Formal verification of some mutual exclusion protocols with CafeInMaude, its proof assistant and its proof generator

1810446 TRAN Dinh Duong

Mutual exclusion is the problem such that at most one thread, process, node or any execution entity is allowed to enter its critical section to acquire the permission of using some shared resources, such as shared memory in concurrent and/or distributed systems. Mechanisms or protocols that solve the problem are called mutual exclusion protocols. It is important to guarantee that these protocols enjoy the mutual exclusion property and some other desired properties as well. In formal method, theorem proving is one promising technique that can be used to formally verify such problems. This technique especially shows its power when dealing with infinite-state systems, which model checking, although is the most well-known technique in formal method, however, cannot be used.

This thesis uses observational transition systems (OTSs) as state machines and CafeOBJ as a formal specification language to formalize systems (or protocols). Then, we can check whether protocols satisfy some properties by formally verifying that OTSs enjoys such properties. Formal verification, which uses theorem proving as the underlying technique, is essentially done by simultaneous structural induction on a state variable. The verification is conducted in three ways:

(1) by writing what are called proof scores and executing them with CafeInMaude,

(2) by using CafeInMaude Proof Assistant (CiMPA) to write what are called proof scripts, and

(3) by using CafeInMaude Proof Generator (CiMPG) to generate proof scripts from proof scores.

CafeInMaude is a tool to introduce CafeOBJ specifications into the Maude system. CiMPA and CiMPG are two extension tools of CafeInMaude. Three ways of verification all have advantages as well as disadvantages. By conducting formal verification in three ways, we triple-check the correctness of our proofs.

Two mutual exclusion protocols: A-Anderson that is an abstract version of Anderson protocol, and MCS are used as two case studies to illustrate the verification techniques. We formally prove that A-Anderson and MCS enjoy the mutual exclusion property. In both case studies, the most intellectual task is lemma conjecture, which is also considered as one of the most challenging problems in theorem proving. This thesis focuses on invariant properties, which are the most basic and important among various kinds of properties. During each invariant proof, we need to conjecture some auxiliary lemmas that are also invariants on the fly. Once we have constructed some good lemmas, the proof can be accomplished straightforwardly; otherwise, it may become unreasonably tough. This thesis also proposes a lemma conjecture technique that is called Lemma Weakening (LW). The usefulness of LW is demonstrated in the latter case study when conducting formal verification of MCS protocol. Briefly, without the use of LW, we would not have been able to complete the formal proof that MCS enjoys the mutual exclusion property.

Keywords: proof score, algebraic specification language, mutual exclusion protocol, lemma weakening