

Paper Review 《A relational approach to interprocedural shape analysis》

Paper Info

Bertrand Jeannot, Alexey Loginov, Thomas Reps, Mooly Sagiv, TOPLAS 2010

Main Contribution

This paper proposes a method for abstracting relations over memory configurations for use in abstract interpretation. The authors utilize the 3-valued logic to maintain the predicates of program properties, which is theoretically accurate than the traditional 2-valued logic. They combine the transformation relations extracted from each function to express the semantics of interprocedural programs. The main contributions of this work include:

- Encode the properties of memory configurations into logic, and use predicates to express the shape information in each program state.
- Convert the predicates in 2-valued logic to 3-valued logic, and prove that the conversion preserve the over-approximation of the abstraction.
- Propose a compositional approach to shape analysis, and create the procedure summaries using abstracted relations over memory configurations.

Main Work

The main work of this paper consists of the following three parts:

- Abstracting memory configurations

In the previous work, researchers used to model the properties of memory in 2-valued logic, which only has the value as True or False. However, the information might be lost in the path join of abstract interpretation. Sagiv developed the abstraction method which maps 2-valued logic structures of arbitrary size to 3-valued logical structures of bounded size. In this work, the key problem of this part is to merge concrete individuals into a bounded number of abstract individuals and transform the predicates at the same time.

- Representing and abstracting relations between memory configurations

Except for the conversion of predicates, the relation composition and relational instrumentation predicates needs to be defined. They extract the summaries of procedures into the pairs of predicates in 3-valued logic, combine two relations into one to model the function calls, and merge two sets of predicates into one set based on the meet operation.

- Interprocedural shape analysis

The rest of the work is easy. Based on the relations extracted from procedures, the rest work is to define and solve the dataflow equations, which is similar to the traditional dataflow analysis.

Future Work

To sum up, this paper is a ground-breaking work in the field of interprocedural shape analysis. Due to the limitation of knowledge, there still are many details which I can not understand, including the 3-valued logic and memory configurations. In the next few months, I plan to read more materials on these topic.