Research Report 229

Towards a Calculus of Systems Dependability*

Zhiming Liu, Anders P. Ravn, Erling V Sorensen, Chaochen Zhou

RR229

This paper presents a calculus that enables a designer of an embedded, real-time system to reason about and calculate whether a given requirement will hold with a sufficiently high probability for given failure probabilities of components used in the design of the system.

The main idea is:

. to specify requirements and design in DC (Duration Calculus, an extension of real-time, interval logic).

. to define satisfaction probabilities for formulas in this calculus.

. to establish a basic probabilistic calculus, PC, with rules that support calculation of the satisfaction probability for a composite formula from probabilities of its constituents

. and - finally - to develop a collection of theorems expressing specific important PC formulas in terms of the probability matrices used in classical reliability engineering. These theorems are oriented towards systematic numerical calculations.

This ensures that reasoning about probabilities is consistent with requirements and design decisions. We thus avoid introducing separate models for requirements and dependability analysis. The system model is a finite automaton with fixed transition probabilities. This defines discrete Markov processes as basis for the calculus.

Department of Computer Science
University of Warwick
Coventry CV4 7AL
United Kingdom

September 1992

Towards a Calculus of Systems Dependability*

Zhiming Liu†, Anders P. Ravn‡, Erling V. Sørensen‡ and Chaochen Zhou§¶

† Department of Computer Science
University of Warwick
Coventry CV4 7AL, England
‡ Department of Computer Science
Technical University of Denmark
DK-2800 , Lyngby, Denmark
§ International Institute for Software Technology
United Nations University
P.O.Box 3058, Macau
¶ On leave from Software Institute, Academia Sinica
Beijing, P.R. China

Abstract

This paper presents a calculus that enables a designer of an embedded, real-time system to reason about and calculate whether a given requirement will hold with a sufficiently high probability for given failure probabilities of components used in the design of the system.

The main idea is:

- to specify requirements and design in DC (Duration Calculus, an extension of real-time, interval logic),
- to define satisfaction probabilities for formulas in this calculus,
- to establish a basic probabilistic calculus, PC, with rules that support calculation of the satisfaction probability for a composite formula from probabilities of its constituents
- and - finally - to develop a collection of theorems expressing specific important PC formulas in terms of the probability matrices used in classical reliability engineering. These theorems are oriented towards systematic numerical calculations.

This ensures that reasoning about probabilities is consistent with requirements and design decisions. We thus avoid introducing separate models for requirements and dependability analysis. The system model is a finite automaton with fixed transition probabilities. This defines discrete Markov processes as basis for the calculus.

Keywords: duration calculus, real-time systems, probabilistic automata, satisfaction probability, probabilistic calculus.

*This research was supported in part by **ProCoS** ESPRIT BRA 3104, and by the Danish Technical Research Council under project **RapID**. The research of Zhiming Liu was also supported inpart by research grants GR/D11521 and GR/H39499 from the Science and Engineering Research Council of UK.

1 Introduction

Requirements for an embedded, real-time system include functional and safety properties. Consider for instance an on-off gas burner [SNH91]. It is required to turn the flame on or off a short time after requested to do so by a thermostat. It must also prevent excessive leaks of gas to the environment. The latter requirement can be stated as an integrated constraint: the duration of leaking states should only be a small proportion of any interval of length, say 1 minute.

Such a system can be modelled by a dynamic system where a state changes over time. In the gas burner example, we could for instance introduce a discrete state *Leak* which goes on and off with time. A design for discrete control of the system will then be given by constraints on the transitions between states. A designer may now use various mathematical techniques to verify that the design satisfies the requirements. Among these the duration calculus [ZHR92] is recently found promising for reasoning about requirements and designs of real-time, embedded systems [HRR91, RR91, SRRZ92]. A summary of this calculus is given in Section 2.

However, a customer or a certification agency may legitimately ask about the dependability of the system in terms of a failure probability within a certain period of time. Such a question cannot be answered from the design or its mathematical model. In order to answer the questions, the designer may choose to develop alternative models, cf. the two tiered approaches used in the SIFT project [MSS82], or the stochastic model developed from a state machine model for a design in [SNH91].

A two model approach adds complexity to the design activity because the two have somehow to be updated consistently whenever the design changes. Several researchers have seen that there is a potential for making the design activity simpler by using a unified model in the form of a probabilistic automaton with Markov properties [HJ89, LS89]. In [LS89] an untimed logic for specification is extended by adding probabilities to the combinators; this allows reasoning about untimed probabilistic systems. Time and probabilities are introduced together in [HJ89] which extends the computation tree logic (CTL) of [CES83]. There is however not a proof system for the extended logic, and the expressiveness is somewhat restricted. We have thus found it worthwhile to investigate the development of a probabilistic duration calculus.

Based on probabilistic automata, this paper defines the satisfaction probabilities of duration formulas in the duration calculus, and establishes a corresponding probabilistic calculus. The calculus has a set of axioms and rules that support direct reasoning about and calculation of satisfaction probabilities for formulas specifying a given design.

The probabilistic duration calculus, subsequently called PC, is based on three key ideas. The first is to simulate imperfect systems with probabilistic automata. This is presented in Section 3. The second one, in Section 4, is to extend the model of the duration calculus and define the satisfaction probability of a duration formula by a probabilistic automaton. And the third one is to establish a calculus to calculate and reason about satisfaction probabilities. This is done in section 5.

Running examples are given in each section and Section 6 contains a number of examples that illustrate the possible application of the calculus.

However, the examples of Section 6 also indicate that calculation of satisfaction probabilities directly by means of the basic PC rules may turn out to be fairly complex. What is needed is a higher level of theorems provable from PC and oriented towards mechanisable numerical calculations. Such a level is established in Section 7 by introduction of the classical probability matrices, and its ability to treat some of the previous examples more succintly is illustrated.

The conclusion in Section 8 compares this work with related work and indicates directions for further research.

2 The Duration Calculus

This section outlines the duration calculus DC and its application to specification of real-time systems.

2.1 Time

The original duration calculus [ZHR92, HZ92] uses continuous time. In order to have a simple, well understood probabilistic model (see Section 3), we here assume discrete time. Time is represented by the set N of non-negative integers. A time point is denoted t, t_1, etc. and a *time interval* $[t_1, t_2]$, $t_1 \leq t_2$, represents the set of time points from t_1 to t_2.

2.2 States

We assume a finite non-empty set A of *primitive states*. States, ranged over by P, Q, P_1, Q_1, etc., consist of expressions formed by the following rules:

- Each primitive state $P \in A$ is a state.
- 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 $I(P) : N \to \{0, 1\}$. $I(P)(t) = 1$ means that state P is present at time point t, and $I(P)(t) = 0$ means that state P is not present at time point t. We assume that when a state is present at time t, it will persist for the next time unit. A *composite state* is interpreted as a function which is defined by the interpretations for the primitive states and the boolean operators.

2.3 Duration

For an arbitrary state P, its *duration* is denoted $\int P$. Given an interpretation I of the states, a duration $\int P$ will be interpreted over time intervals. It denotes the accumulated time during which P is present within the time interval. So for an arbitrary interval $[t_1, t_2]$, the interpretation $I(\int P)([t_1, t_2])$ is defined as the non-negative integer

$$I(\int P)([t_1, t_2]) = \sum_{t=t_1}^{t_2-1} I(P)(t)$$

where $I(\int P)([t, t]) = 0$. So $\int 1$ always denotes the length of an interval. We will use l to denote the *length* of an interval. That is,

Definition 1 $l \triangleq \int 1$

The set of *primitive duration terms* consists of variables over the integers Z and durations of states. A *duration term* is either a primitive term or an expression formed from terms by using the usual operators on integers, such as addition $+$ and multiplication $*$.

2.4 Duration Formulas

A *primitive duration formula* is an expression formed from terms by using the usual relational operators on the integers, 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 Z.

A duration formula D is satisfied by an interpretation I with an interval $[t_1, t_2]$ just when it is evaluated to *true* [HZ92]. This is written

$$I, [t_1, t_2] \models D$$

where I assigns every primitive state with a function from N to $\{0, 1\}$, and $[t_1, t_2]$ decides the observation window. So the joint satisfaction relation has nothing to do with the values of the primitive state assigned by I outside the observation window $[t_1, t_2]$. That is, for interpretations I_1 and I_2, if

$$I_1(P)(t) = I_2(P)(t) \quad t_1 \leq t \leq t_2$$

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

$$I_1, [t_1, t_2] \models D \quad \textit{iff} \quad I_2, [t_1, t_2] \models D$$

A chopped formula $D_1; D_2$ is true for I with $[t_1, t_2]$ if there exists a t such that $t_1 \leq t \leq t_2$ and D_1 and D_2 are true respectively with $[t_1, t]$ and $[t, t_2]$ for I.

We define shorthands for some duration formulas which are often used.

Definition 2 *For an arbitrary state P,*

$$\lceil P \rceil \triangleq (\int P = l) \wedge (l > 0)$$

This means that P holds everywhere in a non-point interval. We use $\lceil\ \rceil$ to denote the predicate which is true only for a point interval.

Definition 3 $\lceil\ \rceil \triangleq l = 0$

Definition 4 *For a duration formula D,*

$$\Diamond D \triangleq \textit{true};\ D;\ \textit{true}$$

This is true of an interval in which D holds for some subinterval of it.

Definition 5 *For a duration formula D,*

$$\Box D \triangleq \neg \Diamond \neg D$$

This is true of an interval in which D holds for all subintervals of it.

2.5 Proof System of Duration Calculus

This subsection lists the axioms and rules of the duration calculus which have been shown to be sound and (relative) complete in [HZ92] for the case of continuous time. We will make changes according to the discrete time domain we use in this paper. We will number these axioms and rules by **DA**.

The duration of the state 0 is always 0.

DA 1 $\int 0 = 0$

DA 2 *For an arbitrary state P,*

$$\int P \geq 0$$

The additivity rule of integrations 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 1 *For an arbitrary state P,*

1. $\int P + \int \neg P = l$
2. $\int P \leq l$

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

DA 4 *Let P be a state and r, s non-negative integers*

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

From this axiom, we have

Theorem 2 *For a state P*

$$l \geq 2 \Rightarrow ((\lceil P \rceil \Leftrightarrow (\lceil P \rceil;\ \lceil P \rceil))$$

Since we use discrete time, the condition $l \geq 2$ is required. This is different from the continuous time.

The following induction rule extends a hypothesis over adjacent subintervals. It relies on the finite variability of states and on the finitude of the intervals, that any interval can be split into a finite alternation of state P and state $\neg P$. The discrete time model automatically satisfies such an assumption.

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* $R(X \vee (X;\ \lceil P \rceil))$, $R(X \vee (X;\ \lceil \neg P \rceil))$ *are provable from* $R(X)$ *then* $R(true)$ *holds.*

2. *If* $R(\lceil\ \rceil)$ *holds, and* $R(X \vee (\lceil P \rceil;\ X))$, $R(X \vee (\lceil \neg P \rceil;\ X))$ *are 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 *For a state P*

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

As induction hypothesis, the proof uses $R(X) \triangleq X \Rightarrow (true;\ \lceil P \rceil) \vee (true;\ \lceil \neg P \rceil) \vee \lceil\ \rceil$.

2.6 Real Time Specifications

The duration calculus has been used to specify real-time constraints of embedded systems [HRR91, RR91, SRRZ92]. In [ZHR92], one of the time critical requirements of a Gas Burner is specified by a formula of the duration calculus denoted as **Req-1**,

Req-1 $l > 60sec \Rightarrow (20 * \int Leak \leq l)$

This says that if the interval over which the system is observed is at least one minute, the proportion of time spent in the leak state is no more than one twentieth of the elapsed time.

The requirement is refined into two design decisions

Des-1 $\Box(\lceil Leak \rceil \Rightarrow l \leq 1sec)$

Des-2 $\Box(\lceil Leak \rceil;\ \lceil \neg Leak \rceil;\ \lceil Leak \rceil \Rightarrow l > 32sec)$

Des-1 says that any leak state must be detected and stopped within one second, and **Des-2** says that leak must be seperated by at least 30 seconds.

The correctness of the design is reasoned about by proving the implication

Des-1 $\wedge$ **Des-2** $\Rightarrow$ **Req-1**

in the duration calculus [ZHR92].

However, we cannot expect, in practice, a *real* implementation to satisfy the decisions at all time. A real implementation can only satisfy the design decisions with some probability within a given service period. This raises the following problems which are the concerns of this paper. How can we model a real (imperfect) implementation? How can we define and reason about the satisfication probability of a duration formula (requirement or decision)?

3 Imperfect Systems and Probabilistic Automata

We will use a *finite probabilistic automaton* as a mathematical model of the behaviour of an imperfect system in a discrete time domain. Such an automaton is well described by its transition graph. We will continue with the Gas Burner example.

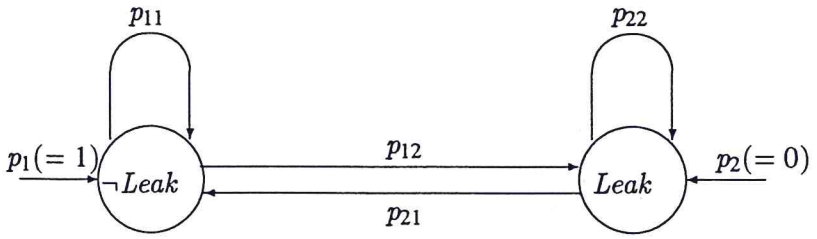

Figure 1: A Gas Burner With Unreliable Detector and Failing Flame

3.1 Gas Burner with Unreliable Flame Detector and Failing Flame

A model of a Gas Burner with an unreliable flame detector and a failing flame can be defined by the transition graph shown in Figure 1. In this Gas Burner, *Leak* is the only primitive state considered, and $\neg Leak$ denotes the absence of the primitive state. The probabilities of the system starting in states $\neg Leak$ and *Leak* are p_1 and p_2 respectively[1], where $0 \leq p_1, p_2 \leq 1$ and $p_1 + p_2 = 1$. The probability of the system to stay burning within one time unit is p_{11}. The probability of flame failure within one time unit is p_{12}. So $0 \leq p_{11}, p_{12} \leq 1$ and $p_{11} + p_{12} = 1$. The probability of the detector to detect the leakage (thereby causing re-ignition of the flame) within one time unit is p_{21}. The probability with which the detector fails to detect the leakage within one time unit is p_{22}, where $0 \leq p_{21}, p_{22} \leq 1$ and $p_{21} + p_{22} = 1$. Here we assume that the transition probabilities are independent of the transition history. This is the main feature of a Markov chain.

3.2 Gas Burner with Unreliable Detector, Unreliable Ignition and Failing Flame

An implementation with more imperfect components is modelled by a larger graph. The model of a Gas Burner with an unreliable flame detector, an unreliable ignition system and a failing flame is illustrated in Figure 2.

This graph uses two primitive states *gas* (gas is released), and *flame* (the flame is on) to model the system:

- At any time the system can be only in one of the following mutually exclusive states,

  $$V = \{\neg gas \wedge \neg flame\ ,\ gas \wedge flame\ ,\ gas \wedge \neg flame\}$$

  So it is assumed that

  $$\neg gas \wedge flame = 0 \text{ and } \neg gas \wedge \neg flame \vee gas \wedge flame \vee gas \wedge \neg flame = 1$$

- It starts in the idle state, i.e. both the gas and the flame are off,

  $$p_1 = 1 \quad \text{and} \quad p_2 = p_3 = 0$$

- It idles with probability p_{11} for one time unit;
- The ignition succeeds with probability p_{12} within one time unit;

[1] We usually assume that the Gas Burner starts from the state $\neg Leak$, i.e. $p_1 = 1$ and $p_2 = 0$.

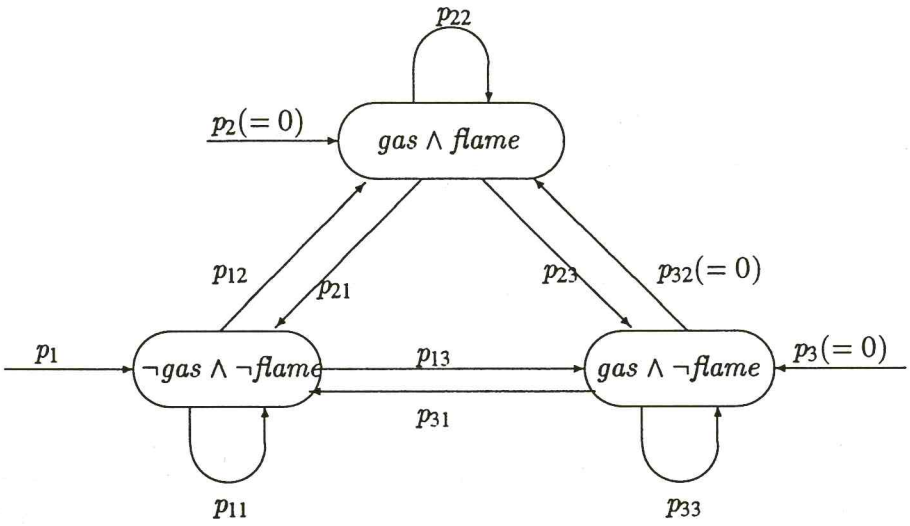

Figure 2: A Gas Burner With Unreliable Detector, Unreliable Ignition and Failing Flame

- The ignition fails with probability p_{13} within one time unit;
- The system finishes service with probability p_{21} within one time unit;
- The system stays burning with probability p_{22} within one time unit;
- The flame fails with probability p_{23} within one time unit;
- The system detects and stops a failure (by returning to the idle state) with probability p_{31} within one time unit;
- Detection or recovery fails with probability p_{33} within one time unit.

Notice that p_{32} is assumed to be zero. This means that spontaneous re-ignition after a flame failure is ruled out.

We have $0 \leq p_{ij} \leq 1$ and

$$p_{i1} + p_{i2} + p_{i3} = 1 \quad (i = 1,2,3)$$

Leak is now the composite state

$$Leak \triangleq gas \wedge \neg flame$$

3.3 Probabilistic Automaton

We end this section with a general definition of a probabilistic automaton (PA).

Definition 6 *A PA is a tuple* $G = (V, \tau_0, \tau)$ *where*

- $V = \{v_1, \ldots, v_m\}$, *is a finite non-empty set of multually exclusive states. That is, for any* $i,j : i \neq j \wedge 1 \leq i,j \leq m$,

  $$v_i \wedge v_j = 0$$

  V is also complete in the sense that

  $$\bigvee_{i=1}^{m} v_i = 1$$

  The set V is ranged by v, v', v_i, *etc.*

- $\tau_0 : V \rightarrow [0,1]$ *is a function called the initial probability mass function, such that*

  $$\sum_{v \in V} \tau_0(v) = 1$$

  $\tau_0(v)$ *defines the probability of the system starting from state* v.

- $\tau : V \times V \rightarrow [0,1]$ *is a function called the single-step probabilistic transition function such that for every* $v \in V$

  $$\sum_{v' \in V} \tau(v, v') = 1$$

For example, in Section 3.1, $V = \{Leak, \neg Leak\}$. The initial probability mass function is $\tau_0(\neg Leak) = 1$, $\tau_0(Leak) = 0$, and the probabilistic transition function is as follows.

$$\tau(\neg Leak, \neg Leak) = p_{11} \qquad \tau(\neg Leak, Leak) = p_{12}$$

$$\tau(Leak, \neg Leak) = p_{21} \qquad \tau(Leak, Leak) = p_{22}$$

4 Satisfaction Probability

Given an automaton $G = (V, \tau_0, \tau)$, let A be the set of primitive states each of which occurs in some state in V.

4.1 Behaviour

Given a non-negative integer t, the sequence of states in V,

$$\sigma^{[t]} : \ v_1, \ldots, v_t$$

defines a possible *behaviour* of G within its first t units of operating time. That is, start from state v_1 and transit from state v_{i-1} to v_i within one time unit, ending at v_t within the t^{th} time unit. We call $\sigma^{[t]}$ a behaviour of length t.

τ_0 determines the probability of starting from an initial state, and τ determines the probability of a transition from one state to another. Therefore, τ_0 and τ together determine the probability of the behaviour $\sigma^{[t]}$ within t time units.

For example,

$$\sigma^{[1]} = Leak$$

is a behaviour of length one of the PA in Section 3.1. It means that the system starts from *Leak*. But $\tau_0(Leak) = p_2 = 0$, i.e. the system cannot start from *Leak*. So the probability of $\sigma^{[1]}$ should be zero. Let $\mu(\sigma^{[1]})$ denote the probability of $\sigma^{[1]}$ with respect to the given PA, then $\mu(\sigma^{[1]}) = 0$.

$$\sigma^{[5]} : \neg Leak, \neg Leak, Leak, Leak, \neg Leak$$

is another behaviour of the PA in Section 3.1 with length 5. So

$$\mu(\sigma^{[5]}) = p_1 * p_{11} * p_{12} * p_{22} * p_{21}$$

In general if $\sigma^{[t]} = v_1, \ldots, v_t$,

$$\mu(\sigma^{[t]}) \triangleq \tau_0(v_1) * \prod_{i=1}^{t-1} \tau(v_i, v_{i+1})$$

where $\mu(\sigma^{[t]}) = 1$ when $t = 0$ and $\mu(\sigma^{[t]}) = \tau_0(v_1)$ when $t = 1$.

Let V^t be the set of all state sequence of V with length t. Thus, V^t defines all the possible behaviours of G with length t. From the definitions of τ_0 and τ, we can easily prove

Theorem 4 *For any non-negative integer t and any behaviour $\sigma^{[t]} \in V^t$ of length t,*

$$0 \leq \mu(\sigma^{[t]}) \leq 1$$

Theorem 5 *For any non-negative integer t,*

$$\sum_{\sigma^{[t]} \in V^t} \mu(\sigma^{[t]}) = 1$$

Thus, for every non-negative integer t we have a *probabilistic space* $\langle V^t, \mu \rangle$ with elements of V^t as the probabilistic samples.

4.2 Satisfaction

A behaviour $\sigma^{[t]}$ of G determines presence and absence of the primitive states in V at each of the first t time units, and thus defines an interpretation $I_{\sigma[t]}$ of duration formulas with A as the primitive states as far as the first t time units are concerned. That is,

$$I_{\sigma[t]}(P)(j) \triangleq \begin{cases} 1 & \text{if } \sigma(j) \Rightarrow P \\ 0 & \text{if } \sigma(j) \Rightarrow \neg P \end{cases}$$

where $j \in N$ and $0 \leq j \leq t$.

Referring to Section 2.4, it is justifiable to define the satisfaction of a duration formula D (with A as primitive states) by a behaviour of G as follows.

A duration formula D is *satisfied* by a behaviour $\sigma^{[t]}$, denoted

$$\sigma^{[t]} \models D$$

if and only if there is an interpretation I which is an extension[2] of $I_{\sigma^{[t]}}$ over $[0, t]$, such that

$$I, [0, t] \models D$$

For example, let

$$\sigma^{[5]} \triangleq \neg Leak, \neg Leak, Leak, Leak, \neg Leak$$

Then we have

$$\sigma^{[5]} \models l = 5, \quad \sigma^{[5]} \models \int \neg Leak = 3, \quad \sigma^{[5]} \models \Box(\lceil Leak \rceil \Rightarrow l \leq 2)$$

$$\sigma^{[5]} \not\models l \leq 3, \quad \sigma^{[5]} \not\models \Box(\lceil Leak \rceil \Rightarrow l \leq 1)$$

4.3 Satisfaction Probability

The probability of a PA satisfying a requirement (a duration formula) within a certain operating time (starting from time zero) should be the probability of the set of behaviours of the system up to that time which satisfy the requirement. Let D be a duration formula, and $V^t(D)$ be the set of behaviours in V^t which satisfy D. Then $\mu(D)[t]$, denoting the *satisfaction probability* of D by G within the time interval $[0, t]$, is defined

$$\mu(D)[t] \triangleq \sum_{\sigma^{[t]} \in V^t(D)} \mu(\sigma^{[t]})$$

which corresponds to an event in the space $\langle V^t, \mu \rangle$.

For example, for the PA defined in Section 3.1, let $D \triangleq \Box(\lceil Leak \rceil \Rightarrow l \leq 1)$. Then the behaviours of length 2 satisfying D are

$$V^2(D) = \{(\neg Leak, \neg Leak), (\neg Leak, Leak), (Leak, \neg Leak)\}$$

Thus

$$\mu(D)[2] = p_1 * p_{11} + p_1 * p_{12} + p_2 * p_{21} = p_{11} + p_{12} = 1$$

since $p_1 = 1$ and $p_2 = 0$.

5 PC: A Probabilistic Calculus

This section establishes a calculus for determination of the satisfaction probability $\mu(D)[t]$ which is consistent with the semantic definition of $\mu(D)[t]$ in Section 4.3.

[2]For an interpretation I_1 over a time interval $[t_1, t_2]$, an interpretation I_2 over N is an *extension* of I_1 if for every primitive state P and any time point $t \in [t_1, t_2]$, $I_1(P) = I_2(P)$.

The probabilistic logic is an extension of the first order real arithmetic with $\mu(D)$'s as the only additional functions. For an arbitrary duration formula D, $\mu(D)$ belongs to $N \rightarrow [0,1]$ and assigns each time point t with the satisfaction probability $\mu(D)[t]$.

Therefore, in this logic a *primitive term* is $\mu(D)[t]$ or a variable x ranging in the real numbers. A *term* is a primitive term, or an expression of terms built using the usual operators on real numbers, such as addition $+$ and multiplication $*$, with their standard meanings.

A *primitive formula* is an expression built from terms using the relational operators, such as equal $=$ and less than $<$ with their standard meanings.

A *formula* is a primitive formula or an expression built from formulas using the first order logic operators and the quantifiers over variables (including t in the term $\mu(D)[t]$). We assume the standard interpretations for the logic operators and quantifiers.

In this logic, we can write down and reason about probabilistic formulas such as (cf. Section 2.6)

$$\forall\, t : \mu(\neg\textbf{Req-1})[t] \leq \mu(\neg\textbf{Des-1})[t] + \mu(\neg\textbf{Des-2})[t]$$

which asserts that the probability of violating the requirement will not be greater than the sum of the probabilities of violating the design decisions. This formula tells the designer that there is a trade off between the design decisions with respect to probabilities. It also allows the designer to consider the reliability of each one separately.

Satisfaction probabilities can also be calculated with this logic by reasoning about formulas of the form

$$\mu(D)[t] = p$$

As an extension, PC will include all axioms and rules from the real arithmetic. We present in what follows the additional ones for functions $\mu(D)$'s. We will use the abbreviation $R(f,g)$ to stand for $\forall\, t : R(f[t], g[t])$, where R is a relation of functions f and g over N.

The duration formula *true* defines the set of all behaviours of G for any interval.

AR 1 *For the duration formula true*

$$\mu(true) = 1$$

For any given interval, the sets of behaviours defined by D and $\neg D$ form a partition of all the behaviours. So the sum of their probabilities is 1.

AR 2 *For an arbitrary duration formula D*

$$\mu(D) + \mu(\neg D) = 1$$

The following axiom formalizes the additivity rule in probability theory.

AR 3 *For arbitrary duration formulas D_1 and D_2*

$$\mu(D_1 \vee D_2) + \mu(D_1 \wedge D_2) = \mu(D_1) + \mu(D_2)$$

The satisfaction probability is monotonic in the sense that

AR 4 *If $D_1 \Rightarrow D_2$ holds in the duration calculus, then $\mu(D_1) \leq \mu(D_2)$ holds in PC.*

That is, if $D_1 \Rightarrow D_2$, then no more behaviours satisfy D_1 than D_2.

The above four axioms and rules follow directly from probability theory. The following theorem can easily be proven from them.

Theorem 6 *For arbitrary duration formulas D, D_1, D_2 and D_3*

1. $\mu(false) = 0$
2. $0 \leq \mu(D) \leq 1$
3. *If $D_1 \Leftrightarrow D_2$ in the duration calculus, then $\mu(D_1) = \mu(D_2)$*
4. *If $D_1 \wedge D_2 \Rightarrow D_3$ in the duration calculus, then*

$$(\mu(D_1) = 1) \Rightarrow (\mu(D_2) \leq \mu(D_3))$$

Proof: The proofs first three items of this theorem are trivial. We present the proof of the last item as follows.

By the second item of this theorem,

$$(1).\ 0 \leq \mu(D_1 \vee D_2) \leq 1$$

From duration calculus,

$$(2).\ D_1 \Rightarrow D_1 \vee D_2$$

So by (2) and **AR** 4,

$$(3).\ \mu(D_1) \leq \mu(D_1 \vee D_2)$$

Thus, by (1) and (3),

$$(4).\ (\mu(D_1) = 1) \Rightarrow (\mu(D_1 \vee D_2) = 1)$$

By **AR** 3,

$$(5).\ \mu(D_1 \vee D_2) + \mu(D_1 \wedge D_2) = \mu(D_1) + \mu(D_2)$$

Hence by (4) and (5),

$$(6).\ (\mu(D_1) = 1) \Rightarrow (\mu(D_1 \wedge D_2) = \mu(D_2))$$

By $D_1 \wedge D_2 \Rightarrow D_3$ and **AR** 4,

$$(7).\ \mu(D_1 \wedge D_2) \leq \mu(D_3)$$

Therefore, from (6) and (7),

$$(8).\ (\mu(D_1) = 1) \Rightarrow (\mu(D_2) \leq \mu(D_3))$$

□

Duration formulas D and $D \wedge (l = t)$ are satisfied by the same behaviours of length t. That is,

AR 5 *For an arbitrary duration formula D,*

$$\mu(D)[t] = \mu(D \wedge (l = t))[t]$$

Theorem 7

$$(\mu(l = t)[t] = 1) \wedge (\mu(l \neq t)[t] = 0)$$

Proof: By **AR** 5, Theorem 6.3 and **AR** 1,

$$\mu(l = t)[t] = \mu(true)[t] = 1$$

By **AR** 2,

$$\mu(l \neq t)[t] = 1 - \mu(l = t)[t] = 0$$

□

A behaviour $\sigma^{[t]}$ of length t satisfies a duration formula D if and only if each extension of it to a behaviour of length $t + t'$ satisfies the duration formula $(D;\ l = t')$. Therefore,

AR 6 *For an arbitrary duration formula D,*

$$\mu(D;\ l = t')[t + t'] = \mu(D)[t]$$

Now we can prove the following theorem.

Theorem 8 *For arbitrary duration formulas D_1 and D_2, if $\mu(D_1) = 0$, then $\mu(D_1;\ D_2) = 0$.*

Proof: From the monotonicity of the chop operator (cf. [ZHR92]) we have $(D_1;\ D_2) \Rightarrow (D_1;\ true)$. Combining this with **AR** 4 we get

$$(1).\ \ \mu(D_1;\ D_2) \leq \mu(D_1;\ true)$$

We prove $\mu(D_1;\ true) = 0$ by induction on t. By $(D_1;\ true) \wedge (l = 0) \Leftrightarrow (D_1 \wedge (l = 0))$, Theorem 6.3 and **AR** 5,

$$(2).\ \ \mu(D_1;\ true)[0] = \mu((D_1;\ true) \wedge (l = 0))[0] = \mu(D_1 \wedge (l = 0))[0] = \mu(D_1)[0] = 0$$

Assume that

$$(3).\ \ \mu(D_1;\ true)[t] = 0, \quad t = k$$

Since in duration calculus,

$$(4).\ \ (D_1;\ true) \wedge (l = k + 1) \Leftrightarrow (((D_1;\ true) \wedge (l = k);\ l = 1) \vee (D \wedge (l = k + 1)))$$

From Theorem 6.3 and Theorem 6.2, **AR** 3 and **AR** 5,

$$(5).\ \ \mu(D_1;\ true)[k + 1] \leq \mu((D_1;\ true) \wedge (l = k);\ l = 1)[k + 1] + \mu(D_1)[k + 1]$$

By induction assumption (3) and **AR** 6,

$$(6).\ \ \mu((D_1;\ true) \wedge (l = k);\ l = 1)[k+1] = \mu(D_1;\ true)[k] = 0$$

Since $\mu(D_1)[k+1] = 0$, from (5), (6) and Theorem 6.2,

$$(7).\ \ \mu(D_1;\ true)[k+1] = 0$$

By the natural induction rule,

$$(8).\ \ \mu(D_1;\ true) = 0$$

Thus, by (1) and Theorem 6.2,

$$(9).\ \ \mu(D_1;\ D_2) = 0$$

□

The axioms and rules described so far are independent of the Markov properties of the PA defined by the probabilistic space $\langle V^t, \mu \rangle$. We consider, in this paper, only those PAs which are Markov chains. The two following axioms formalize the Markov properties for a PA $G = (V, \tau_0, \tau)$.

AR 7 *For an arbitrary state* $v \in V$,

$$\mu(\lceil v \rceil^1)[1] = \tau_0(v)$$

Here we have used the convention $\lceil v \rceil^1 \triangleq \lceil v \rceil \wedge (l = 1)$.

This axiom formalizes the initial probability mass function τ_0. The probabilistic transition function τ is formalized as follows.

AR 8 *For an arbitrary duration formula* D *and states* $v_i, v_j \in V$,

$$\mu((D \wedge (true;\ \lceil v_i \rceil^1));\ \lceil v_j \rceil^1)[t+1] = \tau(v_i, v_j) * \mu(D \wedge (true;\ \lceil v_i \rceil^1))[t]$$

Notice that

$$(D;\ \lceil v_i \rceil^1;\ \lceil v_j \rceil^1) \Leftrightarrow ((D;\ \lceil v_i \rceil^1) \wedge (true;\ \lceil v_i \rceil^1);\ \lceil v_j \rceil^1)$$

Thus from **AR** 8, the following theorem holds.

Theorem 9 *For an arbitrary duration formula* D *and states* $v_i, v_j \in V$,

$$\mu(D;\ \lceil v_i \rceil^1;\ \lceil v_j \rceil^1)[t+1] = \tau(v_i, v_j) * \mu(D;\ \lceil v_i \rceil^1)[t]$$

This provides a way for calculating the probability of behaviours by chopping of unit intervals. The following axiom gives a way to calculate the probability from the middle of a behaviour.

AR 9 *For arbitrary duration formulas* D_1 *and* D_2, *and* $v_i, v_j, v_k \in V$,

$$\tau(v_i, v_j) * \tau(v_j, v_k) * \mu(D_1 \wedge (l = r);\ \lceil v_i \rceil^1;\ \lceil v_k \rceil^1;\ D_2)[t]$$

$$= \quad \tau(v_i, v_k) * \mu(D_1 \wedge (l = r);\ \lceil v_i \rceil^1;\ \lceil v_j \rceil^1;\ \lceil v_k \rceil^1;\ D_2)[t+1]$$

Theorem 10 *For arbitrary duration formulas D, D_1 and D_2, and $v, v' \in V$,*

1. $(\tau_0(v) = 0) \Rightarrow (\mu(\lceil v \rceil;\ D) = 0)$
2. $(\tau(v, v') = 0) \Rightarrow (\mu(D;\ \lceil v \rceil;\ \lceil v' \rceil;\ D_2) = 0)$

Proof: We prove the first item as follows.

(1). $(\lceil v \rceil;\ D) \Rightarrow (\lceil v \rceil;\ true)$

(2). $(\lceil v \rceil;\ true) \Rightarrow (\lceil v \rceil^1;\ true)$

By Theorem 7 and **AR** 7,

(3). $(\tau_0(v) = 0) \Rightarrow (\mu(\lceil v \rceil^1;\ true) = 0)$

By Theorem 8

(4). $(\tau_0(v) = 0) \Rightarrow (\mu(\lceil v \rceil^1;\ true) = 0)$

By (1), (2), **AR** 4 and Theorem 6.2,

(5). $(\tau_0(v) = 0) \Rightarrow (\mu(\lceil v \rceil;\ D) = 0)$

To prove the second item of this theorem, we can first prove,

(i). $(\tau(v, v') = 0) \Rightarrow (\mu(D_1;\ \lceil v \rceil;\ \lceil v' \rceil) = 0)$

Then by Theorem 8, the result is proven. For proving (i), we have only to prove,

(ii). $(\tau(v, v') = 0) \Rightarrow (\mu(true;\ \lceil v \rceil^1;\ \lceil v' \rceil^1;\ true) = 0)$

This can be proven by using **AR** 8 and Theorem 8 again. □

6 Examples

6.1 A Gas Burner

In this example we show how to estimate the satisfaction probability of **Req-1** stated in Section 2.6 for the simple Gas Burner discussed in Section 3.1. We assume that the time unit is one second, and as the starting point we take the following result proved in [ZHR92],

$$(\textbf{Des-1} \wedge \textbf{Des-2}) \Rightarrow \textbf{Req-1} \ \text{(i.e. } \neg\textbf{Req-1} \Rightarrow (\neg\textbf{Des-1} \vee \neg\textbf{Des-2}))$$

From **AR** 3 and **AR** 4, we then have

$$\mu(\neg\textbf{Req-1}) \leq \mu(\neg\textbf{Des-1} \vee \neg\textbf{Des-2}) \leq \mu(\neg\textbf{Des-1}) + \mu(\neg\textbf{Des-2})$$

where, from Section 2.6

$$\mu(\neg\textbf{Des-1}) = \mu(true;\ (\lceil Leak\rceil \wedge (l > 1));\ true)$$

$$\mu(\neg\textbf{Des-2}) = \mu(true;\ ((\lceil Leak\rceil;\ \lceil\neg Leak\rceil;\ \lceil Leak\rceil) \wedge (l < 32));\ true)$$

In what follows, we present a recursive calculation of $\mu(\neg\textbf{Des-1})[t]$. From the duration calculus,

$$\neg\textbf{Des-1} \wedge (l \leq 1) \Leftrightarrow false$$

Therefore, by Theorem 6.1 and Theorem 6.3,

$$t \leq 1 \Rightarrow \mu(\neg\textbf{Des-1})[t] = 0$$

Also, $(\neg\textbf{Des-1} \wedge l = 2) \Leftrightarrow \lceil Leak\rceil^1;\ \lceil Leak\rceil^1$; but $\tau_0(Leak) = 0$ thus

$\mu(\neg\textbf{Des-1})[2] = 0$, by Theorems 6.3 and **AR** 7 and **AR** 8.

Des-1 is violated for the first $t+1$ time units, $t > 1$, if and only if **Des-1** has been violated for the first t time units already, or **Des-1** holds for the first t time units but is violated one time unit later. This is written

$$\begin{array}{rcl}(\neg\textbf{Des-1} \wedge l = t+1) & \Leftrightarrow & ((\neg\textbf{Des-1} \wedge l = t);\ l = 1) \vee \\ & & ((\textbf{Des-1};\ l = 1) \wedge \neg\textbf{Des-1} \wedge l = t+1)\end{array}$$

where the two disjunctive terms on the right side are mutually exclusive.

For $t \geq 2$ and - due to the specific form of **Des-1** - the second term on the right side is equivalent to $(\textbf{Des-1};\ \lceil\neg Leak\rceil^1;\ \lceil Leak\rceil^1;\ \lceil Leak\rceil^1) \wedge (l = t+1)$

From Theorem 6.3, **AR** 3, **AR** 5, **AR** 6 and Theorem 9 it then follows that

$$\begin{array}{l}\mu(\neg\textbf{Des-1})[t+1] \ = \ \mu(\neg\textbf{Des-1})[t] \ + p_{12} * p_{22} * \mu(\textbf{Des-1};\ \lceil\neg Leak\rceil^1)[t-1] \\ \text{where } t \geq 2\end{array}$$

In order to solve this recursive equation we need an auxiliary recursive equation for the second μ-expression on the right side. This is established as follows:

For $t \geq 2$ and - due to the specific form of **Des-1** - we have

$$\begin{array}{rcl}((\textbf{Des-1};\ \lceil\neg Leak\rceil^1) \wedge l = t+1) & \Leftrightarrow & ((\textbf{Des-1};\ \lceil\neg Leak\rceil^1;\ \lceil\neg Leak\rceil^1) \wedge l = t+1) \vee \\ & & ((\textbf{Des-1};\ \lceil Leak\rceil^1;\ \lceil\neg Leak\rceil^1) \wedge l = t+1) \\ & \Leftrightarrow & ((\textbf{Des-1};\ \lceil\neg Leak\rceil^1;\ \lceil\neg Leak\rceil^1) \wedge l = t+1) \vee \\ & & ((\textbf{Des-1};\ \lceil\neg Leak\rceil^1;\ \lceil Leak\rceil^1;\ \lceil\neg Leak\rceil^1) \wedge l = t+1)\end{array}$$

again, the two disjunctive terms on the right side are mutually exclusive. From Theorem 6.3, **AR** 3, **AR** 5, and Theorem 9 it then follows that

$$\begin{array}{rcl}\mu(\textbf{Des-1};\ \lceil\neg Leak\rceil^1)[t+1] & = & p_{11} * \mu(\textbf{Des-1};\ \lceil\neg Leak\rceil^1)[t] \\ & + & p_{12} * p_{21} * \mu(\textbf{Des-1};\ \lceil\neg Leak\rceil^1)[t-1] \\ & & \text{where } t \geq 2\end{array}$$

It is easy to show, that $\mu(\textbf{Des-1};\ \lceil\neg Leak\rceil^1)[1]$ and $\mu(\textbf{Des-1};\ \lceil\neg Leak\rceil^1)[2]$ both are 1. These are the initial values for the recursion.

In summary, if we introduce the functions $\mathcal{P}(t)$ and $\mathcal{Q}(t)$ by

$$\begin{cases} \mathcal{P}(t) \triangleq \mu(\neg\textbf{Des-1})[t] \\ \mathcal{Q}(t) \triangleq \mu(\textbf{Des-1};\ \lceil\neg Leak\rceil)[t], \end{cases}$$

the probability $\mathcal{P}(t+1)$ that design-decision 1 is violated in the observation interval: $[0, t+1]$, where $t \geq 2$, can be calculated by solution of the mutually recursive equations

$$\begin{cases} \mathcal{P}(t+1) = \mathcal{P}(t) + p_{12} * p_{22} * \mathcal{Q}(t-1) \\ \mathcal{Q}(t+1) = p_{11} * \mathcal{Q}(t) + p_{12} * p_{21} * \mathcal{Q}(t-1) \\ \text{where } t \geq 2\,;\ \mathcal{P}(2) = 0, \mathcal{Q}(1) = 1 \text{ and } \mathcal{Q}(2) = 1 \end{cases}$$

The calculation of $\mu(\neg\textbf{Des-2})[t]$ is given recursively as follows. From **AR** 2,

$$\mu(\neg\textbf{Des-2}) = 1 - \mu(\textbf{Des-2})$$

And in the duration calculus,

$$(\textbf{Des-2} \wedge l > 0) \Leftrightarrow (\textbf{Des-2} \wedge (true;\ \lceil Leak\rceil^1)) \vee (\textbf{Des-2} \wedge (true;\ \lceil\neg Leak\rceil^1))$$

So by **AR 3** and Theorem 6.3, we have

$$\mu(\textbf{Des-2}) = \mu(\textbf{Des-2} \wedge (true;\ \lceil Leak\rceil^1)) + \mu(\textbf{Des-2} \wedge (true;\ \lceil\neg Leak\rceil^1))$$

Let $\mathcal{U}(t)$ and $\mathcal{V}(t)$ be the functions defined as

$$\begin{cases} \mathcal{U}(t) \triangleq \mu(\textbf{Des-2} \wedge (true;\ \lceil Leak\rceil^1))[t] \\ \mathcal{V}(t) \triangleq \mu(\textbf{Des-2} \wedge (true;\ \lceil\neg Leak\rceil^1))[t] \end{cases}$$

then, recalling that $p_1\ (= \tau_0(\neg Leak)) = 1$ and $p_2\ (= \tau_0(Leak)) = 0$, we can derive the following recursive equations for $\mathcal{U}(t)$ and $\mathcal{V}(t)$ in the calculus.

$$\begin{cases} \mathcal{U}(t+1) = p_{22} * \mathcal{U}(t) + \begin{cases} p_{11}^{28} * p_{12} * \mathcal{V}(t-29) & \text{if } t > 29 \\ p_{11}^{t-1} * p_{12} & \text{if } 1 \leq t \leq 29 \\ 0 & \text{if } t < 1 \end{cases} \\ \mathcal{V}(t+1) = \begin{cases} p_{21} * \mathcal{U}(t) + p_{11} * \mathcal{V}(t) & \text{if } t \geq 1 \\ 1 & \text{if } t < 1 \end{cases} \\ \text{where } t \geq 0 \text{ and } \mathcal{U}(0) = \mathcal{V}(0) = 0 \end{cases}$$

Using the above mutually recursive equations, we can calculate $\mu(\textbf{Des-2})$ and thus $\mu(\neg\textbf{Des-2})$.

6.2 A Protocol Over an Unreliable Communication Medium

Consider a *medium* through which a *sender* process sends messages to a *receiver* process. To describe the behaviour of the protocol, we introduce the following states.

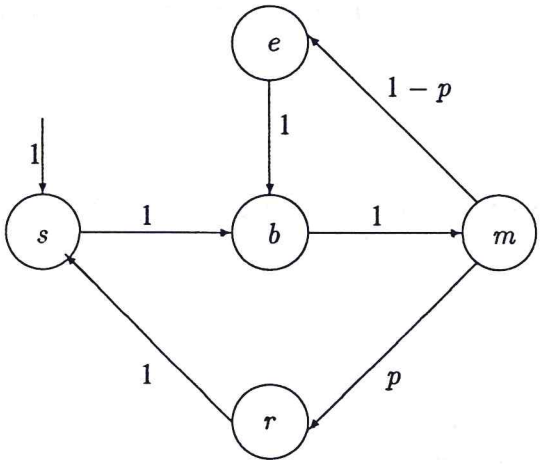

Figure 3: A Protocol Over an Unreliable Medium

- s, b, m and r represent that the sender, buffer, medium and receiver are active respectively. e represents an error state of the medium.
- The protocol starts from state s, i.e. the sender is active to send a message.
- The sent message is written into a buffer within one time unit.
- The medium receives the message from the buffer within one time unit.
- Within one time unit, the message sent by the medium may be received by the receiver with probability p and the protocol enters state r, or the message is lost with probability $1 - p$ and the protocol enters error state e.
- If the message is lost, within one time unit, the medium re-reads the message from the buffer.
- If the message is received by the receiver, within one time unit, the receiver acknowledges the sender and the sender is ready to send another message.

The protocol is illustrated in Figure 3, where the transitions with 0 probability are eliminated.

The first kind of properties we are interested in are the so called *soft-deadline* properties [HJ89]. It describes that starting from the state s, within t time units, i.e. within the interval $[0, t]$, the receiver receives at least one message with probability q. This is formalized in terms of PC as

$$\mu(\neg(\textstyle\int r = 0))[t] = q \text{ or equivalently, } \mu(\textstyle\int r > 0)[t] = q$$

It is not difficult to derive

$$3k < t \leq 3(k+1) \Rightarrow \mu(\neg(\textstyle\int r = 0))[t] = 1 - (1-p)^k$$

When $p = 0.9$, i.e. ten percent of the messages are lost, we have $\mu((\int r > 0))[7] = 0.99$. This gives the same result as presented in [HJ89].

Another kind of properties is to describe the *upper bound* of error occurrences for a given interval $[0, t]$. This property can be specified by the satisfaction probability of $\int e \leq n$, and also reasoned about in the calculus.

Now let us discuss the probability of the *reoccurrence of the error* state. We define the following formulas for shorthands.

$$D_1 \triangleq (true;\ \lceil e \rceil) \wedge (l = k);\ \lceil \neg e \rceil \wedge (l = k_1);\ \lceil e \rceil;\ true$$

$$D_2 \triangleq (true;\ \lceil e \rceil) \wedge (l = k);\ true$$

The conditional probability of D_1 under D_2 defines the probability of error reoccurrence in k_1 time units. When $\mu(D_2)[t] \neq 0$, it is equal to $\dfrac{\mu(D_1 \wedge D_2)[t]}{\mu(D_2)[t]}$, denoted $a(t, k_1)$.

Using natural induction on k_1, we can derive

$$a(t, k_1) = \begin{cases} 1 - p & \text{if } k_1 = 2 \\ p^{n+1} * (1 - p) & \text{if } k_1 = 4n + 6\ (n \geq 0) \\ 0 & \textbf{otherwise} \end{cases}$$

by proving

$$t \geq k + k_1 + 1 \Rightarrow \mu(D_1 \wedge D_2)[t] = a(t, k_1) * \mu(D_2)[t]$$

7 Calculation Technique

The examples in the previous section illustrate, that even though it is possible to calculate $\mu(D)[t]$ for specific problems directly by means of the basic rules and theorems of PC, the establishment of the necessary equations following this approach is somewhat intuistic and may turn out to be fairly complex. What we need is a higher level of theorems, provable from PC and oriented towards more mechanisable numerical calculations.

In this section we establish such a level by introduction and application of the classical *single-step transition probability matrix* $\boldsymbol{P}$ and *initial state occupation probability vector* $\boldsymbol{p}$. These matrices are defined by means of τ and τ_0 respectively.

The computation theorems will then of the form $\mu(D)[t+1] = f(\boldsymbol{p}, \boldsymbol{P})$ or $\mu(D)[t+1] = f(\boldsymbol{p}, \boldsymbol{P}, \mu(D_1)[t_1])$ where $t_1 \leq t$.

7.1 Introducing Matrices

An $m \times n$ *matrix* $\boldsymbol{M}_{m \times n}$ of real numbers is a function

$$\boldsymbol{M}_{m \times n} : \{1, \ldots, m\} \times \{1, \ldots, n\} \longrightarrow \mathcal{R}$$

where m and n range over the positive integers and $\mathcal{R}$ is the set of real numbers.

An $m \times n$ matrix $\boldsymbol{M}_{m \times n}$ is then totally determined by assigning a real number m_{ij} to $\boldsymbol{M}_{m \times n}(i, j)$ for $(i, j) \in \{1, \ldots, m\} \times \{1, \ldots, n\}$. Thus, such a matrix is also denoted

$$\boldsymbol{M}_{m \times n} \triangleq \begin{pmatrix} m_{11} & \cdot & \cdot & m_{1n} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ m_{m1} & \cdot & \cdot & m_{mn} \end{pmatrix}$$

where m_{ij} is called the (i,j)-*element* of $\boldsymbol{M}_{m\times n}$. When there is no confusion, $\boldsymbol{M}_{m\times n}$ is simply wrriten as $\boldsymbol{M}$.

Let $\mathcal{M}_{m\times n}$ denote the set of all $m\times n$ matrices and $\mathcal{M}$ the set of all matrices of real numbers. Operations on matrices are defined interm of their elements. For example, the addition "+" of matrices is defined on $\mathcal{M}_{m\times n}\times\mathcal{M}_{m\times n}$ by

$$(\boldsymbol{M}+\boldsymbol{M}')(i,j)\triangleq \boldsymbol{M}(i,j)+\boldsymbol{M}(i,j)$$

where $(i,j)\in\{1,\ldots,m\}\times\{1,\ldots,n\}$.

Similarly, the multiplication "$\cdot$" is defined on $\mathcal{M}_{m\times n}\times\mathcal{M}_{n\times m'}$ by

$$(\boldsymbol{M}_{m\times n}\cdot\boldsymbol{M}'_{n\times m'})_{m\times m'}(i,j)\triangleq\sum_{k=1}^{n}\boldsymbol{M}(i,k)*\boldsymbol{M}'(k,j)$$

where $(i,j)\in\{1,\ldots,m\}\times\{1,\ldots,m'\}$.

Predicates of matrices are defined in terms of predicates of their elements. For example, the equality "=" between two matrix is defined by

$$\boldsymbol{M}_{m\times n}=\boldsymbol{M}'_{m'\times n'}\triangleq(m=m')\wedge(n=n')\wedge(\bigwedge_{(i,j)=(1,1)}^{(m,n)}(\boldsymbol{M}(i,j)=\boldsymbol{M}'(i,j))$$

These definitions show that the arithmetic of matrices of real numbers is within the first order real arithmetic which is the basis of PC.

7.2 Auxiliary Notation

Definition 7 *The following auxiliary vectors and matrices will be needed:*

Let $\mathbf{1}_c$ *denote an* $m\times 1$ *matrix (column vector) in which all elements are 1.*

Let $\mathbf{1}_r$ *denote an* $1\times m$ *matrix (row vector) in which all elements are 1.*

Let $\boldsymbol{E}$ *denote the* $m\times m$ *identity matrix (*$\boldsymbol{E}(i,j)=1$ *for* $i=j$ *and* $\boldsymbol{E}(i,j)=0$ *for* $i\neq j$*).*

Let $\boldsymbol{E}_i$ *denote the* $m\times m$ *identity matrix with the* (i,i)*-element changed from* 1 *to* 0.

Let $\boldsymbol{Z}_i$ *denote the* $m\times m$ *matrix of zeros with the* (i,i)*-element changed from* 0 *to* 1.

Let $\boldsymbol{z}_i$ *denote the* $1\times m$ *matrix of zeros with the i'th element changed from* 0 *to* 1,

Let $\boldsymbol{h}_i$ *denote the* $m\times 1$ *matrix of zeros with the i'th element changed from* 0 *to* 1.

Notice that $\boldsymbol{Z}_i+\boldsymbol{E}_i=\boldsymbol{E}$ and that $\boldsymbol{z}_i$ and $\boldsymbol{h}_i$ are just short-hand notations for the row vector $(\mathbf{1}_r\cdot Z_i)$ and the column vector $(Z_i\cdot\mathbf{1}_c)$ respectively.

Definition 8 *Let* $\boldsymbol{I}$ *denote the index set* $\{1,\cdots,m\}$ *and* $\boldsymbol{I}_j$ *denote the subset* $\boldsymbol{I}\setminus\{j\}$ *where* $q\in\boldsymbol{I}$.

7.3 The Probability Matrices and some Basic Theorems

Definition 9 *With $V = \{v_1, v_2, \cdots, v_m\}$, where the subscripts are in the fixed index set $\boldsymbol{I}$, the single-step transition probability matrix $\boldsymbol{P}$ is a real $m \times m$ matrix defined by:*

$$\boldsymbol{P} \triangleq \begin{pmatrix} p_{11} & \cdot & \cdot & p_{1m} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ p_{m1} & \cdot & \cdot & p_{mm} \end{pmatrix} \quad \textit{where:} \quad \begin{array}{l} p_{ij} \triangleq \tau(v_i, v_j) \\ \sum_{j \in \boldsymbol{I}} p_{ij} = 1 \end{array}$$

and the initial state occupation probability vector $\boldsymbol{p}$ is a real $1 \times m$ row vector defined by:

$$\boldsymbol{p} \triangleq (p_1, \cdots, p_m) \quad \textit{where:} \quad \begin{cases} p_i \triangleq \tau_0(v_i) \\ \sum_{i \in \boldsymbol{I}} p_i = 1 \end{cases}$$

In the litterature on stochastic processes (e.g. [CM90]), p_{ij} and p_i are normally defined in the following way:

$$p_{ij} \triangleq \mathcal{P}[v = v_j \text{ at time } t+1 \mid v = v_i \text{ at time } t], \quad (t \geq 0)$$

$$p \triangleq \mathcal{P}[v = v_i \text{ at time } 0]$$

The first theorem is well known from the theory of Markov chains [CM90].

Theorem 11 *For $t \geq 0$:*

$$\boldsymbol{P}^t \cdot \mathbf{1}_c = \mathbf{1}_c$$

where $\boldsymbol{P}^0$ is defined to be the identity matrix $\boldsymbol{E}$.

The theorem expresses that the sum of each row in the t'th power of the single-step transition probability matrix is 1.

Proof: Use induction on t.

For $t = 0$,

$$\boldsymbol{P}^0 \cdot \mathbf{1}_c = \boldsymbol{E} \cdot \mathbf{1}_c = \mathbf{1}_c$$

Further, for $t = 1$, using the fact that for all $i \in \boldsymbol{I}$: $\sum_{j \in \boldsymbol{I}} p_{ij} = 1$,

$$\boldsymbol{P}^1 \cdot \mathbf{1}_c = \mathbf{1}_c$$

Assume that the result holds for $t \leq k$, then:

$$\boldsymbol{P}^{k+1} \cdot \mathbf{1}_c = \boldsymbol{P}^k \cdot (\boldsymbol{P}^1 \cdot \mathbf{1}_c) = \boldsymbol{P}^k \cdot \mathbf{1}_c = \mathbf{1}_c$$

This ends the proof. □

Definition 10 *Let $\boldsymbol{p}^{(t)}$ $(t \geq 0)$ denote the row vector $(p_1^{(t)}, \cdots, p_m^{(t)})$ defined by*

$$\boldsymbol{p}^{(t)} \triangleq \boldsymbol{p} \cdot \boldsymbol{P}^t$$

The following theorem states that $p_i^{(t)}$ is the (unconditional) probability, that the system occupies state v_i after the t'th transition. This is also well known from the theory of Markov chains, but here it is expressed and proved in terms of PC.

Theorem 12 *For $t \geq 0$,*

$$(\mu(true;\ \lceil v_1 \rceil^1)[t+1], \cdots, \mu(true;\ \lceil v_m \rceil^1)[t+1]) = \boldsymbol{p}^{(t)}$$

Proof: Use induction on t.

For $t = 0$, the result follows from **AR7** and the fact that,

$$\boldsymbol{p} = (\tau_0(v_1), \cdots, \tau_0(v_m))$$

Assume that the result holds for $t = k$, then from Theorem 9 and the definition of p_{ji},

$$\begin{aligned}
\mu(true;\ \lceil v_i \rceil^1)[k+2] &= \sum_{j \in \boldsymbol{I}} \mu(true;\ \lceil v_j \rceil^1;\ \lceil v_i \rceil^1)[k+2] \\
&= \sum_{j \in \boldsymbol{I}} \mu(true;\ \lceil v_j \rceil^1)[k+1] * \tau(v_j, v_i) \\
&= \sum_{j \in \boldsymbol{I}} \mu(true;\ \lceil v_j \rceil^1)[k+1] * p_{ji}
\end{aligned}$$

By the induction assumption,

$$\mu(true;\ \lceil v_j \rceil^1)[k+1] = p_j^{(k)}$$

Therefore, for $i \in \boldsymbol{I}$,

$$\mu(true;\ \lceil v_i \rceil^1)[k+2] = \sum_{j \in \boldsymbol{I}} p_j^{(k)} * p_{ji}$$

Thus from the rules in Section 7.1,

$$(\mu(true;\ \lceil v_1 \rceil^1)[k+2], \cdots, \mu(true;\ \lceil v_m \rceil^1)[k+2]) = \boldsymbol{p}^{(k)} \cdot \boldsymbol{P}$$

But,

$$\boldsymbol{p}^{(k)} \cdot \boldsymbol{P} = (\boldsymbol{p} \cdot \boldsymbol{P}^k) \cdot \boldsymbol{P} = \boldsymbol{p} \cdot \boldsymbol{P}^{k+1} = \boldsymbol{p}^{(k+1)}$$

This proves the theorem. □

Theorems 11 and 12 imply that the initial probability vector $\boldsymbol{p}$ and the single-step transition matrix $\boldsymbol{P}$ suffice to determine the distribution $\boldsymbol{p}^{(t)}$. Taken together, the theorems characterise $\boldsymbol{P}^t$ as the *t-step transition probability matrix*[3].

The last theorem in this section gives a symbolic interpretation of $\mu(true)[t+1]$ and its proof constitutes a proof-model for the subsequent computation oriented theorems.

[3] In the theory of stochastic processes the elements of P^t, denoted $p_{ij}^{(t)}$, are defined by:

$$p_{ij}^{(t)} \triangleq \mathcal{P}[v = v_j \text{ at time } n+t \mid v = v_i \text{ at time } n],\ (t \geq 0)$$

Theorem 13 *For a non-negative integer t:*

$$\mu(true)[t+1] = \boldsymbol{p} \cdot \boldsymbol{P}^t \cdot \mathbf{1}_c = 1$$

Proof: From **AR** 1,

$$\mu(true)[t+1] = 1$$

From definition 10,

$$\boldsymbol{p} \cdot \boldsymbol{P}^t \cdot \mathbf{1}_c = \boldsymbol{p}^{(t)} \cdot \mathbf{1}_c$$

From Theorem 11,

$$(\mu(true;\ \lceil v_1 \rceil^1)[t+1], \cdots, \mu(true;\ \lceil v_m \rceil^1)[t+1]) = \boldsymbol{p}^{(t)}$$

Thus,

$$\begin{aligned} \boldsymbol{p} \cdot \boldsymbol{P}^t \cdot \mathbf{1}_c &= (\mu(true;\ \lceil v_1 \rceil^1)[t+1], \ldots, \mu(true;\ \lceil v_m \rceil^1)[t+1]) \cdot \mathbf{1}_c \\ &= \sum_{j \in \boldsymbol{I}} \mu(true;\ \lceil v_j \rceil^1)[t+1] \end{aligned}$$

Again from PC,

$$\sum_{j \in \boldsymbol{I}} \mu(true;\ \lceil v_1 \rceil^1)[t+1] = \mu(true)[t+1]$$

This proves the theorem. □

Example

For a two-state system such as the simple Gas Burner and for a time interval of length 3

$$\begin{aligned} \mu(true)[3] &= (p_1, p_2) \cdot \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix}^2 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ &= p_1 p_{11} p_{11} + p_1 p_{11} p_{12} + p_1 p_{12} p_{21} + p_1 p_{12} p_{22} \\ &+ p_2 p_{21} p_{11} + p_2 p_{21} p_{12} + p_2 p_{22} p_{21} + p_2 p_{22} p_{22} \quad = \quad 1 \end{aligned}$$

7.4 Computation Oriented Theorems

The first theorem is useful for computation of e.g. the probability that a transition to a catastrophic state does not occur (case a) or occurs (case b) within the the first $t+1$ time units.

Theorem 14 *For a state v_i and a non-negative integer t:*

$$a: \quad \mu(\Box \neg \lceil v_i \rceil)[t+1] = \boldsymbol{p} \cdot \boldsymbol{E}_i \cdot (\boldsymbol{P} \cdot \boldsymbol{E}_i)^t \cdot \mathbf{1}_c$$

$$b: \quad \mu(\Diamond \lceil v_i \rceil])[t+1] = 1 - \boldsymbol{p} \cdot \boldsymbol{E}_i \cdot (\boldsymbol{P} \cdot \boldsymbol{E}_i)^t \cdot \mathbf{1}_c$$

(Notice, that $\boldsymbol{p} \cdot \boldsymbol{E}_i$ is the row vector obtained from $\boldsymbol{p}$ when p_i is changed to zero and that $\boldsymbol{P} \cdot \boldsymbol{E}_i$ is the matrix obtained from $\boldsymbol{P}$ when all elements in column i are changed to zero. Accordingly $\boldsymbol{p} \cdot \boldsymbol{E}_i \cdot (\boldsymbol{P} \cdot \boldsymbol{E}_i)^t \cdot \mathbf{1}_c$ is equal to $\boldsymbol{p} \cdot \boldsymbol{P}^t \cdot \mathbf{1}_c$ (i.e. $\mu(true)[t+1]$) with all terms containing p_i and p_{ji} , $j \in \boldsymbol{I}$ removed.)

In order to prove this theorem we need the following lemma:

Lemma 1 *For a state v_i and a non-negative integer t:*

$$(\mu(D_1)[t+1], \cdots \mu(D_m)[t+1]) = \boldsymbol{p} \cdot \boldsymbol{E}_i \cdot (\boldsymbol{P} \cdot \boldsymbol{E}_i)^t$$

where: for $k \in \boldsymbol{I}$

$$D_k \triangleq (\Box\neg\lceil v_i \rceil) \wedge (true;\ \lceil v_k \rceil)$$

This lemma states, that the k'th element of the row vector $\boldsymbol{p} \cdot \boldsymbol{E}_i \cdot (\boldsymbol{P} \cdot \boldsymbol{E}_i)^t$ is the probability that the system occupies state v_k after the t'th transition and that state v_i does not occur during the first $t+1$ time units.

Proof: Use induction on t.

For $t = 0$ we have $\boldsymbol{p} \cdot \boldsymbol{E}_i \cdot (\boldsymbol{P} \cdot \boldsymbol{E}_i)^t = \boldsymbol{p} \cdot \boldsymbol{E}_i \cdot \boldsymbol{E} = \boldsymbol{p} \cdot \boldsymbol{E}_i$. The result then follows from **AR** 7 and the fact that:

$$\boldsymbol{p} \cdot \boldsymbol{E}_i = (\tau_0(v_1), \cdots, \tau_0(v_{i-1}), 0, \tau_0(v_{i+1}), \cdots, \tau_0(v_m))$$

For $t \geq 0$, assume that the result holds for $t = n$, then for $t = n+1$ and for the k'th element of the vector:

$$\mu((\Box\neg\lceil v_i \rceil) \wedge (true;\ \lceil v_k \rceil))[n+2] = \mu((\Box\neg\lceil v_i \rceil) \wedge (true;\ \lceil v_k \rceil^1))[n+2] =$$
$$\sum_{j \in \mathbf{I}} \mu((\Box\neg\lceil v_i \rceil) \wedge (true;\ \lceil v_j \rceil^1;\ \lceil v_k \rceil^1))[n+2]$$

For $k = i$ this sum is zero by Theorem 6.1 ($\mu(false) = 0$).

For $k \neq i$ we can rewrite the sum, denoted *Sum*, as follows (notice the brackets !)

$$Sum = \sum_{j \in \mathbf{I}} \mu(((\Box\neg\lceil v_i \rceil) \wedge (true;\ \lceil v_j \rceil^1));\ \lceil v_k \rceil^1)[n+2]$$

By **AR** 8 we then get

$$Sum = \sum_{j \in \mathbf{I}} \mu((\Box\neg\lceil v_i \rceil) \wedge (true;\ \lceil v_j \rceil^1))[n+1] * \tau(v_j, v_k))$$

Replacing $\tau(v_j, v_k)$ by p_{jk} and returning to the vector form this implies:

$$(\mu(D_1)[n+2], \cdots, \mu(D_m)[n+2]) = (\mu(D_1)[n+1], \cdots, \mu(D_m)[n+1]) \cdot (\boldsymbol{P} \cdot \boldsymbol{E}_i)$$

where the factor $\boldsymbol{E}_i$ takes care of the exception for $k = i$.

By the induction assumption the last expression is equal to

$$\boldsymbol{p} \cdot \boldsymbol{E}_i \cdot (\boldsymbol{P} \cdot \boldsymbol{E}_i)^n \cdot (\boldsymbol{P} \cdot \boldsymbol{E}_i) = \boldsymbol{p} \cdot \boldsymbol{E}_i \cdot (\boldsymbol{P} \cdot \boldsymbol{E}_i)^{n+1}$$

This proves the lemma. □

Proof of Theorem 14:

Notice that b is proven from a and the fact that:

$$\mu(\Diamond\lceil v_i \rceil)[t+1] = 1 - \mu(\Box\neg\lceil v_i \rceil)[t+1]$$

From lemma 1,

$$\begin{aligned} \boldsymbol{p}\cdot\boldsymbol{E}_i\cdot(\boldsymbol{P}\cdot\boldsymbol{E}_i)^t\cdot\mathbf{1}_c &= \sum_{k\in\mathbf{I}}\mu((\Box\neg\lceil v_i\rceil)\wedge(true;\ \lceil v_k\rceil))[t+1] \\ &= \mu(\bigvee_{k\in\boldsymbol{I}}(\Box\neg\lceil v_i\rceil)\wedge(true;\ \lceil v_k\rceil))[t+1] \\ &= \mu(\Box\neg\lceil v_i\rceil)[t+1] \end{aligned}$$

This proves a and thereby Theorem 14. □

Notice, that if state v_i is absorbing ($p_{ii}=1$), then theorem 14 gives the probability that absorption in this state has occurred (b) or has not occurred (a) within the first $t+1$ time units.

The next theorem is useful for computation of e.g. the probability that a transition from a hazardous state v_i to a catastrophic state v_j does not occur (case a) or occurs (case b) within the first $t+1$ time units.

Theorem 15 *For states v_i, v_j and a non-negative integer t:*

$$a:\ \mu(\Box\neg(\lceil v_i\rceil;\ \lceil v_j\rceil))[t+1] = \boldsymbol{p}\cdot(\boldsymbol{P}-\boldsymbol{Z}_i\cdot\boldsymbol{P}\cdot\boldsymbol{Z}_j)^t\cdot\mathbf{1}_c$$

$$b:\ \mu(\Diamond(\lceil v_i\rceil;\ \lceil v_j\rceil))[t+1] = 1-\boldsymbol{p}\cdot(\boldsymbol{P}-\boldsymbol{Z}_i\cdot\boldsymbol{P}\cdot\boldsymbol{Z}_j)^t\cdot\mathbf{1}_c$$

(Notice, that $(\boldsymbol{P}-\boldsymbol{Z}_i\cdot\boldsymbol{P}\cdot\boldsymbol{Z}_j)$ is the matrix obtained from $\boldsymbol{P}$ when the element p_{ij} is changed to zero. Accordingly $\boldsymbol{p}\cdot(\boldsymbol{P}-\boldsymbol{Z}_i\cdot\boldsymbol{P}\cdot\boldsymbol{Z}_j)^t\cdot\mathbf{1}_c$ is equal to $\boldsymbol{p}\cdot\boldsymbol{P}^t\cdot\mathbf{1}_c$ (i.e. $\mu(true)[t+1]$) with all terms containing p_{ij} removed.)

The proof of this theorem follows exatly the same pattern as the proof of theorem 14, and is omitted. The required lemma, which resembles lemma 1, is:

Lemma 2 *For states v_i and v_j and a non-negative integer t:*

$$(\mu(D_1)[t+1],\cdots,\mu(D_m)[t+1]) = \boldsymbol{p}\cdot(\boldsymbol{P}-\boldsymbol{Z}_i\cdot\boldsymbol{P}\cdot\boldsymbol{Z}_j)^t$$

where: for $k\in\boldsymbol{I}$

$$D_k \triangleq (\Box\neg(\lceil v_i\rceil;\ \lceil v_j\rceil))\wedge(true;\ \lceil v_k\rceil)$$

This lemma states, that the k'th element of the row vector $\boldsymbol{p}\cdot(\boldsymbol{P}-\boldsymbol{Z}_i\cdot\boldsymbol{P}\cdot\boldsymbol{Z}_j)^t$ is the probability that the system occupies state v_k after the t'th transition and no transition from state v_i to state v_j occurs during the first $t+1$ time units.

Theorem 15 has the following immediate corollary:

Corollary 1 *For a state v_i and a non-negative integer t:*

$$a:\ \mu(\Box(\lceil v_i\rceil\Rightarrow l\leq 1))[t+1] = \boldsymbol{p}\cdot(\boldsymbol{P}-\boldsymbol{Z}_i\boldsymbol{P}\boldsymbol{Z}_i)^t\cdot\mathbf{1}$$

$$b:\ \mu(\Diamond(\lceil v_i\rceil\wedge l>1))[t+1] = 1-\boldsymbol{p}\cdot(\boldsymbol{P}-\boldsymbol{Z}_i\boldsymbol{P}\boldsymbol{Z}_i)^t\cdot\mathbf{1}$$

(Notice that this corollary provides a more straight-forward way to calculate μ(**Des-1**) (case a) or $\mu(\neg$**Des-1**) (case b) for the Gas Burner example, cf. Section 6.)

The next theorem deals with certain chopped formulas, which generalize and unite **AR** 8 and **AR** 2. However, before we can state the theorem a definition is needed.

Definition 11 *For each subset J of the index set $\boldsymbol{I} = \{1, \cdots, m\}$, $J \subseteq \boldsymbol{I}$, we define:*

1. *an auxiliary matrix $\boldsymbol{P}_J$ from the single step transition probability matrix $\boldsymbol{P}$ as follows:*

$$\boldsymbol{P}_J \triangleq \begin{pmatrix} p'_{11} & \cdot & \cdot & p'_{1m} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ p'_{m1} & \cdot & \cdot & p'_{mm} \end{pmatrix} \quad \text{where} \quad p'_{ij} = \begin{cases} p_{ij} & \text{if } j \in J \\ 0 & \text{if } j \in \overline{J} \end{cases}$$

here $\overline{J}$ is the complement $\boldsymbol{I} \setminus J$ of J.

2. *a composite state V_J as follows:*

$$v_J \triangleq \bigvee_{j \in J} v_j$$

Notice that, according to the definition of v_J, $(\lceil v_J \rceil \wedge l = t)$ represents any sequence

$$(\lceil v_{j_1} \rceil^1;\ \lceil v_{j_2} \rceil^1;\ \cdots \lceil v_{j_t} \rceil^1)$$

of elementary states of duration 1 such that $j_i \in J$ for $i \in \{1, \cdots, t\}$.

The theorem makes use of the short-hand notation $\boldsymbol{z}_i$ for the row vector $(\mathbf{1}_r \cdot Z_i)$ (cf. Definition 7).

Theorem 16 *For an arbitrary index set $J \subseteq \boldsymbol{I}$, an arbitrary duration formula D and an arbitrary state $v_i \in V$*

$$a: \quad \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_J \rceil)[t + k + 1] = \\ \mu(D \wedge (true;\ \lceil v_i \rceil)[k] \cdot \boldsymbol{z}_i \cdot (\boldsymbol{P}_J)^{t+1} \cdot \mathbf{1}_c$$

$$b: \quad \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \Diamond \lceil v_J \rceil)[t + k + 1] = \\ \mu(D \wedge (true;\ \lceil v_i \rceil)[k] \cdot (1 - \boldsymbol{z}_i \cdot (\boldsymbol{P}_{\overline{J}})^{t+1} \cdot \mathbf{1}_c)$$

To prove this theorem, the following notations and the following lemma are helpful.

$$q \triangleq \mu(D \wedge (true;\ \lceil v_i \rceil))[k]$$

And for $j \in \boldsymbol{I}$

$$q_j[t] \triangleq \begin{cases} \mu((D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_J \rceil) \wedge (true;\ \lceil v_j \rceil))[t + k + 1] & \text{if } j \in J \\ 0 & \text{if } j \in \overline{J} \end{cases}$$

Lemma 3 *For the q, $q_j[t]$ defined above,*

$$(q_1[t], \cdots, q_m[t]) = q \cdot \boldsymbol{z}_i \cdot (\boldsymbol{P}_J)^{t+1}$$

The proofs of lemma 3 and theorem 16 are placed in appendix A and appendix B respecitively.

A common feature of all the previous theorems in this section is that they are obtained by means of matrix functions which replace certain entries in the probability matrices $\boldsymbol{p}$ and $\boldsymbol{P}$ by zeros.

A more general class of theorems dealing with state sequences is based on matrix functions which also introduce deficiencies in the probability matrices, but now these matrices are of increased order (more

specifically, they can be interpreted as the probability matrices for a probabilistic automaton which is obtained form the original one by addition of auxiliary state(s) in such a way, that the terms in the expansion of $\mu(true)[t+1]$ (cf. the example following Theorem 13) remain the same. This idea was suggested to the authors by Niels Herman Hansen, Institute of Mathematical Statistics and Operations Research, Technical University of Denmark.). The last theorem in this paper is an illustration of this approach.

Before we can state the theorem a definition of the relevant matrices is needed.

Definition 12 *For the $m \times m$ transition probability matrix $\boldsymbol{P}$ let $\boldsymbol{P}^{+}_{ijk}$ denote the $(m+1) \times (m+1)$ matrix obtained from $\boldsymbol{P}$ as follows:*

$$\boldsymbol{P}^{+}_{ijk} = \left\{ \begin{array}{c|c} \boldsymbol{A}_{n\times n} & \boldsymbol{B}_{n\times 1} \\ \hline \boldsymbol{C}_{1\times n} & \boldsymbol{D}_{1\times 1} \end{array} \right\}$$

where:

$$\boldsymbol{A}_{n\times n} \triangleq \boldsymbol{P} - \boldsymbol{Z}_i \boldsymbol{P} \boldsymbol{Z}_j \quad i.e. \quad a_{hl} = \left\{ \begin{array}{ll} p_{hl} & for \quad hl \neq ij \\ 0 & for \quad hl = ij \end{array} \right.$$

$$\boldsymbol{B}_{n\times 1} \triangleq \boldsymbol{Z}_i \boldsymbol{P} \boldsymbol{Z}_j \boldsymbol{1}_c \quad i.e. \quad b_h = \left\{ \begin{array}{ll} p_{ij} & for \quad h = i \\ 0 & for \quad h \neq i \end{array} \right.$$

$$\boldsymbol{C}_{1\times n} \triangleq \boldsymbol{1}_r \boldsymbol{Z}_j \boldsymbol{P} \boldsymbol{E}_j \boldsymbol{E}_k \quad i.e. \quad c_h = \left\{ \begin{array}{ll} p_{jh} & for \quad h \neq k \wedge h \neq k \\ 0 & for \quad h = k \vee h = k \end{array} \right.$$

$$\boldsymbol{D}_{1\times 1} \triangleq \boldsymbol{1}_r \boldsymbol{Z}_j \boldsymbol{P} \boldsymbol{Z}_j \boldsymbol{E}_k \boldsymbol{1}_c \quad i.e. \quad d = \left\{ \begin{array}{ll} p_{jj} & for \quad j \neq k \\ 0 & for \quad j = k \end{array} \right.$$

Further, for the $1 \times m$ initial probability vector $\boldsymbol{p}$ let $\boldsymbol{p}^{+}$ denote the $1 \times (m+1)$ vector:

$$\boldsymbol{p}^{+} \triangleq (p_1, p_2, \cdots p_n, 0)$$

Finally, let $\boldsymbol{1}^{+}_c$ denote the $(m+1) \times 1$ column vector in which all elements are 1.

Example

For:

$$\boldsymbol{P} = \left\{ \begin{array}{cccc} p_{11} & p_{12} & p_{13} & p_{14} \\ p_{21} & p_{22} & p_{23} & p_{24} \\ p_{31} & p_{32} & p_{33} & p_{34} \\ p_{41} & p_{42} & p_{43} & p_{44} \end{array} \right\}$$

we have:

$$\boldsymbol{P}^{+}_{123} = \left\{ \begin{array}{cccc|c} p_{11} & 0 & p_{13} & p_{14} & p_{12} \\ p_{21} & p_{22} & p_{23} & p_{24} & 0 \\ p_{31} & p_{32} & p_{33} & p_{34} & 0 \\ \hline p_{41} & p_{42} & p_{43} & p_{44} & 0 \\ \hline p_{21} & 0 & 0 & p_{24} & p_{22} \end{array} \right\} \quad \text{and} \quad \boldsymbol{P}^{+}_{122} = \left\{ \begin{array}{cccc|c} p_{11} & 0 & p_{13} & p_{14} & p_{12} \\ p_{21} & p_{22} & p_{23} & p_{24} & 0 \\ p_{31} & p_{32} & p_{33} & p_{34} & 0 \\ \hline p_{41} & p_{42} & p_{43} & p_{44} & 0 \\ \hline p_{21} & 0 & p_{23} & p_{24} & 0 \end{array} \right\}$$

(The deficiency of the probability matrix $\boldsymbol{P}^+_{123}$ is manifested by the lack of the element p_{23} in row 5 (thus, the sum of the elements in this row becomes less than 1 if $p_{23} > 0$. Similarly the deficiency of $\boldsymbol{P}^+_{122}$ is manifested by the lack of the element p_{22} in row 5.)

Theorem 17 *For all $i,j,k \in \boldsymbol{I}$ and for a non-negative integer t:*

$$a: \quad \mu(\Box\neg(\lceil v_i\rceil;\ \lceil v_j\rceil;\ \lceil v_k\rceil))[t+1] = \boldsymbol{p}^+(\boldsymbol{P}^+_{ijk})^t\mathbf{1}^+_c$$

$$b: \quad \mu(\Diamond(\lceil v_i\rceil;\ \lceil v_j\rceil;\ \lceil v_k\rceil))[t+1] = 1 - \boldsymbol{p}^+(\boldsymbol{P}^+_{ijk})^t\mathbf{1}^+_c$$

In order to prove this theorem we need the following lemma

Lemma 4 *For all $i,j,k,n: \{1,\cdots,m\}$ and for a non-negative integer t:*

$$(\mu(D_1[t+1],\cdots\mu(D_{m+1})[t+1]) = \boldsymbol{p}^+(\boldsymbol{P}^+_{ijk})^t$$

where:

$$D_n \triangleq \begin{cases} D \wedge (true;\ \lceil v_n\rceil) & \text{if } n \neq j \\ D \wedge (true;\ \lceil v_j\rceil) \wedge \neg(true;\ \lceil v_i\rceil;\ \lceil v_j\rceil) & \text{if } n = j \\ D \wedge (true;\ \lceil v_i\rceil;\ \lceil v_j\rceil) & \text{if } n = m+1 \end{cases}$$

$$D \triangleq \Box\neg(\lceil v_i\rceil;\ \lceil v_j\rceil;\ \lceil v_k\rceil)$$

The proof of lemma 4 is lengthly and is therefore placed in appendix C.

Proof of theorem 17: Notice that b is proved from a and the fact that:

$$\mu(\Diamond(\lceil v_i\rceil;\ \lceil v_j\rceil;\ \lceil v_k\rceil))[t+1] = 1 - \mu(\Box\neg(\lceil v_i\rceil;\ \lceil v_j\rceil;\ \lceil v_k\rceil))[t+1]$$

From lemma 4 (and recalling that $\mathbf{I} = \{1,\cdots,m\}$ and $\mathbf{I}_j = \mathbf{I} \setminus \{j\}$):

$$\begin{aligned} \boldsymbol{p}^+(\boldsymbol{P}^+_{ijk})\mathbf{1}_c{}^+ &= \sum_{n\in\mathbf{I}_j} \mu(D_n)[t+1] + \mu(D_j)[t+1] + \mu(D_{m+1})[t+1] \\ &= \sum_{n\in\mathbf{I}} \mu(\Box\neg(\lceil v_i\rceil;\ \lceil v_j\rceil;\ \lceil v_k\rceil) \wedge (true;\ \lceil v_n\rceil))[t+1] \\ &= \mu(\bigvee_{n\in\mathbf{I}} (\Box\neg(\lceil v_i\rceil;\ \lceil v_j\rceil;\ \lceil v_k\rceil) \wedge (true;\ \lceil v_n\rceil))[t+1] \\ &= \mu(\Box\neg(\lceil v_i\rceil;\ \lceil v_j\rceil;\ \lceil v_k\rceil))[t+1] \end{aligned}$$

This proves a and thereby theorem 17. □

7.5 Applying to The Examples

Gas Burner

Consider the Gas Burner illustrated in Section 3.1. Let

$$V \triangleq \{v_1, v_2\} \text{ where: } v_i \triangleq \begin{cases} \neg Leak & \text{if } i = 1 \\ Leak & \text{if } i = 2 \end{cases}$$

$$\boldsymbol{p} \triangleq (p_1, p_2) \text{ (where } p_1 = 1 \text{ and } p_2 = 0)$$

$$\boldsymbol{P} \triangleq \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix}$$

As we mentioned in connection with the corollary of Theorem 15,

$$\mu(\textbf{Des-1})[t] = \boldsymbol{p} \cdot (\boldsymbol{P} - \boldsymbol{Z}_2 \cdot \boldsymbol{P} \cdot \boldsymbol{Z}_2)^t \cdot \mathbf{1}_c = (p_1, p_2) \cdot \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & 0 \end{pmatrix}^t \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

In duration calculus we can rewrite ¬**Des**-2 as follows:

$$\begin{aligned} \neg\textbf{Des-2} &\Leftrightarrow \Diamond((\lceil Leak \rceil;\ ]\neg Leak[;\ \lceil Leak \rceil) \wedge (l \leq 31)) \\ &\Leftrightarrow \exists k : ((true;\ \lceil Leak \rceil) \wedge (l = k);\ \lceil \neg Leak \rceil \wedge (l \leq 29);\ \lceil Leak \rceil^1;\ true) \end{aligned}$$

For a given t, $\mu(\neg\textbf{Des-2})[t]$ is only non-zero if $t \geq k + h + 1$ where $k \geq 1$ and $1 \leq h \leq 29$.

Introducing

$$h_{max} = min((t - k - 1), 29)$$

we can express $\mu(\neg\textbf{Des} - \textbf{2}[t]$ by a double summation over all possible k's and h's (this is because we can treat the existential quantification as a disjunction over all possible k's and h's in which the disjuncts are mutually exclusive).

$$\begin{aligned} & \mu(\neg\textbf{Des-2})[t] \\ & \qquad \text{(by AR 6)} \\ = & \sum_{k=1}^{t-2} \sum_{h=1}^{h_{max}} \mu(true;\ \lceil Leak \rceil) \wedge (l = k);\ \lceil \neg Leak \rceil \wedge (l = h);\ \lceil Leak \rceil^1)[k + h + 1] \\ & \qquad \text{(by Theorem 16 and Definition 7)} \\ = & \sum_{k=1}^{t-2} \sum_{h=1}^{h_{max}} \mu(true;\ \lceil Leak \rceil) \wedge (l = k);\ \lceil \neg Leak \rceil \wedge (l = h))[k + h] \cdot (\boldsymbol{z}_1 \cdot \boldsymbol{P}_{\{2\}} \cdot \mathbf{1}_c) \\ & \qquad \text{(by Theorem 16 again)} \\ = & \sum_{k=1}^{t-2} \sum_{h=1}^{h_{max}} \mu(true;\ \lceil Leak \rceil)[k] \cdot (\boldsymbol{z}_2 \cdot \boldsymbol{P}_{\{1\}}^h \cdot \mathbf{1}_c) \cdot (\boldsymbol{z}_1 \cdot \boldsymbol{P}_{\{2\}} \cdot \mathbf{1}_c) \\ & \qquad \text{(by Theorem 12, Definition 9 and Definition 7)} \\ = & \sum_{k=1}^{t-2} \sum_{h=1}^{h_{max}} (\boldsymbol{p} \cdot \boldsymbol{P}^{k-1} \cdot h_2) \cdot (\boldsymbol{z}_2 \cdot \boldsymbol{P}_{\{1\}}^h \cdot \mathbf{1}_c) \cdot (\boldsymbol{z}_1 \cdot \boldsymbol{P}_{\{2\}} \cdot \mathbf{1}_c) \end{aligned}$$

The Protocol

For the protocol over an unreliable medium in Section 6.2, we define the following notations. For $\boldsymbol{I} = \{1,2,3,4,5\}$, let

$$
\begin{aligned}
V &\triangleq \{v_i \mid i \in \boldsymbol{I}, v_1 = s, v_2 = b, v_3 = m, v_4 = r, v_5 = e\} \\
\boldsymbol{P} &\triangleq \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & p & 1-p \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} \\
\boldsymbol{p} &\triangleq (1,0,0,0,0)
\end{aligned}
$$

Consider the conditional reoccurrence of the error state e. Still let

$$D_1 \triangleq (true;\ \lceil e \rceil) \wedge (l = k);\ \lceil \neg e \rceil \wedge (l = k_1);\ \lceil e \rceil;\ true)$$

$$D_2 \triangleq (true;\ \lceil e \rceil) \wedge (l = k);\ true)$$

We would like to find the conditional probabilisty of D_1 given D_2. That is, $\dfrac{\mu(D_1 \wedge D_2)[t]}{\mu(D_2)[t]}$ when $\mu(D_2)[t] \neq 0$.

If $t < k + k_1 + 1$, $\mu(D_1)[t] = 0$. Therefore we are only intersted in cases where $t \geq k + k_1 + 1$ and accordingly we consider the probabilities $\mu(D_1)[k + k_1 + 1 + u]$ and $\mu(D_2)[k + k_1 + 1 + u]$ where $u > 0$.

Notice also, that with the definitions of D_1 and D_2 given above, $\mu(D_1 \wedge D_2)[t] = \mu(D_1)[t]$.

From **AR** 6, Theorem 12 and Definition 9

$$
\begin{aligned}
\mu(D_2)[k + k_1 + 1] &= \mu(true;\ \lceil e \rceil)[k] \\
&= \begin{cases} \boldsymbol{p} \cdot \boldsymbol{P}^{k-1} \cdot \boldsymbol{h}_5 & \text{if } k > 0 \\ 0 & \text{if } k = 0 \end{cases}
\end{aligned}
$$

When $k_1 = 0$, $\mu(D_1)[t] = 0$. Thus we assume $k_1 > 0$.

$$
\begin{aligned}
& \mu(D_1)[t + k + k_1 + 1] \\
&= \mu((true;\ \lceil e \rceil) \wedge (l = k);\ \lceil \neg e \rceil \wedge (l = k_1);\ \lceil e \rceil)[k + k_1 + 1] && \text{(AR6)} \\
&= \mu(\bigvee_{j=1}^{4}((true;\ \lceil e \rceil) \wedge (l = k);\ \lceil \neg e \rceil \wedge (l = k_1) \wedge (true;\ \lceil v_j \rceil);\ \lceil e \rceil))[k + k_1 + 1] && \text{(Th.6(3))} \\
&= \sum_{j=1}^{4} \mu((true;\ \lceil e \rceil) \wedge (l = k);\ \lceil \neg e \rceil \wedge (l = k_1) \wedge (true;\ \lceil v_j \rceil);\ \lceil e \rceil)[k + k_1 + 1] && \text{(AR3)} \\
&= \sum_{j=1}^{4} \mu((true;\ \lceil e \rceil) \wedge (l = k);\ \lceil \neg e \rceil \wedge (l = k_1) \wedge (true;\ \lceil v_j \rceil))[k + k_1] \cdot z_j \cdot \boldsymbol{P}_{\{5\}} \cdot \mathbf{1_c} && \text{(Th.16)} \\
&= \mu(true;\ \lceil e \rceil)[k] \cdot z_5 \cdot (\boldsymbol{P}_{\boldsymbol{I}_5})^{k_1} \cdot \overline{\boldsymbol{E}} \cdot \mathbf{1_c} && \text{(Lem.3)} \\
&= \boldsymbol{p}^{(k-1)} \cdot \boldsymbol{h}_5 \cdot z_5 \cdot (\boldsymbol{P}_{\boldsymbol{I}_5})^{k_1} \cdot \overline{\boldsymbol{E}} \cdot \mathbf{1_c} && \text{(Th. 12)}
\end{aligned}
$$

where:

$$\overline{E} \triangleq \begin{pmatrix} z_1 \cdot P_{\{5\}} \cdot \mathbf{1_c} & 0 & 0 & 0 & 0 \\ 0 & z_2 \cdot P_{\{5\}} \cdot \mathbf{1_c} & 0 & 0 & 0 \\ 0 & 0 & z_3 \cdot P_{\{5\}} \cdot \mathbf{1_c} & 0 & 0 \\ 0 & 0 & 0 & z_4 \cdot P_{\{5\}} \cdot \mathbf{1_c} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1-p & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Finally, for $a(t,k_1) = \dfrac{\mu(D_1 \wedge D_2)[t]}{\mu(D_2)[t]} = \dfrac{\mu(D_1)[t]}{\mu(D_2)[t]}$, defined for $\mu(D_2)[t] > 0$, we have:

$$a(t,k_1) = z_5 \cdot P_{I_5}^{k_1} \cdot \overline{E} \cdot \mathbf{1}_c = (0,0,0,0,1) \cdot \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & p & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}^{k_1} \cdot \begin{pmatrix} 0 \\ 0 \\ 1-p \\ 0 \\ 0 \end{pmatrix}$$

where the last column vector is the product of $\overline{E}$ and $\mathbf{1}_c$.

8 Conclusion and Discussion

In this paper we have developed a Probabilistic Calculus (PC) based on Duration Calculus (DC), a time-interval logic, and Markov chains over discrete time. The work was motivated by a desire to establish a common framework for verification of correctness as well as dependability of a design.

The use of PC has been illustrated by two running examples

1. Dependability analysis of a simple Gas Burner with unreliable flame detector and failing flame. Here we estimate the probability that a safety requirement **Req-1**, known to be satisfied by two design decisions **Des-1** and **Des-2**, is violated during the first t time-units because of the imperfections. The analysis involves determination of the probabilities of violation of either design decision.
2. Dependability analysis of a protocol for transmission via an unreliable communication medium. Here we investigate soft-deadline properties as well as the conditional probability of error re-occurrences within the first t time units.

It is shown, that these examples can be handled by means of the basic calculus, but these calculations also reveals a need for more advanced computation theorems oriented towards mechanizable numerical calculations.

Such a level has therefore been established by application of the probability matrices from the theory of stochastic processes. So far, theorems for calculation of the probability of specific behaviours within the first t time units have been developed for the following cases:

- Transition to a specific state (e.g. an absorbing state representing that an accident has occurred), Theorem 14. and Corollary 1.

- Transition from a specific state to another specific state (e.g. from a hazardous state to an accident state), Theorem 15 and Corollary 1.
- Certain chopped behaviours, Theorem 16
- Transitions involving a specified path of three consecutive states, Theorem 17.

With this collection of theorems the running examples were revisited. Whereas Corollary 1 applies directly to **Des-1**, it still takes some effort to prepare **Des-2** and the re-occurrence problem for the protocol for application of the theorems (this is especially true for **Des-2** which is rather sophisticated). This motivates future development of still stronger theorems.

For previous work on timed probabilistic calculi we refer to [HJ89] and [LRSZ92]

The approach in [HJ89], based on CTL in [CES83], can be used to analyse the soft-deadline properties of the protocol. It can also be used to analyse **Des-1**; but we have not succeded in using it to analyse the probabilities of **Des-2** or the error re-occurrence problem of the protocol. In [LRSZ92], we presented a probabilistic duration calculus which is a modal logic about the prefix time intervals. In the present paper, however, we have developed a first order logic for calculation of $\mu(D)[t]$. We believe that a first order logic is easier to be understand and can be used without loss of expressiveness. Compared to [LRSZ92], the present paper also give more details on PC and adds computation oriented theorems to the theory.

A more indirect approach to joint verification of correctness and dependability of a design has been reported in [SNH91]. In this work the dependability analysis is based on a Markov model over continous time, developed in such a way that it is consistent with a CSP model used for verification of correctness. With this approach, a main problem is that all waiting times must be stochastic with exponential distributions, i.e. it is not suited for problems involving fixed time intervals.

Future work will include reinforcement of the collection of computation oriented theorems with regard to important topics in reliability engineering (for example, we have not considered asymptotic behaviour or determination of mean values in this paper).

Finally, a major goal is to investigate how this theory can be merged with existing theories for design of fault-tolerant systems [LJ91, Liu91, Nor92] with regard to joint verification of design as well as dependability.

Acknowledgements: We would like to acknowledge helpful discussions with N.H. Hansen, M.R. Hansen and H. Rischel.

References

[CES83] E.M. Clarke, E.A Emerson, and A.P. Sistla. Automatic verification of finite-state concurrent systems using temporal logic specification: A practical approach. In *Proc. 10th ACM Symp. on Principles of Programming Languages*, pages 117–126, 1983.

[CM90] D. R. Cox and H. D. Miller. *The Theory of Stochastic Processes.* Chapman and Hall, six'th edition edition, 1990.

[HJ89] H. Hansson and B. Jonsson. A framework for reasoning about time and reliability. In *Proc. 10th IEEE Real-Time System Symposium, S:a Monica, Ca.*, 1989.

[HRR91] K.M. Hansen, A.P. Ravn, and H. Rischel. Specifying and verifying requirements of real-time systems. In *ACM SIGSOFT '91 Conference on Software for Critical Systems*, December 1991.

[HZ92] M. R. Hansen and C.C. Zhou. Semantics and completeness of duration calculus. Technical report, ProCoS, 1992. To appear in *Real-Time: Theorem in Practice*, J.W. de Bakker, W.-P. de Rover and G. Rozenberg (Eds.) in the LNCS-series.

[Liu91] Z. Liu. *Fault-Tolerant Programming by Transformations*. PhD thesis, Department of Computer Science, University of Warwick, 1991.

[LJ91] Z. Liu and M. Joseph. Transformation of programs for fault-tolerance. *Formal Aspects of Computing*, To appear, 1991.

[LRSZ92] Z. Liu, A.P. Ravn, E.V. Sørensen, and C.C. Zhou. A probabilistic duration calculus. Technical report, Department of Computer Science, Technical University of Demark, 1992. Submitted for Second International Workshop on Responsive Computing Systems, Japan.

[LS89] K. Larsen and A. Skou. Bisimulation through probabilistic testing. In *Proc. 16th ACM Symposium on Principles of Programming Languages*, 1989.

[MSS82] P. M. Melliar-Smith and R. L. Schwartz. Formal specification and mechanical verification of SIFT: A fault tolerant flight control system. *IEEE Trans. on Computers*, 31(7), 1982.

[Nor92] J. Nordahl. *Specification and Design of Dependable Communicating Systems*. PhD thesis, Department of Computer Science, Technical University of Denmark, 1992.

[RR91] A.P. Ravn and H. Rischel. Requirements capture for embedded real-time systems. In *IMACS-IFAC Symposium MCTS, Lille, France*, pages vol. 2, pp. 147–152, 1991.

[SNH91] E.V. Sørensen, J. Nordahl, and N.H. Hansen. From CSP models to Markov models: a case study. Technical Report (Submitted for publication in IEEE Transactions on Software Engineering), Institute of Computer Science, Technical University of Denmark, 1991.

[SRRZ92] J.U. Skakkebæk, A.P. Ravn, H. Rischel, and Chaochen Zhou. Specification of embedded, real-time systems. In *EuroMicro Workshop on Formal Methods for Real-Time Systems (submitted)*, 1992.

[ZHR92] C.C. Zhou, C.A.R. Hoare, and A.P. Ravn. A calculus of durations. *Information Processing Letters*, 40(5):269–276, 1992.

A Proof of Lemma 3

The proof is by induction on t.

$t = 0$:

It is easy to check that

$$(q_1[0], \cdots, q_m[0]) = q \cdot (\boldsymbol{P}_J)$$

Assume that the lemma holds for $t = u \geq 0$

$$(q_1[u], \cdots, q_m[u]) = q \cdots (\boldsymbol{P}_J)^{u+1}$$

We want to prove that

$$(q_1[u+1], \cdots, q_m[u+1]) = q \cdot \mathbf{1}_i \cdot (\boldsymbol{P}_J)^{u+2}$$

Look at the right hand side of this equation

$$\begin{aligned} q \cdot \mathbf{1_i} \cdot (\boldsymbol{P}_J)^{u+2} &= q \cdot \mathbf{1_i} \cdot (\boldsymbol{P}_J)^{u+1} \cdot \boldsymbol{P}_J \\ &= (q_1[u], \cdots, q_m[u]) \cdot \boldsymbol{P}_J && \text{(by induction assumption)} \\ &= (\sum_{j\in 1}^{m} q_j[u] * p'_{j1}, \cdots, \sum_{j=1}^{m} q_j[u] * p'_{jm}) \end{aligned}$$

We now have to prove that for $n \in \boldsymbol{I}$

$$\sum_{j=1}^{m} q_j[u] * p'_{jn} = q_n[u+1]$$

For $n \in \overline{J}$, since $p'_{jn} = 0$,

$$\sum_{j=1}^{m} q_j[u] * p'_{jn} = 0 = q_n[u+1]$$

For $n \in J$, since $q_j[u] = 0$ if $j \in \overline{J}$,

$$\begin{aligned} & \sum_{j=1}^{m} q_j[u] * p'_{jn} \\ = & \sum_{j\in J} q_j[u] * p_{jn} \\ = & \sum_{j\in J} \mu((D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_J \rceil) \wedge (true;\ \lceil v_j \rceil)[u+k+1] * p_{jn} \\ = & \sum_{j\in J} \mu((D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_J \rceil) \wedge (true;\ \lceil v_j \rceil);\ \lceil v_n \rceil^1)[u+k+2] && \textbf{(AR8)} \\ = & \mu(\bigvee_{j\in J}((D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_J \rceil) \wedge (true;\ \lceil v_j \rceil));\ \lceil v_n \rceil^1))[u+2] && \textbf{(AR3)} \\ = & \mu((D \wedge (true;\ \lceil v_i \rceil \wedge (l = k);\ \lceil v_J \rceil) \wedge (true;\ \lceil v_n \rceil))[u+2] && \text{(Th.6(3))} \\ = & q_n[u+2] \end{aligned}$$

This ends the proof of the lemma.

B Proof of Theorem 16

For the case a:

$$\begin{aligned} & \mathbf{1_i} \cdot q \cdot (\boldsymbol{P}_J)^{t+1} \cdot \mathbf{i_c} = \sum_{j=1}^{m} q_j[t] \\ = & \sum_{j\in J} q_j[t] && \text{(Notice } q_j[t] = 0 \text{ if } j \in \overline{J}) \\ = & \sum_{j\in J} \mu((D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_J \rceil) \wedge (true;\ \lceil v_j \rceil)[t+k+1] \\ = & \mu(\bigvee_{j\in J}((D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_J \rceil) \wedge (true;\ \lceil v_j \rceil))[t+k+1] && \textbf{(AR3)} \\ = & \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_J \rceil)[t+k+1] && \text{(Th.6(3))} \end{aligned}$$

Case b is proven from case a:

$$
\begin{aligned}
& q \cdot (1 - \mathbf{1_i} \cdot (\boldsymbol{P}_{\overline{J}})^{t+1} \cdot \mathbf{1_c} \\
= \; & q - q \cdot \mathbf{1_i} \cdot (\boldsymbol{P}_{\overline{J}})^{t+1} \cdot \mathbf{1_c} \\
= \; & q - \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_{\overline{J}} \rceil)[t + k + 1] && \text{(Th.17}(a)\text{)} \\
= \; & \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ (l = t + 1))[t + k + 1] - && \textbf{(AR6)} \\
& \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_{\overline{J}} \rceil)[t + k + 1] \\
= \; & \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_{\overline{J}} \rceil \vee \Diamond \lceil v_J \rceil))[t + k + 1] - && \text{(Th.6(3))} \\
& \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_{\overline{J}} \rceil)[t + k + 1] \\
= \; & \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_{\overline{J}} \rceil)[t + k + 1] + \\
& \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \Diamond \lceil v_J \rceil)[t + k + 1] - && \textbf{(AR3)} \\
& \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \lceil v_{\overline{J}} \rceil)[t + k + 1] \\
= \; & \mu(D \wedge (true;\ \lceil v_i \rceil) \wedge (l = k);\ \Diamond \lceil v_J \rceil)[t + k + 1]
\end{aligned}
$$

Thus we have proven the theorem.

C Proof of Lemma 4

The proof of the lemma is by induction on t.

$t = 0$:

It is easy to check that

$$(\mu(D_1)[1], \cdots, \mu(D_{m+1})[1]) = \boldsymbol{p}^+ (\boldsymbol{P}^+_{ijk})^0 = \boldsymbol{p}^+$$

This shows the lemma holds for $t = 0$.

Assume that the lemma holds for $t = u \geq 0$

$$(\mu(D_1)[u + 1], \cdots, \mu(D_{m+1})[u + 1]) = \boldsymbol{p}^+ (\boldsymbol{P}^+_{ijk})^u$$

Let $t = u + 1$:

$$\boldsymbol{p}^+ (\boldsymbol{P}^+_{ijk})^{u+1} = \boldsymbol{p}^+ (\boldsymbol{P}^+_{ijk})^u \boldsymbol{P}^+_{ijk}$$

From the induction assumption

$$\boldsymbol{p}^+ (\boldsymbol{P}^+_{ijk})^u \boldsymbol{P}^+_{ijk} = (\mu(D_1)[u + 1], \cdots, \mu(D_{m+1})[u + 1]) \cdot \boldsymbol{P}^+_{ijk}$$

Notice that the right hand side of this equation is the following row vector, denoted $\mathbf{r}[u + 2]$

$$(\sum_{h=1}^{m+1} \mu(D_h)[u + 1] * q_{h1}, \cdots, \sum_{h=1}^{m+1} \mu(D_h)[u + 1] * q_{hm+1})$$

where q_{hn} is the (h,n)-element of $\boldsymbol{P}^{+}_{ijk}$, for $h,n \in \{1,\ldots,m+1\}$.

Now we want to prove that the n'th element of this row vector equals to $\mu(D_n)[u+2]$, for $n \in \{1,\ldots,m+1\}$.

For the index set $\boldsymbol{I} = \{1,\ldots,m\}$, let $\boldsymbol{I}_j$ denote the index set $\boldsymbol{I} \setminus \{j\}$. Then the n'th element of $\mathbf{r}[u+2]$ is

$$\begin{array}{lll} & \sum_{h=1}^{m+1} \mu(D_h)[u+1] * q_{hn} & \\ = & \sum_{h\in \boldsymbol{I}_j} \mu(D_m)[u+1] * q_{hn} & \cdots \quad \cdots \quad (F_1) \\ + & \mu(D_j)[u+1] * q_{jn} & \cdots \quad \cdots \quad (F_2) \\ + & \mu(D_{m+1})[u+1] * q_{m+1n} & \cdots \quad \cdots \quad (F_3) \end{array}$$

Hence, we have to prove that, for $n \in \{1,\ldots,m+1\}$

$$\mu(D_n)[u+2] = F_1 + F_2 + F_3$$

There are five cases to be considered.

Case 1: $n \neq j \wedge n < m+1$

From the definition of $\boldsymbol{P}^{+}_{ijk}$, $q_{hn} = p_{hn}$ when $h \in I_j$. Thus

$$\begin{array}{lll} F & = & \sum_{h\in \boldsymbol{I}_j} \mu(D_h)[u+1] * p_{hn} \\ & = & \sum_{h\in \boldsymbol{I}_j} \mu(D \wedge (true;\ \lceil v_h \rceil))[u+1] * p_{hn} \\ & = & \sum_{h\in \boldsymbol{I}_j} \mu(D \wedge (true;\ \lceil v_h \rceil);\ \lceil v_n \rceil^1)[u+2] \qquad \textbf{(AR8)} \\ & = & \mu(\bigvee_{h\in \boldsymbol{I}_j} (D \wedge (true;\ \lceil v_h \rceil);\ \lceil v_n \rceil^1)[u+2] \quad \cdots \quad (F_{11}) \text{ (exclusiveness)} \end{array}$$

Since $n < m+1$, $q_{jn} = p_{jn}$

$$\begin{array}{lll} F_2 & = & \mu(D_j)[u+1] * p_{jn} \\ & = & \mu(D \wedge (true;\ \lceil v_j \rceil) \wedge \neg(true;\ \lceil v_i \rceil;\ \lceil v_j \rceil);\ \lceil v_n \rceil^1)[u+2] \quad \cdots \quad (F_{21}) \end{array}$$

Notice that

$$q_{m+1n} = \begin{cases} p_{jn} & \text{if } n \neq k \\ 0 & \text{if } n = k \end{cases}$$

Subcase 1.1 $n \neq k$

$$\begin{array}{lll} F_3 & = & \mu(D_{m+1})[u+1] * p_{jn} \\ & = & \mu(D \wedge (true;\ \lceil v_i \rceil;\ \lceil v_j \rceil);\ \lceil v_n \rceil^1)[u+2] \quad \cdots \quad (F_{31}) \end{array}$$

Now look at the duration formulas in F_{11}, F_{12} and F_{13}.

$$D \wedge (true;\ \lceil v_n \rceil) \wedge (l = u+2) \Leftrightarrow$$

$$\begin{array}{ll} \bigvee_{h\in \boldsymbol{I}_j} (D \wedge (true;\ \lceil v_h \rceil);\ \lceil v_n \rceil^1) \wedge (l = u+2) \vee & \cdots \quad (D_{11}) \\ (D \wedge (true;\ \lceil v_j \rceil) \wedge \neg(true;\ \lceil v_i \rceil;\ \lceil v_j \rceil);\ \lceil v_n \rceil^1) \wedge (l = u+2) \vee & \cdots \quad (D_{21}) \\ (D \wedge (true;\ \lceil v_i \rceil;\ \lceil v_j \rceil);\ \lceil v_n \rceil^1) \wedge (l = u+2) & \cdots \quad (D_{31}) \end{array}$$

Also D_{11}, D_{21} and D_{31} are mutually exclusive. Therefore

$$\begin{aligned}\mu(D_n)[u+2] &= \mu(D \wedge (true;\ \lceil v_n \rceil) \wedge (l = u+2))[u+2] \\ &= F_1 + F_2 + F_3\end{aligned}$$

Subcase 1.2: $n = k$ in this case, $F_3 = 0$. But

$$D_{11} \vee D_{21} \Leftrightarrow D \wedge (true;\ \lceil v_k \rceil) \wedge (l = u+2)$$

Thus, we still have

$$\mu(D_k)[u+2] = F_1 + F_2 + F_3 = F_1 + F_2$$

Case 2: $n = j$

$$\begin{aligned}F_1 &= \sum_{h \in \boldsymbol{I}_j} \mu(D_h)[u+1] * p_{hj} \\ &= \mu(\bigvee_{h \in \boldsymbol{I}_j} (D \wedge (true;\ \lceil v_h \rceil);\ \lceil v_j \rceil^1))[u+2] \quad \cdots \quad \cdots (F_{12})\end{aligned}$$

Notice that

$$q_{jj} = \begin{cases} p_{jj} & \text{if } j \neq i \\ 0 & \text{if } j = i \end{cases}$$

Also notice that $q_{m+1j} = 0$. Thus, $F_3 = 0$.

Subcase 2.1: $j \neq i$

$$\begin{aligned}F_2 &= \mu(D_j)[u+1] * p_{jj} \\ &= \mu(D \wedge (true;\ \lceil v_j \rceil) \wedge \neg(true;\ \lceil v_i \rceil;\ \lceil v_j \rceil);\ \lceil v_j \rceil^1)[u+2] \quad \cdots \quad (F_{22})\end{aligned}$$

As in the previous case, look at the duration formulas in F_{12} and F_{22}.

$$D \wedge (true;\ \lceil v_j \rceil) \wedge \neg(true;\ \lceil v_i \rceil;\ \lceil v_j \rceil) \wedge (l = u+2) \Leftrightarrow$$

$$\bigvee_{h \in \boldsymbol{I}_j} (D \wedge (true;\ \lceil v_h \rceil);\ \lceil v_j \rceil^1) \wedge (l = u+2) \vee \quad \cdots \quad (D_{12})$$

$$(D \wedge (true;\ \lceil v_j \rceil) \wedge \neg(true;\ \lceil v_i \rceil;\ \lceil v_j \rceil);\ \lceil v_j \rceil^1) \wedge (l = u+2) \quad \cdots \quad (D_{22})$$

Also, D_{12} and D_{22} are exclusive. Thus

$$\mu(D_j)[u+2] = F_1 + F_2 = F_1 + F_2 + F_3$$

Subcase 2.2: $j = i$

In this case, $F_2 = 0$. But

$$\bigvee_{h \in \boldsymbol{I}_j} (D \wedge (true;\ \lceil v_h \rceil);\ \lceil v_j \rceil^1) \wedge (l = u+2)$$

is equivalent to

$$D \wedge (true;\ \lceil v_j \rceil) \wedge \neg(true;\ \lceil v_i \rceil) \wedge (l = u+2)$$

Thus we still have

$$\mu(D_j)[u+2] = F_1 = F_1 + F_2 + F_3$$

Case 3: $n = m+1 \wedge j \neq i$

Notice that

$$q_{hm+1} = \begin{cases} p_{ij} & \text{if } h = i \\ 0 & \text{if } h \neq i \end{cases}$$

$$\begin{array}{rcl} F_1 & = & \sum_{h \in \boldsymbol{I}_j} \mu(D_h)[u+1] * q_{hm+1} \\ & = & \mu(D_i)[u+1] * p_{ij} \\ & = & \mu(D \wedge (true;\ \lceil v_i \rceil);\ \lceil v_j \rceil^1)[u+2] \quad \cdots \quad (F_{13}) \end{array}$$

Since $j \neq i$, $q_{jm+1} = 0$ and thus $F_2 = 0$. Also notice that

$$q_{m+1m+1} = \begin{cases} p_{jj} & \text{if } j \neq k \\ 0 & \text{if } j = k \end{cases}$$

Subcase 3.1: $j \neq k$

$$\begin{array}{rcl} F_3 & = & \mu(D_{m+1})[u+1] * p_{jj} \\ & = & \mu(D \wedge (true;\ \lceil v_i \rceil;\ \lceil v_j \rceil);\ \lceil v_j \rceil^1)[u+2] \quad \cdots \quad (F_{33}) \end{array}$$

Again look at the duration formulas in F_{13} and F_{33}.

$$D \wedge (true;\ \lceil v_i \rceil;\ \lceil v_j \rceil) \wedge (l = u+2) \Leftrightarrow$$

$$\begin{array}{ll} (D \wedge (true;\ \lceil v_i \rceil);\ \lceil v_j \rceil^1) \wedge (l = u+2) \vee & \cdots \quad (D_{13}) \\ (D \wedge (true;\ \lceil v_i \rceil;\ \lceil v_j \rceil);\ \lceil v_j \rceil^1) \wedge (l = u+2) & \cdots \quad (D_{33}) \end{array}$$

D_{13} and D_{33} are exclusive. Thus

$$\mu(D_{m+1})[u+2] = F_1 + F_3 = F_1 + F_2 + F_3$$

Subcase 3.2: $j = k$

In this case, $F_3 = 0$. However

$$D \wedge (true;\ \lceil v_i \rceil;\ \lceil v_j \rceil) \wedge (l = u+2) \Leftrightarrow (D \wedge (true;\ \lceil v_i \rceil);\ \lceil v_j \rceil^1) \wedge (l = u+2)$$

Thus we still have

$$\mu(D_{m+1})[u+2] = F_1 = F_1 + F_2 + F_3$$

Case 4: $n = m+1 \wedge i = j \neq k$

Since $q_{hm+1} = 0$ when $h \neq i$, thus $F_1 = 0$. And $q_{jm+1} = p_{ij}$ when $j = i$. Also $q_{m+1m+1} = p_{jj}$ when $j \neq k$.

$$
\begin{aligned}
F_2 &= \mu(D_j)[u+1] * p_{jj} \\
&= \mu(D \wedge (true;\ \lceil v_j \rceil) \wedge \neg(true;\ \lceil v_j \rceil;\ \lceil v_j \rceil);\ \lceil v_j \rceil^1)[u+2] \quad \cdots \quad (F_{24})
\end{aligned}
$$

$$
\begin{aligned}
F_3 &= \mu(D_{m+1})[u+1] * p_{jj} \\
&= \mu(D \wedge (true;\ \lceil v_j \rceil;\ \lceil v_j \rceil);\ \lceil v_j \rceil^1)[u+2] \quad \cdots \quad (F_{34})
\end{aligned}
$$

The same argument about the duration formulas of F_{24} and F_{34} as before leads to

$$
\begin{aligned}
\mu(D_{m+1})[u+2] &= \mu(D \wedge (true;\ \lceil v_j \rceil;\ \lceil v_j \rceil) \wedge (l = u+2))[u+2] \\
&= F_2 + F_3 \\
&= F_1 + F_2 + F_3
\end{aligned}
$$

Case 5: $n = m+1 \wedge i = j = k$

In this case,

$$
\begin{aligned}
q_{hm+1} &= 0 \quad \text{when } h \neq i = j \\
q_{jm+1} &= p_{jj} \quad \text{when } i = j \\
q_{m+1m+1} &= 0 \quad \text{when } j = k
\end{aligned}
$$

Thus, $F_1 = 0$ and $F_3 = 0$.

$$
\begin{aligned}
F_2 &= \mu(D_j)[u+1] * p_{jj} \\
&= \mu(D \wedge (true;\ \lceil v_j \rceil) \wedge \neg(true;\ \lceil v_j \rceil;\ \lceil v_j \rceil);\ \lceil v_j \rceil^1)[u+2] \quad \cdots \quad (F_{35})
\end{aligned}
$$

Notice that now

$$D = \Box\neg(\lceil v_j \rceil;\ \lceil v_j \rceil;\ \lceil v_j \rceil)$$

Thus

$$D \wedge (true;\ \lceil v_j \rceil;\ \lceil v_j \rceil) \wedge (l = u+2)$$

is equivalent to

$$(D \wedge (true;\ \lceil v_j \rceil) \wedge \neg(true;\ \lceil v_j \rceil;\ \lceil v_j \rceil);\ \lceil v_j \rceil^1) \wedge (l = u+2)$$

Therefore

$$\mu(D_{m+1})[u+2] = F_2 = F_1 + F_2 + F_3$$

This ends the proof of the lemma.