HAL
open science

Model Checking by Censoring Markov Chains and Stochastic Comparison

Nihal Pekergin, Sana Younes

To cite this version:

Nihal Pekergin, Sana Younes. Model Checking by Censoring Markov Chains and Stochastic Comparison. 12th European Workshop on Dependable Computing, EWDC 2009, May 2009, Toulouse, France. 7 p. hal-00380667

HAL Id: hal-00380667

https://hal.science/hal-00380667

Submitted on 12 May 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Model Checking by Censoring Markov Chains and Stochastic Comparison

Nihal Pekergin *
* LACL, University Paris-Est,
61 avenue Général de Gaulle 94010,
Créteil, France
Email: nihal.pekergin@univ-paris12.fr

Sana Younès † *
† PRiSM, Université Versailles St Quentin,
45, Av. des États-Unis, 78035
Versailles, France
Email: sayo@prism.uvsq.fr

***Abstract*— We study how to combine the censoring technique for Markov chains and the strong stochastic comparison to perform model checking of discrete-time Markov chains. Our goal is to reduce the complexity of the model checking in order to be able to consider numerically intractable models. In model checking we do not need the exact values but we must decide if the required guarantees are satisfied or not. Thus bounding methods are suitable in this context : if the bounds meet the threshold we can decide for the satisfaction of the formula. In the case when it is not possible to decide the satisfaction of the underlying formula through the bounds, we can refine the bounds by considering a larger set of states.**

I. Introduction

Model checking is a method to automatically check if complex performability measures expressed by using formal logics are satisfied or not. Traditional model-checking techniques for the integrated analysis of both qualitative and quantitative system properties has been extended to stochastic models. Especially, labelled Markov chains in which a list of atomic propositions are assigned to states are used as models in probabilistic model checking: Probabilistic Computation Tree Logic (PCTL) [13] with Discrete Time Markov Chains (DTMC) and Continuous Stochastic Logic (CSL) [4] with Continuous Time Markov Chains (CTMC). In these logics the properties over paths are described by path formulas. Thus it is possible to study transient properties as well as long run behaviours. In numerical model checking, the state space explosion problem may limit the size of tractable models with conventional techniques. Different methods as decomposition, bounding, storage methods have been proposed to overcome this problem.

Bounding methods are suitable in model checking context since we need to verify if some thresholds are satisfied or not without computing the exact values. In [9], the bounds on state reachability probabilities of Markov decision processes are computed by abstraction of the underlying model defined on smaller state spaces. If the verification of the considered property cannot be concluded, the abstract model is refined until a verdict to the property can be deduced from the computations. We propose the stochastic comparison techniques which have been largely applied in different areas of applied probability as well as in reliability, performance evaluation, dependability applications [17]. Intuitively speaking, this method consists in computing bounding distributions rather than the exact distributions by analysing "simpler" bounding chains. This method let us to derive bounds on transient distributions as well as on the steady-state distribution. The stochastic comparison techniques have been applied in [18], [6] to overcome state space explosion problem in the model checking context. In [18], the underlying models are simplified by means of bounding aggregations and in [6] by bounding Markov chains having closed-form solutions for transient and the steady-state distributions.

In this paper we propose to combine censoring and stochastic comparison techniques to perform efficiently model checking. Censored Markov chains take values in a restricted state space and observed at successive visits to these states. In [14], bounds on rewards and absorption times for large (which may be infinite) Markov chains by censoring Markov chains and stochastic comparison techniques have been derived. We study in this paper discrete-time model checking formulas by bounds derived by censoring. Thus we can reduce substantially the complexity of the model checking procedure. If we can not decide with the computed bounds, then we can refine the bounds by considering a larger set of states.

The remaining of the paper is organised as follows: In section 2, we briefly describe censored Markov chains, the bounds on performability measures and the algorithms to derive these bounds. We present the model checking of DTMCs in section 3. Section 4 is devoted to the proposed methodology to check formulas using censoring techniques and stochastic comparison (summarized in the appendix). Finally in section 5 we give some numerical results to illustrate the proposed methodology.

II. Censoring Markov chains

In this section we first recall the definition of censoring Markov chains. We then present the bounds on the performability measures that we can derive by using this technique. Some of these bounds are derived by combining censoring and stochastic comparison techniques (see appendix). We then briefly present the bounding algorithms.

A. Definition

Consider a discrete-time Markov chain (DTMC) $\{\mathcal{X}_t : t = 1, 2, \ldots\}$ with finite state space S. Suppose that $S = E \cup E^c$, $E \cap E^c = \emptyset$. Suppose that the successive visits of $\mathcal{X}_t$ to E take place at time epochs $0 < t_1 < t_2 < \ldots <$. Then the chain $\{\mathcal{X}_u^E = \mathcal{X}_{t_u}, u = 1, 2, \ldots\}$ is called the censored process (or chain) with censoring set E [21].

Lemma 1 (Theorem 2 in [21]): Let Q be the transition probability matrix of a DTMC $\mathcal{X}_t$. Consider a partition of the finite state space $\mathcal{S}$ into two subsets E and E^c.

$$Q = \begin{pmatrix} Q_E & Q_{EE^c} \\ Q_{E^cE} & Q_{E^c} \end{pmatrix} \begin{matrix} E \\ E^c \end{matrix}$$

Then, the censored process $\mathcal{X}_t^E$ is a Markov chain and its transition probability matrix is given by:

$$S_E = Q_E + Q_{EE^c} \left(\sum_{i=0}^{\infty} (Q_{E^c})^i \right) Q_{E^cE} \tag{1}$$

If Q is irreducible, with steady-state distribution $\pi_Q = (\pi_E, \pi_{E^c})$ then the steady-state distribution π_{S_E} of the censored matrix S_E are given by:

$$\pi_{S_E} = \frac{\pi_E}{\sum_{i \in E} \pi_E(i)} \tag{2}$$

Let us mention that the π_{S_E} represents the conditional probability distribution to be in E. Assume that (Q_{E^c}) does not contain any recurrent class, the fundamental matrix [19] is $\sum_{i=0}^{\infty} (Q_{E^c})^i = (I - Q_{E^c})^{-1}$. When the chain is ergodic there are strong relations with the theory of stochastic complement [16]. Note that it is not necessary for censored Markov chains to be ergodic and we can study for instance the absorbing time. In many problems Q can be large and therefore it is difficult to compute $(I - Q_{E^c})^{-1}$ to finally get S_E. Deriving bounds of S_E from Q_E and some information on the other blocks without computing S_E is therefore interesting idea.

B. Bounding performability measures by censoring techniques

In this subsection, by applying stochastic comparison techniques (see appendix) we derive monotone bounding chains to the censored Markov chain. First we state the bounds on performance measures that we can deduce from these bounding chains. In section IV we show how these bounds may be applied to provide model checking of DTMCs.

First we give the following proposition which states that the steady-state probability in a state $i \in E$ of the original chain is less or equal to the steady-state probability in the censored chain.

Proposition 1 (Upper bounds on steady-state probabilities): Let $\pi_E(i)$ (resp. $\pi_{S_E}(i)$) the steady-state probability in state $i \in E$ of the original (resp. censored) chain. It is clear that:

$$\pi_E(i) \leq \pi_{S_E}(i) \quad \forall i \in E$$

Proof:

The upper bounds to $\pi_E(i)$ can be deduced from equation 2. Indeed π_{S_E} is the steady-state distribution for censored states (E), under the condition that the process is in E. The denominator of equation 2 is the sum of probabilities to be in partition E which is less or equal to 1. ■

Assume that we have derived a monotone stochastic matrix S_E^{sup} such that $S_E \preceq_{st} S_E^{sup}$.

Proposition 2 (Sum of steady-state probabilities): Assuming that $E = S' \cup S''$ is the censored subset and that states of S'' are placed at the end of E, then:

$$\sum_{i \in S''} \pi_E(i) \leq \sum_{i \in S''} \pi_{S_E}(i) \leq \sum_{i \in S''} \pi_{S_E^{sup}}(i)$$

Proof: The first part of inequality is obviously derived from proposition 1. Since by construction $S_E \preceq_{st} S_E^{sup}$ and S_E^{sup} is $\preceq_{st}$-monotone we deduce from corollary 1 of appendix that $\pi_{S_E} \preceq_{st} \pi_{S_E^{sup}}$. Therefore we can derive the second part inequality since S'' is placed in the last position (see property 1 of appendix). ■

Proposition 3 (Steady-state rewards): Let $\rho : S \to \mathbb{R}$ be the reward function that assigns to each state $i \in S$ a reward value $\rho(i)$. Assume that $\rho(i) \geq 0$ for all i. Let E be the set of states which has non zero rewards. Assuming that we sort the states in E such that function ρ is non decreasing ($\rho(i) \leq \rho(j)$, if $i \leq j$), then

$$\sum_{i \in E} \rho(i) \pi_E(i) \leq \sum_{i \in E} \rho(i) \pi_{S_E}(i) \leq \sum_{i \in E} \rho(i) \pi_{S_E^{sup}}(i) \tag{3}$$

Proof: The first part is derived from proposition 1 and by the fact that $\rho(i) > 0$. Since states belonging to E are ordered such that function ρ is non decreasing and since $\preceq_{st}$ order is associated to increasing reward functions (see definition 1), we can deduce then the second part of inequality 3. ■

In the following proposition we state the results concerning the absorption probability and the mean time to absorption for censored Markov chains. We omit the proofs because of lack of space, but they can be found in [14].

Proposition 4 (Absorption probability): We consider a chain $\mathcal{X}$ with a finite number of absorbing states. Let $\mathcal{Y}$ be the censored chain, such that all absorbing states and the states which immediately precede absorbing states are in E. Moreover we assume that the initial state is in E.

1) Obviously, the sum of absorption probabilities is 1 in both chains. Moreover the absorbing probabilities in each absorbing state are the same in both chains.
2) Let $M_{\mathcal{X}}[i, j]$ (resp. $M_{\mathcal{Y}}[i, j]$) be the mean number of passages in j before absorption knowing that the initial state is i for chain $\mathcal{X}$ (resp. $\mathcal{Y}$), then:

$$M_{\mathcal{X}}[i, j] = M_{\mathcal{Y}}[i, j] \text{ if } j \in E$$

Proposition 5 (Absorption time): Let $T_{\mathcal{X}}[i]$ (resp. $T_{\mathcal{Y}}[i]$) be the random variable denoting the absorption time in chain $\mathcal{X}$ (resp. $\mathcal{Y}$), i is the initial state. The mean absorption time in chain $\mathcal{Y}$ is less or equal than the mean absorption time in chain $\mathcal{X}$:

$$\mathbf{E}(T_{\mathcal{Y}}[i]) \leq \mathbf{E}(T_{\mathcal{X}}[i]) \tag{4}$$

Proof: The mean absorption time is indeed the mean number of passages in non absorbing states. Then for the censored chain, $\mathbf{E}(T_{\mathcal{Y}}[i]) = \sum_{j \in E} M_{\mathcal{Y}}[i, j]$. This inequality 4 follows from the fact that the mean number of passages are

the same in both chains for states E and in the original chain there are other non absorbing states which are not in E:

$\mathbf{E}(T_{\mathcal{X}}[i]) = \sum_{j \in E \cup E^c} M_{\mathcal{X}}[i,j]$
$= \mathbf{E}(T_{\mathcal{Y}}[i]) + \sum_{j \in E^c} M_{\mathcal{X}}[i,j] \geq \mathbf{E}(T_{\mathcal{Y}}[i])$ ■

Proposition 6 (Bounds to absorption probability and time): Let $\mathcal{Z}$ be an $\preceq_{st}$ monotone upper bounding chain to the censored chain $\mathcal{Y}$. Assume that both chains ($\mathcal{Y}$ and $\mathcal{Z}$) have an absorbing state k placed at the end of E.

1) Let $\pi_{\mathcal{Y}}[i,k]$ (resp. $\pi_{\mathcal{Z}}[i,k]$) the absorption probability in k for chain $\mathcal{Y}$ (resp. $\mathcal{Z}$) when initial state is i, then:

$$\pi_{\mathcal{Y}}[i,k] \leq \pi_{\mathcal{Z}}[i,k]$$

2) Let $T_{\mathcal{Y}}[i]$ (resp. $T_{\mathcal{Z}}[i]$) be the random variable denoting the absorption time in chain $\mathcal{Y}$ (resp. $\mathcal{Z}$) where i is the initial state, then:

$$T_{\mathcal{Z}}[i] \preceq_{st} T_{\mathcal{Y}}[i] \text{ and } \mathbf{E}(T_{\mathcal{Z}}[i]) \leq \mathbf{E}(T_{\mathcal{Y}}[i])$$

Notice that the $\preceq_{st}$ comparison of random variables $T_{\mathcal{Y}}[i]$ and $T_{\mathcal{Z}}[i]$ is defined on dates that $\in \mathbb{N}$ and not on states.

Proof: Let $\pi_{\mathcal{Y}}[i]$ (resp. $\pi_{\mathcal{Z}}[i]$) the steady-state distribution of the chain $\mathcal{Y}$ (resp. $\mathcal{Z}$). We note that $\pi_{\mathcal{Y}}[i]$ and $\pi_{\mathcal{Z}}[i]$ depends of the initial state i because both chains $\mathcal{Y}$ and $\mathcal{Z}$ are reducible. Since by construction $\mathcal{Y} \preceq_{st} \mathcal{Z}$ and $\mathcal{Z}$ is $\preceq_{st}$ monotone we can deduce from corollary 1 that $\pi_{\mathcal{Y}}[i] \preceq_{st} \pi_{\mathcal{Z}}[i]$. Moreover, absorbing state k is placed at the end of E we can deduce then from property 1 that $\pi_{\mathcal{Y}}[i,k] \leq \pi_{\mathcal{Z}}[i,k]$.

In proposition 2.9 of [5], it has been shown that if the absorbing state is placed at the end then $T_{\mathcal{Z}}[i] \preceq_{st} T_{\mathcal{Y}}[i]$. Therefore $\mathbf{E}(T_{\mathcal{Z}}[i]) \leq \mathbf{E}(T_{\mathcal{Y}}[i])$ can be derived (see definition 1). Let us remark here that by considering the sub-stochastic matrix restricted to non absorbing states, and by applying the definitions of stochastic monotonicity and comparison extended to sub-stochastic cases [12] we can also prove this property.

■

Now, we will present algorithms developed to construct bounds for censored Markov chain.

C. Algorithms

Several methods have been proposed to derive bounds on S_E. The main idea is to take the probability transition matrix restricted to censored states and bound the second part of equation 1 in the sense of $\preceq_{st}$ order. Then by making the bounding matrix $\preceq_{st}$ monotone, we can derive bounds on transient and the steady-state distributions of S_E. The worst-case in the sense of $\preceq_{st}$ is reached when all the returns from E_c to E occur to the last state. In [20], Truffet has proposed a bounding method that consists in the following two steps: first add the slack probability in the last column of Q_E to make it stochastic and then apply Vincent's algorithm [1] to obtain a monotone upper bound $T(Q_E)$ to S_E. Let us denote by T(L) the stochastic monotone matrix obtained when we apply Truffet's method on a sub-stochastic matrix L.

In [14], we have developed a new approach based on the computation of element-wise lower bounds to S_E that provide a more accurate bound than the bound given by Truffet's method. It consists on the determination of an element-wise lower bounds to S_E that is better than Q_E by exploring some paths that return to partition E passing through partition E^c. Assume that this element-wise lower bounds to S_E is L such that $Q_E \preceq_{el} L \preceq_{el} S_E$. By applying Truffet's method to L we obtain a better stochastic monotone bound $T(L)$ than $T(Q_E)$: $S_E \preceq_{st} T(L) \preceq_{st} T(Q_E)$.

In [10], we have proposed an algebraic algorithm based on blocks Q_E and Q_{EE^c}. By dispatching the slack probabilities more precisely than Truffet's method using the block matrix Q_{EE^c} we derive a stochastic bound to S_E that is more accurate than $T(Q_E)$. Moreover that if Q_{EE^c} is rank 1, the proposed algorithm gives the exact matrix S_E.

These algorithms for constructing bounding stochastic monotone matrices to S_E presented above have been assembled in a tool named $\mathcal{CUT}$ [15].

Let us remark that due to the monotonicity constraints, the ordering of states has an impact on the accuracy of bounds. Obviously, the results are more accurate if we consider an order implying a small number of matrix entry modifications due to the monotonicity constraints.

III. Model checking of Discrete Time Markov Chains

The underlying system is modeled by a labeled, finite, ergodic (irreducible, aperiodic, positive recurrent) discrete-time Markov chain $\mathcal{M} = (S, P, L)$ where S is a finite set of states, $P : S \times S \to [0,1]$ is the transition matrix and $L : S \to 2^{AP}$ is the labeling function which assigns to each state s, the set $L(s)$ of atomic propositions valid in s. AP denotes the finite set of atomic propositions. An execution of $\mathcal{M}$ is represented by a path that can be finite or infinite. An infinite path σ is a sequence of states $s_0 s_1 s_2 \cdots$ with $s_i \in S$ and $P(s_i, s_{i+1}) > 0, \forall i$.

For Markov chains, there are two types of state probabilities: transient probabilities where the system is considered at time n. Let $\pi(s, s', n)$ be the probability that the system is in state s' within n steps given the system starts in state s. The steady-state probabilities are the long-run probabilities where the system reaches an equilibrium: $\pi(s, s') = lim_{n \to \infty} \pi(s, s', n)$ is the steady-state probability of state s'. For ergodic DTMC, $\pi(s, s')$ exists and is independent of the initial state s and that will be noted by $\pi(s')$.

We present in the following subsection, the considered formulas by giving their syntax and semantics.

A. Considered formulas

Let $p \in [0,1]$ a probability threshold, $r \in \mathbb{R}$ a real value and $n \in \mathbb{N}$ a natural number. Let $\lhd \in \{\leq, >, \geq, >\}$ a comparison operator. In the sequel, we denote by ϕ-states or S_ϕ the set of states that satisfy ϕ and by $\models$ the satisfaction relation. We consider the following formulas:

$$\phi ::= \mathcal{L}_{\lhd p}(\phi) \mid \mathcal{E}_{\lhd r}(\phi) \mid \mathcal{P}_{\lhd p}(\phi U \phi) \mid \mathcal{P}_{\lhd p}(\phi U^{\leq n} \phi) \mid \mathcal{D}_{\lhd r}(\phi)$$

Now we give the semantic of each operator.

1) Long-run average operator $\mathcal{L}_{\lhd p}(\phi)$: the long-run average operator $\mathcal{L}_{\lhd p}(\phi)$ was defined in [3] to enrich PCTL [13] which is an extension of CTL [7] with probabilistic operators to specify performability measures over discrete-time Markov chains. The state formula $\mathcal{L}_{\lhd p}(\phi)$ asserts that the long-run average fraction of time spent in S_ϕ states meets the bound $\lhd p$. Let π (if it exists) the steady-state distribution of the considered Markov chain $\mathcal{M}$.

$$\mathcal{L}_{\lhd p}(\phi) \text{ is satisfied iff } \sum_{s' \models \phi} \pi(s') \lhd p \tag{5}$$

Let us just remark that:

$$\mathcal{L}_{\leq p}(\phi) = \mathcal{L}_{>1-p}(\neg\phi) \tag{6}$$

In the next section we will present our verification approach based on constructing bounds to the censored Markov chain. The remark given in equation 6 let us to consider only upper bound case whatever $\lhd \in \{\leq, <, \geq, >\}$.

2) Long-run reward rate operator $\mathcal{E}_{\lhd r}(\phi)$: This formula expresses the long run expected reward per unit-time for ϕ-states. It is a state formula of PRCTL [3] that is an extension of PCTL allows to specify constraints over reward measures. Let $\rho : S \to \mathbb{R}_{\geq 0}$ be the reward function that assign to each state $s \in S$ a reward value $\rho(s) \in \mathbb{R}_{\geq 0}$. The state formula $\mathcal{E}_{\lhd r}(\phi)$ holds if the long-run expected reward rate per time-unit for ϕ-states meets the bounds of $\lhd r$. If the steady-state exists, $\mathcal{E}_{\lhd r}(\phi)$ is satisfied if:

$$\mathcal{E}_{\lhd r}(\phi) \text{ is satisfied iff } \sum_{s' \models \phi} \pi(s')\rho(s') \lhd r \tag{7}$$

3) Bounded until operator $\mathcal{P}_{\lhd p}(\phi_1 U^{\leq n} \phi_2)$: This path formula of PCTL asserts that the probability measure of path satisfying $\phi_1 U^{\leq n} \phi_2$ meets the bound given by $\lhd p$. Whereas, the path formula $\phi_1 U^{\leq n} \phi_2$ asserts that the state formula ϕ_2 will be satisfied at some time $k \leq n$ and that at all preceding time ϕ_1 holds. Let s be the initial state, then:

$$s \models \mathcal{P}_{\lhd p}(\phi_1 U^{\leq n} \phi_2) \text{ iff } Prob(s, \phi_1 U^{\leq n} \phi_2) \lhd p \tag{8}$$

Where $Prob(s, \phi_1 U^{\leq n} \phi_2)$ denotes the probability measure of all paths σ starting from s and satisfying $\phi_1 U^{\leq n} \phi_2$. In [11], authors show that computation of $Prob(s, \phi_1 U^{\leq n} \phi_2)$ requires the computation of the transient distribution in a modified Markov chain $\mathcal{M}'$. This chain is deduced from $\mathcal{M}$ by making absorbing states that satisfy $\neg\phi_1 \vee \phi_2$. Let $\pi_{\mathcal{M}'}(s, s', n)$ be the transient probability in state s' at time n of the chain $\mathcal{M}'$ when the initial state is s, then $Prob(s, \phi_1 U^{\leq n} \phi_2)$ is defined as (see proposition 1 in [11]):

$$Prob(s, \phi_1 U^{\leq n} \phi_2) = \sum_{s' \in S_{\phi_2}} \pi_{\mathcal{M}'}(s, s', n)$$

Let us remark that $\sum_{s' \in S_{\phi_2}} \pi_{\mathcal{M}'}(s, s', n)$ represents the absorption probabilities of ϕ_2-states at time n of the absorbing Markov chain $\mathcal{M}'$ when s is the initial state. Therefore the verification of the bounded until operator is reduced to the computation of the absorption probabilities at time n of ϕ_2-states in the Markov chain $\mathcal{M}'$.

4) Unbounded until operator $\mathcal{P}_{\lhd p}(\phi_1 U \phi_2)$: The standard unbounded until operator $\mathcal{P}_{\lhd p}(\phi_1 U \phi_2)$ is obtained by taking n equal to ∞ in the bounded until formula:

$$\mathcal{P}_{\lhd p}(\phi_1 U \phi_2) = \mathcal{P}_{\lhd p}(\phi_1 U^{\leq \infty} \phi_2)$$

Similarly, the verification of the unbounded operator requires the computation of $Prob(s, \phi_1 U \phi_2)$ that is equal to the absorption probability of ϕ_2-states in the chain $\mathcal{M}'$. Let $\pi_{\mathcal{M}'}(s, s') = lim_{n \to \infty} \pi_{\mathcal{M}'}(s, s', n)$ be the steady-state probability of state s', then:

$$Prob(s, \phi_1 U \phi_2) = \sum_{s' \in S_{\phi_2}} \pi_{\mathcal{M}'}(s, s') \tag{9}$$

5) Mean first passage time $\mathcal{D}_{\lhd r}(\phi)$: This operator was studied by de Alfaro in [2] and Andova et al. in [3]. Let s be an initial state, $\mathcal{D}_{\lhd r}(\phi)$ holds in s if the mean time to reach ϕ states in Markov chain $\mathcal{M}$ meets the bound $\lhd r$.

By making ϕ-states absorbing, the verification of $\mathcal{D}_{\lhd r}(\phi)$ is reduced to the computation of the mean absorption time of the obtained chain $\mathcal{M}a$, when the initial state is s:

$$s \models \mathcal{D}_{\lhd r}(\phi) \text{ iff } \mathbf{E}(T_{\mathcal{M}a}[s]) \lhd r \tag{10}$$

IV. Proposed verification approach

In this section, we will explain the proposed approach based on stochastic comparison and censoring techniques to check the formulas presented previously. First we present different steps of the verification procedure in an abstract way. These steps must be precised depending on the underlying formula.

Step 1: Defining the censored state space such E such that E contains S_ϕ states.
Step 2: Reordering of the state space. This is necessary in order to provide probability inequalities from the stochastic comparison relations.
Step 3: Constructing of bounding models.
Step 4: Computing bounds on the considered measures.
Step 5: Checking the formula by means of bounds.

In the first step we define the partition of the state space. Recall that, depending on the formula that we check, we are interested in evaluating a performance measure on states of S_ϕ. Thus we have to put states of S_ϕ in the watched subset E. We include other states in E, obviously if we have more states in this set, the bounds are more accurate. Thus the determination of E is a tradeoff between the complexity and the accuracy of bounds.

After the determination of E we have to reorder this subset. Indeed we put always S_ϕ in the last rank to deduce inequalities to S_ϕ probabilities (see proposition 2) or to S_ϕ increasing reward measures (see proposition 3). Once the censored subset E is defined and states are ordered, we construct bounding chains to the censored Markov chain by using one of the algorithms presented in subsection II-C. Then by analyzing the bounding chain, that has a reduced size (number of states in E) comparing to the size of the original chain (the whole state space S), and depending of the formula that we check we deduce bounds on the exact measure.

The last step consists in comparing the obtained bound with the threshold given by $\lhd p$ or $\lhd r$. Suppose that the given threshold is $\leq p$ and that the obtained upper bound is b^{sup}.

- if $b^{sup} \leq p$ then we can conclude that the considered formula is satisfied.
- else we can not conclude and therefore the obtained bound must be refined. To do this we can increase the size of E by including other states. The second possibility is to modify the order of states belonging to E with respecting the assumptions given form each formula. Indeed, the accuracy of bounds depends on the effect of monotonicity constraint that we impose to the bounding chain.

Now we give further details on the verification of each operator.

A. Checking $\mathcal{L}_{\lhd p}(\phi)$

Recall that the verification of this operator requires the computation of the steady-state probabilities of ϕ-states, if they exist, (see equation 5). If $\lhd \in \{<, \leq\}$ then we put in E, ϕ-states and other states of S (i.e. $E = S' \cup S_\phi, S' \subseteq S$.) Obviously, the bounds are more accurate if we have a larger S' set. We order states of E by putting S_ϕ at the end. Then we construct an upper bounding matrix to S_E, that we denote by S_E^{sup}, using proposed algorithms. By taking $S'' = S_\phi$ in proposition 2 we have the following steady-state probability bounds for ϕ-states:

$$\sum_{s \in S_\phi} \pi(s) \leq \sum_{s \in S_\phi} \pi_{S_E^{sup}}(s)$$

Therefore, if $\sum_{s \in S_\phi} \pi_{S_E^{sup}}(s) \leq p$, we can conclude that the formula is satisfied else the bound must be refined by taking into account more states (increasing the size of S' set).

Let us mention that if $\lhd = \geq$ we have just to verify the formula $\mathcal{L}_{<1-p}(\neg\phi)$ by the same approach presented above (see equality 6).

B. Checking $\mathcal{E}_{\lhd r}(\phi)$

The verification of this operator is similar to the previous case. It requires the computation of the steady-state reward measure of ϕ-states (see equation 7). We put in E states belonging to S_ϕ then we reorder ϕ-states according to their increasing reward values. In the case of this operator, we will only consider the case when $\lhd \in \{\leq, <\}$ because we can only obtain an upper bound to the exact steady-state reward measure of ϕ-states (see equation 3). Hence, we construct an upper bound matrix to S_E to derive bounds on the reward rates and conclude that the formula is satisfied if this bound meets the threshold.

C. Checking $\mathcal{P}_{\lhd p}(\phi_1 U \phi_2)$

The verification of this operator requires the computation of absorption probability of ϕ_2-states in the modified Markov chain $\mathcal{M}'$ (see equation 9). Let us denote by S' the set of states that precede immediately absorbing states ($S_{\neg\phi_1 \vee \phi_2}$). We must put in the censored state set (E) all absorbing states ($S_{\neg\phi_1 \vee \phi_2}$), S' and the initial state s. Since we are interested in the absorption probability of ϕ_2-states, we aggregate S_{ϕ_2} to one macro-state θ_{ϕ_2}. Recall that under these assumptions the absorption probability of θ_{ϕ_2} in $\mathcal{M}'$ ($\pi_{\mathcal{M}'}[s, \theta_{\phi_2}]$) and in its censored chain $\mathcal{M}'_E$ ($\pi_{\mathcal{M}'_E}[s, \theta_{\phi_2}]$) are the same (see proposition 4). So, by deriving bounds to $\pi_{\mathcal{M}'_E}[s, \theta_{\phi_2}]$, we derive bounds to $\pi_{\mathcal{M}'}[s, \theta_{\phi_2}]$. This allows us the possibility to consider the lower bound comparison operators $\lhd \in \{\leq, <\}$ and the upper bound comparison operators $\lhd \in \{\geq, >\}$. The only difference between the two cases is that if $\lhd \in \{\leq, <\}$ we put θ_{ϕ_2} at the end of E to derive upper bound to $\pi_{\mathcal{M}'_E}[s, \theta_{\phi_2}]$ (see equation 11 of appendix) however if $\lhd \in \{\geq, >\}$ we place θ_{ϕ_2} at the beginning of E to obtain a lower bound to $\pi_{\mathcal{M}'_E}[s, \theta_{\phi_2}]$ (see equation 12 of appendix). Then we construct an upper bounding chain to $\mathcal{M}'_E$ that we denote by $\mathcal{M}'^{sup}_E$. Let $\pi_{\mathcal{M}'^{sup}_E}[s, \theta_{\phi_2}]$ be the absorption probability of θ_{ϕ_2} in $\mathcal{M}'^{sup}_E$, we can deduce from proposition 4 and 6 that:

- If θ_{ϕ_2} is placed at the end of E then:

  $$\pi_{\mathcal{M}'}[s, \theta_{\phi_2}] = \pi_{\mathcal{M}'_E}[s, \theta_{\phi_2}] \leq \pi_{\mathcal{M}'^{sup}_E}[s, \theta_{\phi_2}]$$

  Then we compare the obtained bound $\pi_{\mathcal{M}'^{sup}_E}[s, \theta_{\phi_2}]$ to $\lhd p$, $\lhd \in \{\leq, <\}$.
- If θ_{ϕ_2} is placed at the beginning of E then:

  $$\pi_{\mathcal{M}'}[s, \theta_{\phi_2}] = \pi_{\mathcal{M}'_E}[s, \theta_{\phi_2}] \geq \pi_{\mathcal{M}'^{sup}_E}[s, \theta_{\phi_2}]$$

  We check then if $\pi_{\mathcal{M}'^{sup}_E}[s, \theta_{\phi_2}]$ meets the threshold $\lhd p$, $\lhd \in \{\geq, >\}$.

D. Checking $\mathcal{D}_{\lhd r}(\phi)$

The verification of this operator requires the computation of the mean absorption time of $\mathcal{M}a$ obtained from the considered chain $\mathcal{M}$ by making absorbing states that belong to S_ϕ (see equation 10). To check this operator with the proposed approach we must put in E, states belonging to S_ϕ and states that precede immediately S_ϕ and the initial state s. Obviously, we include other states in this set by considering the tradeoff between the accuracy and the complexity. We aggregate S_ϕ to one macro-state that we put it at the end of E. Then we construct an upper bounding chain to the censored chain $\mathcal{M}a_E$ that we denote by $\mathcal{M}a_E^{sup}$. We derive after that the mean absorption time of $\mathcal{M}a_E^{sup}$ that is a lower bound to the mean absorption time of $\mathcal{M}a$ (see proposition 5 and 6):

$$\mathbf{E}(T_{\mathcal{M}a_E^{sup}}[s]) \leq \mathbf{E}(T_{\mathcal{M}a}[s])$$

where $T_{\mathcal{M}a_E^{sup}}[s]$ (resp. $T_{\mathcal{M}a}[s]$) is the random variable denoting absorption time when the initial state is s in the chain $\mathcal{M}a_E^{sup}$ (resp. $\mathcal{M}a$).

To conclude we have to check if $\mathbf{E}(T_{\mathcal{M}a_E^{sup}}[s])$ meets the threshold $\lhd r$, $\lhd \in \{\geq, >\}$. We note that for this operator we consider only the case when $\lhd \in \{\geq, >\}$ because we can derive only a lower bound to the mean time absorption of $\mathcal{M}a$.

E. Checking $\mathcal{P}_{\lhd p}(\phi_1 U^{\leq n} \phi_2)$

The verification of this formula requires the transient analysis of the underlying chain. However the time evolution is not the same in the original and the censored chain. Recall that the censored process is observed at time epochs when the chain is visiting states of E. Therefore the probability transition matrix given by equation 1 and the bounds on it do not let us to derive transient bounds and to check time bounded until formula.

In [8], the authors considered the model checking of Generalized Stochastic Petri Nets (GSPN) which is the extension of Stochastic Petri Nets (SPN) with immediate transitions (vanishing states). By defining E as normal states and E^c as vanishing states, the probability transition matrix given by equation 1 is the underlying chain for these models. Therefore the proposed bounds on the censored chains can be applied to provide model checking of these models including time bounded formula.

V. Numerical examples

In this section we present numerical results obtained by applying the proposed methodology for an example of repairable system. The considered example can have more than 10^7 reachable states and more than 10^8 non zero transitions (see table I). We consider a system that contains N resources that can be operational or faulty. There are two failure modes: soft and hard that we denote respectively by s and h. We consider that the fault arrival of errors (hard and soft) is a batch process with maximum size G. In this example we take $G = 1$. We denote by p^a_{si} (resp. p^a_{hi}) the probability that i soft (resp. hard) errors happen in the system in a time slot and by p^r_{si} (resp. p^r_{hi}) the probability that i soft (resp. hard) errors are repaired during a time slot. At the end of a slot, it is assumed that first the end of reparation takes place and then the arrival of errors is considered.

The considered system can be modelled by a discrete-time Markov chain with state space $S = \{(f_s, f_h), f_s + f_h \leq N\}$, where f_s (resp. f_h) represents the number of faulty resources caused by soft (resp. hard) error. The size of the underlying DTMC is $\frac{(N+1)(N+2)}{2}$. We associate to each state s of the chain a set a atomic propositions that characterize the state and which are verified by the state. We assign to state $(0, 0)$ which is the state when the system has N resources operational, the atomic proposition up. Moreover we assign to states when there is no soft (resp. hard) errors in the system the atomic proposition $(f_s = 0)$ (resp. $(f_h = 0)$) and we assign to states when there is one (resp. two) hard errors in the system the atomic proposition $(f_h = 1)$ (resp. $(f_h = 2)$).

In this example we give results for checking unbounded until formula (see table II), steady-state formula (see table III) and mean first passage time formula (see table IV) using censoring techniques and stochastic comparison. We present in table I the size of the exact chain and the censored chain that we have considered in the verification of these formulas. We give in column $Size$ the state space size and in column $Entries$ the number of non null entries of the exact and the bounding chain. We also report computation time (in $second$) in column $Time$ needed to obtain the exact and bounding measure. We can see clearly that computation times are drastically reduced using the proposed bounding approach which also provide results when the exact analysis fails ($N = 10000$).

	Exact Markov chain			Bounding Markov chain		
N	Size(S)	Entries	Time	Size(E)	Entries	Time
100	5151	45351	0.27	202	1298	0.06
500	125751	1126751	23.46	1002	6498	2.21
1000	501501	4503501	154.46	2002	12998	4.36
10000	50015001	-	-	20002	129998	55.05

TABLE I

Comparison of original and bounding model sizes

In table II we present results obtained for the verification of the unbounded until formula $\mathcal{P}_{\geq 0.7}(\neg(f_h = 0)\ \mathcal{U}\ up)$ and $\mathcal{P}_{\leq 0.3}(\neg up\ \mathcal{U}\ (f_h = 0))$. By making absorbing states that verify $(f_h = 0) \vee up$ we compute a lower bound (resp. upper bound) to the absorption probability of states up (resp. $(f_h = 0)$) to check the formula $\mathcal{P}_{\geq 0.7}(\neg(f_h = 0)\ \mathcal{U}\ up)$ (resp. $\mathcal{P}_{\leq 0.3}(\neg up\ \mathcal{U}\ (f_h = 0))$). For both formulas we suppose that we start from state $(0, 1)$.

In table III we give results for checking steady-state formula. We can observe that if the bound is not very accurate we can not conclude through the bound (see symbol ?).

In table IV we give results for checking mean time operator $\mathcal{D}_{\geq 10^2}(up)$. By making up-state absorbing we compute a lower bound to the mean first passage time before absorption. We suppose that we start from the initial state $(N, 0)$.

We note that numerical results are computed in an Intel Pentium 4 with CPU 2.8 GHz and 1.5GBytes memory and that probabilities $p^a_{s0} = p^a_{h0} = 0.8$, $p^a_{s1} = p^a_{h1} = 0.2$, $p^r_{s0} = p^r_{h0} = 0.1$ and $p^r_{s1} = p^r_{h1} = 0.9$.

VI. Conclusion

In this paper we show how we can combine stochastic bounding techniques with censoring Markov chains techniques to check formulas under discrete-time Markov chain. Thus the proposed approach lets us to reduce substantially the complexity of the model checking and to consider the model

Formulas	N	Exact prob.	Bound prob.	Is it satisfied?
$\mathcal{P}_{\geq 0.7}(\neg(f_h = 0)\ \mathcal{U}\ up)$	1000	$7.95\ 10^{-1}$	$7.3\ 10^{-1}$	yes
	10000	-	$7.01\ 10^{-1}$	yes
$\mathcal{P}_{\leq 0.3}(\neg up\ \mathcal{U}\ (f_h = 0))$	1000	$2.04\ 10^{-1}$	$2.69\ 10^{-1}$	yes
	10000	-	$2.99\ 10^{-1}$	yes

TABLE II

Checking unbounded until formula

Formulas	N	Exact prob.	Upper bound prob.	Is it satisfied?
$\mathcal{L}_{\leq 0.2}((f_s = 0) \wedge (f_h = 1))$	1000	$1.60\ 10^{-1}$	$1.98\ 10^{-1}$	yes
$\mathcal{L}_{\leq 0.1}((f_s = 0) \wedge (f_h = 2))$	1000	$0.40\ 10^{-3}$	$2.08\ 10^{-1}$	?

TABLE III

Checking steady state formula

N	Exact time(second)	bound time (second)	Is it satisfied?
100	$2.19\ 10^3$	$1.58\ 10^2$	yes
500	$6.62\ 10^3$	$5.07\ 10^2$	yes
1000	$9.06\ 10^3$	$9.07\ 10^2$	yes
10000	-	$7.52\ 10^3$	yes

TABLE IV

CHECKING MEAN FIRST PASSAGE TIME FORMULA $\mathcal{D}_{\geq 10^2}(up)$

checking of numerically intractable models. The extension of this approach to infinite size cases are under study.

REFERENCES

[1] O. Abu-Amsha and J.M. Vincent. An algorithm to bound functionals of Markov chains with large state space. *4th INFORMS*, Boca Raton, Florida, (1998).

[2] L.d. Alfaro. Temporal logics for the specification of performance and reliability. *STACS*, volume 1200 of *LNCS*, pages 165-176, (1997).

[3] S. Andova, H. Hermanns and J.P. Katoen. Disrete-time rewards model-checked. In Formal Modelling and Analysis of Timed Systems (*FORMATS*), pages 88-104, (2003).

[4] A. Aziz, K. Sanwal, V. Singhal and R. Brayton. Model checking continuous time Markov chains. *ACM Trans. on Comp. Logic*, 1(1), pages 162-170, (2000).

[5] M. Benmammoun, A. Busic, J.M. Fourneau and N. Pekergin. Increasing convex monotone Markov chains: theory, algorithms and applications. *MAM*, pages 189-210, (2006).

[6] M. Benmamoun, N. Pekergin and S. Younès. Model Checking of Continuous-Time Markov Chains by Closed-Form Bounding Distributions. *QEST*, pages 189-198, (2006).

[7] E.M. Clarke, A. Emerson and A.P. Sistla. Automatic verification of finite-state concurrent systems using temporal logic specifications. *ACM Trans. on Programming Languages and Systems*, pages 244-263, (1986).

[8] D. Cerotti, S. Donatelli, A. Horvath and J. Sproston. CSL Model Checking for Generalized Stochastic Petri Nets. *QEST*, pages 199-210, (2006).

[9] P.R. D'Argenio, B. Jeannet, H.E Jensen and K.G Larsen. Reduction and Refinement Strategies for Probabilistic Analysis. *PAPMPMV*, pages 57-76, (2001).

[10] T. Dayar, N. Pekergin and S. Younès. Conditional Steady-State Bounds for a Subset of States in Markov Chains. *SMCTools*, pages 3-10, (2006).

[11] J.P. Katoen, M. Kwiatkowska, G. Norman and D. Parker. Faster and Symbolic CTMC Model Checking. *PAPM-PROBMIV*, pages 23-38, (2001).

[12] S. Haddad and P. Moreaux. Sub-stochastic matrix analysis for bounds computation-Theoretical results. *European Journal of Operational Research*, pages 999-1015, (2007).

[13] H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing*, pages 512-535, (1994).

[14] J.M. Fourneau, N. Pekergin and S. Younès. Censoring Markov Chains and Stochastic Bounds. *EPEW*, pages 213-227, (2007).

[15] J.M. Fourneau, N. Pekergin and S. Younès. CUT: Combining stochastic ordering and censoring to bound steady-state rewards and first passage time. *QEST tools*, pages 211-212, (2007).

[16] C.D. Meyer. Stochastic complementation, uncoupling Markov chains, and the theory of nearly reducible systems. *SIAM Review*, Volume 31, pages 240-272, (1989).

[17] A. Muller and D. Stoyan. Comparison Methods for Stochastic Models and Risks. Wiley, New York, 2002.

[18] N. Pekergin and S. Younès. Stochastic Model Checking with Stochastic Comparison. *EPEW*, pages 109-123, (2005).

[19] K.S Trivedi. Probability and Statistic with Reliability, Queueing and Computer Science Applications. Second Edition, Wiley, 2002.

[20] L. Truffet. Near Complete Decomposability: Bounding the error by a Stochastic Comparison Method. *Journal of Applied Probability*, Volume 29, pages 830-855, (1997).

[21] Y.Q. Zhao and D. Liu. The Censored Markov chain and the Best Augmentation. *Journal of Applied Probability*, Volume 33, pages 623-629, (1996).

APPENDIX

We present some preliminaries on the stochastic comparison method and we refer to the books [17] for the theoretical issues and different applications of this method.

Definition 1: Let X and Y be random variables taking values on a totally ordered space S. Then X is said to be less than Y in the strong stochastic sense, ($X \preceq_{st} Y$) if and only if $\mathbf{E}[f(X)] \leq \mathbf{E}[f(Y)]$ for all non decreasing functions $f : S \rightarrow R$, whenever the expectations exist.

We give in the next property the $\preceq_{st}$ comparison in the case of finite state space $S = \{1, 2, \cdots, n\}$.

Property 1: Let X, Y be random variables taking values on $\{1, 2, \cdots, n\}$ and p, q be probability vectors which denote respectively distributions of X and Y.

$$X \preceq_{st} Y \text{ iff } \sum_{j=i}^{n} p[j] \leq \sum_{j=i}^{n} q[j] \ \ \forall i = \{n, n-1, \cdots, 1\} \quad (11)$$

$$X \preceq_{st} Y \text{ iff } \sum_{j=1}^{i} p[j] \geq \sum_{j=1}^{i} q[j] \ \ \forall i = \{n, n-1, \cdots, 1\} \quad (12)$$

The stochastic comparison of random variables has been extended to the comparison of Markov chains. It is shown in Theorem 5.2.11 of [17, p.186] that monotonicity and comparability of the probability transition matrices of time-homogeneous Markov chains yield sufficient conditions to compare stochastically the underlying chains. We first define the monotonicity and comparability of stochastic matrices and then state this theorem and some useful corollaries.

Definition 2: Let P be a stochastic matrix. P is said to be stochastically st-monotone if for any probability vectors p and q:

$$p \preceq_{st} q \implies p\ P \preceq_{st} q\ P$$

Theorem 1: Let P (resp. Q) be the probability transition matrix of the time-homogeneous Markov chain $\{\mathcal{X}_t, t \geq 0\}$ (resp. $\{\mathcal{Y}_t, t \geq 0\}$). $\mathcal{X}_t \preceq_{st} \mathcal{Y}_t\ \forall t$ if:

- $\mathcal{X}_0 \preceq_{st} \mathcal{Y}_0$,
- at least one of the probability transition matrices is monotone, that is, either P or Q is monotone,
- the transition matrices are comparable, (i.e. $P \preceq_{st} Q$).

In [1] an algorithm based on this theorem is given to construct an optimal st-monotone upper bounding Markov chain. This algorithms takes an irreducible stochastic matrix P as input and returns as output a st-monotone upper bounding matrix, Q, such that, $P \preceq_{st} Q$. Indeed, the monotonicity and comparability constraints can be given as in equation 13. Note that inequalities are replaced by equalities to construct optimal bounds.

$$\begin{cases} \sum_{k=j}^{n} Q[1,k] & = & \sum_{k=j}^{n} P[1,k] \\ \sum_{k=j}^{n} Q[i+1,k] & = & max(\sum_{k=j}^{n} Q[i,k], \sum_{k=j}^{n} P[i+1,k]) \end{cases} \quad (13)$$

Corollary 1: Let Q be a monotone, upper bounding matrix for P for the st-ordering. If the steady-state distributions (π_P and π_Q) exist, then $\pi_P \preceq_{st} \pi_Q$.