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

Talk Outline

MATH 441 Commutative Algebra and Algebraic Geometry
Simon Fraser University, 2006, 2008, 2010, 02012

- 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.

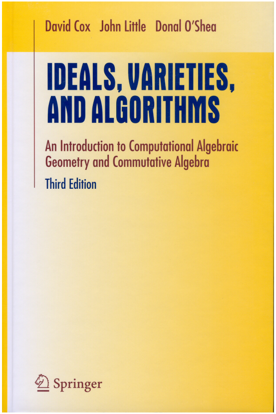
Who takes the course?

4th undergraduate students and
1st year graduate students.

major	**2006**	**2008**	**2010**	**2012**	total
mathematics	5	15	11	27	58
computing	0	0	0	1	1
math & cmpt	0	2	2	2	6
other	0	4	0	0	4
graduate	5	6	4	1	16
total	10	27	17	31	85

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



Content

1. Varieties, Graphing varieties, Ideals.
2. Monomial orderings and the division algorithm.
   The Hilbert basis theorem.
   Gröbner bases and Buchberger's algorithm.
3. Solving equations (using Gröbner bases).
   Elimination theory and resultants.
4. Hilbert's Nullstellensatz.
   Radical ideals and radical membership.
   Zariski topology.
   Irreducible varieties, prime ideals, maximal ideals.
   Ideal decomposition.
5. Quotient rings, computing in quotient rings.
6. 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.

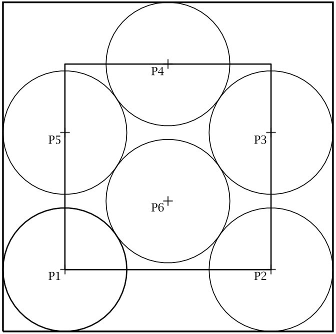
Maple and Assessment

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

	MATH 441	MATH 819
6 assignments	60%	60%
project	–	10%
24 hour final	40%	30%

- 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

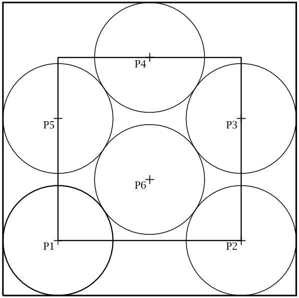


Pack $n = 6$ circles in the unit square maximizing the radius r.

Pack $n = 6$ points in the unit square maximizing their separating distance m.

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

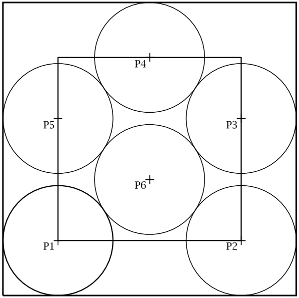
D. Würtz, M. Monagan and R. Peikert.
The History of Packing Circles in a Square.
MapleTech, Birkhauser, 1994.



Given a packing, find m.

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



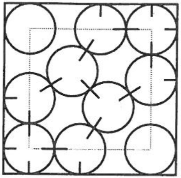
Given a packing, find m.

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

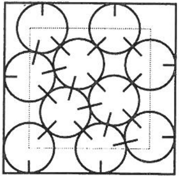
Do not solve for $m, x_1, ..., x_6, y_1, ..., y_6$. Instead let
$I = \langle x_6 - \frac{1}{2}, x_6^2 + y_6^2 - m^2, \ldots \rangle \subset \mathbb{Q}[x_1, \ldots, x_6, y_1, \ldots, y_6, m]$
and compute a Gröbner basis G for $I \cap \mathbb{Q}[m] = \langle g \rangle$.
I get $G = \{(4m^2 - 5)(36m^2 - 13)\}$.
Figure out that $4m^2 - 5 = 0$ is a degenerate case.

Application 1: Circle Packing Problems

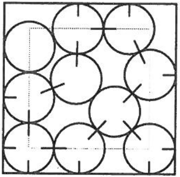
Case $n = 10$



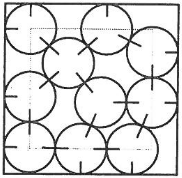
$m = 0.41953$
J. Schaer



$m = 0.42013$
R. Milano



$m = 0.42118$
G. Valette

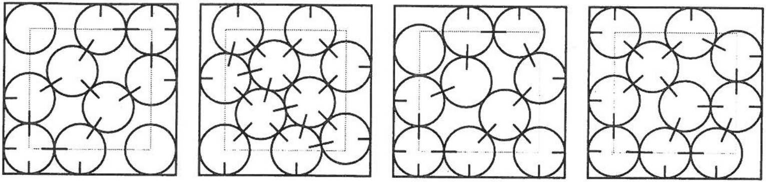


$m = 0.42129$
WMP

What can go wrong?

Application 1: Circle Packing Problems

Case $n = 10$

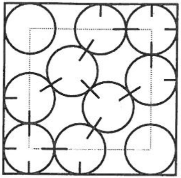


$m = 0.41953$	$m = 0.42013$	$m = 0.42118$	$m = 0.42129$
J. Schaer	R. Milano	G. Valette	WMP

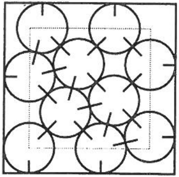
What can go wrong?
Input equations incorrectly.

Application 1: Circle Packing Problems

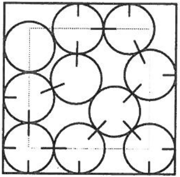
Case $n = 10$



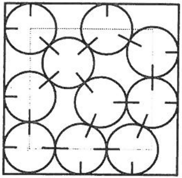
$m = 0.41953$
J. Schaer



$m = 0.42013$
R. Milano



$m = 0.42118$
G. Valette

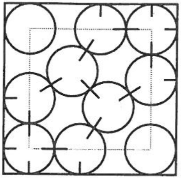


$m = 0.42129$
WMP

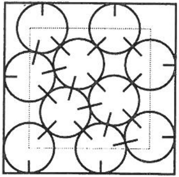
What can go wrong?
Input equations incorrectly.
Errors in the figures.

Application 1: Circle Packing Problems

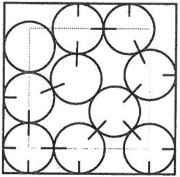
Case $n = 10$



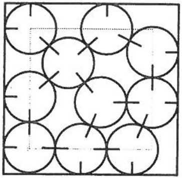
$m = 0.41953$
J. Schaer



$m = 0.42013$
R. Milano



$m = 0.42118$
G. Valette

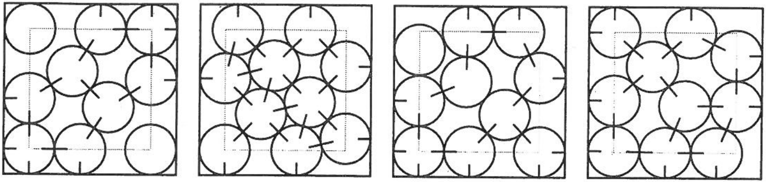


$m = 0.42129$
WMP

What can go wrong?
Input equations incorrectly.
Errors in the figures.
Setup may have degenerate solutions.

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.
Errors in the figures.
Setup may have degenerate solutions.
Too many quadratic equations $\Longrightarrow$ long time.

Which of these graphs can be colored with three colors?

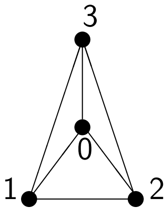
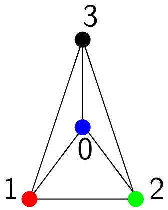


Figure: Wheel graphs W_3 and W_4.



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 $S := S \cup \left\{ \frac{x_u^k - x_v^k}{x_u - x_v} = 0 \right\}$.

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 $k \geq 3$.

Application 2: Graph Coloring and Hilbert's Nullstellensatz.

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.
In *Proc. ISSAC 2008*, ACM Press, 197–206, 2008.

Application 2: Graph Coloring and Hilbert's Nullstellensatz.

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 $\iff V = \phi \overset{HNS}{\iff} 1 \in I$.

Application 2: Graph Coloring and Hilbert's Nullstellensatz.

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

Theorem

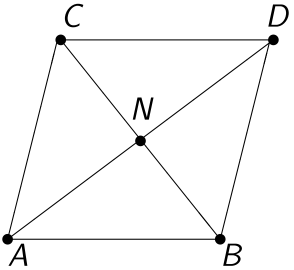
G *is NOT* k*-colorable* $\iff V = \phi \overset{HNS}{\iff} 1 \in I$.

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 $\mathbb{Q}[x_1, x_2, \ldots, x_n]$.

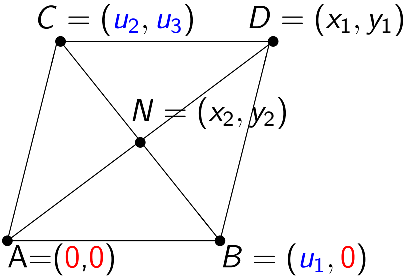
Idea 1: Try to find h_i with degree $d = 1, 2, 3, \ldots$.
Idea 2: The larger d the harder the combinatorial problem.
Idea 3: Replace $\mathbb{Q}$ with $\mathbb{F}_2$.
Get the students to experiment.



Theorem

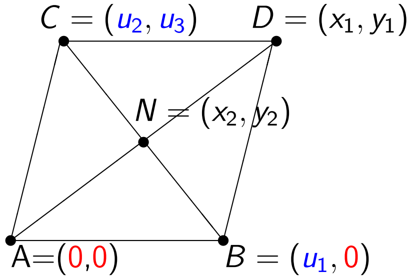
Let ABCD be a parallelogram and $N = \overline{AC} \cap \overline{BD}$.
Then N is the midpoint of $\overline{AC}$ *and* $\overline{BD}$.

Can we automate the proof?



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.

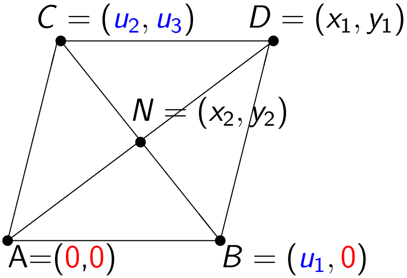


Step 1: Fix co-ordinates.
3 parameters u_1, u_2, u_3.
4 unknowns x_1, y_1, x_2, y_2.
Solutions are in $\mathbb{R}(u_1, u_2, u_3)$.

Step 2: Need 4 equations.
$ABDC$ is a parallelogram $\implies$ the slope of $\overline{AC} = \overline{BD}$

$$\implies \frac{u_3}{u_2} = \frac{y_1}{x_1 - u_1} \implies (x_1 - u_1)u_3 = u_2 y_1.$$

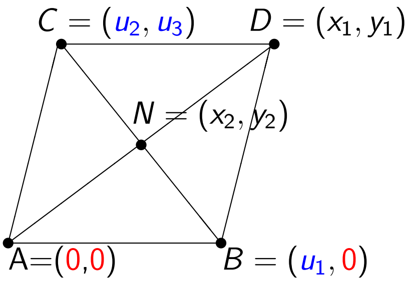
Similarly the slope of $\overline{AB} = \overline{CD} \implies y_1 = u_3$.



Let N be the intersection of $\overline{AD}$ and $\overline{BC}$.
Hence A, N, D are co-linear $\implies$

$$\mathbf{det}\left(\begin{bmatrix} x_2 & x_1 \\ y_2 & y_1 \end{bmatrix}\right) = 0 \implies x_2 y_1 - y_2 x_1 = 0.$$

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



Equations

$h_1 = (x_1 - u_1)u_3 - u_2 y_1$
$h_2 = y_1 - u_3$
$h_3 = x_2 y_1 - y_2 x_1$
$h_4 = (u_1 - u_2)y_2 - u_3(u_1 - x_2)$

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

$$\implies \quad x_2^2 + y_2^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2.$$

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

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

Step 3. Computation to prove theorem.

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

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

Similarly verify $g_2 \in \sqrt{I}$.

What can go wrong?

Application 3: What can go wrong?

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

Application 3: What can go wrong?

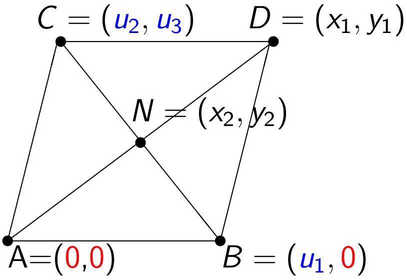
Errors: **any claim is true if** $I = \langle h_1, h_2, \ldots \rangle = \langle 1 \rangle$.
$\implies$ check that the Gröbner basis for I is not $\{1\}$!!

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



N is the midpoint of $\overline{AD}$
$\implies N = \frac{(A+D)}{2}$ so
$x_2 = \frac{x_1}{2}, \quad y_2 = \frac{y_1}{2}$!!

Graduate student project

1. Implement Buchberger's algorithm.
2. Study and implement the **FGLM** basis conversion.

   J.C. Faugere, P. Gianni, D. Lazard, T. Mora.
   Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comp.*, **16**, 329–344, 1993.

3. Show that **FGLM works** using Trinks' system.

$$\{45p + 35s - 165b = 36,\quad 35p + 40z + 25t - 27s = 0,$$

$$15w + 25ps + 30z - 18t - 165b^2 = 0,\quad -9w + 15pt + 20zs = 0,$$

$$wp + 2zt = 11b^3,\quad 99w - 11sb + 3b^2 = 0\}$$

Thank you for coming.

On-line course materials

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