Open Problems in Computational Algebraic Geometry

From a talk given at the

Cortona Conference on Computational Algebraic Geometry June 17–21, 1991

DAVID EISENBUD

Abstract. We specify some desiderata for a future system for computational algebraic geometry. We then survey a smattering of open problems at the interface between algebraic geometry and computation: A combinatorial problem that comes from the desire to make computations efficiently; problems to find (practical, and in some cases even impractical) algorithms to answer important algebraic or geometric questions; and problems in "theoretical" algebraic geometry on which some light might be thrown by investigations using computers, with resources and programs perhaps just a little better than those of the present.

Introduction

The main usefulness of computational methods in algebraic geometry and commutative algebra is in producing and analysing examples, both for cases where one knows in advance that a finite list of examples exists (as with the finite number of families of surfaces in P^4 not general type which are currently being studied by computer in the work of Decker, Schreyer, and others) and for cases where one hopes to guess or verify new phenomena through the examination of nontrivial examples. As John Von Neumann said, the principal use of computers in mathematics will be to extend the intuition.

I have chosen some open problems in computational algebraic geometry to illustrate aspects of this idea. None of the problems was invented "to be a problem"; all are from the present practice and needs of my mathematical friends and acquaintances.

There is of course one open problem which will probably always remain, and change even as it is solved: the problem of having a satisfactory programming system in which the methods of computational algebraic geometry can be used. Therefore I have begun with a list, based partly on my experience with Macaulay and other systems, of some basic desiderata. I would like to emphasize that no current system is very close to fulfilling these desiderata, but I think that the techniques for making a satisfactory system are well in hand, and I hope very much that someone will produce one soon.

The next section deals with a mathematical problem – essentially a combinatorial problem – that I find very interesting, but which I probably would not have thought much about if it had not come up as an important obstacle to efficient computation. Problems from Physics have always enriched and inspired Mathematics, and we should expect problems whose original motivation is from Computation to become increasingly visible. The one outlined here has to do with finding sparse regular sequences in a given ideal.

Sections 2 and 3 contain problems from Commutative Algebra and Algebraic Geometry respectively (though it is of course artificial to draw a line). I have presented some "chestnuts", but I hope with a novel twist, as well as some problems that I have not seen discussed before. Both sections contain problems of two kinds: mathematical problems on which one could hope to shed some light by computation (possibly on a future system), and problems to make effective certain more or less "standard" mathematical constructions.

To help the reader in finding what is of interest, here is an outline of these sections:

1) A combinatorial problem from computational practice

2) Problems in Commutative Algebra

A) Find the Samuel polynomial of an ideal

B) Decompose a module

C) Regularity

D) Galois Theory

3) Problems in Algebraic Geometry

I) General constructions

A) Normalization

B) Deformation theory

II) Curves

A) Classify plane curve singularities

B) What kind of singularities can a plane curve of given degree have?

C) Brill-Noether theory

D) Uniformization

III) Surfaces

A) Resolution of surface singularities

B) Smooth curves on singular surfaces

C) Finding reducible divisors

D) Can a smooth quintic surface in P^3 contain a rational curve of high degree?

E) Discriminant of an intersection form

F) Parametrization of rational surfaces

G) Classification of polarized surfaces

IV) Reals and Rationals

A) Real algebraic geometry

B) Rational points

I have discussed the problems and ideas presented below with many people, and would like to thank them all. Among them: Dave Bayer, Mike

Stillman, Constantine Kahn, Klaus Hulek, Craig Huneke and Wolmer Vasconcelos.

Desiderata for a system to do computational algebraic geometry and commutative algebra

There are a relatively small number of "hard" algorithms which must be carefully optimized, and which will use up the vast majority of time ace in computational algebraic geometry. (Since they are so costly, in space as well as in time, they should of course be designed to make efficient use of extended memory techniques such as page swapping...)

On the other hand the path between the output of these basic algorithms and the computations useful to algebraic geometers and commutative algebraists is quite long, so that a complete programming language is required to make good use of the system. Experience with Macaulay and other systems has shown that algorithms other than the few hardest ones are probably best implemented as programs in this language, especially since the algorithms themselves are still in flux, and may be continuously improved and augmented by users. We will follow Macaulay usage and call such programs "scripts" to distinguish them from the programs that implement the hard basic algorithms.

The user language must contain facility for "taking apart polynomials" – enough for example that a user could write a polynomial differentiation routine (though such basic algebraic manipulation routines should probably be included as primitives). Inevitably, some necessary facilities will turn out to have been forgotten, or will be available more conveniently in other systems; thus it is important to build in as far as possible the ability to export and import data from major general purpose systems (Macsyma, Mathematica, Maple...).

It is important for computations to be interuptible, with as much information as possible retained; it is quite typical for a user to begin a computation which is too hard, and to want to stop it and try a different variant if it seems to be running too long. For the same reason it would be desirable to output (preferably to a separate output stream) as much data about ongoing "hard" computations (see below) as possible. For a Gröbner basis computation this should be at least the number and degree of the standard basis elements found, but perhaps also the codimension and degree of the initial ideal found thus far. It should be possible to test this output stream once in a while (once a minute?) and branch on the results.

The fundamental "hard" operations that must be done quickly are:

I. Gröbner basis and syzygy computations with respect to various orders in particular lexicographic products of reverse lexicographic orders on subsets of the variables. The homogeneous case should be optimized. It is perhaps not necessary to build in the inhomogeneous case, as this may be easily programmed (homogenize, compute, dehomogenize ...). It is important to allow for the presence of multigradings, and to have the machine keep track of these when applying the algorithms (the kernel of a multigraded map is multigraded ...). Modules must be treated on the same basis as ideals. It should be possible to work over a factor ring; this could be implemented through scripts, but there may be some advantage in doing it directly (see III below).

It should be possible to "continue" Gröbner basis and syzygy computations: for example, it is a common problem to show that a given ideal has codimension $\geq$ a given number. If the ideal has very many generators (for example a determinantal ideal) the natural way to approach this may be to take a subset of the generators and compute the codimension of the ideal they generate; if it is not high enough, add some more generators and continue the computation.

Unique division of an element of a module by a computed Gröbner basis of a submodule should be available.

II. Monomial ideals (and monomial submodules of free modules): Hilbert series (given as a rational function over the integers), codimension, degree, regularity, and primary decomposition. Of course the Hilbert series of arbitrary ideals and modules is also crucial, but could be handled through scripts from the monomial case. I have included degree and codimension, though they can be deduced from the Hilbert series, because there are much faster algorithms (Bayer-Stillman [1990]) for computing them. All the combinatorial data should be easily accessible to the user: for example, the coefficients of the Hilbert polynomial, the degree and codimension, etc. It is important to keep in mind the multigradings (Hilbert series in 2 or more variables) and the possibility of a ring with generators in different degrees.

III. Ideals of minors and determinants must be computed so often that it is important to have good methods here, and in particular to recognize sparse matrices and use appropriate algorithms for them. The algorithms should also work over a factor ring (possibly not a domain) and take advantage of the possible simplifications in computation coming from terms being 0. It might be worthwhile to have a version that computes a Gröbner basis and minimal set of generators as it proceeds to find minors, since ideals involving very large numbers of minors may actually require quite small numbers of generators.

Although used less frequently, it would be good to have efficient computation of ideals of Pfaffians built in as well.

IV. Factorization of polynomials, both in one and several variables. Initially just for factorizations over the base domain but eventually with adjunction of algebraic quantities (see V).

V. Base domains, and change of domains. (In order of what I consider most important):

A. For efficient computation, all the above operations should be optimized to run over a prime field Z/p, with p selectable by the user, and "numbers" fitting into one word.

B. It should also be possible to select computation over Q and perhaps Z: the precision should either be infinite from the start or user selectable to an arbitrary value, with good facilities for warnings of overflow.

C. Parametrized Gröbner basis computations should be possible (that is, something that will produce the Gröbner basis of an ideal in a ring of form $K(a \dots c)[x \dots z]$, with respect to an ordering on the monomials in $x \dots z$ where K is one of the permitted ground fields. However, this need not be built in if it can be programmed in the higher level language.

D. Last, and most sophisticated, it should eventually be possible to specify a finite extension field of Z/p, and and make all computations over this extension. Once this is possible, there should be an optimized command for finding a point on a variety automatically extending the base field as necessary. (Perhaps "lazy" algorithms will eventually allow one to avoid using this facility most of the time.) Similarly extensions of Q should be available.

1. A combinatorial problem from computational practice

Often the needs of efficient computation lead one to consider problems which would not have been considered (or not taken so seriously) without this need. One of my favorites is the problem of finding a maximal regular sequence contained in a given ideal $I = (f_1, \ldots, f_m)$ in a polynomial ring $S := k[x_1, \ldots, x_n]$, say; the question is also important for factor rings of polynomial rings, but we consider only the simple case. A rather analogous problem is that of finding a "good" Noether Normalization for S/I, but we will not treat this here.

(Since this paper was written, Bernd Sturmfels and I have found the answers to a few of the questions below, a given a method for finding a fairly good maximal regular sequence along the lines suggested here. Our work will appear in: "Finding sparse regular sequences", where the reader will find proofs of some of the results stated below.)

To set the stage, I begin by discussing a naively plausible but very bad method for solving the problem:

Let us suppose that we already know the codimension c of the ideal I (having computed it, perhaps, by means of a Gröbner basis). Of course it is easy to solve the problem theoretically, and it is even easy to adapt this to what one might naively suppose to be a reasonable computational technique: c sufficiently general linear combinations

$$g_i = \sum_1^m a_{i,j} f_j$$

will form a maximal regular sequence in I. In principle one needs an infinite domain of choices for the $a_{i,j}$ for this; in practice, algebraic sets are so thin that taking the $a_{i,j}$ to be random elements from even a moderate sized finite field will suffice. Of course one should check afterwards that the choice was "sufficiently general" by computing the codimension of the ideal generated by the g_i; if this codimension is not c one should try again with a new random choice. (Beginners are often worried that they will have to do this often, just as they are often worried about an atypical choice of characteristic. In years of practice, I have never seen the first choice fail, nor the characteristic 31,991 prove atypical!)

In practice, it is important to keep things as sparse as possible, and one should probably choose the elements of the regular sequence one at a time: having chosen p elements of the regular sequence, one might first test whether any of the f_i themselves could be used to form the $(p+1)^{\mathrm{st}}$ element; if not whether a linear combination of 2 of the elements could be used, and so forth. The simplification in subsequent Gröbner basis computations which can come from a sparse choice are usually worth the computational overhead that this process entails.

It is easy to improve this idea a little: one should probably start by replacing f_i by a minimal subset generating an ideal of codimension c; one might do this by testing one element at a time to see if it can be left out, etc.

Usually one will start with homogeneous forms f_i and one will want to choose the g_i again homogeneous. If, for example, the maximum degree of an f_i is d, one might bring everything up to degree d before forming the linear combinations g_i. One could simply multiply each f_i of degree d_i by all the forms of degree $d - d_i$, and use these new forms in place of the f_i in the formula above. But if we are working with large numbers of variables (I would certainly consider 10 a large number in this context!) or large differences in degree this can lead to a very large number of monomials. Therefore in some circumstances it will be better to multiply f_i by the $(d - d_i)^{th}$ power of a randomly chosen linear form.

Whichever of these choices one makes, the answer one gets is in practice often surprisingly bad: one may have gone from an ideal with rather sparse generators, each perhaps with only a few terms, to an ideal whose generators are extremely nonsparse! Subsequent Gröbner basis computations, using the g_i, then often run at a speed near the theoretical worst behavior of

Buchberger's algorithm, which is of course disastrous in terms of practical computation.

Thus it is of practical importance to ask whether one couldn't do better. With the reductions made above, it is clear that every one of the f_i must be involved. Thus an obvious approach is to partition the f_i into consecutive subsets

$$f_1, \dots f_{i(1)}, f_{i(1)+1}, \dots, f_{i(2)}, \dots$$

in such a way that taking g_j to be a (random) linear combination of the elements of the j^{th} subset makes the g_j into a regular sequence. The "obvious" way of choosing the necessary partition is surely to take $i(j)$ to be the smallest index such that

$$(f_1 \dots f_{i(j)})$$

is an ideal of codimension j. However, this does not work! For example, if the sequence of f_i is

$$ab, bc, d^2, ac$$

then $c = 3$ and the partition is

$$\{ab\}, \{bc, d^2\}, \{ac\},$$

but no sequence of the form

$$ab, \lambda bc + \mu d^2, ac$$

is a regular sequence, since it is contained in the height 2 ideal $(a, \lambda bc + \mu d^2)$. In this case a simple rearrangement of the sequence of f_i suffices: if we apply the procedure suggested above to

$$ab, bc, ac, d^2$$

a regular sequence such as

$$ab, \lambda bc + \mu ac, d^2$$

results. Now we can state a refined version of our initial problem:

Is there an arrangement (and, if possible, a good algorithm for finding it) of the generators of every ideal such that the process above produces a regular sequence?

Unfortunately, the answer to this question is still "no!" But there is a better problem waiting in the wings, based on the fact that there is a monomial ideal with the same Hilbert function. In precise terms, we would like to make use of the following:

PROPOSITION. *Fixing a multiplicative order on S, and supposing that the f_j are homogeneous of the same degree,the polynomials*

$$h_i = \sum_j a_{i,j} in(f_j)$$

form a regular sequence, then (possibly after changing the coefficients $a_{i,j}$) so do the polynomials

$$g_i = \sum_j a_{i,j} f_j.$$

This says that if we begin by replacing the f_i with a Gröbner basis of the ideal I, then we may reduce our problem to the problem of finding a regular sequence inside an ideal generated by monomials. According to the philosophy above, we want to replace a given set of monomials by a minimal subset generating an ideal of the same codimension, and then partition this subset into disjoint subsets such that general linear combinations of elements of these subsets already form a regular sequence.

The virtue of this is that the problem has become combinatorial in character, and should admit a combinatorial solution. One might even hope that the coefficients could all be ±1.

To sum up with an equivalent formulation:

PROBLEM. *Given a set of monomials $F = f_i$, all of the same degree, is there a partition of F into disjoint subsets F_j and a regular sequence whose jth term is the sum of the elements of F_j, possibly with signs, or if necesary with other coefficients?*

2. Problems in Commutative Algebra

In this section we will sketch a few favorite problems from algebra which seem to require new algorithms for their solution.

We begin with a problem whose solution is probably not too hard: indeed, a solution is known in a leading special case, though not implementable on any current system so far as I know.

A) Find the Hilbert–Samuel polynomial of an ideal.

That is, given an ideal I and a module M (over a polynomial ring $S = k[x_1, \dots, x_n]$ say) such that M/IM has finite length, compute the polynomial over Z whose values agree for large t with the function $H(t) =$ length M/I^tM.

If I is the ideal $(x_1, \dots, x_n)$ then the solution is easy: compute the "associated graded module" of M (first compute the ring $R = S[Ix] \subset S[x]$ and then find, for example by elimination theory, the R-submodule M' generated by M inside $M \otimes S[x]$; the associated graded module is M'/IM' – the current Macaulay has scripts to do these operations) and then compute its ordinary hilbert series from the module of initial forms.

A more general special case occurs when I is a homogeneous ideal. In this case the answer could be computed from the two variable Hilbert series associated to the (naturally bigraded) associated graded module of M with respect to I – if there were any system prepared to compute such two variable Hilbert series and to carry out the operations necessary for the associated graded module.

B) Decompose a module

This problem seems to me likely to be much harder. It comes in two flavors, homogeneous and inhomogeneous. In the homogeneous case it is at least clear that an algorithm is possible; in the inhomogeneous case I cannot show that one exists, even if the module to be decomposed is projective!

1. Let M be a graded module over a polynomial ring. Decide whether M is the direct sum of two nonzero modules.

Of course what we are looking for are idempotents in $\mathrm{Hom}(M,M)$. These must lie in the degree 0 part, which is a finite dimensional algebra, so one might generalize and ask for idempotents in any finite dimensional algebra.

(Actually, I am jumping over one point: it is not too hard to find a basis for $\mathrm{Hom}(M,M)_0$, ertainly possible to obtain the map corresponding to a basis element – Macaulay can already do this. But I do not know a very efficient way to write down the algebra structure besides multiplying out every pair of basis elements.)

Now given a finite dimensional algebra A, the equation $e^2 = e$ may be thought of as a system of quadratic equations in the coordinates of the element e in terms of a basis for A. Of course the elements 1 and 0 satisfy these equations. If we represent the equations explicitly, we can use primary decomposition techniques to remove these two solutions, and we can then use Gröbner basis techniques to determine the codimension and degree of the set of "nontrivial " idempotents which remain. However, this only gives us a count of the idempotents *over the algebraic closure* of the original field; to find whether there are idempotents over the original field, requires determining whether the variety of nontrivial idempotents has a rational point, and is thus considerably harder.

Is there a better way?

2. The inhomogeneous case. Unlike many inhomogeneous problems, I am not aware of any way of reducing this to the corresponding homogeneous problem! Thinking again in terms of finding idempotents in Hom, the problem is that I do not know how to bound the degree of the polynomials that may be involved in the idempotent. This problem is already present in the apparently simple case when the module is known to be projective. One measure of present ignorance is that I don't think that anyone knows an algebraic proof (other than by a proof using étale cohomology, which simply imitates the usual topological proof) that the cokernel of the map

$$\begin{aligned}\phi : S &\to S^3\\ 1 &\to (x, y, z),\end{aligned}$$

where

$$S = Q[x, y, z]/(x^2 + y^2 + z^2 - 1),$$

is indecomposable. If we had a bound on the degree of an idempotent in Hom(cok ϕ, cok ϕ), or indeed any effective algorithm, then surely this could be checked. (Added in proof: Richard Swann has found such a proof.)

C) Regularity

Of course regularity questions (in the sense of Castelnuovo and Mumford: bounding the degrees of syzygies of graded modules) are among the most important from a theoretical point of view, and there are many open conjectures in this area. I am quite fond of one that I made in 1983 (others made it too!): As usual, let $S = k[x_1, \ldots, x_n]$. If P is a homogeneous prime in S, is it true that the regularity of P is bounded by deg $P -$ codim $P + 1$? Another, more generally applicable version is due to Dave Bayer: Define the "regularity defect" of a homogeneous ideal I to be the difference between the regularity of I and the maximal degree of a minimal generator of I. Is it true that the regularity defect of an ideal I without embedded components is at worst the sum of the degrees of the components? Note that nonreduced components are allowed here, as are components of all dimensions.

Here I want to indicate a regularity problem which arose in the work I did with Huneke and Vasconcelos. I will state a special case; the reader will have no trouble generalizing if (s)he has any idea how to solve the problem. Given an ideal I (about which we may suppose we know anything that Gröbner basis and syzygy computations can tell us) suppose that we know that $I = P \cap Q$, where P and Q are prime ideals. What is a bound for the regularity of P and Q? Of course if we apply the first conjecture mentioned above, then since the degree of P is less than that of I, we get a fairly good bound. But this problem should really be easier than the general problem, and perhaps the bound should be better (maybe in terms of some further information about I).

D) Galois Theory

Finally, let me mention an old chestnut, perhaps in a slightly different form than the usual: Given a ring extension $R \subset S$ with S a finite R-module, compute the Galois group of the Galois closure (or, if we are brave enough for characteristic p, the normal closure) of the quotient field of S in the algebraic closure of the quotient field of R. The possible novelty is this: for geometric applications, one should consider finitely generated rings over a field k, and one would like to go directly to the Galois group that one would get after extending the field to the algebraic closure of k – in the geometric context, this appears as a monodromy group.

3. Problems in Algebraic Geometry

The problems we will discuss fall naturally (?) into several groups. I have mixed together, however, problems which call for better methods of computation and problems which suggest the use of computation for the exploration of some mathematical topic.

I. General constructions

A) Normalization

Given a pair of affine domains $R \subset S$, compute the integral closure of R in S (as it is relatively easy to construct Rees rings, this would allow one to compute integral closures of ideals as well). Some constructions are known (the most recent reference I know (6/91) is a preprint of Vasconcelos); but they involve complex computations and many iterations, so that they are currently not very practical. Normalization is such a fundamental process that it would be very interesting to have other, and one hopes better, methods.

B) Deformation theory

Compute the base space and total space of a versal deformation of an isolated singularity. It is relatively easy to compute first order deformations. Once this is done one can use the "standard" method of lifting syzygies to get an approximation valid up to degree n for any n. This leads in principle to a power series representation of the desired family. But it is known that the base space is actually algebraic! How to get an algebraic (finite) answer instead of an analytic (infinite) one does not seem to be understood.

II. Curves

A) Classify Plane curve singularities

To begin with a problem that has recently been solved, for example by Dominique Duval and her students (see for example Duval [1989]): Describe the type of a singular point of a plane curve. That is, describe its characteristic pairs (equivalently the multiplicities of its infinitely near points, or again equivalently it's semigroup), and perhaps a Puiseux series parametrization (adjoining algebraic quantities as necessary). Of course if we know that the singularity is unibranched we should be able to derive at least the characteristic pairs without any such root adjunction, for example by computing multiplicities of blowups. This should be possible to do quite efficiently.

B) What kind of singularities can a plane curve of given degree have?

To give a few questions of this sort explicitly:

1. How many cusps can lie on a plane curve of degree d? Zariski proved for example that there cannot be 11 on a curve of degree 7, and our knowledge has progressed a little since his result.

2. What are the integers n for which a plane curve of degree d can have an A_n singularity? A given configuration of such singularities? (Note that a plane curve of degree d can easily have an A_n singularity with $n > d$. For example, a quartic can have an oscnode $x^2 - y^6 = 0$ – take the canonical embedding of the union of two rational curves meeting triply at a point.)

Such problems should be accessible to some computer investigation because it is possible to write equations that specify that a curve (represented by the coefficients of its defining equation) has a singularities of (at least) certain types at certain specified points. Taking the coordinates of these points to be indeterminate, we can in principle use these equations to decide whether such curves exist, and if they do whether they are all degenerate in some way. However, the computations are rather hard, and I think that they surpass the capabilities of current systems. Is there a more efficient way?

C) Brill-Noether Theory

How special is a given curve in the sense of Brill-Noether theory? Specifically, given the equations of a curve, compute its gonality (= least degree of a map to P^1), its Clifford index (which measures how 'small' a projective representation the curve admits), the dimension of the varities of special divisors W_d^r, and so forth.

To solve these problems we might begin by replacing the given embedding of the curve by its canonical embedding (using the computation of the canonical line bundle as an Ext module, and the ideas of Brundu and Stillman [1990] on embeddings defined by line bundles, for example). It is then reasonable to try to compute the locus of "k-secant l-planes" by simply looking at the equations which say that k variable points on the curve span at most an l-space. The geometric Riemann-Roch theorem allows us to deduce the dimensions of the W_d^r from the dimensions of these varieties, and thus in particular to deduce the Gonality and Clifford index. But it is probably not yet practical to carry out the computation this way in any interesting case. Is there a better way?

Green's conjecture, if proved (or assumed!) gives another, much more efficient way of computing the Clifford index.

However, I do not know of any method for computing something like the smallest degree of an embedding.

D) Uniformization

A problem which is probably too transcendental to be feasible: Given the equation of an elliptic curve, find the corresponding period lattice, and conversely. Of course the difficulty is that the periods tend to be transcendental functions of the coefficients of an equation. A good compromise in this case is to find the j-invariant, but even here there is a small problem to be solved. The rational functions that express j as a function of the coefficients of the curve represented as a plane cubic were worked out in the nineteenth century [****reference]; but I do not know whether one can go from an arbitrary embedding of the curve to such a representation, or at least to the j-invariant, without finding points on the curve, and thus without need to introduce algebraic numbers. Can one write down the j-invariant directly from a higher dimensional embedding?

Along with periods, one may consider a related problem for curves of higher genus: how do you go from equations for the curve to a Fuchsian group, and back?

III. Surfaces

A) Resolution of surface singularities.

Produce the "resolution graph". Several basic strategies are possible, and some experience will be necessary to choose between them and to implement them efficiently. Among them are:

1) Repeat the process {Normalize and then blow up the reduced singular locus}

2) Repeat the normalized Nash transformation (blow up the Jacobian subscheme and then normalize) until the singularities become simple (see Spivakovsky [1990]).

3) Project to P^2 and do embedded resolution on the branch curve (Jung's method; see Lipman [1975]).

B) Smooth curves on singular surfaces

As for IIC: If a surface S in P^3 contains a smooth curve C, what kind of singularities can S have at points of C? For example, the rational singularity E_8 cannot occur, as it is factorial! (I heard this problem from M. Boratyński.)

C) Finding reducible divisors

Given a divisor on a variety (for example on a smooth surface) decide whether its class is divisible, or more generally whether some linearly equivalent divisor is reducible. A special case: given a smooth surface in P^3, decide whether it has a divisor which is not a hypersurface section (that is, decide whether it's homogeneous coordinate ring is factorial). This is probably out of reach; an interesting (and presumably easier) question would be to determine whether the surface has any divisor of degree $\leq$ some fixed number e other than a multiple of the hyperplane section. To do this, one needs to try to decompose a big multiple of the hyperplane section.

Such an algorithm could also serve in determining the polarization of an embedded abelian surface.

D) Can a smooth quintic surface in $\mathbf{P}^3$ contain a rational curve of high degree?

That is, does there exist an upper bound on the degree of C over all pairs

$$(S \text{ a smooth quintic } \supset C \text{ a geometrically rational curve?})$$

A simple dimension count suggests that there might be none of degree > 55. This is, I think, just over the horizon of current computational power, but might be a good test problem. Here are two results which also suggest that at least rational curves on quintics should be rather rare:

1. (Bogomolov [1979]): A smooth quintic cannot contain infinitely many rational curves.

2. A general quintic is hyperbolic, and this condition is open in the analytic topology. Thus the set of smooth quintics containing any rational curve is a proper closed subset of the space of all quintics (in the analytic topology).

On the other hand, it is of course easy to produce rational curves of any degree on an irreducible but singular quintic, such as the projection to $\mathbf{P}^3$ of a rational normal scroll in $\mathbf{P}^6$.

E) Discriminant of an intersection form

A possible generalization of the preceding problem to all surfaces in $\mathbf{P}^3$ is the following question, due to Kieran O'Grady: Can you bound the discriminant of the intersection form of surfaces with Picard number $= 2$ in $\mathbf{P}^3$? For a quintic with a rational curve of degree d the form would be (or at least contain)

$$\begin{pmatrix} 5 & d \\ d & -d+2 \end{pmatrix},$$

and would thus have discriminant on the order of d^2.

F) Parametrization of rational surfaces

Find an algorithm for parametrizing a rational surface given by equations. Perhaps one should start by studying some special classes of surfaces here – say del Pezzo or ruled. I first became aware of this problem from Abhyankar. Abhyankar and Bajaj have worked out the cases of quadrics and cubics in P^3 (see their papers [1987 and 1988]).

G) Classification of polarized surfaces

It seems to me likely that a little work would yield algorithms for the (Enriques) classification of surfaces given by explicit equations. Recent work of Decker, Popescu, Schreyer, and their students on surfaces in P^4 includes a number of steps in this direction. Perhaps the simplest project in this direction would be the classification as polarized surfaces – that is, surfaces with a given very ample divisor class, coming from the hyperplane section – in cases like those of ruled surfaces and abelian surfaces where one understands something of the possible polarizations.

Here are some basic operations for which there are already algorithms, on which such an "automatic" classification or parametrization could be based: (here to "give" a bundle means to give a graded module whose associated sheaf is the bundle. We will write the linear combinations of divisors (tensor products of line bundles) additively, as in $2K$, to distinguish them from intersections, which we write multiplicatively, as in K^2.

1. Compute cohomology of bundles; in particular, given a module M representing a bundle L, compute the module $\Gamma_* L$.

2. Compute the divisor corresponding to a section of a bundle.

3. Compute the intersection number of two divisors (including self intersections).

4. Compute the map to projective space corresponding to a divisor, (see Brundu and Stillman [1990] for a treatment of this) and the singular locus of such a map.

5. Compute the base locus of a divisor.

6. Compute the blowup of a surface at a subscheme.

7. Decide whether two given line bundles are isomorphic. (This does not need even the probabilistic method used for general sheaves: taking Hom of one into the other should produce the ground field, and the (unique up to scalars) map giving a nonzero element of this Hom should be an isomorphism. Of course before testing, each of the line bundles should be represented by a depth 2 module (double dual into the coordinate ring).

8. Find the canonical sheaf of a variety V in P^n :

$$\omega_V = \mathrm{Ext}^c_S(S/I,\ \omega_{\mathrm{P}^n})$$

as modules.

Given these things, and given a surface V in a projective space, we proceed as follows. Write H and K for the hyperplane bundle and canonical bundle of V (or for divisors in these classes...).

a. Determine the numerical invariants,

$$q = h^1(\mathcal{O}_V), p_g = h^2(\mathcal{O}_V), H^2, HK, K^2.$$

b. Determine the the Kodaira dimension $\kappa(V)$: If $K^2 \neq 0$ then either nK or $-nK$ has lots of sections when $n >> 0$ (You can tell how large n must be from Riemann-Roch: $\chi(D) = D(D-K)/2+1-q+p_g$). If $K^2 > 0$ then nK has at least two sections iff $\kappa(V) = 2$, while $-nK$ has at least two sections iff $\kappa(V) = -\infty$.

If $K^2 = 0$ then $\kappa(V) = 0$ iff a multiple of K is isomorphic to $\mathcal{O}_S$. (There is a bounded power that has to be checked.) Else $\kappa(V) = 1$.

c. One would then divide into cases, according to the value of κ. Discussions that I had with Klaus Hulek, Wolfram Decker, Frank Schreyer and others suggest that this could be carried out in most of the cases pretty directly. A few of the things I don't yet see how to do: Find the type of polarization of an albelian surface, find the type of a bielliptic surface, find the fundamental group of any surface... .

d. In performing the classification it is sometimes useful to have a minimal models. These can generally be found by using adjunction theory (see Sommese and Van de Ven [1987]; and Okonek [1986] for an example of how the technique is used), as is done for example in the recent work of Decker, Popescu, Schreyer [1991].

IV. Reals and Rationals

A) Real algebraic geometry

What are the possible images of real algebraic maps? For example, is there a polynomial map $\mathbf{R}^2 \to \mathbf{R}^2$ whose image is precisely the open positive quadrant? (I learned of this problem from Rioboo, in Madrid.)

Although it is possible to find the image of a given real algebraic map, or more generally to eliminate quantifiers and solve a system of real polynomial equalities and inequalities using "cylindric decompositions", this can defy computation even in relatively easy cases. For example, there seems no system currently capable of solving for u, v the system

$$\exists a, b, c, d \quad \forall x$$

$$(x-c)(x^3-u)+(x-c)(a+bx)>0$$

$$ea(a-v)>0$$

$$e>c.$$

(Lazard told me that he got this problem from the physicist Comon. Exploiting the quasihomogeneity of the system, Lazard was able to solve it by hand; but current mechanical techniques lead to intermediate problems which are out of reach.)

B) Rational points

How do we look for rational points of at most given height on a variety, or at least estimate their number? Aside from the obvious intrinsic interest in such a question, recent conjectures and problems of Manin and his school have leant this problem new urgency, particulary for varieties of Kodaira dimension $-\infty$, which are the ones that can be expected to have infinitely many rational points.

References

S.S. Abhyankar and C.L. Bajaj, *Automatic parametrization of rational curves and surfaces and conicoids*, Computer Aided Design **19** (1987), 11–14; *II: Cubics and cubicoids*, Computer Aided Design **19** (1987), 499–502; *III: Algebraic Plane Curves*, Computer Aided Geometric Design **5** (1988), 309–321.

D. Bayer and M. Stillman, *Computation of Hilbert functions*, J. Symb. Comp. **14** (1992), 31–50.

M. Beltrametti, P. Francia, and A. J. Sommese, *On Reider's method and higher order embeddings*, Duke J. Math. (to appear).

A. Biancofiore and E.-L. Livorni, *On the iteration of the adjunction process in the study of rational surfaces.*, Manuscripta Math. **36** (1987), 167–188.

A. Biancofiore and E.-L. Livorni, *On the iteration of the adjunction process for surfaces of negative Kodaira dimension.*, Manuscripta Math. **64** (1989), 35–54.

F. Bogomolov, Math. USSR Izvestiya **13** (1979).

M. Brundu and M. Stillman, *Computing the equations of a variety*, Trans. Am. Math. Soc. (to appear). Preprint, 1990.

D. Duval, *Rational Puiseux expansions*, Compositio Math. **70** (1989), 119–154.

D. Eisenbud, *Green's conjecuture; an orientation for algebraists*, in "Sundance 91: Proceedings of a Conference on Free resolutions in Commutative Algebra and Algebraic Geometry," Jones and Bartlett, 1992 (to appear).

D. Eisenbud, C. Huneke, and W. Vasconcelos, *Direct methods for primary decomposition*, Invent. Math. **110** (1992), 207–235.

J. Lipman, *Introduction to resolution of singularities*, in "Proceedings of Symposia in Pure Mathematics 29: Algebraic Geometry, Arcata 1974," Amer. Math. Soc., Providence, RI, 1975.

C. Okonek, *Flächen vom Grad* 8 *im* $\mathbf{P}^4$, Math. Z. **191** (1986), 207–223.

A. J. Sommese and A. Van de Ven, *On the adjunction mapping*, Math. Annalen **278** (1987), 593–603.

M. Spivakovsky, *Sandwiched singularities and desingularization of surfaces by normalized Nash transformations.*, Annals of Math. **131** (1990).

W. Vasconcelos, *Computing the integral closure of an affine domain*, Proc. Amer. Math. Soc. **113** (1991), 633–638.

Department of Mathematics, Brandeis University, Waltham MA 02254
eisenbud@brandeis.bitnet