ProbDiVinE: A Parallel Qualitative LTL Model Checker*

Jiří Barnat, Luboš Brim, Ivana Černá, Milan Češka, and Jana Tůmová
Faculty of Informatics, Masaryk University, Botanická 68a, 60200 Brno, Czech Republic

Abstract

We introduce a parallel model checker for checking Markov decision processes against linear time properties. The model checker extends the parallel model checker DiVinE and supports verification of qualitative properties.

1. Introduction

Probabilistic systems like Markov chains and Markov decision processes provide a reasonable semantics for systems that exhibit uncertainty. Model checking of probabilistic systems branches into qualitative and quantitative approach. In the qualitative setting it is checked whether a property holds with probability 0 or 1; in a quantitative setting it is verified whether the probability for a certain property meets a given lower or upper bound.

For probabilistic systems the state explosion problem is more critical than in the non-probabilistic case. Several methods that have been developed for non-probabilistic systems to avoid the state explosion, were adapted to probabilistic systems. For branching time logics these are the symbolic approach implemented in the model checker PRISM [8, 7] and the MDP model checker RAPTURE [3] which uses an iterative abstraction refinement. For linear time logic the most prominent partial order approach has been recently adapted as well [1] and implemented in the verification tool LiQuor [4].

Over the past decade, many techniques using distributed and/or parallel processing have been proposed to combat the computational complexity of non-probabilistic verification, model checking in particular. However, not much has been done in applying these techniques to the verification and analysis of probabilistic systems. A notable exception is the work on parallelizing the symbolic model checker PRISM [10].

In this short tool paper we introduce a parallel model checker ProbDiVinE for qualitative model checking of finite state Markov decision processes (MDPs) against LTL properties. We use the automata-theoretic approach [9, 5, 6] where qualitative LTL model checking of MDPs is reduced to the question whether the product automaton for a given MDP with a Büchi acceptance condition contains an accepting end component (AEC).

2. How the tool works

The tool implements a parallel adaptation of the algorithm of de Alfaro (dA) [2]. It computes the set of states that contain all accepting end components. In particular, the algorithm maintains an approximation set of states that may belong to an AEC. The algorithm repeatedly refines the approximation set by locating and removing states that cannot belong to an AEC, we call this a pruning step. The core of the algorithm is the set of conditions determining the states to prune.

The algorithm by de Alfaro was the only one from the existing sequential approaches that allowed for a reasonable parallelization. The other algorithms, like the one of Courcoubetis and Yannakakis (CY) and CY with recursive elimination (CY+RE) [5] are based on repeated decomposition of the underlying graph of product MDP into strongly connected components and elimination of states violating their ergodic consistency or other techniques that are inherently sequential. For convenience ProbDiVinE also provides these serial algorithms and can use them on a single machine.

The input language PROBDVE of ProbDiVinE is a modification of DivINE’s native language DVE. PROBDVE models systems as a composition of processes, which can change their states via probabilistic (\(\rightarrow\)) or non-probabilistic (\(\Rightarrow\)) transitions and can synchronize using channels. An example of a PROBDVE source-code for randomized solution to the dining philosophers problem is given in Figure 1.

A non-probabilistic transition may have a guard (a condition which has to be satisfied for the transition to be enabled), an effect (assignment to a variable), and a sync expression (for synchronization with another transition via channel). A probabilistic transition just determines probability of resulting state, which is given by weights assigned...
byte fork[3] = {0, 0, 0}; byte hungry[3] = {1, 1, 1};

process Philosopher_0 {
  state thinks, eats, want_L, want_R, has_L, has_R;
  init thinks;
  trans
    thinks => { want_L: 1, want_R: 1 },
    want_L -> has_L { guard fork[0] == 0; },
    has_L -> eats { guard fork[1] == 0; },
    has_L -> thinks { guard fork[1] == 1; },
    want_R -> has_R { guard fork[1] == 0; },
    has_R -> eats { guard fork[0] == 0; },
    has_R -> thinks { guard fork[0] == 1; },
    eats -> thinks { effect hungry[0] = 0; },
}

process Philosopher_1 { ... }

... system async;

Figure 1. Example of PROBDVE source-code.

Figure 2. ProbDiVinE structure.

PROBDVE is currently operated in command-line mode. The input is given as a .probdve file and the LTL formula given as an .ltl file. Further parameters include the algorithm to be used, number of workstations involved in the computation etc. Details are given in the documentation. The tool can be downloaded together with the DIVINE tool from the page http://anna.fi.muni.cz/divine/probdive.

Our initial experiments confirmed good scalability on many examples. In several cases the sequential algorithms were much faster than the parallel algorithm, however, once the internal memory has been exhausted only the parallel algorithm was able to finish the computation.

Our intention is to extend ProbDiVinE to quantitative LTL model checking by using a distributed linear solver, to add the possibility of checking reward properties, as well as to build a suitable graphical user interface.

References


