On Strategies for Inductive Theorem Proving

Bernhard Gramlich*

Fakultät für Informatik, TU Wien
Favoritenstr. 9 – E185/2, A–1040 Wien, Austria

Abstract

Inductive Theorem Proving (ITP) is a challenging field in automated reasoning and theorem proving. Typically, *Automated Theorem Proving* (ATP) refers to methods, techniques and tools for automatically proving *general* (most often first-order) theorems. Nowadays, the field of ATP has reached a certain degree of maturity and powerful ATP systems are widely available and used. The situation with ITP is strikingly different, in the sense that proving inductive theorems in an essentially automatic way still is a very challenging task, even for the most advanced existing ITP systems. Both in general ATP and in ITP strategies for guiding the proof search process are of fundamental importance, in automated as well as in interactive or mixed settings. In the talk we will try to give a thorough assessment of strategies in ITP and, more generally, of the main structural, conceptual and technical problems and challenges that need to be addressed in order to achieve major progress towards *Automated Inductive Theorem Proving* (AITP).

1 Background and Overview

Theorem proving tasks are ubiquitous in computer science, e.g. in fields like program specification, transformation and verification. Most often the given, generated or resulting proof tasks are not *general* ones (in the sense, that validity in all models of the underlying logic specification is to be established), but more specific ones, where (in)validity is to be shown only in some subclass of models (or in a unique *standard model* provided it exists). The class of formulae being valid in such restricted classes of models is usually much bigger than the one consisting of the general theorems. Typically, any reasonable approach for proving such properties needs some kind of *induction* (which is one source of explanation why such theorems are called *inductive theorems*). In fact, in computer science applications, in particular in (formal foundations of) software engineering and reasoning about specifications and programs, most often the specifier, programmer or user is not interested so much in all models of a given specification (or axiomatization), but rather in a specific (and often unique) natural model that is induced by the specification and that closely corresponds to her/his intuition. This means that for proving properties (general) ATP is usually insufficient and can only be used as a kind of first default approach. If a conjecture is provable via ATP, then it is also

*email: `gramlich@logic.at` www: `www.logic.at/staff/gramlich/`

an inductive theorem, but if it's not provable by ATP (or even proved to be not valid in general), then it may still be an inductive theorem.

ATP has turned out to be fairly successful nowadays (in its range of applications), whereas this does not really hold for ITP, more precisely for AITP. Hence, in the presentation we will also emphasize and analyze the differences between ATP and (A)ITP, from the point of view of strategies, but also regarding more fundamental, conceptual and proof search aspects.

The issues we intend to cover in the talk include the following:

- ATP vs. (A)ITP
- different underlying frameworks (and logics) for ITP
- the importance of strategies in (A)ITP
- the current state of the art in (A)ITP
- assumptions about and basic settings for (A)ITP
- strategies in (A)ITP
- major problems in (A)ITP
- challenges
- theses

Though we will illustrate various aspects by examples, the nature of this work is more conceptual and primarily non-technical. Its main contributions are intended to be a thorough analysis of the nature of inductive theorem proving tasks and of possible proof strategies, and an attempt to interrelate, classify and estimate the difficulties arising from many different sources in ITP. In particular, we will identify a couple of requirements (and obstacles) for the design and implementation of successful (A)ITP systems, and some main challenges regarding further essential progress in the field. Finally, we also present and discuss a few theses about the state of the field and future research perspectives that may not be widely shared, but for which there is quite some evidence. If the latter considerations were to entail a lively discussion in the research community, this would already be a very positive consequence.