Interactive Theorem Proving in Geometry: Issues and Applications

Jacques Fleuriot
School of Informatics
University of Edinburgh

Mechanical theorem proving in geometry is one of the earliest areas of automated reasoning. The first geometry theorem prover, the Geometry Machine, was developed as early as 1959 and could prove a number of textbook theorems through a mixture of encoded geometric knowledge, backward chaining search, and counterexample finding [8]. However, despite this promising start and many extensions to the work over the ensuing fifteen years or so, no significant results could be proved. Instead numerous problems emerged due to difficulties in tackling the huge space (of geometry rule applications) and the field more or less stagnated until the seminal work of Wu Wen-tsün in 1977.

The so-called Wu's method [17] was an algebraic or coordinate-based approach that departed from the axiomatic or synthetic nature of previous work and laid the foundations for modern automatic geometry theorem proving (GTP). It single-handedly improved the power of mechanical reasoning in geometry and led to a flurry of work on algebraic methods for GTP (e.g. using Gröbner bases) [1], which is still ongoing.

The main attraction of the algebraic GTP methods lies in their ability to produce non-trivial geometric proofs fully automatically. However, one major drawback rests with the long and hard to read proofs that they generate. This makes it difficult to explain the proofs geometrically and may be viewed as taking away the intuitive appeal usually associated with geometric reasoning. Fortunately, over the past few years – influenced to some extent by algebraic techniques – new coordinate-free approaches have been developed and used successfully in automated GTP. These new methods are usually based on geometrically meaningful notions such as signed areas of triangles [4], full-angles between lines [5], or directed number systems (Clifford Algebra) [9] and can often produce short, more readable proofs through the use of geometrically-motivated heuristics.

Viewed collectively, the extensive work done on fully automatic GTP over the past 40 years has resulted in a mature field, which can be of benefit to areas of geometric reasoning that do not yield to full automation but instead require interactive theorem proving. In recent work [6], for example, we investigated the use of the signed-area and full-angle methods within the higher-order logic of the interactive theorem prover Isabelle (Isabelle/HOL). We formalized the basic concepts underlying these approaches and used them to produce geometric proofs in this new setting. This work showed, for instance, that Isabelle's generic simplifier and natural deduction tools could be used to automate much of the geometric reasoning, while preserving geometrically intuitive and high-level steps that enabled the *fully-checked* proofs to remain short. Thus, techniques from automated GTP enabled us to get non-trivial proofs in an interactive setting without the need to formalize from scratch theories such as those of Hilbert [10] or Tarski [15], which some may view as more natural candidates for mechanization in Isabelle/HOL. In fact, we should remark here that Hilbert's 'rigorous' approach to geometry has itself many non-trivial formalization issues, such as ambiguities of definitions, which we highlighted in some of our latest work in Isabelle [13]. Moreover, mechanizing such foundational approaches means that a large amount of work has to be done before any significant (or interesting) geometric theorems can be mechanized. This may be considered a prohibitively expensive effort if one wants to reason formally about the high-level properties of geometric algorithms, for example.

Once suitable GTP techniques are formalized in an interactive theorem prover such as Isabelle, one can then draw on the rich logical language and numerous mathematical theories of the system to reason about areas that would ordinarily fall beyond the scope of the methods. We have shown, for example, how one may combine the signed-area and full-angle methods with nonstandard analysis concepts to give a geometry where one can reason rigorously about infinitesimal or vanishing quantities [6] (which arise in Newton's *Principia*, for instance) and infinite approximations of geometric objects [7]. Such proofs are not possible using traditional GTP methods as they require deduction in so-called *degenerate* situations, where reasoning usually breaks down. Moreover, formalization in a powerful system like Isabelle enables the use of other forms of representation and reasoning such as inductive ones (e.g. over the number of points), which is impossible under normal circumstances.

As mentioned previously, a major issue is the lack of human readable proof when it comes to algebraic GTP techniques. This makes these automated techniques of little pedagogic use, for instance. Although the more recent coordinate-free methods provide geometrically more intuitive proofs, the latter still tend to be machine oriented in nature. Thus, another appeal of using an interactive system such as Isabelle, as opposed to some *ad-hoc* geometry theorem prover, lies in its support for declarative proof scripts [16]. This enables formal proofs to be expressed in a readable language more closely related to the mathematical vernacular used in textbooks, for instance. In situations, where one needs to understand the proofs, and not merely trust some black-box procedure, structured, declarative proofs have an undeniable advantage.

We believe that, in an interactive theorem proving setting, the ability to combine the underlying logic of the theorem prover, mathematical theories, GTP techniques, and readable proofs provides a powerful framework for the formalization of complicated arguments found in geometric algorithms. As an example, it is possible to reason about convex hulls algorithms without much effort: this was tackled recently in the theorem prover Coq [14] with much success. Convex hull procedures, along with other core computational geometry algorithms, are currently being formalized at Edinburgh too as part of formal verification work in Isabelle/HOL. Interestingly, it should be possible to capitalise on the Isabelle formalization of GTP methods for the verification of convex hull algorithms. This is because a number of these procedures (e.g. the gift-wrapping algorithm) rely on an orientation predicate (characterized axiomatically by Knuth [11], for instance) that corresponds exactly to the signed area used in automatic GTP. This relation to GTP was not exploited in the Coq formalization but we aim to do so in Isabelle.

In general, reasoning about the correctness of geometric algorithms is a hard task since much of the geometric intuition is usually lost when dealing with actual implementations. Moreover, robustness issues such as round-off errors due to the use of floating-point arithmetic, as well as degeneracies in the input data, can further complicate reasoning. The importance of these geometric algorithms, however, is increasing as they are at the heart of many applications ranging from safety-critical ones to VLSI design to bioinformatics (e.g. in molecular modelling of protein structures).

Of particular interest is the formalization and verification of the correctness of geometric air-traffic algorithms (ATM) used for conflict detection and resolution (CD&R) in aircraft trajectories [3]. Over the last decade or so, aeronautics researchers have proposed many procedures for real-time CD&R [12]. These often involve complex reasoning, especially for multiple-aircraft situations, and are difficult to prove correct. In most cases, correctness arguments have been provided either by means of (often intricate) pen-and-paper proofs or through computer simulations. Both of these approaches to verification are time-consuming, potentially error-prone, and hence correctness checking would probably benefit from mechanization. A theorem-proving approach to reasoning about CD&R algorithms – which places like NASA have started to use [2] – results, once fully formalized, in a guarantee that the desired properties hold. This is a highly desirable situation when dealing with such safety-critical problems and, moreover, may prove invaluable if the proposed shift from from the current air-traffic control system to the new, highly automated ATM regime known as *free-flight* is to happen.

References

[1] B. Buchberger, G. E. Collins, and B. Kutzler. Algebraic methods for geometric reasoning. *Annual Review of Computational Science*, 3:85–119, 1988.

[2] R. Butler, J. Maddon, A. Geser, and C. Munoz. Formal analysis of air traffic management systems: the case of conflict resolution and recovery. In S. Chick, P. J. Sanchez, D. Ferrin, and D. J. Morrice, editors, *2003 Winter Simulation Conference*, pages 906–914, 2003.

[3] Y.-J Chiang, J. T. Klosowski, C. Lee, and J. S. B. Mitchell. Geometric algorithms for conflict detection/resolution in air traffic management. In *Proceedings of the 36th IEEE Conference on Decision and Control*, volume 2, pages 1835–1840, 1997.

[4] S. C. Chou, X. S. Gao, and J. Z. Zhang. Automated generation of readable proofs with geometric invariants, I. multiple and shortest proof generation. *Journal of Automated Reasoning*, 17:325–347, 1996.

[5] S. C. Chou, X. S. Gao, and J. Z. Zhang. Automated generation of readable proofs with geometric invariants, II. theorem proving with full-angles. *Journal of Automated Reasoning*, 17:349–370, 1996.

[6] J. Fleuriot. *A Combination of Geometry Theorem Proving and Nonstandard Analysis, with Application to Newton's Principia.* Springer-Verlag, 2001.

[7] J. D. Fleuriot. Theorem proving in infinitesimal geometry. *Logic Journal of the IGPL*, 9(3):471–498, 2001.

[8] H. Gelernter. Realization of a geometry theorem-proving machine. In *Computers and Thought*, pages 134–152. 1959.

[9] D. Hestenes and G. Sobczyk. *Clifford Algebra to Geometric Calculus.* Reidel Publishing Company, 1984.

[10] D. Hilbert. *The Foundations of Geometry.* The Open Court Company, 1901. Translation by E. J. Townsend.

[11] D. E. Knuth. *Axioms and Hulls.* Number 606 in Lecture Notes in Computer Science. Springer-Verlag, 1992.

[12] J. Kuchar and L. Yang. A review of conflict detection and resolution modeling methods. *IEEE Transactions on Intelligent Transportation Systems*, 1(4):179–189, 2000.

[13] L. I. Meikle and J. D. Fleuriot. Formalizing Hilbert's Grundlagen in Isabelle/Isar. In *Theorem Proving in Higher Order Logics: 16th International Conference, TPHOLs 2003*, volume 2758 of *Lecture Notes in Computer Science*, pages 319–334, 2003.

[14] D. Pichardie and Bertot Y. Formalizing convex hull algorithms. In Richard J. Boulton and Paul B. Jackson, editors, *Theorem Proving in Higher Order Logics, 14th International Conference, TPHOLs 2001, Edinburgh, Scotland, UK, September 3-6, 2001*, volume 2152 of *Lecture Notes in Computer Science.* Springer, 2001.

[15] A. Tarski. *A Decision Method for Elementary Algebra and Geometry.* University of California Press, 1951.

[16] M. Wenzel. *Isabelle/Isar – A versatile environment for human-readable formal proof documents.* PhD thesis, Institut für Informatik, Technische Universität München, 2002.

[17] W. Wu. On the decision problem and the mechanization of theorem in elementary geometry. In *Automated Theorem Proving: After 25 years*, volume 29 of *Contemporary Mathematics*, pages 213–234. A. M. S., 1984.