

Towards Constraint-Solving over Higher-Order Unbounded Datatypes using Formal Methods Tools

Invited talk

Michael Leuschel

Institut für Informatik, Universität Düsseldorf
`leuschel@cs.uni-duesseldorf.de`

Abstract

We argue that formal methods such as B can be used to conveniently express a wide range of constraint satisfaction problems. We also show that some problems can be solved quite effectively by existing formal methods tools such as Alloy or ProB. We illustrate our claim on several examples. Our approach is particularly interesting when a high assurance of correctness is required. Indeed, validation and double checking of solutions is available for certain formal methods tools and formal proof can be applied to establish important properties or provide unambiguous semantics to problem specifications. The experiments also provide interesting insights about the effectiveness of existing formal method tools, and highlight interesting avenues for future improvement.