

External Memory Algorithms for State Space Exploration in Model Checking and Action Planning

Abstract

RAM is a scarce resource. Several real-world problems in model checking and action planning are beyond the reach of traditional RAM-based algorithms, due to the so-called state space explosion problem. This dissertation aims at designing a set of algorithms that mitigates the memory bottleneck problem in model checking and planning, through a controlled and efficient usage of secondary storage mediums, such as hard disks. We consider a broad variety of system models ranging from simple undirected and unweighted state spaces to highly complex Markov decision processes (MDP). Path/cycle search problem in the case of deterministic state spaces and policy search problem in the case of MDPs are the focal points of this thesis. The state spaces, or the implicit graphs, are not provided beforehand, but are generated on-the-fly through a set of initial states and a set of transformation rules. The proposed algorithms belong to the category of External Memory (EM) algorithms and are analyzed for their asymptotic I/O complexity.

An EM guided search algorithm, called External A* (for being derived from the famous Best-First Search algorithm A*), is developed. External A* distinguishes itself from other external guided search approaches by being completely oblivious to the state space structure. Directed model checking has proved itself to be very effective in delivering shorter error trails and in memory savings. We incorporate external search into automata-based LTL model checking of concurrent systems through an extended variant of External A*. Accepting cycle detection lies at the heart of LTL model checking. Due to the inherent difficulty in cycle search in large graphs, earlier disk-based approaches distanced themselves from taking care of the full LTL model checking. In this dissertation, two algorithms for accepting cycle detection are put forward: a blind search algorithm based on Breadth-First

traversal, and a guided algorithm evolved from External A*. To be able to utilize the full potential of modern multi-core architectures and easily accessible networks of workstations, External A* is further extended into a distributed algorithm. For model checking large real-time systems and optimal real-time scheduling, EM algorithms for exploration in timed automata and priced timed automata are presented.

Graph-based action planning methods have achieved a significant level of maturity in the field of planning and scheduling. To integrate external heuristic search into planning, External Enforced Hill-Climbing is contributed. For optimal planning in PDDL3 domains involving preferences, a Cost-Optimal External Breadth-First Search is proposed. Nondeterministic and probabilistic state spaces are encountered both in model checking of stochastic systems and in planning under uncertainty. In such state spaces, one is interested not in a path but rather in a policy that maximizes the reward in reaching to a goal state. Due to the back-propagation of information in policy search, no efficient disk-based solution was ever contributed. We present an EM algorithm based on the standard Value Iteration procedure for policy search. The algorithm, External Value Iteration, is able to solve Bellman equations not only for large MDPs, but also for AND/OR graphs and Game trees.

The algorithms developed in this dissertation have been successfully integrated in some state-of-the-art tools including the SPIN model checker, MIPS-XXL (based on FF) planning system and UPPAAL-CORA for real-time scheduling. The largest reported exploration consumed 3 Terabytes of hard disk, while using only 3 Gigabytes of RAM lasting for 479 hours – time went down to 196 hours when 4 processors were engaged.