Teaching Commutative Algebra and Algebraic Geometry using Computer Algebra Systems

Michael Monagan*
Department of Mathematics, Simon Fraser University
Burnaby B.C. V5A 1S6, Canada
mmonagan@cecm.sfu.ca

Abstract

In teaching a mathematics course in commutative algebra and algebraic geometry, we would like students also be able to use a computer algebra system to solve real problems that they might encounter in the future, whether in their own research or in industry. The purpose of this paper is to firstly describe how we use computer algebra in the course and secondly to provide a list of applications problems that we have found to be suitable for such a course.

1 Introduction

We have been teaching a mathematics course in *Commutative Algebra and Algebraic Geometry* which uses Gröbner bases and `Maple` for computations at Simon Fraser University since 2006. The course has been offered in 2006, 2008, 2010, and 2012 to senior undergraduate students and graduate students. These students are mostly mathematics majors. Typically we also have one or two computing majors. We require students to have taken a first course in abstract algebra (in groups or rings and fields) as a prerequisite, so that students have learned to write proofs.

The course was first offered in 2006 to undergraduate students as *MATH 439 Algebraic Systems* and graduate students as *MATH 819 Special Topics in Algebra: Gröbner Bases and Algebraic Geometry*. We subsequently offered it in 2008, 2010 and 2012. For 2012 we formalized the undergraduate course as *MATH 441 Commutative Algebra and Algebraic Geometry*. The course ran as a 12 week course with two 2 hour lecture periods per week. Enrollment in the course is shown in the following table.

major	2006	2008	2010	2012
mathematics	5	15	11	27
computing	0	0	0	1
math & cmpt	0	2	2	2
other	0	4	0	0
graduate	5	6	4	1
total	10	27	21	31

In this paper we wish to share with the reader how we integrate computer algebra into the course. This requires a careful choice of a textbook which we will consider in section 2. We use Maple. Maple has three capabilities that we use, (i) tools for graphing curves and surfaces, (ii) the `Groebner` package for computing Gröbner bases and related operations, and the `PolynomialIdeals` package for ideal theoretic

*This work was supported by Maplesoft and the MITACS NCE of Canada.

computations. The main contribution we make in this paper is to describe three applications problems that we have found are both genuine applications and provide useful training for the student. These are presented in section 3. In section 2 we provide some information about the content and textbooks currently available, and the course project that we assign graduate students. To end the introduction we provide some information about the level of Maple training that we provide and assessment. We mention also here that we maintain a website for the course where we put assignments and supplementary materials, primarily Maple worksheets and papers at http://www.cecm.sfu.ca/~mmonagan/teaching.

Maple Training

Our university has a campus wide site license for Maple. Maple is available on desktop computers in assignment labs, the library, and on our department's computers and is thus generally accessible. Our mathematics majors have already used Maple in a previous second year course. For students who have not used Maple before, or who would like a refresher, we give them a one hour hands-on tutorial on Maple in a lab setting and point them to Maple worksheet that we have prepared which has examples of all the Maple commands that we will use in the course. Subsequent Maple training is provided by some in-class demos and several handouts of Maple worksheets. We have found that this is sufficient Maple training for most students. However, having said that, students do get stuck with Maple. Maple problems are resolved after class or in office hours. Some problems require us to execute the student's worksheet.

Assessment

Undergraduate students were asked to complete six assignments worth 10% of the course grade each and a final exam worth 40% of the course grade. At least 25% of each assignment is done in Maple. In addition, graduate students were given a course project and approximately one additional exercise per assignment. Students used Maple on each assignment and because we wanted to have problems which required computation on the final exam, we ran the final exam as a 24 hour take home final. Students had access to the textbook, their notes, and other course materials for the final exam. The final exam consisted of 10 questions, Maple was needed for $3\frac{1}{3}$ questions worth 36% of the marks and could be used to check answers to 2 questions. We maintain a website for the course where we put assignments and supplementary materials, primarily Maple worksheets and papers at http://www.cecm.sfu.ca/ mmonagan/teaching.

2 Course Content

In constructing the course outline, faculty listed the following topics as possible topics for a first course in commutative algebra and algebraic geometry.

- affine varieties and ideals in polynomial rings,
- the Hilbert basis theorem, Hilbert's Nullstellensatz
- the elimination theorem, solving equations, and resultants,
- Zariski topology
- singular points, genus of a curve,
- irreducible varieties, prime ideals, maximal ideals,
- quotient rings and rational maps,
- dimension, Bezout's theorem,
- projective varieties.
- Gröbner bases, Buchberger's algorithm, and applications.

We strongly feel that students taking a course in commutative algebra and algebraic geometry should be equipped to do computations in the area. Whether the student goes on to grad school to do research in this area, or gets a job in industry, he or she will probably need to do computations. Even if the student becomes a teacher, being able to use a tool like Maple will be invaluable, even if it is only to graph surfaces and solve equations. We provide intruction for doing the following in Maple.

- graphing of curves and surfaces,
- solving polynomial equations exactly and numerically,
- computing Gröbner bases and related operations,
- other algorithms e.g. computing the prime components of the radical of an ideal,
- using Gröbner bases to solve polynomial systems and eliminate variables,
- other applications e.g. using Gröbner bases to prove theorems in geometry

2.1 Textbooks

The number of textbooks which cover Gröbner bases is steadily increasing. Early texts were mostly at the graduate level. They focused on developing the theory of Gröbner bases, describing Buchberber's algorithm for computing them, and showing applications in various areas of mathematics. These include Adams and Loustaunau (1), Becker and Weispfenning (2), Cox, Little, and O'Shea (5), Schenck (11), and Vasconcelos (15). These texts are not suitable for an undergraduate course in commutative algebra and algebraic geometry. The material is either too advanced or the focus is too heavy on computation.

There are now several undergraduate texts in algebra which include substantial introductions to Gröbner bases and some material on commutative algebra, such as Reilly (10), Fraleigh (8), and Lauritzen (9). But these do not integrate the application of Gröbner bases into the material in a substantive way. Furthermore, there are few or no computer based exercises. And since computing Gröbner bases by hand is not feasible for most applications, these texts are not suitable for our purpose.

We need is a text in commutative algebra and algebraic geometry which integrates the use of Gröbner bases and the use of the computer. The only text that we know of that attempts this is Cox, Little and O'Shea's *Ideals, Varieties and Algorithms*. So this is the text that we use. We will refer to it as CLO. There is sufficient material in this text for graduate students who have not already taken a course in commutative algebra and algebraic geometry.

2.2 Course project

To develop computation skills for graduate students in mathematics, we give graduate students a course project with a "research feel" to it. We ask them to read the paper of Faugere, Gianni, Lazard and Mora (7) which shows how to convert a Gröbner basis for an ideal in one term ordering to another.[1] We ask the student to implement Buchberger's algorithm and the FGLM algorithm in Maple. Typically students need some help with coding and debugging. But it has not been an insurmountable challenge for them. To test the FGLM algorithm we use the Trinks system from (14).

$$\{45p + 35s - 165b = 36, 35p + 40z + 25t - 27s = 0, 15w + 25ps + 30z - 18t - 165b^2 = 0,$$
$$-9w + 15pt + 20zs = 0, wp + 2zt = 11b^3, 99w - 11sb + 3b^2 = 0\}$$

This system has 10 solutions. It is just big enough so that if you try to compute a lex Gröbner basis using a Buchberger's algorithm, it will probably take a very long time. We ask the student to find a permutation of p, s, b, z, t, w for which Buchberger's algorithm does take a long time. Then we ask the

[1] The description of the algorithm and example in Chapter 2 of (5) is sufficient for the student to understand the algorithm.

student to compute this lex basis via a graded basis and the FGLM algorithm, to verify that FGLM is indeed much faster. Mathematics students are often very surprised, but satisfied, when they see their own implementation of one method run 50 times faster than another.

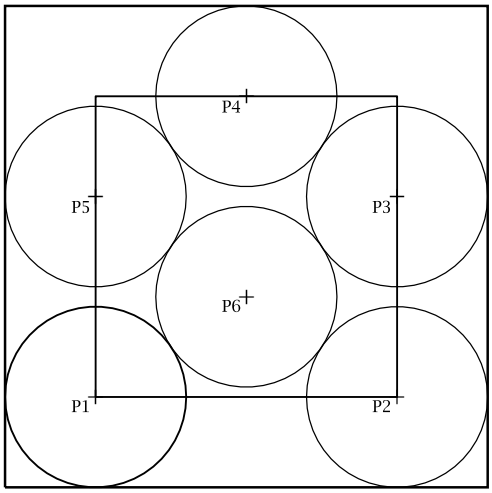
3 Applications

It is easy to give the students "routine" exercises in which they need to compute a Gröbner basis and do something with it. What we really need is applications which force the student do more than just follow a recipe. Three applications that we have found to be valuable are described in this section. We spend the last two weeks focussed on applications. Many of our students have said in the course evaluation that these problems were the most interesting and useful part of the course.

3.1 Circle Packing Problems

Consider the problem of putting n points in the unit square maximizing their separating distance m. This problem is equivalent to the problem of packing n disks in the unit square maximizing their radius r. The relationship between the two is $r = \frac{m}{2(m+1)}$. The problem has a long history with optimal solution for $n = 10$ quite difficult. In (16) Würtz, Monagan and Peikert find optimal solutions for several n including $n = 10$ and $n = 13$ and determine m.

For our course we assume we are given a packing and we want to determine r and m. That is, we are given which disks touch the boundary of the unit square, which disks touch each other, and which disks are free, and we want to determine r then m. For example, below is the optimal packing for $n = 6$.



We will determine m using the inner square rather than r using the outer square because the equations are simpler. Given co-ordinates (x_i, y_i) for the n points P_i, we have simple boundary conditions, e.g. $x_1 = y_1 = 0$. For each two touching disks we apply Pythagoras' theorem to obtain e.g. $(x_6 - x_1)^2 + (y_6 - y_1)^2 = m^2$. Next we can obtain simpler relations from any symmetry present in the packing, e.g. $y_3 = y_5$. We construct the ideal

$$I = \langle x_1,\ y_1,\ (x_6 - x_1)^2 + (y_6 - y_1)^2 - m^2,\ y_3 - y_5,\ \ldots,\ \rangle$$

and compute $I \cap \mathbb{Q}[m]$ using the elimination theorem using the appropriate Gröbner basis computation.

Many things can go wrong. First we can easily input equations incorrectly for larger n. In this regard, it is helpful if the student is instructed to write a little Maple procedure $P(a,b)$ which generates the equation $(x_b - x_a)^2 + (y_b - y_a)^2 - m^2$ automatically. Second is degeneracy. We may think, since there are 13 unknowns $x_1, ..., x_6, y_1, ..., y_6$ and m, that any 13 equations will do. However, this is usually not the case in real applications. For example, we when we first solved this problem, we constructed the following system which has a degeneracy.

$$\{x_1 = 0,\ y_1 = 0,\ x_2 = 1,\ y_2 = 0,\ x_3 = 1,\ x_5 = 0,\ y_4 = 1,\ y_3 = y_5,\ x_4 = 1/2,\ x_6 = 1/2,$$

$$(x_6 - x_1)^2 + (y_6 - y_1)^2 = m^2,\ (x_4 - x_3)^2 + (y_4 - y_3)^2 = m^2,\ (x_3 - x_6)^2 + (y_3 - y_6)^2 = m^2\}$$

Using Gröbner bases to eliminate x_i, y_i we obtain $144m^4 - 232m^2 + 65 = 0$. This polynomial factors as $4m^2 - 5 = 0$ and $36m^2 - 13 = 0$. The latter is the correct solution with $m = 0.601$. The former with $m = 1.118$ is a degenerate solution which arises because it allows P_2 to be on top of P_3, P_5 to be on top of P_1 and P_6 to be on top of P_4.

Dealing with and explaining degeneracy is a very good exercise for the student. Another typical degeneracy is $m = 0$. It is often useful to impose a priori that $m \neq 0$. How do we do this algebraically? We include $1 - mt = 0$ for a dummy variable t as an equation. In this way students learn the "tricks of the trade".

For the assignment we ask the student to compute the minimal polynomial for four packings for $n = 10$ from (16) (the last one is the optimal one). Here it becomes necessary that the student identify symmetry in the packing as otherwise the Gröbner basis computation will take a very long time.

Another thing that can go wrong is that in real papers, there are errors and students need to learn to detect and correct them. In particular, there are two errors in the figures of the four packings in (16). There are disks which are not shown as touching but are touching. If the equation is not included one cannot solve for m as $I \cap \mathbb{Q}[m] = \{0\}$.

3.2 Hilbert's Nullstellensatz and Graph Coloring

Let G be a graph on n vertices and m edges. Recall that G is k-colorable if we can assign each vertex in G to one of k colors in such a way that no two adjacent vertices have the same color. The problem of testing if G is k-vertex colorable can be formulated as testing whether a polynomial system has a solution over $\mathbb{C}$. For example, consider the wheel graphs W_3 and W_4 below.

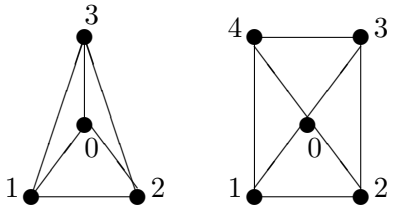


Figure 1: Wheel graphs W_3 and W_4.

Suppose $k = 3$ and we use colors red, green and blue. Consider the wheel graph W_3 above. W_3 is not 3-colorable because vertices 1, 2, and 3 form a triangle and so require 3 distinct colors. Hence vertex 0 needs a 4'th color. Graph W_4 is 3-colorable; assign vertex 0 red, vertex 1 and 3 blue and vertex 2 and 4 green.

The construction of the polynomial system is as follows. For each vertex v in G equate $x_v^k = 1$. This equation has k roots over $\mathbb{C}$, namely the k roots of unity. The k roots of unity represent the possible colors of the vertices. Thus the system

$$\{x_1^k - 1 = 0,\ x_2^k - 1 = 0,\ \ldots,\ x_n^k - 1 = 0\}$$

encodes all colorings of G with no edges. Now if u, v is an edge in G, we want to constrain G so that vertices u and v have different colors. We do this by adding the equation $\frac{x_u^k - x_v^k}{x_u - x_v} = 0$.[2] Thus for W_3 we obtain the polynomial system

$$S = \{x_0^3 - 1,\ x_1^3 - 1,\ x_2^3 - 1,\ x_3^3 - 1,\ x_0^2 + x_0x_1 + x_1^2,$$

$$x_0^2 + x_0x_2 + x_2^2,\ x_0^2 + x_0x_3 + x_3^2,\ x_1^2 + x_1x_2 + x_2^2,\ x_1^2 + x_1x_3 + x_3^2,\ x_2^2 + x_2x_3 + x_3^2\}.$$

Thus we construct a system S with $n + m$ equations in n unknowns such that G is k-colorable if and only if the variety $\mathbb{V}(S)$ is not empty over $\mathbb{C}^n$. Equivalently, G is k-colorable if and only if the ideal $I = \mathbb{I}(S)$ is not $\langle 1 \rangle$. It is now straight foward to compute a reduced Gröbner basis for I and check if it is $\{1\}$.

In (6), de Loera, Lee, Malkin and Margulies develop an alternative approach based on the Nullstellensatz. The Nullstellensatz says $\mathbb{V}(S)$ is not-empty over $\mathbb{C} \iff 1 \in I$. Now letting $I = \langle f_1,\ f_2,\ \ldots,\ f_{n+m} \rangle$, if $1 \in I$ then there exist polynomials $h_1,\ h_2,\ \ldots h_{n+m} \in \mathbb{Q}[x_0, x_1, \ldots, x_n]$ satisfying

$$1 = h_1f_1 + h_2f_2 + \ldots h_{n+m}f_{n+m}. \tag{1}$$

The idea of the method is to try to find the polynomials $h_1,\ h_2,\ \ldots,\ h_{n+m}$ satisfying (1) by trying polynomials with unknown coefficients of total degree $d = 1$ then $d = 2$ then $d = 3$, etc., up to some bound. Equating coefficients in $x_0, x_1, \ldots, x_n$ in (1) leads to a system of linear equations over $\mathbb{Q}$. If this system has a solution then G is not k-colorable and we say the polynomials $h_1,\ h_2,\ \ldots,\ h_{n+m}$ are a *certificate* of the non-colorability of G.

Students can try this on familiar graphs e.g. the Petersen graph, a graph with 10 vertices and 15 edges, hence 25 equations to see how big d is. The smallest value of d for which a certificate exists is a measure of the difficulty of the graph. The authors prove that instead of solving the linear system over $\mathbb{Q}$ we can solve over $\mathbb{Z}_p$ instead for any p for which p does not divide k. In particular, to test for 3-colorability, we can work over $\mathbb{Z}_2$ which greatly simplifies the arithmetic.

This is lovely connection between algebra and graph theory, between the Nullstellensatz and graph 3-colorability. Many students liked this application.

3.3 Automatic Theorem Proving

Chapter 6 of CLO (4) is devoted to presenting two major applications. The first is the use of Gröbner bases in robotics. The second is the use of Gröbner bases to proving theorems in geometry. Of these two, we have found the application to theorem proving to be the better by far. Not only is it the more interesting, but it is also the richest in terms of application problems that the students can reasonably attempt. Furthermore, it requires less time to develop. To illustrate how this is done we follow the first example from Chapter 6 of CLO. Figure 2 shows a parallelogram $ABCD$.

The theorem says that the diagonal bisectors AC and BD intersect at N the midpoint of AC and BD. To prove the theorem we fix co-ordinates of the points A, B, C, D and N and write down equations. To simplify the equations, and the resulting Gröbner basis computation, we place the parallelogram with A

[2] An alternative would be to add the equation $t(x_u - x_v) = 1$ for dummy t.

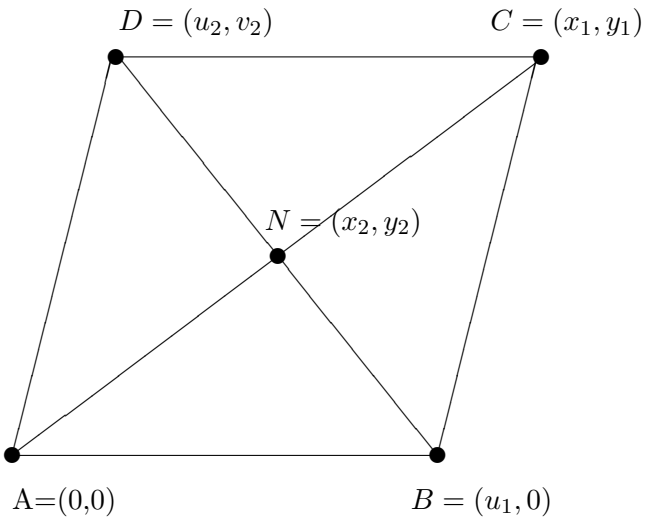


Figure 2: A parallelogram $ABCD$.

at origin and B on x axis. The parameters u_1, u_2, v_2 complete the specification of the parallelogram. The variables x_1, y_1 and x_2, y_2 are fixed by the parameters, that is, they are functions of them that we will solve for. Thus there are 4 unknowns so we need 4 equations. The equations $h1 = 0, h2 = 0, h3 = 0, h4 = 0$ can be obtained by asserting that (i) AD is parallel to BC, (ii) AB is parallel to CD, and (iii) N is at the the intersection of AC and BD. We could do this by requiring N is on the line segment AC and N is on the line segment BD. Now the theorem says that N is at the midpoint of AC and BD. How do we encode this? The text suggests requiring that the lengths of AN and NC are the same and the lengths BN and ND are the same. This leads to two quadratic equations $x2^2 + y_2^2 = x_1^2 + y_1^2$ and $(x_2 - u_2)^2 + (y_2 - v_2)^2 = (x_2 - u_1)^2 + y_2^2$. One of the things we want to teach the student is that linear equations lead to much simpler computations than quadratic equations. So a better way to encode this is that N is at the midpoint of AC means that the vectors N, A, C satisfy $N = (A + C)/2$ from which we get linear equations $x_2 = (0 + x_1)/2$ and $y_2 = 0 + y_1/2$. We express the theorem as two polynomial *consequences* $g_1 = x_2 - x_1/2$ and $g_2 = y_2 - y_1/2$.

To prove the theorem, we could solve the four equations $h_1 = 0, h_2 = 0, h_3 = 0, h_4 = 0$ to obtain solutions for x_1, y_1, x_2, y_2 as functions of u_1, u_2, v_2 and then check that $g_1(x_1, x_2, y_1, y_2) = 0$ and $g_2(x_1, x_2, x_3, x_4) = 0$. But explicitly solving equations may lead to nasty radicals, though not for this trivial example. We proceed as follows. We want to check that g_1 and g_2 vanish on the variety $\mathbb{V}(h_1, h_2, h_3, h_4)$. Over $\mathbb{C}$ this is equivalent to checking if g_1, g_2 are in the radical of the ideal $I = \langle h_1, h_2, h_3, h_4 \rangle$. Or is it? Here is a key point. We want to consider the ideal I in the polynomial ring $\mathbb{R}(u_1, u_2, v_2)[x_1, y_1, x_2, y_2]$ and not in the polynomial ring $\mathbb{R}[u_1, u_2, v_2, x_1, y_1, x_2, y_2]$ because if we use the former we have $\langle v_2 x_2 - u_1 v_2 \rangle = \langle x_2 - u_1 \rangle$ which corresponds to canceling out v_2 in the equation $v_2 x_2 = v_2 u_1$ which we want to allow.

How do we test if $g_1, g_2 \in \sqrt{I}$, the radical of I? Note, if we can show that $g_1, g_2 \in I$ then this implies $g_1, g_2 \in I$ but the reverse is not necessarily true. In CLO we have already seen in 4.2 how to test for radical membership. The procedure is as follows. Let $J = \langle I, 1 - t g_1 \rangle$ for a dummy variable t. Then g_1 is in $\sqrt{I}$ if and only if $J = \langle 1 \rangle$ over $\mathbb{R}(u_1, u_2, v_2)[x_1, y_1, x_2, y_2, t]$. So it suffices to simply check that a reduced Gröbner basis for J is $\{1\}$. Herein lies a trap for the student. If the student makes a mistake in the equations such that $I = \langle 1 \rangle$, which is easy to do if you they additional "simpler" equations, then every polynomial g will be in the radical of $\langle 1 \rangle$! It is better to first compute a Gröbner basis for I and look at it, to check that it is not $\{1\}$, then test if $g_1, g_2 \in I$ and if not, apply the radical membership test.

Another more likely problem to occur is that g is not in $\sqrt{I}$ because of an error in the equations. Since the theorems will typically have 10, 20 or more equations, this forces the student to carefully write out the equations. Another difficulty is that some geometric theorems are true over $\mathbb{R}$ (e.g. true in the plane) but not true over $\mathbb{C}$. The tests for ideal membership and radical membership using Gröbner bases are being done over $\mathbb{C}$.

References

[1] William Adams and Philippe Loustaunau. *An Introduction to Gr"obner Bases.* Graduate Texts in Mathematics, American Math. Soc., 1994.

[2] Thomas Becker and Volker Weispfenning. *Gröbner Basis - A Computational Approach to Commutative Algebra,* Springer Verlag Graduate Texts in Mathematics **141**, 1993.

[3] Francisco Botana and Tomas Recio. *Automated Deduction in Geometry,* Springer Verlag LNAI **4869**, 2006.

[4] David Cox, John Little and Donal O'Shea. *Ideals, Varieties and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra,* Springer Verlag, 3rd ed., 2007.

[5] David Cox, John Little and Donal O'Shea. *Using Algebraic Geometry,* Springer Verlag, Graduate Texts in Mathematics **185**, 1998.

[6] 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.

[7] 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.

[8] John B. Fraleigh. *A First Course in Abstract Algebra,* Addison Wesley, 7th ed., 2003.

[9] N. Lauritzen. *Concrete Abstract Algebra - From Numbers to Gröbner Bases,* Cambridge University Press, 2003.

[10] Norman Reilly. *Introduction to Applied Algebraic Systems,* Oxford University Press, 2010.

[11] Hal Schenck. *Computational Algebraic Geometry,* Cambridge University Press, 2003.

[12] Pascal Schreck, Julien Narboux, Jürgen Richter-Gebert (Eds.) *Automated Deduction in Geometry,* Springer Verlag LNAI **6877**, 2011.

[13] Thomas Sturm, Christoph Zengler (Eds.) *Automated Deduction in Geometry,* Springer Verlag LNAI **6301**, 2011.

[14] W. Trinks. Über B. Buchbergers Verfahren, Systeme algebraische Gleichungen zu lösen. *J. Number Theory* **10**, 475–488, 1978.

[15] Wolmer Vasconcelos. *Computational Methods in Commutative Algebra and Algebraic Geometry,* Springer Verlag, Algorithms and Computation in Mathematics **2**, 1998.

[16] D. Würtz, M. Monagan and R. Peikert. The History of Packing Circles in a Square. *MapleTech* Special Issue, Birkhaüser, 35–42, 1994.