Bounded Probabilistic Model Checking
with the Murϕ Verifier

Giuseppe Della Penna1, Benedetto Intrigila1, Igor Melatti1,⋆, Enrico Tronci2, and Marisa Venturini Zilli2

1 Dip. di Informatica, Università di L’Aquila, Coppito 67100, L’Aquila, Italy
{dellapenna,intrigila,melatti}@di.univaq.it
2 Dip. di Informatica Università di Roma “La Sapienza”
Via Salaria 113, 00198 Roma, Italy
{tronci,zilli}@dsi.uniroma1.it

Abstract. In this paper we present an explicit verification algorithm for
Probabilistic Systems defining discrete time/finite state Markov Chains.
We restrict ourselves to verification of Bounded PCTL formulas
(BPCTL), that is, PCTL formulas in which all Until operators are
bounded, possibly with different bounds. This means that we consider
only paths (system runs) of bounded length. Given a Markov Chain M
and a BPCTL formula Φ, our algorithm checks if Φ is satisfied in M.
This allows to verify important properties, such as reliability in Discrete
Time Hybrid Systems.

We present an implementation of our algorithm within a suitable exten-
sion of the Murϕ verifier. We call FHP-Murϕ (Finite Horizon Probabilis-
tic Murϕ) such extension of the Murϕ verifier.

We give experimental results comparing FHP-Murϕ with (a finite horizon
subset of) PRISM, a state-of-the-art symbolic model checker for Markov
Chains. Our experimental results show that FHP-Murϕ can effectively
handle verification of BPCTL formulas for systems that are out of reach
for PRISM, namely those involving arithmetic operations on the state
variables (e.g. hybrid systems).

1 Introduction

Model checking techniques [5, 12, 19, 18, 25, 32] are widely used to verify correct-
ness of digital hardware, embedded software and protocols by modeling such
systems as Nondeterministic Finite State Systems (NFSSs).

However, there are many reactive systems that exhibit uncertainty in their
behavior, i.e. which are stochastic systems. Examples of such systems are: fault
tolerant systems, randomized distributed protocols and communication proto-
cols. Typically, stochastic systems cannot be conveniently modeled using NFSSs.
However, they can often be modeled by Markov Chains [2, 15]. Roughly speaking,
a Markov Chain can be seen as an automaton labeled with (outgoing) probabil-
ities on its transitions.

⋆ Corresponding Author: Igor Melatti. Tel: +39 0862 43 3189 Fax: +39 0862 43 3057.
For stochastic systems correctness can only be stated using a probabilistic approach, e.g. using a Probabilistic Logic (e.g. [33,8,14]). This motivates the development of Probabilistic Model Checkers [9,1,20], i.e. of model checking algorithms and tools whose goal is to automatically verify (probabilistic) properties of stochastic systems (typically Markov Chains). For example, a probabilistic model checker may automatically verify a system property like “the probability that a message is not delivered after 0.1 seconds is less than 0.80”. Note that, following [20,21], we are using the expression “probabilistic model checking” to mean model checking of probabilistic systems.

Many methods have been proposed for probabilistic model checking, e.g. [11,3,8,14–16,22,31,33].

To the best of our knowledge, currently, the state-of-the-art probabilistic model checker is PRISM [30,1,21]. PRISM overcomes the limitations due to the use of linear algebra packages in Markov Chain analysis by using Multi Terminal Binary Decision Diagrams (MTBDDs) [7], a generalization of Ordered Binary Decision Diagrams (OBDDs) [4] allowing real numbers in the interval [0,1] on terminal nodes. Roughly speaking, PRISM can use three approaches to Markov Chain analysis. Namely: a sparse matrix based approach (based on linear algebra packages), a symbolic approach (based on the CUDD package [10]) and a hybrid approach, which uses MTBDDs to represent the system transition matrix and sparse matrix algorithms to carry out the (quantitative) probabilistic analysis [21]. As shown in [21], PRISM hybrid approach is faster than probabilistic model checkers based only on MTBDDs (e.g., ProbVerus [34]) and avoids the state explosion problem of probabilistic model checkers based only on sparse matrices (e.g., ETMCC [17] or the algorithms in [14,15]).

Here we are mainly interested in automatic analysis of discrete time/finite state Markov Chains modeling Discrete Time Hybrid Systems. Such Markov Chains can in principle be analyzed using PRISM. However, our experience is that, using PRISM on our systems, quite soon we run into a state explosion problem, i.e. we run out of memory because of the huge OBDDs built during the model checking process. This is due to the fact that hybrid systems dynamics typically entails many arithmetical operations on the state variables. This makes life very hard for OBDDs, thus making usage of a symbolic probabilistic model checker (e.g. like PRISM) on such systems rather problematic.

To this end in [27] is presented an explicit disk based algorithm for automatic Finite Horizon safety analysis of Markov Chains. The algorithm in [27] has been implemented in the probabilistic model checker FHP-Murϕ (Finite Horizon Probabilistic Murϕ) [6].

The experimental results in [27] show that FHP-Murϕ outperforms PRISM on (discrete time) hybrid systems verification. Note however that PRISM can handle all PCTL [14] logic, whereas FHP-Murϕ only handles finite horizon safety properties (e.g. like “the probability of reaching an error state in k steps is less than a given threshold”). Moreover, in [28] it is shown that FHP-Murϕ input language is more natural than the PRISM one in order to specify many Stochastic Systems.