Paper Review《Property-Directed Shape Analysis》

Paper Info

S. Itzhaky, N. Bjorner, T. Reps, M. Sagiv and A. Thakur

CAV 2014

Main Contribution

In this work, the authors express the shape information in the logic expressions. They attempt to obtain the shape invariants by adding the counter examples. The counter examples can be genereated based on SAT solver.

Different from other kinds of shape analysis, the approach in this work only takes advantages of the logic expressions in order to describe the shape information. Other instances of shape analysis abstract the memory locations and construct the shape graphs, which are not used in this work.

The major constributions of this paper include:

- Propose a framework for finding an inductive invariant in a certain abstract domain and describe the pre/post condition
- Instantiate of the framework for finding invariants of programs that manipulate single-linked or doubly-linked lists.

Main Work

Similiar to the logical abstraction in other instances of shape analysis, the authors propose some predicates to describe the shape info, such as equality, point-to relations and so on. They express such predicates in the form of AFr and EAr logics. In Table 3, five predicates are describe by AFr formulas.

In the dataflow framework, the senamics of each statement also need to be formalized by logic. Table 5 gives the post conditions of each command with a given pre condition. With these definitions, it is available to get the shape info in the dataflow framework.

The last problem is how to generate the shape invariants. The key insight is to find a counter examples of the shape logical expression and add it to the previous expression. In this way, the fixed point can be reached after several iterations.

Future Work

The approach in this paper is a parametric framework. When applied to an instance, it needs to be concretized. In Section 4, all the predicates need to be defined explicitly.

In other applications, the framework should also be concretized in different ways. For example, the predicates needs to be defined and expressed in some certain logic expressions. Also, the statements should be describe by the formulas. This process demands manual efforts. It contradicts the idea of the automatic analysis. This is the limitation of the logic methods in the shape analysis.