Refutationally Complete Inference Rules for Inductive Theorem Proving based on Term Rewriting Techniques
(Extended Abstract)

Akihiko Ohsuga
Systems and Software Engineering Laboratory
Research and Development Center, Toshiba Corporation
70, Yanagi-cho, Saiwai-ku, Kawasaki, Kanagawa 210, Japan
ohsuga@ssel.toshiba.co.jp

Kô Sakai
Institute of Information Sciences and Electronics
University of Tsukuba
1-1-1, Tennodai, Tsukuba, Ibaragi 305, Japan
sakai@is.tsukuba.ac.jp

Shin-ichi Hon-iden
Systems and Software Engineering Laboratory
Research and Development Center, Toshiba Corporation
honiden@ssel.toshiba.co.jp

An equation valid in the initial model of an equational theory is called an inductive theorem. In this paper, we present an inductive theorem proving method in the form of inference rules. The method can be seen as an extension of the inductive completion procedures presented by Goguen Musser, Huet, Fribourg, and Bachmair. Compared with their procedures, our method can handle unorientable axioms and theorems. Moreover, it can prove theorems even when the canonical term rewriting system corresponding to a given equational theory contains an infinite number of rewrite rules. The method is refutationally complete; that is, if at least one of theorems is not correct, then it always finds a disproof.

Musser and Goguen showed that the correctness of an inductive theorem T in an equational theory E is equivalent to the consistency of an extended axiom system E' obtained by adding T to an axiom set of E as a new axiom[4, 8]. Moreover, they suggested that the Knuth-Bendix completion procedure[7] can be used to prove the consistency of the new system E'. Their method has only one kind of inconsistency, that is true=false. Huet and Hullot proposed a method that finds inconsistencies more easily by decomposing function symbols into constructors and defined symbols. Dershowitz pointed out that an equation T is valid in the initial model defined by

R if and only if no equality between two distinct irreducible ground terms follows from R and T[2]. Fribourg presented a linear proof method which restricts the number of critical pairs to be generated[3]. These proof methods are called inductive completion procedures. Bachmair showed that the proof ordering method can be applied to prove the completeness of these inductive completion procedures[1].

In spite of the fact that the inductive completion procedure works efficiently, several problems still remain to be solved. Those are: (1) it does not work if the canonical term rewriting system corresponding to the given equational theory contains an infinite number of rewrite rules, (2) it fails if at least one generated equation is not orientable under the given ordering, and (3) it loops if an infinite number of critical pairs are generated. In this paper, we address all of these problems by presenting a new inductive theorem proving method which is based on Bachmair's proof by consistency[1]. Our method starts with E, given equational theory, and T, inductive theorems to be proved; while other completion procedures start with R, the canonical rewriting system corresponding to E, and T. The method performs inductive theorem proving by generating a term rewriting system corresponding to E, and terminates after sufficient rewrite rules are obtained. Therefore, the first problem can be avoided. As for the second problem, we employ orientation-free rewrite rules. With these rewrite rules, the method can obtain a ground convergent rewriting system. Since inductive completion needs confluence only on the set of ground terms, the extended method is still refutationally complete. It is well-known that the termination problem of the Knuth-Bendix procedure is undecidable. Then, for the last problem, we introduce a criterion, called a recursive pair, to detect cases where the procedure fails to terminate. This criterion is based on Hermann's crossed pair which examines the structure of critical pairs to find infinite loops in the Knuth-Bendix completion[5].

References

[1] Bachmair, L.: *Canonical Equational Proofs*, Progress in Theoretical Comput. Sci., Birkhäuser (1991).

[2] Dershowitz, N.: Applications of the Knuth-Bendix Completion Procedure, in *Seminaire d'Informatique Theorique* (1982), pp. 95–111.

[3] Fribourg, L.: A Strong Restriction of the Inductive Completion Procedure, *J. Symbolic Computation*, Vol. 8, No. 3&4 (1989), pp. 253–276.

[4] Goguen, J. A.: How to Prove Algebraic Induction Hypothesis without Induction, with Application to the Correctness of Data Type Implementation, LNCS 87, Springer-Verlag (1980), pp. 356–373.

[5] Hermann, M. and Privara, I.: On Nontermination of Knuth-Bendix Algorithm, LNCS 226, Springer-Verlag (1986), pp. 146–156.

[6] Huet, G. and Hullot, J.-M.: Proofs by Induction in Equational Theories with Constructors, *J. Comput. Syst. Sci.*, Vol. 25, No. 2 (1982), pp. 239–266.

[7] Knuth, D. E. and Bendix, P. B.: Simple Word Problems in Universal Algebras, in *Proc. Computational problems in abstract algebra*, Pergamon Press (1970), pp. 263–297.

[8] Musser, D. R.: On Proving Inductive Properties of Abstract Data Types, in *Proc. 7th ACM Symposium on Principles of Programming Languages* (1980), pp. 154–162.