Teaching Commutative Algebra and Algebraic Geometry using Computer Algebra Systems

Michael Monagan

Department of Mathematics,
Simon Fraser University
British Columbia, CANADA

Computer Algebra in Education
ACA 2012, Sofia, Bulgaria
June 25-28, 2012
MATH 441 Commutative Algebra and Algebraic Geometry

- Who takes the course?
- Textbook and course content.
- Maple and Assessment.
- Three applications.
  - Read material (paper).
  - Reproduce computational results.
  - Correct errors.
- Course project for graduate students.
Who takes the course?

4th undergraduate students and 1st year graduate students.

<table>
<thead>
<tr>
<th>major</th>
<th>2006</th>
<th>2008</th>
<th>2010</th>
<th>2012</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>mathematics</td>
<td>5</td>
<td>15</td>
<td>11</td>
<td>27</td>
<td>58</td>
</tr>
<tr>
<td>computing</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>math &amp; cmpt</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>other</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>graduate</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>total</td>
<td>10</td>
<td>27</td>
<td>17</td>
<td>31</td>
<td>85</td>
</tr>
</tbody>
</table>
Ch. 1 Geometry, Algebra and Algorithms
Ch. 2 Groebner Bases
Ch. 3 Elimination Theory
Ch. 4 The Algebra-Geometry Dictionary
Ch. 5 Quotient Rings
Ch. 6 Automatic Geometric Theorem Proving
Ch. 7 Invariant Theory of Finite Groups
Ch. 8 Projective Algebraic Geometry

Appendix C. Computer Algebra Systems
Varieties, Graphing varieties, Ideals.

Monomial orderings and the division algorithm.
The Hilbert basis theorem.
Gröbner bases and Buchberger’s algorithm.

Solving equations (using Gröbner bases).
Elimination theory and resultants.

Hilbert’s Nullstellensatz.
Radical ideals and radical membership.
Zariski topology.
Irreducible varieties, prime ideals, maximal ideals.
Ideal decomposition.

Quotient rings, computing in quotient rings.

Applications (of Gröbner bases).
Maple and Assessment

- One intro Maple tutorial in lab.
- Detailed examples worksheet for self study.
- Five in class demos.
- Maple worksheet handouts.

Michael Monagan

Teaching Commutative Algebra and Algebraic Geometry
Maple and Assessment

- One intro Maple tutorial in lab.
- Detailed examples worksheet for self study.
- Five in class demos.
- Maple worksheet handouts.

<table>
<thead>
<tr>
<th></th>
<th>MATH 441</th>
<th>MATH 819</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 assignments</td>
<td>60%</td>
<td>60%</td>
</tr>
<tr>
<td>project</td>
<td>–</td>
<td>10%</td>
</tr>
<tr>
<td><strong>24 hour final</strong></td>
<td>40%</td>
<td>30%</td>
</tr>
</tbody>
</table>

- Assignment questions, final exam, and project need Maple.
- Post take home final on web at 9am.
  Hand in following day before 10am in person.
Application 1: Circle Packing Problems

Pack \( n = 6 \) circles in the unit square maximizing the radius \( r \).

Pack \( n = 6 \) points in the unit square maximizing their separating distance \( m \).

\[
    r = \frac{m}{2(m + 1)}
\]

D. Würtz, M. Monagan and R. Peikert.
The History of Packing Circles in a Square.
Given a packing, find $m$.

Let $P_i = (x_i, y_i)$ for $1 \leq i \leq 6$.

So $P_1 = (0, 0)$, $P_6 = (x_6, y_6)$, etc.

Pythagoras: $(x_6 - x_1)^2 + (y_6 - y_1)^2 = m^2$.

Symmetry: $x_6 = 1/2$, $y_6 = (y_0 + y_5)/2$.

Do not solve for $m$, $x_1$, ..., $x_6$, $y_1$, ..., $y_6$. Instead let
Application 1: Circle Packing Problems

Given a packing, find $m$.

Let $P_i = (x_i, y_i)$ for $1 \leq i \leq 6$.
So $P_1 = (0, 0)$, $P_6 = (x_6, y_6)$, etc.

Pythagoras: $(x_6 - x_1)^2 + (y_6 - y_1)^2 = m^2$.
Symmetry: $x_6 = 1/2$, $y_6 = (y_0 + y_5)/2$.

Do not solve for $m, x_1, \ldots, x_6, y_1, \ldots, y_6$. Instead let

$I = \langle x_6 - \frac{1}{2}, x_6^2 + y_6^2 - m^2, \ldots \rangle \subset \mathbb{Q}[x_1, \ldots, x_6, y_1, \ldots, y_6, m]$

and compute a Gr"obner basis $G$ for $I \cap \mathbb{Q}[m] = \langle g \rangle$.
I get $G = \{(4m^2 - 5)(36m^2 - 13)\}$.
Figure out that $4m^2 - 5 = 0$ is a degenerate case.

Michael Monagan  
Teaching Commutative Algebra and Algebraic Geometry
Case $n = 10$

$\begin{align*}
\text{J. Schaer} & \quad m = 0.41953 \\
\text{R. Milano} & \quad m = 0.42013 \\
\text{G. Valette} & \quad m = 0.42118 \\
\text{WMP} & \quad m = 0.42129
\end{align*}$

What can go wrong?
Application 1: Circle Packing Problems

Case $n = 10$

$m = 0.41953$  
J. Schaer

$m = 0.42013$  
R. Milano

$m = 0.42118$  
G. Valette

$m = 0.42129$  
WMP

**What can go wrong?**

Input equations incorrectly.

---

Michael Monagan  
Teaching Commutative Algebra and Algebraic Geometry
Application 1: Circle Packing Problems

Case $n = 10$

What can go wrong?
Input equations incorrectly.
Errors in the figures.
Case $n = 10$

$m = 0.41953$  \hspace{1cm} m = 0.42013  \hspace{1cm} m = 0.42118  \hspace{1cm} m = 0.42129$

J. Schaer  \hspace{1cm} R. Milano  \hspace{1cm} G. Valette  \hspace{1cm} WMP

**What can go wrong?**
Input equations incorrectly.
Errors in the figures.
Setup may have degenerate solutions.
Case $n = 10$

$m = 0.41953$  J. Schaer  
$m = 0.42013$  R. Milano  
$m = 0.42118$  G. Valette  
$m = 0.42129$  WMP

**What can go wrong?**
Input equations incorrectly.
Errors in the figures.
Setup may have degenerate solutions.
Too many quadratic equations $\implies$ long time.
Application 2: Graph Coloring and Hilbert’s Nullstellensatz.

Which of these graphs can be colored with three colors?

![Wheel graphs $W_3$ and $W_4$.](image)

Figure: Wheel graphs $W_3$ and $W_4$. 
To color a graph on $n$ vertices with $k = 3$ colors, set

$$S := \{x_1^k = 1, x_2^k = 1, \ldots, x_n^k = 1\}.$$ 

For each edge $(u, v) \in G$ set $S := S \cup \left\{ \frac{x_u^k - x_v^k}{x_u - x_v} = 0 \right\}$. 

**Theorem**

$G$ is $k$-colorable $\iff$ $S$ has solutions over $\mathbb{C}$. 

Nice! So let $I = \langle x_1^k - 1, \ldots \rangle$.

Compute a reduced Gröbner basis $B$ for $I$.

Et voila! $B = \{1\} \iff G$ is not $k$-colorable.
To color a graph on \( n \) vertices with \( k = 3 \) colors, set

\[
S := \{x_1^k = 1, x_2^k = 1, \ldots, x_n^k = 1\}.
\]

For each edge \((u, v) \in G\) set \(S := S \cup \left\{ \frac{x_u^k - x_v^k}{x_u - x_v} = 0 \right\}\).

**Theorem**

\( G \) is \( k \)-colorable \( \iff \) \( S \) has solutions over \( \mathbb{C} \).
Application 2: Graph Coloring and Hilbert’s Nullstellensatz.

To color a graph on \( n \) vertices with \( k = 3 \) colors, set

\[
S := \{x_1^k = 1, x_2^k = 1, \ldots, x_n^k = 1\}.
\]

For each edge \((u, v) \in G\) set \( S := S \cup \left\{ \frac{x_u^k - x_v^k}{x_u - x_v} = 0 \right\} \).

**Theorem**

\( G \) is \( k \)-colorable \( \iff \) \( S \) has solutions over \( \mathbb{C} \).

Nice! So let \( I = \langle x_1^k - 1, \ldots, \rangle \).

Compute a reduced Gröbner basis \( B \) for \( I \).

Et voila! \( B = \{1\} \iff G \) is not \( k \)-colorable.
But

**Theorem**

*Graph k-colorability is NP-complete for $k \geq 3$.***
But

**Theorem**

*Graph k-colorability is NP-complete for* $k \geq 3$.

J.A. de Loera, J. Lee, P.N. Malkin and S. Margulies. **Hilbert’s Nullstellensatz** and an algorithm for proving combinatorial infeasibility.

Let $V = \mathbb{V}(x_1^k - 1, \ldots, \ldots)$ and $I = \langle x_1^k - 1, \ldots, \rangle$.

**Theorem**

$G$ is NOT $k$-colorable $\iff V = \emptyset \iff HNS 1 \in I$. 

Idea 1: Try to find $h_i$ with degree $d = 1, 2, 3, \ldots$.

Idea 2: The larger $d$ the harder the combinatorial problem.

Idea 3: Replace $Q$ with $F_2$.

Get the students to experiment.
Let $V = \mathbb{V}(x_1^k - 1, \ldots, \ldots)$ and $I = \langle x_1^k - 1, \ldots, \rangle$.

**Theorem**

$G$ is NOT $k-$colorable $\iff V = \emptyset \overset{HNS}{\iff} 1 \in I$.

But if $I = \langle f_1, f_2, \ldots, f_m \rangle \subset \mathbb{Q}[x_1, x_2, \ldots, x_n]$ then

$$1 \in I \implies 1 = h_1 f_1 + h_2 f_2 + \ldots h_m f_m$$

for some $h_1, h_2, \ldots, h_m$ in $\mathbb{Q}[x_1, x_2, \ldots, x_n]$.

**Idea 1:** Try to find $h_i$ with degree $d = 1, 2, 3, \ldots$.

**Idea 2:** The larger $d$ the harder the combinatorial problem.

**Idea 3:** Replace $\mathbb{Q}$ with $\mathbb{F}_2$.

**Get the students to experiment.**
Theorem

Let $ABCD$ be a parallelogram and $N = \overline{AC} \cap \overline{BD}$. Then $N$ is the midpoint of $\overline{AC}$ and $\overline{BD}$.

Can we automate the proof?
Application 3: Automatic Geometric Theorem Proving.

\[ C = (u_2, u_3) \quad D = (x_1, y_1) \]

Step 1: Fix co-ordinates.
3 parameters \( u_1, u_2, u_3 \).
4 unknowns \( x_1, y_1, x_2, y_2 \).
Solutions are in \( \mathbb{R}(u_1, u_2, u_3) \).

Step 2: Need 4 equations.
Application 3: Automatic Geometric Theorem Proving.

\[ A = (0,0) \quad B = (u_1, 0) \quad C = (u_2, u_3) \quad D = (x_1, y_1) \quad N = (x_2, y_2) \]

\begin{align*}
\text{Step 1: Fix co-ordinates.} \\
3 \text{ parameters } u_1, u_2, u_3. \\
4 \text{ unknowns } x_1, y_1, x_2, y_2. \\
\text{Solutions are in } \mathbb{R}(u_1, u_2, u_3).
\end{align*}

\begin{align*}
\text{Step 2: Need 4 equations.} \\
ABDC \text{ is a parallelogram} & \implies \text{the slope of } \overrightarrow{AC} = \overrightarrow{BD} \\
\implies \frac{u_3}{u_2} = \frac{y_1}{x_1 - u_1} & \implies (x_1 - u_1)u_3 = u_2y_1. \\
\text{Similarly the slope of } \overrightarrow{AB} = \overrightarrow{CD} & \implies y_1 = u_3.
\end{align*}
Let $N$ be the intersection of $\overline{AD}$ and $\overline{BC}$. Hence $A, N, D$ are co-linear $\implies$

$$\det\begin{bmatrix} x_2 & x_1 \\ y_2 & y_1 \end{bmatrix} = 0 \implies x_2y_1 - y_2x_1 = 0.$$ 

Similarly $B, N, C$ are co-linear $\implies (u_1 - u_2)y_2 = u_3(u_1 - x_2)$. 

Michael Monagan  Teaching Commutative Algebra and Algebraic Geometry
Application 3: Automatic Geometric Theorem Proving.

\[ C = (u_2, u_3) \quad D = (x_1, y_1) \]
\[ N = (x_2, y_2) \]
\[ A = (0, 0) \quad B = (u_1, 0) \]

**Equations**
\[ h_1 = (x_1 - u_1)u_3 - u_2y_1 \]
\[ h_2 = y_1 - u_3 \]
\[ h_3 = x_2y_1 - y_2x_1 \]
\[ h_4 = (u_1 - u_2)y_2 - u_3(u_1 - x_2) \]

**Step 2 (cont.):** To prove \( N \) is the midpoint of \( AD \) and \( BC \) show \( \| N - A \|^2 = \| D - N \|^2 \)

\[ \implies x_2^2 + y_2^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2. \]

Similarly
\[ \| N - B \|^2 = \| C - N \|^2 \implies (x_2 - u_1)^2 + y_2^2 = (u_2 - x_2)^2 + u_3^2. \]
Application 3: Automatic Geometric Theorem Proving.

\[ h_1 = (x_1 - u_1)u_3 - u_2 y_1 \]
\[ h_2 = y_1 - u_3 \]
\[ h_3 = x_2 y_1 - y_2 x_1 \]
\[ h_4 = (u_1 - u_2)y_2 - u_3(u_1 - x_2) \]
\[ g_1 = x_2^2 + y_2^2 - (x_1 - x_2)^2 - (y_1 - y_2)^2 \]
\[ g_2 = (x_2 - u_1)^2 + y_2^2 - (u_2 - x_2)^2 - u_3^2 \]

**Step 3. Computation to prove theorem.**

Let \( I = \langle h_1, h_2, h_3, h_4 \rangle \in \mathbb{R}(u_1, u_2, u_3)[x_1, y_1, x_2, y_2] \).
Application 3: Automatic Geometric Theorem Proving.

\[ h_1 = (x_1 - u_1)u_3 - u_2y_1 \]
\[ h_2 = y_1 - u_3 \]
\[ h_3 = x_2y_1 - y_2x_1 \]
\[ h_4 = (u_1 - u_2)y_2 - u_3(u_1 - x_2) \]
\[ g_1 = x_2^2 + y_2^2 - (x_1 - x_2)^2 - (y_1 - y_2)^2 \]
\[ g_2 = (x_2 - u_1)^2 + y_2^2 - (u_2 - x_2)^2 - u_3^2 \]

Step 3. Computation to prove theorem.

Let \( I = \langle h_1, h_2, h_3, h_4 \rangle \in \mathbb{R}(u_1, u_2, u_3)[x_1, y_1, x_2, y_2] \).

Then \( g_1 \in \sqrt{\mathbb{V}(h_1, h_2, h_3, h_4)} \iff g_1 \in \sqrt{I} \)
\[ \iff 1 \in \langle h_1, h_2, h_3, h_4, 1 - g_1z \rangle \subset \mathbb{R}(u_1, u_2, u_3)[x_1, y_1, x_2, y_2, z] \].

Similarly verify \( g_2 \in \sqrt{I} \).

What can go wrong?
Errors: any claim is true if $I = \langle h_1, h_2, \ldots \rangle = \langle 1 \rangle$.  
$\implies$ check that the Gröbner basis for $I$ is not $\{1\}$!!
Application 3: What can go wrong?

Errors: any claim is true if \( I = \langle h_1, h_2, \ldots \rangle = \langle 1 \rangle \).

\[ \implies \text{check that the Gröbner basis for } I \text{ is not } \{1\} \]

Show that working in \( \mathbb{R}[u_1, u_3, x_1, y_1, x_2, y_2] \) leads to the degenerate cases \( u_1 = 0 \) where the theorem does not hold.
Application 3: What can go wrong?

Errors: any claim is true if \( I = \langle h_1, h_2, \ldots \rangle = \langle 1 \rangle \). 
\( \implies \) check that the Gröbner basis for \( I \) is not \( \{1\} \) !!

Show that working in \( \mathbb{R}[u_1, u_2, u_3, x_1, y_1, x_2, y_2] \) leads to the degenerate cases \( u_1 = 0 \) where the theorem does not hold.

\[ C = (u_2, u_3) \quad D = (x_1, y_1) \]

\[ N = (x_2, y_2) \]

\( N \) is the midpoint of \( \overline{AD} \)
\( \implies N = \frac{(A+D)}{2} \) so
\[ x_2 = \frac{x_1}{2}, \quad y_2 = \frac{y_1}{2} \]!!
1. Implement Buchberger’s algorithm.
2. Study and implement the FGLM basis conversion.
   J.C. Faugere, P. Gianni, D. Lazard, T. Mora.
3. Show that **FGLM works** using Trinks’ system.

\[
\begin{align*}
45p + 35s - 165b &= 36, \\
35p + 40z + 25t - 27s &= 0, \\
15w + 25ps + 30z - 18t - 165b^2 &= 0, \\
-9w + 15pt + 20zs &= 0, \\
wpt + 2zt &= 11b^3, \\
99w - 11sb + 3b^2 &= 0
\end{align*}
\]
Thank you for coming.

On-line course materials

www.cecm.sfu.ca/~mmonagan/teaching/MATH441