Proof Techniques for the Synthesis of Sorting Algorithms

Tudor Jebelean

RISC, JKU Linz, Austria
Tudor.Jebelean@jku.at

Abstract

We develop proof techniques for the synthesis of sorting algorithms in the automated reasoning environment *Theorema* (www.theorema.org), which allows to define and organize the logical formulae expressing mathematical theories and algorithm specifications, as well as to construct proofs. In this system, we prove automatically the formalization of the synthesis statement "*for any list, there exists a sorted version of it*" and we extract the algorithm from the proof. For this purpose, a suitable theory of lists is constructed, consisting in basic axioms and proven properties, the specification of the sorting problem is formalized, and then the proof of the synthesis statement is carried out automatically. By user choice of the appropriate knowledge given to the prover, as well as of various proof strategies and induction principles, we synthesize four different known sorting algorithms: selection-sort, insertion-sort, merge-sort, and quick-sort, plus one which is a new variation of merge-sort. In principle most parts of the proofs could be carried out by SLD resolution (as in Prolog interpreters), however this leads to very large proofs. Therefore we follow the *Theorema* tradition of generating proofs in natural style, by using novel proof techniques for lists. For instance we introduce specific inference rules and strategies for reasoning with the equivalence relation over lists (induced by the predicate "have the same elements") and with various ordering relations on lists (induced by the ordering among elements). We also use a novel treatment of the failed proof branches on goals containing no lists, in order to improve the proof and to generate case distinctions in the algorithms. The case study provides a basis for further investigation of the general principles of theory exploration and of proof–based synthesis, and the results are encouraging for extending this approach to other domains.

Keywords: Automated Reasoning, Algorithm Synthesis, Sorting