Département d'Informatique de l'Ecole Normale Supérieure

Abstraction of Relations between Memory States

Internship location : École Normale Supérieure ; 45, rue d'Ulm ; 75 230, PARIS.

Team : Équipe Sémantique et Interprétation Abstraite / Équipe-Projet "ANTIQUE".

Advisor & Contact : Xavier RIVAL (*email* : `rival@di.ens.fr`, phone : 01 44 32 21 50, fax : 01 44 32 21 51)

Internship objective :

Shape analysis [1] aims at inferring properties of data structures of unbounded size, that are generally dynamically allocated. Common examples are lists, graphs, trees. These structures usually rely on chains of pointers. Several abstractions have been proposed for the representation of properties of such structures. For instance, [1] relies on shape graphs and separation logic in order to describe complex memory states.

Several techniques can be used in order to analyze programs that consist of several procedures or functions. A first common technique consists in analyzing each function in its calling context. A second technique computes *once* an over-approximation of the relations between inputs and outputs, that can be utilized to analyze each instance of a procedure call [2]. The main difficulty of this second approach is that it is hard to discover a precise abstraction for input-output relations, that can describe precisely the behavior of a function.

In this internship, we propose to extend the shape graph representation of [1] into a notion of overlaid graphs, that share some of their edges, in order to describe sets of relations between memory states.

Work plan :

The first step of this internship will aim at formalizing an abstract domain to represent sets of relations between memory states, using overlaid graphs.

In a second phase, we will define transfer functions and abstract operators for the analysis of common program statements such as assignments, conditions and loops. This will require the design of an unfolding scheme and of a widening operator. These operators will be proved sound with respect to the concretization defined in the first phase.

Last, this abstract domain will be put to work in the context of a modular analysis, where each function is described by a relation between inputs and outputs.

The analysis will be implemented, and the **MemCAD** shape anlayzer can be used as a basis for this implementation. An empirical evaluation will also assess the behavior of the analysis using a library of small data-structures, and exceprts from micro-kernel code.

Pre-requisite :

The only pre-requisite is a strong interest in semantics, static analysis and program verification.

The course "2-6 Abstract interpretation" introduces the foundations required to accomplish this work.

Références

[1] Bor-Yuh Evan Chang and Xavier Rival. Relational inductive shape analysis. In POPL'08, pages 247–260, 2008.

[2] Bertrand Jeannet, Denis Gopan, Thomas W. Reps. A Relational Abstraction for Functions. In SAS'05, pages 186-202, 2005.