Abstract: Towards an SMT-LIB Theory of Heap

Zafer Esen and Philipp Rümmer

Abstract

Constrained Horn Clauses (CHC) are a convenient intermediate verification language that can be generated by several verification tools, and that can be processed by several mature and efficient Horn solvers. One of the main challenges when using CHC in verification is the encoding of program with heap-allocated data-structures: such data-structures are today either represented explicitly using the theory of arrays, or are transformed away with the help of invariants or refinement types. Both approaches have disadvantages: they are low-level, do not preserve the structure of a program well, and leave little design choice with respect to the handling of heap to the Horn solver. This abstract presents ongoing work on the definition of a high-level SMT-LIB theory of heap, which in the context of CHC gives rise to standard interchange format for programs with heap data-structures. The abstract presents the signature and intuition behind the theory. A preliminary version of the theory axioms can be found in the appendix. The abstract is meant as a starting point for discussion, and request for comments.

François Bobot, Tjark Weber (eds.); SMT 2020, pp. 60–60