Automated and Interactive Theorem Proving

John Harrison
Intel Corporation, Hillsboro OR, USA

The idea of mechanizing reasoning is an old dream that can be traced at least back to Leibniz. Since about 1950, there has been considerable research on having computers perform logical reasoning, either completely autonomously (automated theorem proving) or in cooperation with a person (interactive theorem proving). Both approaches have achieved notable successes. For example, several open mathematical problems such as the Robbins Conjecture have been settled by automated theorem provers, while interactive provers have been applied to formalization of non-trivial mathematics and the verification of complex computer systems. However, it can be difficult for a newcomer to gain perspective on the field, since it has already fragmented into various special subdisciplines. The aim of these lectures will be to give a broad overview that tries to establish some such perspective. I will cover a range of topics from Boolean satisfiability checking (SAT), several approaches to first-order automated theorem proving, special methods for equations, decision procedures for important special theories, and interactive proof. I will not say much in detail about applications, but will give some suitable references for those interested.

References

For readable semi-popular accounts with some historical background, see Davis (2000), Devlin (1997), MacKenzie (2001) and Marciszewski and Murawski (1995).For purely Boolean methods and their applications see Kropf (1999). Classical topics in firstorder and propositional logic are discussed by Bibel (1987), Chang and Lee (1973), Duffy (1991), Fitting(1990) and Wos, Overbeek, Lusk, and Boyle (1992). For equational reasoning, see Baader and Nipkow (1998) and the survey articles by Huet and Oppen (1980), Klop (1992) andPlaisted (1993). Decision procedures for algebraic theories lying partly in logic and partly in algebra or algebraic geometry are considered by Cox, Little, and O'Shea (1992), Mishra (1993), Mignotte (1991) and Weispfenning and Becker (1993). For a nice survey of some of the main interactive systems, see Wiedijk (2006).

1. Baader,F. and Nipkow,T. *Term Rewriting and All That*. Cambridge University Press, 1998.
2. Bibel,W. *Automated Theorem Proving*(2nd ed.). Vieweg Verlag, 1987.
3. Chang, C.-L. and Lee, R. C. *Symbolic Logic and Mechanical Theorem Proving*. Academic Press, 1973.
4. Cox, D., Little, J., and O'Shea, D. *Ideals, Varieties, and Algorithms*. Springer-Verlag, 1992.
5. Davis, M. (2000) *The Universal Computer: The Road from Leibniz to Turing*. W. W. Norton and Company, 2000. Paperback edition entitled "Engines of Logic: Mathematicians and the Origin of the Computer", 2001.
6. Devlin, K. *Goodbye Descartes: The End of Logic and the Search for a New Cosmology of the Mind*. Wiley, 1997.
7. Duffy, D. A. *Principles of Automated Theorem Proving*. Wiley, 1991.
8. Fitting, M. *First-Order Logic and Automated Theorem Proving*. Graduate Texts in Computer Science. Springer-Verlag, 1990. 2nd edition 1996.
9. Huet, G. and Oppen, D. C. *Equations and Rewrite Rules: A Survey*. In Book, R.V. (ed.), *Formal Language Theory: Perspectives and Open Problems*, pp. 349–405. Academic Press, 1980.

10. Klop, J. W. *Term Rewriting Systems*. In Abramsky, S., Gabbay, D. M., and Maibaum,T.S.E. (eds.), *Handbook of Logic in Computer Science, vol. 2. Background: Computational Structures*, pp. 1–116, Clarendon Press, 1992.
11. Kropf, T. *Introduction to Formal Hardware Verification*. Springer-Verlag, 1999.
12. MacKenzie, D. *Mechanizing Proof: Computing, Risk andTrust*. MIT Press, 2001.
13. Marciszewski, W. and Murawski, R. *Mechanization of Reasoning in a Historical Perspective*, Vol. 43 of *Poznań Studies in the Philosophy of the Sciences and the Humanities*. Rodopi, Amsterdam, 1995.
14. Mignotte, M. (1991) *Mathematics for Computer Algebra*. Springer-Verlag, 1991.
15. Mishra, B. *Algorithmic Algebra*. Springer-Verlag, 1993.
16. Plaisted, D. A. *Equational Reasoning and Term Rewriting Systems*. In Gabbay, D. M., Hogger, C. J., and Robinson, J. A. (eds.), *Handbook of Logic in Artificial Intelligence and Logic Programming, vol 1(logical foundations)*, pp. 273–364, Oxford University Press, 1993.
17. Weispfenning, V. and Becker, T. *Groebner Bases: A Computational Approach to Commutative Algebra*. Graduate Texts in Mathematics. Springer-Verlag, 1993.
18. Wiedijk, F. *The Seventeen Provers of the World*, LNCS 3600, Springer-Verlag, 2006.
19. Wos, L., Overbeek, R., Lusk, E., and Boyle, J. *Automated Reasoning: Introduction and Applications*. McGraw Hill, 1992.