Logical Decision Procedures in Practice

John Harrison
Intel Corporation, Hillsboro, USA

The aim of these lectures is to give a clear and explicit overview of the most important decidable and undecidable problems in automated theorem proving. We put particular emphasis on practical algorithms that are useful in real–world problems, but we pay due attention to traditional theoretical issues including the well–known limitative results (Gödel's incompleteness theorem, Tarski's theorem on the undefinability of truth etc.) Looking at the problem from both a theoretical and practical angle is quite instructive. It quite often happens that theoretical decision procedures have limited usefulness in practice (e.g. Tarski's original quantifier elimination peocedure for real algebra), or conversely that apparently hopeless combinatorial explosions often fail to manifest themselves in many problems of real interest (e.g. in DPLL–based SAT checking). Towards the end of our lectures we will focus on a special topic that is of some interest to us: how can we implement decision methods so that they always produce proofs or certificates rather than merely a yes/no answer?

Reading list

For decidable subsets of pure first–order logic, see Ackermann (1954) and Dreben and Goldfarb (1979). Decision procedures for particular theories, often based on quantifier elimination, are given in many logic texts including Enderton (1972) and Kreisel and Krivine (1971), while a sharply focused survey is given by Rabin (1991). The usual limitative results are a staple of traditional logic texts; see for example Smullyan (1992) and Smoryński (1980). Discussions of practical implementation and use of decision procedures are mostly scattered in research papers rather than assembled into a neat textbook canon — we hope these lectures will contribute to a clearer picture. One major practical decision method that is well represented is the Gröbner basis method – see for example Cox, Little, and O'Shea (1992), Weispfenning and Becker (1993). For automated methods in geometry, see Chou (1988).

The following Web site contains explicit OCaml code written by the author for various simple decision algorithms: `http://www.cl.cam.ac.uk/users/jrh/atp/index.html`

References

1. W. Ackermann. *Solvable Cases of the Decision Problem. Studies in Logic and the Foundations of Mathematics*, North–Holland, 1954
2. S.-C. Chou. *Mechanical Geometry Theorem Proving*, Reidel, 1988
3. D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms*, Springer–Verlag, 1992
4. B. Dreben, W.D. Goldfarb. *The Decision Problem: Solvable Cases of Quantificational Formulas*, Addison–Wesley, 1979

5. H.B. Enderton. *A Mathematical Introduction to Logic*, Academic Press, 1972
6. G. Kreisel, J.-L. Krivine. *Elements of Mathematical Logic: Model Theory* (Revised second ed.), Studies in Logic and the Foundations of Mathematics, North–Holland, 1971
   First edition 1967: Translation of the French *Eléments de logique mathématique, théorie des modeles* published by Dunod, Paris, 1964.
7. M.O. Rabin. *Decidable Theories*, In: J. Barwise, H. Keisler (eds.), Handbook of Mathematical Logic, Vol.90 of Studies in Logic and the Foundations of Mathematics, pp. 595-629. North–Holland, 1991
8. C. Smoryński. *Logic Number Theory I: An Introduction*, Springer–Verlag, 1980
9. R.M. Smullyan. *Gödel's Incompleteness Theorems*, Vol.19 of Oxford Logic Guides. Oxford University Press, 1992
10. V. Weispfenning, T. Becker. *Groebner Bases: a Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics. Springer–Verlag, 1993