Decidability and Undecidability in Symbolic-Heap System with Inductive Definitions

Makoto Tatsuta\textsuperscript{1} and Daisuke Kimura\textsuperscript{2}

\textsuperscript{1} National Institute of Informatics, Tokyo, Japan, tatsuta@nii.ac.jp
\textsuperscript{2} Toho University, Chiba, Japan

A symbolic-heap system is a fragment of separation logic, and characterizes only shapes of heaps by abstraction. It is useful for memory error checking in software verification. The truth of entailments in this system is known to be decidable.

Extensions of the symbolic-heap systems with inductive definitions have been actively studied recently. Inductive definitions enable us to use recursive data structures such as lists and trees in a symbolic-heap system.

The bounded-treewidth separation logic given in [1] is one of promising extensions with inductive definitions. The fragment is decidable. However they impose some condition for existential variables and this condition excludes implicit existentials.

An implicit existential is an existential variable such that the variable occurs only once in a give formula. So its value is not related to other values. An implicit existential is often denoted by the underscore _ for this reason. Implicit existentials are necessary for keeping data in each node in recursive data structure such as a list of pointers.

We first show the undecidability of the truth of entailments in the bounded-treewidth separation logic with implicit existentials. It is proved by simulating the Post corresponding problem in the system.

We next show the decidability of that in the same system under the restriction that every inductively defined predicate is essentially unary. It is proved by introducing some distinguished address in heaps, transforming heaps so that the addresses given by implicit existentials are changed into local addresses or the distinguished address, and showing that this transformation preserves the truth of logical formulas.

The research is supported by Core-to-Core Program (A. Advanced Research Networks) of the Japan Society for the Promotion of Science.

References