NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

PH.D DEFENCE - PUBLIC SEMINAR

Title:	**Automated Verification of Complete Specifications with Shape Inference**
Speaker:	Mr Le Quang Loc
Date/Time:	5 December 2014, Friday, 03:00 PM to 04:30 PM
Venue:	MR3, COM2-02-26
Supervisor :	Dr Chin Wei Ngan, Associate Professor, School of Computing

Abstract:

To achieve the highest Evaluation Assurance Level, mission-critical software components are required to be specified by formal specification and be verified by a proof system. However, existing verification systems focus mostly on good (safe) scenarios of functional properties (nothing bad will happen), while real world programs often contain bad scenarios. To bridge this gap, the thesis presents a solution for specifying, verifying and synthesizing both good and bad scenarios of heap-manipulating programs.

In the first part of this thesis, we present a complete specification mechanism that can specify both good and bad scenarios of program executions. A good execution is one that takes any permitted input and produces the expected output without any errors. A bad execution is one that takes some input but leads to some unexpected error. We present a verification system that supports complete specification. Our proposed system is capable of ensuring good scenarios (from safety proving) and detecting bad scenarios (from errors validation). A key principle of our proposal is a lattice of program status at the logic level, that is used to denote good and bad program states, and a new calculus to support systematic reasoning in the presence of errors.

In the second part of this thesis, we propose to automate verification system with specification inference. In the context of heap-manipulating programs, specification inference captures the analysis of shapes to describe abstractions for data structures used by each method. While previous shape analysis proposals rely on using a predefined vocabulary of shape definitions (typically limited to singly-linked list segments), our approach is able to synthesize, from scratch, a set of shape abstractions that is needed for ensuring memory-safe operations. The key concept behind our novel proposal is a second-order bi-abduction mechanism. With bi-abduction, we infer missing information that helps verifiers to either prove memory safety (for the good scenarios) or disprove it (for the bad scenarios). In this second-order mechanism, we use unknown predicates (or second-order variables) as place-holders for shape predicates that are to be synthesized. Our second-order bi-abduction

generates missing information as a set of relational assumptions on the unknown predicates that are obtained directly from proof obligations gathered by our verification process.

We next propose a transformational approach on each gathered set of relational assumptions. Our approach includes derivation and normalization steps. While the derivation infers sound definition for each unknown predicate, the normalization step further simplifies those definitions into a more concise, understandable and re-usable predicate form.

We have implemented the proposals in a prototype system and evaluated them by using the system to specify, verify, and synthesize specifications of programs with complex data structures. The experimental results demonstrate the viability of our proposals in inferring memory-safe specification and the verification of programs with complete specifications.