Probabilistic Model Checking of Regenerative Concurrent Systems

Marco Paolieri, András Horváth, and Enrico Vicario, Member, IEEE Computer Society

Abstract—We consider the problem of verifying quantitative reachability properties in stochastic models of concurrent activities with generally distributed durations. Models are specified as stochastic time Petri nets and checked against Boolean combinations of interval until operators imposing bounds on the probability that the marking process will satisfy a goal condition at some time in the interval \([\alpha, \beta]\) after an execution that never violates a safety property. The proposed solution is based on the analysis of regeneration points in model executions: a regeneration is encountered after a discrete event if the future evolution depends only on the current marking and not on its previous history, thus satisfying the Markov property. We analyze systems in which multiple generally distributed timers can be started or stopped independently, but regeneration points are always encountered with probability 1 after a bounded number of discrete events. Leveraging the properties of regeneration points in probability spaces of execution paths, we show that the problem can be reduced to a set of Volterra integral equations, and we provide algorithms to compute their parameters through the enumeration of finite sequences of stochastic state classes encoding the joint probability density function (PDF) of generally distributed timers after each discrete event. The computation of symbolic PDFs is limited to discrete events before the first regeneration, and the repetitive structure of the stochastic process is exploited also before the lower bound \(\alpha\), providing crucial benefits for large time bounds. A case study is presented through the probabilistic formulation of Fischer’s mutual exclusion protocol, a well-known real-time verification benchmark.


1 INTRODUCTION

In the engineering of non-functional requirements, verification of quantitative properties of stochastic models enables early assessment of design choices and provides model-driven guidance for implementation and integration stages. This becomes particularly valuable in the development of systems where the effects of concurrency are intertwined with probabilistic behavior and stochastic durations.

Probabilistic model checking supports a systematic practice through which the same model can be verified against multiple probabilistic properties specified in some well-defined language, and open to automated regression verification when the model evolves. Empirical evidence indicates that most probabilistic requirements occurring in industrial practice can be specified through a limited set of specification patterns [1]. In particular, most transient properties can be reduced to the form of the probabilistic interval until operator, which specifies a bound on the probability that the model will be in a goal state at some time in the interval \([\alpha, \beta]\) after having visited only legal states. A large body of techniques and tools have been developed and demonstrated on industrial case studies following either a statistical [2], [3], [4], [5] or numerical [6], [7], [8], [9] approach.

In particular, numerical probabilistic model checking aims at computing results with high accuracy and confidence through exhaustive state-space analysis [10], often at the expense of a restriction on the class of models amenable to verification.

Most numerical approaches addressed the verification of real-time properties over models of concurrent activities with exponentially distributed (EXP) durations. In this case, due to the memoryless property of the exponential distribution, the underlying stochastic process of the model satisfies the Markov property at each time instant, i.e., the current state provides sufficient information to predict future evolution, regardless of elapsed sojourn times. Efficient algorithms for the analysis of continuous-time Markov chains (CTMCs) can thus be applied to the verification of requirements specified in continuous stochastic logic (CSL), also allowing nesting of temporal operators [11], [12], [13], [9], [14]. Properties specified as deterministic timed automata can also be verified through the analysis of piecewise-deterministic Markov processes resulting from the synchronous composition of the model with a specification automaton [15], [16].

However, for valid modeling of several classes of systems, some durations must be represented as generally distributed (GEN) random variables, i.e., variables that break the limit of memoryless EXPs. Notable examples include aging processes, which structurally depend on GEN variables, or real-time systems, in which correctness depends on firm time bounds resulting from worst-case execution times, minimum intervals between releases, deterministic durations of synchronous periods, timeouts and watchdogs. In this case, the future evolution of the model depends on random timers encoding the remaining time of GEN durations. The underlying stochastic process is no more a CTMC and rather...
belongs to some wider class, which is determined by the persistence of GEN timers after discrete events [17].

If GEN timers cannot persist to any discrete event, the underlying stochastic process is semi-Markov (SMP): the system has “memory” of the sojourn time elapsed in the current state (i.e., its future evolution depends on this continuous variable, in addition to the discrete state), but the Markov property is satisfied immediately after each discrete event. In the terminology of Markov renewal theory [18], the corresponding time instants are called regeneration points and, by a renewal argument [18], each execution path reaching some goal state within time $\beta$ can be decomposed into a prefix that reaches the first regeneration at some time $t \leq \beta$ and an independent suffix that reaches the goal state within the remaining time $\beta - t$. In [19], verification of a probabilistic interval until with $\alpha = 0$ is reduced for SMPs to a first-passage analysis problem by making illegal and goal states absorbing (i.e., disabling any timer in such states). Following a different approach, [20] verifies non-nested until operators on stochastic automata with underlying SMPs by unfolding the set of model behaviors into a tree where nodes impose distinct pairwise orderings on timers. A fragment of the tree is analyzed to compute the probability of reaching each node and to decide a formula with $\alpha \neq 0$, but regenerations are not exploited and complexity is exponential with respect the number of events feasible within $\beta$. As a common limitation of [19] and [20], the SMP assumption that GEN timers are disabled or reset after each discrete event is still a significant hurdle for model validity, as it rules out important design mechanisms such as timeouts that span across multiple activities, or asynchronous components that start their timers independently.

When GEN timers can persist after the occurrence of discrete events, memory of elapsed sojourn times can be carried across multiple states, but regeneration points can still be encountered, delimiting regeneration epochs. If this happens infinitely often with probability 1 (w.p.1), the process is Markov regenerative (MRP) [17], [18]. A large literature has addressed numerical solution for models in the subclass of MRPs that satisfy the so-called enabling restriction, i.e., models where at most a single GEN timer is enabled in each state. In this case, GEN timers cannot overlap their intervals of activity, and bounded reachability can be evaluated through the analysis of CMTCs subordinated to the activity intervals of GEN timers [21], [22], [23]. Nonetheless, the enabling restriction imposes a severe limitation, as it rules out models with multiple concurrent GEN timers (e.g., a timeout over a GEN timer).

When regeneration points are not guaranteed to be reached infinitely often w.p.1, the underlying process belongs to the class of generalized semi-Markov processes (GSMPs) [17], [24], [25], for which very few results of numerical evaluation were developed. Evaluation of (non-nested) probabilistic interval until operators with $\alpha = 0$ was proposed in [26] under the assumption of a bound on the number of discrete events feasible within time $\beta$; the solution is based on the enumeration of a tree of probability density functions (PDFs) of active timers with supports encoded as regions [27]. In [28], the assumption of a bound on the number of events within time $\beta$ is removed and fairly general conditions that guarantee termination in exact or approximate evaluation are provided, through the enumeration of stochastic state classes [29], [30], [31] representing the joint PDF of timers over Difference Bound Matrix zones [32], [33]. While a calculus based on zones largely reduces the branching factor of enumerated trees, the complexity of [26] and [28] grows exponentially with the length of event sequences within time $\beta$, and no computational advantage is gained when the underlying stochastic process falls in the subclass of MRPs.

In this paper, we propose a technique for the verification of non-nested interval until operators in MRPs that always encounter a regeneration point or a conclusive state (i.e., an illegal state, or a goal state reached after $\alpha$, or any state reached after $\beta$) w.p.1 within a bounded number of discrete events. This contribution extends the class of stochastic models amenable to numerical solution by including models that fall in the class of MRPs but do not satisfy the enabling restriction, without bounds on the number of events executed within time $\beta$, and with a major reduction of complexity when the stochastic process has a repetitive structure and multiple regenerations can be traversed before time $\beta$.

In Section 2, we introduce stochastic time Petri nets for the specification of stochastic models. A probability measure on model executions is defined by establishing a formal relation between cylinder sets (i.e., sets of execution paths that follow a common qualitative ordering of events and given timing restrictions) and stochastic state classes. We provide an algorithm for the detection of regeneration points during the enumeration of stochastic state classes; in so doing, we generalize the state of the art in the literature on stochastic Petri nets [17] by encompassing the case of regenerations where all GEN timers have been enabled for a deterministic time (Section 3). Coming to the core result of the work, we then show that the verification of an interval until operator can be reduced to a set of Volterra integral equations of the second kind that extend generalized Markov renewal equations [18] into a bivariate form based on three kernels, and we provide algorithms to compute the kernels through the enumeration of stochastic state classes reachable before the first regeneration (Section 4). We finally illustrate how the approach extends the class of models amenable to numerical solution through the study of a probabilistic formulation of Fischer’s mutual exclusion protocol (Section 5), and draw our conclusions on the verification of regenerative stochastic systems (Section 6).

2 PROBLEM DEFINITION

2.1 Stochastic Time Petri Nets

We specify concurrent systems with stochastic activity durations using stochastic time Petri nets (STPNs) [29], [31]. An STPN is defined by a set of transitions, representing activities with stochastic duration, and a set of places; a marking assigns a natural number of tokens to each place. Places can serve as input or output places of a transition: when the marking assigns at least one token to each input place, the transition is enabled; after its firing, one token is removed from each input place and one token is added to each output place. STPNs have a natural graphical representation illustrated in Fig. 1a: transitions are drawn as bars, places as circles, and tokens as dots inside each place. Directed arcs connect input places to transitions, and transitions to output places.
The color of a transition represents the PDF type of its stochastic duration: white for exponential distributions, gray for deterministic durations, and black for other distributions (as a special case, a thin black bar is used for transitions with zero duration, see Fig. 8). Each transition samples a time to fire when it becomes enabled; as in discrete event systems, the transition with minimum time to fire is the next event and its firing enables, disables, or restarts other events by removing tokens from input places and adding tokens to output ones. Similarly to stochastic reward nets [34] or stochastic activity networks [35], the enabling of a transition can be limited using enabling functions, arbitrary constraints on token counts that are annotated next to the transition, after the symbol \( ? \); update functions of the form \( place \leftarrow expression \) can specify additional updates of the token count of a place after the firing of the transition (see Fig. 8). In the following, we adopt STPNs to specify stochastic systems, although our techniques can be extended to other formalisms after defining a calculus for the computation of times to fire PDFs given a sequence of events (e.g., stochastic timed automata [36]). As a requirement, the underlying stochastic process must encounter regenerations w.p.1 after a bounded number of fired events, and the state space must be finite (e.g., for STPNs, the number of tokens accumulated in each place must be bounded).

### 2.1.1 Syntax

**Definition 1.** An STPN is a tuple

\[
(P, T, A^-, A^+, B, U, EFT, LFT, F, W)
\]

where: \( P \) and \( T \) are disjoint sets of places and transitions; \( A^- \subseteq P \times T \) and \( A^+ \subseteq T \times P \) are the precondition and post-condition relations, respectively; \( B \) and \( U \) associate each transition \( t \in T \) with an enabling function \( B(t) : \mathbb{N}_+ \to \{ \text{true, false} \} \) and with an update function \( U(t) : \mathbb{N}_+ \to \mathbb{N}_+ \).

In addition, for each transition \( t \in T \), the STPN specifies:

- an earliest firing time \( EFT(t) \in \mathbb{Q}_{\geq 0} \), a latest firing time \( LFT(t) \in \mathbb{Q}_{\geq 0} \cup \{ \infty \} \) such that \( EFT(t) \leq LFT(t) \),
- a cumulative distribution function (CDF) \( F_t(x) \) such that \( x < EFT(t) \Rightarrow F_t(x) = 0 \) and \( x > LFT(t) \Rightarrow F_t(x) = 1 \),
- and a weight \( W(t) \in \mathbb{R}_{\geq 0} \).

A place \( p \) is said to be an input or output place for a transition \( t \) if \((p, t) \in A^- \) or \((t, p) \in A^+ \), respectively. Following the usual terminology of stochastic Petri nets, a transition \( t \) is called immediate (IMM) if \( EFT(t) = LFT(t) = 0 \) and timed otherwise; a timed transition is called exponential (EXP) if \( F_t(x) = 1 - e^{-\lambda x} \) for some rate \( \lambda \in \mathbb{R}_{\geq 0} \), or general (GEN) if its time to fire is distributed according to a non-exponential distribution; as a special case, a GEN transition \( t \) is deterministic (DET) if \( EFT(t) = LFT(t) > 0 \). For each transition \( t \) with \( EFT(t) < LFT(t) \), we assume that \( F_t \) can be expressed as the integral function of a PDF \( f_t \), i.e., \( F_t(x) = \int_0^x f_t(y) \, dy \). The same notation is also adopted for IMM and DET transitions, which are associated with Dirac impulse functions \( f_t(y) = \delta(y - \gamma) \) with \( \gamma = EFT(t) = LFT(t) \). For GEN transitions, we consider the class of piecewise expolynomial PDFs obtained by piecewise composition of products of exponentials and polynomials, on bounded or unbounded supports (also known in the literature as exponomials [14]).
Example 1. Fig. 1a introduces a small running example inspired by [23] and representing a G/D/1/2/2 queue (1 server with DET service time, a population of 2 customers with GEN arrival times, a capacity of 2). Tokens in places free and buffer specify the number of customers in the idle state or inside the queue, respectively. Customers arrive in series after times uniformly distributed over [1,2) (transition arrival), while service has a deterministic duration of 1.5 (transition service) and requires the server to be operational; the time to failure of the server is exponentially distributed with rate 0.1 (transition fail), and repairs are completed in a time uniformly distributed over [1,2) (transition restart). Fig. 1b depicts transient probabilities for the number of customers in the buffer and for the state of the server.

2.2 Probability space and cylinder sets

In the formulation of the probabilistic model checking problem, we will need to refer to the probability measure of selected sets of paths of an STPN model. We thus formalize the concept by defining the probability space \((\Omega_{m_0}, F_{m_0}, Pr_{m_0,f_0})\) induced by the semantics of STPNs for a given initial marking \(m_0\) and initial times to fire \(f_0\). The outcomes \(\Omega_{m_0}\) of the probability space are all paths \(\omega = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots\) with initial marking \(m_0\). Note that \(\Omega_{m_0}\) may include paths that are not feasible under the initial distribution \(f_0\) due to temporal constraints of the model; for these paths, the probability measure \(Pr_{m_0,f_0}\) will be zero.

To identify a \(\sigma\)-algebra \(F_{m_0}\) of events over \(\Omega_{m_0}\), we define as cylinder set \(C(m_0, \gamma, I_1, I_2, \ldots, \gamma_n, I_n)\) the set of all paths with initial marking \(m_0\) that fire the sequence of transitions \(\gamma_1, \gamma_2, \ldots, \gamma_n\) at absolute times contained in the intervals \(I_1, I_2, \ldots, I_n\), respectively:

\[
C(m_0, \gamma_1, I_1, \gamma_2, I_2, \ldots, \gamma_n, I_n) := \{ \omega \in \Omega_{m_0} | |\omega| \geq n \text{ and } \forall 0 < k \leq n, (\omega[k] = \gamma_k \text{ and } T(k, \omega) \in I_k) \}
\]

where \(|\omega|\) is the number of firings in \(\omega\), \(\omega[k]\) is the \(k\)th transition fired along \(\omega\) for all \(0 < k \leq |\omega|\), and \(T(k, \omega)\) is the absolute time of the \(k\)th firing in \(\omega\), for all \(k > 0\):

\[
T(k, \omega) := \left\{ \begin{array}{ll}
\sum_{i=0}^{k-1} \min_{t \in E(m_0)} \bar{t}(i) & \text{if } k \leq |\omega|, \\
+\infty & \text{if } k > |\omega|.
\end{array} \right.
\]

We let \(T(0, \omega) := 0\), so that \(T(k, \omega)\) also represents, for all \(0 \leq k \leq |\omega|\), the time at which state \(s_k\) is reached in \(\omega\). Note that, in contrast with the usual definition of cylinder sets for CTMCs [11], [12], constraints refer to absolute firing times rather than sojourn times. This formulation enables a simpler treatment of the dependence among subsequent sojourn times in models with underlying stochastic processes more general than SMPS.

The set of events \(F_{m_0}\) is defined as the smallest \(\sigma\)-algebra on \(\Omega_{m_0}\) that contains all the cylinder sets \(C(m_0, \gamma_1, I_1, \gamma_2, I_2, \ldots, \gamma_n, I_n)\) for \(n \in \mathbb{N}\), \(\gamma_1, \gamma_2, \ldots, \gamma_n\) ranging over all sequences of \(n\) transitions in \(T\), and \(I_1, I_2, \ldots, I_n\) ranging over all sequences of \(n\) non-empty intervals with rational endpoints (possibly right-unbounded).

Proposition 1. \(F_{m_0}\) is countable, the intersection of cylinder sets is a cylinder set, and the complement of a cylinder set is a finite union of disjoint cylinder sets.

Proof. The elements of \(F_{m_0}\) are uniquely identified by finite strings alternating transitions and firing intervals with rational endpoints: pairs of rational numbers and finite strings from a finite alphabet are countable sets, and thus \(F_{m_0}\) is also countable. The intersection of the cylinder sets \(C(m_0, \gamma_1, I_1, \gamma_2, I_2, \ldots, \gamma_n, I_n)\) and \(C(m'_0, \gamma'_1, I'_1, \gamma'_2, I'_2, \ldots, \gamma'_m, I'_n)\) with \(n \leq m\) is non-empty only if \(\gamma_i = \gamma'_i\) for \(i = 1, \ldots, n\) and it corresponds to the cylinder set \(C(m_0, \gamma_1, I_1 \cap I'_1, \gamma_2, I_2 \cap I'_2, \ldots, \gamma_n, I_n \cap I'_n, \gamma_{n+1}, I'_{n+1}, \ldots, \gamma'_m, I'_n)\). Finally, the complement of \(C(m_0, \gamma_1, I_1, \gamma_2, I_2, \ldots, \gamma_n, I_n)\) corresponds to the finite union of all disjoint cylinder sets \(C(m_0, \gamma'_1, I'_1, \gamma'_2, I'_2, \ldots, \gamma'_m, I'_n)\) such that \(\exists i \leq n. (\gamma_i \neq \gamma'_i)\) and \(\forall i \leq n. I_i = [0, \infty)\), or \(\forall i \leq n. (\gamma_i = \gamma'_i)\) and, for each non-empty subset \(A \subseteq \{1, \ldots, n\}\), \(I_i = [0, \inf I_i] \lor I'_i = [\sup I_i, \infty)\) for all \(i \in A\).

The probability measure \(Pr_{m_0,f_0}\) can be expressed in terms of transient stochastic state classes [37] and, if GEN transitions are associated with piecewise exponential PDFs, it can be computed numerically using the Sirio package of the ORIS Tool [38].

Definition 3. A transient stochastic state class is a tuple \(\Sigma = \langle m, D, f_{\{\tau_{age}, \bar{\tau}\}} \rangle\) where \(m \in \mathbb{N}^p\) is a marking; \(f_{\{\tau_{age}, \bar{\tau}\}}\) is the PDF (immediately after a firing) of the random vector \(\{\tau_{age}, \bar{\tau}\}\) including the absolute time \(\tau_{age}\) (elapsed from the start of the process until the transition firing) and the times to fire \(\bar{\tau} = (\tau_1, \ldots, \tau_n)\) of transitions \(E(m) = \{t_1, \ldots, t_n\}\) enabled by \(m\); \(D \subseteq \mathbb{N}^n+1\) is the support of \(f_{\{\tau_{age}, \bar{\tau}\}}\).

The initial (unconditioned) transient stochastic state class \(\Sigma_0\) assigns non-zero probability to states with marking \(m_0\) and absolute time \(\tau_{age} = 0\) according to the times to fire PDF \(f_{\tau_0}\), i.e., \(\Sigma_0 = \langle m_0, D_0, f_{\{\tau_{age}, t_0\}} \rangle\), where \(D_0 = [0, \infty] \times [\text{support of } f_{\tau_0}]\) and \(f_{\{\tau_{age}, t_0\}}(x_{\tau_{age}}, x_1, \ldots, x_n) = \delta(x_{\tau_{age}}) \cdot f_{\tau_0}(x_1, \ldots, x_n)\) for \(E(m_0) = \{t_1, \ldots, t_n\}\). Given a class \(\Sigma\), the state PDF conditioned on the execution of a transition \(\gamma\) at an absolute time in the interval \(I\) is given by the successor class of \(\Sigma\) through \(\gamma\) and \(I\).

Definition 4. We say that \(\Sigma' = \langle m', D', f'_{\{\tau_{age}, \bar{\tau}\}} \rangle\) is the successor of \(\Sigma = \langle m, D, f_{\{\tau_{age}, \bar{\tau}\}} \rangle\) in state \(I\) and with succession probability \(\mu\), and we write \(\Sigma \xrightarrow{\gamma,I,\mu} \Sigma'\), if, given that the marking of the STPN is \(m\) and \(\tau_{age}\) is a random vector distributed over \(D\) according to \(f_{\{\tau_{age}, \bar{\tau}\}}\), then: (1) \(\gamma\) has non-zero probability \(\mu\) of firing in \(\Sigma\) at some time in \(I\), and (2) if \(\gamma\) fires in \(\Sigma\) at some time in \(I\), its firing yields the marking \(m'\) and, conditioned on this event, the times to fire and \(\tau_{age}\) after the firing are distributed over \(D'\) according to \(f'_{\{\tau_{age}, \bar{\tau}\}}\).

The relation \(\Sigma \xrightarrow{\gamma,I,\mu} \Sigma'\) can be enumerated through a calculus for the computation of the probability of outgoing events, and for the symbolic derivation of the support and closed-form PDF of \(\{\tau_{age}, \bar{\tau}\}\) in successor classes. Given a class \(\Sigma\), an enabled transition \(\gamma\) and a firing interval \(I\), this calculus computes the succession probability \(\mu\) and the (unique) successor class \(\Sigma'\) such that \(\Sigma \xrightarrow{\gamma,I,\mu} \Sigma'\). Each class encodes the PDF of the current state given the past history, providing a full characterization of future evolution. The treatment in this paper does not assume knowledge of the calculus;
for convenience, we provide a summary in the additional material, and refer to [30, 31, 37] for a detailed description.

The probability measure of set systems can be evaluated through the repeated computation of successor classes.

**Proposition 2.** Given an initial marking \( m_0 \) and PDF \( f_{\vec{\tau}_0} \) of the times to fire, the probability measure of a cylinder set \( C(m_0, \gamma_1, I_1, \gamma_2, I_2, \ldots, \gamma_n, I_n) \) according to \( Pr_{m_0,f_{\vec{\tau}_0}} \) is equal to the product \( \prod_{i=1}^n \mu_i \) of succession probabilities for the sequence of transient stochastic state classes

\[
\Sigma_0 \gamma_1 f_{\vec{\tau}_0} \Sigma_1 \gamma_2 f_{\vec{\tau}_0} \ldots \sum_n \gamma_n f_{\vec{\tau}_0} \Sigma_n,
\]

or equal to 0 if the sequence is not defined (i.e., \( \exists i \leq n, \mu_i = 0 \)).

*Proof.* The event \( C(m_0, \gamma_1, I_1, \gamma_2, I_2, \ldots, \gamma_n, I_n) \) for \( n \in \mathbb{N} \) can be expressed as \( E_0 \cap E_1 \cap \cdots \cap E_n \), where \( E_0 = \Omega_{m_0} \) and, for each \( i > 0 \),

\[
E_i = \{ \omega \in \Omega_{m_0} \mid |\omega| \geq i, \omega[i] = \gamma_i \text{ and } T(i, \omega) \in I_i \}
\]

is the constrained set of paths imposing an absolute time only on the \( i \)th transition. By induction on the definition of succession of stochastic state classes, for all \( i \leq n \), the class \( \Sigma_i \) in

\[
\Sigma_0 \gamma_1 f_{\vec{\tau}_0} \Sigma_1 \gamma_2 f_{\vec{\tau}_0} \ldots \sum_n \gamma_n f_{\vec{\tau}_0} \Sigma_n
\]

represents the joint PDF of the absolute time and current state given the events \( E_0, E_1, \ldots, E_i \). \( \mu_i \) is the probability \( Pr_{m_0,f_{\vec{\tau}_0}} \{ E_i \mid E_0, E_1, \ldots, E_{i-1} \} \) that paths that performed \( \gamma_1, \ldots, \gamma_i \) in \( I_1, \ldots, I_{i-1} \) will also perform \( \gamma_i \) at some time in \( I_i \). Then \( Pr_{m_0,f_{\vec{\tau}_0}} \{ E_0 \cap E_1 \cap \cdots \cap E_n \} = Pr_{m_0,f_{\vec{\tau}_0}} \{ E_0 \} \cdot Pr_{m_0,f_{\vec{\tau}_0}} \{ E_1 \mid E_0, \ldots, E_{n-1} \} = \prod_{i=1}^n \mu_i \) if \( \mu_i > 0 \) for all \( i \leq n \); if some event \( E_i \) has zero probability given \( E_0, E_1, \ldots, E_{i-1} \) (i.e., \( \Sigma_i = \emptyset \)), then \( \mu_i = 0 \), the measure of the cylinder set is zero.

\[ \square \]

### 2.3 Probabilistic Temporal Logic

We specify quantitative properties of STPNs with a probabilistic temporal logic based on an interval until operator with predicates over the markings of the net. The logic can express bounds on the probability that the marking of the STPN satisfies a global predicate \( \varphi_2 \) at some time in the interval \([\alpha, \beta] \) without violating a safety predicate \( \varphi_1 \) in previous states. The syntax of the logic is

\[
\psi ::= \text{TRUE} \mid \neg \psi \mid \psi \land \psi \mid P_{\gamma_p}[\varphi U^{[\alpha,\beta]} \varphi_2]
\]

where \( \alpha, \beta \in Q_{\geq 0}, \) and atomic predicates on markings are defined as

\[
\neg \psi :: \neg \varphi \land \varphi \land AP
\]

with \( \gamma_p \in \mathbb{R} \). The probability that the STPN satisfies a predicate \( \varphi_2 \) at some time in the interval \([\alpha, \beta] \) and does not violate a safety predicate \( \varphi_1 \) in previous states is defined as \( Pr_{\gamma_p}[\varphi U^{[\alpha,\beta]} \varphi_2] \).

According to Eq. (1), a path satisfying the interval until operator \( \varphi_1 U^{[\alpha,\beta]} \varphi_2 \) must visit only \( \varphi_1 \)-states and then either reach a \( \varphi_2 \)-state in \([\alpha, \beta] \), or reach a \( \varphi_1 \land \varphi_2 \)-state before time \( \alpha \) and let time advance past \( \alpha \). It is worth noting that this formulation based on the index \( n \) of each state in a path ensures that also intermediate states with zero sojourn time (which may occur with non-zero probability when the model includes IMM or DET transitions) satisfy \( \varphi_1 \), which could not be specified in the continuous-time formulation of [12].

**Example 2.** In the G/D/1/2/2 queue of Fig. 1a, the property \( P_{<0.4}(\text{buffer < 2}) U^{[0,1]}(\text{failed = 1}) \land P_{<0.2}(\text{buffer < 2}) U^{[2,5,7]}(\text{failed = 1}) \) is satisfied when the probability of the server being down without ever reaching its full capacity is lower than 0.4 in the interval \([0, 7] \) and lower than 0.2 in the interval \([2, 5, 7] \).

The following proposition shows that, for every pair of marking predicates \( \varphi_1, \varphi_2 \), and \( \alpha, \beta \in Q_{\geq 0}, \) the set of paths satisfying the interval until operator is an event of \( F_{\gamma_p} \). Concretely, this means that the value of \( Pr_{\gamma_p}[\varphi U^{[\alpha,\beta]} \varphi_2] \) is well-defined and the semantics of Definition 5 can be computed with stochastic state classes.

**Proposition 3.** For each \( \varphi_1, \varphi_2 \in \mathbb{P} \) and \( \alpha, \beta \in Q_{\geq 0}, \) the set \( \{ \omega \in \Omega_{m_0} \mid \omega \models \varphi_1 U^{[\alpha,\beta]} \varphi_2 \} \) of paths satisfying the interval until operator is a countable union of cylinder sets.

*Proof.* The cylinder sets that end on a \( \varphi_2 \)-marking reached only through \( \varphi_1 \)-markings are countable. Each cylinder set is in fact uniquely identified by the sequence of transitions \( \gamma_1 \gamma_2 \cdots \gamma_n \) fired from \( m_0 \), which are strings on a finite alphabet. For each cylinder set \( C(m_0, \gamma_1, I_1, \gamma_2, I_2, \ldots, \gamma_n, I_n) \) that ends on a \( \varphi_2 \)-marking only through \( \varphi_1 \)-markings, we consider (1) the cylinder set imposing only an absolute
time in \( I_n = [\alpha, \beta] \) for the \( n \)th transition firing, and (2) if the marking reached after \( \gamma_n \) satisfies also \( \varphi_1 \), the cylinder sets \( C(m_0, \gamma_1, I_1, \gamma_2, I_2, \ldots, \gamma_n, I_n, \gamma_{n+1}, I_{n+1}) \) for each \( \gamma_{n+1} \in T \) that impose a bound \( I_n = [0, \alpha] \) for the firing of \( \gamma_n \) and a bound \( I_{n+1} = [\alpha, \infty) \) for the firing of \( \gamma_{n+1} \). The countable union of these cylinder sets is an event of \( F_{m_0} \) including all and only the successful paths. 

3 COMPOSING PATHS ACROSS REGENERATIONS

Paths satisfying an interval until operator can be represented as a countable union of disjoint cylinder sets; when the union is finite or some bounded error is allowed, the formal relation between the measure of cylinder sets and stochastic state classes presented in Section 2.2 provides a concrete solution for the evaluation of \( Pr_{m_0, f_{\varphi}} \{ \omega \in \Omega_{m_0} \mid \omega = \varphi_1 \cup^\alpha_\beta \varphi_2 \} \). In [28], a solution algorithm is formulated based on the enumeration of stochastic state classes for all finite sequences of fired transitions \( \gamma_1, \gamma_2, \ldots, \gamma_n \) and maximal firing time intervals \( I_1, I_2, \ldots, I_n \) that satisfy \( \varphi_1 \cup^\alpha_\beta \varphi_2 \). Similarly to [26], the enumeration of closed-form PDFs enables the accurate evaluation of low probability events, and the on-the-fly analysis of cylinder sets can be stopped early if the interval until operator is decided. As a major limit, the number of discrete events, and thus the number of closed-form PDFs to compute, can grow exponentially with the bound \( \beta \). To reduce this complexity, we identify discrete events after which the stochastic process exhibits the Markov property; the corresponding (random) time instants, called regeneration points, can be leveraged to decompose the evolution of the process through a Markov renewal argument: either a given property is satisfied before hitting a regeneration point, or, if a regeneration point is reached, the probability of satisfying the property in the remaining time is conditionally independent of the previous history given the current state. In Section 4, the computation of PDFs will be limited to discrete events before the first regeneration, combining measures associated with distinct initial states into a system of integral equations. In this section, we generalize the concept of regeneration of state-of-the-art techniques for stochastic Petri nets [17, 21, 39] by detecting states in which the time elapsed since the enabling of each GEN transition is deterministic; moreover, we highlight the properties of regeneration points in the context of stochastic state classes, and provide an algorithm for their on-the-fly detection during the enumeration of discrete events.

3.1 Extended regenerations

In the evolution of a stochastic process, a regeneration point occurs whenever the state of the process subsumes any information on its previous history.

Definition 6. Let \( \{ M(t), t \geq 0 \} \) be a stochastic process defined on a probability space \((\Omega, \mathcal{F}, P)\) with finite state space \( S \). We say that \( \{ M(t), t \geq 0 \} \) encounters a regeneration point at time \( t \geq 0 \) if it satisfies the Markov property in \( t \):

\[
P\{ M(t + t') = j \mid M(t) = i, (\forall u \in A_t).M(u) = i_u \} = \\
P\{ M(t') = j \mid M(0) = i \}
\]

for all \( j \in S, t' \geq 0, A_t \subseteq [0, t), \) and \( i_u \in S \) for \( u \in A_t \).

While CTMCs encounter a regeneration point at every time instant, in STPNs regeneration points correspond to discrete events after which GEN timers do not “carry memory” of the previous evolution [17], similarly to EXP timers (which are always memoryless). This is the case of GEN timers that are either reset, or have been enabled for a deterministic time: given the current marking and the deterministic enabling times of GEN timers, the probability distribution of future states is conditionally independent of the previous history. A stochastic state class where times to fire satisfy this condition is called regenerative, and the PDF of the vector \( \langle \tau_{\text{age}}, \vec{t} \rangle \) is always in product form.

Definition 7. A stochastic state class \( \Sigma \) is regenerative if, for each enabled GEN transition \( t_i \), the time elapsed from its enabling until the firing that led to \( \Sigma \) is equal to some deterministic value \( d_i \in \mathbb{R}_{\geq 0} \), which we call the enabling time of \( t_i \) in \( \Sigma \).

Remark 1. In a regenerative state class \( \Sigma = \langle m, D, f_{\langle \tau_{\text{age}}, \vec{t} \rangle} \rangle \) where the sets of enabled GEN, EXP, and IMM transitions are \( \{ t_1, \ldots, t_n \}, \{ t_{n+1}, \ldots, t_m \}, \) and \( \{ t_{m+1}, \ldots, t_l \} \), respectively, if \( \vec{d} = (d_1, \ldots, d_n) \in \mathbb{R}_{\geq 0}^n \) is the vector of enabling times of GEN transitions, the support \( D \) and the probability density function \( f_{\langle \tau_{\text{age}}, \vec{t} \rangle} \) of \( \langle \tau_{\text{age}}, \vec{t} \rangle \) in \( \Sigma \) are equal to

\[
D = D_{\text{age}} \times \prod_{i=1}^n [\max\{0, EFT(t_i) - d_i\}, LFT(t_i) - d_i] \times \prod_{i=n+1}^m [0, +\infty) \times \prod_{i=m+1}^l [0, 0]
\]

and

\[
f_{\langle \tau_{\text{age}}, \vec{t} \rangle}(x_{\text{age}}, \vec{x}) = f_{\text{age}}(x_{\text{age}}) \cdot \prod_{i=1}^n \frac{f_{\text{EFT}}(x_i + d_i)}{\int_{-\infty}^{\max\{0, \text{EFT}(t_i)\}} f_{\text{EFT}}(u) \, du} \cdot \prod_{i=n+1}^m \lambda_i e^{-\lambda_i x_i} \cdot \prod_{i=m+1}^l \delta(x_i)
\]

respectively, for some PDF \( f_{\text{age}} \) of \( \tau_{\text{age}} \) with support \( D_{\text{age}} \).

Remark 2. As a notable case, a class in which all GEN transitions are newly enabled is regenerative with \( \vec{d} = 0 \); this case corresponds to the usual concept of regeneration in the literature on stochastic Petri nets [17, 21]. In particular, this is the regeneration of the initial class \( \Sigma_0 \).

Remark 3. A regenerative class is uniquely identified by its marking \( m \), by the vector \( \vec{d} \) of enabling times, and by the PDF \( f_{\text{age}} \) and support \( D_{\text{age}} \) of the absolute time \( \tau_{\text{age}} \) of the discrete event associated with the stochastic state class. The marking \( m \) identifies the set of enabled transitions, and the support and distribution of EXP and IMM transitions, while the enabling times \( \vec{d} \) identify the support and distribution of GEN timers.

Remark 4. In the following, given a pair \( i = (m, \vec{d}) \), where \( m \) is a marking and \( \vec{d} \) is a vector of enabling times, we denote by \( \langle \Omega_i, \mathcal{F}_i, P_i \rangle \) the probability space for the STPN paths with initial marking \( m \) when times to fire are initially distributed according to the product-form PDF \( f_{\vec{d}} \), described in Remark 1 for the given enabling times \( \vec{d} \) and for \( \tau_{\text{age}} \) equal to zero (i.e., \( f_{\text{age}}(x_{\text{age}}) = \delta(x_{\text{age}}) \) and \( D_{\text{age}} = [0, 0] \)).
3.2 Detection of regeneration points in the enumeration of stochastic state classes

At regeneration points, the time elapsed since the enabling of each GEN transition must be deterministic. In order to detect regeneration points in the enumeration of successor classes, we analyze synchronizations between the enabling of DET/IMM and GEN transitions over sequences of firings: immediately after the firing of a DET or IMM transition \( u \), a GEN transition \( t \) has been enabled for a deterministic time if \( t \) was enabled together with \( u \), or with a deterministic delay (or advance) with respect to the enabling of \( u \).

We define the map \( \text{ENABLELING}(u, t) \) to record, for each DET/IMM transition \( u \), the deterministic time from the enabling of each GEN transition \( t \) until the scheduled firing of \( u \), or NIL if this time is not deterministic. The algorithm in Fig. 2 constructs \( \text{ENABLELING}(u, t) \) for an initial regeneration \( (m_0, \vec{d}_0) \) which assigns deterministic enabling time \( \vec{d}_0(t) \) to each GEN transition \( t \) (lines 1–3). After the firing of the \( i \)th transition in the sequence \( \gamma_1, \ldots, \gamma_n \), the enabling time \( \vec{d}(t) \) of each GEN transition \( t \) is recomputed from \( \text{ENABLELING}(\gamma_i, t) \) (lines 5–13): if \( \vec{d} \) assigns a deterministic enabling time to each enabled GEN transition, a regeneration point is detected, and the regeneration \((m, \vec{d})\) is returned (line 16), where \( m \) is the marking reached after the firing of \( \gamma_i \). Otherwise, the map \( \text{ENABLELING}(u, t) \) is updated to maintain its invariant: information on each disabled transition is removed (lines 18–21) and, for each DET/IMM transition \( u \) and GEN transition \( t \) with deterministic enabling times \( \vec{d}(u) \) and \( \vec{d}(t) \), respectively, the enabling time of \( t \) at the firing of \( u \) is set to \( \vec{d}(t) + [\text{LFT}(u) - \vec{d}(u)] \) (lines 22–24).

While the algorithm presented in Fig. 2 detects the first regeneration on a finite sequence of transition firings, lines 5–24 can be executed after the enumeration of each stochastic state class to identify regenerative classes and regenerations on-the-fly.

3.3 Properties of regeneration points

The transient behavior of an STPN is fully characterized by an infinite tree encoding the succession relation among stochastic state classes for all sequences of fired transitions. In the following, we omit the firing time interval \( I \) in the notation \( \Sigma I \rightarrow \Sigma' \) whenever \( I = [0, +\infty) \) (i.e., no constraint is imposed on the absolute firing time).

Definition 8. The transient stochastic tree from an initial class \( \Sigma_0 \) is a tuple \( \langle N, E, n_0, \Sigma \rangle \) where: the set \( N \) is a countable set of nodes; \( n_0 \in N \) is the root node; the function \( \Sigma \) associates each node \( n \in N \) with a stochastic state class \( \Sigma(n) \), with \( \Sigma(n_0) = \Sigma_0 \); the labeled edges \( E \subseteq N \times T \times (0, 1] \times N \) represent the (unconstrained) successions of stochastic state classes associated with transition firings, i.e., \( (n, \gamma, \mu, n') \in E \) if and only if \( \Sigma(n) \rightarrow_{\gamma, \mu} \Sigma(n') \).

The transient tree enumerates all the sequences of transition firings with non-zero probability, and associates each node with the resulting PDF over states and absolute reaching times. A node \( n \) associated with a regenerative class \( \Sigma(n) = (m, D, \vec{f}(\gamma_{\text{neg}}, \vec{\tau})) \) is said to be regenerative, and it satisfies two major properties presented in the following. The first property guarantees that two regenerative nodes reached at different times, but associated with the same marking and deterministic enabling times, enable the same firing sequences with the same probabilities.

Lemma 1. Let \( n_i \) and \( n_j \) be two regenerative nodes associated with stochastic state classes \( \Sigma(n_i) \) and \( \Sigma(n_j) \) with the same marking \( m \) and the same deterministic enabling times \( \vec{d} \). Then, the sequences feasible from \( n_i \) and from \( n_j \) are the same, they have the same probability, and they end up in nodes associated with stochastic state classes that have the same marking and the same random vector \( \vec{\tau} \) of times to fire for enabled transitions.

Proof. The proof runs by induction on the length of succession sequences originating from the nodes \( n_i \) and \( n_j \), and leverages the fact that the two classes have the same marginal distribution of times to fire, so that they will allow the same set of feasible behaviors with the same probabilities: according to Remark 3, \( \Sigma(n_i) \) and \( \Sigma(n_j) \) have the same support and distribution for the vector of times to fire of enabled transitions; the former condition implies that they accept the same sets of feasible behaviors (sequences of firable transitions), and that equal succession sequences result in the same final markings and times to fire supports (due to the underlying non-deterministic model); the latter condition implies that probabilities of these firing sequences are also the same, and that the sequences end up in classes with the same PDF of times to fire.

Lemma 1 gives relevance to the pair \( (m, \vec{d}) \), which captures a condition that can be reached at different times in distinct regenerative nodes, but always produces the same
subsequent behaviors. In the sequel, we refer to the pair $(m, d)$ as regeneration condition.

The next lemma completes the picture by focusing on the time advancement before and after a regenerative node, and it fully exploits the properties of regenerative stochastic state classes to show that the times elapsed before and after a regeneration are independent.

**Lemma 2.** Let $n_j$ be a regenerative node, $n_k$ be the descendant of $n_j$ reached through the transitions $\rho = \gamma_1, \ldots, \gamma_n$, and $f_{age}^j$ and $f_{age}^k$ be the marginal PDF of the $\tau_{age}$ variables in $\Sigma(n_j)$ and $\Sigma(n_k)$, respectively. Then,

$$f_{age}^k(x_{age}) = \int_{-\infty}^{+\infty} f_{age}^j(u) f_{age}^i(x_{age} - u) \, du (2)$$

where $f_{age}^i$ is the marginal PDF of $\tau_{age}$ for the node $\hat{n}_i$ reached through $\rho$ in the transient tree rooted in a node $\hat{n}_j$ with the same marking and random vector as $n_j$, but with $\tau_{age}$ distributed as $f_{age}^j(x_{age}) = \delta(x_{age})$.

**Proof.** The time spent in the execution of $\rho$ from $n_j$ or from $\hat{n}_j$ is the same as it only depends on the marginal distribution of times to fire in $n_j$ and $\hat{n}_j$ (Lemma 1); moreover, the distribution of this time is given by $f_{age}^k$, since the age is equal to zero in $\hat{n}_j$, i.e., $f_{age}^j(x_{age}) = \delta(x_{age})$. Since $n_j$ is regenerative, $f_{age}^i$ is in product form with respect to the marginal PDF of times to fire (Remark 1), and thus the evolution from $n_j$ to $\hat{n}_j$ is independent of the time at which the node is reached; the age in $n_k$ is the sum of the independent random variables associated with the age in $n_j$ and with the duration of $\rho$, and it is distributed as the convolution $f_{age}^k(x_{age}) = \int_{-\infty}^{+\infty} f_{age}^j(u) f_{age}^i(x_{age} - u) \, du$.

Note that in Lemma 1 the assumption that $n_i$ and $n_j$ are regenerative is used only to guarantee that they have the same marginal PDF for the vector of times to fire $\tau$. In Lemma 2, the assumption of regeneration is used also to guarantee that the PDFs of $\tau_{age}$ and $\tau$ are in product form.

**Example 3.** In order to illustrate the concept of regeneration points, we report in Fig. 3 the stochastic state classes corresponding to the cylinder set with initial marking $\mathbf{2free operational}$ and sequence of discrete events fail, restart, arrival, service (without constraints on the absolute firing times) for the STPN of Fig. 1a. The probability measure of the continuous set of paths contained in the cylinder set is given by the product of succession probabilities (which we report up to the fourth significant figure). In regenerative stochastic state classes $\Sigma_0, \Sigma_3, \Sigma_4$, the absolute time of the last event and all the times to fire of enabled transitions are independent random variables with product-form PDF; notably, the GEN transition arrival in $\Sigma_3$ is not newly enabled, but its PDF is uniquely identified by the deterministic enabling time 1.5. Note that, as discussed in [37], $\tau_{age}$ encodes the negation of the absolute firing time, in order to operate on variables decreasing with the same rate.

**Remark 5 (Nesting of until operators).** In a Markov regenerative process, the discrete component of the state does not carry sufficient information to verify nested sub-formulas independently. We illustrate the problem with an example inspired by [5]. Consider an STPN with only one place $p$ and one transition $t$ with time to fire uniform on $[0, 4]$. Let $p$ be a precondition for $t$, and let the initial marking assign one token to $p$; at the firing of $t$, the token is removed and no further transition is enabled. The underlying marking process is semi-Markov with two states: $p = 1$ and $p = 0$. Consider now the nested formula $\varphi_{ext} = P_{p > 1/3}[\varphi_{in} U^0(0, 2) (p = 0)]$ with $\varphi_{in} = P_{p < 1/3}(p = 1) U^0(0, 1)$ (for $p = 0$). Intuitively, for $\varphi_{ext}$ to hold, $\varphi_{in}$ must be satisfied continuously until the firing of $t$. However, due to the dependency on past evolution introduced by the GEN sojourn time, the satisfaction of the inner formula $\varphi_{in}$ changes over time: given a sojourn of $x$ time units, the probability of $(p = 1) U^0(0, 1) (p = 0)$ is $f_p^\circ_\varphi [x, 4]/(4 - x) \, dy$, which is monotonically nondecreasing and remains under $1/3$ only when $x \in [0, 1)$. Therefore, the only paths that satisfy $\varphi_{in}$ continuously are those that sojourn in $p = 1$ less than $\bar{x} = 1$ time units, and the probability of satisfying the nested operator $\varphi_{in} U^0(0, 2) (p = 0)$ is $f_p^\circ_\varphi 1/4 \, dy = 1/4$. By this argument, we conclude that the external formula $\varphi_{ext}$ is not satisfied; the important remark is that this conclusion requires that initial states be distinguished not only by their marking, but also by the sojourn duration.

### 4. Regenerative Solution of an Interval Until Operator

#### 4.1 Renewal equations for the interval until operator
Given the predicates $\varphi_1$ and $\varphi_2$, a real interval $[\alpha, \beta]$ with $\alpha, \beta \in \mathbb{Q}_{\geq 0}$, and a regeneration condition $i = (m, d)$, we define

$$\Omega_i(\alpha, \beta) := \{ \omega \in \Omega_i | \omega = \varphi_1 U^{[\alpha, \beta]} \varphi_2 \}$$

to be the set of paths that start from the marking of $i$ and satisfy the interval until operator, and we denote by $p_i(\alpha, \beta) := Pr_i(\Omega_i(\alpha, \beta))$ its probability measure, as defined...
in Remark 4 (Section 4). For each path $\omega = s_0 \xrightarrow{\gamma_1} s_1 \xrightarrow{\gamma_2} \ldots$ in $\Omega_\iota(\alpha, \beta)$, with $s_n = (m_n, \bar{\tau}_n)$, $m_n \in \mathbb{N}^p$ and $\bar{\tau}_n \in \mathbb{R}^{E(m_n)}$, we indicate as $\text{REG}(\omega)$ the index of the first regeneration along the path:

$$\text{REG}(\omega) := \min\{n \in \mathbb{N} \mid s_{n-1} \xrightarrow{\gamma_n} s_n \text{ is a regeneration}\}$$

and we indicate as $\text{OK}(\omega)$ the index of the first state leading to the satisfaction of the until operator:

$$\text{OK}(\omega) := \min\{n \in \mathbb{N} \mid n \leq |\omega| \land (m_n \models \varphi_2) \land \left( \forall k < n. (m_k \models \varphi_1) \land (T(n, \omega) \in [\alpha, \beta] \lor (T(n, \omega) < \alpha \land T(n+1, \omega) \geq \alpha \land m_n \models \varphi_1) \right) \}.$$.

Moreover, we indicate with $t_{\text{REG}}(\omega) := T(\text{REG}(\omega), \omega)$ the time of the first regeneration in $\omega$, and with $(m_{\text{REG}(\omega)}, d_{\text{REG}(\omega)})$ the corresponding regeneration condition. The probability $p_i(\alpha, \beta)$ can then be decomposed so as to separately account for paths in $\Omega_\iota(\alpha, \beta)$ that satisfy the until operator under different timings of the first regeneration. To this end, we distinguish paths that satisfy the until operator before reaching a regeneration from those that encounter the first regeneration before $\alpha$, or between $\alpha$ and $\beta$, and then satisfy the until operator:

$$\Omega_\iota^L(\alpha, \beta) := \{ \omega \in \Omega_\iota(\alpha, \beta) \mid \text{OK}(\omega) < \text{REG}(\omega) \},$$

$$\Omega_\iota^G(\alpha, \beta) := \{ \omega \in \Omega_\iota(\alpha, \beta) \mid \text{OK}(\omega) \geq \text{REG}(\omega) \land t_{\text{REG}}(\omega) < \alpha \},$$

$$\Omega_\iota^H(\alpha, \beta) := \{ \omega \in \Omega_\iota(\alpha, \beta) \mid \text{OK}(\omega) \geq \text{REG}(\omega) \land t_{\text{REG}}(\omega) \in [\alpha, \beta] \}. $$

**Proposition 4.** For any regeneration condition $i$ and $\alpha, \beta \in \mathbb{Q}_{\geq 0}$, it holds $p_i(\alpha, \beta) = P_{\iota_i}(\Omega_\iota^L(\alpha, \beta)) + P_{\iota_i}(\Omega_\iota^G(\alpha, \beta)) + P_{\iota_i}(\Omega_\iota^H(\alpha, \beta))$.

**Proof.** The sets $\Omega_\iota^L(\alpha, \beta), \Omega_\iota^G(\alpha, \beta), \Omega_\iota^H(\alpha, \beta)$ are a partition of the set of paths $\Omega_\iota(\alpha, \beta)$: on the one hand, they are clearly disjoint; on the other hand, to prove that their union is $\Omega_\iota(\alpha, \beta)$ it is sufficient to consider that $\forall \omega \in \Omega_\iota(\alpha, \beta), t_{\text{REG}}(\omega) > \beta$ implies $\text{OK}(\omega) < \text{REG}(\omega)$. ∎

The probability measure of the three sets $\Omega_\iota^L(\alpha, \beta), \Omega_\iota^G(\alpha, \beta), \Omega_\iota^H(\alpha, \beta)$ can be expressed in terms of three kernels characterizing the behavior of the stochastic process within the first regeneration epoch.

The measure of $\Omega_\iota^L(\alpha, \beta)$ is directly defined as the local kernel $L_{\iota_i}^{\varphi_1, \varphi_2}(\alpha, \beta) := P_{\iota_i}(\Omega_\iota^L(\alpha, \beta))$, which evaluates the probability measure of paths that satisfy the until operator before reaching a regeneration. In contrast, the measures of $\Omega_\iota^G(\alpha, \beta)$ and $\Omega_\iota^H(\alpha, \beta)$ are not limited to the first regeneration epoch and require the next Propositions 5 and 6.

**Proposition 5.** The measure $P_{\iota_i}(\Omega_\iota^G(\alpha, \beta))$ is equal to

$$\sum_k \int_{x \in [0, \alpha)} dG_{\iota_k}^G(x) p_k(\alpha - x, \beta - x)$$

where $k = (m, \bar{d})$ ranges over all reachable regeneration conditions and the global kernel $G_{\iota_k}^G(x)$ is defined as

$$G_{\iota_k}^G(x) := P_{\iota_k}(\{ \omega \in \Omega_\iota \mid t_{\text{REG}}(\omega) \leq x \land (m_{\text{REG}(\omega)}, d_{\text{REG}(\omega)}) = k \land (\forall j < \text{REG}(\omega)).(m_j \models \varphi_1) \}.$$.

**Proposition 6.** The measure $P_{\iota_i}(\Omega_\iota^H(\alpha, \beta))$ is equal to

$$\sum_k \int_{x \in [\alpha, \beta]} dH_{\iota_k}^{\varphi_1, \varphi_2}(x) p_k(0, \beta - x)$$

where $k = (m, \bar{d})$ ranges over all reachable regeneration conditions and the conditional global kernel $H_{\iota_k}^{\varphi_1, \varphi_2}(x, a)$ is defined as

$$H_{\iota_k}^{\varphi_1, \varphi_2}(x, a) := P_{\iota_k}(\{ \omega \in \Omega_\iota \mid t_{\text{REG}}(\omega) \leq x \land (m_{\text{REG}(\omega)}, d_{\text{REG}(\omega)}) = k \land (\forall j < \text{REG}(\omega)).(m_j \models \varphi_1 \land (m_j \models \varphi_2) \Rightarrow T(j + 1, \omega) < \alpha) \}.$$.

**Proof.** For each $\omega \in \Omega_\iota^H(\alpha, \beta)$, it must be that $\text{OK}(\omega) \geq \text{REG}(\omega)$ and $t_{\text{REG}}(\omega) < \alpha$ (i.e., $\omega$ encounters a goal state after reaching a regeneration point before time $\alpha$). According to Lemmas 1 and 2, the process evolution after the regeneration point depends only on the regeneration condition $(m_{\text{REG}(\omega)}, d_{\text{REG}(\omega)})$, and the remaining time for the satisfaction of the until operator is reduced by $t_{\text{REG}}(\omega)$: since the only condition required by Eq. (1) for states $(m_j, \bar{\tau}_j)$ with $j < \text{OK}(\omega)$ is $m_j \models \varphi_1$, and $\text{OK}(\omega) \geq \text{REG}(\omega)$ for $\omega \in \Omega_\iota^H(\alpha, \beta)$, the measure $P_{\iota_i}(\Omega_\iota^H(\alpha, \beta))$ is equal to

$$\int_X P_{\iota_k}(m_{\text{REG}(\omega)}, d_{\text{REG}(\omega)})(\alpha - t_{\text{REG}}(\omega), \beta - t_{\text{REG}}(\omega)) dP_{\iota}(\omega)$$

where $X(\alpha) := \{ \omega \in \Omega_\iota \mid t_{\text{REG}}(\omega) < \alpha \land (\forall j < \text{REG}(\omega)).(m_j \models \varphi_1) \}$. In Eq. (5), the measure of each path reaching its first regeneration point before $\alpha$ without violating $\varphi_1$ is multiplied by the probability that the until operator will be satisfied from that regeneration in the remaining time. By conditioning on all reachable regeneration conditions $(m_{\text{REG}(\omega)}, d_{\text{REG}(\omega)}) = k$ and times $t_{\text{REG}}(\omega) = x$ of the first regeneration before $\alpha$, we obtain Eq. (3), where the global kernel $G_{\iota_k}(x)$ represents the probability of reaching, within time $x$, a regeneration with regeneration condition $k$ while always satisfying $\varphi_1$ in previous states. ∎

**Propositions 5 and 6** provide an important result, as they apply renewal arguments to the satisfaction of the until operator and distinguish the properties that must be satisfied by paths before a regeneration point in $[0, \alpha)$ or in $[\alpha, \beta)$. We can now present our main result, which follows directly from Propositions 4 to 6 and shows that the measure $p_{(m_0, \bar{0})}(\alpha, \beta)$ of paths satisfying the until operator from the initial regeneration condition $(m_0, \bar{0})$ can be computed from the measures $p_i(\alpha, \beta)$ for all possible $i, \alpha, \beta$. 


Fig. 4: Constraints on paths contributing to the kernels.

**Theorem 1.** The measures \( p_i(\alpha, \beta) \) for all \( i = (m, d) \), each corresponding to the probability that the model satisfies the interval until operator \( \varphi_1 U^{[\alpha, \beta), \varphi_2} \) from the initial marking \( m \) with PDF of GEN timers given by the deterministic enabling times \( d \), are given by the system of integral equations

\[
p_i(\alpha, \beta) = L^i_{\varphi_1, \varphi_2}(\alpha, \beta) + \sum_k \int_{x \in [0, \alpha]} dG^i_{\varphi_2}(x) p_k(\alpha - x, \beta - x) + \sum_k \int_{x \in [\alpha, \beta]} dH^i_{\varphi_1, \varphi_2}(\alpha, x) p_k(0, \beta - x)
\]

where \( i \) and \( k \) range over all reachable regenerative conditions.

The theorem represents a bivariate generalization of Markov renewal equations [18], [40] leveraging three kernels that result from a renewal argument specific to the interval until operator: the model can satisfy \( \varphi_2 \) between \( \alpha \) and \( \beta \) either (1) without regenerations, (2) reaching the first regeneration before \( \alpha \), or (3) reaching the first regeneration in \([\alpha, \beta]\). As illustrated in Fig. 4, \( \varphi_1 \) must always be satisfied; additionally, \( \varphi_1 \) must be satisfied between \( \alpha \) and the first regeneration in paths that satisfy the until operator only after a regeneration in \([\alpha, \beta] \).

The bivariate unknowns \( p_i(\alpha, \beta) \) take into account both a minimum and maximum time for the satisfaction of \( \varphi_2 \); after a regeneration at time \( x \) with regeneration condition \( k \), the success probability is given by the solution from \( k \) with reduced time constraints: \( p_k(\alpha - x, \beta - x) \) if \( x < \alpha \) and \( p_k(0, \beta - x) \) if \( x \geq \alpha \). In the next section, we will show that the numerical solution of the integral equations for \( p_i(\alpha, \beta) \) requires a number of unknowns \( p_k(x, y) \) that grows linearly with respect to \( \beta \), similarly to the required values of \( L^i_{\varphi_1, \varphi_2} \) and \( G^i_{\varphi_1, \varphi_2} \); in contrast, the number of required values of \( H^i_{\varphi_1, \varphi_2} \) grows linearly with the product \( \alpha(\beta - \alpha) \), as illustrated in Fig. 5.

### 4.2 Numerical integration and kernels evaluation

The kernels can be evaluated through the enumeration of stochastic state classes after discrete events limited to the first regeneration epoch; Eq. (8) can then be solved numerically in the time domain through techniques such as Newton–Cotes formulas or Runge–Kutta methods [41], with various trade-offs between accuracy and complexity. Given a step \( h \), discretizing the temporal domain \([0, \beta]\) into points \( t_n = nh \), with \( \alpha = ah \) and \( \beta = bh \), Newton–Cotes formulas define the linear system

\[
p(t_a, t_b) = \bar{L}^i_{\varphi_1, \varphi_2}(t_a, t_b) + \sum_{m=0}^a w_m dG^{\varphi_2}(t_m) p(t_{a-m}, t_{b-m}) + \sum_{m=0}^b w_m dH^{\varphi_1, \varphi_2}(t_m) p(0, t_{b-m})
\]

in the unknowns \( p(t_a, t_b) \) for \( a = 0, \ldots, b - a \), and \( p(t_a, t_{a+b-a}) \) for \( a = 1, \ldots, a \), where, for first-degree formulas (trapezoidal rule), \( w_m = h/2 \) for \( m = 0, m = a \), or \( m = b \), and \( w_m = h \) otherwise. For regular MRPs, \( dG^{\varphi_2}(0) = 0 \) and \( dH^{\varphi_1, \varphi_2}(0, 0) = 0 \), and Eq. (9) can be solved by forward substitution:

\[
p(t_a, t_b) = \bar{L}^i_{\varphi_1, \varphi_2}(0, t_b) + \sum_{m=1}^b w_m dH^{\varphi_1, \varphi_2}(0, t_m) p(t_{b-m})
\]

for \( b = 0, \ldots, b - a \), and

\[
p(t_a, t_b) = \bar{L}^i_{\varphi_1, \varphi_2}(t_a, t_b) + \sum_{m=1}^a w_m dG^{\varphi_2}(t_m) p(t_{a-m}, t_{b-m}) + \sum_{m=0}^b w_m dH^{\varphi_1, \varphi_2}(t_m) p(0, t_{b-m})
\]

for \( a = 1, \ldots, a \) and \( b = a + b - a \). By evaluating the unknowns \( p(t_a, t_b) \) in this order, the solution \( p(t_a, t_b) \) can be computed as a direct sum that requires:

- local kernel values \( \bar{L}^i_{\varphi_1, \varphi_2}(0, t_b) \) for \( b = 0, \ldots, b - a \) and \( \bar{L}^i_{\varphi_1, \varphi_2}(t_a, t_{a+b-a}) \) for \( a = 1, \ldots, a \);
- global kernel values \( dG^{\varphi_2}(t_m) \) for \( m = 1, \ldots, a \);
- conditional global kernel values \( dH^{\varphi_1, \varphi_2}(t_a, t_m) \) for \( a = 0, \ldots, a \) and \( m = a, a + b - a \).

Values of \( L^i_{\varphi_1, \varphi_2}(t_a, t_b) \), \( dG^{\varphi_2}(t_m) \), and \( dH^{\varphi_1, \varphi_2}(t_a, t_m) \) can be derived from the transient tree enumerated from regeneration condition \( i \), halting on (1) regenerative nodes, (2) nodes not satisfying \( \varphi_1 \), (3) nodes with minimum reaching time greater than \( \beta \). In the enumeration, the successors of a class \( \Sigma_i \) indicated as \( \text{SUCCESSORS}(\Sigma_i) \), are derived according to the calculus described in the supplemental material and in [30], [31], [37]. A class \( \Sigma_i \) derived through successions \( \Sigma_{i-1} \overset{\gamma_{i-1} \delta_{i}}{\rightarrow} \Sigma_i \) for \( i = 1, \ldots, n \) is associated with the
Fig. 6: Algorithm evaluating $L_i^{\varphi_1 \land \varphi_2}(\alpha, \beta)$.

Probability measure $\eta(\Sigma_n) = \prod_{i=1}^{n} \mu_i$ of the cylinder set of paths that perform the sequence of discrete events $\gamma_1, \ldots, \gamma_n$. Additional constraints on paths can be imposed by restricting the set of values of times to fire; in particular, given a stochastic state class $\Sigma = (m, D, f)$ and real intervals $I_1$ and $I_2$, we indicate as $\Sigma_{m_1 \in I_1, out \in I_2} = \{m, D_{\text{in} \in I_1, out \in I_2, f_{\text{in} \in I_1, out \in I_2}\}$

$D_{\text{in} \in I_1, out \in I_2} := \{\langle \tau_{\text{age}}, \vec{x} \rangle \in D \mid -\tau_{\text{age}} \in I_1$
$\text{and } (\min_i \tau_i) - \tau_{\text{age}} \in I_2 \}$

$\eta(\Sigma_{m_1 \in I_1, out \in I_2}) := \eta(\Sigma) \int D_{\text{in} \in I_1, out \in I_2} (x_{\text{age}}, \vec{x}) d\tau_{\text{age}} d\vec{x}$

the class $\Sigma$ conditioned on the event imposing that the last firing happened at some time in $I_1$ and the next firing will happen at some time in $I_2$ (note that $\tau_{\text{age}}$ encodes the negation of the absolute reaching time). Correspondingly, $\eta(\Sigma_{m_1 \in I_1, out \in I_2})$ represents the measure of the cylinder set of paths where the firings that enter and leave $\Sigma$ occur in the intervals $I_1$ and $I_2$, respectively. In the following, the superfluous restrictions $in \in [0, +\infty)$ and $out \in [0, +\infty)$ will be omitted in the notation.

Local kernel values $L_i^{\varphi_1 \land \varphi_2}(t_a, t_b)$. The algorithm in Fig. 6 evaluates $L_i^{\varphi_1 \land \varphi_2}(\alpha, \beta)$ by enumerating the transient tree from regeneration condition $i$. Specifically, $\Gamma$ is the frontier set containing classes to be processed and $p$ accumulates the value of $L_i^{\varphi_1 \land \varphi_2}(\alpha, \beta)$. For each non-regenerative class $\Sigma$ selected from $\Gamma$, three cases are possible, depending on the satisfaction of $\varphi_1$ and $\varphi_2$:

- A state in a class $\neg \varphi_1 \land \varphi_2$ (line 8), contributes to the probability $p$ if it is reached in $[\alpha, \beta]$; according to this, $p$ is incremented by the measure of the subset of $\Sigma$ restricted with the constraint $in \in [\alpha, \beta]$.
- A state in a class $\varphi_1 \land \neg \varphi_2$ (line 10) does not contribute to $p$, but its successors can, provided that they are reached within $\beta$; according to this, the successors of $\Sigma$ that are reached within $\beta$ are added to $\Gamma$.
- A state in a class $\varphi_1 \land \varphi_2$ (line 12) can contribute both to $p$ and to the frontier $\Gamma$: $p$ is incremented by the measure of the states in $\Sigma$ that are reached in $[\alpha, \beta]$, or reached before $\alpha$ and left after $\alpha$; the successors of $\Sigma$ are added to $\Gamma$ if and only if they are reached before $\alpha$.

Global kernel values $dG_{ik}^{\varphi_1}(t_m)$. The values $dG_{ik}^{\varphi_1}(t_m)$ for $m = 1, \ldots, a$ can be derived from the transient tree enumerated from regeneration condition $i$, stopping on any regenerative class, or on any $(\neg \varphi_1)$-class, or after the time limit $\alpha$. In particular, the value $dG_{ik}^{\varphi_1}(t_m)$ can be obtained by summing up, for each regenerative leaf $n$ with regeneration $k$, the PDF value of the absolute reaching time multiplied by $\eta(n)$, i.e., $dG_{ik}^{\varphi_1}(t_m) = \sum_{n} \eta(n) f_{\text{age}}(-t_m)$.

Conditional global kernel values $dH_{ik}^{\varphi_1,\varphi_2}(t_a, t_m)$. The values $dH_{ik}^{\varphi_1,\varphi_2}(t_a, t_m)$ can be approximated as $(H_{ik}^{\varphi_1,\varphi_2}(t_a, t_m) - H_{ik}^{\varphi_1,\varphi_2}(t_a, t_{m-1})) / h$, where the values $H_{ik}^{\varphi_1,\varphi_2}(\alpha, x)$ are derived from the transient tree enumerated from regeneration condition $i$, stopping on regenerations, on $(\neg \varphi_1)$-classes, and on classes reached after $x$. The evaluation discards also states in $(\varphi_1 \land \varphi_2)$-classes that are left after $\alpha$, since $H_{ik}^{\varphi_1,\varphi_2}(\alpha, x)$ gives the measure of the set of paths that end on regeneration condition $k$ within time $x$, after visiting only $\varphi_1$-states, and without visiting any $\varphi_2$-state after $\alpha$. The algorithm in Fig. 7 evaluates $H_{ik}^{\varphi_1,\varphi_2}(\alpha, x)$ for all $k$ by enumerating the transient tree from regeneration condition $i$; similarly to Fig. 6, $\Gamma$ is the frontier set and $p_k$ accumulates the value of $H_{ik}^{\varphi_1,\varphi_2}(\alpha, x)$.

For each state class $\Sigma$ selected from $\Gamma$:

- A state in a regenerative class with regeneration condition $k$ (line 6), contributes to the probability $p_k$ of $H_{ik}^{\varphi_1,\varphi_2}(\alpha, x)$ if it is reached before time $x$; according to this, $p_k$ is incremented by the measure of the subset of $\Sigma$ restricted with the constraint $in \in [0, x]$.
- A state in a class $\varphi_1 \land \neg \varphi_2$ (line 8) does not contribute to any $p_k$, but its successors can, provided that they are reached within $x$; according to this, the successors of $\Sigma$ that are reached within $x$ are added to $\Gamma$.
- The successors of a state in a class $\varphi_1 \land \varphi_2$ (line 10) can contribute to $H_{ik}^{\varphi_1,\varphi_2}(\alpha, x)$ if the state is left before time $\alpha$; according to this, the successors of $\Sigma$ that are reached before $\alpha$ are added to $\Gamma$.

Overall, for each regeneration condition $i$, the transient tree enumeration is repeated:

$\frac{\beta}{\alpha} + 1$ times to compute $L_i^{\varphi_1 \land \varphi_2}(t_a, t_b)$ for $a = 0$ and $b = 0, \ldots, b - a$, and for $a = 1, \ldots, a$ and $b = a + b - a$;
once for the evaluation of the global kernel values
dG_{ik}^a(t_m) for m = 1, \ldots, a and all k;
\left(\frac{a}{k} + 1\right)\left(\frac{\beta - \alpha}{\beta}\right) + 2\right) times for the evaluation of the
conditional global kernel values H_{ik}^{h_1,\phi_2}(t_a, t_m) for
a = 0, 1, \ldots, a, m = a - 1, \ldots, a + b - a and all k.

If R is the number of reachable regeneration conditions, the
number of transient tree enumerations is thus \(O\left(\frac{\beta - \alpha}{\beta}\right) R\).
The advantage with respect to [26], [28], where model checking is
performed with a single transient tree enumeration, lies in the
reduced depth of these transient trees: the computation of
successors for the leaves of the tree now halts not only on ¬\phi_1 classes, but also on regenerative ones. Notably, both
the worst-case space and time required for the computation
of a successor class grow exponentially with the depth of the
predecessor in the tree [30]; when the time bound \beta is
large and regenerations are reached in a limited number of
discrete events, the repeated enumeration of shallow trees
becomes extremely beneficial.

4.3 Eliminating the lower bound \alpha

The availability of deterministic transitions in STPNs can be
leveraged to remove the lower bound \alpha for the satisfaction of \phi_2, reducing the evaluation of an interval until operator to
a first-passage problem. We present this alternative approach
by discussing the effect of \alpha = 0 on Eq. (8), and then the negative consequences of extending the model with an
additional transition with deterministic duration equal to \alpha.

The complexity of Eq. (8) is largely reduced if the until
operator does not impose a minimum time for the acceptance
of the goal condition \phi_2, i.e., if \alpha = 0. In this case, both Eq. (8)
and its kernels are simplified: the local kernel \(L_{i}^{\phi_1,\phi_2}(0, \beta)\)
becomes the probability that, starting from the regenerative
condition \(i\), a \phi_2-state is encountered before the first
regeneration and within time \beta, traversing only \phi_1-states.
Moreover, the second term of Eq. (8) gives zero contribution,
while the conditional global kernel \(H_{ik}^{\phi_1,\phi_2}(0, x)\) becomes the
probability that regeneration condition \(k\) is reached within \(x\)
after visiting only states that satisfy \(\phi_1 \land \neg \phi_2\).

The kernels \(L_{i}^{\phi_1,\phi_2}(0, \beta)\) and \(H_{ik}^{\phi_1,\phi_2}(0, x)\) can be derived from
transient trees enumerated from each regeneration condition
\(i\) and halting on regenerative nodes, nodes not
satisfying \(\phi_1 \land \neg \phi_2\), or nodes with minimum reaching
time greater than \beta. The local kernel \(L_{i}^{\phi_1,\phi_2}(0, \beta)\) can be computed from the \(\tau_{age}\) PDF of leaf nodes satisfying \(\phi_2\),
while \(H_{ik}^{\phi_1,\phi_2}(0, x)\) can be computed from the \(\tau_{age}\) PDF
of regenerative leaf nodes. This construction applies the
strategy of [12] to the context of non-Markovian processes.
In fact, restrictions made in the enumeration of transient trees
correspond to manipulations performed on the underlying
stochastic process to turn any state that satisfies \(\phi_2\) or \(\neg \phi_1\)
into an absorbing state (i.e., disabling any transition).

The case \([0, \beta]\) can be lifted to solve the case \([\alpha, \beta]\) by
exploiting the ability of STPNs to represent DET transitions.
Following the same principle of techniques that reduce
probabilistic model checking to the analysis of a synchronous
composition of the model with a specification automaton [15],
[16], the STPN model can be extended with a DET transition
t with PDF \(f_t(x) = \delta(x - \alpha)\) and \(\phi_2\) can be restricted to
\(\phi'_2 = \phi_2 \land \{t \text{ has fired}\}\). In so doing, regenerations before \alpha
of the original model are not exploited, since the additional
DET transition \(t\) is not “memoryless”. Only after the firing of \(t\) at time \alpha, regenerations will be fully exploited in the
analysis. This approach is thus well-suited only for cases
with a small \alpha with respect to the duration of regeneration
epochs.

Example 4. The property of Example 2 (Section 2.3) is
not satisfied. In fact, the measure of paths satisfying
\(\phi_1 U^{[\alpha, \beta]} \phi_2\) from the initial marking \(2\)free operational with
\(\phi_1 = (\text{buffer} < 2)\) and \(\phi_2 = (\text{failed} = 1)\) is 0.3313 < 0.4 for
\(\alpha = 0\) and \(\beta = 7\), and 0.2339 > 0.2 for \(\alpha = 2.5\) and \(\beta = 7\).
In the latter case, when limited to \(\phi_1\)-markings, the model
can reach only 3 distinct regenerations before time \beta = 7
and the corresponding transient trees include a total of 44
classes. In contrast, if a transition with deterministic value
\(\alpha = 2.5\) is added to the model, a total of 130 classes need to
be enumerated. In particular, the transient tree enumerated
from the initial regeneration includes 115 classes: this larger
number is a consequence of the deterministic timer added to
the initial state, which results in a larger number of transition
firings required to reach the first regeneration.

5 FISCHER’S MUTUAL EXCLUSION PROTOCOL

5.1 Model definition

We illustrate the proposed technique on a stochastic model of
n concurrent processes \(P_1, P_2, \ldots, P_n\) accessing a critical
section with Fischer’s protocol [42]. The protocol ensures mutual exclusion using atomic read and write operations
on a shared communication variable id taking the values
0, 1, \ldots, n. When \(id = 0\), each process \(P_i\) can attempt the
access to the critical section. To this end, it performs the
(time-consuming) write operation \(i \leftarrow i\), waits for a time
not lower than \(W\), and then reads \(id\) again: if \(id = i\), it can
access the critical section and write \(id \leftarrow 0\) on exit; whereas,
if \(id \neq i\), it has to wait until \(id = 0\) to attempt again.

Fischer’s protocol is a typical benchmark for real-time
model checking, as it neatly illustrates the interaction be-
between concurrency and firm timing: mutual exclusion is
guaranteed provided that the waiting time \(W\) is greater than
the maximum time required by the write operation of any
process. This condition inherently requires a model with
multiple concurrent timers with upper and lower bounds.
While the protocol has been verified in the qualitative
perspective using real-time model checkers such as Kronos [43]
and Uppaal [44], randomized versions have been analyzed in
closed-form [45] or through simulation [46], [47] only with
timed activities modeled through exponential or gamma
distributions. In this case, due to unbounded PDF supports,
mutual exclusion can be violated with probability greater
than zero.

We analyze quantitative properties in a stochastic model
of the protocol enforcing the requirement of mutual exclusion
with certainty through the use of concurrent GEN timers with
bounded supports. Fig. 8 illustrates an STPN model with
three processes \(P_1, P_2, P_3\) (the same scheme can be extended
to any number of processes). The shared variable is encoded
by the marking of place id (initially empty). Each process
\(P_i\) eventually leaves its idle state through transition arrival_i
(EXP with rate 0.1), and enters the contention by reaching
We consider a deadline requirement prescribing that the latency for the access of \( P_1 \) to the critical section be (1) not higher than \( \beta \) (which we call base deadline) with probability greater than \( p \), and (2) not higher than \( \beta_r > \beta \) (which we call relaxed deadline) with probability greater than \( p_r > p \). This property can be encoded as the Boolean conjunction of two probabilistic existence properties [1]:

\[
P_{>p}[\text{TRUE } \mathcal{U}^{[0,\beta]}(c_{S1} = 1)] \land 
\]

\[
P_{>p_r}[\text{TRUE } \mathcal{U}^{[0,\beta_r]}(c_{S1} = 1)].
\]

Fig. 9 reports the measure \( Pr_{(m,\bar{m})}(\omega \in \Omega_m \mid \omega = \text{TRUE } \mathcal{U}^{[0,\beta]}(c_{S1} = 1)) \) as a function of \( \beta \), for \( m \in \{m_A, m_B, m_C\} \) where: \( m_A = \text{ready}_1 \text{idle}_2 \text{idle}_3 \) (which occurs when \( P_1 \) becomes ready while both \( P_2 \) and \( P_3 \) are in the contention, with \( P_2 \) writing to \( id \) and \( P_3 \) waiting to check \( id \) after a write operation). As intuitive, the latency of \( P_1 \) increases when the initial condition changes from \( m_A \) to \( m_B \), and from \( m_B \) to \( m_C \). Properties in the form of Eq. (11) are decided by comparing the probability computed for a given value of \( \beta \) with the threshold \( p \). For example, with initial condition \( m_A \), for \( \beta = 2, p = 0.9, \beta_r = 6 \) and \( p_r = 0.95 \), we conclude from Fig. 9 that \( P_{>p}[\text{TRUE } \mathcal{U}^{[0,\beta]}(c_{S1} = 1)] = \text{FALSE} \) and \( P_{>p_r}[\text{TRUE } \mathcal{U}^{[0,\beta_r]}(c_{S1} = 1)] = \text{TRUE} \). The relaxed deadline is thus met with the required probability, but the base deadline is not.

In order to understand the role of different design parameters in the overall distribution of latency, the probability measure of subsets of successful paths can be evaluated with additional until properties. For instance, the probabilistic until...
The probability of paths satisfying \((cs_1 = 0)\) \(U^{[0,\beta]}(\sum_{i=2}^{n} completed_i = 1 \land \sum_{i=2}^{n} ready_i \geq k)\) as a function of \(\beta\), from marking \(m_A = ready\_idle_2\_idle_3\), and different service times.

Fig. 10: The probability of paths satisfying \((cs_1 = 0)\) \(U^{[0,\beta]}(\sum_{i=2}^{n} completed_i = 1 \land \sum_{i=2}^{n} ready_i \geq k)\) as a function of \(\beta\), from marking \(m_A = ready\_idle_2\_idle_3\), and different service times.

The corresponding probability measure is determined by the policy of Fischer’s protocol, a lower writing time favors the first one to enter the critical section. To give a quantitative insight into this mechanism, we consider a setting in which the writing times of \(P_2\) and \(P_3\) are distributed uniformly over \([0,1]\) (mean value 0.5), while the writing time of \(P_1\) has either a truncated Erlang PDF \(f(x) = xe^{-20x}/400\) over \([0,1]\) (mean value 0.1) or its symmetrical \(g(x) = f(1-x)\) (mean value 0.9).

As a last example, we evaluate the probability that process \(P_3\) is in the critical section within a given time window \([\alpha, \beta]\) after an execution in which \(P_3\) has never accessed the critical section. This property might be of interest in a problem of real-time testing where the system can be observed only within an interval \([\alpha, \beta]\) and the test case requires \(P_3\) in the critical section without prior accesses of \(P_3\). The requirement can be formulated as the probabilistic interval until

\[
P_{>p}[\{cs_3 = 0\} \ U^{[\alpha,\beta]}(cs_1 = 1)\] (14)

and verified for given values of \(\alpha, \beta\) and \(p\) so as to determine the time \(\alpha\) at which it is best to start the observation, or the minimum duration of \(\beta - \alpha\) to obtain a probability of conclusive execution greater than a given threshold \(p\). Fig. 12 plots the probability measure of paths satisfying \((cs_3 = 0)\) \(U^{[\alpha,\beta]}(cs_1 = 1)\) for different values of \(\alpha\) and duration \(\beta - \alpha\) of the observation window. For each window size \(\beta - \alpha \in \{0.1, 0.5, 1.0, 1.5, 2.0\}\), the probability \(P_{\alpha,\beta}(cs_3 = 0) = P_{\alpha,\beta}(cs_1 = 1)\) is plotted in Fig. 12 for \(\alpha = 0, 0.1, \ldots, 4\), which might serve to select an optimum time \(\alpha\) to start the observation.
Enumerated classes follow the solid line. In this approach crucially affects regenerative transient analysis [37]: it is now the deterministic timer that carries memory until its elapse, in order to characterize the state distribution of the system at time \( \alpha \). Regeneration points before \( \alpha \) are thus inevitably lost, forcing the enumeration of all sequences of discrete events until \( \alpha \).

We provided a solution based on the bivariate extension of Markov renewal equations, explicitly accounting for a satisfaction interval \([\alpha, \beta]\). The result is based on the formal definition of the probability space of STPN paths, which established the theoretical relation between cylinder sets of paths and stochastic state classes [37]. Enumeration of stochastic state classes was in turn the basis for algorithms computing kernels of bivariate Markov renewal equations.

The computation of the kernels requires to repeat the enumeration of stochastic state classes from each regeneration condition for a number of times linear in \( \alpha(\beta - \alpha) \), but each enumeration is limited to the first regeneration epoch and regeneration points are exploited also before \( \alpha \). In so doing, since the number of feasible events grows exponentially with the time bound, repeated enumeration of a limited number of shallow trees can produce considerable benefits when the stochastic process has a repetitive structure and multiple regenerations can be traversed before reaching the time bound \( \beta \). Moreover, the enumeration is always restricted to paths satisfying the safety condition \( \varphi_1 \), and the underlying stochastic process needs to encounter regeneration points w.p.1 in a bounded number of events only on paths that always satisfy \( \varphi_1 \).

We provided a solution based on the formal definition of the probability space of STPN paths, which established the theoretical relation between cylinder sets of paths and stochastic state classes [37]. Enumeration of stochastic state classes was in turn the basis for algorithms computing kernels of bivariate Markov renewal equations.

We provided a solution based on the bivariate extension of Markov renewal equations, explicitly accounting for a satisfaction interval \([\alpha, \beta]\). The result is based on the formal definition of the probability space of STPN paths, which established the theoretical relation between cylinder sets of paths and stochastic state classes [37]. Enumeration of stochastic state classes was in turn the basis for algorithms computing kernels of bivariate Markov renewal equations.

We provided a solution based on the bivariate extension of Markov renewal equations, explicitly accounting for a satisfaction interval \([\alpha, \beta]\). The result is based on the formal definition of the probability space of STPN paths, which established the theoretical relation between cylinder sets of paths and stochastic state classes [37]. Enumeration of stochastic state classes was in turn the basis for algorithms computing kernels of bivariate Markov renewal equations.

The verification of an interval until operator \( \varphi_1, U^{[\alpha, \beta]} \varphi_2 \) in regenerative systems presents major challenges, both theoretical and practical, that cannot leverage existing approaches for CTMCs [12] nor established results of Markov renewal theory [18], [40].

Stochastic models with concurrent GEN timers “accumulate memory” over time: the state at time \( \alpha \) does not summarize, in general, the past evolution of the system, and the process cannot be verified independently before and after \( \alpha \), in contrast to CTMCs, in which every time instant, and thus \( \alpha \), is a regeneration point. On the other hand, the reduction to a first-passage analysis with \( \alpha = 0 \) requires the introduction of a deterministic timer in order to account for the minimum time \( \alpha \) for the satisfaction of \( \varphi_2 \). Unfortunately, this approach crucially affects regenerative transient analysis [37]: it is now the deterministic timer that carries memory until its elapse, in order to characterize the state distribution of the system at time \( \alpha \). Regeneration points before \( \alpha \) are thus inevitably lost, forcing the enumeration of all sequences of discrete events until \( \alpha \).

We provided a solution based on the bivariate extension of Markov renewal equations, explicitly accounting for a satisfaction interval \([\alpha, \beta]\). The result is based on the formal definition of the probability space of STPN paths, which established the theoretical relation between cylinder sets of paths and stochastic state classes [37].

Fig. 13 highlights the reduction of complexity achieved by the proposed regenerative approach. A transient analysis eliminating the lower bound \( \alpha \) through the inclusion of a deterministic transition forgoes all regeneration points occurring before \( \alpha \), forcing the enumeration of each discrete event along any feasible path within \( \alpha \) and producing the number of enumerated classes shown by the dotted line. In contrast, in the regenerative approach based on the bivariate Markov renewal equations of Eq. (8), the total number of enumerated classes follows the solid line.

6 CONCLUSIONS

The verification of an interval until operator \( \varphi_1, U^{[\alpha, \beta]} \varphi_2 \) in regenerative systems presents major challenges, both theoretical and practical, that cannot leverage existing approaches for CTMCs [12] nor established results of Markov renewal theory [18], [40].

Stochastic models with concurrent GEN timers “accumulate memory” over time: the state at time \( \alpha \) does not summarize, in general, the past evolution of the system, and the process cannot be verified independently before and after \( \alpha \), in contrast to CTMCs, in which every time instant, and thus \( \alpha \), is a regeneration point. On the other hand, the reduction to a first-passage analysis with \( \alpha = 0 \) requires the introduction of a deterministic timer in order to account for the minimum time \( \alpha \) for the satisfaction of \( \varphi_2 \). Unfortunately, this approach crucially affects regenerative transient analysis [37]: it is now the deterministic timer that carries memory until its elapse, in order to characterize the state distribution of the system at time \( \alpha \). Regeneration points before \( \alpha \) are thus inevitably lost, forcing the enumeration of all sequences of discrete events until \( \alpha \).

We provided a solution based on the bivariate extension of Markov renewal equations, explicitly accounting for a satisfaction interval \([\alpha, \beta]\). The result is based on the formal definition of the probability space of STPN paths, which established the theoretical relation between cylinder sets of paths and stochastic state classes [37].

Fig. 13 highlights the reduction of complexity achieved by the proposed regenerative approach. A transient analysis eliminating the lower bound \( \alpha \) through the inclusion of a deterministic transition forgoes all regeneration points occurring before \( \alpha \), forcing the enumeration of each discrete event along any feasible path within \( \alpha \) and producing the number of enumerated classes shown by the dotted line. In contrast, in the regenerative approach based on the bivariate Markov renewal equations of Eq. (8), the total number of enumerated classes follows the solid line.

6 CONCLUSIONS

The verification of an interval until operator \( \varphi_1, U^{[\alpha, \beta]} \varphi_2 \) in regenerative systems presents major challenges, both theoretical and practical, that cannot leverage existing approaches for CTMCs [12] nor established results of Markov renewal theory [18], [40].

Stochastic models with concurrent GEN timers “accumulate memory” over time: the state at time \( \alpha \) does not summarize, in general, the past evolution of the system, and the process cannot be verified independently before and after \( \alpha \), in contrast to CTMCs, in which every time instant, and thus \( \alpha \), is a regeneration point. On the other hand, the reduction to a first-passage analysis with \( \alpha = 0 \) requires the introduction of a deterministic timer in order to account for the minimum time \( \alpha \) for the satisfaction of \( \varphi_2 \). Unfortunately, this approach crucially affects regenerative transient analysis [37]: it is now the deterministic timer that carries memory until its elapse, in order to characterize the state distribution of the system at time \( \alpha \). Regeneration points before \( \alpha \) are thus inevitably lost, forcing the enumeration of all sequences of discrete events until \( \alpha \).

We provided a solution based on the bivariate extension of Markov renewal equations, explicitly accounting for a satisfaction interval \([\alpha, \beta]\). The result is based on the formal definition of the probability space of STPN paths, which established the theoretical relation between cylinder sets of paths and stochastic state classes [37].

Fig. 13 highlights the reduction of complexity achieved by the proposed regenerative approach. A transient analysis eliminating the lower bound \( \alpha \) through the inclusion of a deterministic transition forgoes all regeneration points occurring before \( \alpha \), forcing the enumeration of each discrete event along any feasible path within \( \alpha \) and producing the number of enumerated classes shown by the dotted line. In contrast, in the regenerative approach based on the bivariate Markov renewal equations of Eq. (8), the total number of enumerated classes follows the solid line.

6 CONCLUSIONS

The verification of an interval until operator \( \varphi_1, U^{[\alpha, \beta]} \varphi_2 \) in regenerative systems presents major challenges, both theoretical and practical, that cannot leverage existing approaches for CTMCs [12] nor established results of Markov renewal theory [18], [40].
ablilistic model of Fischer’s mutual exclusion protocol, a typical benchmark for real-time model checking. Notably, quantitative properties were analyzed in a stochastic model that guarantees the correctness of the protocol due to generally distributed timers with bounded supports. The construction of these results highlighted important problems of probabilistic model checking of transient properties in regenerative systems, which can serve as the basis for further analysis techniques.

References

Marco Paolieri is a research scientist at the University of Florence, where he received his Ph.D. in Computer Science, Systems and Telecommunications (2015) and his B.S. and M.S. in Computer Engineering (2011). His research interests focus on stochastic modeling and quantitative evaluation of performance and reliability in concurrent and distributed systems.

Enrico Vicario (IEEE CS Member) is full professor of computer science and engineering at the University of Florence, since 2002. His scientific activity is focused on model-based methods for correctness verification and quantitative evaluation of concurrent systems with non-deterministic or stochastic temporal parameters. He also carries out a relevant activity of experimentation and technology transfer in software architectures and software development methods.

András Horváth was born in 1974 in Budapest where he received the M.Sc. degree in Computer Science from the University of Technology and Economics. From 1998 to 2002 he was a Ph.D. student supervised by Miklós Telek at the same university. From 2003 he is at the University of Turin (Italy). His research interests are in the area of stochastic processes including performance analysis of Markovian and non-Markovian models with application to communication networks and manufacturing systems.
APPENDIX A

CALCULUS OF STOCHASTIC STATE CLASSES

The succession relation τage among stochastic state classes can be enumerated through symbolic operations on the support and probability density function (PDF) of vectors of random variables. While a complete presentation is in [30], [31], [37], we report the main steps required by the calculus.

A stochastic state class Σ = (m, D, f (τage, x)) includes the marking m ∈ N^P, and the joint PDF f (τage, x) and support D ⊆ R_n+1 of the random vector (τage, x), where:

- the random variable τage encodes the negation of the time of the previous firing;
- the components of τ = (τ₁, ..., τ_n) encode the times to fire of enabled transitions E(m).

As detailed in Remark 1, the initial stochastic state class given by a regeneration condition (m, d) can be constructed for an STPN (P, T, A⁻, A⁺, B, U, EFT, LFT, F, W) from the marking m, the enabling times d, and the sampling PDF ft of each enabled transition t ∈ E(m), where ft is the PDF of the distribution F(t). Initially, the components of the vector (τage, τ) are independent random variables and their joint PDF f (τage, x) is in product form.

Given a stochastic state class Σ = (m, D, f (τage, x)), a transition γ ∈ E(m) and a firing interval I, the probability µ that γ fires in Σ at some time in I can be computed as

\[ µ = \int_{D} \int_{\tau} W(t) \sum_{i : x_i = 1} W(t) f (τage, x) dx_{age} dx \]  (15)

where (without loss of generality) enabled transitions correspond to the times to fire τ₁, ..., τ_n are indicated as t₁, ..., t_n with t = γ, and D is the set of values for (τage, x) such that the time to fire of t₁ is minimum, and the time of the next firing (obtained increasing τage by the sojourn time τ₁) is contained in I. By integrating the PDF f (τage, x) over this set of values, we obtain the succession probability µ. The ratio of weights in Eq. (15) accounts for the case in which τ₁ is deterministic and other deterministic times to fire attain the minimum value: according to the semantics of STPNs, the probability that t₁ is selected is W(t₁) / Σ W(t₁).

The unique successor class Σ' such that Σ = Σ' can be derived as follows. The marking m' is computed by removing one token from each input place of t₁, adding one token to each output place of t₁, and applying the update function U(t₁) to the resulting marking. The support D' and PDF f (τage, x) of the vector of times to fire (τage, x) immediately after the firing of t₁ (and conditioned on this event) are computed in four steps.

Precedence conditioning. The assumption that t₁ fires at some time in I before any other transition yields a new random vector (τage, x) distributed over D' according to f (τage, x) = f (τage, x) / µ.

Time advancement and marginalization. When t₁ fires, τage and the times to fire τ₂, ..., τ_n of enabled transitions are reduced by the random variable τage associated with t₁. The time to fire of t₁ is eliminated from the joint PDF f (τage, x) and from its support D by integrating the joint PDF over all values of τage. The PDF of the resulting random vector (τage, x) with τage = τage - τ₁ and x = x - (τ₂ - τ₁, ..., τ_n - τ₁) is

\[ f (τage, x) = \int_{L_n} f (τage, x) dx \]  (16)

where U_n (x, ..., x) and L_n (x, ..., x) are the maximum and minimum value of x such that (x, ..., x) ∈ D, respectively. As detailed in [30], U_n and L_n are piecewise functions; as a consequence, the PDF f (τage, x) is a piecewise function defined on a partitioning of its support D = \{ (x, ..., x) ∈ R^n | ∃ x ∈ R : (x, ..., x) ∈ D \}.

Disabling. Times to fire associated with transitions disabled during the firing (i.e., after removing tokens from input places of t₁, or after adding tokens to output places of t₁, or after updating the function B(t₁)) are eliminated one at a time from the vector (τage, x) by integrating the PDF f (τage, x) over all of their values in D. For example, the disabling of transition t₂ yields the random vector (τage, x) with x = (τ₁, ..., τ_n) that has PDF f (τage, x) = \int_{L_n} f (τage, x) dx. With support D = \{ (x, ..., x) ∈ R^n | ∃ x ∈ R : (x, ..., x) ∈ D \}.

Newly enabling. Times to fire of transitions newly enabled after the firing (i.e., enabled by the new marking m', but not by m or by some intermediate marking) are added one at a time as independent random components to the vector (τage, x). For example, the newly enabling of transition tₙ₁ yields the random variable (τage, x) that has PDF f (τage, x) = \int_{L_n} f (τage, x) dx. With support D = \{ (x, ..., x) ∈ R^n | ∃ x ∈ R : (x, ..., x) ∈ D \}.

Example 5. For the STPN of Fig. 1a, the successor of Σ₀ in Fig. 3 through the firing of transition fail (without constraints on the firing time) is computed as follows. The new marking m' failed is obtained from m' free operational by removing one token from the input place operational and adding one token to the output place failed. The integral of the PDF f (τage, x) = (age, arrival, fail) = 0.1 (age) exp(-0.1 fail) over D = \{ (age, arrival, fail) ∈ R³ | age = 0, 0 ≤ arrival ≤ 2, fail ≤ 0.1 \} gives µ = 1 + 10 (e^-0.2 - e^-0.1) ≈ 0.1389 and f (τage, x) = (age, arrival, fail) = 0.7198 (age) exp(-0.1 fail). Time advancement and marginalization of timer fail give f (τage, x) = (age, arrival) = \int_{D} 0.7198 (age + fail) exp(-0.1 fail) d(age + fail) = 0.7198 exp(0.1 age) and

\[ D = \{ (age, arrival) ∈ R² | -2 ≤ age ≤ 0, \]  (17)

0 ≤ arrival ≤ 2, -2 ≤ age - arrival ≤ -1 \}.

No other transition is disabled thus f (τage, x) = (age, arrival) = (age, arrival) and D = D', while restart (uniformly distributed over [1, 2]) is newly enabled after the firing, resulting in f (τage, x) = (age, arrival, restart) = (age, arrival, restart) and D = D × [1, 2] for the final vector of times to fire (τage, x) = (age, arrival, restart).