Séminaires & Congrès
13, 2006, p. 367–387

FORMALIZED PROOF, COMPUTATION, AND THE CONSTRUCTION PROBLEM IN ALGEBRAIC GEOMETRY

by

Carlos Simpson

Abstract. — This is an informal discussion of how the construction problem in algebraic geometry, that is the problem of constructing algebraic varieties with various topological behaviors, motivates the search for methods of doing mathematics in a formal, machine-checked way. I also include a brief discussion of some of my work on the formalization of category theory within a ZFC-like environment in the Coq proof assistant.

***Résumé* (Les preuves formalisées, le calcul, et le problème de la construction en géométrie algébrique)**

Ceci est une discussion informelle de la façon dont le problème de la construction des variétés algébriques avec diverses comportements topologiques, motive la recherche des méthodes formelles dans l'écriture des mathématiques vérifée sur machine. Aussi incluse est une discussion brève de mes travaux sur la formalisation de la théorie des catégories dans un environnement « ZFC » en utilisant l'assistant de preuves Coq.

It has become a classical technique to turn to theoretical computer science to provide computational tools for algebraic geometry. A more recent transformation is that now we also get *logical* tools, and these too should be useful in the study of algebraic varieties. The purpose of this note is to consider a very small part of this picture, and try to motivate the study of computer theorem-proving techniques by looking at how they might be relevant to a particular class of problems in algebraic geometry. This is only an informal discussion, based more on questions and possible research directions than on actual results.

This note amplifies the themes discussed in my talk at the "Arithmetic and Differential Galois Groups" conference (March 2004, Luminy), although many specific points in the discussion were only finished more recently.

2000 *Mathematics Subject Classification.* — 03B35, 32J25, 18A25.
Key words and phrases. — Connection, fundamental group, representation, category, formalized proof, algebraic variety, Bogomolov-Gieseker inequality, limit, functor category.

I would like to thank: André Hirschowitz and Marco Maggesi, for their invaluable insights about computer-formalized mathematics as it relates to algebraic geometry and category theory; and Benjamin Werner, M. S. Narasimhan, Alain Connes, Andy Magid and Ehud Hrushowski for their remarks as explained below.

1. The construction problem

One of the basic problems we currently encounter is to give constructions of algebraic varieties along with computations of their topological or geometric properties. We summarize here some of the discussion in [**Sim04a**].

Hodge theory tells us much about what *cannot* happen. However, within the restrictions of Hodge theory, we know very little about natural examples of what *can* happen. While a certain array of techniques for constructing varieties is already known, these don't yield sufficiently many examples of the complicated topological behavior we expect. And even for the known constructions, it is very difficult to calculate the properties of the constructed varieties.

This has many facets. Perhaps the easiest example to state is the question of what collections of Betti numbers (or Hodge numbers) can arise for an algebraic variety (say, smooth and maybe projective)? For the present discussion we pass directly on to questions about the fundamental group. What types of π_1 can arise? We know a somewhat diverse-sounding collection of examples: lattices, braid groups (in the quasiprojective case) [**MT88**], all kinds of virtually abelian groups, solvable groups [**SVdV86**], plenty of calculations for plane complements of line arrangements and other arrangements in low degrees [**Lib82**] [**CO00**] [**ACT02**], Kodaira surfaces, many examples of non-residually finite groups [**Tol93**]. Which π_1's have nontrivial representations? Recall for example an old result:

Theorem. — *Any nonrigid representation of a Kähler group in* $PSL(2,\mathbb{C})$ *comes by pullback from a curve.*

Conversely, there exist nonrigid representations of rank > 2 which don't come by pullback from curves. However, in a more extended sense all of the known examples of representations come from rigid representations (which conjecturally are motivic) and from representations on curves, by constructions involving Grothendieck's "six operations" (cf. [**Moc03**]). In particular, the irreducible components of moduli varieties of flat connexions M_{DR} which are known, are all isomorphic to moduli varieties of representations on curves.

An early example of this phenomenon was Lawrence's construction of representations of the braid group [**Law90**]. For braid groups or generalized mapping class groups, Kontsevich has a conjecture dating from around 15 years ago, which would give an explicit description of what all representations should be in terms of higher direct images. (These two things should have been mentionned in [**Sim04a**]).

Nonetheless, over general quasiprojective varieties it seems likely that there are other "new" representations but that we don't know about them because it is difficult to master the computational complexity of looking for them.

An intermediate construction might be as follows: suppose we have a family $\{V_t\}$ of local systems on X, such that there is a closed locus $Z \subset M_{DR}(X)$ where $\dim H^i(X_y, V_t)$ jumps for $t \in Z$. Then the family $\{R^i\pi_*\}_{t\in Z}$ might be a component of the moduli space of local systems on Y. Thus the whole topic of variation of differential Galois groups could lead to some "semi-new" components in this way. Nonetheless, this doesn't go too far toward the basic question of finding cases where there are lots of representations for a general reason.

2. Logic and calculation

The construction problem results in a complex logical and computational situation, not directly amenable either to pure theoretical considerations, or to brute-force calculation. This could open up the road to a new type of approach, in a direction which was forseen by the INRIA group in Rocquencourt, when they baptised their research group "Logi-Cal". The idea behind this name was that it is becoming necessary to combine logic and calculation. The origins of this requirement lay in computer science, exemplified for example by the notions of "proof-carrying code" and verified and extracted programs. The "Logi-Cal" idea was very cogently explained by Benjamin Werner in an exposé in Nice a few years ago, in which he described its possible applications to pure mathematics using the example of the four-color theorem. He explained that it would be good to have a proof of the four-color theorem which combines computer verification of the theoretical details of the argument, with the computer computations which form the heart of the proof. He said that we could hope to have the whole thing contained in a single document verified by a single program. In a spectacular advance, this project has recently been completed by G. Gonthier, who gives a full computer-verified proof of the four-color theorem in Coq [**Gon04**].

Thomas Hales' "Flyspeck project" [**Hal**] is another current example of a project in the direction of using computer proof techniques to combine theory with calculation, in that case for the proof of the Kepler conjecture.

It seems clear that this very nice idea should have repercussions for a much wider array of topics. The possibility of combining logic and computation will open up new routes in algebraic geometry. This is because there are questions such as those related to the construction problem above, which are susceptible neither to pure reasoning nor to pure computation. At this conference Andy Magid mentionned an interesting case: he had tried some time ago to compute examples of positive-dimensional representation varieties for finitely presented groups with more relations than generators (cf. [**AB00**] [**Gro89**] [**Cat96**]). He reported that the computational complexity of the question (which depends on parameters like the number of generators, the number and length of the relations, and the value of n if we look for representations in $GL(n)$) became overwhelming even for very small parameters. In the algebraic-geometric case, we might want to take concrete varieties, compute presentations for their fundamental groups (using braid-group techniques for example) and then compute the representation spaces. Magid's remarks suggest that a brute-force approach to this computation will not be feasible. On the other hand, purely theoretical techniques are unlikely to answer the most interesting question in this regard, namely: are there new or exceptional examples which are not accounted for by known theoretical reasons? Thus the interest of looking for a mixed approach combining theory and computation. Implementation of such an approach could be significantly enhanced by computer-formalized proof techniques providing an interface between theory and calculation.

Another example seen in this conference was Ehud Hrushowski's talk about algorithmic solutions to the problem of computing differential Galois groups. While showing that in principle there were algorithms to make the computation, it appeared likely that the complexity of the algorithms would be too great to permit their direct implementation. It would be good to have precise information about the complexity of this kind of question. This undoubtedly would require substantial input from algorithmic complexity theory. Some things are known for related problems, see [**vdDS84**] for example. The known bounds tend to be be high, so again one would like to envision a mixed approach in which theory provides shortcuts in determination of the answers. An interesting theoretical question is then to what extent there is a relation between proof complexity for the theory part [**Bus98**], and algorithmic complexity for the calculational part.

Of course mixing between theory and computation has always taken place within mathematical work, a good example is [**GP78**]. There have also recently been advances in the use of algorithmic methods to attack problems such as the topology of real varieties [**Bas03**] [**BPR03**]. The editor points out [**Bro87**] which constitutes a striking example (for the case of the Nullstellensatz) where mathematical theory can considerably improve computational bounds.

The relevance of computerized formulation of the theory part is that it might well permit the process to go much farther along, as it would make available the advances in computational power to both sides of the interaction. Currently we can benefit from advanced computational power on the calculation side, but this can outstrip the capacity of theory to keep up. This phenomenon was emphasized by Alain Connes in his talk (and subsequent comments) at the PQR conference in Brussels, June 2003. He pointed out that with computer algebra programs he could come up with new identities which took pages and pages just to print out; and that it would be good to have tools for interpreting this new information which often surpasses our classical human sensory capacities. It is possible that interface tools could be of some help, but likely in the end that we would want to connect these things directly to theoretical proof software—a step which might on some levels bypass human understanding altogether.

A related area in which it might be useful to have a mixture of theory and computation when looking for construction results is the Hodge conjecture. There are many concrete situations in which we expect to find certain algebraic cycles, but don't in general know that they exist. For example, the Lefschetz operators or Kunneth projectors are automatically Hodge cycles. It would be interesting to take explicit varieties and search for algebraic cycles representing these Hodge classes. As in the search for representations, a brute-force approach would probably run out of steam pretty fast, and it would be interesting to see what a mixed approach could attain. A related question is the search for constructions of varieties where the Lefschetz or Kunneth operators are topologically interesting, namely cases where the cohomology is not mostly concentrated in the middle dimension.

Finally we mention a more vague direction. In the above examples we are looking for constructions with a certain desired topological or geometrical behavior. However, it may also be interesting to consider the question of what we get when we look at an arbitrary algebraic-geometric construction process or algorithm. This type of question is related to the field of dynamical systems, and has been popularized by S. Wolfram. There are probably many places to look for interesting processes in algebraic geometry. Insofar as a given process produces an infinite, combinatorially arranged collection of output, it opens up questions of asymptotic behavior, and more generally the arrangement of results with respect to measurable properties on the output, as well as dependence on the algorithm in question. For this type of research it would seem essential to have tools relating theoretical properties in algebraic geometry to algorithmic questions.

3. The Bogomolov-Gieseker inequality for filtered local systems

We go back to look more closely at the computational issues in constructing representations of algebraic fundamental groups. There are various different possible approaches:
–construct the representations directly on a presentation of π_1;
–construct directly the connections (E, ∇) or the Higgs bundles (E, θ);
–in the quasiprojective case, construct directly parabolic bundles, logarithmic connections, or "filtered local systems".

Most work up to now on the first approach has already had the flavor of mixing computation and theory [**MT88**] [**PS02**] [**Lib82**] [**GLS98**] [**DN01**] [**Bro83**]. For the second and third approaches, there is a *Bogomolov-Gieseker inequality* lurking about. The basic example is the classical $3c_2 - c_1^2 \geq 0$ for surfaces of general type,