$, the impulse response.

$$x_n \longrightarrow \boxed{h_n} \longrightarrow y_n$$

With the convolution operator $*$, we compute

$$y = h * x = \sum_k x_k h_{n-k}.$$

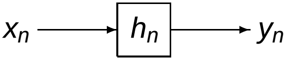
Via the Z-transform, $Z(\{x_n\}) = \sum_n x_n z^{-n}$, $h * x$ becomes

$$Y(z) = H(z)X(z),$$

with $X(z) = Z(\{x_n\})$, $H(z) = Z(\{h_n\})$, and $Y(z) = Z(\{y_n\})$.

filtering a signal

A filter with input $\{x_n\}$ and output $\{y_n\}$ is completely determined by $\{h_n\}$, the impulse response.



With the convolution operator $*$, we compute

$$y = h * x = \sum_k x_k h_{n-k}.$$

Via the Z-transform, $Z(\{x_n\}) = \sum_n x_n z^{-n}$, $h * x$ becomes

$$Y(z) = H(z)X(z),$$

with $X(z) = Z(\{x_n\})$, $H(z) = Z(\{h_n\})$, and $Y(z) = Z(\{y_n\})$.

filter design

The function $H(z)$ is called the transfer function of the filter.

We design a filter by determination of H.

Example of conditions on the transfer function:

1. $h_2 = h_3$, $h_1 = h_4$;
2. $(z+1)^2$ divides $H(z)$;
3. $\displaystyle\sum_n h_n h_{n-2k} = \delta(k)$,
   with $\delta(k) = 1$ if $k = 0$, $\delta(k) = 0$ if $k \neq 0$.

filter design

The function $H(z)$ is called the transfer function of the filter.

We design a filter by determination of H.

Example of conditions on the transfer function:

1. $h_2 = h_3$, $h_1 = h_4$;
2. $(z+1)^2$ divides $H(z)$;
3. $\displaystyle\sum_n h_n h_{n-2k} = \delta(k)$,
   with $\delta(k) = 1$ if $k = 0$, $\delta(k) = 0$ if $k \neq 0$.

a polynomial system

$$\left\{\begin{array}{r} h_0 + h_1 + h_2 + h_3 + h_4 + h_5 + h_6 + h_7 - 1 = 0 \\ h_2h_0 + h_3h_1 + h_4h_2 + h_5h_3 + h_6h_4 + h_7h_5 = 0 \\ h_6h_2 + h_4h_0 + h_5h_1 + h_7h_3 = 0 \\ h_6h_0 + h_7h_1 = 0 \\ h_0 - h_2 - 3h_4 - 5h_6 + 6h_7 + 4h_5 + 2h_3 = 0 \\ h_1 + 3h_3 + 5h_5 + 7h_7 - 6h_6 - 4h_4 - 2h_2 = 0 \\ h_2 - h_3 = 0 \\ h_1 - h_4 = 0 \end{array}\right.$$

Appending the equation

$$h_0 + h_1 + 2h_2 + 3h_3 + 4h_4 + 5h_5 + 6h_6 + 7h_7 - A = 0$$

leads to a more compact Gröbner basis.

Gröbner Bases

1. S-polynomials
   - eliminating the leading term
   - Buchberger's criterion and algorithm
2. Wavelet Design
   - construct wavelet filters
3. Proof of the Buchberger Criterion
   - two lemmas
   - proof of the Buchberger criterion
   - termination and elimination

cancellation of leading terms

Lemma 1

Let $f_1, f_2, \ldots, f_N \in \mathbb{C}[\mathbf{x}]$ *be such that* $\mathrm{LM}(f_i) = \mathbf{x}^\mathbf{a}$*, for all* $i = 1, 2, \ldots, N$*. Consider* $f = \displaystyle\sum_{i=1}^{N} \gamma_i f_i$*, for* $\gamma_i \in \mathbb{C}$*.*
If $\mathrm{LM}(f) < \mathbf{x}^\mathbf{a}$*, then* f *is a linear combination of the S-polynomials* $S(f_i, f_j)$*,* $1 \leq i \neq j \leq N$*.*

Proof. Denote $\mathrm{LT}(f_i) = c_i \mathbf{x}^\mathbf{a}$ for $c_i \in \mathbb{C} \setminus \{0\}$.

For all i, j: $\mathrm{LM}(f_i) = \mathrm{LM}(f_j)$: $S(f_i, f_j) = \frac{1}{c_i} f_i - \frac{1}{c_j} f_j$.

cancellation of leading terms

Lemma 1

Let $f_1, f_2, \ldots, f_N \in \mathbb{C}[\mathbf{x}]$ *be such that* $\mathrm{LM}(f_i) = \mathbf{x}^{\mathbf{a}}$*, for all* $i = 1, 2, \ldots, N$*. Consider* $f = \sum_{i=1}^{N} \gamma_i f_i$*, for* $\gamma_i \in \mathbb{C}$*. If* $\mathrm{LM}(f) < \mathbf{x}^{\mathbf{a}}$*, then* f *is a linear combination of the S-polynomials* $S(f_i, f_j)$*,* $1 \leq i \neq j \leq N$*.*

Proof. Denote $\mathrm{LT}(f_i) = c_i \mathbf{x}^{\mathbf{a}}$ for $c_i \in \mathbb{C} \setminus \{0\}$.

For all i, j: $\mathrm{LM}(f_i) = \mathrm{LM}(f_j)$: $S(f_i, f_j) = \frac{1}{c_i} f_i - \frac{1}{c_j} f_j$.

telescoping sums

proof continued

As $\mathrm{LM}(f) < \mathbf{x}^{\mathbf{a}}$: $\displaystyle\sum_{i=1}^{N} \gamma_i c_i = 0$.

Using telescoping sums in case $N = 3$:

$$\begin{aligned} f &= \gamma_1 f_1 + \gamma_2 f_2 + \gamma_3 f_3 \\ &= \gamma_1 c_1 \left(\frac{1}{c_1} f_1 \right) + \gamma_2 c_2 \left(\frac{1}{c_2} f_2 \right) + \gamma_3 c_3 \left(\frac{1}{c_3} f_3 \right) \\ &= \gamma_1 c_1 \left(\frac{1}{c_1} f_1 - \frac{1}{c_2} f_2 \right) + (\gamma_1 c_1 + \gamma_2 c_2) \left(\frac{1}{c_2} f_2 - \frac{1}{c_3} f_3 \right) \\ &\quad + (\gamma_1 c_1 + \gamma_2 c_2 + \gamma_3 c_3) f_3 \\ &= \gamma_1 c_1 S(f_1, f_2) + (\gamma_1 c_1 + \gamma_2 c_2) S(f_2, f_3), \end{aligned}$$

because $\gamma_1 c_1 + \gamma_2 c_2 + \gamma_3 c_3 = 0$.

The extension for any N is clear. ☐

telescoping sums

proof continued

As $\mathrm{LM}(f) < \mathbf{x}^{\mathbf{a}}$: $\displaystyle\sum_{i=1}^{N} \gamma_i c_i = 0$.

Using telescoping sums in case $N = 3$:

$$\begin{aligned}
f &= \gamma_1 f_1 + \gamma_2 f_2 + \gamma_3 f_3 \\
&= \gamma_1 c_1 \left(\frac{1}{c_1} f_1 \right) + \gamma_2 c_2 \left(\frac{1}{c_2} f_2 \right) + \gamma_3 c_3 \left(\frac{1}{c_3} f_3 \right) \\
&= \gamma_1 c_1 \left(\frac{1}{c_1} f_1 - \frac{1}{c_2} f_2 \right) + (\gamma_1 c_1 + \gamma_2 c_2) \left(\frac{1}{c_2} f_2 - \frac{1}{c_3} f_3 \right) \\
&\quad + (\gamma_1 c_1 + \gamma_2 c_2 + \gamma_3 c_3) f_3 \\
&= \gamma_1 c_1 S(f_1, f_2) + (\gamma_1 c_1 + \gamma_2 c_2) S(f_2, f_3),
\end{aligned}$$

because $\gamma_1 c_1 + \gamma_2 c_2 + \gamma_3 c_3 = 0$.

The extension for any N is clear. ☐

telescoping sums

proof continued

As $\mathrm{LM}(f) < \mathbf{x}^{\mathbf{a}}$: $\displaystyle\sum_{i=1}^{N} \gamma_i c_i = 0$.

Using telescoping sums in case $N = 3$:

$$\begin{array}{rcl} f & = & \gamma_1 f_1 + \gamma_2 f_2 + \gamma_3 f_3 \\ & = & \gamma_1 c_1 \left(\dfrac{1}{c_1} f_1 \right) + \gamma_2 c_2 \left(\dfrac{1}{c_2} f_2 \right) + \gamma_3 c_3 \left(\dfrac{1}{c_3} f_3 \right) \\ & = & \gamma_1 c_1 \left(\dfrac{1}{c_1} f_1 - \dfrac{1}{c_2} f_2 \right) + (\gamma_1 c_1 + \gamma_2 c_2) \left(\dfrac{1}{c_2} f_2 - \dfrac{1}{c_3} f_3 \right) \\ & & + (\gamma_1 c_1 + \gamma_2 c_2 + \gamma_3 c_3) f_3 \\ & = & \gamma_1 c_1 S(f_1, f_2) + (\gamma_1 c_1 + \gamma_2 c_2) S(f_2, f_3), \end{array}$$

because $\gamma_1 c_1 + \gamma_2 c_2 + \gamma_3 c_3 = 0$.
The extension for any N is clear. $\square$

termination of division

Lemma 2

For any $p \in \mathbb{C}[\mathbf{x}]$ *and* $f = (f_1, f_2, \ldots, f_N)$, $f_i \in \mathbb{C}[\mathbf{x}]$ *for* $i = 1, 2, \ldots, N$ *on input, the division algorithm terminates yielding*

$$q_1, q_2, \ldots, q_N, r \in \mathbb{C}[\mathbf{x}] : p = q_1 f_1 + q_2 f_2 + \cdots + q_N f_N + r.$$

Moreover: $\mathrm{LM}(p) = \max\left(\max_{k=1}^{N} (\mathrm{LM}(q_i)\mathrm{LM}(f_i)), \mathrm{LM}(r) \right)$.

Proof. We first show that the division algorithm terminates.

Observe that at each stage of the division algorithm we subtract from r (initialized with p), producing a sequence of polynomials $r_0 = p$, r_1, r_2, ...

termination of division

Lemma 2

For any $p \in \mathbb{C}[\mathbf{x}]$ *and* $f = (f_1, f_2, \ldots, f_N)$, $f_i \in \mathbb{C}[\mathbf{x}]$ *for* $i = 1, 2, \ldots, N$ *on input, the division algorithm terminates yielding*

$$q_1, q_2, \ldots, q_N, r \in \mathbb{C}[\mathbf{x}] : p = q_1 f_1 + q_2 f_2 + \cdots + q_N f_N + r.$$

Moreover: $\mathrm{LM}(p) = \max\left(\max_{k=1}^{N}(\mathrm{LM}(q_i)\mathrm{LM}(f_i)), \mathrm{LM}(r)\right)$.

Proof. We first show that the division algorithm terminates.

Observe that at each stage of the division algorithm we subtract from r (initialized with p), producing a sequence of polynomials $r_0 = p$, r_1, r_2, $\ldots$.

exploiting monomial orders

To obtain r_{i+1} we subtract $\frac{\mathrm{LT}(r_i)}{\mathrm{LT}(f_k)}$ from r_i, so we have: $\mathrm{LM}(r_{i+1}) < \mathrm{LM}(r_i)$, for all i in the sequence.

This sequence must terminate for a monomial order $<$ where every set of monomials has a smallest element.

To show $\mathrm{LM}(p) = \max\left(\max_{k=1}^{N}(\mathrm{LM}(q_i)\mathrm{LM}(f_i)), \mathrm{LM}(r)\right)$, first recall that as the algorithm terminates: $\mathrm{LM}(r) \leq \mathrm{LM}(p)$.

To compute the q_i's we collect terms $\frac{\mathrm{LT}(r)}{\mathrm{LT}(f_k)}$ where $\frac{\mathrm{LT}(r)}{\mathrm{LT}(f_k)} g_k$ cancels $\mathrm{LT}(r)$.

Therefore: $\mathrm{LM}(q_i)\mathrm{LM}(f_i) \leq \mathrm{LM}(p)$ and we are done. ☐

exploiting monomial orders

To obtain r_{i+1} we subtract $\frac{\mathrm{LT}(r_i)}{\mathrm{LT}(f_k)}$ from r_i, so we have: $\mathrm{LM}(r_{i+1}) < \mathrm{LM}(r_i)$, for all i in the sequence.

This sequence must terminate for a monomial order $<$ where every set of monomials has a smallest element.

To show $\mathrm{LM}(p) = \max\left(\max_{k=1}^{N}(\mathrm{LM}(q_i)\mathrm{LM}(f_i)), \mathrm{LM}(r)\right)$, first recall that as the algorithm terminates: $\mathrm{LM}(r) \leq \mathrm{LM}(p)$.

To compute the q_i's we collect terms $\frac{\mathrm{LT}(r)}{\mathrm{LT}(f_k)}$ where $\frac{\mathrm{LT}(r)}{\mathrm{LT}(f_k)} g_k$ cancels $\mathrm{LT}(r)$.

Therefore: $\mathrm{LM}(q_i)\mathrm{LM}(f_i) \leq \mathrm{LM}(p)$ and we are done. $\square$

exploiting monomial orders

To obtain r_{i+1} we subtract $\frac{\mathrm{LT}(r_i)}{\mathrm{LT}(f_k)}$ from r_i, so we have: $\mathrm{LM}(r_{i+1}) < \mathrm{LM}(r_i)$, for all i in the sequence.

This sequence must terminate for a monomial order $<$ where every set of monomials has a smallest element.

To show $\mathrm{LM}(p) = \max\left(\max_{k=1}^{N}(\mathrm{LM}(q_i)\mathrm{LM}(f_i)), \mathrm{LM}(r)\right)$, first recall that as the algorithm terminates: $\mathrm{LM}(r) \leq \mathrm{LM}(p)$.

To compute the q_i's we collect terms $\frac{\mathrm{LT}(r)}{\mathrm{LT}(f_k)}$ where $\frac{\mathrm{LT}(r)}{\mathrm{LT}(f_k)}g_k$ cancels $\mathrm{LT}(r)$.

Therefore: $\mathrm{LM}(q_i)\mathrm{LM}(f_i) \leq \mathrm{LM}(p)$ and we are done. □

Gröbner Bases

proof of Buchberger's criterion

Theorem (Buchberger's criterion)

A set $g = \{g_1, g_2, \ldots, g_s\}$ is a Gröbner basis if and only if for all pairs g_i and g_j, $i \neq j$, the remainder of the division of $S(g_i, g_j)$ by g equals zero.

Proof. The $\Rightarrow$ of the theorem follows from $S(g_i, g_j) \in \langle g \rangle$.

For the $\Leftarrow$ direction, let $f \in I$. While we may write f in many ways, we choose this representation of f:

$$f = \sum_{i=1}^{s} h_i g_i, h_i \in \mathbb{C}[\mathbf{x}] \quad \text{for which} \quad x^{\mathbf{a}} = \max_{i=1}^{s} \mathrm{LM}(h_i g_i)$$

is least. If $\mathrm{LM}(f) = \mathbf{x}^{\mathbf{a}}$, then $\mathrm{LT}(f) \in \langle \mathrm{LT}(g) \rangle$ and we are done. Otherwise, ...

proof of Buchberger's criterion

Theorem (Buchberger's criterion)

A set $g = \{g_1, g_2, \ldots, g_s\}$ is a Gröbner basis if and only if for all pairs g_i and g_j, $i \neq j$, the remainder of the division of $S(g_i, g_j)$ by g equals zero.

Proof. The $\Rightarrow$ of the theorem follows from $S(g_i, g_j) \in \langle g \rangle$.

For the $\Leftarrow$ direction, let $f \in I$. While we may write f in many ways, we choose this representation of f:

$$f = \sum_{i=1}^{s} h_i g_i, h_i \in \mathbb{C}[\mathbf{x}] \quad \text{for which} \quad x^{\mathbf{a}} = \max_{i=1}^{s} \mathrm{LM}(h_i g_i)$$

is least. If $\mathrm{LM}(f) = \mathbf{x}^{\mathbf{a}}$, then $\mathrm{LT}(f) \in \langle \mathrm{LT}(g) \rangle$ and we are done. Otherwise, …

proof of Buchberger's criterion

Theorem (Buchberger's criterion)

A set $g = \{g_1, g_2, \ldots, g_s\}$ is a Gröbner basis if and only if for all pairs g_i and g_j, $i \neq j$, the remainder of the division of $S(g_i, g_j)$ by g equals zero.

Proof. The $\Rightarrow$ of the theorem follows from $S(g_i, g_j) \in \langle g \rangle$.

For the $\Leftarrow$ direction, let $f \in I$. While we may write f in many ways, we choose this representation of f:

$$f = \sum_{i=1}^{s} h_i g_i, h_i \in \mathbb{C}[\mathbf{x}] \quad \text{for which} \quad x^{\mathbf{a}} = \max_{i=1}^{s} \mathrm{LM}(h_i g_i)$$

is least. If $\mathrm{LM}(f) = \mathbf{x}^{\mathbf{a}}$, then $\mathrm{LT}(f) \in \langle \mathrm{LT}(g) \rangle$ and we are done. Otherwise, . . .

deriving a contradiction

Otherwise we rewrite f into a representation

$$f = \sum_{i=1}^{s} \widetilde{h}_i g_i, \widetilde{h}_i \in \mathbb{C}[\mathbf{x}] \quad \text{where} \quad \max_{i=1}^{s} \mathrm{LM}(\widetilde{h}_i g_i) = \mathbf{x}^{\mathbf{a}},$$

contradicting our first choice ($\mathbf{x}^{\mathbf{a}}$ is least among all representations for f), leaving only $\mathrm{LM}(f) = \mathbf{x}^{\mathbf{a}}$.

To derive the contradiction, take $H = \{ i \mid g_i \in g : \mathrm{LM}(h_i g_i) = \mathbf{x}^{\mathbf{a}} \}$ and consider $p = \sum_{i \in H} \mathrm{LT}(h_i) g_i$.

We have $\mathrm{LM}(\mathrm{LT}(h_i) g_i) = \mathbf{x}^{\mathbf{a}}$, for all $i \in H$ and $\mathrm{LM}(p) < \mathbf{x}^{\mathbf{a}}$, because $\mathrm{LM}(f) < \mathbf{x}^{\mathbf{a}}$.

deriving a contradiction

Otherwise we rewrite f into a representation

$$f = \sum_{i=1}^{s} \widetilde{h}_i g_i, \widetilde{h}_i \in \mathbb{C}[\mathbf{x}] \quad \text{where} \quad \max_{i=1}^{s} \mathrm{LM}(\widetilde{h}_i g_i) = \mathbf{x}^{\mathbf{a}},$$

contradicting our first choice ($\mathbf{x}^{\mathbf{a}}$ is least among all representations for f), leaving only $\mathrm{LM}(f) = \mathbf{x}^{\mathbf{a}}$.

To derive the contradiction, take
$H = \{ \, i \mid g_i \in g : \mathrm{LM}(h_i g_i) = \mathbf{x}^{\mathbf{a}} \, \}$ and consider
$p = \displaystyle\sum_{i \in H} \mathrm{LT}(h_i) g_i$.

We have $\mathrm{LM}(\mathrm{LT}(h_i) g_i) = \mathbf{x}^{\mathbf{a}}$, for all $i \in H$ and $\mathrm{LM}(p) < \mathbf{x}^{\mathbf{a}}$, because $\mathrm{LM}(f) < \mathbf{x}^{\mathbf{a}}$.

applying Lemma 1

Application of Lemma 1 yields coefficients $c_{ij} \in \mathbb{C}$:

$$p = \sum_{i,j \in H, i \neq j} c_{ij} S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j).$$

As $\mathrm{LCM}(\mathrm{LM}(h_i g_i), \mathrm{LM}(h_j g_j)) = \mathbf{x}^{\mathbf{a}}$:

$$\begin{aligned} S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j) &= \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(h_i g_i)} h_i g_i - \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(h_j g_j)} h_j g_j \\ &= \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(g_i)} g_i - \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(g_j)} g_j \\ &= \frac{\mathbf{x}^{\mathbf{a}}}{\mathbf{x}^{\mathbf{b}}} S(g_i, g_j). \end{aligned}$$

where $\mathbf{x}^{\mathbf{b}} = \mathrm{LCM}(\mathrm{LT}(g_i)), \mathrm{LT}(g_j)).$

The expression for $S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j)$ shows: if $S(g_i, g_j)$ reduces to 0, then also $S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j)$ reduces to 0.

applying Lemma 1

Application of Lemma 1 yields coefficients $c_{ij} \in \mathbb{C}$:
$$p = \sum_{i,j \in H, i \neq j} c_{ij} S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j).$$

As $\mathrm{LCM}(\mathrm{LM}(h_i g_i), \mathrm{LM}(h_j g_j)) = \mathbf{x}^{\mathbf{a}}$:

$$\begin{aligned} S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j) &= \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(h_i g_i)} h_i g_i - \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(h_j g_j)} h_j g_j \\ &= \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(g_i)} g_i - \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(g_j)} g_j \\ &= \frac{\mathbf{x}^{\mathbf{a}}}{\mathbf{x}^{\mathbf{b}}} S(g_i, g_j). \end{aligned}$$

where $\mathbf{x}^{\mathbf{b}} = \mathrm{LCM}(\mathrm{LT}(g_i)), \mathrm{LT}(g_j))$.

The expression for $S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j)$ shows: if $S(g_i, g_j)$ reduces to 0, then also $S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j)$ reduces to 0.

applying Lemma 1

Application of Lemma 1 yields coefficients $c_{ij} \in \mathbb{C}$:

$$p = \sum_{i,j \in H, i \neq j} c_{ij} S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j).$$

As $\mathrm{LCM}(\mathrm{LM}(h_i g_i), \mathrm{LM}(h_j g_j)) = \mathbf{x}^\mathbf{a}$:

$$\begin{aligned} S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j) &= \frac{\mathbf{x}^\mathbf{a}}{\mathrm{LT}(h_i g_i)} h_i g_i - \frac{\mathbf{x}^\mathbf{a}}{\mathrm{LT}(h_j g_j)} h_j g_j \\ &= \frac{\mathbf{x}^\mathbf{a}}{\mathrm{LT}(g_i)} g_i - \frac{\mathbf{x}^\mathbf{a}}{\mathrm{LT}(g_j)} g_j \\ &= \frac{\mathbf{x}^\mathbf{a}}{\mathbf{x}^\mathbf{b}} S(g_i, g_j). \end{aligned}$$

where $\mathbf{x}^\mathbf{b} = \mathrm{LCM}(\mathrm{LT}(g_i)), \mathrm{LT}(g_j))$.

The expression for $S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j)$ shows: if $S(g_i, g_j)$ reduces to 0, then also $S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j)$ reduces to 0.

applying Lemma 2

Collecting quotients from the division algorithm:

$$S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j) = \sum_{k=1}^{s} \widetilde{h}_{ijk} g_k$$

where by the second formula of Lemma 2:

$$\begin{aligned} \max_{k=1}^{s} \mathrm{LM}(\widetilde{h}_{ijk} \mathrm{LM}(g_k)) &= \mathrm{LM}(S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j)) \\ &< \max(\mathrm{LM}(h_i g_i)\mathrm{LM}(h_j g_j)) = \mathbf{x}^{\mathbf{a}}. \end{aligned}$$

Substituting the expressions back into g we get the representation for f which gives the contradiction. $\square$

applying Lemma 2

Collecting quotients from the division algorithm:

$$S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j) = \sum_{k=1}^{s} \widetilde{h}_{ijk} g_k$$

where by the second formula of Lemma 2:

$$\begin{array}{rcl} \max\limits_{k=1}^{s} \mathrm{LM}(\widetilde{h}_{ijk}\mathrm{LM}(g_k)) & = & \mathrm{LM}(S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j)) \\ & < & \max(\mathrm{LM}(h_i g_i)\mathrm{LM}(h_j g_j)) = \mathbf{x}^{\mathbf{a}}. \end{array}$$

Substituting the expressions back into g we get the representation for f which gives the contradiction. ☐

Gröbner Bases

1. S-polynomials
   - eliminating the leading term
   - Buchberger's criterion and algorithm
2. Wavelet Design
   - construct wavelet filters
3. Proof of the Buchberger Criterion
   - two lemmas
   - proof of the Buchberger criterion
   - termination and elimination

the Buchberger algorithm terminates

Showing that this algorithm terminates also shows the Hilbert basis theorem, i.e.: any ideal has a finite basis.

The key observation is that as long as the repeat loop does not terminate, we augment g with a nonzero polynomial $S = S(p, q)$ for which $\mathrm{LM}(S) < \mathrm{LM}(p)$ and $\mathrm{LM}(S) < \mathrm{LM}(q)$, with respect to the term order $<$.

Compared to h, we thus have that $\langle \mathrm{LT}(h) \rangle \subset \langle \mathrm{LT}(g) \rangle$.

So as long as the loop runs, we create a chain of monomial ideals which cannot stretch for ever.

the Buchberger algorithm terminates

Showing that this algorithm terminates also shows the Hilbert basis theorem, i.e.: any ideal has a finite basis.

The key observation is that as long as the repeat loop does not terminate, we augment g with a nonzero polynomial $S = S(p,q)$ for which $\mathrm{LM}(S) < \mathrm{LM}(p)$ and $\mathrm{LM}(S) < \mathrm{LM}(q)$, with respect to the term order $<$.

Compared to h, we thus have that $\langle \mathrm{LT}(h) \rangle \subset \langle \mathrm{LT}(g) \rangle$.

So as long as the loop runs, we create a chain of monomial ideals which cannot stretch for ever.

Elimination Ideals

Consider again a system of homogeneous linear equations. Applying row reduction to bring such a system into triangular form can be written in terms of taking S-polynomials.

For an ideal I in $\mathbb{C}[\mathbf{x}]$, $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, the kth elimination ideal is $I_k = I \cap \mathbb{C}[x_{k+1}, \ldots, x_n]$.

So I_k consists of all polynomials in I for which the first k variables have been eliminated.

Theorem (The Elimination Theorem)

Let g be a Gröbner basis for an ideal I with respect to the pure lexicographical order $x_1 > x_2 > \cdots > x_n$. Then the set $g_k = g \cap \mathbb{C}[x_{k+1}, \ldots, x_n]$ is a Gröbner basis of the kth elimination ideal I_k.

Elimination Ideals

Consider again a system of homogeneous linear equations. Applying row reduction to bring such a system into triangular form can be written in terms of taking S-polynomials.

For an ideal I in $\mathbb{C}[\mathbf{x}]$, $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, the kth elimination ideal is $I_k = I \cap \mathbb{C}[x_{k+1}, \ldots, x_n]$.

So I_k consists of all polynomials in I for which the first k variables have been eliminated.

Theorem (The Elimination Theorem)

Let g be a Gröbner basis for an ideal I with respect to the pure lexicographical order $x_1 > x_2 > \cdots > x_n$. Then the set $g_k = g \cap \mathbb{C}[x_{k+1}, \ldots, x_n]$ is a Gröbner basis of the kth elimination ideal I_k.

proof of the Elimination theorem

Proof. To prove this theorem, we must show that $\langle \mathrm{LT}(I_k) \rangle = \langle \mathrm{LT}(g_k) \rangle$. By construction, $\langle \mathrm{LT}(g_k) \rangle \subset \langle \mathrm{LT}(I_k) \rangle$, so what remains to show is that $\langle \mathrm{LT}(I_k) \rangle \subset \langle \mathrm{LT}(g_k) \rangle$.

For any $f \in I_k$, we must then show that $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(p)$ for some $p \in g_k$.

As $f \in I$: $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(p)$ for some $p \in g$. Since $f \in I_k$, the only variables in f are $x_{k+1}, \ldots, x_n$.

Because of the lexicographic order: if $\mathrm{LT}(p) \in \mathbb{C}[x_{k+1}, \ldots, x_n]$, then all other terms of p also $\in \mathbb{C}[x_{k+1}, \ldots, x_n]$.

Thus the p for which $\mathrm{LT}(p)$ divides $\mathrm{LT}(f)$ belongs to g_k. ☐

proof of the Elimination theorem

Proof. To prove this theorem, we must show that $\langle \mathrm{LT}(I_k) \rangle = \langle \mathrm{LT}(g_k) \rangle$. By construction, $\langle \mathrm{LT}(g_k) \rangle \subset \langle \mathrm{LT}(I_k) \rangle$, so what remains to show is that $\langle \mathrm{LT}(I_k) \rangle \subset \langle \mathrm{LT}(g_k) \rangle$.

For any $f \in I_k$, we must then show that $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(p)$ for some $p \in g_k$.

As $f \in I$: $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(p)$ for some $p \in g$. Since $f \in I_k$, the only variables in f are $x_{k+1}, \ldots, x_n$.

Because of the lexicographic order: if $\mathrm{LT}(p) \in \mathbb{C}[x_{k+1}, \ldots, x_n]$, then all other terms of p also $\in \mathbb{C}[x_{k+1}, \ldots, x_n]$.

Thus the p for which $\mathrm{LT}(p)$ divides $\mathrm{LT}(f)$ belongs to g_k. ☐

proof of the Elimination theorem

Proof. To prove this theorem, we must show that $\langle \mathrm{LT}(I_k) \rangle = \langle \mathrm{LT}(g_k) \rangle$. By construction, $\langle \mathrm{LT}(g_k) \rangle \subset \langle \mathrm{LT}(I_k) \rangle$, so what remains to show is that $\langle \mathrm{LT}(I_k) \rangle \subset \langle \mathrm{LT}(g_k) \rangle$.

For any $f \in I_k$, we must then show that $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(p)$ for some $p \in g_k$.

As $f \in I$: $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(p)$ for some $p \in g$. Since $f \in I_k$, the only variables in f are $x_{k+1}, \ldots, x_n$.

Because of the lexicographic order: if $\mathrm{LT}(p) \in \mathbb{C}[x_{k+1}, \ldots, x_n]$, then all other terms of p also $\in \mathbb{C}[x_{k+1}, \ldots, x_n]$.

Thus the p for which $\mathrm{LT}(p)$ divides $\mathrm{LT}(f)$ belongs to g_k. ☐

Summary + Exercises

We gave a definition for the Gröbner basis, explained Buchberger's criterion and algorithm.

Exercises:

1. Solve the system for filter design. Use Maple or Sage to create a lexicographical Gröbner basis. Verify that by adding one more equation, the resulting Gröbner basis is more compact. How many real solutions do you find?
2. Apply Buchberger's algorithm by hand (you can use a Maple worksheet to compute all S-polynomials) to the ideal generated by the equations $\{x_1^2 + x_2^2 - 1, x_1x_2 - 1\}$ using a pure lexicographical monomial order.
3. Show that for two systems $f(\mathbf{x}) = \mathbf{0}$ and $g(\mathbf{x}) = \mathbf{0}$: if $\langle f \rangle = \langle g \rangle$, then their solutions are the same. Give an example of a case for which the opposite direction does hold.

more exercises

④ Consider the example

$$f(x,y) = \left\{ \begin{array}{r} x^2 + \epsilon xy + y^2 - 1 = 0 \\ y^3 - 3x^2 y = 0 \end{array} \right. \qquad \text{for } \epsilon \approx 0.$$

Although the solution set varies continuously with ϵ, we will verify that a Gröbner basis cannot be a continous function of ϵ. Use Maple or Sage for the following calculations:

1. Make a plot of the two curves defined by the polynomials in the system. Justify why all intersection points are well conditioned roots.
2. Compute Gröbner bases for various values of ϵ and examine the growth of the coefficients as ϵ gets smaller.
3. Compute a Gröbner basis where ϵ is a parameter. Interpret the results.

and more exercises

5. The twisted cubic is a curve in 3-space defined by $(x_1 = t, x_2 = t^2, x_3 = t^3)$, for a parameter t. Equivalently, the equations $x_1^2 - x_2 = 0$ and $x_1^3 - x_3 = 0$ defined the twisted cubic in implicit form. The surface of all lines tangent to points on the twisted cubic is

$$\left\{ \begin{array}{l} x_1 = t + s \\ x_2 = t^2 + 2ts \\ x_3 = t^3 + 3t^2 s, \end{array} \right. \qquad (1)$$

for parameters s and t. Compute a lexicographical Gröbner basis using a monomial order that eliminates s and t. Find an equation for the surface that defines all tangent lines to the twisted cubic.

one last exercise

6. With a lexicographical Gröbner basis and a solver for polynomials in one variable we can solve zero dimensional polynomial systems, systems that have only isolated solutions. Write a procedure in a computer algebra system that takes on input a lexicographical Gröbner basis and computes all solutions by applying the univariate solver repeatedly and substituting the solutions into the remaining equations. For a numerical solver, show that the working precision must be sufficiently high enough as the solver progresses, considering the example of exercise 4.