Verified Decision Procedures for Linear Arithmetic

Tobias Nipkow
Technische Universität München, Germany

The focus of this lecture series will be on decision procedures for linear arithmetic (only $+$, no $*$) and their realization in foundational theorem provers. By foundational I mean theorem provers like LCF, Isabelle and Coq, which have a small trusted kernel performing small inference steps, and where all inferences have to go through this kernel. Although we use arithmetic for concreteness, the course is also a general introduction of how to implement arbitrary decision procedures in foundational provers.

The course will cover the following topics:

Quantifier elimination The course focusses on two well-known quantifier elimination algorithms (and hence decision procedures) for linear arithmetic: Fourier-Motzkin elimination, which is complete for rationals and reals, and Cooper's method, which is complete for the integers. These algorithms are first introduced on an abstract mathematical level.

Tactics were introduced in the LCF theorem prover to program decision procedures based on a fixed set of inference rules using an external functional language. We explain how to implement the above quantifier elimination procedures as tactics.

Proof by reflection This is a technique for programming decision procedures for fragments of the logic *within* the logic. Again we demonstrate this approach by means of the above decision procedures.

No previous exposure to theorem provers is required. Familiarity with functional programming (e.g. [2]) and the basics of first-order logic (e.g. [1]) is assumed.

References

1. M. Huth and M. Ryan. *Logic in Computer Science*. Cambridge University Press, 2000.
2. L. C. Paulson. *ML for the Working Programmer*. Cambridge University Press, 2nd edition, 1996.