Probabilistic Duration Calculus for Continuous Time

Dang Van Hung[1] and Zhou Chaochen[2]

The United Nations University
International Institute for Software Technology
UNU/IIST, P.O.Box 3058 Macau

Keywords: Dependability; Real Time Systems; Duration Calculus; Probabilistic Duration Calculus; Probabilistic Automata; Stochastic Processes

Abstract. This paper deals with dependability of imperfect implementations concerning given requirements. The requirements are assumed to be written as formulas in Duration Calculus. Implementations are modelled by continuous semi-Markov processes with finite state space, which are expressed in the paper as finite automata with stochastic delays of state transitions. A probabilistic model for Duration Calculus formulas is introduced, so that the satisfaction probabilities of Duration Calculus formulas with respect to semi-Markov processes can be defined, reasoned about and calculated through a set of axioms and rules of the model.

1. Introduction

Functional requirements and dependability requirements are two kinds of top-level requirements on the design of computing systems which include software embedded hard real-time systems. The functional requirements express what a system must be able to do and what it must not do. The dependability requirements express that the probability for undesirable but unavoidable behaviour of a system must be below a certain limit.
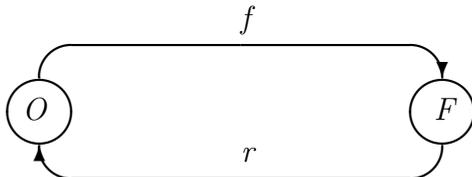
For the specification and verification of functional requirements for software

[1] On leave from Institute of Information Technology, NCNST, Hanoi, Vietnam.
[2] On leave from Software Institute, Academy Sinica, Beijing, P.R. China.

Fig. 1. A system model

embedded hard real-time systems, many formal tools have been proposed, such as Real-Time Logics [AlH89], Timed CSP [Sch91], Metric Temporal Logics [Koy90], timed transition systems [HMP92], etc. Among them, Duration Calculus (DC) [ZHR92] has proved to be a promising tool. One of the main features of DC is that it can handle continuous time without explicitly referring to absolute time. For dealing with the dependability requirements, the methods based on principles from the fields of reliability engineering [Joh90] are used. The mathematical foundation of these methods is the theory of probability and stochastic processes (e.g. Markov processes). Clearly, a combined calculus capable of coping with both kinds of requirements would be desirable. Some attempts have been made to extend DC to handle dependability requirements resulting in a probabilistic DC [LSRZ94, LSRZ92]. However, these attempts are only for discrete time. The model of implementations used in [LSRZ94, LSRZ92] is based on probabilistic automata, in which transitions (events, actions) take place at discrete time points represented by integers. The discrete time model is not suitable for many practical applications because physical components work in continuous time. As inspired by [SNH93], the present paper makes another attempt in this direction. It uses probabilistic automata with transitions occurring in continuous time to model implementations, and then establishes a probabilistic DC for continuous time.

To illustrate our approach, let us consider an example. A simple and abstract model of a system (computer system, telephone system, etc.) can be an automaton consisting of two states: the *operating* state O and the *failure* state F. Initially, the system is in state O. The system will be transited to state F when failure occurs, which is modelled by the transition f from O to F. The system can return to state O again when it is repaired, which is modelled by the transition r from F to O (see Figure 1).

When the system enters state O, the transition f is enabled and happens randomly, and therefore the delay time of f, denoted by t_f, is a random variable (or stochastic variable specifically). Similarly for the transition r. However the delay time of r may be "less" random than the delay time of f, since system repair may be more predictable than system failure. In order to characterise this randomness, according to the probability theory, we can assume a function of t and Δt, denoted

$$\mathcal{P}[t < t_f \le t + \Delta t],$$

defines the probability of an occurrence of f in the time period of $(\tau+t, \tau+t+\Delta t]$, under the condition that the system enters (or begins with) the state O at time τ. Suppose that

$$\lim_{\Delta t \to 0} \mathcal{P}[t < t_f \le t + \Delta t]/\Delta t = p_f(t),$$

then for a small Δt, we have $\mathcal{P}[t < t_f \leq t + \Delta t] \approx p_f(t)\Delta t$. In probability theory, the function $p_f(t)$ is called the probability density function of the stochastic variable t_f. From the density function $p_f(t)$ we can calculate the probability that the transition f occurs in $(\tau + a, \tau + b]$ as

$$\mathcal{P}[a < t_f \leq b] = \int_a^b p_f(t)dt.$$

Thus, in an automaton, we associate with each transition a probability density function characterising the randomness of its occurrence at each moment of time after it becomes enabled. In reliability theory, the popular probability density function for failure transition f is taken to be $\lambda e^{-\lambda t}$ (known as exponential distribution [Joh90]), where λ is called the failure rate, since in this case

$$
\begin{array}{rcl}
\mathcal{P}[0 < t_f \leq \Delta t] & = & \lambda \int_0^{\Delta t} e^{-\lambda t}dt \\
& = & 1 - e^{-\lambda \Delta t} \\
& = & 1 - 1 + \lambda \Delta t - (\lambda^2(\Delta t)^2)/2 + \ldots \\
& \approx & \lambda \Delta t.
\end{array}
$$

There are many well-known probabilistic distributions in the literature which can characterise various stochastic variables.

In the previous paragraph, we have actually assumed that $\mathcal{P}[t < t_f \leq t + \Delta t]$ is independent of system history and also of the time τ at which f becomes enabled, but depends only upon t, the length of time since f became enabled. This assumption simplifies the model, and defines a so-called semi-Markov process (see e.g. [Whi80]).

The untimed behaviour of the system in Figure 1 can be described by transition sequences such as fr, frf, $frfr$, etc. In order to represent real-time system behaviour, we use transition sequences with time stamps, which record transition delay time. We write, for example, $(f, t_1)(r, t_2)$ to mean two consecutive transitions f and r with delay times t_1 and t_2 respectively. It represents a behaviour of the system in which the system starts in state O at time 0, stays in state O until making transition f at time t_1, and then stays in state F until making transition r at time $t_1 + t_2$. Let $h = t_1 + t_2$. Then h is the completion time of the timed transition sequence. (If $h < t$, by saying that the timed transition sequence $(f, t_1)(r, t_2)$ is a behaviour of the system at time t, we mean additionally that the system makes no transitions for a period of $(h, t]$.) Then, h is also a stochastic variable and, from the probability theory, the probability density function of the transition sequence fr is

$$p_{fr}(h) = \int_0^h p_f(t_1)p_r(h - t_1)dt_1$$

where $p_f(t)$ is the density function of f and $p_r(t)$ is the density function of r. In fact,

$$p_f(t_1)p_r(h - t_1)$$

is the probability density of the occurrence of r at h on the condition that f occurs at t_1. $p_{fr}(h)$ defines the probability density of the transition sequence fr with completion time h. Similarly, we can derive the probability density function of an arbitrary transition sequence of the system.

After deriving the density function of system behaviour, we can consider the

satisfaction probability of a system requirement. Following the previous example, a requirement of the system in Figure 1 may be that in the period $[0, t]$ the total time that the system is in state F must be less than 5 percent of t. The behaviour $(f, t_1)(r, t_2)$ satisfies this requirement iff

$$t_1 + t_2 < t \quad \text{and} \quad t_2 < t/20,$$

and the behaviour $(f, t_1)(r, t_2)(f, t_3)(r, t_4)$ satisfies the requirement at t iff

$$t_1 + t_2 + t_3 + t_4 < t \quad \text{and} \quad t_2 + t_4 < t/20.$$

The satisfaction probability of the requirement can be calculated by integrating the probabilities of the system behaviours which satisfy the requirement.

In the following sections, we elaborate the ideas listed above. We define in the next section finite automata with stochastic delays of state transitions which model imperfect implementations of systems, and introduce a probability measure on the set of system behaviours to establish a probability space. In the third section we give a brief summary of DC. Since behaviours of finite automata with stochastic delays of transitions correspond to semi-Markov processes with finite state space in continuous time, we can easily define the probability that a system satisfies a DC formula in a interval of time $[0, t]$. The definition of satisfaction probability of DC formulas is given in the fourth section.

Once the definition is given, one can deduce properties concerning satisfaction probabilities of DC formulas. We establish a formal calculus to formalise property deductions in the fifth section. With the calculus the satisfaction probabilities of DC formulas can be reasoned about, estimated or calculated formally. The calculus is for continuous time, but it shares some axioms and rules with the probabilistic DC presented in [LSRZ94, LSRZ92] for discrete time.

The sixth section is devoted to an example, which uses (generalised) exponential and normal distributions to model a gas burner. We apply the calculus to reasoning about its dependability.

2. Continuous time probabilistic automata

In this section, we give a probabilistic model for analysing system dependability. We introduce finite probabilistic automata with stochastic delays of state transitions, and call them continuous time probabilistic automata.

Definition 2.1. A continuous time probabilistic automaton is a tuple $M = (S, A, s_0, p_A, q_A)$, where

1. S is a finite set of states,
2. A is a finite set of transitions, $A \subseteq (S \times S) \setminus \{(s, s) \mid s \in S\}$ (here we reject idle transitions, and therefore assume $(s, s) \notin A$ for all $s \in S$),
3. $s_0 \in S$ is the initial state of M,
4. p_A is an indexed set of probability density functions:

$$p_A = \{p_a(t) \mid a \in A\},$$

5. q_A is an indexed set of probabilities,

$$q_A = \{q_a \mid a \in A\}$$

which satisfies the condition below.

Let $a = (s, s') \in A$ and $A_s = \{(s, s') \in A | s' \in S\}$. As mentioned in the introduction, our intention of introducing $p_a(t)$ is to specify that if M enters the state s at an instant τ of time, then the probability density that the transition a occurs at $\tau + t$ (delay-time of a is t) and causes M to change to the state s' is $p_a(t)$ independent of τ, given that this transition is chosen to occur in the case that there is more than one transition enabled in s. The probability that a is chosen to occur when M is in s is given by q_a. Thus, we require that $\sum_{a \in A_s} q_a = 1$ for $s \in S$ which satisfies $A_s \neq \emptyset$.

From the model, it follows that if M enters the state s at time τ, then the fact that M remains in the state s during $(\tau, \tau + t]$ is equivalent to the fact that no transition in A_s occurs in $(\tau, \tau + t]$. Therefore, the probability that M is still in the state s during $(\tau, \tau + t]$ given that M enters the state s at time τ is

$$u_s(t) = 1 - \sum_{a \in A_s} q_a \int_0^t p_a(t) dt$$

independent of τ, where $q_a \int_0^t p_a(t) dt$ is the probability that a is chosen and occurs within $(\tau, \tau + t]$. Clearly, when $A_s = \emptyset$, $u_s(t) = 1$ for all t.

Exponential distributions form an interesting special case of probabilistic automata. In this case, for $s \in S$, there is $\lambda_a > 0$ assigned to each $a \in A_s$ such that

$$p_a(t) = \left(\sum_{a' \in A_s} \lambda_{a'} \right) e^{-t \sum_{a' \in A_s} \lambda_{a'}},$$

$$q_a = \lambda_a / \left(\sum_{a' \in A_s} \lambda_{a'} \right),$$

$$u_s(t) = e^{-t \sum_{a' \in A_s} \lambda_{a'}}.$$

Then, for this case, we can prove that for all $a \in A_s$

$$p_a(t + t') = u_s(t) p_a(t').$$

Since $u_s(t)$ is the probability that M stays in state s during $[\tau, \tau + t]$ given that M enters s at time τ, the equation means that, given that M remains in s at time t, the probability of occurrence of a at t' time units later is independent of t. This property is known as the Markovian property in probability theory. In this paper, when we say that M *has the Markovian property in the state* s we means that $p_a(t + t') = u_s(t) p_a(t')$ holds for any $t, t' \geq 0$.

For convenience, for $a = (s, s') \in A$, we denote s and s' by a^- and a^+ respectively.

A behaviour of the automaton M is a sequence $\sigma = (a_1, t_1)(a_2, t_2) \ldots (a_n, t_n)$ of transitions with delay-times such that $a_1^- = s_0, a_i^- = a_{i-1}^+$ for $i = 2, 3, \ldots, n$, and $t_i > 0$ for $i = 1, 2, \ldots, n$. The projected sequence $a_1 a_2 \ldots a_n$ is the sequence of transitions of σ. The behaviour is characterised not only by the transition sequence, but also by the transition delay-times. Hence, unlike in the case of discrete time as in [LSRZ94, LSRZ92], the set of all behaviours of M is uncountable. As mentioned in the introduction to the paper, given that M starts at time 0 in state s_0, the probability density that the transition sequence $w = a_1 a_2 \ldots a_m$
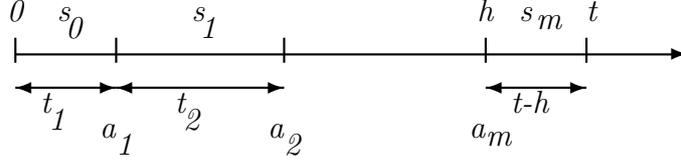
Fig. 2. A behaviour of automata

finishes exactly at time h (i.e. the last transition in the sequence takes place at time h) is

$$p_{a_1 a_2 \ldots a_m}(h) = \int_0^h p_{a_1 a_2 \ldots a_{m-1}}(t) p_{a_m}(h-t) dt$$

given that the sequence is chosen to occur.

For a behaviour σ, its prefix $(a_1, t_1)(a_2, t_2) \ldots (a_m, t_m)$ is called its prefix at t if it is the maximal prefix of σ with the property $\sum_{i=1}^m t_i < t$. It implies that until time t the behaviour σ performs the sequence of transitions $a_1 a_2 \ldots a_m$, but no more.

For a transition sequence $w = a_1 a_2 \ldots a_m$ accepted by finite automaton M and for a time $t > 0$, the set of behaviours of M having prefix at t with w being as the sequence of transitions (its projection on transitions) is denoted by $B_{w,t}$.

We can conclude that a behaviour σ of M is in $B_{w,t}$ iff it satisfies (see fig. 2):

1. w is a prefix of the transition sequence of σ,
2. if h is the occurrence time of the last transition a_m of w, then $h < t$, and
3. within $(h, t]$ there is no occurrence of transitions.

Hence, the probability $P(B_{w,t})$ that M performs a behaviour in $B_{w,t}$ can be calculated as follows (ϵ denotes the empty sequence).

$$P(B_{w,t}) = \begin{cases} u_{s_0}(t) & \text{if } w = \epsilon \\ q_w \int_0^t p_w(h) u_{a_m^+}(t-h) dh & \text{otherwise,} \end{cases}$$

where for $w \neq \epsilon$, $q_w = q_{a_1} \ldots q_{a_m}$ is the probability that w is chosen to occur, $p_w(h) = p_{a_1 a_2 \ldots a_m}(h)$ is the probability density that w finishes at h, given that it is chosen to occur, and $u_{a_m^+}(t-h)$ is the probability that no transition occurs within $(h, t]$ given that w occurs at h. $P(B_{w,t})$ can be written in the following form

$$P(B_{w,t}) = \int_{\substack{\sum_{i=1}^m t_i < t, \\ \forall i : t_i > 0}} \left(\prod_{i=1}^m (q_{a_i} p_{a_i}(t_i)) \right) u_{a_m^+} \left(t - \sum_{i=1}^m t_i \right) dt_1 \ldots dt_m .$$

Notice that, given t, the sets $B_{w,t}$ with different w are disjoint, and for any behaviour σ of M, there exists w such that σ is in $B_{w,t}$. This means that the set X of all behaviours of M is

$$X = \bigcup_{w \in W} B_{w,t} ,$$

where W is the set of all transition sequences of M (W is the regular language recognised by the finite automaton M, with S as the set of final states. Hence, W is a finite or countable set). It is expected that
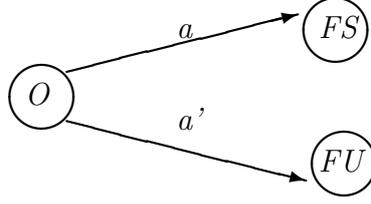
Fig. 3. A probabilistic automaton

$$P(X) = \sum_{w \in W} P(B_{w,t}) = 1$$

for any time instant t. This is shown in the following theorem of which a proof is given in the Appendix.

Theorem 2.1. For any $t > 0$, $P(X) = 1$.

From Theorem 2.1, for any $t > 0$, the countable family $\{B_{w,t} | w \in W\}$ forms a complete, disjoint base of events. Therefore, given a subset R of behaviours of M (say, R is the set of behaviours of M satisfying some requirement), the probability that a behaviour belongs to R can be calculated as

$$P(R) = \sum_{w \in W} P(B_{w,t} \cap R)$$

where $P(B_{w,t} \cap R)$ denotes the probability that a behaviour in $B_{w,t}$ belongs to R.

Example 2.1. The following simple example, taken from [Joh90], illustrates our notions. Let M be the automaton represented by the state transition graph in Figure 3. M has three states: O (operation), FS (failed safe) and FU (failed unsafe), and two transitions: $a = (O, FS)$ and $a' = (O, FU)$. Let

$$p_a(t) = p_{a'}(t) = \lambda e^{-\lambda t}, \ q_a = C, \ q_{a'} = (1 - C),$$

where $0 \leq C \leq 1$. Then we can calculate

$$u_O(t) = e^{-\lambda t}, \ u_{FS}(t) = u_{FU}(t) = 1, \ W = \{\epsilon, a, a'\}.$$

and

$$
\begin{aligned}
P(B_{\epsilon,t}) &= u_o(t) = e^{-\lambda t} \\
P(B_{a,t}) &= \int_0^t \lambda C e^{-\lambda h} dh = C(1 - e^{-\lambda t}) \\
P(B_{a',t}) &= \int_0^t \lambda (1 - C) e^{-\lambda h} dh = (1 - C)(1 - e^{-\lambda t}).
\end{aligned}
$$

Therefore the probability of the fact "FU is absent up to t" is

$$P(B_{\epsilon,t}) + P(B_{a,t}) = e^{-\lambda t} + C(1 - e^{-\lambda t}),$$

which is the same as in [Joh90].

In order to define the probability that the behaviours of a system satisfy a given requirement, where requirements are written as Duration Calculus (DC) formulas, the following section presents a brief overview of DC.

3. Duration Calculus: a brief summary

In this section, we give a brief summary of DC and its application to specification of real-time systems. For more details, readers are referred to [ZHR92].

Time in DC is the set R^+ of non-negative real numbers. For $t, t' \in R^+, t \leq t', [t, t']$ denotes the time interval from t to t'.

We assume a finite set E of Boolean variables called primitive states. E includes the Boolean constants 0 and 1 denoting *false* and *true* respectively. States, denoted by P, Q, P_1, Q_1, etc., consist of expressions formed by the following rules:

1. Each primitive state $P \in E$ is a state.
2. If P and Q are states, then so are $\neg P, (P \wedge Q), (P \vee Q), (P \Rightarrow Q), (P \Leftrightarrow Q)$.

A primitive state P is interpreted as a function $I(P) : R^+ \to \{0, 1\}$. $I(P)(t) = 1$ means that state P is present at time instant t, and $I(P)(t) = 0$ means that state P is not present at time instant t. We assume that a state has finite variability in a finite time interval. A composite state is interpreted as a function which is defined by the interpretations for the primitive states and Boolean operators.

For an arbitrary state P, its duration is denoted by $\int P$. Given an interpretation I of states and an interval, duration $\int P$ is interpreted as the accumulated length of time within the interval at which P is present. So for an arbitrary interval $[t, t']$, the interpretation $I(\int P)([t, t'])$ is defined as $\int_t^{t'} I(P)(t)dt$. Therefore, $\int 1$ always gives the length of the intervals and is denoted by ℓ.

The set of primitive duration terms consists of variables over the set R^+ of non-negative real numbers and durations of states. In this paper, a duration term is defined either as a primitive term or as a linear combination of primitive terms.

A primitive duration formula is an expression formed from terms by using the usual relational operations on the reals, such as equality $=$ and inequality $<$. A duration formula is either a primitive formula or an expression formed from formulas by using the logical operators $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$, and the chop ; (see below) and quantifiers $\forall, \exists$ applied to variables ranging over R^+.

A duration formula D is satisfied by an interpretation I in an interval $[t', t'']$ just when it evaluates to true for that interpretation over that time interval. This is written as

$$I, [t', t''] \models D,$$

where I assigns every primitive state a finitely variable function from R^+ to $\{0,1\}$, and $[t', t'']$ decides the observation window. So the satisfaction relation has nothing to do with the values of the primitive state assigned by I outside the observation window $[t', t'']$. That is, for interpretations I and I', if

$$I(P)(t) = I'(P)(t), \; t' \leq t \leq t''$$

holds for all primitive states in D, then we can prove

$$I, [t', t''] \models D \text{ iff } I', [t', t''] \models D.$$

Given an interpretation I, the chop-formula $D_1; D_2$ is true for $[t', t'']$ if there exists a t such that $t' \leq t \leq t''$ and D_1 and D_2 are true for $[t', t]$ and $[t, t'']$ respectively.

We give now shorthands for some duration formulas which are often used. For an arbitrary state P, $\lceil P \rceil$ stands for $(\int P = \ell) \wedge (l > 0)$. This means that

P holds everywhere in a non-point interval. We use $\lceil\ \rceil$ to denote the predicate which is true only for point intervals. Modalities $\Diamond, \Box$ are defined as: $\Diamond D = true; D; true,\ \Box D = \neg\Diamond\neg D$. This means that $\Diamond D$ is true for an interval iff D holds for some subinterval of it, and $\Box D$ is true for an interval iff D holds for all subintervals of it.

DC has a set of axioms about states and rules which is sound and (relatively) complete [HaZ91]. These axioms and rules are listed below.

DA 1. $\int 0 = 0$.

DA 2. For an arbitrary state P, $\int P \geq 0$.

The additivity rule of durations is described as

DA 3. For arbitrary states P and Q,

$$\int P + \int Q = \int(P \vee Q) + \int(P \wedge Q).$$

The following theorem is provable from these axioms.

Theorem 3.1. For an arbitrary state P,

1. $\int P + \int \neg P = \ell$,
2. $\int P \leq \ell$.

The basic axiom relating chop (;) and duration ($\int$) states that the duration of a state in an interval is the sum of its durations in subintervals constituting a partition of the interval.

DA 4. Let P be a state and r, s non-negative real numbers.

$$(\int P = r + s) \Leftrightarrow (\int P = r; \int P = s).$$

From this axiom, we have

Theorem 3.2. For a state P,

$$\lceil P \rceil \Leftrightarrow \lceil P \rceil; \lceil P \rceil.$$

The following induction rule extends a hypothesis over adjacent subintervals. It relies on the finite variability of states and on the finiteness of the intervals, that any interval can be split into a finite alternation of states P and $\neg P$.

DA 5. Let X denote a formula letter occurring in the formula $R(X)$, and let P be a state.

1. If $R(\lceil\ \rceil)$ holds, and if $R(X \vee (\lceil P \rceil; X) \vee (\lceil \neg P \rceil; X))$ is provable from $R(X)$ then $R(true)$ holds.
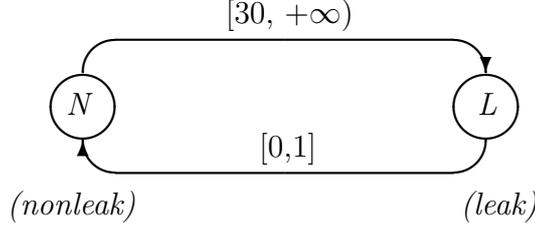
This rule can be used to prove that a proper interval ends with either P or $\neg P$.

Theorem 3.3. For a state P

$$(true; \lceil P \rceil) \vee (true; \lceil \neg P \rceil) \vee \lceil\ \rceil.$$

As induction hypothesis, the proof uses as $R(X)$ the formula

$$X \Rightarrow (true; \lceil P \rceil) \vee (true; \lceil \neg P \rceil) \vee \lceil\ \rceil.$$

$$[30, +\infty)$$

(nonleak)   *(leak)*

Fig. 4. A simple gas burner

To conclude this section, we give some examples of using DC in specifying real-time system. The requirement of the system (Figure 1) mentioned in the introduction of the paper can be written as $\int F \leq 1/20\ell$. Another example is a simple gas burner taken from [ZHR92]. One of the time critical requirements of a gas burner is specified by a DC formula denoted by **Req-1**, defined as

Req-1 $\qquad\qquad\qquad \ell > 60s \Rightarrow (20 * \int leak \leq \ell).$

This says that if the interval over which the system is observed is at least 1 min, the proportion of time spent in the leak state is not more than one-twentieth of the elapsed time. The requirement is refined into two design decisions

Des-1 $\qquad\qquad\qquad \Box(\lceil leak \rceil \Rightarrow \ell \leq 1s),$

Des-2 $\qquad\qquad\qquad \Box(\lceil leak \rceil; \lceil \neg leak \rceil; \lceil leak \rceil \Rightarrow \ell \geq 30s).$

Des-1 says that any leak state must be detected and stopped within 1s, and **Des-2** says that leak must be separated by at least 30s. The correctness of the design is reasoned about by proving the implication

$$\textbf{Des-1} \wedge \textbf{Des-2} \Rightarrow \textbf{Req-1}.$$

A timed automaton representing the design is shown in Figure 4.

In this timed automaton, each transition has a range of delay-time. For example, the transition from state *non-leak* (N) to *leak* (L) has allowable delay-time ranging from 30 to $+\infty$, the transition from state *leak* to *non-leak* has allowable delay-time ranging from 0 to 1. Every behaviour of the automaton which has allowable delay-times of its transitions satisfies **Des-1** $\wedge$ **Des-2**, and thus satisfies **Req-1**.

Now, suppose that in implementation, the delay-times of transitions are stochastic variables with the probability density functions

$$p_{(N,L)}(t) = \begin{cases} \lambda e^{-\lambda(t-30)} & \text{if } t \geq 30, \\ 0 & \text{otherwise,} \end{cases}$$

$$p_{(L,N)}(t) = \frac{a}{\sqrt{2\pi\delta}} e^{-\frac{(t-0.5)^2}{2\delta}},$$

where

$$a = \frac{1}{1 - \Phi(-0.5/\sqrt{\delta})},$$

$$\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{t^2}{2}} dt.$$

Thus, $p_{(L,N)}(t)$ is approximated by the normal density function with mean value 0.5 and deviation δ, which says that the average leak period is 0.5 second and that the average difference between the period of a leak and 0.5 second (the
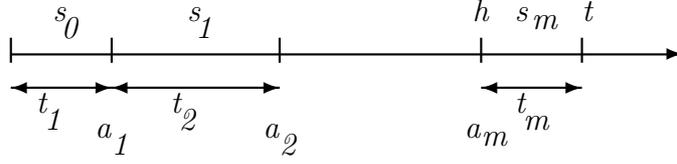
Fig. 5. DC Interpretation by a behaviour

average leak period) is δ. The density function $p_{(N,L)}(t)$ ensures that whenever the system enters the state *non-leak*, it remain in *non-leak* for at least 30 seconds (e.g. by ignoring heat requests, if any, during this time). After 30 seconds from entering the state *non-leak*, the rate of becoming *leak* for the system is a constant, namely λ.

4. Satisfaction probability of DC formulas

Given a continuous time probabilistic automaton $M = (S, A, s_0, p_A, q_A)$, and a DC formula D over state variables in S, we are going to define the probability for the fact that M satisfies D in an interval $[0, t]$ of time.

For a behaviour $\sigma = (a_1, t_1)(a_2, t_2) \ldots (a_m, t_m)$, the interpretation I_σ of state variables defined by σ for DC formulas is as follows (see Figure 5).

$$I_\sigma(s)(t) = true \quad \Leftrightarrow$$

$$\left(\exists i.1 \le i \le m.a_i^- = s \wedge \sum_{j=1}^{i-1} t_j \le t < \sum_{j=1}^{i} t_j \right)$$

$$\vee \quad \left(a_m^+ = s \wedge \sum_{j=1}^{m} t_j \le t \right).$$

We say that D is satisfied by σ in $[0, t]$ iff $I_\sigma, [0, t] \models D$. Thus, if σ satisfies D in $[0, t]$, then every behaviour for which the interpretation coincides with I_σ up to the time t also satisfies D in $[0, t]$. In other words, the satisfaction of D by σ in $[0, t]$ depends only on its history up to time t. Let $w = a_1 a_2 \ldots a_m \in W$, we define

$$V_{w,t}(D) = \left\{ (t_1, t_2, \ldots, t_m) \mid \begin{array}{l} (\sum_{j=1}^{m} t_j < t) \text{and } (\forall i \le m : t_i \ge 0) \\ \text{and } I_{(a_1, t_1) \ldots (a_m, t_m)}, [0, t] \models D \end{array} \right\}.$$

Lemma 4.1. For all $w \in W$ and $t > 0$,

$$\mu_w(D)(t) = \int_{V_{w,t}(D)} \left(\prod_{i=1}^{m} (q_{a_i} p_{a_i}(t_i)) \right) u_{a_m^+} \left(t - \sum_{i=1}^{m} t_i \right) dt_1 \ldots dt_m$$

is well defined and

$$\mu_w(D)(t) \le P(B_{w,t}).$$

Proof. By induction on the structure of DC formulas, it can be shown that for all $w \in W$ and $t > 0$, there is a finite number of sets of linear equations and linear inequalities such that $(t_1, t_2, \ldots, t_m) \in V_{w,t}(D)$ if and only if $(t_1, t_2, \ldots, t_m)$

satisfies one of them. Thus, $V_{w,t}(D)$ is a finite union of polyhedra in the m-dimensional Euclidean space. Furthermore, by the definition of $V_{w,t}(D)$,

$$V_{w,t}(D) \subseteq \{(t_1, t_2, \ldots, t_m) | \, (\forall i \leq m : t_i \geq 0) \wedge \sum_{i=1}^{m} t_i < t\}.$$

From the definition of the Riemann integral and the properties of density functions, it follows that $\mu_{w,t}(D)$ is defined for all DC formulas D, and $\mu_{w,t}(D) \leq P(B_{w,t})$. The details of the proof are omitted. $\square$

By the definition, $\mu_{w,t}(D)$ is the probability that a behaviour in $B_{w,t}$ satisfies the DC formula D in the interval $[0, t]$. From the remarks at the end of Section 2, we define the satisfaction probability of a DC formula D by M as follows.

Definition 4.1. For a DC formula D, the probability $\mu(D)(t)$ that M satisfies D in $[0, t]$ is defined as

$$\mu(D)(t) = \sum_{w \in W} \mu_{w,t}(D).$$

Notice that by Lemma 4.1 and Theorem 2.1, $\mu(D)(t)$ is always defined (i.e. Definition 4.1 is meaningful), and

Theorem 4.1. $\mu(D)(t) \leq \sum_{w \in W} P(B_{w,t}) = 1$ for all DC formulas D and for all $t \geq 0$.

For the continuous time probabilistic automaton modelling the implementation of the simple gas burner in the last section, let, for example,

$$D = (\lceil N \rceil \wedge \ell \geq 30; \lceil L \rceil \wedge \ell \leq 1; \lceil N \rceil),$$

and

$$D' = \lceil N \rceil.$$

Then, $\mu_{w,t}(D) = 0$ for all $w \neq (N,L)(L,N)$, and $\mu_{w,t}(D') = 0$ for all $w \neq \epsilon$. Thus, the probability that the system satisfies D in $[0, 31]$ is

$$
\begin{aligned}
\mu(D)(31) &= \mu_{(N,L)(L,N),31}(D) \\
&= \int_{\substack{t_1 \geq 30, \\ 0 < t_2 \leq 1, \\ t_1 + t_2 \leq 31}} p_{(N,L)}(t_1) p_{(L,N)}(t_2) u_N(t - t_1 - t_2) dt_1 dt_2 \\
&= \int_{\substack{t_1 \geq 30, \\ 0 < t_2 \leq 1, \\ t_1 + t_2 \leq 31}} p_{(N,L)}(t_1) p_{(L,N)}(t_2) dt_1 dt_2 \\
&\qquad (u_N(t) = 1 \text{ when } t \leq 30) \\
&= \int_0^{31} (p_{(N,L)}(t_1) \int_0^{\min(31 - t_1, 1)} p_{(L,N)}(t_2) dt_2) dt_1 \\
&= \int_{30}^{31} (p_{(N,L)}(t_1) \int_0^{31 - t_1} p_{(L,N)}(t_2) dt_2) dt_1.
\end{aligned}
$$

The probability that the system satisfies D' is $\mu(D')(t) = \mu_{\epsilon,t}(D') = u_N(t)$, which is 1 if $t \leq 30$, and is $e^{-\lambda(t-30)}$ otherwise.

Here, we should note that, since DC formulas do not refer to absolute time, the probability $\mu(D)$ depends only on the duration of time that M is in operation and is independent of the absolute time when the system starts. In other words, $\mu(D)(t)$ is the probability that D is satisfied by M in the interval of time $[\tau, \tau+t]$ given that M starts in s_0 at time τ, and $\mu(D)(t)$ is independent of τ.

For the simplicity of our presentation, in the sequel we assume that each $(s, s') \in S \times S$ which is not a transition (i.e. $(s, s') \notin A$), where $s \neq s'$, is associated with a probability $q_{(s,s')} = 0$ and an arbitrary density function $p_{(s,s')}(t)$. From Definition 2, this assumption preserves the satisfaction probability of DC formulas.

5. Probabilistic Duration Calculus for semi-Markov models with continuous time

As mentioned in the introduction to the paper, we extend DC to handle both kinds of requirements in a uniform model. The extended calculus has $\mu_s(D)$ as additional functions, where D is a DC formula, and can calculate and reason about those additional functions, where $\mu_s(D)(t)$ denotes the satisfaction probability of D in $[0, t]$ by M, assuming that M starts in state s. To distinguish from the calculus proposed in [LSRZ94, LSRZ92], we call it Probabilistic Duration Calculus (PDC) for continuous time, or just PDC when the time is understood to be continuous from the context.

The PDC is based on DC and real analysis with additional functions $\mu_s(D)(t)$.

A *primitive formula* of PDC is an expression built from terms of function $\mu_s(D)(t)$, using relational operators, such as equal $=$ and less than $<$ with their usual meanings.

A *formula* of PDC is a primitive formula or an expression built from formulas using the first order logic operators.

As an extension, PDC includes all axioms and rules from DC for DC formulas. We present here the additional ones for PDC formulas. The soundness of our axioms and rules can be proved easily using the definitions in previous sections.

In the sequel, to avoid the heavy use of the brackets, we assume that the operator $\wedge$ binds more tightly than the operator $;$.

The Duration Calculus formula *true* is satisfied by any behaviour for any time t, and t is the length of the interval $[0, t]$.

AR 1. For the formula *true*,

$$\forall s \in S \forall t \geq 0 : \mu_s(true)(t) = \mu_s(\textstyle\int 1 = t)(t) = 1.$$

The following axiom formalises the additivity rule in probability theory.

AR 2. Let $\{D_k | k \in K\}$ be a finite or countable set of DC formulas such that $D_i \Rightarrow \neg \wedge D_j$ for all $i, j \in K$, $i \neq j$. Let D be a DC formula satisfying $D \Leftrightarrow \exists k \in K : D_k$. Then, for all $s \in S$, $t > 0$

$$\mu_s(D)(t) = \sum_{k \in K} \mu_s(D_k)(t).$$

The satisfaction probability is monotonic in the sense that

AR 3. If $D_1 \Rightarrow D_2$ holds in the duration calculus, then for all $t > 0$, $\mu(D_1)(t) \leq \mu(D_2)(t)$ holds in PDC.

The three axioms and rules given above come directly from probability theory, and the following theorem can be easily proved from them.

Theorem 5.1. For arbitrary duration formulas D, D_1, D_2 and D_3, for all $t \geq 0$, $s \in S$

1. $\mu_s(D_1 \vee D_2)(t) + \mu_s(D_1 \wedge D_2)(t) = \mu_s(D_1)(t) + \mu_s(D_2)(t)$,
2. $\mu_s(D)(t) + \mu_s(\neg D)(t) = 1$,
3. $\mu_s(false)(t) = 0$,
4. $0 \leq \mu_s(D)(t) \leq 1$,
5. If $D_1 \Leftrightarrow D_2$ in duration calculus, then $\mu_s(D_1)(t) = \mu_s(D_2)(t)$,
6. If $D_1 \wedge D_2 \Rightarrow D_3$ in duration calculus, then

$$\mu_s(D_1)(t) = 1 \Rightarrow \mu_s(D_2)(t) \leq \mu_s(D_3)(t) \,.$$

The following axioms formalise our probabilistic model. The axiom AR 4 formalises our assumption on initial states, and AR 5 formalises the meaning of the probability density functions of transitions.

AR 4. For any $s \in S$, $t \geq 0$,

$$\mu_s(\lceil s \rceil; true)(t) = 1$$

AR 5. For arbitrary states $s, s' \in S$, $s \neq s'$ such that $a = (s, s') \in A_s$ and $t > 0$, $0 \leq c \leq b < t$

$$\mu_s((\lceil s \rceil \wedge c \leq \textstyle\int 1 \leq b); (\lceil s' \rceil; true \wedge D))(t) = \int_c^b q_a p_a(h) \mu_{s'}(D)(t - h) dh.$$

From AR 4 and AR 5, we have the following theorem.

Theorem 5.2. For an arbitrary DC formula D, for $s, s' \in S$, $s \neq s'$ and for $t > 0$

1. $\mu_s(\lceil s' \rceil; true)(t) = 0$,
2. $\mu_s(\lceil s \rceil)(t) = u_s(t)$.

Proof. From our definition of interpretations of DC over the set S of states, it follows that

$$true = \lceil \; \rceil \vee \bigvee_{s' \in S} \lceil s' \rceil; true.$$

Taking into account that $(\lceil s' \rceil; true \wedge \lceil s'' \rceil; true) \Rightarrow false$ when $s' \neq s''$, from AR 2 and AR 1, we have for all $t > 0$

$$1 = \sum_{s' \in S} \mu_s(\lceil s' \rceil; true)(t) + \mu_s(\lceil \; \rceil).$$

Since $\mu_s(\lceil \; \rceil) \geq 0$ and $\mu_s(\lceil s' \rceil; true)(t) \geq 0$ by Theorem 6, from AR 4 it follows that $\mu_s(\lceil \; \rceil) = \mu_s(\lceil s' \rceil; true)(t) = 0$ when $s \neq s'$, which is the first part of the theorem.

Similarly, we have

$$\lceil s \rceil; true = \lceil s \rceil \vee (\bigvee_{s' \in S, s' \neq s} \lceil s \rceil; \lceil s' \rceil; true)$$

from which it follows, combining with AR 2, AR 5,

$$\mu_s(\lceil s \rceil; true)(t) = \mu_s(\lceil s \rceil)(t) + \sum_{s' \in S, s' \neq s} \mu_s(\lceil s \rceil; \lceil s' \rceil; true)(t)$$

$$= \mu_s(\lceil s \rceil)(t) + \sum_{a \in A_s} q_a \int_0^t p_a(h)dh.$$

This implies, by the definition of the function $u_s(t)$ and AR 4,

$$\mu_s(\lceil s \rceil)(t) = 1 - \sum_{a \in A_s} q_a \int_0^t p_a(h)dh$$

$$= u_s(t).$$

The proof is completed. $\square$

The following axiom is for the Markovian property.

AR 6. Let M have the Markovian property in a state $s' \in S$. Then, for arbitrary DC formulas D and D', for $a = (s', s'') \in A_s$, $s \neq s'$

1. $\mu_s((D \wedge (true; \lceil s' \rceil) \wedge \int 1 = t); ((\lceil s' \rceil; true) \wedge D'))(t + t') = \mu_s(D \wedge (true; \lceil s' \rceil))(t)\mu_{s'}(D')(t')$,
2. $\mu_s((D \wedge (true; \lceil s' \rceil)); \lceil s'' \rceil)(t) = \int_0^t \mu_s(D \wedge (true; \lceil s' \rceil))(h)q_a p_a(0)u_{s''}(t-h)dh.$

AR 6-1 is true, because if the Markovian property is satisfied in the state s' then the event "starting in the state s' at time t, M satisfies DC formula D' in t' time units forward" is independent of the event "starting at time 0 in the state s, M arrives in the state s' at time t with the satisfaction of D in $[0, t]$". Thus, in this case, the probability in the left hand side of AR 6-1 is the product of the probabilities listed in the right hand side. A similar reasoning applies for AR 6-2.

Since the set of behaviours satisfying formula D in a interval $[0, t]$ can be partitioned into the countable union of subsets of $B_{w,t}$, each of which represent finite variability of the states of the system in the interval $[0, t]$, we have the following induction rule. PDC Let $R(X)$ be a PDC formula, where X is a variable ranging over duration formulas. R is said to be disjunction closed, if $R(X \vee Y)$ is provable from $R(X)$ and $R(Y)$ assuming that $X \wedge Y \Leftrightarrow false$.

AR 7. Let $R(X)$ be disjunction closed.

1. If $R(\lceil \ \rceil)$ holds, and $R(X; \lceil s' \rceil)$ is provable from $R(X)$ for any $s' \in S$, then $R(true)$ holds.
2. If $R(\lceil \ \rceil)$ holds, and $R(\lceil s' \rceil; X)$ is provable from $R(X)$ for any $s' \in S$, then $R(true)$ holds.

The following theorem follows from AR 7 and the properties of the integral.

Theorem 5.3. For all $s, s', s_0 \in S$, $s \neq s'$, for $t > 0$

$$\mu_{s_0}(((true; \lceil s \rceil) \wedge \int 1 = x); (\lceil s' \rceil; true))(t) = 0.$$

Proof. From AR 5, we have for any y

$$\mu_s((\lceil s\rceil \wedge \int 1 = y); (\lceil s'\rceil; true))(t) = 0.$$

Let

$$R(X) \Leftrightarrow \forall s'' \in S : (\mu_{s''}(((\lceil s''\rceil; X; \lceil s\rceil) \wedge \int 1 = x); (\lceil s'\rceil; true))(t) = 0).$$

Clearly, by Theorems 5.1 and 5.2 and AR 3, $R(X)$ satisfies the condition AR 7 trivially. Further, by AR 1 and AR 5, for all $s'' \in S$, $s'' \neq s$

$$
\begin{aligned}
&\mu_{s''}(((\lceil s''\rceil; \lceil s\rceil) \wedge \int 1 = x); (\lceil s'\rceil; true))(t) \\
={} &\mu_{s''}((\lceil s''\rceil; \lceil s\rceil); ((\lceil s'\rceil; true) \wedge \int 1 = t - x))(t) \\
={} &\int_0^h q_{(s'',s)} p_{(s'',s)}(t') \mu_s(\lceil s\rceil; ((\lceil s'\rceil; true) \wedge \int 1 = t - x))(t - t')dt' \\
={} &\int_0^h q_{(s'',s)} p_{(s'',s)}(t') \mu_s((\lceil s\rceil \wedge \int 1 = x - t'); (\lceil s'\rceil; true))(t - t')dt'
\end{aligned}
$$

Since $\mu_s((\lceil s\rceil \wedge \int 1 = x - t'); (\lceil s'\rceil; true))(t) = 0$ as mentioned at the beginning of the proof, it can be seen that $R(\lceil\ \rceil)$ is true.

Now, suppose that $R(X)$ holds. Similarly, we can show, for any $s''' \in S$

$$\mu_{s'''}((\lceil s'''\rceil; \lceil s''\rceil; X; \lceil s\rceil) \wedge \int 1 = x; (\lceil s'\rceil; true))(t) = 0.$$

By AR 7, we can conclude that $R(true)$ holds, which implies the conclusion of the theorem. $\square$

The property of the Markov model is presented in the following theorems.

Theorem 5.4. Assume that M has the Markovian property at $s' \in S$. Then, for arbitrary DC formulas D, D_1 and D_2

1. $\mu_s(D \wedge (true; (\lceil s'\rceil \wedge \int 1 > m)))(t+m) = \mu_s(D \wedge (true; \lceil s'\rceil))(t)u_{s'}(m)$, where $m \geq 0$.
2. If for all $t > 0$, $\mu_s(D_1; \lceil s'\rceil)(t) = \mu_s(D_2; \lceil s'\rceil)(t)$, then $\mu_s(D_1; \lceil s'\rceil; (D \wedge \int 1 = r))(t) = \mu_s(D_2; \lceil s'\rceil; (D \wedge \int 1 = r))(t)$.

Proof. The first item follows directly from AR 6-1 and Theorem 5.2. The second item is proved as follows. From the property of DC formulas, by AR 2 we have, for $i = 1, 2$,

$$
\begin{aligned}
\mu_s(D_i; \lceil s'\rceil; (D \wedge \int 1 = r))(t) = \\
\sum_{s'' \in S} \mu_s(D_i; \lceil s'\rceil; (D \wedge \int 1 = r \wedge (\lceil s''\rceil; true)))(t).
\end{aligned}
$$

For $s'' \neq s'$, $\mu_s(D_i; \lceil s'\rceil; (D \wedge \int 1 = r \wedge (\lceil s''\rceil; true)))(t) = 0$ by Theorem 5.3 taking into account the fact that $\mu_s(D_i; \lceil s'\rceil; (D \wedge \int 1 = r \wedge (\lceil s''\rceil; true)))(t) = \mu_s((D_i; \lceil s'\rceil) \wedge \int 1 = t - r; (D \wedge (\lceil s''\rceil; true)))(t)$ which is derived from Theorem 5.1 (6) and AR 1. Furthermore, by AR 6, we have for $i = 1, 2$,

$$
\begin{aligned}
&\mu_s(D_i; \lceil s'\rceil; (D \wedge \int 1 = r \wedge (\lceil s'\rceil; true)))(t) \\
&= \mu_s(D_i; \lceil s'\rceil)(t - r)\mu_{s'}(D \wedge \int 1 = r \wedge (\lceil s'\rceil; true))(r)
\end{aligned}
$$

From the assumption of the theorem, we have

$$
\begin{aligned}
&\mu_s(D_2; \lceil s'\rceil)(t - r)\mu_{s'}(D \wedge \int 1 = r \wedge (\lceil s'\rceil; true))(r) \\
&= \mu_s(D_1; \lceil s'\rceil)(t - r)\mu_{s'}(D \wedge \int 1 = r \wedge (\lceil s'\rceil; true))(r)
\end{aligned}
$$

Thus,

$$\mu_s(D_1; \lceil s' \rceil; D \wedge \int 1 = r)(t) = \mu_s(D_2; \lceil s' \rceil; D \wedge \int 1 = r)(t).$$

$\square$

The next theorem demonstrates the power of AR 6 (a proof is given in the Appendix).

Theorem 5.5. Let the Markovian property be satisfied for all $s \in S$, and let $f_s(t) = \mu_{s_0}(true; \lceil s \rceil)(t)$. Let, for $s, s' \in S$,

$$c_{s,s'} = \begin{cases} q_{(s,s')}p_{(s,s')}(0) & \text{if } s \neq s', \\ -\sum_{(s,s'') \in A} q_{(s,s'')}p_{(s,s'')}(0) & \text{otherwise.} \end{cases}$$

Then $f_s(t)$, $s \in S$, are the unique solutions of the forward equation

$$\frac{d}{dt} f_s(t) = \sum_{s' \in S} f_{s'}(t) c_{s,s'}, \ s \in S.$$

Hence, $f_s(t)(s \in S)$ define the probability distribution of a time-homogeneous honest Markov process (see [CoM90]). Note that $f_s(t)$ is the probability that M is in s at time t given that M started in s_0 at time 0. From the equation, many interesting properties of $f_s(t)$ (see e.g. [CoM90]) can be derived.

Theorem 5.6. Assume that the Markovian property is satisfied for all $s \in S$. Then, for $t' \geq t$

$$\mu_s(D)(t) = d \Leftrightarrow \mu_s((D \wedge \int 1 = t); true)(t') = d.$$

Proof. By writing

$$true = \lceil \ \rceil \vee \bigvee_{s' \in S} \lceil s' \rceil; true,$$

we have

$$D = (D \wedge \lceil \ \rceil) \vee \bigvee_{s' \in S} D \wedge (true; \lceil s' \rceil).$$

Now, by writing

$$true = \lceil \ \rceil \vee \bigvee_{s'' \in S} true; \lceil s'' \rceil$$

we have by AR 2,

$$\mu_s(D \wedge \int 1 = t; true)(t')$$
$$= \sum_{s',s'' \in S} \mu_s \left(D \wedge \int 1 = t \wedge (true; \lceil s' \rceil); (\lceil s'' \rceil; true) \right)(t').$$

From AR 2 and 6 and Theorem 5.3, it follows that

$$\mu_s(D \wedge \int 1 = t; true)(t')$$
$$= \sum_{s' \in S} \mu_s \left(D \wedge \int 1 = t \wedge (true; \lceil s' \rceil); (\lceil s' \rceil; true) \right)(t')$$
$$= \sum_{s' \in S} \mu_s(D \wedge \int 1 = t \wedge (true; \lceil s' \rceil)(t) \times 1$$
$$= \mu_s(D)(t).$$

$\square$

6. Example

Now we use the calculus to estimate the satisfaction probability of **Req-1** in an interval of time $[0, t]$ of the simple gas burner system in the example given at the end of Section 3. For simplicity we adopt the following denotations (by our convention, $\mu(D)(t) = 0$ for all $t < 0$).

$$
\begin{aligned}
D_1 &= \lceil N \rceil & D'_1 &= \lceil N \rceil \\
R_1 &= \lceil L \rceil \wedge \ell \leq 1 & R'_1 &= \lceil L \rceil \\
D_{2k} &= \lceil L \rceil \wedge \ell \leq 1; D_{2k-1} & D'_{2k} &= \lceil L \rceil; D'_{2k-1} \\
D_{2k+1} &= \lceil N \rceil \wedge \ell \geq 30; D_{2k} & D'_{2k+1} &= \lceil N \rceil; D'_{2k} \\
R_{2k} &= \lceil N \rceil \wedge \ell \geq 30; R_{2k-1} & R'_{2k} &= \lceil N \rceil; R'_{2k-1} \\
R_{2k+1} &= \lceil L \rceil \wedge \ell \leq 1; R_{2k} & R'_{2k+1} &= \lceil L \rceil; R'_{2k} \\
a_{2k}(t) &= \mu_L(D_{2k})(t) & a'_{2k}(t) &= \mu_L(D'_{2k})(t) \\
a_{2k-1}(t) &= \mu_N(D_{2k-1})(t) & a'_{2k-1}(t) &= \mu_N(D'_{2k-1})(t) \\
b_{2k}(t) &= \mu_N(R_{2k})(t) & b'_{2k}(t) &= \mu_N(R'_{2k})(t) \\
b_{2k-1}(t) &= \mu_L(R_{2k-1})(t) & b'_{2k-1}(t) &= \mu_L(R'_{2k-1})(t)
\end{aligned}
$$

$k = 1, 2, 3, \ldots$

Assume that the system starts in the state N. The duration formula D_{2k-1} is satisfied at time t by the system iff the system satisfies **Des-1** $\wedge$ **Des-2** at time t and there are $2k - 2$ transition occurrences in $(0, t)$; the duration formula D'_{2k-1} is satisfied at time t by the system iff there are $2k - 2$ transition occurrences in $(0, t)$. Similarly, the duration formula R_{2k} is satisfied at time t by the system iff the system satisfies **Des-1** $\wedge$ **Des-2** at time t and there are $2k - 1$ transition occurrences in $(0, t)$; the duration formula R'_{2k} is satisfied at time t by the system iff there are $2k - 1$ transition occurrences in $(0, t)$. Since D_i and D_j, D'_i and D'_j, R_i and R_j are mutually exclusive when $i \neq j$, from AR 2 it follows that

$$
\mu_N(\textbf{Des-1} \wedge \textbf{Des-2})(t) = \sum_{k=1}^{\infty} (a_{2k-1}(t) + b_{2k}(t)),
$$

$$
1 = \mu_N(true)(t) = \sum_{k=1}^{\infty} (a'_{2k-1}(t) + b'_{2k}(t)).
$$

Let

$$
\rho(t) = \int_0^t p_{(N,L)}(h)dh = \begin{cases} 1 - e^{-\lambda(t-30)} & \text{if } t > 30 \\ 0 & \text{otherwise,} \end{cases}
$$

$$
\varepsilon(t) = \begin{cases} \int_1^t p_{(L,N)}(h)dh & \text{if } t > 1 \\ 0 & \text{otherwise,} \end{cases}
$$

$$
\varepsilon'(t) = \begin{cases} \int_t^{\infty} p_{(L,N)}(h)dh & \text{if } t > 1 \\ 0 & \text{otherwise.} \end{cases}
$$

We have that $\rho(t) \geq \rho(t')$, $\varepsilon(t) \geq \varepsilon(t')$ for $t \geq t' > 1$, and $\varepsilon'(t) < c = \int_1^{\infty} p_{(L,N)}(h)dh$ for all $t > 0$.

We show by induction on k that when $t < (k-1)30$

$$
\begin{aligned}
a_{2k-1}(t) &= a_{2k}(t) = b_{2k-1}(t) = b_{2k}(t) = \\
a'_{2k-1}(t) &= a'_{2k}(t) = b'_{2k-1}(t) = b'_{2k}(t) = 0,
\end{aligned} \tag{1}
$$

otherwise,

$$a_{2k}(t) \geq a'_{2k}(t) - \varepsilon(t)\frac{1 - \rho(t)^{k-1}}{1 - \rho(t)} \tag{2}$$

$$a_{2k+1}(t) \geq a'_{2k+1}(t) - \varepsilon(t)\frac{1 - \rho(t)^k}{1 - \rho(t)}\rho(t) \tag{3}$$

$$b_{2k}(t) \geq b'_{2k}(t) - \varepsilon(t)\frac{1 - \rho(t)^{k-1}}{1 - \rho(t)}\rho(t) - c\rho(t)^k \tag{4}$$

$$b_{2k+1}(t) \geq b'_{2k+1}(t) - \varepsilon(t)\frac{1 - \rho(t)^k}{1 - \rho(t)} - c\rho(t)^k \tag{5}$$

Basic step. Let $k = 1$. When $t < 0$, (1) is satisfied obviously. Let us verify the remainder. If $t \geq 1$, from AR 5,

$$
\begin{aligned}
a_2(t) &= \int_0^1 p_{(L,N)}(h)\mu_N(D_1)(t - h)dh \\
&= \int_0^t p_{(L,N)}(h)\mu_N(D_1)(t - h)dh - \\
&\qquad \int_1^t p_{(L,N)}(h)\mu_N(D_1)(t - h)dh \\
&\geq \mu_L(D_2)(t) - \varepsilon(t) \\
&= a'_2 - \varepsilon(t).
\end{aligned}
$$

Since $\varepsilon(t) = 0$ when $t < 1$, also by AR 5, $a_2(t) = a'_2(t) - \varepsilon(t)$. Therefore, (2) is satisfied for all $t \geq 0$. From this, we have

$$
\begin{aligned}
a_3(t) &= \int_0^t p_{(N,L)}(t)a_2(t - h)dh \\
&\geq \int_0^t p_{(N,L)}(t)a'_2(t - h)dh - \varepsilon(t)\int_0^t p_{(N,L)}(t)dh \\
&\geq a'_3(t) - \varepsilon(t)\rho(t).
\end{aligned}
$$

So, (3) is true for $k = 1$.

$$
\begin{aligned}
b_1(t) &= \mu_L(R_1)(t) = \begin{cases} \mu_L(R'_1)(t) & \text{if } t \leq 1 \\ 0 & \text{otherwise} \end{cases} \\
&= \begin{cases} \mu_L(R'_1)(t) & \text{if } t \leq 1 \\ 1 - \int_0^t p_{(L,N)}(h)dh - \int_t^\infty p_{(L,N)}(h)dh & \text{otherwise} \end{cases} \\
&= \begin{cases} \mu_L(R'_1)(t) & \text{if } t \leq 1 \\ q_L(t) - \int_t^\infty p_{(L,N)}(h)dh & \text{otherwise} \end{cases} \\
&= b'_1(t) - \varepsilon'(t) \\
&\geq b'_1(t) - c
\end{aligned}
$$

Consequently, by AR 5,

$$b_2(t) = \int_0^t p_{(N,L)}(t)b_1(t - h)dh$$

$$\geq \int_0^t p_{(N,L)}(t)b_1'(t-h)dh - c\int_0^t p_{(N,L)}(t)dh$$

$$\geq b_2'(t) - c\rho(t).$$

Thus, (4) is satisfied. (5) follows immediately from (4) and AR 5.

Induction step. Assume that (1)-(5) are true for some natural number k. We show that they are true for $k+1$.

(1) follows immediately from AR 5, the induction hypothesis and the fact that $p_{(N,L)} = 0$ when $t \leq 30$. (2), (3) and (4), (5) are similar, so we prove (4), (5). By AR 5, the induction hypothesis, the definitions of $\varepsilon, \varepsilon'$, and the properties of probability density functions, we have, for $t \geq k \times 30$,

$$
\begin{aligned}
b_{2k+2}(t) &= \int_0^t p_{(N,L)}(h)b_{2k+1}(t-h)dh \\
&\geq \int_0^t p_{(L,N)}(h)b_{2k}'(t-h)dh - \\
&\qquad \frac{1-\rho(t)^k}{1-\rho(t)}\varepsilon(t)\int_0^t p_{(N,L)}(h)dh - c\rho(t)^k\int_0^t p_{(N,L)}(h)dh \\
&= b_{2k+2}'(t) - \frac{1-\rho(t)^k}{1-\rho(t)}\rho(t)\varepsilon(t) - c\rho(t)^{k+1}.
\end{aligned}
$$

So, (4) is true for $k+1$. From this, we have

$$
\begin{aligned}
b_{2k+3}(t) &= \int_0^1 p_{(L,N)}(h)b_{2k+2}(t-h)dh \\
&\geq \int_0^1 p_{(L,N)}(h)b_{2k+2}'(t-h)dh - \\
&\qquad \frac{1-\rho(t)^k}{1-\rho(t)}\rho(t)\varepsilon(t)\int_0^1 p_{(L,N)}(h)dh - \\
&\qquad c\rho(t)^{k+1}\int_0^1 p_{(L,N)}(h)dh \\
&\geq b_{2k+3}'(t) - \int_1^t p_{(L,N)}(h)b_{2k+2}'(t-h)dh - \\
&\qquad \frac{1-\rho(t)^k}{1-\rho(t)}\rho(t)\varepsilon(t) - c\rho(t)^{k+1} \\
&\geq b_{2k+3}'(t) - \varepsilon(t) - \frac{1-\rho(t)^k}{1-\rho(t)}\rho(t)\varepsilon(t) - c\rho(t)^{k+1} \\
&= b_{2k+3}'(t) - \left(\frac{1-\rho(t)^k}{1-\rho(t)}\rho(t) + 1\right)\varepsilon(t) - c\rho(t)^{k+1} \\
&= b_{2k+3}'(t) - \frac{1-\rho(t)^{k+1}}{1-\rho(t)}\varepsilon(t) - c\rho(t)^{k+1}.
\end{aligned}
$$

Thus, (5) is satisfied for $k+1$ as well. The proof is completed.

Now, we estimate $\mu_N(\textbf{Des-1} \wedge \textbf{Des-2})(t)$. Let $n = \lfloor t/30 \rfloor$. Then, it follows from (1) that $a_{2k-1}(t) = b_{2k}(t) = a'_{2k-1}(t) = b'_{2k}(t) = 0$ for all $k > n$. Combining with (2) and (5), we have

$$
\begin{aligned}
\mu_N(&\textbf{Des-1} \wedge \textbf{Des-2})(t) \\
&= \sum_{k=1}^{n}(a_{2k-1}(t) + b_{2k}(t)) \\
&\geq \sum_{k=1}^{n}(a'_{2k-1}(t) + b'_{2k}(t)) - 2\frac{\rho(t)}{1-\rho(t)}\varepsilon(t)\sum_{k=1}^{n}(1 - \rho(t)^{k-1}) - \\
&\quad\quad c\sum_{k=1}^{n}\rho(t)^k \\
&= 1 - 2\frac{\rho(t)}{1-\rho(t)}\varepsilon(t)\left(n - 1 - \rho\frac{1-\rho(t)^{n-1}}{1-\rho(t)}\right) - c\rho(t)\frac{1-\rho(t)^n}{1-\rho(t)},
\end{aligned}
$$

or, more roughly,

$$
\begin{aligned}
\mu_N(\textbf{Des-1} \wedge \textbf{Des-2})(t) \quad &\geq \quad 1 - \frac{\rho(t)}{1-\rho(t)}c\left(2n - 1 - 2\frac{1-\rho(t)^{n-1}}{1-\rho(t)} - \rho(t)^n\right) \\
&\geq \quad 1 - \frac{\rho(t)}{1-\rho(t)}c\left(2n - 1 - 2\frac{1-\rho(t)^{n-1}}{1-\rho(t)}\right).
\end{aligned}
$$

Therefore, for a fixed t and a given probability $\Delta < 1$, the formula $\textbf{Des-1} \wedge \textbf{Des-2}$ is satisfied by the system in $[0, t]$ with probability at least Δ if

$$
\frac{\rho(t)}{1 - \rho(t)}c\left(2n - 1 - 2\frac{1 - \rho(t)^{n-1}}{1 - \rho(t)}\right) \leq 1 - \Delta.
$$

We now suppose that the rate of becoming *leak* is

$$
\lambda = (10 \times 24 \times 3600)^{-1} \text{ (in one second)},
$$

and determine δ such that the requirement $\textbf{Req-1}$ is satisfied by the system in one day ($t = 24 \times 3600$ seconds) with the probability at least 0.99. In this case, we have

$$
n = 8 \times 360,
$$

$$
\rho(t) = 1 - e^{\lambda t} \approx \lambda t = 0.1,
$$

$$
\frac{\rho(t)}{1 - \rho(t)} = 1/9,
$$

$$
\frac{\rho(t)}{1 - \rho(t)}c\left(2n - 1 - 2\frac{1 - \rho(t)^{n-1}}{1 - \rho(t)}\right) \leq 1/9 \times 16 \times 360 \times c = 640c.
$$

Thus, it is sufficient to have δ such that $c \leq 0.01/640 \approx 0.000015$. This means,

$$
c = a\Phi(-0.5/\sqrt{\delta}) = \frac{\Phi(-0.5/\sqrt{\delta})}{1 - \Phi(-0.5/\sqrt{\delta})} \leq 0.000015.
$$

0r, equivalently,

$$
\Phi(-0.5/\sqrt{\delta}) \leq 0.000015/(1 + 0.000015) = 0.000015.
$$

From the table of values of the function Φ, it follows that

$$
0.5/\sqrt{\delta} \geq 4.2
$$

which implies that $\delta \leq 0.0142$. This value characterises the precision of the components of the system with which the system satisfies $\textbf{Req}$ in one day with probability at least 0.99.

7. Conclusion

We have presented our approach to the problem of the verification of dependability. This paper can be considered as a generalisation of [SNH93]. [SNH93] establishes *forward equations* to verify whether a probabilistic automaton with transitions of exponentially distributed delays satisfies a requirement concerning the time when the automaton reaches its failure state. With forward equations, it is impossible to determine the satisfaction probability of a requirement with real-time constraints on intermediate transitions. However, this paper derives probabilistic density functions of timed transition sequences of a probabilistic automaton, and therefore can adopt DC as a real-time functional specification language. Another difference is apparent: [SNH93] only deals with exponential distributions, but our calculus can treat more distributions.

This paper is only the first of our attempts to combine DC with continuous time semi-Markov processes. In our future work, we shall develop a computation-oriented theory based on this calculus and more general probabilistic models.

Acknowledgement The authors would like to thank to the anonymous referees and Mr Dimitar Guelev for their helpful comments and criticisms that lead to this improvement of the paper.

References

[AlH89]   Alur, R. Henzinger, T.A.: A Really Temporal Logic, *Proceedings of the Thirtieth Symposium on the Foundations of Computer Science*, pages 164-169, 1989.

[CoM90]   Cox, D. R. Miller, H. D.: *The Theory of Stochastic Processes*, London, Chapmann and Hall, 1965 (reprinted 1968, 1970, 1972, 1980, 1984, and 1990).

[HaZ91]   Hansen, M. R. and Zhou, C. C.: Semantics and completeness of duration calculus, in J. W. de Bakker, K. Huizing, W. P. de Roever, and G. Rozenberg, eds., *Real-Time: Theory in Practice*, LNCS 600, pages 209-225, 1991.

[HMP92]   Henzinger, T. A. Manna, Z. and Pnueli, A.: Timed transition systems, in J. W. de Bakker, K. Huizing, W. P. de Roever, and G. Rozenberg, eds., *Real-Time: Theory in Practice*, LNCS 600, pages 226-251, 1992.

[Hoa85]   Hoare, C. A. R. *Communicating Sequential Processes*, Prentice-Hall, 1985.

[Joh90]   Johnson, B. W. *Evaluation techniques*, ch. 4 in Design and Analysis of Fault Tolerant Digital Systems, Reading, MA: Addison-Wesley, 1989.

[Koy90]   Koymans, R.: Specifying real-time properties with metric temporal logic, *Journal of Real-Time Systems*, Vol. 2, No. 4, pages 225-299, 1990.

[LSRZ94]   Liu, Z. Sørensen, E. V. Ravn, A. P. and Zhou, C. C.: Towards a calculus of systems dependability, *Journal of High Integrity Systems*, Vol. 1, No. 1, Oxford Press, pages 49-65, 1994.

[LSRZ92]   Liu, Z. Sørensen, E. V. Ravn A. P. , and Zhou, C. C.: A Probabilistic Duration Calculus, presented in *the 2nd Intl. Workshop on Responsive Computer Systems*, Saitama, Japan, Oct. 1-2, 1992, published in H. Kopetz and Y. Kakuda (eds), *Dependable Computing and Fault-Tolerant Systems Vol. 7 : Responsive Computer Systems*, Springer-Verlag, pages 30-52, 1993.

[Sch91]   Schneider, S.: *et al.*, Timed CSP: Theory and Practice, in J. W. de Bakker, K. Huizing, W. P. de Roever, and G. Rozenberg, eds., *Real-Time: Theory in Practice*, LNCS 600, pages 640-675, 1991.

[SNH93]   Sørensen, E. V. Nordahl, J. and Hansen, N. H.: From CSP models to Markov models, *IEEE Trans. on Soft. Eng.*, Vol. 19, No. 6, pages 554-570, June 1993.

[Whi80]   Whitt, W.: Continuity of generalized semi-Markov processes, Math. Oper. Res. 5, 1980.

[ZHR92]   Zhou, C. C. Hoare, C. A. R. and Ravn, A. P.: A calculus of duration, *Information Processing Letter*, Vol. 40, No. 5, pages 269-276, 1992.

Appendix

Proof of Theorem 2.1

Proof. Since $P(B_{w,t}) \geq 0$, the series $P(X) = \sum_{w \in W} P(B_{w,t})$ has sum (which may be the infinity) independent of the order of the terms. For $w \neq \epsilon$, we have

$$P(B_{w,t}) = \int_{\sum_{i=1}^{m} t_i < t, \forall i: t_i > 0} \left(\prod_{i=1}^{m} (q_{a_i} p_{a_i}(t_i)) \right) u_{a_m^+} \left(t - \sum_{i=1}^{m} t_i \right) dt_1 \ldots dt_m$$

With the substitution of the function $u_{a_m^+}(t - \sum_{i=1}^{m} t_i)$ by its definition, we have

$$P(B_{w,t}) = \int_{\sum_{i=1}^{m} t_i < t, \forall i: t_i > 0} \left(\prod_{i=1}^{m} (q_{a_i} p_{a_i}(t_i)) \right)$$
$$\times \left(1 - \sum_{a \in A_{a_m^+}} \int_{t_{m+1} \leq (t - \sum_{i=1}^{m} t_i)} q_a p_a(t_{m+1}) \, dt_{m+1} \right) dt_1 \ldots dt_m$$

Let $C_w = \int_{\sum_{i=1}^{m} t_i < t, \forall i: t_i > 0} (\prod_{i=1}^{m} (q_{a_i} p_{a_i}(t_i))) dt_1 \ldots dt_m$ for $w \in W$, $w \neq \epsilon$. Then, from the definition of the integrand, the previous equality implies

$$P(B_{w,t}) = C_w - \sum_{we \in W} C_{we}$$

From this and the prefix-closeness of X, it follows that $P(X) = P(B_{\epsilon,t}) + \sum_{a \in A_{s_0}} \int_0^t q_a p_a(h) dh = 1$. This completes the proof. $\square$

Proof of Theorem 5.5

Proof. As mentioned in Section 3, for each $c = (s, s')$, there exists $\lambda_a \geq 0$ such that

$$p_a(t) = \left(\sum_{a' \in A_s} \lambda_{a'} \right) e^{-t \sum_{a' \in A_s} \lambda_{a'}},$$

$$q_a = \lambda_a / \left(\sum_{a' \in A_s} \lambda_{a'} \right),$$

$$u_s(t) = e^{-t \sum_{a' \in A_s} \lambda_{a'}}.$$

Thus,

$$c_{s,s'} = \begin{cases} \lambda_{(s,s')} & \text{if } s \neq s' \\ -\sum_{a \in A_s} \lambda_a & \text{otherwise} \end{cases}$$

where $\lambda_{(s,s')} = 0$ if (s, s') is not a transition. From the axioms and rules of DC, we have

$$true; \lceil s \rceil = \lceil s \rceil \vee \left(\bigvee_{s' \in S \wedge s \neq s'} true; \lceil s' \rceil; \lceil s \rceil \right)$$

Since $s' \neq s'' \Rightarrow (true; \lceil s' \rceil; \lceil s \rceil) \wedge (true; \lceil s'' \rceil; \lceil s \rceil) = false$, by AR 3 and Theorem 6 we have

$$
\mu_{s_0}(true; \lceil s \rceil)(t) \quad = \sum_{s' \in S \wedge s \neq s} \mu_{s_0}(true; \lceil s' \rceil; \lceil s \rceil)(t) + \mu_{s_0}(\lceil s \rceil)(t) \qquad (6)
$$

$$
= \sum_{s' \in S \wedge s \neq s} \int_0^t \mu_{s_0}(true; \lceil s' \rceil)(h) c_{s',s} e^{c_{s,s}(t-h)} dh + \quad (7)
$$
$$
\mu_{s_0}(\lceil s \rceil)(t)
$$

$$
= \sum_{s' \in S \wedge s \neq s} e^{c_{s,s}t} \int_0^t \mu_{s_0}(true; \lceil s' \rceil)(h) c_{s',s} e^{-c_{s,s}h} dh + (8)
$$
$$
\mu_{s_0}(\lceil s \rceil)(t)
$$

By taking the derivative of both sides (it can be seen easily that $f_s(t)$ is differentiable), we have

$$
\frac{d}{dt} f_s(t)
$$
$$
= \sum_{s' \in S \wedge s \neq s} e^{c_{s,s}t} \int_0^t \mu_{s_0}(true; \lceil s' \rceil)(h) c_{s',s} e^{-c_{s,s}h} dh + \frac{d}{dt} \mu_{s_0}(\lceil s \rceil)(t)
$$
$$
= \sum_{s' \in S \wedge s \neq s}
$$
$$
\left(c_{s,s} e^{c_{s,s}t} \int_0^t \mu_{s_0}(true; \lceil s' \rceil)(h) c_{s',s} e^{-c_{s,s}h} dh + c_{s',s} \mu_{s_0}(true; \lceil s' \rceil) \right) +
$$
$$
+ \frac{d}{dt} \mu_{s_0}(\lceil s \rceil)(t)
$$

Since, by Theorem 5.2,

$$
\mu_{s_0}(\lceil s \rceil)(t) = \begin{cases} e^{c_{s,s}t} & \text{if } s = s_o \\ 0 & \text{otherwise} \end{cases}
$$

we have $\frac{d}{dt} \mu_{s_0}(\lceil s \rceil)(t) = c_{s,s} \mu_{s_0}(\lceil s \rceil)(t)$ for all $s \in S$. With this substitution in the previous equality, taking into account the first equality (6), we obtain

$$
\frac{d}{dt} f_s(t) \quad = \quad c_{s,s} f_s(t) + \sum_{s' \in S \wedge s \neq s} c_{s',s} f_{s'}(t)
$$

$$
= \quad \sum_{s' \in S} c_{s',s} f_{s'}(t)
$$

The proof is completed. □