Teaching Commutative Algebra and Algebraic Geometry using Computer Algebra Systems

Michael Monagan
mmonagan@cecm.sfu.ca
Department of Mathematics, Simon Fraser University
Burnaby, BC, V5A 1S6,
CANADA

Abstract

In teaching a mathematics course in commutative algebra and algebraic geometry, we would like to equip students with a computer algebra system so they can solve problems that they might encounter in their own research or in industry. The purpose of this paper is to firstly describe how we use computer algebra in the course that we teach and secondly, to share with the reader a list of applications which make use of the computer 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 at Simon Fraser University since 2006. We use `Maple` for Gröbner bases computations and applications. The course has been offered in 2006, 2008, 2010, and 2012 to senior undergraduate students, mostly mathematics majors, and first year graduate students. 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
math & computing	0	2	2	2
other	0	4	0	1
graduate	5	6	4	1
total	10	27	21	31

In 2012 we formalized the course as *MATH 441 Commutative Algebra and Algebraic Geometry*. 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 text we use is Cox, Little, and O'Shea's `Ideals, Varieties and Algorithms` from [5]. This text is unique in its attempt to integrate the use of computer algebra into the material as well as into the exercises. In addition

to posing exercises that require the use of the computer, the authors develop algorithmic solutions to problems in commutative algebra and algebraic geometry in the material. As the authors note, this brings a classical, constructive approach to the subject, which makes the material more accessible to undergraduate mathematics students.

The development and application of Gröbner bases in the text plays an analogous role that the development and application of Gaussian elimination to row-reduce matrices to row Echelone form plays in a first course in Linear Algebra. Would you teach Linear Algebra without teaching Gaussian elimination? Probably not. You would not only lose out on concrete applications but you would have to find alternative proofs to some theorems.

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 more detail in section 2. It also requires selecting a computer algebra system. We use Maple though other computer algebra systems with a Gröbner basis facility and graphics facilities could be used.

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. One is from our own research in [16] and the other two are from the work of others. These are presented in section 3.

To end the introduction we provide some information about the level of Maple training that we provide and assessment. We maintain a website for the course where we put assignments and supplementary materials, primarily Maple worksheets and papers at MATH 441.

1.1 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 in a lab setting and point them to Maple worksheet which has examples of all the Maple commands that we will use in the course. Subsequent Maple training is provided by in-class demos and 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 and require the instructor to be able to examine a student's Maple worksheet. We found that Email is not a good medium for resolving problems with Maple. I encourage students to bring their Maple worksheet to my office on a memory stick where I can open it and work with the student.

1.2 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. About 25% of the assignment problems are done in Maple. The rest are traditional pencil and paper exercises including proofs. Graduate students were also given a course project and approximately one additional exercise per assignment. 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.

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 think students taking a course in commutative algebra and algebraic geometry should be equipped to do computations in the area, hence, Gröbner bases need to be covered. 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 at some point. 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 instruction for doing the following in Maple. The main capabilities of Maple that we use include

- tools for graphing curves and surfaces,
- factoring polynomials and computing roots of polynomials,
- the `Groebner` package for computing Gröbner bases and related operations,
- the `PolynomialIdeals` package for ideal theoretic computations, e.g., computing the ideal quotient, intersection, and computing the prime components of the radical of an ideal.

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 [6], Schenck [12], 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 such as Reilly [11], Fraleigh [8], and Lauritzen [10]. But these texts do not integrate the application of Gröbner bases into the material in a substantive way and there are few, if any computer based exercises. We need a commutative algebra and algebraic geometry text which integrates the use of Gröbner bases and the use of the computer. The only text that we know of that achieves this is Cox, Little and O'Shea's *Ideals, Varieties and Algorithms*. So this is the text that we use.

2.2 Gröbner bases

For the reader who is not familiar with Gröbner bases we develop an example to illustrate some applications. Gröbner bases were discovered by Bruno Buchberger in [4]. He named them after his Ph.D. supervisor. Buchberger gave an algorithm for computing them which is now known as Buchberger's algorithm. Consider the following system of 3 equations in 3 unknowns x, y, z over $\mathbb{R}$.

$$S = \{x^2 + y^2 + z^2 = 1, xy + yz + zx = 1, xyz = 1\}.$$

Let I be the corresponding ideal, that is,

$$I = \langle x^2 + y^2 + z^2 - 1, xy + yz + zx - 1, xyz - 1\rangle.$$

A Gröbner basis for I is a basis for I that depends on how we order monomials. The simplest monomial ordering is lexicographical or alphabetical order. In lexicographical order, with $x > y > z$, the terms of the polynomial

$$f = xyz^2 + xy^2z + x^2y$$

are ordered as $x^2y > xy^2z > xyz^2$ corresponding to the alphabetical ordering $xxy < xyyz < xyzz$ and hence we would write the polynomial as

$$f = x^2y + xy^2z + xyz^2$$

showing x^2y as the leading term of f. There are many characterizations for a Gröbner basis for a given ideal I and monomial ordering $>$. The following one captures a key property of Gröbner bases.

Definition 1 *Let $I = \langle f_1, f_2, \ldots, f_s\rangle$ be an ideal in a polynomial ring $k[x_1, x_2, \ldots, x_n]$ for some field k. Let $G = \{g_1, g_2, \ldots, g_t\}$ be a set of polynomials and let $<$ be any monomial ordering. Then G is a Gröbner basis for I wrt $<$ if the remainder of f divided by G is 0 if and only if $f \in I$.*

Note, the monomial ordering fixes the leading terms of the divisor and dividend in the division algorithm and the definition automatically forces G to be a basis for I. The unique *reduced* Gröbner basis for our example I is given by

$$\begin{aligned} G = \{ \quad & x + y - z^5 - z^4 + z^3 + 3\,z^2 + z + 1, \\ & y^2 - yz^5 - yz^4 + yz^3 + 3\,yz^2 + yz + y - z^5 + z^3 + 2\,z^2 - z + 2, \\ & z^6 - z^4 - 2\,z^3 + z^2 - 2\,z + 1\} \end{aligned}$$

where the leading terms x, y^2, and z^6 are highlighted in blue. It was obtained by imposing that each polynomial $g \in G$ additionally satisfies (i) it is monic and (ii) no term in g is divisible by the leading terms of the other polynomials in G.

A Maple worksheet showing how to compute this Gröbner basis is available at Groebner.mw along with a .pdf version at Groebner.pdf. Now the zeroes of the polynomials in G are the same as those of the original system (the main application of Gröbner bases). Notice how the polynomials in G progressively eliminate variables and tell us how to solve the original polynomial system by back substitution. This follows more generally from the following elimination theorem.

Theorem 2 *If $>$ is lexicographical order with $x_1 > x_2 > \ldots > x_n$ and G is a Gröbner basis for I wrt $>$ then $G \cap k[x_i, x_{i+1}, \ldots x_n]$ is a Gröbner basis for (the ideal) $I \cap k[x_i, x_{i+1}, \ldots x_n]$ wrt $>$ for $1 \leq i \leq n$.*

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 focused 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. Another valuable aspect of these applications is that the student is asked to read a research paper and, by implementing some of the ideas, be forced to understand the results in the paper, and secondly, by reproducing some of the computational results, be able to check results in the paper.

3.1 Circle Packing Problems

Consider the problem of putting n points in the unit square maximizing their separating distance m. Figure 1 shows the optimal packing for $n = 6$ points $P_1, P_2, \ldots, P_6$. This problem is equivalent to the problem of packing n disks in the unit square maximizing their radius r. Again, see Figure 1. The relationship between the two is $r = \frac{m}{2(m+1)}$.

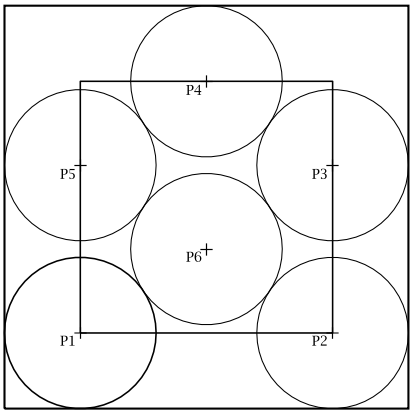
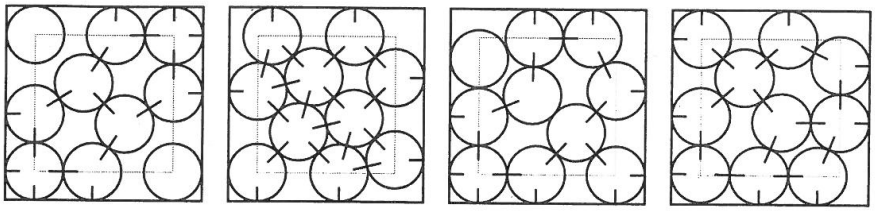


Figure 1: Optimal packing for $n = 6$ circles in the unit square.

For $n = 10$, the problem has a long history with optimal solution being quite difficult to find. Figure 2 shows a sequence of successively better packings for $n = 10$. The last one is the optimal one. It was found by Würtz, Monagan and Peikert in [16]. Note, the bottom left circle does not touch the x axis which is indicated by the lack of a bold dash.

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 or m. We will determine m using the inner square rather than r using the outer square because the equations are simpler.



$m = 0.41953$ $m = 0.42013$ $m = 0.42118$ $m = 0.42129$

Figure 2: Packings for $n = 10$ circles. The last is the optimal one.

We outline the procedure for $n = 6$. Referring back to Figure 1, 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 disks that touch 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. This we hope will give us the minimal polynomial for m.

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, when we first solved this problem, we constructed the following system which has a degeneracy.

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

$$(x_6 - x_1)^2 + (y_6 - y_1)^2 = m^2,\ (x_6 - x_5)^2 + (y_6 - y_5)^2 = m^2,\ (x_4 - x_5)^2 + (y_4 - y_5)^2 = m^2\}$$

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.

A Maple worksheet for the computations that illustrates the degenerate case mentioned here may be found at Scattering.mw. A .pdf file for the worksheet may be found at Scattering.pdf.

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 learns the value of the "tricks of the trade".

For the assignment we ask the students to compute the minimal polynomial for four packings for $n = 10$ from [16] shown in Figure 2. 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, in the third packing shown in Figure 2, the middle two disks should be touching each other.

3.2 Automatic Theorem Proving in Geometry

Chapter 6 of [5] is devoted to presenting two main 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 prefer the application to theorem proving. Not only is it the more interesting, but it is also richer in terms of application problems that students can reasonably attempt. For more information about proving theorems in algebraic geometry we refer the reader to [3, 14, 13] for the 2006, 2008, and 2010 proceedings of Automated Deduction in Geometry. An early reference is Kuntzler and Stifter [9]. To illustrate how this is done we follow the first example from Chapter 6 of [5]. Figure 3 shows a parallelogram $ABCD$.

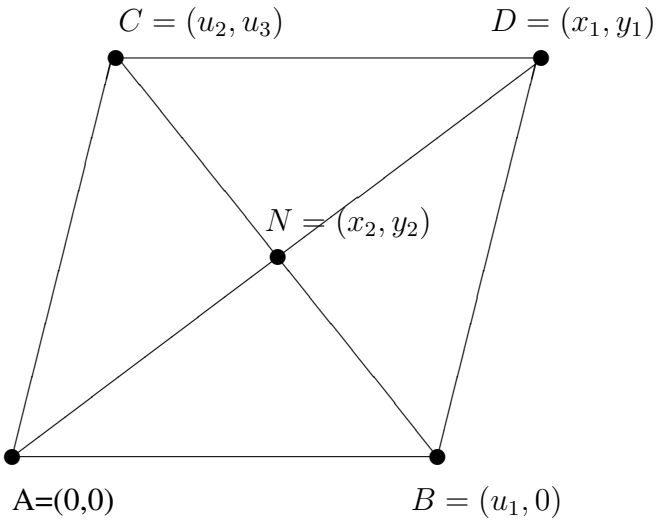


Figure 3: A parallelogram $ABCD$.

Let N be the intersection of the diagonal bisectors AD and BC. The theorem says that N is the midpoint of AD and BC. 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 deliberately place the parallelogram with A at origin and B on x axis so that three co-ordinates are 0. The parameters u_1, u_2, u_3 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 $h_1 = 0, h_2 = 0, h_3 = 0, h_4 = 0$ which can be obtained by asserting that (i) AC is parallel to BD, (ii) AB is parallel to CD, and N is at the the intersection of AC and BD which we impose by requiring (iii) N is on the line segment AD and (iv) N is on the line segment BC.

Now the theorem says that N is midpoint of AD and BC. How do we encode this? The text suggests requiring the lengths of AN and ND to be equal and the lengths BN and NC to be equal.

To avoid square roots, we work with the square of the lengths. This leads to two quadratic equations $x_2^2 + y_2^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$ and $(x_2 - u_2)^2 + (y_2 - u_3)^2 = (x_2 - u_1)^2 + y_2^2$. 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 impose that N is at the midpoint of AD is to require that the vectors $N - A = (D - A)/2$. From this we obtain two linear equations $(x_2 - 0) = (x_1 - 0)/2$ and $(y_2 - 0) = (y_1 - 0)/2$. 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, u_3 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 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 $\mathbb{R}(u_1, u_2, u_3)[x_1, y_1, x_2, y_2]$ and not in the polynomial ring $\mathbb{R}[u_1, u_2, u_3, x_1, y_1, x_2, y_2]$ because if we use the former we have the ideal $\langle u_3 x_2 - u_1 u_3 \rangle = \langle x_2 - u_1 \rangle$ which corresponds to canceling out u_3 in the equation $u_3 x_2 = u_3 u_1$ 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 $g_1, g_2 \in \sqrt{I}$ but the reverse is not necessarily true. The procedure to test for radical membership 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 $\mathbb{R}(u_1, u_2, u_3)[x_1, y_1, x_2, y_2, t]$. 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, 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.

An obvious question is, which theorems in geometry can be solved automatically following the procedure outlined. Another issue that we did not explore is that there are examples of geometric theorems which are true over $\mathbb{R}$ (e.g. true in the plane) but not true over $\mathbb{C}$. Our tests for ideal membership and radical membership using Gröbner bases implicitly work over $\mathbb{C}$.

A Maple worksheet of the parallelogram problem from CLO may be found at AutoGeo.mw. A .pdf file for the worksheet may be found at AutoGeo.pdf.

3.3 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. It is well known that the problem is $NP-$complete for $k \geq 3$ in general. The problem of testing if G is k-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 shown in Figure 4.

Suppose $k = 3$ and we use colors red, green and blue. Observe that W_3 is not 3-colorable because vertices 0, 1, and 2 form a triangle and so require 3 distinct colors. Hence vertex 3 needs a 4'th color. Graph W_4 is 3-colorable; assign vertex 0 green, vertices 2 and 4 red, and vertices 1 and 3 blue as shown in Figure 3.

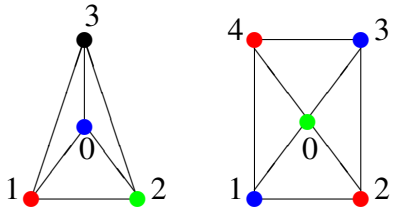


Figure 4: Wheel graphs W_3 and W_4.

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

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

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 $\frac{x_u^k - x_v^k}{x_u - x_v} = 0$. Thus for W_3 we obtain the polynomial system

$$S = \{x_0^3 = 1,\ x_1^3 = 1,\ x_2^3 = 1, x_3^3 = 1, x_0^2 + x_0x_1 + x_1^2 = 0,\ x_0^2 + x_0x_2 + x_2^2 = 0,$$
$$x_0^2 + x_0x_3 + x_3^2 = 0,\ x_1^2 + x_1x_2 + x_2^2 = 0,\ x_1^2 + x_1x_3 + x_3^2 = 0,\ x_2^2 + x_2x_3 + x_3^2 = 0\}.$$

Thus we construct a system S with $n + m$ equations in n unknowns such that G is k-colorable if and only if S has solutions, that is, 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 forward to compute a Gröbner basis for I and check if $1 \in I$.

In [7], de Loera, Lee, Malkin and Margulies develop an alternative approach based on the Nullstellensatz. The Nullstellensatz says $\mathbb{V}(S)$ is not-empty over $\mathbb{C} \iff 1 \in I$. Letting $I = \langle f_1,\ f_2,\ ...,\ f_{n+m} \rangle$, if $1 \in I$ then $\exists$ polynomials $h_1,\ h_2,\ \ldots h_{n+m} \in \mathbb{Q}[x_0, x_1, ..., x_n]$ 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 $h_1,\ h_2,\ ...,\ h_{n+m}$ 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 $x_0, x_1, ..., x_n$ 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 $h_1,\ h_2,\ ...,\ h_{n+m}$ 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 the finite field $\mathbb{F}_p$ instead for any prime p which does not divide k. In particular, to test for 3-colorability, we can work over $\mathbb{F}_2$ which greatly simplifies the arithmetic. But more significantly, they discovered that the degree d of the certificates is often reduced significantly. For W_3 it is reduced from 4 to 1. This is lovely connection between algebra and graph theory, between the Nullstellensatz and graph 3-colorability. Many students liked this application.

A Maple worksheet exploring these computations for W_3 may be found at GraphCol.mw. A .pdf file for the worksheet may be found at GraphCol.pdf.

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 (Eds.). *Automated Deduction in Geometry, Proceedings of ADG 2006,* Springer Verlag LNAI **4869**, 2007.

[4] Bruno Buchberger. *Groebner bases: an algorithmic method in polynomial ideal theory*. Multidimensional Systems Theory. D. Reidel Publishing Company, Dordrecht, pp. 184-232, 1985.

[5] 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.

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

[7] 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.

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

[9] Bernhard Kutzler and Sabine Stifter. On the application of Buchberger's algorithm to automated geometry theorem proving. *J. Symb. Comp.* **2**(4) 389–397, 1986.

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

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

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

[13] Pascal Schreck, Julien Narboux, Jürgen Richter-Gebert (Eds.). *Automated Deduction in Geometry, Proceedings of ADG 2010*, Springer Verlag LNAI **6877**, 2011.

[14] Thomas Sturm and Christoph Zengler (Eds.). *Automated Deduction in Geometry, Proceedings of ADG 2008*, Springer Verlag LNAI **6301**, 2011.

[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.