Research Topics for Seminar Projects – PREMUR 2007

General Information and Logistics

The following are some suggested possible topics for the PREMUR seminar research projects, together with some sources for each topic.

By the end of Week 3 of the seminar, we will aim to have selected the groups and the project topics for three groups of three formed from the seminar. Depending on your preference, this could happen either:

- by you choosing who you would like to work with and what topic you would like to study yourselves (subject to Prof. Little's approval), or
- by having Prof. Little (in consultation with Josean and Luis) form the groups and/or select the topics.

During Weeks 4,5,6,7 of the seminar, you will be working on the project full time (this means working your way through original papers, doing new computations of examples, making conjectures about patterns and trying to prove them, etc.) Each group will have a relatively brief (˜ 30 minute) regularly scheduled meeting for questions and "brainstorming" with Prof. Little each day. Prof. Little and the TA's will be available on the regular schedule for questions as well. In addition, starting on Friday of Week 4, each group will make a short presentation on where they are and what they have done each week to the whole seminar. These presentations will happen on Friday afternoons before the colloquium speakers' talks.

Week 8 will be devoted to writing up the final technical reports on your research and preparing for the final public presentation of your group's results.

Project Topics

1. Linkages and Kempe's Theorem

In mechanical engineering and robotics, an important area of the study is the motions of *mechanical linkages* – collections of rigid segments joined by joints of various types. (For example, simple planar linkages would have rigid segments of fixed length, joined by revolute joints.) We will have looked at a few examples of how varieties, Gröbner bases and resultants can be used to study questions about linkages already in the seminar.

The original interest in linkages started in the 19th century with the invention of steam engines for farm implements, manufacturing, locomotives, etc. One of the early questions in the subject was: How can a linkage be constructed to "turn circular motion into straight-line motion"? This was eventually solved by a French engineer named Peaucellier. Another 19th century British mathematician, A. Kempe (who also published a well-known but unfortunately incomplete proof of the Four Color Theorem for planar maps), studied linkages in great detail.

One of Kempe's interesting results here was a sketch of a proof of a theorem that says that (a bounded portion of) *every* variety $\mathbf{V}(f(x,y))$ in $\mathbf{R}^2$ can be "drawn" by following the trajectory of some point in a suitable mechanical linkage. For this topic, you would start by learning the ideas behind Kempe's proof, which gives (in principle) a method to synthesize a linkage to draw an arc of any given variety, given the polynomial equation $f(x, y) = 0$.

One unfortunate aspect of Kempe's approach is that his linkages to draw even relatively simple curves are extremely complicated. His approach is mainly useful to give an *existence proof* for the linkage. It is an interesting question what a minimal (or close-to-minimal) linkage for a given curve might look like. Recently, there has been some work studying the complexity of the synthesis of Kempe linkages. In particular the paper of Gao, Zhu, Chou, and Ge (see below) gives a polynomial ($O(n^4)$) upper bound on the number of links needed in the mechanism to draw a curve of degree n. The article by Kapovich and Millson (see below) uses a much more sophisticated approach, and is consequently not very easy reading. But its results are much more powerful and general.

The first part of the project would be to understand the proof of Kempe's theorem, and how to synthesize linkages for given curves. The paper of Gao, et. al. is OK for this, but there are some issues they do not address. Part of Kapovich and Millson's contribution was to fix some ambiguities and incomplete aspects of the original work (the "rigidified parallelograms," etc.) The main portion of the project here would be to try to address the following questions:

- A first, more concrete, line of questions would be: Try to find "small" linkages for "simple" curves like $y = x^n$. What do *minimal* linkages (i.e. smallest number of links) for these look like? How might you prove that a linkage is minimal? I do not know of any published work on these specific questions.
- A second, more theoretical line of questions: Is the complexity bound of Gao, et. al. *optimal*, or are there simplifications that are possible? That is, are there better upper bounds for the number of segments in a linkage one would need to draw a general curve of a given degree, or is this bound tight?

References

1) IVA, Chapter 6 for general information on applications of Gröbner bases to questions in geometry of robots, etc.
2) Gao, X.-S., Zhu, C.-C., Chou, S.-S., and Ge, J.-X., "Automated generation of Kempe linkages for algebraic curves and surfaces," Mechanism and Machine Theory, 36 (2001), 1019-1033.
3) Kapovich, M. and Millson, J. "Universality Theorems for configuration spaces of planar linkages," Topology 41 (2002), no. 6, 1051–1107.
4) King, H. "Planar Linkages and Algebraic Sets," ArXiv: math/9807023v1.

2. Offset Curves and Surfaces

The *offset curve* $\mathcal{O}_d(C)$ of a plane curve C at distance d is *essentially* the envelope of the family of circles of radius d centered at the points of the curve ("essentially" since there are are a few technicalities and degenerate situations that must be handled to make the idea precise.)

We saw an example of this construction in the lab work for Week 3 of the seminar in the "robot problem." There is an analogous notion for the offset surface of a surface S in $\mathbf{R}^3$. These ideas are actually very widely applied in applications such as computer-aided manufacturing of machine parts, etc. (For instance, if a circular tool with some fixed radius is moved along a path C in the plane, then the edges of the tool travel along pieces of an offset curve. So it is important to understand the algebraic and geometric properties of these curves.)

The obstacle to understanding curve and surface offsets is that they are typically *much* more complicated objects than the varieties they come from. For instance, the offset of the curve $\mathbf{V}(y - x^3)$ at distance r is given by

$$\begin{aligned}
\mathbf{V}(&- 16r^2 - 216r^6 - 729r^{10} - 2052r^4x^2 + 3645r^8x^2 - 873r^2x^4 - 7290r^6x^4 \\
&+ 16x^6 + 7290r^4x^6 - 3645r^2x^8 + 729x^{10} + 432r^2xy - 4860r^6xy - 32x^3y \\
&+ 7830r^4x^3y - 1080r^2x^5y - 1890x^7y + 16y^2 + 1188r^4y^2 + 1458r^8y^2 + 594r^2x^2y^2 \\
&- 5832r^6x^2y^2 + 1593x^4y^2 + 8748r^4x^4y^2 - 5832r^2x^6y^2 + 1458x^8y^2 - 432xy^3 + 9234r^4xy^3 \\
&- 6318r^2x^3y^3 - 2916x^5y^3 - 1701r^2y^4 - 729r^6y^4 + 1458x^2y^4 + 2187r^4x^2y^4 - 2187r^2x^4y^4 \\
&+ 729x^6y^4 - 4374r^2xy^5 - 1458x^3y^5 + 729y^6),
\end{aligned}$$

a rather complicated curve of degree 10 in x, y (!)

Much research has been done concerning questions such as how the degree and other features of C determines the degree and other invariants (such as the integer called the *genus*) of $\mathcal{O}_d(C)$ (see the articles below). In addition, a very interesting recent article of Alcazar and Sendra (see below) has introduced some interesting tools for understanding the *local shape* of offsets.

For this project, the first step would be to do some experimentation to generate some conjectures concerning the singularities on the offset curves $\mathcal{O}_d(C)$ for $C = \mathbf{V}(y - x^n)$. At the same time, or after, you would read and understand the Alcazar and Sendra article. This will require you to master two new, but very important, ideas in the theory of plane algebraic curves – the notions of *places* and *Puiseux* expansions. (The computer algebra system Singular has a library package that computes these expansions.) Then, you would use the methods from this article to prove answers to the following:

- For which d are there singularities?
- Which points (or places) of the original curve C produce singular points (or places) of the offset?
- Why do the singularities have the shapes or types they do?
- You would then study other curves or families of curves, and try to generalize these results.
- A larger question would be: Exactly what types of singular points can appear on offset curves?
- Also (and this is completely open, as far as I know!) how does any or all of this generalize to offset surfaces of surfaces in $\mathbf{R}^3$?

References

1) Alcazar, J.G. and Sendra, J.R., "Local shape of offsets to algebraic curves," Journal of Symbolic Computation 42 (2007), 338-351.
2) Farouki, R.T. and Neff, C.A. "Algebraic properties of plane offset curves," Computer Aided Geometric Design 7 (1990), 101-127.
3) Farouki, R.T. and Neff, C.A., "Analytic properties of plane offset curves," Computer Aided Geometric Design 7 (1990), 83-99.

3. Automorphisms of the Affine Plane and the Jacobian Conjecture

This topic is more theoretical – no "obvious applications," although that is not to say there are not any(!) An *automorphism* of the affine plane is a polynomial mapping

$$T : (x, y) \mapsto (u(x, y), v(x, y))$$

which is invertible. A famous (notorious?) conjecture states that a mapping T of this form over $\mathbf{C}$ is invertible if the Jacobian determinant:

$$det \begin{pmatrix} \frac{\partial u}{\partial x} & \frac{\partial u}{\partial y} \\ \frac{\partial v}{\partial x} & \frac{\partial v}{\partial y} \end{pmatrix}$$

is a nonzero constant. Although many partial results are known and this question has been studied for about 60 years, there is no known proof(!) One promising reduction has been achieved by H. Bass. The "Jacobian Conjecture" is true for mappings T of degree d if and only if there is a uniform bound C_d on the degrees of the components of the inverse mappings of automorphisms of the affine plane not only over $\mathbf{C}$, but also over all (finitely-generated) $\mathbf{Q}$-algebras. An important reduction in the class of algebras that must be considered here has been made by H. Derksen. It is known that the components of the inverse of a polynomial mapping with degree $d = 2$ always have degree ≤ 2 (that is $C_2 = 2$). Similarly, it was proved in 1998 by Fournié, Furter, and Pinchon, by extensive Gröbner basis calculations, that $C_3 = 9$ (the inverse of every cubic polynomial automorphism of the affine plane has components of degree ≤ 9). However the cases $d \geq 4$ are essentially completely open.

The place to start here would be by working through the calculations in the Fournié, Furter, Pinchon article below to check their results and try to develop an efficient way to carry out these computations. Then, the main goal for this project would be to try to attack the $d = 4$ case, conjecture and hopefully prove a value for C_4. The computations for $d = 3$ are already rather complicated, so cleverness, faster computers than were available in 1998 (check!), and/or a new idea will be needed here!

References

1) Derksen, H. "Inverse degrees and the Jacobian Conjecture," Communications in Algebra, 22 (1994), 4793-4794.

2) Fournié, Furter, Pinchon, "Computation of the Maximal Degree of the Inverse of a Cubic Automorphism of the Affine Plane with Jacobian 1 via Gröbner bases", JSC 26 (1998), 381-386.
3) Van den Essen, "A criterion to decide if a polynomial map is invertible and to compute the inverse", Communications in Algebra 18 (1990), 3183-3186.
4) Van den Essen, "On Bass' inverse degree approach to the Jacobian conjecture and exponential automorphisms." in: Combinatorial and computational algebra (Hong Kong, 1999), 207–214, Contemp. Math., 264, Amer. Math. Soc., Providence, RI, 2000

4. Applications of Computational Commutative Algebra in Statistics

One of the very exciting developments over the last 10 years or so in computational commutative algebra and algebraic geometry has been the application of many of these ideas to problems in statistics. Indeed, a whole new area of *algebraic statistics* is in the process of coming into existence, and the techniques introduced here have been applied in a number of "hot" areas of computational biology such as bioinformatics for the analysis of genomic data (for instance to identify genes that cause particular diseases) and phylogenetics (determination of how species are related via evolution of their DNA).

The basic idea here is that *discrete* probability models can be represented via polynomials in several variables. Coefficients in those polynomials serve as *parameters* in the models. From experimental data, we might want to *estimate* those parameters, or in other words, determine the parameter values for which the model "best fits" the data in a certain sense. The "bread and butter" technique for this kind of parameter estimation problem in statistics is called *maximum likelihood estimation.* One sets up a function giving the probability that the observed data occurs as a function of the parameters (the "likelihood function") and then, applying the usual optimization method from multivariable calculus (i.e. set all partial derivatives equal to zero and solve), one determines the parameter values yielding a maximum for the likelihood function. When the likelihood is polynomial, this leads to a system of polynomial equations and we are back in familiar territory.

One very basic question here is: How many complex or real solutions are there of the equations for the max likelihood? Usually, only the real solutions are of interest. Then, one needs to take into account possible constraints on the values for solutions of interest in the statistical problem.

For instance, in the class of *mixture models*, which would be the major focus of this project, the parameters $\theta_1, \ldots, \theta_n$ themselves represent probabilities, so they should all be real values ≥ 0, and

$$\theta_1 + \cdots + \theta_n = 1.$$

These equations and inequalities define the *probability simplex* in (a hyperplane in) $\mathbf{R}^n$. For this project, you would

- Learn some of the basics of discrete mixture models and maximum likelihood estimation, and
- Learn some basic tools for counting the number of complex solutions of a system of polynomial equations based on Newton polytopes and mixed volumes ("BKK theory")

- Learn other basic tools for counting the number of *real* solutions. (These do not seem to have been used before in this context, but could shed some light on the situation!)
- Apply these ideas to some examples.

References

1) Pistone, G., Riccomagno, E., Wynn, H.P., Algebraic Statistics, Computational Commutative Algebra in Statistics, Chapman and Hall, 2001.
2) Pachter, L. and Sturmfels, B. Algebraic Statistics for Computational Biology, Cambridge U. Press, 2005.
3) Buot, M.L. and Richards, D.St-P. "Counting and locating the solutions of maximum likelihood equations, I," Journal of Symbolic computation 41 (2006), 234-244, and II, preprint.
4) Cox, D., Little, J., and O'Shea, D. Using Algebraic Geometry, 2nd ed., Springer 2005.

5. The Moreno Socías Conjecture

Another possible question to consider is one directly related to the process of computing Gröbner bases via Buchberger's algorithm (or any other method). The question here was originally posed by Guillermo Moreno Socías in his Ph.D. thesis in the early 1990's. A few people (including a group at the SIMU 2000 REU at the UPR Humacao – see their paper below) have worked on this, but there is no general solution known at this time.

The question is this: Suppose we take a *generic* homogeneous ideal $I \subset k[x_1, \ldots, x_n]$ generated by forms of specified degrees $d_1, d_2, \ldots, d_s$. (Genericity here means that the coefficients do not satisfy any special algebraic relations in particular any coefficients that can be nonzero are nonzero, so these are completely *dense* polynomials. Technically the coefficients are *independent parameters*, so the polynomials actually live in a ring of the form

$$k(a)[x_1, \ldots, x_n],$$

where a is the list of all coefficients in all polynomials in the generating set. In practice the a's could be taken as *random elements* of the field if we are working over $\mathbf{Q}$, although then some care would have to be exercised in interpreting the results with any one random polynomial.) The question is: What can we say about the *grevlex* ideal of leading terms of I, $M = \langle LT_{grevlex}(I)\rangle$? In particular, is it a *weakly reverse lexicographic* monomial ideal, where this means:

Whenever $x^\beta \in M$ is a minimal generator of M, then every monomial of the same total degree that precedes x^β in the grevlex order is also in M.

The Moreno Socías conjecture is that this property *does always* hold for generic grevlex leading term ideals. But this is not known in general (it is known for a number of special cases). Finding new cases where it does hold, or a countexample would be a big advance in the current state of knowledge(!)

The SIMU group attacked the case $n = 2$ (two variables) and proved the conjecture in that case, essentially by tracing the operation of Buchberger's algorithm to see which monomials were produced as leading terms from the S-polynomial remainders.

This direct (or "brute force") method might just be possible too in the case $n = 3$, so this would be a good place to start. You would probably want to experiment quite a bit with "small" degrees $d_1, d_2, \ldots$ to see if you could see some patterns. As mentioned above, the genericity hypothesis could be "simulated" with randomly selected coefficients, but you would probably want to take several random examples each time to make sure you're not finding an improbable case where relations between the coefficients produce a special leading term ideal.

Longer-term goals would be to *prove* patterns you find with $n = 3$. Other approaches for computing the Gröbner basis (i.e. methods other than Buchberger's algorithm) might conceivably shed some light on the situation too. In this situation (i.e. homogeneous ideals), the computation of the Gröbner basis can also be done *degree-by-degree*, using *linear algebra* techniques. You would learn about these as a benefit of working on this project.

References

1) Aguirre, E., Jarrah, A.S., Laubenbacher, R., Ortiz-Navarro, J.A., Torrez, R.,"Generic Ideals and the Moreno Socías Conjecture, Proceedings of ISSAC 2001, 21-23 (also available from arXiv: math/0104047.
2) Cox, D., Little, J., O'Shea, D. Using Algebraic Geometry.
2) Kreuzer, M. and Robbiano, L. Computational Commutative Algebra 2.
3) Becker, T, Weispfenning, V. Gröbner Bases.

(Background on graded rings and modules, and the homogeneous Buchberger algorithm.)

6. Applications of Gröbner Bases in Public-Key Cryptography

With the proliferation of online commerce and other pursuits requiring secure communication over public channels, public-key cryptography has become a very "hot" topic over the last 15 years or so. One commonly-used system, the RSA public-key cryptosystem is based on the fact that while it is relatively easy to test whether a given integer divides another integer (even when the integers are very large), or even to test whether an integer is prime, there are currently no known fast algorithms for *factoring integers*. Since such an algorithm could conceivably be discovered in the future, the security of RSA is not assured, and people have eagerly sought other mathematical operations to form the basis of other public-key cryptosystems.

The key property that they seek is that it should be easy to verify that the results of the operation are correct, but difficult to actually compute the results. Gröbner bases are one potentially attractive way to build cryptosystems because there are theoretical results saying that, in the worst case, Buchberger's algorithm can have run-time complexity that is *doubly exponential* in the number of variables n (i.e. $O\left(2^{2^n}\right)$). Moreover, other provably hard computations can be encoded or simulated in Gröbner basis computations.

One proposal for a Gröbner basis cryptosystem is the so-called "Polly Cracker" system introduced by N. Koblitz in the mid-1990's. However this system was shown to be susceptible to various attacks that bypass Buchberger's algorithm and obtain the information needed to read encrypted messages by other means. Moreover, a well-known (and very humorous) article by "Boo Barkee," et. al. (see item 2. below) has suggested that the whole idea of Gröbner basis cryptosystems is doomed from the start. Nevertheless, interest remains in this area, and a recent article by Ackermann and Kreuzer (item 3. below) has introduced the idea of using *noncommutative* analogs of Gröbner bases for this purpose. The goals of this project would be to:

- understand the basic "Polly Cracker" system based on Gröbner bases for polynomials in commuting variables,
- understand the linear algebra attacks that make this system not very secure,
- learn about the analogs of Gröbner bases for noncommutative rings (and modules over those rings) proposed by Ackermann and Kreuzer,
- investigate the possibility of using the specific class of rings known as *path algebras* of graphs for this purpose.

References

1. Koblitz, N. *Algebraic Aspects of Cryptography*, Algorithms in Comp. and Math. **3**, Springer, 1998.
2. Barkee, B., et al., "Why you cannot even hope to use Gröbner bases in public key cryptography: An open letter to a scientist who failed and a challenge to those who have not yet failed," J. Symb. Comp. **18** (1994), 497-501.
3. Ackermann, P. and Kreuzer, M. "Gröbner Basis Cryptosystems," preprint 2005 (to appear Applied Algebra in Engineering Communications, and Computing).