Abstract

The research underlying this thesis concerns the verification of concurrent systems. In particular, strategies are studied to tackle the state explosion problem which arises during the verification of concurrent systems by state space exploration. State (space) exploration, commonly known also as reachability analysis, amounts to exploring in a systematic manner the entire state space of a system, i.e. all states and transitions of the system that can be reached from a given initial state. It is a simple and fully automatic technique that can be employed in principle to verify many different types of correctness requirements of concurrent systems, ranging from various general consistency requirements to more system-specific, functional requirements. However, the state explosion problem severely limits the applicability of reachability analysis in practice. The state spaces of most realistic industrial-strength systems are excessive in size (comprising hundreds of thousands or even millions of states and transitions), and thereby surpass any conceivable amount of memory and time available for analysis.

One of the main causes of the state explosion problem in the verification of concurrent systems is the modeling of concurrency by interleaving or, more accurately, the exploration of all possible interleavings of concurrent events/translations. During reachability analysis, each possible way in which the execution of concurrent transitions can be ordered in time is examined. Yet, it has been recognized for quite some time that many interesting correctness properties of concurrent systems are insensitive to the interleaving order of concurrent transitions. Consequently, such systems often manifest a large number of reachable states and transitions that are redundant for verification purposes. For nearly two decades, this apprehension has inspired researchers to devise improved state exploration techniques that relieve the state explosion problem. These state exploration based relief strategies reduce the complexity of conventional reachability analysis by examining just part of the state space of a system, a part that is provably sufficient to verify one or several desirable properties. In effect, they enable the verification of concurrent systems without incurring (most of) the cost of modeling concurrency by interleaving.
Several of the strategies proposed to relieve the state explosion problem in the verification of concurrent systems have proved promising indeed, enabling in many cases substantial memory and time savings for state exploration. With the advent of these relief strategies, the applicability of verification by state exploration has thus certainly been widened to “larger” concurrent systems. Nevertheless, since concurrent systems are inherently complex and since this complexity is there to stay, pursuing further performance improvements in verification clearly remains of utmost importance. This thesis contributes by proposing improvements of three existing relief strategies, namely fair reachability analysis, simultaneous reachability analysis and partial-order reduction methods. These are among the most evolved state exploration based relief strategies to date. First, the technique of fair reachability analysis (FRA) is generalized from cyclic protocols to multi-cyclic protocols modeled as networks of communicating finite state machines (CFSMs). A multi-cyclic protocol constitutes one or more cyclic protocols, i.e. unidirectional rings, which are interconnected such that no two component cyclic protocols share more than one CFSM. FRA is established as an effective and efficient relief strategy for the detection of deadlocks in multi-cyclic protocols with a finite fair reachable state space (i.e. the reduced state space of the protocol explored by FRA). Furthermore, it is also shown that FRA is infeasible as a relief strategy beyond the class of multi-cyclic protocols.

Secondly, a technique called leaping reachability analysis (LRA) is presented as an incremental improvement of simultaneous reachability analysis (SRA), which was proposed as a relief strategy for the verification of logical correctness properties of protocols specified in the CFSM model without topological or structural constraints. For any protocol in this model, LRA is proven to maintain the power of SRA to detect all deadlocks, all non-executable transitions, all unspecified receptions and all buffer overflows of the protocol, while enabling further reductions in the size of the state space that needs to be analyzed. These analytical results are complemented by an empirical evaluation of the performance of LRA and SRA, which reveals that LRA can indeed yield important extra savings in space and time over SRA.

Lastly, an enhancement of partial-order reduction methods is proposed for linear-time temporal logic (LTL) model-checking. More precisely, the concepts underlying LRA are integrated with those underlying partial-order reduction methods to enable further savings in both space and time for the verification of linear-time temporal properties of general, finite-state concurrent systems (i.e. any system whose behavior can be defined as a finite transition system). This approach is subsequently fine-tuned for protocols specified in the CFSM model, whereby LRA emerges as an effective and uniform relief strategy for the verification of both logical (i.e. syntactic) and functional (i.e. semantic) correctness properties of protocols. Empirical results are provided which attest that the proposed approach to LTL model-checking is indeed a notable enhancement of the partial-order reduction approach.