Specification and Refinement of Probabilistic Processes

Bengt Jonsson
Swedish Institute of Computer Science &
Uppsala Univ. Dept. CS., Sweden *

Kim Guldstrand Larsen
Aalborg University, Denmark †

Abstract

Probabilistic transition systems is a basic semantic model for description and analysis of e.g. reliability aspects of concurrent and distributed systems. We present a formalism for specifying probabilistic transition systems, or processes, which itself is based on transition systems. Roughly, a specification has the form of a transition system where transitions are labeled by sets of allowed probabilities. For instance, a sufficiently reliable medium can be specified by a transition system where transitions that represent loss and delivery of messages are labeled by appropriate intervals of probabilities.

We define a satisfaction relation between processes and specifications which generalizes probabilistic bisimulation equivalence as proposed by Larsen and Skou. We also propose two criteria for refinement between specifications. One stronger criterion is analogous to the definition of simulation between non–probabilistic processes. This criterion is relatively unproblematic to establish. We show that it is analogous to the extension from processes to modal transition systems by Larsen and Thomsen. Another weaker criterion views a specification as defining a set of probabilistic processes; refinement is then simply containment between sets of processes. We present a complete method for verifying containment between specifications, which extends methods for deciding containment between finite automata or tree acceptors.

1 Introduction

Transition systems is well-established as a basic semantic model for the formal description, specification, and analysis of concurrent and distributed systems (e.g. [MP89, Mil89, Plo81]). This model describes the possible transitions of a system when interacting with an arbitrary environment. However, there is no information as to how frequently or with which probability the various transitions will be taken. Thus, the model can not make distinctions that relate e.g. to the reliability of systems. Clearly, from a practical point of view, it is essential that we are able to make such distinctions: a system which never performs an error–transition may not be feasible to construct, and we may be content with an imperfect system which performs error–transitions as long as their probability is sufficiently small.

The above considerations has called for a finer model where transitions are assigned probabilities. Several frameworks have been proposed for describing and analyzing probabilistic transition systems (e.g. [Chr90, vGSST90, GJS89, HJ90, LS89, Mol82, PZ86, PS89, Rab63]). Logics have been proposed for expressing properties of such systems (e.g. [HJ89, HS84, Koz83, LS89]). In these works, a system under study has precise probabilities ascribed to the transitions that define its behavior. For instance, a communication medium which can either lose or deliver a message has a precise probability ascribed to the possibility of losing of a message. Consequently, properties that are verified about a system that contains such a medium are not *a priori* valid for a medium with a different probability of loss. However, in many situations one wants only to give bounds on the probability of losing a message, leaving a system builder the freedom to buy or implement any medium which is reliable enough. Furthermore, if the system is developed through a sequence of refinements, it should be possible to improve such bounds, e.g. by introducing protocols.

Thus, one needs a loose specification formalism for probabilistic processes, in which one can specify e.g. when a system is reliable enough. Probabilistic log-

*Full Address: Bengt Jonsson, Swedish Institute of Computer Science, Box 1263, 164 28 Kista, Sweden. Tel. +46 - 8 - 752 1500. Fax +46 - 8 - 751 7230. E–mail: bengt@sics.se. Supported in part by the Swedish Board for Technical Development (STU) under contract No. 89–01220P as part of Esprit BRA project SPEC, No. 3096, and by the Swedish Telecom Administration as part of project PROMETHEUS.

†Full Address: Kim Guldstrand Larsen, Aalborg University, Department of Mathematics and Computer Science, Fredrik Bajersvej 7, 9220 Aalborg, Denmark. Tel. +45 - 98 - 15 85 22. E–mail: kgl@iesd.auc.dk

ics could be used for this purpose. Another possibility, which is the one we pursue in this paper, is to look for loose specification formalisms based on transition systems. For non-probabilistic systems, transition system based specification formalisms and their use in refinement have been rather succesful for the specification and verification of distributed systems [AL88, Jon87, LT87]. Transition system based specifications are often easy to understand through their similarity with processes and the possibility of displaying them graphically. This motivates an investigation into how these formalisms can be extended to probabilistic systems.

In this paper, we present a specification formalism for probabilistic processes, which is based on transition systems. Roughly, a specification is a transition system in which each transition is labeled by a *set* of allowed probabilities. For instance, a sufficiently reliable medium can be specified by a transition system where transitions that represent loss and delivery of messages are labeled by appropriate intervals of probabilities. The idea is that a process satisfies such a specification if its probabilities of loss and delivery lie within these intervals. We can also refine such a specification by another specification whose sets of probabilities labeling loss and delivery are subintervals (or, more generally, subsets) of the original intervals. In summary, this paper investigates the use of transition system based specifications for loose specifications and refinement of probabilistic processes.

We define a satisfaction relation between processes and specifications which generalizes probabilistic bisimulation equivalence as proposed by Larsen and Skou [LS89] (also used by [GJS89, HJ90]). Probabilistic bisimulation extends ordinary bisimulation and abstracts from the particular structure of transitions. A major contribution is the study of refinement between probabilistic specifications. We define two criteria for refinement between specifications. One stronger criterion is analogous to the extension from processes to modal transition systems by Larsen and Thomsen [LT88] in that it views sets of probabilities on transitions as modalities, which can be refined by strengthening them. We prove a correspondence with the refinement defined for modal transition systems. Another weaker criterion views a specification as defining a set of probabilistic processes, in analogy with the way an automaton defines a set of strings [HU79]. Refinement is then simply containment between sets of processes. We present a method for verifying this kind of refinement, which shares some elements (viz. the use of subsets and simulations) with methods for analogous problems for finite automata [HU79], transition systems, [AL88, Jif89, VW86], and tree acceptors [Don70].

Since our aim is to study the particular problems concerned with the treatment of probabilities, we keep other aspects of a specification as simple as possible. In particular, we do not want our work to be tied to any particular type of probabilistic transition system (e.g. reactive, generative, stratified, alternating as defined by [vGSST90]), and consequently we have chosen to use unlabeled transition systems, which also allow us to explain our ideas more clearly. However, we are confident that our ideas and results can be generalized to various sorts of labeled probabilistic transition systems.

The remainder of this paper is organized as follows: In the next section, we shortly review related work. In Section 3, we recall the definition of probabilistic processes and probabilistic bisimulation, and in Section 4 we define probabilistic specifications and the satisfaction relation. In Section 5 we define the weaker refinement relation between probabilistic specifications and presents a complete verification method for its verification. In Section 6 we present our stronger verification criterion, called simulation, and show how our extension from probabilistic processes to probabilistic specifications is analogous to the extension from processes to modal transition systems.

2 Related Work

Several frameworks for analyzing correctness properties of probabilistic transition systems in the form of e.g. Markov chains, Timed Petri Nets, etc. have been proposed [HJ89, HS84, LS89, Mol82, PZ86, PS89, VW86, Zub85]. Typical properties that are analyzed are: whether some correctness property (e.g. termination) holds with probability 1 (or sometimes some lesser probability), average response times, expected throughput, etc. There are also a number of logics for expressing properties of probabilistic transition systems [FH82, HJ89, Koz83, LS82, LS89]. Recently, probabilistic extensions of process algebras ([Hoa85, Mil89]) have been proposed [GJS89, HJ90, LS89] and several equivalences between probabilistic processes have been studied [Chr90, vGSST90, JS90, LS89] which generalize ordinary bisimulation, testing, and trace equivalence. These equivalences are exact, and do not allow to state e.g. arbitrary bounds on probabilities. Giacalone, Jou, and Smolka [GJS89] propose a way of loosening probabilistic bisimulation equivalence by using ϵ-equivalence, where ϵ is a number that measures similarity between processes. This loosening seems a rather obtuse tool for specification, since it does not allow specification of different deviations from specified behavior on different transitions.

3 Probabilistic Processes

We begin by recalling the definitions of probabilistic processes and probabilistic bisimulation. A probabilistic process is essentially a discrete Markov chain, the states of which are labeled by a set of propositions which are true in that state.

For $f : M \rightarrow N$ and $F : M \rightarrow 2^N$ we write $f \in F$ iff $(\forall m \in M)[f(m) \in F(m)]$. If R is an equivalence relation on M, we write M/R for the set of equivalence classes of M induced by R and write $[m]_R$ for the equivalence class which contains m.

A *probability distribution* on a set M is a function $f : M \rightarrow [0,1]$ such that $\sum_{m \in M} f(m) = 1$. The *support* of a probability distribution f on M is the set of $m \in M$ such that $f(m) > 0$. To avoid problems, we require that the support of each probability distribution be at most countable. For a probability distribution δ on $M \times N$ and subsets $K \subseteq M$ and $L \subseteq N$, we define $\delta(K,L) = \sum_{m \in K, n \in L} \delta(m,n)$ and use the conventions $\delta(m,L) = \delta(\{m\},L)$ and $\delta(K,n) = \delta(K,\{n\})$. For a probability distribution f on M, we similarly define $f(L) = \sum_{m \in L} f(m)$.

For the reasons given in the introduction, we have chosen to work with unlabeled transition systems. Instead we assume a set A of atomic propositions, which is intended to represent what can be observed about the system in a given state and thus will provide the source for distinguishing processes through observation. For non–probabilistic systems, there are well-known transformation techniques between state–labeled and transition–labeled transition systems.

Definition 3.1 A *probabilistic process system* is a triple $\langle P, \pi, V_P \rangle$, where

P is a set of *probabilistic processes*,

$\pi : P \rightarrow (P \rightarrow [0,1])$ is a *transition probability function* which for each $p \in P$ gives a probability distribution $\pi(p)$ on P.

$V_P : P \rightarrow 2^A$ is a *valuation function.* □

Probabilistic bisimulation is an extension of Milner's ordinary bisimulation [Mil89] which was proposed by Larsen and Skou [LS89]. We have adopted Larsen's and Skou's definition to our framework, where we use valuations in states rather than labels on transitions.

Definition 3.2 Let $\langle P, \pi, V_P \rangle$ be a probabilistic process system. An equivalence relation R on P is a *probabilistic bisimulation* on P if whenever $p \; R \; q$ then

1. $V_P(p) = V_P(q)$,
2. for all equivalence classes $Q \in P/R$ it holds that $\pi(p)(Q) = \pi(q)(Q)$.

Two processes p and q are called *probabilistic bisimulation equivalent*, written $p \simeq q$, if $p \; R \; q$ for some probabilistic bisimulation R. □

Probabilistic bisimulation equivalence is an equivalence which abstracts from the structure of individual transitions by comparing $\pi(p)(Q)$ with $\pi(q)(Q)$, rather than just individual transitions, to see whether p and q are equivalent. Recall that $\pi(p)(Q)$ denotes the probability that p will make a transition to become one of the processes in Q. Intuitively, if all states in Q are equivalent then all transitions from p to some process in Q are indistinguishable to an observer, and can therefore be regarded as an indivisible unit, i.e., their probabilities are added up. It can easily be shown that $\simeq$ is a maximal probabilistic bisimulation on P.

4 Probabilistic Specifications

In this section, we generalize the definition of probabilistic processes and probabilistic bisimulation to probabilistic specifications and the satisfaction relation between processes and specifications. A probabilistic specification differs from a process in that labels of transitions are sets of allowed probabilities rather than single probabilities.

Definition 4.1 A *probabilistic specification system* is a triple $\langle S, \sigma, V_S \rangle$, where

S is a set of *probabilistic specifications,*

$\sigma : S \rightarrow (S \rightarrow 2^{[0,1]})$ is a *transition probability predicate,* which for each $s \in S$ and $s' \in S$ gives a set of probabilities $\sigma(s)(s')$.

$V_S : S \rightarrow 2^A$ is a valuation function. □

Intuitively, the set $\sigma(s)(s')$ of probabilities of a transition from s to s' is the set of probabilities that are allowed for a process which satisfies the specification. In practice, one may not need the freedom of ascribing arbitrary sets of probabilities to transitions. One may be content with one of the following special cases of probabilistic specification systems.

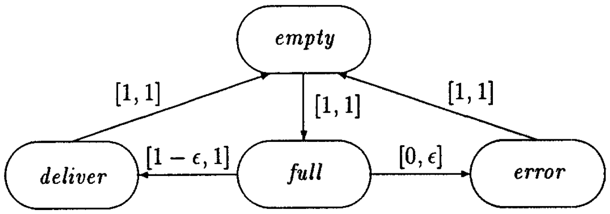

Figure 1: Specification of an Unreliable Medium

- *interval specification systems* in which all transition probability predicates give intervals of form $[\mu_1, \mu_2]$, $[\mu_1, \mu_2[$, $]\mu_1, \mu_2]$, or $]\mu_1, \mu_2[$ for $0 \leq \mu_1 \leq \mu_2 \leq 1$. Intuitively, interval specification systems give bounds on the probability of performing a certain transition from a given state,
- *modal specification systems* in which all transition probability predicates give intervals of form $]0, 1]$ or $[0, 1]$. An interval of form $]0, 1]$ can be interpreted as stating that a process *must* be able to perform the transition, whereas an interval of form $[0, 1]$ can be interpreted as stating that a process *may* be able to perform the transition. With this interpretation, we obtain an analogy to modal transition systems [LT88] where each transition is labeled either by a diamond $\Diamond$ or a box $\Box$. Then
  - $s \longrightarrow_{\Diamond} s'$ denotes that $\sigma(s)(s') = [0, 1]$ or $\sigma(s)(s') =]0, 1]$, and
  - $s \longrightarrow_{\Box} s'$ denotes that $\sigma(s)(s') =]0, 1]$.

  This analogy will be explored further in Section 6.

Example 4.2 Figure 1 shows graphically a probabilistic specification which is intended to specify the allowed behavior of a simple unreliable medium. The medium has a capacity of one message. The specification has four states. In the *empty* state, the medium is ready to receive a message. In the *full* state, it has received a message but can not yet deliver it. In the *deliver* state, the medium is ready to deliver a correct message, and can thereafter enter the *empty* state. In the *error* state, the message has been corrupted, whereafter the medium can enter the empty state. The specification prescribes an upper bound on the probability of message corruption by labeling the transition from *full* to *error* by the interval $[0, \epsilon]$, where ϵ is some suitably chosen number. Correspondingly, the transition from *full* to *deliver* is labeled by the interval $[1 - \epsilon, 1]$. All other transitions are labeled by the singleton probability set $[1, 1]$. We assume that the valuations in states are chosen in a manner suitable to distinguish the four states of the specification. □

We present a definition of satisfaction between processes and specifications which is based on the idea that the probabilities that label the transitions of a process must be in the set of probabilities that label the corresponding transitions of a specification. The actual definition of satisfaction, however, is more involved than a simple comparison of transitions, since we wish to abstract from the particular transition structure, just as for probabilistic bisimulation.

Definition 4.3 Let $\langle P, \pi, V_P \rangle$ be a probabilistic process system and let $\langle S, \sigma, V_S \rangle$ be a probabilistic specification system. A relation $R \subseteq P \times S$ is a ***satisfaction relation*** if whenever $p \; R \; s$ then

1. $V_P(p) = V_S(s)$
2. there is a probability distribution δ on $P \times S$ such that
   (a) $\delta(p', S) = \pi(p)(p')$ for all $p' \in P$,
   (b) $\delta(P, s') \in \sigma(s)(s')$ for all $s' \in S$,
   (c) $p' \; R \; s'$ whenever $\delta(p', s') > 0$.

We write p **sat** s iff $p \; R \; s$ for some satisfaction relation R. □

Note that δ may in general depend on p and s. Intuitively, p **sat** s means that the valuations in p and s are the same and that the probabilities of the transitions from p are allowed by the sets labeling transitions from s. Just as for probabilistic bisimulation, we abstract from the particular structure of transitions. For instance, it may be the case that p **sat** s and that there are five transitions from p which correspond to a

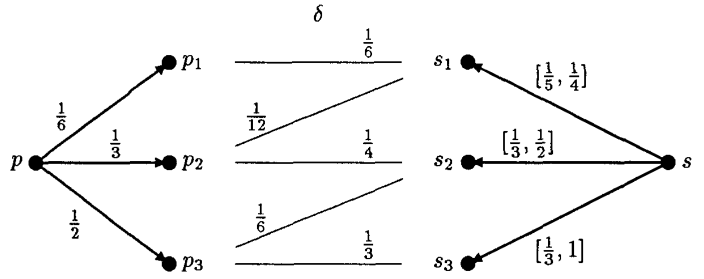

Figure 2: Illustration of Satisfaction.

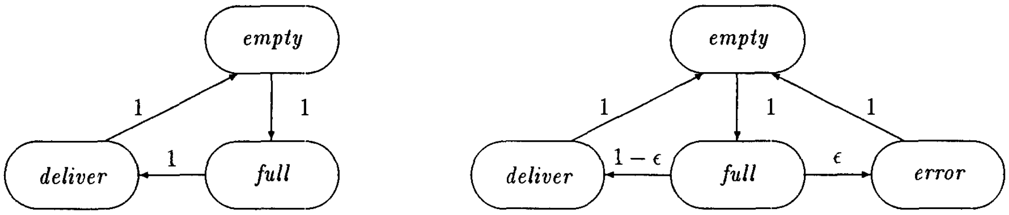

Figure 3: Reliable Medium (left) and Unreliable Medium (right)

single transition from s to s'. The sum of the probabilities of these five transitions must then be in $\sigma(s)(s')$. The function δ describes how the transitions from p and s can be divided into pieces which are combined with each other. Intuitively, if $\delta(p', s') = x$ then we combine a part of the transition from p to p' with a part of a transition from s to s'. Both these parts have probability x. In the above definition, the first requirement checks that the the probabilities of the parts containing p' indeed add up to $\pi(p)(p')$ and the second requirement checks that the the probabilities of the parts containing s' indeed add up to an element in $\sigma(s)(s')$. The last condition checks that combined pieces indeed are related to each other.

It is easy to see that **sat** is itself a satisfaction relation, in fact **sat** is the maximal satisfaction relation.

Example 4.4 To illustrate the definition of satisfaction 4.3 we consider the process p and the specification s (partly) given in Figure 2. Now assume $V_P(p) = V_S(s)$, p_1, p_2 **sat** s_1, p_2, p_3 **sat** s_2 and p_3 **sat** s_3. Then the distribution δ (only the non–zero part of which is indicated) validates condition 2 of Definition 4.3. For (a) simply check the following three equalities: $\frac{1}{6} = \frac{1}{6}$, $\frac{1}{3} = \frac{1}{12} + \frac{1}{4}$ and $\frac{1}{2} = \frac{1}{6} + \frac{1}{3}$. For (b) check the following three inclusions: $\frac{1}{6} + \frac{1}{12} \in [\frac{1}{5}, \frac{1}{4}]$, $\frac{1}{4} + \frac{1}{6} \in [\frac{1}{3}, \frac{1}{2}]$ and $\frac{1}{3} \in [\frac{1}{3}, 1]$. □

Example 4.5 In Figure 3 are two probabilistic processes, both representing media that satisfy the specification in Figure 1. To the left is a perfect medium which never corrupts messages, and to the right is a medium which corrupts messages with a probability of ϵ. The intended meaning of the states is analogous to that in Figure 1. It is easy to see that by relating states with the same label to each other, we obtain a satisfaction relation. □

As a first test of our definition of satisfaction, we shall show that satisfaction coincides with probabilistic bisimulation in the degenerate case that the specification is a process. For a transition probability function π, we write $\tilde{\pi}$ for the transition probability predicate defined by $\tilde{\pi}(p)(p') = \{\pi(p)(p')\}$. A probabilistic process system $\langle P, \pi, V_P \rangle$ can then be viewed as the probabilistic specification system $\langle P, \tilde{\pi}, V_P \rangle$.

Theorem 4.6 *Let $\langle P, \pi, V_P \rangle$ be a probabilistic process system and let $\langle P, \tilde{\pi}, V_P \rangle$ be the corresponding probabilistic specification system. Then $p \simeq p'$ iff p **sat** p'.* □

Proof: We shall first prove that **sat** is an equivalence relation on P. Reflexivity of **sat** follows immediately since the identity relation is trivially a satisfaction relation. Symmetricity follows since if R is a satisfaction relation, then R^{-1} is also, since Definition 4.3 is symmetric in p and q. To show that **sat** is transitive, assume that R_1 and R_2 are satisfaction relations. We shall prove that $R_1 \circ R_2$ is a satisfaction relation. So assume that $p\ (R_1 \circ R_2)\ r$, i.e., that there is a process q such that $p\ R_1\ q$ and $q\ R_2\ r$. Then there are probability distributions δ_1 and δ_2, where δ_1 shows that $p\ R_1\ q$ and δ_2 shows that $q\ R_2\ r$ according to Definition 4.3. Now define the probability distribution δ on $P \times P$ by

$$\delta(p', r') = \sum_{q' \in P} \frac{\delta_1(p', q') \star \delta_2(q', r')}{\pi(q)(q')} \quad .$$

We check that δ satisfies the three conditions in Definition 4.3. To check the first condition, note that

$$\begin{aligned}
\delta(p', P) &= \sum_{r' \in P} \sum_{q' \in P} \frac{\delta_1(p', q') \star \delta_2(q', r')}{\pi(q)(q')} \\
&= \sum_{q' \in P} \frac{\delta_1(p', q')}{\pi(q)(q')} \sum_{r' \in P} \delta_2(q', r') \\
&= \sum_{q' \in P} \delta_1(p', q') = \pi(p)(p')
\end{aligned}$$

where the third equality follows since $\delta_2(q', P) = \pi(q)(q')$ and the last equality follows since $\delta_1(p', P) = \pi(p)(p')$. The second condition follows by proving that $\delta(r', P) = \pi(r, r')$ analogously. The last condition follows trivially since both δ_1 and δ_2 satisfy it. Thus $R_1 \circ R_2$ is a satisfaction relation, from which we conclude that **sat** is transitive.

We shall now prove that **sat** is a probabilistic bisimulation. Assume that p **sat** q. We check the conditions in Definition 3.2. The condition $V_P(p) = V_P(q)$ is also required for satisfaction relations, and thus holds trivially. To check the second condition, note that since **sat** is itself a satisfaction relation there is a probability distribution δ on $P \times P$ such that (1) $\delta(p', S) = \pi(p)(p')$ for all $p' \in P$, (2) $\delta(P, q') = \pi(q)(q')$ for all $q' \in S$, and (3) p' **sat** q' whenever $\delta(p', q') > 0$. Assume that Q is an equivalence class induced by **sat**. We then have

$$\begin{aligned}
\pi(p)(Q) &= \sum_{p' \in Q} \pi(p)(p') \\
&= \sum_{p' \in Q} \delta(p', P) = \sum_{p' \in Q} \delta(p', Q) = \delta(Q, Q)
\end{aligned}$$

where the first equality follows the definition of $\pi(p)(Q)$, the second equality follows by (1), the third equality follows by noting that (3) implies that $\delta(p', q')$ is nonzero only if q' is in the same equivalence class as p', i.e., $q' \in Q$, and the last equality is the definition of notation. In the same manner we can prove that $\pi(q)(Q) = \delta(Q, Q)$, from which we conclude that $\pi(p)(Q) = \pi(q)(Q)$. Thus **sat** is a probabilistic bisimulation.

Conversely, assume that $p \simeq q$, i.e., that there is a probabilistic bisimulation R on P. We shall prove that R is also a satisfaction relation. So assume that $p\ R\ q$. We check the conditions in Definition 4.3. The condition $V_P(p) = V_P(q)$ is also required for probabilistic bisimulations, and thus holds trivially. To check the second condition, define a probability distribution δ on $P \times P$ by

$$\delta(p', q') = \\ \text{if } p'\ R\ q' \text{ then } \frac{\pi(p)(p') \star \pi(q)(q')}{\pi(p)([p']_R)} \text{ else } 0 \quad .$$

We then have that

$$\begin{aligned}
\delta(p', P) &= \sum_{\{q' \mid p'\ R\ q'\}} \frac{\pi(p)(p') \star \pi(q)(q')}{\pi(p)([p']_R)} \\
&= \frac{\pi(p)(p')}{\pi(p)([p']_R)} \star \sum_{\{q' \mid p'\ R\ q'\}} \pi(q)(q') \quad ,
\end{aligned}$$

where the first equality follows from the definition of δ and the second equality follows since $\pi(p)(p')$ and $\pi(p)([p']_R)$ are independent of q'. Now note that the sum of $\pi(q)(q')$ over all q' such that $p'\ R\ q'$ is equal to $\pi(q)([p']_R)$, which is equal to $\pi(p)([p']_R)$ by the assumption that $p\ R\ q$. It follows that $\delta(p', P) = \pi(p)(p')$. In a similar way we can prove that $\delta(P, q') = \pi(q)(q')$ for all q'. From the definition of δ we trivially have $p'\ R' q'$ whenever $\delta(p', q') > 0$. Thus R is a satisfaction relation. □

5 Refinement

We define refinement between probabilistic specifications as inclusion between the sets of processes that satisfy the respective specifications. This is analogous to commonly used definitions of refinement for non-probabilistic specifications.

Let $\langle S, \sigma, V_S \rangle$ be a probabilistic specification system, and let $s \in S$. A specification $s \in S$ is ***image-finite*** if the support of $\sigma(s)$ is finite and each s' in the support of $\sigma(s)$ is also image-finite. Image-finiteness is defined analogously for processes.

Definition 5.1 Let $\langle S, \sigma, V_S \rangle$ be a probabilistic specification system. We say that the specification s ***refines*** the specification t, written $s \sqsubseteq t$, iff for any probabilistic process system $\langle P, \pi, V_P \rangle$ and image-finite $p \in P$ we have p **sat** s implies p **sat** t. □

For interval specifications, we present a complete method for verifying refinement, which is an extension of methods for proving containment between finite automata [HU79] or tree acceptors [Don70], and in addition has to consider the abstraction from the transition structure in the definition of satisfaction. Here, we consider only *closed* interval specifications, i.e., specifications in specification systems $\langle S, \sigma, V_S \rangle$ where $\sigma(s)(s')$ is either *closed* interval or $\emptyset$ for all $s, s' \in S$.

Definition 5.2 Let $\langle S, \sigma, V_S \rangle$ be a closed interval specification system. A *subset-simulation* R on S is a relation $R \subseteq S \times 2^S$ such that

1. for each $s \in S$ there is a $T \subseteq S$ such that $s\ R\ T$,
2. if $s\ R\ T$ then $V_S(s) = V_S(t)$ for all $t \in T$,
3. for each $s \in S$ and probability distribution δ on $S \times 2^S$, such that $\delta(s', 2^S) \in \delta(s)(s')$ and $\delta(s', T') > 0 \implies s'\ R\ T'$ for all $s' \in S$ and $T' \subseteq S$, there is a set $T \subseteq S$ such that $s\ R\ T$ and such that for each $t \in T$ there is a probability distribution γ on $S \times 2^S$, such that
   (a) $\gamma(t', 2^S) \in \sigma(t)(t')$ for all $t' \in S$,
   (b) $\gamma(S, T') = \delta(S, T')$ for all $T' \subseteq S$,
   (c) $t' \in T'$ whenever $\gamma(t', T') > 0$.
4. For each $s \in S$ there are only finitely many sets T with $s\ R\ T$.

□

Intuitively, the third condition states that if the state s is followed by a distribution δ over pairs $\langle s', T' \rangle$ of successor states s' and simulating sets T' of states, then there is a set T which simulates s in the sense that for each state $t \in T$ there is a distribution over successor states of t which is consistent with δ. For closed interval specifications, the third condition can be checked using methods from linear algebra.

Theorem 5.3 *Let $\langle S, \sigma, V_S \rangle$ be a closed interval specification system. Assume that $s_0 \in S$ is image-finite. If R is a subset-simulation such that $t_0 \in T$ whenever $s_0\ R\ T$, then $s_0 \sqsubseteq t_0$.* □

Proof: Assume that R is a subset-simulation such that $t_0 \in T$ whenever $s_0\ R\ T$, and that p_0 is an image-finite process such that p_0 **sat** s_0. We shall prove that p_0 **sat** t_0. We define a tree, denoted *unfold*(p_0, s_0), in which each node is labeled by a pair $\langle p, s \rangle$ such that p **sat** s and each edge is labeled by a probability, as follows. The root of *unfold*(p_0, s_0) is labeled by $\langle p_0, s_0 \rangle$. If a node is labeled by $\langle p, s \rangle$ then (by the definition of **sat**) there is a probability distribution δ on $P \times S$ such that $\delta(p', S) = \pi(p)(p')$ for all $p' \in P$, and $\delta(P, s') \in \sigma(s)(s')$ for all $s' \in S$, and $p'\ R\ s'$ whenever $\delta(p', s') > 0$. For each $\langle p', s' \rangle$ such that $\delta(p', s') > 0$ let there be a son of this node labeled $\langle p', s' \rangle$ and let the arc to that node be labeled $\delta(p', s')$. Note that *unfold*(p_0, s_0) is in general not uniquely defined; it depends on the choice of δ at each node.

Consider a fixed $n > 0$. Let *unfold*$(p_0, s_0)\lceil n$ be the tree containing all nodes of *unfold*(p_0, s_0) whose depth is at most n. Label each node of *unfold*$(p_0, s_0)\lceil n$ by a set of specifications (in addition to the process specification pair) as follows. Each leaf of *unfold*$(p_0, s_0)\lceil n$ which is labeled by a pair $\langle p, s \rangle$ is labeled by a set T such that $s\ R\ T$. If the sons of a father node labeled by $\langle p, s \rangle$ have been labeled by sets of specifications, where $\delta(p', s')$ labels the arc to a son labeled by $\langle p', s' \rangle$ and T', then define $\mu(s', T')$ as the sum of the labels $\delta(p', s')$ on arcs from the father node to a son labeled $\langle p', s' \rangle$ and T' for $p' \in P$. We have $\mu(s', 2^S) = \delta(P, s') \in \sigma(s)(s')$ and $\mu(s', T') > 0 \implies s'\ R\ T'$. Thus by condition 3 there is a set $T \subseteq S$ such that $s\ R\ T$ and such that for all $t \in T$ there is a probability distribution γ on $S \times 2^S$ such that (1) $\gamma(t', 2^S) \in \sigma(t)(t')$ for all $t' \in S$, (2) $\gamma(S, T') = \mu(S, T')$ for all $T' \subseteq S$, and (3) $t' \in T'$ whenever $\gamma(t', T') > 0$. Let the father node (labeled by $\langle p, s \rangle$) be labeled by such a T.

For each n we now consider all possible labelings of *unfold*$(p_0, s_0)\lceil n$ by sets of specifications, obtained as above. If $\mathcal{C}_n$ is a labeling of *unfold*$(p_0, s_0)\lceil n$ and $\mathcal{C}_{n+1}$ is a labeling of *unfold*$(p_0, s_0)\lceil n + 1$, then we write $\mathcal{C}_n \longrightarrow \mathcal{C}_{n+1}$ to denote that $\mathcal{C}_n$ and $\mathcal{C}_{n+1}$ have the same labeling of *unfold*$(p_0, s_0)\lceil n$. For each n there is at least one labeling of *unfold*$(p_0, s_0)\lceil n$. Furthermore, by condition 4 and the assumption that p_0 and s_0 are image-finite, there are at most finitely many different labelings of *unfold*$(p_0, s_0)\lceil n$. It follows that we can organize the labelings into a tree, where $\mathcal{C}_{n+1}$ is a son of $\mathcal{C}_n$ if $\mathcal{C}_n \longrightarrow \mathcal{C}_{n+1}$, which has infinitely many nodes and is finitely branching. By König's lemma we can extract an infinite path in the tree. Consider the labeling of *unfold*(p_0, s_0) obtained as the union of the labelings in this infinite path. Define the relation Q on $P \times S$ defined by $p\ Q\ t$ if there are s, T such that a node is labeled by $\langle p, s \rangle$ and T and $t \in T$. We claim that Q is a satisfaction relation. To prove this, let a node be labeled by $\langle p, s \rangle$ and T, which has arcs labeled $\delta(p', s')$ to sons labeled by $\langle p', s' \rangle$ and T'. Let $\mu(s', T')$ be obtained as above. If $t \in T$ there is a a probability distribution γ on $S \times 2^S$ such that (1) $\gamma(t', 2^S) \in \sigma(t)(t')$

for all $t' \in S$, (2) $\gamma(S, T') = \mu(S, T')$ for all $T' \subseteq S$, and (3) $t' \in T'$ whenever $\gamma(t', T') > 0$. Define a probability distribution κ on $P \times S$ by

$$\kappa(p', t') = \sum_{s', T'} \left[\gamma(t', T') \star \frac{\delta(p', s')}{\sum_{p', s'} \delta(p', s')} \right] .$$

We can now check that $\kappa(p', S) = \pi(p)(p')$ for all $p' \in P$, and $\kappa(P, s') \in \sigma(s)(s')$ for all $s' \in S$, and that $p' \; Q \; s'$ whenever $\kappa(p', s') > 0$. Having proven that Q is a satisfaction relation, we conclude that p_0 **sat** t_0 for each t_0 in a set labeling the root of *unfold*(p_0, s_0). The theorem follows. □

Next we give a restricted completeness theorem.

Theorem 5.4 *Let $\langle S, \sigma, V_S \rangle$ be a probabilistic specification system where S is finite. If $s_0 \subseteq t_0$ for $s_0, t_0 \in S$, then there is a subset-simulation R such that $s_0 \; R \; T$ implies $t_0 \in T$.* □

Proof Sketch: Define the subset-simulation R by $s \; R \; T$ if there is a process p such that p **sat** s and $T = \{t \in S \mid p \textbf{ sat } t\}$. One can then verify that R satisfies the conditions for being a subset-simulation. □

6 Simulations and Modal Transition Systems

In the previous section we presented a refinement criterion, together with a complete but somewhat complex method for verification. We will also define a stronger criterion for refinement, which is simpler to apply in practice. Analogously, for non-probabilistic systems, refinement mappings [Lam83] and simulations [Jon87, LT87, LS90] are practically very useful in spite of their incompleteness.

In this section, we also show how the modal transition systems defined by Larsen and Thomsen [LT88] can be viewed as a special class of our probabilistic specifications. Essentially, a modal transition system is a transition system where the transitions are of two kinds: allowed transitions and required transitions. The idea of our correspondence is to view the modalities as predicates on probabilities. Under this correspondence, the refinement criterion presented in this section for probabilistic specifications corresponds to modal refinement as defined by Larsen and Thomsen.

Definition 6.1 Let $\langle S, \sigma, V_S \rangle$ be a probabilistic specification system. A *simulation* R on S is a relation $R \subseteq S \times S$ such that whenever $s \; R \; t$ we have

1. $V_S(s) = V_S(t)$,
2. there is a function $\rho : S \rightarrow (S \rightarrow [0,1])$, which for each $s \in S$ gives a probability distribution $\rho(s)$ on S, such that
   (a) for any $f \in \sigma(s)$ and $t' \in S$ it holds that $\sum_{s' \in S} (f(s') \star \rho(s')(t')) \in \sigma(t)(t')$
   (b) $s' \; R \; t'$ whenever $\rho(s')(t') > 0$.

We say that t *simulates* s if there is a simulation R such that $s \; R \; t$. □

Intuitively, the function ρ gives for each transition from s to s' a way of distributing the probability of this transition onto the transitions from t: the transition from t to t' receives the fraction of $\rho(s')(t')$. The first condition on ρ checks that for any particular probability distribution that conforms with $\sigma(s)$, the fractions add up correctly.

If $\langle S, \sigma, V_S \rangle$ is a closed interval specification system and $s \in S$ is an image-finite specification, then a *corner* of $\sigma(s)$ is a probability distribution f on S such that $f(s')$ is either the upper or lower bound in $\sigma(s)(s')$ for all but possibly one s' in the support of S. Intuitively, f is then an extreme point in the polytope of all probability distributions g such that $g \in \sigma(s)$.

For arbitrary specifications, the first condition on ρ may be difficult to check in practice, since it involves the quantification over all $f \in \sigma(s)$. However, for *interval specifications* the situation is considerably better. Simple convexity arguments show that it is enough to check the conditions for the corners of $\sigma(s)$ and thereafter making appropriate adjustments for open or closed intervals.

Proposition 6.2 *If t simulates s then $s \subseteq t$. Furthermore, the definition of simulation coincides with the definition of satisfaction when s is a process.* □

Proof: We shall prove the first claim by proving that **sat** $\circ R$ is a satisfaction relation whenever R is a simulation. So, assume that $s \; R \; t$ and that p is a process such that p **sat** s. We shall check that p and t satisfy the conditions under which **sat** $\circ R$ is a satisfaction relation. The condition $V_P(p) = V_S(t)$ follows immediately. Since p **sat** s and $s \; R \; t$ there is a probability distribution δ_1 on $P \times S$ which satisfies the conditions of Definition 4.3, and a function $\rho : S \rightarrow (S \rightarrow [0,1])$ which satisfies the conditions of Definition 6.1. Now define the probability distribution δ on $P \times S$ by

$$\delta(p', t') = \sum_{s' \in S} \delta_1(p', s') \star \rho(s')(t') .$$

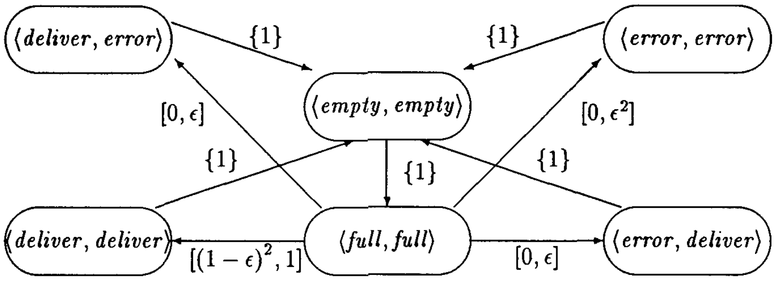

Figure 4: Combined Medium.

We check that δ satisfies the three conditions in Definition 4.3. To check the first condition, note that

$$\begin{aligned} \delta(p',T) &= \sum_{s'\in S}\sum_{t'\in P} \delta_1(p',s') \star \rho(s')(t') \\ &= \sum_{s'\in S} \delta_1(p',s') \star \sum_{t'\in P} \rho(s')(t') \\ &= \sum_{s'\in S} \delta_1(p',s') = \pi(p)(p') \end{aligned}$$

where the third equality follows since $\rho(s')$ is a probability distribution on S, and the last follows by the choice of δ_1. To check the second condition, note that

$$\begin{aligned} \delta(P,t') &= \sum_{p'\in P}\sum_{s'\in P} \delta_1(p',s') \star \rho(s')(t') \\ &= \sum_{s'\in P} \rho(s')(t') \star \delta_1(P,s') \ . \end{aligned}$$

Now there must be an $f \in \sigma(s)$ such that $f(s') = \delta_1(P,s')$ for all $s' \in S$ whence we conclude that

$$\begin{aligned} &\sum_{s'\in P} \rho(s')(t') \star \delta_1(P,s') \\ &= \sum_{s'\in P} (\rho(s')(t') \star f(s')) \in \sigma(t)(t') \end{aligned}$$

by the definition of simulation. The third condition is trivial. This concludes the proof that **sat** $\circ\, R$ is a satisfaction relation.

By the proof of the first claim and Theorem 4.6 we conclude that **sat** $\circ\, R$ is a satisfaction relation if R is a simulation between processes and specifications. Since satisfaction is transitive, the claim follows. □

Example 6.3 (Example 4.5 continued) In order to increase the probability of successful transmission of messages we may simply use *two* media. That is, we simultaneously transmit a message over two (unreliable) media being content as long as at least one medium successfully delivers the message. The specification of such a combined medium is obtained as the obvious product [1] of two unreliable medium specifications (see Figure 1) and is illustrated in Figure 4. We now claim that the combined medium simulates (and hence refines) an unreliable medium with error probability ϵ^2 (see Figure 1). Thus the use of two media does indeed lead to improved performance. To justify our claim we will argue that the relation:

$$\begin{aligned} \mathcal{R} = &\ \{(\langle x,x\rangle, x) \mid x = \mathit{empty}, \mathit{full}, \mathit{error}, \mathit{deliver}\} \\ \cup &\ \{(\langle \mathit{deliver}, x\rangle, \mathit{deliver}), (\langle x, \mathit{deliver}\rangle, \mathit{deliver})\} \end{aligned}$$

is a simulation. Assuming that $V(\langle x,x\rangle) = V(x)$ and $V(\langle \mathit{deliver}, x\rangle) = V(\langle x, \mathit{deliver}\rangle) = V(\mathit{deliver})$ condition 1 of Definition 6.1 is clearly satisfied. For condition 2 we may in this case uniformly use the function ρ below for any pair (s,t) in $\mathcal{R}$:

$$\rho(s')(t') \;=\; \begin{cases} 1; & (s',t') \in \mathcal{R} \\ 0; & \mathit{otherwise} \end{cases}$$

With this definition of ρ clearly condition 2(b) is satisfied. We now demonstrate that condition 2(a) is satisfied for the pair $(\langle \mathit{full}, \mathit{full}\rangle, \mathit{full})$ (leaving the remaining pairs to the reader). That is we must show that

[1] For two probabilistic specification systems $\mathcal{S}_i = \langle S_i, \sigma_i, V_{S_i}\rangle$ we define the *product* system $\mathcal{S}_1 \times \mathcal{S}_2 = \langle S_1 \times S_2, \sigma_1 \otimes \sigma_2, V_{S_1} \otimes V_{S_2}\rangle$, where $(\sigma_1 \otimes \sigma_2)(s_1,s_2)(t_1,t_2) = \{p_1 \star p_2 \mid p_i \in \sigma_i(s_i)(t_i)\}$ and $V_{S_1} \otimes V_{S_2}(s_1,s_2) = V_{S_1}(s_1) \bullet V_{S_2}(s_2)$, where $\bullet$ is a given composition on propositions.

whenever:

$$\begin{array}{ll} (a) & p_3 \in [0,\epsilon] \\ (b) & p_4 \in [(1-\epsilon)^2, 1] \\ (c) & p_5 \in [0,\epsilon] \\ (d) & p_6 \in [0,\epsilon^2] \end{array}$$

with $p_3+p_4+p_5+p_6 = 1$ then $p_3+p_4+p_5 \in [1-\epsilon^2, 1]$ and $p_6 \in [0,\epsilon^2]$. Clearly, this is the case. □

In the remainder of this section, we show how the modal transition systems defined by Larsen and Thomsen [LT88] can be viewed as a special class of our probabilistic specifications and that modal refinement can be viewed as a special case of simulation.

Definition 6.4 A *modal transition system* is a structure $\langle Q, \longrightarrow_\Box, \longrightarrow_\Diamond, V_Q\rangle$ where Q is a set of *modal specifications*, and where $\longrightarrow_\Box \subseteq Q \times Q$ and $\longrightarrow_\Diamond \subseteq Q \times Q$ are two transition relations that satisfy the condition $\longrightarrow_\Box \subseteq \longrightarrow_\Diamond$, and where $V_Q : Q \rightarrow 2^A$ is a *valuation function*. □

Intuitively, the relation $\longrightarrow_\Box$ describes the required transitions of a (non-probabilistic) process, and the relation $\longrightarrow_\Diamond$ describes the allowed transitions of a (non-probabilistic) process. The condition $\longrightarrow_\Box \subseteq \longrightarrow_\Diamond$ expresses the natural condition that anything required is also allowed. A standard transition system with only one transition relation $\longrightarrow$ can be regarded as a modal transition system by identifying both $\longrightarrow_\Box$ and $\longrightarrow_\Diamond$ with $\longrightarrow$.

Definition 6.5 Let $\langle Q, \longrightarrow_\Box, \longrightarrow_\Diamond, V_Q\rangle$ be a modal transition system. A binary relation R on Q is a *modal refinement* if whenever $q\ R\ r$ then

- $V_Q(q) = V_Q(r)$,
- whenever $q \longrightarrow_\Diamond q'$ then $r \longrightarrow_\Diamond r'$ for some r' with $q'\ R\ r'$,
- whenever $r \longrightarrow_\Box r'$ then $q \longrightarrow_\Box q'$ for some q' with $q'\ R\ r'$.

If $q\ R\ r$ for some modal refinement R, then q is said to be a modal refinement of r, and we write $q \lhd r$. □

Intuitively, if q is a modal refinement of r then all transitions allowed by q must also be allowed by r and all transitions required by r must also be required by q.

Having recalled the definitions of modal transition systems, we go on to define their probabilistic analogue, called modal specification systems.

Definition 6.6 A *modal specification systems* is a probabilistic specification system in which all transition probability predicates are intervals of form $]0,1]$ or $[0,1]$. □

Definition 6.7 A modal transition system $\langle Q, \longrightarrow_\Box, \longrightarrow_\Diamond, V_Q\rangle$ *corresponds to* a modal specification system $\langle S, \sigma, V_S\rangle$ if $Q = S$, and $V_Q = V_S$, and $s \longrightarrow_\Diamond s'$ iff $\sigma(s)(s') = [0,1]$ or $\sigma(s)(s') =]0,1]$, and $s \longrightarrow_\Box s'$ iff $\sigma(s)(s') =]0,1]$. □

Now say that a modal transition system $\langle Q, \longrightarrow_\Box, \longrightarrow_\Diamond, V_Q\rangle$ is *□-enabled* if the set $\{q' \mid q \longrightarrow_\Box q'\}$ is non–empty for all $q \in Q$. The main result in this section shows that it is correct to view simulation as defined in Definition 6.1 as a generalization of modal refinement under the (mild) assumption of □–enabledness.

Theorem 6.8 *Let $\langle Q, \longrightarrow_\Box, \longrightarrow_\Diamond, V_Q\rangle$ be a □–enabled modal transition system, and let $\langle S, \sigma, V_S\rangle$ be the corresponding modal specification system. Then if $s, t \in S$ we have that $s \lhd t$ iff t simulates s.* □

Proof: Let R be a modal refinement. Then we claim that $R \cup \mathrm{Id}$ is a simulation. For $(s,t) \in R \cup \mathrm{Id}$ we define the function $\rho : S \rightarrow (S \rightarrow [0,1])$ as follows:

- whenever $s \longrightarrow_\Diamond s'$ then $\rho(s')$ is uniform on $\{t' \mid t \longrightarrow_\Diamond t' \text{ and } s'Rt'\}$,
- whenever $s \not\longrightarrow_\Diamond s'$ then $\rho(s')(s') = 1$.

Clearly condition 1 and 2(b) of Definition 6.1 are then satisfied. For 2(a) we must show for all t' and $f \in \sigma(s)$ that:

$$\sum_{s'} (f(s') \star \rho(s')(t')) \qquad (1)$$

$$= \sum_{s'.s \longrightarrow_\Diamond s'} (f(s') \star \rho(s')(t')) \in \sigma(t)(t')$$

Now, for $\sigma(t)(t') = [0,1]$ this is obvious. When $\sigma(t)(t') = [0,0]$, $t \not\longrightarrow_\Diamond t'$ and hence $\rho(s')(t') = 0$ for all s' such that $s \longrightarrow_\Diamond s'$. Again (1) has been established. Finally, consider the case $\sigma(t)(t') =]0,1]$, i.e. $t \longrightarrow_\Box t'$. But then $s \longrightarrow_\Box s'$ with $s'Rt'$ for some s', and hence $\rho(s')(t') > 0$. Also, $f(s') > 0$ as $f(s') \in \sigma(s)(s') =]0,1]$. It follows that the sum in (1) indeed is greater than zero.

Now let R be a simulation. We will show that R is also a modal refinement. Thus, let sRt and let $\rho : S \rightarrow (S \rightarrow [0,1])$ be the function which satisfies the conditions of Definition 6.1. Assume that $s \longrightarrow_{\diamond} s'$, i.e. $\sigma(s)(s')$ equals $[0,1]$ of $]0,1]$. Now let $f \in \sigma(s)$ be such that $f(s') > 0$ (the existence of which can easily argued) and let t' be such that $\rho(s')(t') > 0$. From condition 2(a) of Definition 6.1 it follows that $\sigma(t)(t')$ must have the form $[0,1]$ of $]0,1]$. In all cases $t \longrightarrow_{\diamond} t'$ and $s'Rt'$. Now assume that $t \longrightarrow_{\square} t'$, i.e. $\sigma(t)(t') =]0,1]$. Let $f \in \sigma(s)$ such that $f(s') > 0$ iff $s \longrightarrow_{\square} s'$ (due to the assumption of $\square$-enabledness such an f exists). Then condition 2(a) yields:

$$\begin{aligned}&\sum_{s'} (f(s') \star \rho(s')(t')) \\ &\quad = \sum_{s'.s \longrightarrow_{\square} s'} (f(s') \star \rho(s')(t')) \in]0,1]\end{aligned}$$

Thus for some s' with $s \longrightarrow_{\square} s'$ it must be the case that $\rho(s')(t') > 0$ and hence $s'Rt'$. □

Conclusion

We have presented a transition system based specification formalism for loose specifications of probabilistic processes. The main idea was to label each transition with a set of allowed probabilities. We have given a definition of simulation between specifications, which can be regarded as an extension of ordinary simulation between non-probabilistic systems. We hope that our definition of simulation can be integrated into existing definitions of simulation between nonprobabilistic specifications. A loosening of the simulation relation can be verified by techniques from automata-theory where subset-constructions are used to cope with nondeterminism.

Future research include investigating how existing probabilistic process calculi may be extended to that of probabilistic specification systems. In particular we want the extended process algebraic operators to preserve the simulation ordering as this will provide us with a graphical specification formalism for probabilistic processes allowing compositional verification. Future research also include application of the specification formalism put forward and comparison with various existing probabilistic logics.

References

[AL88] M. Abadi and L. Lamport. The existence of refinement mappings. In *Proc. 3^{rd} IEEE Int. Symp. on Logic in Computer Science*, Edinburgh, 1988.

[Chr90] I. Christoff. Testing equivalences and fully abstract models for probabilistic processes. In Baeten, editor, *Proc. CONCUR, Amsterdam*, volume 458 of *Lecture Notes in Computer Science*, pages 126–140. Springer Verlag, 1990.

[Don70] J. Doner. Tree acceptors and some of their applications. *Journal of Computer and Systems Sciences*, 4:406–451, 1970.

[FH82] Y.A. Feldman and D. Harel. A probabilistic dynamic logic. In *Proc. 14th ACM Symp. on Theory of Computing*, pages 181-195, 1982.

[GJS89] A. Giacalone, C. Jou, and S.A. Smolka. Algebraic reasoning for probabilistic concurrent systems. In *Proc. IFIP TC2 Working Conference on Programming Concepts and Methods*, 1989.

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

[HJ90] H. Hansson and B. Jonsson. A calculus for communicating systems with time and probabilities. In *Proc. 11th IEEE Real -Time Systems Symposium*, Orlando, Florida, 1990.

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

[HS84] S. Hart and M. Sharir. Probabilistic temporal logics for finite and bounded models. In *Proc. 16th ACM Symp. on Theory of Computing*, pages 1–13, 1984.

[HU79] J.E. Hopcroft and J.D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.

[Jif89] H. Jifeng. Process simulation and refinement. *Formal Aspects of Computing*, 1:229–241, 1989.

[Jon87] B. Jonsson. Modular verification of asynchronous networks. In *Proc. 6:th ACM Symp. on Principles of Distributed Computing, Vancouver, Canada*, pages 152–166, Vancouver, Canada, 1987.

[JS90] C.C. Jou and S.A. Smolka. Equivalences, congruences, and complete axiomatizations for probabilistic processes. In Baeten, editor, *Proc. CONCUR, Amsterdam*, volume 458 of *Lecture Notes in Computer Science*, pages 367–383. Springer Verlag, 1990.

[Koz83] D. Kozen. A probabilistic pdl. In *Proc. 15th ACM Symp. on Theory of Computing*, pages 291–297, 1983.

[Lam83] L. Lamport. Specifying concurrent program modules. *ACM Trans. on Programming Languages and Systems*, 5(2):190–222, 1983.

[LS82] D. Lehmann and S. Shelah. Reasoning with time and chance. *Information and Control*, 53:165–198, 1982.

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

[LS90] S.S. Lam and A.U. Shankar. Refinement and projection of relational specifications. In *Stepwise Refinement of Distributed Systems, Models, Formalisms, Correctness, REX Workshop, Mook, The Netherlands, May-June 1989*, volume 430 of *Lecture Notes in Computer Science*, pages 454–486. Springer Verlag, 1990.

[LT87] N.A. Lynch and M.R. Tuttle. Hierarchical correctness proofs for distributed algorithms. In *Proc. 6:th ACM Symp. on Principles of Distributed Computing, Vancouver, Canada*, pages 137–151, 1987.

[LT88] Kim Larsen and Bent Thomsen. A modal process logic. In *Proc. 3rd IEEE Int. Symp. on Logic in Computer Science*, pages 203–210, 1988.

[Mil89] R. Milner. *Communication and Concurrency*. Prentice-Hall, 1989.

[Mol82] M.K. Molloy. Performance analysis using stochastic petri nets. *IEEE Trans. on Computers*, C-31(9):913–917, Sept. 1982.

[MP89] Z. Manna and A. Pnueli. The anchored version of the temporal framework. In de Bakker, de Roever, and Rozenberg, editors, *Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency*, volume 354 of *Lecture Notes in Computer Science*, pages 201–284. Springer Verlag, 1989.

[Plo81] G. Plotkin. A structural approach to operational semantics. Technical Report DAIMI FN-19, Computer Science Department, Aarhus University, 1981.

[PS89] S. Purushothaman and P.A. Subrahmanyam. Reasoning about probabilistic behavior in concurrent systems. *IEEE Trans. on Software Engineering*, SE-13(6):740–745, June 1989.

[PZ86] A. Pnueli and L. Zuck. Verification of multiprocess probabilistic protocols. *Distributed Computing*, 1(1):53–72, 1986.

[Rab63] M.O. Rabin. Probabilistic automata. *Information and Control*, 6:230–245, 1963.

[vGSST90] R. van Glabbeek, S.A. Smolka, B. Steffen, and C. Tofts. Reactive, generative, and stratified models of probabilistic processes. In *Proc. 5th IEEE Int. Symp. on Logic in Computer Science*, 1990.

[VW86] M.Y. Vardi and P. Wolper. An automata-theoretic approach to automatic program verification. In *Proc. 1st IEEE Int. Symp. on Logic in Computer Science*, pages 332–344, June 1986.

[Zub85] Zuberek. Performance evaluation using extended timed Petri nets. In *Proc. International Workshop on Timed Petri Nets*, Torino Italy, 1985. IEEE Computer Society 674.