Testing Preorders for Probabilistic Processes*

Rance Cleaveland†
Dept. of Computer Science
SUNY at Stony Brook
Stony Brook, NY 11794 USA
rance@cs.sunysb.edu

Zeynep Dayar
Dept. of Computer Science
North Carolina State University
Raleigh, NC 27695 USA
zdayar@eos.ncsu.edu

Scott A. Smolka‡
Dept. of Computer Science
SUNY at Stony Brook
Stony Brook, NY 11794 USA
sas@cs.sunysb.edu

Shoji Yuen§
Dept. of Information Engineering
Nagoya University
Chikusa, Nagoya 464-01 Japan
yuen@nuie.nagoya-u.ac.jp

Abstract

We present a testing preorder for probabilistic processes based on a quantification of the probability with which processes pass tests. The theory enjoys close connections with the classical testing theory of De Nicola and Hennessy in that whenever a process passes a test with probability 1 (respectively some non-zero probability) in our setting, then the process *must* (respectively *may*) pass the test in the classical theory. We also develop an alternative characterization of the probabilistic testing preorders that takes the form of a mapping from *probabilistic traces* to the interval $[0, 1]$, where a probabilistic trace is an alternating sequence of actions and probability distributions over actions.

Finally, we give *proof techniques*, derived from the alternative characterizations, for establishing preorder relationships between probabilistic processes. The utility of these techniques is demonstrated by means of some simple examples.

1 Introduction

Communicating systems often exhibit behavior that is probabilistic or statistical in nature. For example, one may observe that a faulty communication link drops a message 2% of the

*Portions of this paper first appeared in preliminary form in [CSZ92] and [YCDS94].

†Research supported in part by NSF/DARPA Grant CCR-9014775, NSF Grant CCR-9120995, ONR Young Investigator Award N00014-92-J-1582, NSF Young Investigator Award CCR-9257963, and NSF Grant CCR-9402807.

‡Research supported in part by NSF Grants CCR-9120995, CCR-9208585 and CCR–9505562, and AFOSR Grants F49620-93-1-0250, F49620-95-1-0508 and F49620-96-1-0087.

§Research performed while on leave at SUNY Stony Brook.

time or that a site in a network is down with probability 0.052. It is therefore interesting to consider *probabilistic processes* as a basis for modeling and specifying system behavior. In a probabilistic process, nondeterministic choice points are augmented with probability information in the form of distributions on outgoing transitions.

A probabilistic process can be viewed as a *labeled Markov chain*, where the label attached to a Markovian transition indicates the communication action that takes place in conjunction with the transition. In this sense, a probabilistic process can be thought of as an *open* system that can communicate with its environment (outside world), whereas a Markov chain represents a closed system. A benefit of open system specifications is that they can be *composed* to form larger and more complex specifications.

Another advantage of the probabilistic process model is that *behavioral relations* may be defined that relate probabilistic processes based on their probabilistic communication behavior. Behavioral relations include equivalence and preorder relations, where two processes are related by an equivalence relation if their behavior is in some sense identical, and by a preorder relation if the behavior of one process is "better than" the behavior of another. In the case of probabilistic processes, a preorder relation of particular interest would be one that relates processes in terms of their relative reliability in different operating environments. Moreover, environments could be modeled by *tests*, which are themselves probabilistic processes equipped with a set of *success* states.

In the case of nondeterministic processes, such a notion of testing, and accompanying preorders, has been developed by De Nicola and Hennessy [DNH83, Hen88]. They begin by defining what it means for a process to *may pass* a test (there exists an interaction sequence between the process and test leading the test to a success state) and *must pass* a test (all interaction sequences lead the test to a success state). They next define the *may* and *must* preorders as follows: a process $\mathcal{P}$ is *may* less than a process $\mathcal{Q}$ if whenever $\mathcal{P}$ *may* pass a test $\mathcal{T}$, then $\mathcal{Q}$ *may* passes $\mathcal{T}$ as well. The *must* preorder is defined similarly. The *testing* preorder is then the conjunction of the *may* and *must* preorders.

In this paper, we present a semantic framework for probabilistic processes based on the testing preorder of De Nicola and Hennessy. We begin by defining the probability with which a probabilistic process passes a test (the measure of the set of interaction sequences leading to a success state). This leads naturally to the definition of a *probabilistic testing preorder* where process $\mathcal{P}$ is less than process $\mathcal{Q}$ (denoted $\mathcal{P} \sqsubseteq \mathcal{Q}$) in the preorder when, for all tests $\mathcal{T}$, the probability that $\mathcal{P}$ passes $\mathcal{T}$ is no greater than the probability that $\mathcal{Q}$ passes $\mathcal{T}$.

We establish close connections with the testing theory of Hennessy and De Nicola by showing that if two probabilistic processes are related by our probabilistic testing preorder, then their "deprobabilized" images (obtained by erasing the probabilities in the underlying transition systems) are related by the testing preorder of De Nicola and Hennessy. Thus, the testing theory of probabilistic processes is a refinement of the testing theory of nonprobabilistic processes.

While intuitively appealing, the operational definition of $\sqsubseteq$ can be difficult to reason about. In particular, establishing that one process is related to another requires a consideration of the behavior of both processes in the context of all possible tests. Accordingly, it would be useful to have an alternative, more denotational characterization of $\sqsubseteq$ to ease the task of establishing relationships between probabilistic processes. Moreover, this characterization should be equivalent to $\sqsubseteq$, relating probabilistic processes in exactly the same manner as $\sqsubseteq$.

We present such alternative characterizations in two stages: probabilistic tests without internal τ-transitions are considered first, followed by (divergence-free) probabilistic tests with τ-transitions. This two-tier presentation allows us to isolate the impact of τ-transitions in tests on the theory. In both cases, we show that our alternative characterization is equivalent to the corresponding testing preorder.

Using the alternative characterizations, we also show that the preorder in which tests may perform τ's is a strict refinement of the one in which tests are τ-free and, more importantly, that the finer preorder is actually an equivalence relation, a fact that went unnoticed in [CSZ92]. Intuition as to why $\sqsubseteq$ is an equivalence relation stems from the fact that when a probabilistic process passes a test with probability π, then it is possible to construct "inverse" tests that the process passes with a cumulative probability of $1 - \pi$. This inverse construction critically depends upon a test's ability to perform τ-transitions.

Finally, we give *proof techniques*, derived from the alternative characterizations, for establishing preorder relationships between probabilistic processes. The utility of these techniques is demonstrated by means of some simple examples.

Framing Our Results

This subsection highlights the main features of our technical framework and provides some motivation for the choices we made.

- Our interest lies in studying *reactive systems* [Pnu86, MP91], which maintain an ongoing interaction with their environment. Examples of reactive systems include embedded-system software, operating systems, and transaction-processing systems. We also want to model *open* reactive systems, in which state transitions can be enabled or disabled, depending on the capabilities of the environment. This leads us to use labeled transition systems in our modeling, as the labels on transitions reflect the synchronizations systems require of the environments in which they execute.

- We wish to add probability information to labeled transition systems so that we can quantify notions such as relative reliability. The literature contains a myriad of proposals for achieving this effect, two of which were studied in [GSS95]. In the *reactive model* of probabilistic behavior [LS91], for any process state, a separate probability distribution is associated with the outgoing transitions labeled by the same action. The choice between actions is nondeterministic, the assumption being that the choice will be made by the environment. In the *generative model*, all outgoing transitions fall under a single probability distribution, regardless of the action names labeling these transitions. It is shown in [GSS95] that the reactive model is an abstraction of, and can therefore be derived from, the generative model. [GSS95] also considers the stratified model which is an extension of the generative model.

In this work we wish for all "nondeterministic" choices to be resolved probabilistically. In the reactive model this is not always possible since if an environment enables more than one action then the model does not contain enough information to resolve the choice among these actions probabilistically. The generative model, on the other hand, does permit this sort of nondeterminism to be handled probabilistically.

- Traditional testing theory for nondeterministic systems [DNH83, Hen88] emphasizes an *extensional* approach to system behavior: systems can only be distinguished on the basis of their interactions with external observers (i.e. tests). This philosophy fits very well with our desire to model reactive systems, and we have consequently focused on developing a testing-based semantic theory.

  Another hallmark of traditional testing theory is its insistence on treating tests as processes. The reason for this is that tests are thought of as representations of "environments" in which systems execute: the environments in essence consist of processes of the same type. Consequently, in our work we use generative probabilistic processes to model tests as well as processes.

Related Work

A number of testing frameworks for probabilistic processes have been proposed in the recent literature. These approaches are distinguished by several design decisions, including the exact nature of the model of probabilistic process and test, and the definition of the probabilistic behavioral relation. We review the ones most closely related to our work, as well as other, non-testing-oriented semantic models.

Christoff [Chr90] proposes four equivalence relations that relate generative probabilistic processes on the basis of the probability distributions they induce over finite sequences of observable events in their interactions with four different classes of nonprobabilistic, deterministic tests. Alternative characterizations of the equivalence relations are also given. In contrast, in our setup, both processes and tests are probabilistic and generative; no structural distinction exists between them.

Wu et al. [WSS97] propose a testing equivalence for *probabilistic I/O automata* and present a fully abstract characterization of the equivalence. No attempt is made to connect this theory of testing to the classical one of De Nicola and Hennessy [DNH83, Hen88]. In I/O automata [LT87], a distinction is made between *input* actions, which come from the environment and are always enabled, and *output* actions, which are locally controlled. Accordingly, in probabilistic I/O automata, separate probability distributions are associated with each input action and a single distribution with all locally controlled actions. Moreover, a *delay parameter*, which plays a key role in probabilistic I/O automata composition, is associated with each automaton state. Probabilistic I/O automata are thus a kind of hybrid of the reactive and generative models of probabilistic processes. The tests considered in [WSS97] are also PIOAs. In contrast, processes and tests in our model are strictly generative.

Yi and Larsen [YL92] add an internal probabilistic choice operator to CCS in order to model processes that exhibit both nondeterministic and probabilistic behavior. They then develop a theory of probabilistic testing in which tests are processes that can perform a distinguished action to report success. In this framework a process passes a test with a *set* of probabilities, with each probability representing a possible resolution of the nondeterministic (i.e. nonprobabilistic) behavior of the process and the test. They also define testing preorders based on De Nicola and Hennessy's [DNH83] testing preorder. Fully abstract denotational characterizations of these preorders are presented by Jonsson and Yi in [JY95]. The possibility of traditional nondeterminism eases the development of testing theories, since traditional notions of parallel composition may be used. However, such models are not "fully probabilistic", and our desire is to model systems in which all nondeterminism has a probabilistic resolution (in keeping with e.g. traditional Markov-chain-style modeling). Consequently, we disallow nondeterministic choices in our models and study the resulting testing theory.

Segala [Seg96] also considers a model with both nondeterministic and probabilistic choice, and two kinds of probabilistic testing preorders for this model: preorders sensitive to infinite traces, and preorders sensitive to finite traces only, with the latter being an extension of the testing preorder of De Nicola and Hennessy. Segala shows that under assumptions of finite branching and strong convergence, the two kinds of preorders coincide. However, as stated above, our interest is in "fully probabilized" systems in which all nondeterminism has a probabilistic resolution.

Other researchers have developed other, more intensional notions of probabilistic process equivalence in which processes are related purely on the basis of information contained in the models (rather than in interactions with tests). Larsen and Skou [LS91] focus on *probabilistic bisimulation*, an elegant extension of Milner and Park's strong bisimulation to probabilistic processes. Based on a simple, yet powerful language for nondeterministic tests in which copying is permitted, they obtain a testing characterization of probabilistic bisimulation for the reactive model of probabilistic computation. They also present a probabilistic extension of Hennessy-Milner logic that induces an equivalence on probabilistic processes that coincides with probabilistic bisimulation. Hansson and Jonsson [HJ90] also define a bisimulation equivalence for probabilistic processes (with probabilistic and nondeterministic choice) and provide a corresponding axiom system.

Baier and Hermanns [BH97] extend probabilistic bisimulation to the weak setting in the context of generative probabilistic processes. Generative processes are also studied in [JS90], where probabilistic extensions of several other well known process equivalences are proposed, including probabilistic trace, completed trace, failure, and ready equivalence.

The structure of the rest of this paper is as follows. Section 2 introduces the testing theory of probabilistic processes. Section 3 establishes the close connection with the classical testing theory of nonprobabilistic processes. Section 4 presents the alternative characterizations of the testing preorders and proof techniques derived from the characterizations. Section 5 concludes and contains our directions for future work.

2 Probabilistic Testing

In this section we first define the basic elements of our theory: probabilistic processes, tests, and interaction systems. This leads us to a natural notion of probabilistic testing and a probabilistic testing preorder.

2.1 Probabilistic Processes and Tests

Probabilistic processes are modeled as transition systems on which transitions are annotated with generative probabilities [GSS95]: from any given state, the sum of the probabilities on outgoing transitions is either 0 or 1. In the former case the process is considered to be terminated. See the Introduction for the motivation behind this model of computation.

Definition 2.1 *A* probabilistic process $\mathcal{P}$ *is a quadruple* (P, Act, μ, p_S) *where*

- P *is a countable set of* states*;*
- Act *is a countable set of* observable actions*, with* $\tau \notin Act$ *a distinguished "silent action" (we write* Act_τ *for* $Act \cup \{\tau\}$*);*
- $\mu : P \times Act_\tau \times P \to [0,1]$*, the* transition probability distribution function*, is required to be* stochastic*, i.e., for all* $p \in P$*,* $\sum_{p' \in P, \alpha \in Act_\tau} \mu(p, \alpha, p') \in \{0, 1\}$*;*
- $p_S \in P$ *is the* start state.

In the sequel, we sometimes write $p \xrightarrow{\alpha,\pi} p'$ if $\pi = \mu(p, \alpha, p') > 0$ and $p \xrightarrow{\alpha} p'$ if $\mu(p, \alpha, p') > 0$ and refer to $p \xrightarrow{\alpha,\pi} p'$ or $p \xrightarrow{\alpha} p'$ as a *transition* in $\mathcal{P}$. We also use $\mu(p, \alpha)$ to stand for $\sum_{p' \in P} \mu(p, \alpha, p')$. We only consider probabilistic processes that are *finite-branching* and *divergence-free* in this paper: process $\mathcal{P} = (P, Act, \mu, p_S)$ is *finite-branching* if for all $p \in P$ the set $\{\langle \alpha, p' \rangle \mid p \xrightarrow{\alpha} p'\}$ is finite, while $\mathcal{P}$ is *divergence-free* if for no $p \in P$ is there an infinite sequence of states $p_0, p_1, \ldots$ with $p = p_0$ and $p_i \xrightarrow{\tau} p_{i+1}$. We use **PP** to refer to the class of all such probabilistic processes.

We now introduce the notion of *execution* of a process and operations on executions.

Definition 2.2 *Let* $\mathcal{P} = (P, Act, \mu, p_S)$ *be a probabilistic process, and let* $p, p_i \in P$*,* $i \geq 0$*.*

- *An* execution e *of* $\mathcal{P}$ *is a finite sequence of the form* $p_0 \xrightarrow{\alpha_1,\pi_1} p_1 \cdots \xrightarrow{\alpha_n,\pi_n} p_n$ *where* $n \geq 0$*.*
- *Let* e *be an execution of* $\mathcal{P}$ *of the form* $p_0 \xrightarrow{\alpha_1,\pi_1} p_1 \cdots \xrightarrow{\alpha_n,\pi_n} p_n$*. Then we define the following.*
  - *The* length*,* $|e|$*, of* e *is* n*.*
  - *The* initial state*,* $\mathsf{i}(e)$*, is* p_0*.*
  - *The* final state*,* $\mathsf{f}(e)$*, is* p_n*.*

- *An execution e of $\mathcal{P}$ is said to be an* execution from p *if* $\mathsf{i}(e) = p$. *We use* $\mathsf{E}_{\mathcal{P}}(p)$ *to represent the set of all executions from p in $\mathcal{P}$,* $\mathsf{E}_{\mathcal{P}}(P)$ *to denote* $\bigcup_{p \in P} \mathsf{E}(p)$*, and* $\mathsf{E}_{\mathcal{P}}$ *for* $\mathsf{E}_{\mathcal{P}}(p_S)$.

- *Let* $e_1, e_2 \in \mathsf{E}_{\mathcal{P}}(P)$ *have form* $p_0 \xrightarrow{\alpha_1,\pi_1} p_1 \cdots \xrightarrow{\alpha_m,\pi_m} p_m$ *and* $q_0 \xrightarrow{\beta_1,\rho_1} q_1 \cdots \xrightarrow{\beta_n,\rho_n} q_n$*, respectively.*
  - *If* $p_m = q_0$ *then the* concatenation*,* $e_1 \cdot e_2$*, of* e_1 *and* e_2 *is the execution*

$$p_0 \xrightarrow{\alpha_1,\pi_1} p_1 \cdots \xrightarrow{\alpha_m,\pi_m} p_m \xrightarrow{\beta_1,\rho_1} q_1 \cdots \xrightarrow{\beta_n,\rho_n} q_n.$$

  - *Let* $\alpha \in Act_\tau, \pi \in (0,1)$*. If* $p_m \xrightarrow{\alpha,\pi} q_0$ *then* $e_1 \xrightarrow{\alpha,\pi} e_2$ *is the execution* $(e_1 \cdot p_m \xrightarrow{\alpha,\pi} q_0) \cdot e_2$.
  - e_1 *is a* prefix *of* e_2*, written* $e_1 \preceq e_2$*, if there is an execution* e' *such that* $e_1 \cdot e' = e_2$*.* e_1 *is a* proper prefix *of* e_2 *if there exists* e'*,* α *and* π *such that* $(e_1 \xrightarrow{\alpha,\pi} e') = e_2$.

- *Let* $E \subseteq \mathsf{E}_{\mathcal{P}}(P)$ *be a set of executions. Then E is* independent *if for every* $e, e' \in E$*,* $e \not\preceq e'$.

Thus an execution represents a sequence of transitions that a probabilistic process may engage in. Note that when a set of executions is independent, no execution in the set may be a proper prefix of another in the set.

We now turn our attention to defining the *tests* that will be applied to processes. Probabilistic tests are probabilistic processes with a set of states designated as *successful*. The reader should note the slight departure from the standard formulation [Hen88], in which a state of a test is considered successful if it can perform a transition labeled by a distinguished "success action" w.

Definition 2.3 *A* probabilistic test *is a quintuple* (T, Act, μ, t_S, G)*, where* (T, Act, μ, t_S) *is a probabilistic process and* $G \subseteq T$ *is a set of* successful ("good") states.

Since tests are processes, the terminology found in Definition 2.2 may also be applied to them. In addition, we may also speak of the (minimal) *successful* executions as follows.

Definition 2.4 *Let* $\mathcal{T} = (T, Act, \mu, t_S, G)$ *be a test, and let* $e \in \mathsf{E}_{\mathcal{T}}(T)$ *be the execution* $t_0 \xrightarrow{\alpha_1,\pi_1} t_1 \cdots \xrightarrow{\alpha_n,\pi_n} t_n$*. Then e is* successful *if* $t_n \in G$*, and e is* minimally successful *if in addition* $t_i \notin G$ *for all* $i < n$.

In what follows we use $\mathsf{MS}_{\mathcal{T}}(t)$ to represent the set of minimally successful executions from t; $\mathsf{MS}_{\mathcal{T}}(T)$ for $\bigcup_{t \in T} \mathsf{MS}_{\mathcal{T}}(t)$; and $\mathsf{MS}_{\mathcal{T}}$ for $\mathsf{MS}_{\mathcal{T}}(t_S)$.

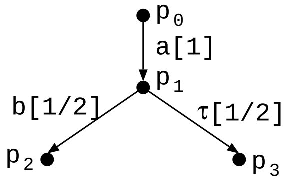
In contrast to [LS91] and [Chr90], tests in our framework are probabilistic. Our motivation for this comes from the classical testing theory of [DNH83, Hen88], in which processes and tests are structurally identical. In the classical setting it has also been shown that *finite* tests are adequate for distinguishing non-equivalent processes. Indeed, it has recently been show that the same result holds in the probabilistic setting considered in this paper [KCS98]. Therefore we shall restrict our attention to tests that are *finite* in the usual sense, i.e. finite-branching and incapable of any infinite execution sequence. We write **PT** for the set of all such tests. For both probabilistic processes and tests, we often drop the adjective "probabilistic" when it is clear from the context.

A test $\mathcal{T} = (T, Act, \mu_T, t_S, G)$ is called τ-*free* if $\mu_T(t,\tau) = 0$ for all $t \in T$. We write $\mathbf{PT}_0$ for the set of all τ-free tests.

To illustrate the above definitions, consider the probabilistic process $\mathcal{P} = (\{p_0, p_1, p_2, p_3\}, \{a, b\}, \mu_P, p_0)$, where μ_P is defined as:

$$\mu_P(p,\alpha,p') = \begin{cases} 1 & \text{if } p = p_0,\ p' = p_1 \text{ and } \alpha = a \\ \frac{1}{2} & \text{if } p = p_1,\ p' = p_2 \text{ and } \alpha = b \\ \frac{1}{2} & \text{if } p = p_1,\ p' = p_3 \text{ and } \alpha = \tau \\ 0 & \text{otherwise} \end{cases}$$

$\mathcal{P}$ can be depicted graphically as follows:



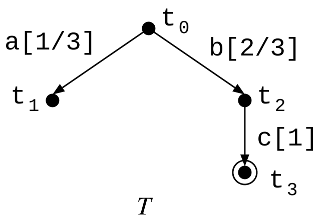
P

The executions $e_1 = p_0 \xrightarrow{a,1} p_1 \xrightarrow{b,\frac{1}{2}} p_2$ and $e_2 = p_0 \xrightarrow{a,1} p_1 \xrightarrow{\tau,\frac{1}{2}} p_3$ of process $\mathcal{P}$ are independent in the sense of Definition 2.2.

Next, consider the probabilistic test $\mathcal{T} = (\{t_0, t_1, t_2, t_3\}, \{a, b, c\}, \mu_T, t_0, \{t_3\})$, where μ_T is defined by:

$$\mu_T(t,\alpha,t') = \begin{cases} \frac{1}{3} & t = t_0,\ t' = t_1 \text{ and } \alpha = a \\ \frac{2}{3} & t = t_0,\ t' = t_2 \text{ and } \alpha = b \\ 1 & t = t_2,\ t' = t_3 \text{ and } \alpha = c \end{cases}$$

$\mathcal{T}$ is depicted in the following, where the circled states are successful:



T

For this test, the execution $e = t_0 \xrightarrow{b,\frac{2}{3}} t_2 \xrightarrow{c,1} t_3$ is the only minimally successful execution from the start state t_0.

2.2 Interaction Systems

We use *interaction systems* to formalize the notion of applying a test $\mathcal{T}$ to a process $\mathcal{P}$. Intuitively our definition of an interaction system can be interpreted in terms of a *coin-flipping protocol*. Consider the interaction between a process $\mathcal{P}$ and test $\mathcal{T}$, where initially $\mathcal{P}$ and $\mathcal{T}$ have n and m transitions of non-zero probability, respectively. To determine the interaction they should engage in, $\mathcal{P}$ flips an n-sided coin (weighted in accordance with the probability distribution on its outgoing transitions) while $\mathcal{T}$ flips an m-sided coin (similarly weighted). Should $\mathcal{P}$'s coin indicate a transition labeled α, with α possibly being τ, and $\mathcal{T}$'s coin indicate an α-transition as well, then each will engage in its respective transition. If the labels on the coins do not match but one of them is τ, then the agent ($\mathcal{P}$ or $\mathcal{T}$) whose coin indicates the τ will do its τ while the other idles. Otherwise, the coin flips are repeated. The protocol continues until the process and test reach a configuration where no further transitions are possible. Probabilistically speaking, if any interaction between a process and test is possible then this coin-flipping protocol will indicate that some interaction should take place. These intuitions can be captured as follows.

Definition 2.5 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$ be a probabilistic process and $\mathcal{T} = (T, Act, \mu_T, t_S, G)$ be a probabilistic test. Then the* interaction system *for $\mathcal{P}$ and $\mathcal{T}$, $\mathcal{P}||\mathcal{T}$, has form $(P \times T, Act, \mu_I, \langle p_S, t_S \rangle)$, where μ_I is defined with respect to a normalization function $\nu : P \times T \to [0,1]$, given by*

$$\nu(p,t) = \Big(\sum_{\alpha \in Act} \mu_P(p,\alpha) \cdot \mu_T(t,\alpha)\Big) + \mu_T(t,\tau) + \mu_P(p,\tau) - \mu_T(t,\tau) \cdot \mu_P(p,\tau)$$

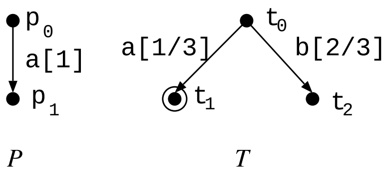
as follows:

$$\mu_I(\langle p,t \rangle, \alpha, \langle p',t' \rangle) = \begin{cases} 0 & \text{if } \nu(p,t) = 0 \\ \frac{\mu_T(t,\tau,t') \cdot (1-\mu_P(p,\tau))}{\nu(p,t)} & \text{if } \alpha = \tau \ \wedge \ p = p' \ \wedge \ \nu(p,t) \neq 0 \\ \frac{\mu_P(p,\tau,p') \cdot (1-\mu_T(t,\tau))}{\nu(p,t)} & \text{if } \alpha = \tau \ \wedge \ t = t' \ \wedge \ \nu(p,t) \neq 0 \\ \frac{\mu_P(p,\alpha,p') \cdot \mu_T(t,\alpha,t')}{\nu(p,t)} & \text{otherwise} \end{cases}$$

These definitions reflect our desire to model probabilistic reactive systems. In a reactive system, if several actions (including, possibly, a τ) are enabled and a test is capable of activating at least one of these actions (or a τ) with a certain probability, then some interaction between the system and test is guaranteed to take place. Viewed in this light, the normalized probabilities represent the conditional probability of a particular interaction taking place, *given that some interaction takes place*.

More specifically, the normalization factor $\nu(p,t)$ is intended to capture the probability of some interaction occurring; note that the last three terms in its definition represent the probability of the process or test, or both, performing a τ. In the definition of μ_I, the first clause represents the case when no interaction between the process and test is possible, while the second clause computes the conditional probability that the test performs an autonomous τ action. The third clause is similar to the second with the roles of p and t reversed. The fourth clause computes the conditional probability that the process and test engage in a joint transition, which in contrast with traditional testing theory may be labeled by a τ.

A by-product of the normalization performed in μ_I is that interaction systems themselves are stochastic. For example, consider $\mathcal{P}||\mathcal{T}$, where $\mathcal{P}$ and $\mathcal{T}$ are given by:



Based on our definition we end up with the interaction system consisting of the single transition $\langle\, p_0, t_0 \,\rangle \xrightarrow{a,1} \langle\, p_1, t_1 \,\rangle$; in other words, the process and test synchronize on a with probability 1. Without normalization, we would obtain a substochastic interaction system whose start state performs an a-transition with probability $\frac{1}{3}$ and no other transitions.

As borne out by the definitions, processes, tests, and interaction systems are all objects of essentially the same form. This homogeneity, which is not present in the approaches to probabilistic testing found in [LS91, Chr90], mirrors that found in the original testing theory of De Nicola and Hennessy. As a result, the terminology given in Definition 2.2 for processes may also be applied to interaction systems. Another desirable consequence of this is that there is a strong connection between applying a test to a process and running a process in a network with other processes.

2.3 Testing Probabilistic Processes

We now formalize the notion of the probability with which a process passes a test, and we use this idea to define a probabilistic testing preorder on processes.

Definition 2.6 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$ be a process and $\mathcal{T} = (T, Act, \mu_T, t_S, G)$ a test, with $\mathcal{P}||\mathcal{T}$ the associated interaction system.*

- *A* configuration *is any element $\langle\, p, t \,\rangle \in P \times T$.*
- *Configuration $\langle\, p, t \,\rangle$ is* successful *if $t \in G$.*
- *Configuration $\langle\, p, t \,\rangle$ is* terminal *if $\sum_{\alpha \in Act_\tau} \mu_I(\langle\, p, t \,\rangle, \alpha) = 0$ (or equivalently if $\nu(p, t) = 0$).*
- *A* partial computation *of $\mathcal{P}||\mathcal{T}$ is an execution $c \in \mathsf{E}_{\mathcal{P}||\mathcal{T}}(P \times T)$ of the form*

$$\langle\, p_0, t_0 \,\rangle \xrightarrow{\alpha_1, \pi_1} \langle\, p_1, t_1 \,\rangle \xrightarrow{\alpha_2, \pi_2} \ldots \xrightarrow{\alpha_n, \pi_n} \langle\, p_n, t_n \,\rangle$$

  such that for all $i < n, t_i \notin G$.

- *A partial computation c of $\mathcal{P}||\mathcal{T}$ is said to be a* partial computation from $\langle\, p, t \,\rangle$ *if* $\mathsf{i}(c) = \langle\, p, t \,\rangle$. *We use* $\mathsf{PC}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle)$ *for the set of all partial computations from* $\langle\, p, t \,\rangle$; $\mathsf{PC}_{\mathcal{P}||\mathcal{T}}(P \times T)$ *for* $\bigcup_{\langle\, p,t \,\rangle \in P\times T} \mathsf{PC}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle)$; *and* $\mathsf{PC}_{\mathcal{P}||\mathcal{T}}$ *for* $\mathsf{PC}_{\mathcal{P}||\mathcal{T}}(\langle\, p_S, t_S \,\rangle)$.

- *A* computation *of $\mathcal{P}||\mathcal{T}$ is a partial computation that is maximal, i.e. its final configuration is either terminal or successful. Computation c is* successful *if* $\mathsf{f}(c)$ *is successful.*

- *Computation c of $\mathcal{P}||\mathcal{T}$ is said to be a* computation from $\langle\, p, t \,\rangle$ *if* $\mathsf{i}(c) = \langle\, p, t \,\rangle$. *We use* $\mathsf{C}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle)$ *and* $\mathsf{S}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle)$ *for the set of all computations and successful computations from* $\langle\, p, t \,\rangle$, *respectively;* $\mathsf{C}_{\mathcal{P}||\mathcal{T}}(P\times T)$ *and* $\mathsf{S}_{\mathcal{P}||\mathcal{T}}(P\times T)$ *for* $\bigcup_{\langle\, p,t \,\rangle \in P\times T} \mathsf{C}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle)$ *and* $\bigcup_{\langle\, p,t \,\rangle \in P\times T} \mathsf{S}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle)$, *respectively; and* $\mathsf{C}_{\mathcal{P}||\mathcal{T}}$ *and* $\mathsf{S}_{\mathcal{P}||\mathcal{T}}$ *for* $\mathsf{C}_{\mathcal{P}||\mathcal{T}}(\langle\, p_S, t_S \,\rangle)$ *and* $\mathsf{S}_{\mathcal{P}||\mathcal{T}}(\langle\, p_S, t_S \,\rangle)$, *respectively.*

It should be noted that since tests are finite and processes divergence-free, interaction systems cannot contain infinite execution sequences. On the basis of this fact and the given definitions, the following clearly hold, for any process $\mathcal{P}$, test $\mathcal{T}$, and configuration $\langle\, p, t \,\rangle$.

$$\mathsf{S}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle) \subseteq \mathsf{C}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle) \subseteq \mathsf{PC}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle) \subseteq \mathsf{E}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle)$$

Consequently, the definitions given for executions in Definition 2.2 may also be applied to computations. The following definitions on (partial) computations will also be useful in what follows.

Definition 2.7 *Let $\mathcal{P}$ be a process and $\mathcal{T}$ a test, and let $c \in \mathsf{PC}_{\mathcal{P}||\mathcal{T}}(P \times T)$ be a partial computation with* $\mathsf{i}(c) = \langle\, p, t \,\rangle$.

- *The* projection, $\Pi_{\mathcal{T}}(c) \in \mathsf{E}_{\mathcal{T}}(t)$, *of c onto $\mathcal{T}$ is defined as follows.*

$$\Pi_{\mathcal{T}}(c) = \begin{cases} t & \text{if } c = \langle\, p, t \,\rangle \\ \Pi_{\mathcal{T}}(c') & \text{if } c = \langle\, p, t \,\rangle \xrightarrow{\alpha,\pi} c' \text{ and } \mathsf{i}(c') = \langle\, p', t \,\rangle \text{ for some } p'. \\ t \xrightarrow{\alpha,\pi} \Pi_{\mathcal{T}}(c') & \text{if } c = \langle\, p, t \,\rangle \xrightarrow{\alpha,\pi'} c',\ \mathsf{i}(c') = \langle\, p', t' \,\rangle \text{ for some } p', \\ & t' \neq t, \text{ and } \pi = \mu_T(t, \alpha, t'). \end{cases}$$

  $\Pi_{\mathcal{P}}(c) \in \mathsf{E}_{\mathcal{P}}$ *may be defined similarly.*

- *The* partial computation probability distribution function $\mathsf{Pr} : \mathsf{PC}_{\mathcal{P}||\mathcal{T}}(P \times T) \rightarrow [0, 1]$ *is defined inductively as follows.*

$$\mathsf{Pr}(\langle\, p, t \,\rangle) = 1$$
$$\mathsf{Pr}(\langle\, p, t \,\rangle \xrightarrow{\alpha,\pi} c') = \pi \cdot \mathsf{Pr}(c')$$

  If $C \subseteq \mathsf{PC}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t \,\rangle)$ is independent then we further define $\mathsf{Pr}(C) = \sum_{c\in C} \mathsf{Pr}(c)$.

- $\mathcal{P}$ *pass*$_\pi$ $\mathcal{T}$ *if* $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}||\mathcal{T}}) \geq \pi$.

Intuitively, $\Pi_{\mathcal{T}}(c)$ and $\Pi_{\mathcal{P}}(c)$ return the executions of $\mathcal{T}$ and $\mathcal{P}$ "exercised" by c. Note that in certain computation steps of an interaction system, the constituent process (resp. test) may idle, and information about such configurations is not recorded in the projection of the computation onto the process (resp. test).

$\mathsf{Pr}(c)$ records the probability that the process and test engage in computation c, starting from the initial configuration of c. The probability with which a process passes a test then becomes the cumulative probability of the successful computations in the interaction system. The inductive definition for Pr works in our setting because interaction systems, like tests, are finite. Otherwise, it would be necessary to use measure-theoretic machinery to handle infinite computations of interaction systems.

In the definition of $\mathcal{P}\, pass_\pi\, \mathcal{T}$, $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}||\mathcal{T}})$ is the measure of the set of successful computations in the interaction system for $\mathcal{P}$ and $\mathcal{T}$. Since the set of computations $\mathsf{C}_{\mathcal{P}||\mathcal{T}}$ is independent due to the maximality condition imposed on computations in Definition 2.6, both $\mathsf{Pr}(\mathsf{C}_{\mathcal{P}||\mathcal{T}})$ and $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}||\mathcal{T}})$ are well-defined.

The next lemma can be used as the basis for showing that Pr is indeed a probability distribution on computations.

Lemma 2.8 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$ and $\mathcal{T} = (T, Act, \mu_T, t_S, G)$. Then $\sum_{c \in \mathsf{C}_{\mathcal{P}||\mathcal{T}}} \mathsf{Pr}(c) = 1$.*

Proof: We prove something stronger: for all $\langle p, t \rangle \in P \times T$, $\sum_{c \in \mathsf{C}_{\mathcal{P}||\mathcal{T}}(\langle p,t \rangle)} \mathsf{Pr}(c) = 1$. The proof proceeds by a straightforward induction on the length of the longest computation in $\mathsf{C}_{\mathcal{P}||\mathcal{T}}(\langle p, t \rangle)$. Note that $\mathsf{C}_{\mathcal{P}||\mathcal{T}}(\langle p, t \rangle)$ is independent. ■

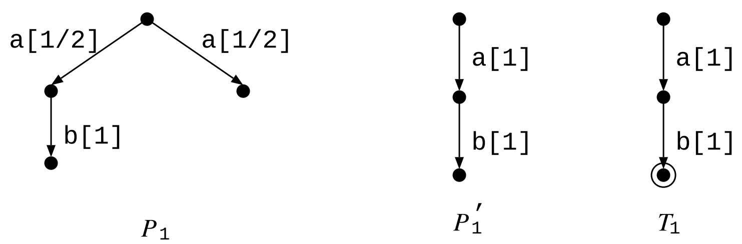
We now use these definitions to introduce preorders on probabilistic processes as follows.

Definition 2.9 (Testing preorder for probabilistic processes) *Let $\mathcal{P}$ and $\mathcal{Q}$ be processes, and let $\mathbf{E}$ be a class of tests. Then $\mathcal{P} \sqsubseteq^{\mathbf{E}} \mathcal{Q}$ holds if for all $\pi \in [0,1]$ and $\mathcal{T} \in \mathbf{E}$, $\mathcal{P}\, pass_\pi\, \mathcal{T}$ implies $\mathcal{Q}\, pass_\pi\, \mathcal{T}$.*

Intuitively, $\mathcal{P} \sqsubseteq^{\mathbf{E}} \mathcal{Q}$ means that $\mathcal{P}$ is "less reliable" with respect to $\mathbf{E}$ than $\mathcal{Q}$. When $\mathbf{E}$ is the class of all finite probabilistic tests, we omit $\mathbf{E}$ and write $\sqsubseteq$. We end this section with some examples of the probabilistic preorder.

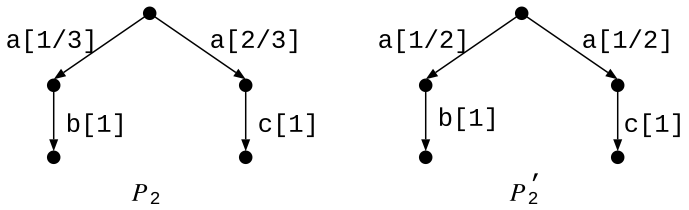
Example 2.10

1. Let $\mathcal{P}_1$ and $\mathcal{P}_1'$ be as follows:

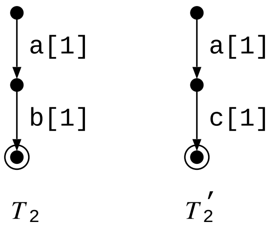


Then $\mathcal{P}_1 \sqsubseteq^{\mathbf{PT}_0} \mathcal{P}_1'$ and $\mathcal{P}_1' \not\sqsubseteq^{\mathbf{PT}_0} \mathcal{P}_1$, where recall $\mathbf{PT}_0$ is the class of τ-free tests. The latter can be seen by considering the test $\mathcal{T}_1$ above: $\mathcal{P}_1' \, pass_1 \, \mathcal{T}_1$, whereas $\mathcal{P}_1 \, pa\not{s}s_1 \, \mathcal{T}_1$.

2. Let $\mathcal{P}_2$ and $\mathcal{P}_2'$ be as follows:

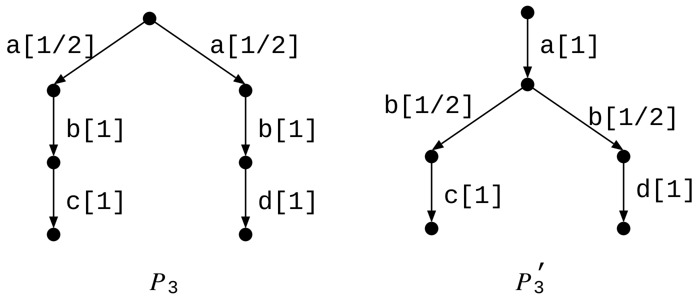


Then $\mathcal{P}_2 \not\sqsubseteq \mathcal{P}_2'$ and $\mathcal{P}_2' \not\sqsubseteq \mathcal{P}_2$, as can be seen by considering the tests $\mathcal{T}_2$ and $\mathcal{T}_2'$ given by:



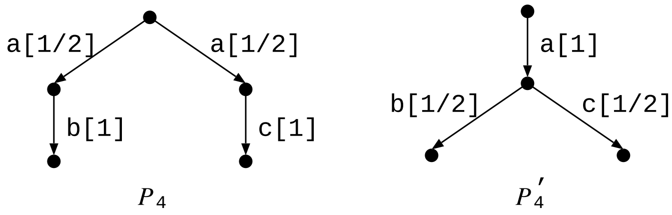
$\mathcal{P}_2 \, pass_{\frac{2}{3}} \, \mathcal{T}_2$ but $\mathcal{P}_2' \, pa\not{s}s_{\frac{2}{3}} \, \mathcal{T}_2$, and $\mathcal{P}_2' \, pass_{\frac{1}{2}} \, \mathcal{T}_2'$ but $\mathcal{P}_2 \, pa\not{s}s_{\frac{1}{2}} \, \mathcal{T}_2'$.

3. Let $\mathcal{P}_3$ and $\mathcal{P}_3'$ be as follows:



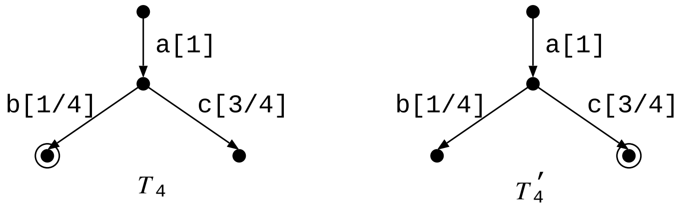
Then $\mathcal{P}_3 \equiv \mathcal{P}_3'$ ($\mathcal{P}_3 \sqsubseteq \mathcal{P}_3'$ and $\mathcal{P}_3' \sqsubseteq \mathcal{P}_3$). This example is just a probabilization of the well known pair of processes that illustrates that bisimulation is a refinement of testing equivalence. Note that these processes are distinguished by probabilistic bisimulation [LS91].

4. Let $\mathcal{P}_4$ and $\mathcal{P}_4'$ be as follows:



Then $\mathcal{P}_4 \not\sqsubseteq \mathcal{P}_4'$ and $\mathcal{P}_4' \not\sqsubseteq \mathcal{P}_4$.

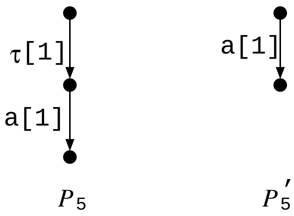
To see this, consider the following tests $\mathcal{T}_4$ and $\mathcal{T}_4'$:



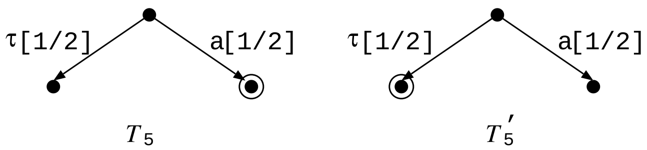
$\mathcal{P}_4\, \mathit{pass}_{\frac{1}{2}}\, \mathcal{T}_4$ but $\mathcal{P}_4'\, \mathit{pa\not{s}s}_{\frac{1}{2}}\, \mathcal{T}_4$, and therefore $\mathcal{P}_4 \not\sqsubseteq \mathcal{P}_4'$. The test $\mathcal{T}_4'$ can be similarly used to establish that $\mathcal{P}_4' \not\sqsubseteq \mathcal{P}_4$.

In this example we have a slight departure from traditional nonprobabilistic testing, in which the deprobabilized version of $\mathcal{P}_4$ would be strictly less than the deprobabilized version of $\mathcal{P}_4'$ in the testing preorder. Intuitively, the reason why $\mathcal{P}_4$ and $\mathcal{P}_4'$ are not related is that after executing an a, the test $\mathcal{T}_4$ (resp. $\mathcal{T}_4'$) is sufficiently "biased" in favor of its c-transition to ensure that $\mathcal{P}_4$ passes it with greater (resp. smaller) probability than $\mathcal{P}_4'$.

5. Let $\mathcal{P}_5$ and $\mathcal{P}_5'$ be as follows:



Then $\mathcal{P}_5 \not\sqsubseteq \mathcal{P}_5'$ and $\mathcal{P}_5' \not\sqsubseteq \mathcal{P}_5$, as can be seen by considering the tests $\mathcal{T}_5$ and $\mathcal{T}_5'$:



$\mathcal{P}_5\, \mathit{pass}_{\frac{3}{4}}\, \mathcal{T}_5'$ but $\mathcal{P}_5'\, \mathit{pa\not{s}s}_{\frac{3}{4}}\, \mathcal{T}_5'$, and $\mathcal{P}_5'\, \mathit{pass}_{\frac{1}{2}}\, \mathcal{T}_5$ but $\mathcal{P}_5\, \mathit{pa\not{s}s}_{\frac{1}{2}}\, \mathcal{T}_5$. Note that the deprobabilized versions of $\mathcal{P}_5$ and $\mathcal{P}_5'$ are testing equivalent in the classical setting. The reason why the probabilistic processes are distinguished is that P_5 in its interaction with $\mathcal{T}_5'$ (resp. $\mathcal{T}_5$) has two chances to succeed (resp. fail), while the success probability of $\mathcal{P}_5'$ is the same ($\frac{1}{2}$) for both tests.

3 Connecting Traditional and Probabilistic Testing

We now establish that the probabilistic testing preorder $\sqsubseteq$ is a strict refinement of the classical testing preorder of [DNH83, Hen88]. The proof relies on a correspondence between a probabilistic process passing a test with probability 1 (respectively some non-zero probability) and the associated nonprobabilistic process *must-passing* (respectively *may-passing*) the associated nonprobabilistic test. We begin by reviewing the classical testing theory of [DNH83, Hen88].

Definition 3.1 *A* nonprobabilistic process *is a quadruple* $(P, Act, \longrightarrow, p_S)$*, where* P *is a set of* states*,* Act *a set of* actions*,* $\longrightarrow \subseteq P \times Act_\tau \times P$ *the* transition relation*, and* $p_S \in P$ *the* start state*. A* nonprobabilistic test *is a quintuple* $(T, Act, \longrightarrow, t_S, G)$*, where* $(T, Act, \longrightarrow, t_S)$ *is a nonprobabilistic process and* $G \subseteq T$ *is the set of* successful states*.*

We only consider finite-branching, divergence-free, nonprobabilistic processes and use $\mathbf{P}$ to denote this class of processes.

As in our definition of probabilistic tests (Definition 2.3), this definition of nonprobabilistic tests differs slightly from the one of [DNH83, Hen88]. There, a test is a process and the successful states are defined to be those capable of performing a special "success action" w. This difference, however, is of no importance.

As stated previously, finite tests suffice when defining both the classical testing preorders of De Nicola and Hennessy and the probabilistic testing preorders of this paper. Accordingly, we only consider finite tests in what follows and use $\mathbf{T}$ to refer to this class of tests.

We write $p \xrightarrow{\alpha}$ if there exists a p' with $p \xrightarrow{\alpha} p'$ and $p \not\xrightarrow{\alpha}$ if this fails to be the case. We also write $p \longrightarrow$ if $p \xrightarrow{\alpha}$ holds for some $\alpha \in Act_\tau$ and $p \not\longrightarrow$ otherwise.

We now define what it means for a nonprobabilistic process to pass a test. We do so by introducing nonprobabilistic interaction systems, which record the executions in which a process may engage in response to a test.

Definition 3.2 *Let* $\mathcal{P} = (P, Act, \longrightarrow_P, p_S)$ *and* $\mathcal{T} = (T, Act, \longrightarrow_T, t_S, G)$ *be a nonprobabilistic process and test, respectively. Then the* nonprobabilistic interaction system of De Nicola and Hennessy*,* $\mathcal{P}\|_{DH}\mathcal{T}$*, is a quadruple* $(P \times T, Act, \longrightarrow_{DH}, \langle p_S, t_S \rangle)$*, where* $\longrightarrow_{DH}$ *is defined as follows.*

- $p \xrightarrow{\alpha}_P p'$, $t \xrightarrow{\alpha}_T t'$, $\alpha \in Act \Rightarrow \langle p, t \rangle \xrightarrow{\alpha}_{DH} \langle p', t' \rangle$
- $p \xrightarrow{\tau}_P p' \Rightarrow \langle p, t \rangle \xrightarrow{\tau}_{DH} \langle p', t \rangle$
- $t \xrightarrow{\tau}_T t' \Rightarrow \langle p, t \rangle \xrightarrow{\tau}_{DH} \langle p, t' \rangle$

Definition 3.3 *Let* $\mathcal{P} = (P, Act, \longrightarrow_P, p_S)$ *and* $\mathcal{T} = (T, Act, \longrightarrow_T, t_S, G)$ *be a nonprobabilistic process and a nonprobabilistic test, respectively, with* $\mathcal{P}\|_{DH}\mathcal{T}$ *the associated interaction system.*

- Successful configurations *are defined as in Definition 2.6.*
- *A* partial computation *from a configuration* $\langle p, t \rangle$ *is a sequence of the form*

$$\langle p, t \rangle = \langle p_0, t_0 \rangle \xrightarrow{\alpha_1}_{DH} \langle p_2, t_2 \rangle \xrightarrow{\alpha_2}_{DH} \ldots \xrightarrow{\alpha_n}_{DH} \langle p_n, t_n \rangle$$

  such that for all $i < n$, $\langle p_i, t_i \rangle$ *is not successful. A* computation *is a maximal partial computation in the sense of Definition 2.6.*
- $\mathsf{PC}_{\mathcal{P}\|_{DH}\mathcal{T}}(\langle p, t \rangle)$, $\mathsf{C}_{\mathcal{P}\|_{DH}\mathcal{T}}(\langle p, t \rangle)$, $\mathsf{S}_{\mathcal{P}\|_{DH}\mathcal{T}}(\langle p, t \rangle)$, *etc. are as in Definition 2.6.*
- $\mathcal{P}$ *may* $_{DH}$ $\mathcal{T}$ *if* $\mathsf{S}_{\mathcal{P}\|_{DH}\mathcal{T}} \neq \emptyset$.
- $\mathcal{P}$ *must* $_{DH}$ $\mathcal{T}$ *if* $\mathsf{S}_{\mathcal{P}\|_{DH}\mathcal{T}} = \mathsf{C}_{\mathcal{P}\|_{DH}\mathcal{T}}$.

We also adapt the definitions of execution, $\Pi_{\mathcal{P}}$ and $\Pi_{\mathcal{T}}$ in the obvious manner.

It should be noted that our definition of computation departs slightly from the one given by De Nicola and Hennessy in that we do not allow intermediate configurations to be successful. This difference, however, is inconsequential. We also require computations to be finite, whereas they allow for infinite ones. However, since our processes are divergence-free and tests are finite, their computations would also all be finite.

We now introduce the nonprobabilistic testing preorders as follows.

Definition 3.4 *Let* $\mathcal{P}, \mathcal{Q} \in \mathbf{P}$.

- $\mathcal{P} \sqsubseteq^{DH}_{may} \mathcal{Q}$ *if for all* $\mathcal{T} \in \mathbf{T}, \mathcal{P}$ *may* $_{DH}$ $\mathcal{T}$ *implies* $\mathcal{Q}$ *may* $_{DH}$ $\mathcal{T}$.
- $\mathcal{P} \sqsubseteq^{DH}_{must} \mathcal{Q}$ *if for all* $\mathcal{T} \in \mathbf{T}, \mathcal{P}$ *must* $_{DH}$ $\mathcal{T}$ *implies* $\mathcal{Q}$ *must* $_{DH}$ $\mathcal{T}$.
- $\mathcal{P} \sqsubseteq^{DH}_{test} \mathcal{Q}$ *if* $\mathcal{P} \sqsubseteq^{DH}_{may} \mathcal{Q}$ *and* $\mathcal{P} \sqsubseteq^{DH}_{must} \mathcal{Q}$.

Our goal in this section is to show that if two probabilistic processes are related by $\sqsubseteq$ then the nonprobabilistic processes obtained by "erasing" probability information are related in appropriate ways by the traditional testing preorders. One appealing approach would be to establish that the nonprobabilistic interaction system obtained from a "deprobabilized" process and test is a "deprobabilization" of the interaction system corresponding to the process and test. Unfortunately, this fails to be the case; intuitively, the problem arises from the fact that, in the probabilistic setting, processes and tests may "synchronize" on τ-transitions.

Instead, we pursue the following approach. We first present an alternative formulation of nonprobabilistic interaction systems and show that the may and must preorders it induces coincide with the ones presented above. Then we show a correspondence between these new nonprobabilistic interaction systems and probabilistic ones.

Let the state predicate only-τ() be given as follows:

$$\text{only-}\tau(p) = p \longrightarrow \wedge \; (p \xrightarrow{\alpha} \text{ implies } \alpha = \tau)$$

only-$\tau(p)$ holds if and only if the only action available to p is τ. The following introduces the new notion of nonprobabilistic interaction system.

Definition 3.5 *Let $\mathcal{P} = (P, Act, \longrightarrow_P, p_S)$ and $\mathcal{T} = (T, Act, \longrightarrow_T, t_S, G)$ be a nonprobabilistic process and a nonprobabilistic test, respectively. Then the* nonprobabilistic interaction system *$\mathcal{P}||_N\mathcal{T}$ is a quadruple $(P \times T, Act, \longrightarrow_N, \langle p_S, t_S \rangle)$, where $\longrightarrow_N$ is defined as follows.*

- $p \xrightarrow{\alpha}_P p',\ t \xrightarrow{\alpha}_T t' \Rightarrow p||_N t \xrightarrow{\alpha} p'||_N t'$
- $p \xrightarrow{\tau}_P p',\ \neg(\text{only-}\tau(t)) \Rightarrow p||_N t \xrightarrow{\tau} p'||_N t$
- $t \xrightarrow{\tau}_T t',\ \neg(\text{only-}\tau(p)) \Rightarrow p||_N t \xrightarrow{\tau} p||_N t'$

We also adapt the definitions of $\Pi_{\mathcal{P}}$ and $\Pi_{\mathcal{T}}$ in the obvious way.

The definition of $\longrightarrow_N$ above differs considerably from that of $\longrightarrow_{DH}$. To begin with, the first clause in the definition of $\longrightarrow_N$ permits synchronization on all actions, including τ. More significantly the second clause disallows autonomous τ-moves by p if the only action available to t is τ; in this case, p must synchronize with t (the first clause) to make a τ-move. The final clause is similar to the second with the roles of t and p reversed.

As the motivation for $\longrightarrow_N$ is purely technical, it is difficult to justify it in isolation. However, it turns out that the nonprobabilistic testing preorders induced by this definition coincide exactly with those of De Nicola and Hennessy. To define these new preorders, we update the terminology in Definition 3.3 by replacing occurrences of DH by N to get definitions of computation, *may* $_N$ and *must* $_N$, etc. The preorders $\sqsubseteq^N_{may}$, $\sqsubseteq^N_{must}$ and $\sqsubseteq^N_{test}$ are then given in the obvious way. The coincidence of the preorders in the context of finite tests is established by the following theorem.

Theorem 3.6 *Let $\mathcal{P}, \mathcal{Q} \in \mathbf{P}$. Then we have the following.*

- $\mathcal{P} \sqsubseteq^N_{may} \mathcal{Q}$ *iff* $\mathcal{P} \sqsubseteq^{DH}_{may} \mathcal{Q}$
- $\mathcal{P} \sqsubseteq^N_{must} \mathcal{Q}$ *iff* $\mathcal{P} \sqsubseteq^{DH}_{must} \mathcal{Q}$

Proof: It suffices to show the following.

- $\mathcal{P}$ *may* $_{DH}$ $\mathcal{T}$ iff $\mathcal{P}$ *may* $_N$ $\mathcal{T}$.
- $\mathcal{P}$ *must* $_{DH}$ $\mathcal{T}$ iff $\mathcal{P}$ *must* $_N$ $\mathcal{T}$.

Fix $\mathcal{P} = (P, Act, \mu_P, p_S)$ and $\mathcal{T} = (T, Act, \mu_T, t_S, G)$. We now have the following, the proofs for which may be found in the Appendix.

- Claim 1: For any $c \in \mathsf{C}_{\mathcal{P}||_N\mathcal{T}}$ there is a $c' \in \mathsf{C}_{\mathcal{P}||_{DH}\mathcal{T}}$ such that $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.
- Claim 2: For any $c \in \mathsf{C}_{\mathcal{P}||_{DH}\mathcal{T}}$ there is a $c' \in \mathsf{C}_{\mathcal{P}||_N\mathcal{T}}$ such that $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.

We now prove that $\mathcal{P}$ *may* $_{DH}\,\mathcal{T}$ iff $\mathcal{P}$ *may* $_N\,\mathcal{T}$ as follows.

(⇒): $\mathcal{P}$ *may* $_{DH}\,\mathcal{T}$ holds iff there exists a $c \in \mathsf{C}_{\mathcal{P}\|_{DH}\mathcal{T}}$ such that c is successful, meaning that $\mathsf{f}(\Pi_{\mathcal{T}}(c)) \in G$. Claim 2 then implies the existence of a $c' \in \mathsf{C}_{\mathcal{P}\|_N\mathcal{T}}$ such that $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$, and c' must therefore be successful. Hence $\mathcal{P}$ *may* $_N\,\mathcal{T}$.

(⇐): Can be proved similarly using Claim 1.

The proof that $\mathcal{P}$ *must* $_{DH}\,\mathcal{T}$ iff $\mathcal{P}$ *must* $_N\,\mathcal{T}$ follows similar lines.

(⇒): We establish the contrapositive of this statement. Assume $\mathcal{P}\ \not{m}ust_N\,\mathcal{T}$. Then there exists a $c \in \mathsf{C}_{\mathcal{P}\|_N\mathcal{T}}$ such that c is unsuccessful, meaning that every test state in $\Pi_{\mathcal{T}}(c)$ is unsuccessful. By Claim 1, this implies the existence of a $c' \in \mathsf{C}_{\mathcal{P}\|_{DH}\mathcal{T}}$ such that $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$. Consequently, c' is unsuccessful, and $\mathcal{P}\ \not{m}ust_{DH}\,\mathcal{T}$.

(⇐): Can be proved similarly using Claim 2.

■

The remainder of this section is devoted to showing that $\sqsubseteq$ refines $\sqsubseteq^N_{test}$ and hence $\sqsubseteq^{DH}_{test}$. We begin by defining a function h that maps probabilistic processes to nonprobabilistic ones by "erasing" the probabilities on transitions.

Definition 3.7 *The mapping* $h : \mathbf{PP} \to \mathbf{P}$ *is defined by*

$$h(P, Act, \mu_P, p_S) = (P, Act, \to_P, p_S),$$

where $(p, \alpha, p') \in \to_P$ *iff* $\mu_P(p, \alpha, p') > 0$.

We extend h to tests and interaction systems in the obvious way. The next lemma establishes that h is a homomorphism with respect to the interaction system constructors $\|$ and $\|_N$.

Lemma 3.8 *Let* $\mathcal{P}$ *be a probabilistic process,* $\mathcal{T}$ *a probabilistic test, and* $\mathcal{I} = \mathcal{P}\|\mathcal{T}$. *Then* $h(\mathcal{I}) = h(\mathcal{P}) \|_N h(\mathcal{T})$.

Proof: Let $\langle p, t \rangle$ be a state in $h(\mathcal{I})$ and $\langle p, t \rangle \xrightarrow{\alpha}_N \langle p', t' \rangle$ a transition. There are two cases to consider.

- $\alpha \neq \tau$. Then $\langle p, t \rangle \xrightarrow{\alpha}_N \langle p', t' \rangle$ in $h(\mathcal{I})$
  iff $\mu_I(\langle p, t \rangle, \alpha, \langle p', t' \rangle) > 0$ in $\mathcal{I}$
  iff $\mu_P(p, \alpha, p') > 0$ in $\mathcal{P}$ and $\mu_T(t, \alpha, t') > 0$ in $\mathcal{T}$
  iff $p \xrightarrow{\alpha}_N p'$ in $h(\mathcal{P})$ and $t \xrightarrow{\alpha}_N t'$ in $h(\mathcal{T})$
  iff $\langle p, t \rangle \xrightarrow{\alpha}_N \langle p', t' \rangle$ in $h(\mathcal{P})\|_N h(\mathcal{T})$.

- $\alpha = \tau$. Then $\langle p, t \rangle \xrightarrow{\tau}_N \langle p', t' \rangle$ in $h(\mathcal{I})$

  iff $\mu_I(\langle p, t \rangle, \tau, \langle p', t' \rangle) > 0$ in $\mathcal{I}$
  iff $\mu_P(p, \tau, p') > 0$ in $\mathcal{P}$ and $\mu_T(t, \tau, t') > 0$ in $\mathcal{T}$
  or $\mu_P(p, \tau, p') > 0$ in $\mathcal{P}$, $t = t'$, and $\mu(t, \tau) < 1$ in $\mathcal{T}$
  or $\mu_T(t, \tau, t') > 0$ in $\mathcal{T}$, $p = p'$, and $\mu(p, \tau) < 1$ in $\mathcal{P}$
  iff $p \xrightarrow{\tau}_N p'$ in $h(\mathcal{P})$ and $t \xrightarrow{\tau}_N t'$ in $h(\mathcal{T})$
  or $p \xrightarrow{\tau}_N p'$ in $h(\mathcal{P})$, $t = t'$, and $\neg(\text{only-}\tau(t))$ in $h(\mathcal{T})$
  or $t \xrightarrow{\tau}_N t'$ in $h(\mathcal{T})$, $p = p'$, and $\neg(\text{only-}\tau(p))$ in $h(\mathcal{P})$
  iff $\langle p, t \rangle \xrightarrow{\tau}_N \langle p', t' \rangle$ in $h(\mathcal{P}) \|_N h(\mathcal{T})$.

■

We now prove the main result of this section, which is that $\sqsubseteq$ is a refinement of $\sqsubseteq^N_{test}$. The proof is broken into several steps. We first establish a relationship between $pass_\pi$ and may_N, and $pass_1$ and $must_N$. We then show that $\sqsubseteq$ implies both $\sqsubseteq^N_{may}$ and $\sqsubseteq^N_{must}$. From this we obtain the result that the probabilistic testing preorder is a refinement of the nonprobabilistic testing preorder.

Lemma 3.9 *Let $\mathcal{P}$ and $\mathcal{T}$ be a probabilistic process and test, respectively.*

- *$\mathcal{P}\ pass_\pi\ \mathcal{T}$ for some $\pi > 0$ iff $h(\mathcal{P})\ may_N h(\mathcal{T})$.*
- *$\mathcal{P}\ pass_1\ \mathcal{T}$ iff $h(\mathcal{P})\ must_N h(\mathcal{T})$.*

Proof:

("may" case): $\mathcal{P}\ pass_\pi\ \mathcal{T}$ for some $\pi > 0$ iff there exists some successful computation from $\langle p_S, t_S \rangle$ in $\mathcal{P} \| \mathcal{T}$ of the form

$$\langle p_S, t_S \rangle \xrightarrow{\alpha_1, \pi_1} \langle p_1, t_1 \rangle \xrightarrow{\alpha_2, \pi_2} \cdots \xrightarrow{\alpha_n, \pi_n} \langle p_n, t_n \rangle$$

where $\pi_i > 0$ for all $1 \leq i \leq n$. From the definition of h, this holds iff there exists a successful computation in $h(\mathcal{P} \| \mathcal{T})$ of the form

$$\langle p_S, t_S \rangle \xrightarrow{\alpha_1}_N \langle p_1, t_1 \rangle \xrightarrow{\alpha_2}_N \cdots \xrightarrow{\alpha_n}_N \langle p_n, t_n \rangle$$

By Lemma 3.8, this is logically equivalent to the existence of a successful computation in $h(\mathcal{P}) \|_N h(\mathcal{T})$ and hence to the statement $h(\mathcal{P})\ may_N h(\mathcal{T})$.

("must" case): By Lemma 2.8, $\mathcal{P}\ pass_1\ \mathcal{T}$ iff every computation from $\langle p_S, t_S \rangle$ in $\mathcal{P} \| \mathcal{T}$ is successful. From the definition of h, this happens iff every computation from $\langle p_S, t_S \rangle$ in $h(\mathcal{P} \| \mathcal{T})$ is successful. By Lemma 3.8 we obtain the desired result.

■

Theorem 3.10 *Let $\mathcal{P}$ and $\mathcal{Q}$ be probabilistic processes.*

- $\mathcal{P} \sqsubseteq \mathcal{Q}$ *implies* $h(\mathcal{P}) \sqsubseteq^N_{may} h(\mathcal{Q})$.
- $\mathcal{P} \sqsubseteq \mathcal{Q}$ *implies* $h(\mathcal{P}) \sqsubseteq^N_{must} h(\mathcal{Q})$.

Proof:

($\sqsubseteq^N_{may}$): Let $\mathcal{P} \sqsubseteq \mathcal{Q}$ and $h(\mathcal{P})\ may\ _N\mathcal{T}$ for some test $\mathcal{T} \in \mathbf{T}$. Then, by Lemma 3.9, $\mathcal{P}\ pass_\pi\ \mathcal{T}_P$ for some $\pi > 0$ and all $\mathcal{T}_P$ such that $h(\mathcal{T}_P) = \mathcal{T}$. This implies $\mathcal{Q}\ pass_\pi\ \mathcal{T}_P$ (since $\mathcal{P} \sqsubseteq \mathcal{Q}$), and by Lemma 3.9, $h(\mathcal{Q})\ may\ _N h(\mathcal{T}_P)$. Thus, $h(\mathcal{Q})\ may\ _N\mathcal{T}$, and hence $h(\mathcal{P}) \sqsubseteq^N_{may} h(\mathcal{Q})$.

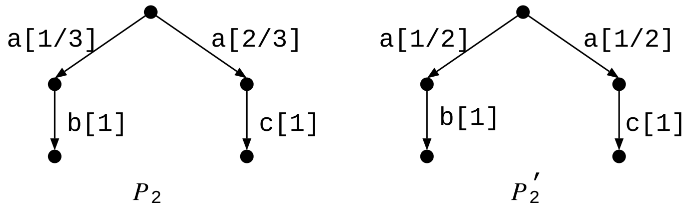
($\sqsubseteq^N_{must}$): Again let $\mathcal{P} \sqsubseteq \mathcal{Q}$ and $h(\mathcal{P})\ must\ _N\mathcal{T}$ for some $\mathcal{T} \in \mathbf{T}$. By Lemma 3.9 $\mathcal{P}\ pass_1\ \mathcal{T}_P$ for all $\mathcal{T}_P$ such that $h(\mathcal{T}_P) = \mathcal{T}$, and since $\mathcal{P} \sqsubseteq \mathcal{Q}$, $\mathcal{Q}\ pass_1\ \mathcal{T}_P$. Lemma 3.9 ensures that $h(\mathcal{Q})\ must\ _N h(\mathcal{T}_P)$, and thus $h(\mathcal{Q})\ must\ _N\mathcal{T}$. Therefore $h(\mathcal{P}) \sqsubseteq^N_{must} h(\mathcal{Q}))$.

■

The next corollary is a trivial consequence of this theorem.

Corollary 3.11 $\mathcal{P} \sqsubseteq \mathcal{Q}$ *implies* $h(\mathcal{P}) \sqsubseteq^N_{test} h(\mathcal{Q})$.

Note that the converse of Corollary 3.11 does not hold. For example, consider once again processes $\mathcal{P}_2$ and $\mathcal{P}'_2$ of Example 2.10:



$h(\mathcal{P}_2) =^N_{test} h(\mathcal{P}'_2)$ but $\mathcal{P}_2 \not\sqsubseteq \mathcal{P}'_2$ and $\mathcal{P}'_2 \not\sqsubseteq \mathcal{P}_2$. Thus, the testing theory of nonprobabilistic processes is strictly more abstract than the testing theory of probabilistic processes.

4 Alternative Characterizations

This section presents an alternative characterization of the probabilistic testing preorder defined in Section 2. The characterization relies only on information that is "local" to processes—that is, it does not require an analysis of process behavior in response to tests—and hence eases the task of establishing that two processes are related. To simplify the presentation, we first give a characterization for the preorder induced by the restricted class $\mathbf{PT}_0$ of tests without τ-moves; we then extend this characterization to the full testing preorder.

4.1 Characterization for Tests without τ

For notational convenience, we denote the preorder generated by τ-free tests as $\sqsubseteq_0$ instead of $\sqsubseteq^{\mathbf{PT}_0}$.

4.1.1 The Characterization

The alternative characterization for $\sqsubseteq_0$ relies on *probabilistic traces* and the probabilities with which processes can execute probabilistic traces. If A is a set then we call $d : A \to [0,1]$ a *(discrete) distribution over* A if $\sum_{a \in A} d(a) \in \{0,1\}$; note the (slight) departure from traditional terminology in that we allow the summation to be 0. We denote the set of all distributions over A by D_A; thus, for example, D_{Act_τ} represents the set of all distributions over Act_τ. If p is a state in process (P, Act, μ, p_S) then we write $\mu(p)$ for the distribution over Act_τ that satisfies $\mu(p)(\alpha) = \mu(p,\alpha)$ for all $\alpha \in Act_\tau$.

Definition 4.1 (Probabilistic Trace) *A* probabilistic trace *over a set A is an element $\langle d_1, \alpha_1 \rangle \cdots \langle d_n, \alpha_n \rangle$ of $(D_A \times A)^*$ such that in each $\langle d_i, \alpha_i \rangle$ the set $\{\beta \in A \mid d_i(\beta) > 0\}$ is finite. Tr_A denotes the set of all probabilistic traces over A.*

In the course of presenting our alternative characterization of $\sqsubseteq_0$, we will focus our attention on Tr_{Act}. In this case, a probabilistic trace consists of a sequence of pairs, with the first component of each pair being a probability distribution over actions and the second being an action. Intuitively, a trace represents a possible "interaction session" with a probabilistic process; each distribution defines the probabilities with which different actions are enabled by the environment, while the action component specifies the action that the environment and process agree to execute. Given such a trace, our goal is to define the probability that the process "executes" the trace to completion. Before doing this, however, we introduce some useful notation on traces.

Definition 4.2 *Let $s = \langle d_1, \alpha_1 \rangle \cdots \langle d_i, \alpha_i \rangle \cdots \langle d_n, \alpha_n \rangle$ be an element of Tr_A. Then $\delta(s) = d_1 \cdots d_i \cdots d_n$, $\delta(s,i) = d_i$, $\lambda(s) = \alpha_1 \cdots \alpha_i \cdots \alpha_n$, and $\lambda(s,i) = \alpha_i$. The length of s is denoted $|s|$; here $|s| = n$. We also use ε to represent the empty probabilistic trace.*

We now turn to defining the probability with which a process exhibits a given probabilistic trace. We begin by introducing probabilistic analogues of *weak transitions*. Intuitively, function $W_{\mathcal{P},\varepsilon} : P \times P \times D_{Act} \to [0,1]$ reflects the probability with which process $\mathcal{P}$ can silently evolve from a given state via some number of τ-transitions to another state, given a particular probability distribution describing the actions the environment is enabling. To define this function, we first give a function $W_{\mathcal{P}} : P \times N \times P \times D_{Act} \to [0,1]$ that computes the probability that $\mathcal{P}$ evolves from one state to another using a specified number of τ-transitions.

$$W_{\mathcal{P}}(p, 0, p', d) \quad = \quad \begin{cases} 1 & \text{if } p = p' \\ 0 & \text{otherwise} \end{cases}$$

$$W_{\mathcal{P}}(p,i+1,p',d) = \begin{cases} \frac{1}{\nu(p,d)} \cdot \sum_{q\in P} \mu_P(p,\tau,q)\cdot W_{\mathcal{P}}(q,i,p',d) & \text{if } \nu(p,d)\neq 0 \\ 0 \quad \text{otherwise} \end{cases}$$

$$W_{\mathcal{P},\varepsilon}(p,p',d) = \sum_{i=0}^{\infty} W_{\mathcal{P}}(p,i,p',d)$$

Here and in what follows, $\nu(p,d) = (\sum_{\alpha\in Act} \mu_P(p,\alpha)\cdot d(\alpha)) + \mu_P(p,\tau)$. The fact that $\mathcal{P}$ is divergence-free ensures that $W_{\mathcal{P},\varepsilon}(p,p',d)$ is well-defined.

We now introduce a probabilistic analogue of weak visible transitions by defining a function $N_{\mathcal{P}} : P \times Act \times P \times D_{Act} \to [0,1]$. Intuitively, $N_{\mathcal{P}}(p,a,p',d)$ captures the probability that from state p, process $\mathcal{P}$ may perform some internal transitions followed by a and arrive at p', given that the environment is enabling actions in accordance with d.

$$N_{\mathcal{P}}(p,\alpha,p',d) = \sum_{\{q\in P\mid \nu(q,d)>0\}} W_{\mathcal{P},\varepsilon}(p,q,d)\cdot \frac{d(\alpha)}{\nu(q,d)}\cdot \mu_P(q,\alpha,p')$$

The function $M_{\mathcal{P}}$ for process $\mathcal{P}$ takes a state p and a probabilistic trace s and returns the probability of $\mathcal{P}$ "executing" s from p.

Definition 4.3 *Function $M_{\mathcal{P}} : P \times Tr_{Act} \to [0,1]$ is defined as follows.*

$$\begin{aligned} M_{\mathcal{P}}(p,\varepsilon) &= 1 \\ M_{\mathcal{P}}(p,\langle\, d,\alpha\,\rangle s') &= \textstyle\sum_{p'\in P} N_{\mathcal{P}}(p,\alpha,p',d)\cdot M_{\mathcal{P}}(p',s') \end{aligned}$$

The alternative characterization for τ-free tests, written $\ll_0$, is now given in terms of $M_{\mathcal{P}}$.

Definition 4.4 *$\mathcal{P} \ll_0 \mathcal{Q}$ if for all $s\in Tr_{Act}$ $M_{\mathcal{P}}(p_S,s) \leq M_{\mathcal{Q}}(q_S,s)$.*

4.1.2 The Equality of $\ll_0$ and $\sqsubseteq_0$

This section is devoted to showing that $\ll_0$ coincides with $\sqsubseteq_0$. We break this proof into two pieces. We first establish that $\sqsubseteq_0 \subseteq \ll_0$; then we show that $\ll_0 \subseteq \sqsubseteq_0$.

$\sqsubseteq_0 \subseteq \ll_0$: We wish to establish that $\mathcal{P} \sqsubseteq_0 \mathcal{Q}$ implies $\mathcal{P} \ll_0 \mathcal{Q}$. To prove this result, we show how to construct a probabilistic test from a probabilistic trace with the property that the probability with which a process passes the test is the same as the probability with which it executes the trace. Given a probabilistic trace s, the test $\mathcal{T}(s)$ is defined as follows.

Definition 4.5 *For $s\in Tr_{Act}$, the test $\mathcal{T}(s)$ is the quintuple $(T(s), Act, \mu_{T(s)}, t_0, \{t_{|s|}\})$ where $T(s) = \{t_i \mid 0\leq i\leq |s|\}\cup\{t_{fail}\}$ and*

$$\mu_{T(s)}(t,\alpha,t') = \begin{cases} \delta(s,i)(\alpha) & \textit{if } t=t_{i-1},\ t'=t_i \textit{ and } \alpha=\lambda(s,i) \\ \delta(s,i)(\alpha) & \textit{if } t=t_{i-1},\ t'=t_{fail} \textit{ and } \alpha\neq\lambda(s,i) \\ 0 & \textit{otherwise} \end{cases}$$

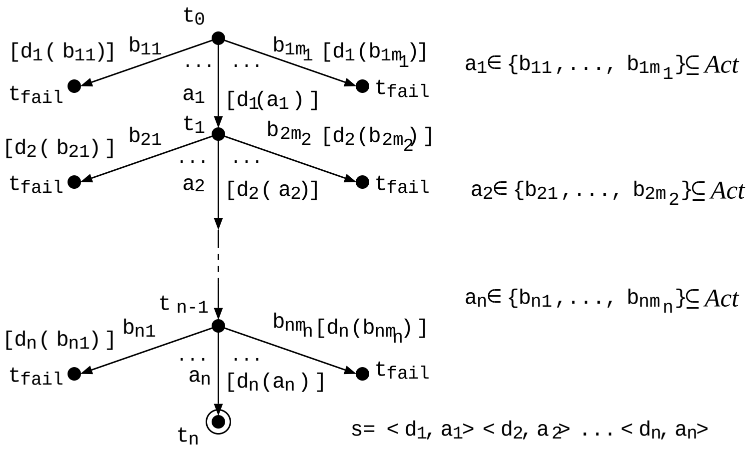


Figure 1: Structure of $\mathcal{T}(s)$

Intuitively, $\mathcal{T}(s)$ has a "spine" labeled by the actions of s that is the unique path to the successful state. Paths not on the spine lead to the failure state. Figure 1 depicts the structure of $\mathcal{T}(s)$. We are now able to prove the following.

Lemma 4.6 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$. Then for all $s \in Tr_{Act}$, $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}) = M_{\mathcal{P}}(p_S, s)$.*

Proof: See the Appendix. ■

The next lemma establishes a correspondence between $\ll_0$ and a restricted testing preorder.

Lemma 4.7 *Let $\mathbf{E}_{Tr} = \{\mathcal{T}(s) | s \in Tr_{Act}\}$. Then, $\mathcal{P} \ll_0 \mathcal{Q}$ iff $\mathcal{P} \sqsubseteq^{\mathbf{E}_{Tr}} \mathcal{Q}$.*

Proof: For the "only if" direction, assume that $\mathcal{P} \ll_0 \mathcal{Q}$, and suppose that $\mathcal{P}\, pass_\pi\, \mathcal{T}(s)$. Then $\mathsf{Pr}(\mathcal{S}_{\mathcal{P}\|\mathcal{T}(s)}) \geq \pi$, and Lemma 4.6 implies that $M_{\mathcal{P}}(p_S, s) \geq \pi$. By the definition of $\ll_0$, $M_{\mathcal{Q}}(q_S, s) \geq M_{\mathcal{P}}(p_S, s) \geq \pi$. Then Lemma 4.6 ensures that $\mathsf{Pr}(\mathcal{S}_{\mathcal{Q}\|\mathcal{T}(s)}) \geq \pi$, i.e. $\mathcal{Q}\, pass_\pi\, \mathcal{T}(s)$.

For the "if" direction, suppose $\mathcal{P} \not\ll_0 \mathcal{Q}$. Then there exists a probabilistic trace s such that $M_{\mathcal{P}}(p_S, s) > M_{\mathcal{Q}}(q_S, s)$. By Lemma 4.6, $\mathsf{Pr}(\mathcal{S}_{\mathcal{P}\|\mathcal{T}(s)}) > \mathsf{Pr}(\mathcal{S}_{\mathcal{Q}\|\mathcal{T}(s)})$, i.e. $\mathcal{P} \not\sqsubseteq^{\mathbf{E}_{Tr}} \mathcal{Q}$. ■

Given this lemma, the proof of Theorem 4.8 follows in a straightforward manner.

Theorem 4.8 *$\mathcal{P} \sqsubseteq_0 \mathcal{Q}$ implies $\mathcal{P} \ll_0 \mathcal{Q}$.*

Proof: Let $\mathbf{E}_{Tr}$ be as defined in Lemma 4.7. As $\mathbf{E}_{Tr} \subseteq \mathbf{PT}_0$, $\mathcal{P} \sqsubseteq_0 \mathcal{Q}$ implies $\mathcal{P} \sqsubseteq^{\mathbf{E}_{Tr}} \mathcal{Q}$. By Lemma 4.7, $\mathcal{P} \sqsubseteq^{\mathbf{E}_{Tr}} \mathcal{Q}$ implies $\mathcal{P} \ll_0 \mathcal{Q}$. Consequently, $\mathcal{P} \sqsubseteq_0 \mathcal{Q}$ implies $\mathcal{P} \ll_0 \mathcal{Q}$. ■

$\ll_0 \subseteq \sqsubseteq_0$**:** We now wish to show that $\mathcal{P} \ll_0 \mathcal{Q}$ implies $\mathcal{P} \sqsubseteq_0 \mathcal{Q}$. To prove this result, we in essence argue that in order to characterize how a process interacts with tests, it suffices to consider only tests of the form $\mathcal{T}(s)$—namely, tests that can be constructed from probabilistic traces. We sometimes refer to these tests as *essential* tests, since they expose all relevant aspects of process behavior.

In order to see why essential tests suffice to characterize processes with respect to $\sqsubseteq_0$, consider the factors that determine the probability with which a process $\mathcal{P}$ passes an arbitrary test $\mathcal{T}$. In general, $\mathcal{T}$ has some number of "minimally successful executions" that lead from its start state to a successful state. When $\mathcal{P}$ interacts with $\mathcal{T}$, each successful computation exercises exactly one of these successful executions. By fixing such an execution in $\mathcal{T}$ and summing up the probabilities of the relevant successful computations, we may speak of the probability with which $\mathcal{P}$ exercises that execution. Then the sum of the probabilities over all such sequences yields the probability with which $\mathcal{P}$ passes $\mathcal{T}$. Consequently, if we can construct an appropriate essential test for each minimally successful execution in $\mathcal{T}$, we can characterize the behavior of $\mathcal{P}$ with respect to $\mathcal{T}$ by looking only at the corresponding essential tests.

To formalize these intuitions, let $\mathcal{P} = (P, Act, \mu_P, p_S)$ and $\mathcal{T} = (T, Act, \mu_T, t_S, G)$ be a process and a test, respectively, let $t \in T$, and let $e \in \mathsf{E}_{\mathcal{T}}(t)$. Then we define

$$\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p,t\rangle|e) = \{c \in \mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p,t\rangle)|e \preceq \Pi_{\mathcal{T}}(c)\}.$$

Intuitively, $\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p,t\rangle|e)$ is the set of computations from $\langle p,t\rangle$ that exercise execution e in $\mathcal{T}$.

Now suppose that $e \in \mathsf{E}_{\mathcal{T}}(t)$ has form $t = t_0 \stackrel{\alpha_1,\rho_1}{\longrightarrow} t_1 \cdots \stackrel{\alpha_m,\rho_m}{\longrightarrow} t_m$ in test $\mathcal{T}$. We write $e(i)$ for the test state t_i. Then the probabilistic trace $tr(e)$ is defined as $tr(e) = \langle d_1, \alpha_1\rangle \cdots \langle d_m, \alpha_m\rangle$, where $d_i = \mu_T(e(i-1))$ is the probability distribution on actions induced by $\mathcal{T}$'s transition relation at state $e(i-1)$. Note that the fact that $\mathcal{T}$ is finite-branching ensures that each d_i returns 0 for all but a finite number of actions.

In general, because of potential nondeterminism in $\mathcal{T}$ (in the form of multiple α_i-transitions out of t_{i-1}), $d_i(\alpha_i)$ will exceed $\mu_T(t_{i-1}, \alpha_i, t_i)$, and hence the probabilistic trace does not accurately reflect the probabilities in the transition sequence. However, the next lemma shows a strong relationship between the two.

Lemma 4.9 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$ be a process and $\mathcal{T} = (T, Act, \mu_T, t_S, G)$ be a test, and let $e \in \mathsf{E}_{\mathcal{T}}$ be the execution sequence $t_S = t_0 \stackrel{\alpha_1,\pi_1}{\longrightarrow} \cdots \stackrel{\alpha_n,\pi_n}{\longrightarrow} t_n$. Then*

$$\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p_S, t_S\rangle|e)) = v \cdot M_{\mathcal{P}}(p_S, s),$$

where $s = tr(e)$ and $v = \prod_{1\le i\le n} \frac{\mu_T(t_{i-1},\alpha_i,t_i)}{\mu_T(t_{i-1},\alpha_i)}$.

Proof: See the Appendix. ∎

In the statement of this lemma, note that v and s only depend on e. Thus, once e is fixed then so are v and s. This fact and Lemma 4.9 enable us now to prove the following.

Lemma 4.10 *Let $e \in \mathsf{E}_{\mathcal{T}}$ be such that $|e| > 0$. Then $\mathcal{P} \ll_0 \mathcal{Q}$ implies $\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p_S, t_S \rangle | e)) \le \mathsf{Pr}(\mathsf{C}_{\mathcal{Q}\|\mathcal{T}}(\langle q_S, t_S \rangle | e))$.*

Proof: By Lemma 4.9, $\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p_S, t_S \rangle | e)) = v \cdot M_{\mathcal{P}}(p_S, s)$. Since v and s are determined by e, we have $\mathsf{Pr}(\mathsf{C}_{\mathcal{Q}\|\mathcal{T}}(\langle q_S, t_S \rangle | e)) = v \cdot M_{\mathcal{Q}}(q_S, s)$. By the assumption $\mathcal{P} \ll_0 \mathcal{Q}$, $M_{\mathcal{P}}(p_S, s) \le M_{\mathcal{Q}}(q_S, s)$, and thus $\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p_S, t_S \rangle | e)) \le \mathsf{Pr}(\mathsf{C}_{\mathcal{Q}\|\mathcal{T}}(\langle q_S, t_S \rangle | e))$. ∎

Theorem 4.11 *$\mathcal{P} \ll_0 \mathcal{Q}$ implies $\mathcal{P} \sqsubseteq_0 \mathcal{Q}$.*

Proof: Let $\mathcal{T} = (T, Act, \mu_T, t_S, G)$ be an arbitrary test, and recall that $\mathsf{MS}_{\mathcal{T}}$ contains the "minimally successful" executions of $\mathcal{T}$ (Definition 2.4). Then

$$\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}}) = \sum_{e \in \mathsf{MS}_{\mathcal{T}}} \mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p_S, t_S \rangle | e))$$

by the definition of $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}})$. Similarly,

$$\mathsf{Pr}(\mathsf{S}_{\mathcal{Q}\|\mathcal{T}}) = \sum_{e \in \mathsf{MS}_{\mathcal{T}}} \mathsf{Pr}(\mathsf{C}_{\mathcal{Q}\|\mathcal{T}}(\langle q_S, t_S \rangle | e)).$$

Since $\mathcal{P} \ll_0 \mathcal{Q}$, Lemma 4.10 ensures that for each $e \in \mathsf{MS}_{\mathcal{T}}$ such that $|e| > 0$, $\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p_S, t_S \rangle | e)) \le \mathsf{Pr}(\mathsf{C}_{\mathcal{Q}\|\mathcal{T}}(\langle q_S, t_S \rangle | e))$. When $|e| = 0$,

$$\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p_S, t_S \rangle | e)) = 0$$

when $e \notin G$ and

$$\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p_S, t_S \rangle | e)) = 1$$

when $e \in G$. The same is true for $\mathcal{Q}$. Consequently,

$$\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}}) \le \mathsf{Pr}(\mathsf{S}_{\mathcal{Q}\|\mathcal{T}})$$

holds, and $\mathcal{P} \sqsubseteq_0 \mathcal{Q}$. ∎

4.1.3 A Proof Technique

We close this section by giving a result that eases the task of showing $\mathcal{P} \ll_0 \mathcal{Q}$ by limiting the number of probabilistic traces that need to be considered. For $\sigma = \alpha_1 \cdots \alpha_n \in Act_\tau^*$, let $\widehat{\sigma}$ be the subsequence of σ induced by eliminating τ's, and let $p \xrightarrow{\sigma} p'$ mean that there exist $p_0, \ldots, p_n$ such that $p = p_0 \xrightarrow{\alpha_1} p_1 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_n} p_n = p'$. Then $traces(\mathcal{P}) = \{\widehat{\sigma} \mid \exists p', p_S \xrightarrow{\sigma} p'\} \subseteq 2^{Act^*}$ is the set of sequences of observable actions that $\mathcal{P}$ can execute from its start state. The following is straightforward.

Lemma 4.12 *For probabilistic trace s over Act, $\lambda(s) \in traces(\mathcal{P})$ iff $M_{\mathcal{P}}(p_S, s) > 0$.*

Proof: The "only if" direction follows directly from Definition 4.3. For the "if" direction, we show that $\lambda(s) \notin traces(\mathcal{P})$ implies $M_{\mathcal{P}}(p_S, s) = 0$. If $\lambda(s) \notin traces(\mathcal{P})$, then $\lambda(s) \neq \varepsilon$, and s can be written as $s = s_1\langle d, \alpha \rangle s_2$, where $\lambda(s_1)$, $\lambda(s_2) \in Act^*$, $d \in D_{Act}$, $\alpha \in Act$, and $\mu_P(p, \alpha) = 0$ for all p and σ such that $\widehat{\sigma} = \lambda(s_1)$ and $p_S \xrightarrow{\sigma} p$.

Let $p_S \xrightarrow{\sigma} p$ with $\widehat{\sigma} = \lambda(s_1)$. Then $M_{\mathcal{P}}(p, \langle d, \alpha \rangle s_2) = 0$ for all d, since $\alpha \neq \tau$. By the definition of $M_{\mathcal{P}}$, all summands of $M_{\mathcal{P}}(p_S, s)$ have the factor $M_{\mathcal{P}}(p, \langle d, \alpha \rangle s_2)$. Thus $M_{\mathcal{P}}(p_S, s) = 0$. ■

It also follows that if $\mathcal{P} \ll_0 \mathcal{Q}$ then any trace of $\mathcal{P}$ is a trace of $\mathcal{Q}$.

Lemma 4.13 *$\mathcal{P} \ll_0 \mathcal{Q}$ implies $traces(\mathcal{P}) \subseteq traces(\mathcal{Q})$*

Proof: $\varepsilon \in traces(\mathcal{Q})$ always. Now consider an arbitrary non-empty probabilistic trace s over Act such that $M_{\mathcal{P}}(p_S, s) > 0$. By Lemma 4.12, $\lambda(s) \in traces(\mathcal{P})$. Since $\mathcal{P} \ll_0 \mathcal{Q}$, $M_{\mathcal{Q}}(q_S, s) > 0$ showing, again by Lemma 4.12, that $\lambda(s) \in traces(\mathcal{Q})$. By Lemma 4.12, no further probabilistic traces need be considered. ■

Now suppose that $S \subseteq Tr_{Act}$. We write $\mathcal{P} \ll_0^S \mathcal{Q}$ if $M_{\mathcal{P}}(p_S, s) \leq M_{\mathcal{Q}}(q_S, s)$ for all $s \in S$. The next theorem shows that to check whether $\mathcal{P} \ll_0 \mathcal{Q}$ holds, we can limit the probabilistic traces that need checking as follows.

Theorem 4.14 *Let $S_{\mathcal{Q}} = \{s \in Tr_{Act} \mid \lambda(s) \in traces(\mathcal{Q})\}$. Then $\mathcal{P} \ll_0 \mathcal{Q}$ iff $\mathcal{P} \ll_0^{S_{\mathcal{Q}}} \mathcal{Q}$ and $traces(\mathcal{P}) \subseteq traces(\mathcal{Q})$.*

Proof: The "only if" direction follows from Definition 4.4 and Lemma 4.13, while the "if" direction is implied by Lemma 4.12. ■

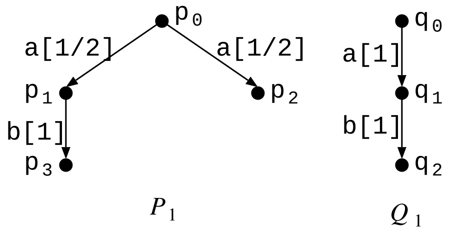
On the basis of this theorem and the equality of $\sqsubseteq_0$ and $\ll_0$, we have the following proof technique for showing that $\mathcal{P} \sqsubseteq_0 \mathcal{Q}$.

1. Check if $traces(\mathcal{P}) \subseteq traces(\mathcal{Q})$.
2. Check if $M_{\mathcal{P}}(p_S, s) \leq M_{\mathcal{Q}}(q_S, s)$ for $s \in Tr_{Act}$ such that $\lambda(s) \in traces(\mathcal{Q})$.

Note that $traces(\mathcal{P})$ and $traces(\mathcal{Q})$ may be infinite and therefore the above proof technique does not yield an automatic verification method. In general, the decidability of $\sqsubseteq_0$ is an open question.

Example 4.15 *We prove that $\mathcal{P}_1 \sqsubseteq_0 \mathcal{Q}_1$, where $\mathcal{P}_1$ and $\mathcal{Q}_1$ are depicted as follows (see also*

Example 2.10.1):

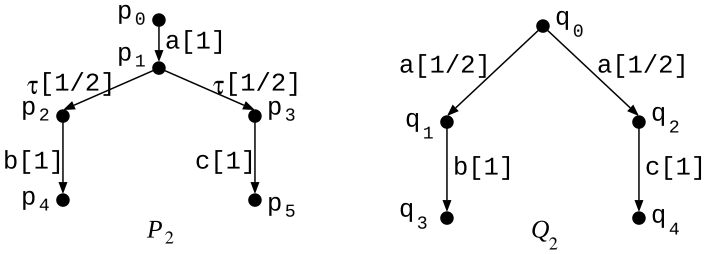


Since traces$(\mathcal{P}_1) =$ *traces*$(\mathcal{Q}_1) = \{\epsilon, a, ab\}$*, we need only check probabilistic traces* $\langle d_1, a \rangle$ *and* $\langle d_1, a \rangle \langle d_2, b \rangle$*, where* d_1 *and* d_2 *are arbitrary distributions over Act.*[1]

(Case 1): $s = \langle d_1, a \rangle$. *Then* $M_{\mathcal{P}_1}(p_S, s) = M_{\mathcal{Q}_1}(q_S, s) = 1$

(Case 2): $s = \langle d_1, a \rangle \langle d_2, b \rangle$. *Then* $M_{\mathcal{P}_1}(p_S, s) = \frac{1}{2} \leq 1 = M_{\mathcal{Q}_1}(q_S, s)$

Example 4.16 *We prove that* $\mathcal{P}_2 \sqsubseteq_0 \mathcal{Q}_2$*, where* $\mathcal{P}_2$ *and* $\mathcal{Q}_2$ *are depicted in the following:*



Since traces$(\mathcal{P}_2) =$ *traces*$(\mathcal{Q}_2) = \{\varepsilon, a, ab, ac\}$*, we need only check the following cases.*

(Case 1): $s = \langle d_1, a \rangle$. $M_{\mathcal{P}_2}(p_S, s) = M_{\mathcal{Q}_2}(q_S, s) = 1$

(Case 2): $s = \langle d_1, a \rangle \langle d_2, b \rangle$.
$M_{\mathcal{P}_2}(p_S, s) = M_{\mathcal{Q}_2}(q_S, s) = \frac{1}{2}$

(Case 3): $s = \langle d_1, a \rangle \langle d_2, c \rangle$. *Similar to Case 2.*

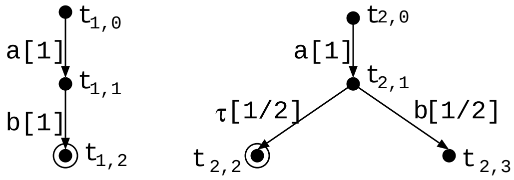
Similarly, we can show that $\mathcal{Q}_2 \sqsubseteq_0 \mathcal{P}_2$*. Consequently, we have that* $\mathcal{P}_2$ *and* $\mathcal{Q}_2$ *are equivalent with respect to* $\sqsubseteq_0 \cap \sqsubseteq_0^{-1}$*.*

4.2 Characterization for General Tests

We next investigate $\sqsubseteq^{\mathbf{PT}}$, the testing preorder induced by tests that may possess transitions labeled by τ. (In the sequel, we simply write $\sqsubseteq$ instead of $\sqsubseteq^{\mathbf{PT}}$.) As the set of tests is now

[1]We assume for the purpose of these examples that for any probabilistic trace s and each $\langle d_i, \alpha_i \rangle$ in s, $d_i(\alpha_i) > 0$. No generality is lost since, were this not the case, $M_{\mathcal{P}}(p, s) = 0$, for any $\mathcal{P}$ and state p of $\mathcal{P}$.

larger, one might expect this new preorder to be strictly finer than $\sqsubseteq_0$, and this is indeed the case. For instance, in Example 4.15, processes $\mathcal{P}_1$ and $\mathcal{Q}_1$ are related by $\sqsubseteq_0$ but not $\sqsubseteq$. To see this, let $\mathcal{T}_1$ and $\mathcal{T}_2$ be the following tests:



$\mathcal{T}_1$ $\mathcal{T}_2$

We have that $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}_1 \| \mathcal{T}_1}) = \frac{1}{2}$ and $\mathsf{Pr}(\mathsf{S}_{\mathcal{Q}_1 \| \mathcal{T}_1}) = 1$, but $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}_1 \| \mathcal{T}_2}) = \frac{3}{4}$ and $\mathsf{Pr}(\mathsf{S}_{\mathcal{Q}_1 \| \mathcal{T}_2}) = \frac{1}{2}$, thereby demonstrating that these processes are not related.

4.2.1 The Alternative Characterization

In order to define the alternative characterization of $\sqsubseteq$ we introduce τ's into probabilistic traces. Although it may seem strange to have τ's in the alternative characterization this is in some sense unavoidable since their occurrence can affect the distribution of actions enabled by the environment.

Again we define a function that gives the probability with which a process exhibits a given trace. Since probabilistic traces may now include τ's, we must modify the functions defined in the previous section.

As before, the function $W_{\tau,\mathcal{P},\varepsilon}(p, p', d)$ is designed to compute the probability that process $\mathcal{P}$ evolves from p to p' via some sequence of τ's in the context of an environment that enables actions as specified by d. The definition is given in terms of $W_{\tau,\mathcal{P}}(p, i, p', d)$ which records the probability of an evolution from p to p' using exactly i τ's.

$$
\begin{aligned}
W_{\tau,\mathcal{P}}(p, 0, p', d) &= \begin{cases} 1 & \text{if } p = p' \\ 0 & \text{otherwise} \end{cases} \\
W_{\tau,\mathcal{P}}(p, i+1, p', d) &= \begin{cases} \frac{1-d(\tau)}{\nu(p,d)} \cdot \sum_{q \in P} \mu_P(p, \tau, q) \cdot W_{\tau,\mathcal{P}}(q, i, p', d) & \text{if } \nu(p, d) \neq 0 \\ 0 \qquad\qquad \text{otherwise} \end{cases} \\
W_{\tau,\mathcal{P},\varepsilon}(p, p', d) &= \sum_{i=0}^{\infty} W_{\tau,\mathcal{P}}(p, i, p', d)
\end{aligned}
$$

Here $\nu(p, d) = (\sum_{\alpha \in Act} \mu_P(p, \alpha) \cdot d(\alpha)) + \mu_P(p, \tau) + d(\tau) - \mu_P(p, \tau) \cdot d(\tau)$. Note that d is not allowed to "execute" its τ in the determination of $W_{\tau,\mathcal{P}}(p, i, p', d)$. As before, $W_{\tau,\mathcal{P},\varepsilon}(p, p', d)$ is well defined since $\mathcal{P}$ is divergence-free.

We now define $N_{\tau,\mathcal{P}}(p, \alpha, p', d)$, the probability that $\mathcal{P}$ evolves from p to p' using internal computation followed by α, given d. When $\alpha = \tau$, we must account for two possibilities, one in which $\mathcal{P}$ participates in the execution of α and one in which it does not.

$$N_{\tau,\mathcal{P}}(p,\alpha,p',d)$$
$$= \begin{cases} \sum_{\{q \mid \nu(q,d)>0\}} W_{\tau,\mathcal{P},\varepsilon}(p,q,d) \cdot \frac{d(\tau)}{\nu(q,d)} \cdot \mu_P(q,\tau,p') & \\ \qquad + W_{\tau,\mathcal{P},\varepsilon}(p,p',d) \cdot \frac{d(\tau)}{\nu(p',d)} \cdot (1-\mu_P(p',\tau)) & \text{if } \alpha=\tau \text{ and } \nu(p',d)\neq 0 \\ \sum_{\{q \mid \nu(q,d)>0\}} W_{\tau,\mathcal{P},\varepsilon}(p,q,d) \cdot \frac{d(\alpha)}{\nu(q,d)} \cdot \mu_P(q,\alpha,p') & \text{otherwise} \end{cases}$$

Function $M_{\tau,\mathcal{P}}$ computes the probability that from a given state process $\mathcal{P}$ completes the given trace.

Definition 4.17 *Function $M_{\tau,\mathcal{P}} : P \times Tr_{Act_\tau} \to [0,1]$ is defined as follows.*

$$\begin{aligned} M_{\tau,\mathcal{P}}(p,\varepsilon) &= 1 \\ M_{\tau,\mathcal{P}}(p,\langle\, d,\alpha\,\rangle s') &= \textstyle\sum_{p'\in P} N_{\tau,\mathcal{P}}(p,\alpha,p',d)\cdot M_{\tau,\mathcal{P}}(p',s') \end{aligned}$$

The alternative characterization for general tests is given in terms of $M_{\tau,\mathcal{P}}$.

Definition 4.18 *$\mathcal{P} \ll \mathcal{Q}$ if for all $s \in Tr_{Act_\tau}$ $M_{\tau,\mathcal{P}}(p_S,s) \le M_{\tau,\mathcal{Q}}(q_S,s)$*

4.2.2 The Equality of $\ll$ and $\sqsubseteq$

In this section we establish that $\ll$ is equivalent to $\sqsubseteq$. To do this, we first show that $\sqsubseteq \subseteq \ll$, and then show that $\ll \subseteq \sqsubseteq$.

$\sqsubseteq \subseteq \ll$: The construction of probabilistic tests from probabilistic traces is the same as in Section 3, the only difference being that the action alphabet is Act_τ. Namely, $\mathcal{T}(s) = (T(s), Act_\tau, \mu_{T(s)}, t_S, \{t_{|s|}\})$ for $s \in Tr_{Act_\tau}$.

Lemma 4.19 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$. Then for all $s \in Tr_{Act_\tau}$, $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}) = M_{\tau,\mathcal{P}}(p_S,s)$.*

Proof: See the Appendix. ∎

Lemma 4.20 *Let $\mathbf{E}_{Tr,\tau} = \{\mathcal{T}(s) | s \in Tr_{Act_\tau}\}$. Then, $\mathcal{P} \ll \mathcal{Q}$ if and only if $\mathcal{P} \sqsubseteq^{\mathbf{E}_{Tr,\tau}} \mathcal{Q}$.*

Proof: Similar to the proof of Lemma 4.7. ∎

The following theorem follows from Lemma 4.20 and the fact that $\mathbf{E}_{Tr,\tau}$ in Lemma 4.20 is a subset of the finite tests.

Theorem 4.21 *$\mathcal{P} \sqsubseteq \mathcal{Q}$ implies $\mathcal{P} \ll \mathcal{Q}$.*

$\ll \subseteq \sqsubseteq$: The proof of this direction is essentially identical to the case of τ-free tests.

Lemma 4.22 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$ be a process and $\mathcal{T} = (T, Act, \mu_T, t_S, G)$ be a test, and let $e \in \mathsf{E}_\mathcal{T}$ be of form $t_S = t_0 \stackrel{\alpha_1,\pi_1}{\longrightarrow} \cdots \stackrel{\alpha_n,\pi_n}{\longrightarrow} t_n$. Then*

$$\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle\, p_S, t_S \,\rangle | e)) = v \cdot M_{\tau,\mathcal{P}}(p_S, s),$$

where $s = tr(e)$ and $v = \prod_{1 \le i \le n} \frac{\mu_T(t_{i-1},\alpha_i,t_i)}{\mu_T(t_{i-1},\alpha_i)}$.

Proof: See the Appendix. ∎

As before, s and v are dependent only on e. Thus the following lemma holds.

Lemma 4.23 *Let $e \in \mathsf{E}_\mathcal{T}$ be such that $|e| > 0$. Then $\mathcal{P} \ll \mathcal{Q}$ implies $\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle\, p_S, t_S \,\rangle | e)) \le \mathsf{Pr}(\mathsf{C}_{\mathcal{Q}\|\mathcal{T}}(\langle\, q_S, t_S \,\rangle | e))$.*

Proof: Similar to the proof of Lemma 4.10. ∎

The next theorem follows from Lemma 4.23 and the fact that:

$$\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}}) = \sum_{e \in \mathsf{MS}_\mathcal{T}} \mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle\, p_S, t_S \,\rangle | e)).$$

Theorem 4.24 *$\mathcal{P} \ll \mathcal{Q}$ implies $\mathcal{P} \sqsubseteq \mathcal{Q}$.*

Proof: Similar to the proof of Theorem 4.11. ∎

4.2.3 The Probabilistic Testing Preorder Is an Equivalence

Somewhat surprisingly, $\sqsubseteq$ turns out to be an equivalence relation. The proof relies on the fact that $\sqsubseteq$ is characterized by a special class of probabilistic tests that are "invertible": if a process passes such a test with probability π then we can find a set of tests (the inverse of the original test) that the process passes with cumulative probability $1 - \pi$. We first define the class of *non-blocking* probabilistic traces. Such traces capture an environment that persistently offers τ.

Definition 4.25 (Non-blocking probabilistic trace) *Probabilistic trace s is* non-blocking *if for all $i \le |s|$, $\delta(s, i)(\tau) > 0$.*

Definition 4.26 *$\mathcal{P} \ll^{NB} \mathcal{Q}$ if $M_{\tau,\mathcal{P}}(p_S, s) \le M_{\tau,\mathcal{Q}}(q_S, s)$ for all non-blocking s.*

We say that a probabilistic trace is "blocking" if it is not non-blocking. We also call an essential test $\mathcal{T}(s)$ "non-blocking" if s is non-blocking; otherwise, $\mathcal{T}(s)$ is said to be "blocking".

To show that $\sqsubseteq$ is characterized by $\ll^{NB}$, we first prove the following lemma.

Lemma 4.27 $\mathcal{P} \ll^{NB} \mathcal{Q}$ *implies* $\mathcal{P} \ll \mathcal{Q}$

Proof: See the Appendix. ■

That $\mathcal{P} \ll \mathcal{Q}$ implies $\mathcal{P} \ll^{NB} \mathcal{Q}$ is trivial; thus we conclude that the non-blocking essential tests give the same preorder as do the essential tests.

Corollary 4.28 $\mathcal{P} \ll \mathcal{Q}$ *if and only if* $\mathcal{P} \ll^{NB} \mathcal{Q}$

A key feature of non-blocking essential tests is that they can be "inverted": from a given non-blocking essential test we can construct a set of non-blocking essential tests with the property that the cumulative probability with which a process passes the derived tests is 1 minus the probability that the process passes the original test. The reason that non-blocking essential tests are invertible is that unsuccessful computations can only end in configurations of the form $\langle p, t_{fail} \rangle$. That is, it is impossible to fail by getting "stuck" on the spine. On the basis of the alternative characterization, then, we conclude that if $\mathcal{P} \sqsubseteq \mathcal{Q}$ holds, then so does $\mathcal{Q} \sqsubseteq \mathcal{P}$.

Definition 4.29 (Inverse Set of Non-blocking Probabilistic Traces) *For a non-blocking s, a set of non-blocking probabilistic traces, denoted by s^{-1}, is inductively constructed as follows:*

$$\begin{aligned} \varepsilon^{-1} &= \emptyset \\ (\langle d, \alpha \rangle s')^{-1} &= \{\langle d, \beta \rangle \mid \beta \neq \alpha, d(\beta) > 0\} \cup \{\langle d, \alpha \rangle s'' \mid s'' \in s'^{-1}\} \end{aligned}$$

Note that, like s, each probabilistic trace u in s^{-1} is non-blocking. The basic idea behind the definition of s^{-1} is the switching of the failure states and success states in $\mathcal{T}(s)$, the essential test constructed from s. In doing so the resulting test may have many successful paths. Therefore, we decompose this test into a set of essential tests.

Lemma 4.30 *If s is non-blocking, then* $M_{\tau,\mathcal{P}}(p_S, s) + \sum_{s' \in s^{-1}} M_{\tau,\mathcal{P}}(p_S, s') = 1$.

Proof: See the Appendix. ■

Due to the invertibility of non-blocking traces, $\ll^{NB}$ may be shown to be commutative; it is therefore an equivalence relation.

Lemma 4.31 $\mathcal{P} \ll^{NB} \mathcal{Q}$ *implies* $\mathcal{Q} \ll^{NB} \mathcal{P}$

Proof: Assume $\mathcal{P} \ll^{NB} \mathcal{Q}$. By the definition of $\ll^{NB}$, $M_{\tau,\mathcal{P}}(p_S, s) \leq M_{\tau,\mathcal{Q}}(q_S, s)$ for all non-blocking s. Also, for all $u \in s^{-1}$, $M_{\tau,\mathcal{P}}(p_S, u) \leq M_{\tau,\mathcal{Q}}(q_S, u)$ since u is non-blocking. Thus

$$\begin{aligned} \textstyle\sum_{u \in s^{-1}} M_{\tau,\mathcal{P}}(p_S, u) &\leq \textstyle\sum_{u \in s^{-1}} M_{\tau,\mathcal{Q}}(q_S, u) \\ 1 - M_{\tau,\mathcal{P}}(p_S, s) &\leq 1 - M_{\tau,\mathcal{Q}}(q_S, s) \\ M_{\tau,\mathcal{Q}}(q_S, s) &\leq M_{\tau,\mathcal{P}}(p_S, s) \end{aligned}$$

■

The equality of $\ll$ and $\ll^{NB}$ leads to the equivalence property of the preorder.

Corollary 4.32 *$\mathcal{P} \ll \mathcal{Q}$ implies $\mathcal{Q} \ll \mathcal{P}$.*

The following is obvious from the equality of $\ll$ and $\sqsubseteq$.

Corollary 4.33 *$\mathcal{P} \sqsubseteq \mathcal{Q}$ implies $\mathcal{Q} \sqsubseteq \mathcal{P}$. Therefore, $\sqsubseteq$ is an equivalence relation.*

4.2.4 A Proof Technique

We now provide a proof technique that is similar to the technique for τ-free tests. We first show that the traces of two processes are identical if they are related by the testing preorder.

Lemma 4.34 *$\mathcal{P} \ll \mathcal{Q}$ implies $traces(\mathcal{P}) = traces(\mathcal{Q})$*

Proof: $\mathcal{P} \ll \mathcal{Q}$ implies $\mathcal{P} \ll_0 \mathcal{Q}$. By Lemma 4.13, $traces(\mathcal{P}) \subseteq traces(\mathcal{Q})$; and Corollary 4.32 then guarantees that $traces(\mathcal{Q}) \subseteq traces(\mathcal{P})$. ■

It also turns out that if the "visible content" of a probabilistic trace is not a (nonprobabilistic) trace of a process, then the process is incapable of executing the probabilistic trace.

Lemma 4.35 *For probabilistic trace s over Act_τ, $\widehat{\lambda(s)} \in traces(\mathcal{P})$ iff $M_{\tau,\mathcal{P}}(p_S, s) > 0$.*

Proof: Similar to the proof of Lemma 4.12. ■

Theorem 4.36 *Let $S = \{s \in Tr_{Act_\tau} \mid \widehat{\lambda(s)} \in traces(\mathcal{P})\}$. Then $\mathcal{P} \ll \mathcal{Q}$ iff $\mathcal{P} \ll^S \mathcal{Q}$ and $traces(\mathcal{P}) = traces(\mathcal{Q})$.*

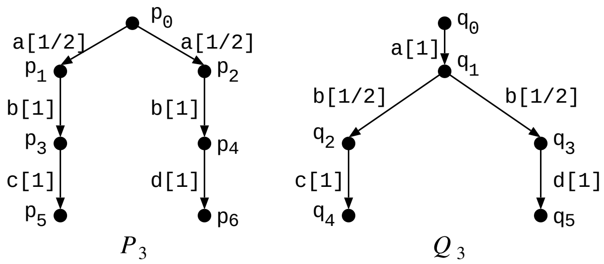
Proof: ("only if") By Definition 4.18 and Lemma 4.34. ("if") By Lemma 4.35. ■

This theorem and the equality of $\sqsubseteq$ and $\ll$ imply the following proof technique for $\mathcal{P} \sqsubseteq \mathcal{Q}$.

- Check if $traces(\mathcal{P}) = traces(\mathcal{Q})$
- Check if $M_{\tau,\mathcal{P}}(p_S, s) = M_{\tau,\mathcal{Q}}(q_S, s)$ for all s such that $\widehat{\lambda(s)} \in traces(\mathcal{P})$.

As in the case of τ-free tests, the decidability of $\sqsubseteq$ is an open question.

Example 4.37 *We use the proof technique to show that $\mathcal{P}_3 \sqsubseteq \mathcal{Q}_3$ where $\mathcal{P}_3$ and $\mathcal{Q}_3$ are depicted in the following:*



Since $traces(\mathcal{P}_3) = traces(\mathcal{Q}_3) = \{\varepsilon, a, ab, abc, abd\}$, we only need consider s such that $\widehat{\lambda(s)} \in \{\varepsilon, a, ab, abc, abd\}$. The details are in the Appendix.

5 Concluding Remarks and Future Work

In this paper we have developed a testing theory for probabilistic processes based on the notion of the probability with which processes pass tests. Close connections with the testing theory of De Nicola and Hennessy have been demonstrated, providing a well established foundation for our approach.

We also have presented alternative characterizations of the testing preorders. Specifically, we have investigated two preorders, distinguished on the basis of whether or not tests are allowed to make τ-transitions. In each case, we have proven the characterization is equivalent to the corresponding testing preorder and given a proof technique that eases the task of establishing the preorder. Moreover, we have shown the second preorder to be an equivalence relation.

Several topics for future study can be identified. Defining a process algebra for specifying probabilistic processes and tests, and investigating the congruence properties of our testing preorders with respect to the operators of this language would be an important addition to the theory. Modifying the theory to accommodate processes with arbitrary τ-transitions would also be a worthwhile pursuit and would likely necessitate the use of measure theory to handle infinite computations in interaction systems.

We also seek to establish more denotational characterizations based entirely on the structure of probabilistic processes. The acceptance tree model of [Hen88] for nondeterministic processes offers an appealing starting point for such an investigation. Progress in this direction has been made in [NdFL95] for a somewhat different model of probabilistic computation.

Interesting questions also arise about the equivalence relation $\equiv = \sqsubseteq \cap \sqsubseteq^{-1}$, i.e. the one induced by our probabilistic testing preorder. In particular, we conjecture that in terms of its distinguishing power, $\equiv$ falls strictly between strong probabilistic bisimulation [LS91] and the probabilistic testing equivalence of [Chr90]. Moreover, Examples 2.10.3 and 2.10.5 demonstrate that $\equiv$ is incomparable with Baier and Hermanns' weak probabilistic bisimulation [BH97].

Integrating real-time into our probabilistic testing preorders represents another direction for future work. The testing preorders of [CZ91], which associate time passage with τ-transitions, seem well suited as a basis for this endeavor. A testing preorder based on time and probability would enable, for example, reasoning about "soft" real-time systems in which deadlines may be missed but not "too often."

In [CSZ92], we have extended our probabilistic testing preorders to *substochastic processes*, in which the sum of the probabilities of a process's outgoing transitions may be strictly less than 1; the deficit represents the process' capacity for *undefined behavior*. Substochastic processes are appropriate for modeling faulty systems and the accompanying preorder can be used to distinguish processes based on their degree of reliability. Extending the alternative characterizations and their proof techniques to the substochastic case is another direction for future work.

References

[BH97] C. Baier and H. Hermanns. Weak bisimulation for fully probabilistic processes. In O. Grumberg, editor, *Computer Aided Verification (CAV '97)*, volume 1254 of *Lecture Notes in Computer Science*, pages 119–130, Haifa, Israel, June 1997. Springer-Verlag.

[Chr90] I. Christoff. Testing equivalences for probabilistic processes. Technical Report DoCS 90/22, Ph.D. Thesis, Department of Computer Science, Uppsala University, Uppsala, Sweden, 1990.

[CSZ92] R. Cleaveland, S. A. Smolka, and A. E. Zwarico. Testing preorders for probabilistic processes. In W. Kuich, editor, *Automata, Languages and Programming (ICALP '92)*, volume 623 of *Lecture Notes in Computer Science*, pages 708–719, Vienna, July 1992. Springer-Verlag.

[CZ91] R. Cleaveland and A. Zwarico. A theory of testing for real time. In *Sixth Annual Symposium on Logic in Computer Science (LICS '91)*, pages 110–119, Amsterdam, July 1991. Computer Society Press.

[DNH83] R. De Nicola and M. C. B. Hennessy. Testing equivalences for processes. *Theoretical Computer Science*, 34:83–133, 1983.

[GSS95] R. J. van Glabbeek, S. A. Smolka, and B. Steffen. Reactive, generative, and stratified models of probabilistic processes. *Information and Computation*, 121(1):59–80, August 1995.

[Hen88] M. C. B. Hennessy. *Algebraic Theory of Processes*. MIT Press, Boston, Mass., 1988.

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

[JS90] C.-C. Jou and S. A. Smolka. Equivalences, congruences, and complete axiomatizations for probabilistic processes. In J. C. M. Baeten and J. W. Klop, editors, *Proceedings of the First International Conference on Concurrency Theory (CONCUR '90),* Vol. 458 of *Lecture Notes in Computer Science*, pages 367–383, Berlin, 1990. Springer-Verlag.

[JY95] B. Jonsson and W. Yi. Compositional testing preorders for probabilistic processes. In *Tenth Annual Symposium on Logic in Computer Science (LICS '95)*, pages 431–441, San Diego, California, June 1995. Computer Society Press.

[KCS98] K. Narayan Kumar, R. Cleaveland, and S. A. Smolka. Infinite probabilistic and non-probabilistic testing. In *Proceedings of the 18th Conference on the Foundations of Software Technology and Theoretical Computer Science*, Lecture Notes in Computer Science. Springer-Verlag, December 1998.

[LS91] K. G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, September 1991.

[LT87] N. A. Lynch and M. Tuttle. Hierarchical correctness proofs for distributed algorithms. In *Proceedings of the* 6*th Annual ACM Symposium on Principles of Distributed Computing*, pages 137–151, 1987.

[MP91] Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems: Specification.* Springer-Verlag, 1991.

[NdFL95] M. Nunez, D. de Frutos, and L. Llana. Acceptance trees for probabilistic processes. In I. Lee and S. A. Smolka, editors, *Proceedings of CONCUR '95 — Sixth International Conference on Concurrency Theory.* Volume 962 of *Lecture Notes in Computer Science*, Springer-Verlag, 1995.

[Pnu86] A. Pnueli. Applications of temporal logic to the specification and verification of reactive systems: A survey of current trends. In J. de Bakker, W.-P. de Roever, and G. Rozenberg, editors, *Current Trends in Concurrency.* Volume 224 of *Lecture Notes in Computer Science*, Springer-Verlag, 1986.

[Seg96] R. Segala. Testing probabilistic automata. In U. Montanari and V. Sassone, editors, *CONCUR '96*, volume 1119 of *Lecture Notes in Computer Science*, pages 299–314, Pisa, Italy, August 1996. Springer-Verlag.

[WSS97] S.-H. Wu, S. A. Smolka, and E. W. Stark. Composition and behaviors of probabilistic I/O automata. *Theoretical Computer Science*, 176(1-2):1–38, 1997.

[YCDS94] S. Yuen, R. Cleaveland, Z. Dayar, and S. A. Smolka. Fully abstract characterizations of testing preorders for probabilistic processes. In B. Jonsson and J. Parrow, editors, *CONCUR '94*, volume 836 of *Lecture Notes in Computer Science*, Uppsala, Sweden, August 1994. Springer-Verlag.

[YL92] W. Yi and K. G. Larsen. Testing probabilistic and nondeterministic processes. In *Protocol Specification, Testing and Verification XII*, pages 47–61. North-Holland, 1992.

A Appendix

Proof of Claims 1 and 2 of Theorem 3.6

Proof of Claim 1. We in fact prove the following stronger claim.

> For every $\langle p,t \rangle \in P \times T$, if $c \in \mathsf{PC}_{\mathcal{P}\|_N\mathcal{T}}(\langle p,t \rangle)$ then there exists $c' \in \mathsf{PC}_{\mathcal{P}\|_{DH}\mathcal{T}}(\langle p,t \rangle)$ such that $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.

The proof proceeds by induction on the length of c.

(Base case): $c = \langle p,t \rangle$.
Pick $c' = \langle p,t \rangle$. We have $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$ trivially.

(Induction step): $c = \langle p,t \rangle \xrightarrow{\alpha}_N c_t$, where c_t has initial configuration $\langle p',t' \rangle$.
We now perform a case analysis on the form of $\langle p,t \rangle \xrightarrow{\alpha}_N \langle p',t' \rangle$.

- $\alpha \neq \tau$. In this case we have $p \xrightarrow{\alpha}_P p'$ and $t \xrightarrow{\alpha}_T t'$, whence $\langle p,t \rangle \xrightarrow{\alpha}_{DH} \langle p',t' \rangle$. By the induction hypothesis, there is a $c_t{}' \in \mathcal{PC}_{\mathcal{P}\|_{DH}\mathcal{T}}(\langle p',t' \rangle)$ such that $\Pi_{\mathcal{T}}(c_t) = \Pi_{\mathcal{T}}(c_t{}')$. We can now pick $c' = \langle p,t \rangle \xrightarrow{\alpha}_{DH} c_t{}'$; by the definition of $\Pi_{\mathcal{T}}$, $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.
- $\alpha = \tau, p = p', t \neq t'$. In this case $t \xrightarrow{\tau}_T t'$, and therefore $\langle p,t \rangle \xrightarrow{\tau}_{DH} \langle p,t' \rangle$. By the induction hypothesis, there is a $c_t{}' \in \mathcal{PC}_{\mathcal{P}\|_{DH}\mathcal{T}}(\langle p,t' \rangle)$ such that $\Pi_{\mathcal{T}}(c_t) = \Pi_{\mathcal{T}}(c_t{}')$. We now choose $c' = \langle p,t \rangle \xrightarrow{\tau}_{DH} c_t{}'$; the definition of $\Pi_{\mathcal{T}}$ ensures that $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.
- $\alpha = \tau, p \neq p', t = t'$. This proof is symmetric to the previous case.
- $\alpha = \tau, p \neq p', t \neq t'$. In this case $p \xrightarrow{\tau}_P p'$ and $t \xrightarrow{\tau}_T t'$, and thus $\langle p,t \rangle \xrightarrow{\tau}_{DH} \langle p',t \rangle \xrightarrow{\tau}_{DH} \langle p',t' \rangle$. By the induction hypothesis, there exists $c_t{}' \in \mathcal{PC}_{\mathcal{P}\|_{DH}\mathcal{T}}(\langle p',t' \rangle)$ such that $\Pi_{\mathcal{T}}(c_t) = \Pi_{\mathcal{T}}(c_t{}')$. Now set $c' = \langle p,t \rangle \xrightarrow{\tau}_{DH} \langle p',t \rangle \xrightarrow{\tau}_{DH} c_t{}'$. Then, by the definition of $\Pi_{\mathcal{T}}$, $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.

Note that there cannot be a case where $\alpha = \tau$, $p = p'$ and $t = t'$, since both processes and tests are divergence-free.

Proof of Claim 2. In order to prove this claim we first establish the following lemmas.

Lemma A.1 *Let* $c = (\langle p,t \rangle = \langle p_0,t_0 \rangle) \xrightarrow{\tau}_{DH} \langle p_1,t_1 \rangle \xrightarrow{\tau}_{DH} \dots \xrightarrow{\tau}_{DH} \langle p_n,t_n \rangle \in \mathsf{PC}_{\mathcal{P}\|_{DH}\mathcal{T}}(\langle p,t \rangle)$. *Then there exists* $c' \in \mathsf{PC}_{\mathcal{P}\|_N\mathcal{T}}(\langle p,t \rangle)$ *such that* $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.

Proof: First note that from Definition 3.3 no $t_i, i < n$ is successful. Given c, we construct the corresponding c' as follows. Since a process and a test are not allowed to synchronize on τ in the DH setting, c can be viewed as an interleaving of τ-moves that the process and the test perform. Let k represent the number of the n τ-moves in c performed by the process, and $(n-k)$ the number performed by the test. So $\Pi_{\mathcal{P}}(c)$ has form

$$p_0 \xrightarrow{\tau}_P p'_1 \xrightarrow{\tau}_P \ldots \xrightarrow{\tau}_P p'_k$$

while $\Pi_{\mathcal{T}}(c)$ has form

$$t_0 \xrightarrow{\tau}_T t'_1 \xrightarrow{\tau}_T \ldots \xrightarrow{\tau}_T t'_{n-k},$$

where for every i there is a j such that $p_i = p'_j$ and $t_i = t'_j$.

There are two cases that need to be considered in the construction of c'.

1. $k \geq (n-k)$. We can choose c' as follows.

$$c' = \langle p_0, t_0 \rangle \xrightarrow{\tau}_N \langle p'_1, t'_1 \rangle \xrightarrow{\tau}_N \ldots \xrightarrow{\tau}_N \langle p'_{n-k}, t'_{n-k} \rangle$$

   Clearly $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.

2. $k < (n-k)$. Here we select c' to be the following.

$$c' = \langle p_0, t_0 \rangle \xrightarrow{\tau}_N \langle p'_1, t'_1 \rangle \xrightarrow{\tau}_N \ldots \xrightarrow{\tau}_N \langle p'_k, t'_k \rangle \xrightarrow{\tau}_N c^{(n-k-(k+1))}$$

   where $c^{(n-k-j)}, k < j \leq n-k$ is constructed recursively as follows:

   - if $p'_{j-1} \not\xrightarrow{\tau}_P$ then set $p'_j = p'_{j-1}$ and $c^{(n-k-j)} = \langle p'_j, t'_j \rangle \xrightarrow{\tau}_N c^{(n-k-(j+1))}$.
   - else choose $p'_j \in P$ such that $p'_{j-1} \xrightarrow{\tau}_P p'_j$ and set $c^{(n-k-j)} = \langle p'_j, t'_j \rangle \xrightarrow{\tau}_N c^{(n-k-(j+1))}$

   Again $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.

■

Lemma A.2 *Let $c = (\langle p, t \rangle = \langle p_0, t_0 \rangle) \xrightarrow{\tau}_{DH} \langle p_1, t_1 \rangle \xrightarrow{\tau}_{DH} \ldots \xrightarrow{\tau}_{DH} \langle p_n, t_n \rangle \in \mathsf{PC}_{\mathcal{P}\|_{DH}\mathcal{T}}(\langle p, t \rangle)$ be such that $\langle p_n, t_n \rangle \xrightarrow{\alpha}_{DH}$ for some $\alpha \in Act$. Then there exists $c' \in \mathsf{PC}_{\mathcal{P}\|_N\mathcal{T}}(\langle p, t \rangle)$ such that $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$ and $\mathsf{f}(c') = \langle p_n, t_n \rangle$.*

Proof: Using the same argument as in the proof of the previous lemma, let k of the n τ-moves in c be performed by the process and the remaining $(n-k)$ be performed by the test. Also let

$$\Pi_{\mathcal{P}}(c) = p_0 \xrightarrow{\tau}_P p'_1 \xrightarrow{\tau}_P \ldots \xrightarrow{\tau}_P p'_k$$

and

$$\Pi_{\mathcal{T}}(c) = t_0 \xrightarrow{\tau}_T t'_1 \xrightarrow{\tau}_T \ldots \xrightarrow{\tau}_T t'_{n-k}.$$

The two cases to consider in the construction of c' are:

1. $k \geq (n-k)$. In this case consider

$$c' \;=\; \langle\, p_0, t_0 \,\rangle \xrightarrow{\tau}_N \langle\, p'_1, t'_1 \,\rangle \xrightarrow{\tau}_N \cdots \xrightarrow{\tau}_N \langle\, p'_{n-k}, t'_{n-k} \,\rangle \xrightarrow{\tau}_N \langle\, p'_{n-k+1}, t'_{n-k} \,\rangle \xrightarrow{\tau}_N \ldots \xrightarrow{\tau}_N \langle\, p'_k, t'_{n-k} \,\rangle.$$

Since t'_{n-k} is the last test state visited by c, $t'_{n-k} = t_n$. We also know that $t_n \xrightarrow{\alpha}_T$ since $\langle\, p_n, t_n \,\rangle \xrightarrow{\alpha}_{DH}$ for some $\alpha \in Act$. By the definition of $\longrightarrow_N$, the process can perform the rest of its τ-moves independently and evolve into the state $p'_k = p_n$. Obviously, $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.

2. $k < (n-k)$. In this case choose

$$c' \;=\; \langle\, p_0, t_0 \,\rangle \xrightarrow{\tau}_N \langle\, p'_1, t'_1 \,\rangle \xrightarrow{\tau}_N \ldots \xrightarrow{\tau}_N \langle\, p'_k, t'_k \,\rangle \xrightarrow{\tau}_N \langle\, p'_k, t'_{k+1} \,\rangle \xrightarrow{\tau}_N \ldots \xrightarrow{\tau}_N \langle\, p'_k, t'_{n-k} \,\rangle$$

Here the process state p'_k is the same as p_n and we know that $p_n \xrightarrow{\alpha}_P$ for some $\alpha \in Act$, so the test performs the rest of its τ-moves independently and evolves into $t'_{n-k} = t_n$. Again, $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.

■

We can now prove Claim 2. As before, we establish something stronger.

> For every $\langle\, p, t \,\rangle \in P \times T$, if $c \in \mathsf{PC}_{\mathcal{P}\|_{DH}\mathcal{T}}(\langle\, p, t \,\rangle)$ then there exists $c' \in \mathsf{PC}_{\mathcal{P}\|_N\mathcal{T}}(\langle\, p, t \,\rangle)$ such that $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.

The proof proceeds by induction on the length of c.

(Base case): $c = \langle\, p, t \,\rangle$. Choose $c' = \langle\, p, t \,\rangle$.

(Induction step): $c = \langle\, p, t \,\rangle \xrightarrow{\alpha}_{DH} c_t$ where c_t has initial configuration $\langle\, p', t' \,\rangle$. The proof splits into several cases based on the form of $\langle\, p, t \,\rangle \xrightarrow{\alpha}_{DH} \langle\, p', t' \,\rangle$.

- $\alpha \neq \tau$. Here we have $p \xrightarrow{\alpha}_P p'$ and $t \xrightarrow{\alpha}_T t'$, and thus $\langle\, p, t \,\rangle \xrightarrow{\alpha}_N \langle\, p', t' \,\rangle$. By the induction hypothesis, there is a $c_t' \in \mathcal{PC}_{\mathcal{P}\|_N\mathcal{T}}(\langle\, p', t' \,\rangle)$ such that $\Pi_{\mathcal{T}}(c_t) = \Pi_{\mathcal{T}}(c_t')$. Pick $c' = \langle\, p, t \,\rangle \xrightarrow{\alpha}_N c_t'$ from which it follows that $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.
- $\alpha = \tau, p = p'$, and $t \neq t'$. So we know that $t \xrightarrow{\tau}_T t'$. We now consider the following subcases.
  - $\neg$(only-$\tau(p)$). In this case we can infer that $\langle\, p, t \,\rangle \xrightarrow{\tau}_N \langle\, p, t' \,\rangle$. By the induction hypothesis, there is a $c_t' \in \mathcal{PC}_{\mathcal{P}\|_N\mathcal{T}}(\langle\, p, t' \,\rangle)$ such that $\Pi_{\mathcal{T}}(c_t) = \Pi_{\mathcal{T}}(c_t')$. We can pick $c' = \langle\, p, t \,\rangle \xrightarrow{\tau}_N c_t'$ to get the desired result.
  - only-$\tau(p)$. This case splits into two subcases.
    - c is a sequence of τ-transitions. Then Lemma A.1 guarantees the existence of $c' \in \mathsf{PC}_{\mathcal{P}\|_N\mathcal{T}}(\langle\, p, t \,\rangle)$ such that $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$, and hence the desired result.

* c contains at least one visible action transition, i.e.

$$c = \langle\, p, t \,\rangle \xrightarrow{\tau}_{DH} \ldots \xrightarrow{\tau}_{DH} \langle\, p_r, t_r \,\rangle \xrightarrow{\beta}_{DH} c_r \text{ with } \beta \in \mathit{Act}.$$

Let $c_h = \langle\, p, t \,\rangle \xrightarrow{\tau}_{DH} \ldots \xrightarrow{\tau}_{DH} \langle\, p_r, t_r \,\rangle$. By Lemma A.2 we know that there exists $c'_h \in \mathcal{PC}_{\mathcal{P}||_N\mathcal{T}}(\langle\, p, t \,\rangle)$ such that $\Pi_{\mathcal{T}}(c_h) = \Pi_{\mathcal{T}}(c'_h)$, and $\mathsf{f}(c'_h) = \langle\, p_r, t_r \,\rangle$. Now consider $\langle\, p_r, t_r \,\rangle \xrightarrow{\beta}_{DH} c_r$. By the induction hypothesis, there exists c'_r such that $\Pi_{\mathcal{T}}(c_r) = \Pi_{\mathcal{T}}(c'_r)$ and $\mathsf{i}(c'_r) = \mathsf{i}(c_r)$. We can now pick c' to be the computation $c'_h \xrightarrow{\beta}_N c'_r$ obtained by connecting the last configuration, $\langle\, p_r, t_r \,\rangle$, in c'_h to the first configuration in c'_r via a $\xrightarrow{\beta}_N$ transition. Clearly $\Pi_{\mathcal{T}}(c) = \Pi_{\mathcal{T}}(c')$.

- $\alpha = \tau, p \neq p'$, and $t = t'$. The proof is symmetric to the previous case.

Note that there cannot be a case where $\alpha = \tau$, $p = p'$, and $t = t'$, since both processes and tests are divergence-free. The case where $\alpha = \tau$, $p \neq p'$, and $t \neq t'$ is also impossible, since a process and a test cannot synchronize on a τ in the De Nicola and Hennessy setting.

Proof of Lemma 4.6

We prove, by induction on the length of s, a stronger result, namely, that for all $p \in P$, $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}||\mathcal{T}(s)}(\langle\, p, t_0 \,\rangle)) = M_{\mathcal{P}}(p, s)$. Before proceeding with the proof, we state and prove a number of sublemmas. The first of these shows the correspondence between the two normalization functions, namely, $\nu : P \times T \to [0,1]$ (defined in Section 2.2), and $\nu : P \times D_{\mathit{Act}} \to [0,1]$ (defined in Section 4.1.1).

Lemma A.3 *Let $\mathcal{P} = (P, \mathit{Act}, \mu_P, p_S)$, $s = \langle\, d, \alpha \,\rangle s'$, and $q \in P$. Then $\nu(q, d) = \nu(q, t_0)$, where t_0 is the start state of $\mathcal{T}(s)$.*

Proof:

$$\begin{aligned} \nu(q,d) &= \textstyle\sum_{\beta \in \mathit{Act}} \mu_P(q,\beta) \cdot d(\beta) + \mu_P(q,\tau) \\ &= \textstyle\sum_{\beta \in \mathit{Act}} \mu_P(q,\beta) \cdot \mu_{T(s)}(t_0,\beta) + \mu_P(q,\tau) \\ &= \nu(q, t_0) \end{aligned}$$

∎

The next sublemma shows the correspondence between the functions $W_{\mathcal{P}} : P \times N \times P \times D_{\mathit{Act}} \to [0,1]$, and $\mathsf{Pr} : 2^{\mathsf{C}_{\mathcal{P}||\mathcal{T}}(P \times T)} \to [0,1]$. First we give a definition.

Definition A.4 *Let $\mathcal{P} = (P, \mathit{Act}, \mu_P, p_S)$, $s = \langle\, d, \alpha \,\rangle s'$, and $p, q \in P$. Then $W_{p,i,q,\mathcal{T}(s)}$, the set of all partial τ-computations of length i from $\langle\, p, t_0 \,\rangle$ to $\langle\, q, t_0 \,\rangle$ in $\mathcal{P}||\mathcal{T}(s)$, is defined as follows.*

$$W_{p,i,q,\mathcal{T}(s)} = \{c \in \mathsf{PC}_{\mathcal{P}||\mathcal{T}}(\langle\, p, t_0 \,\rangle) \mid c = (\langle\, p, t_0 \,\rangle = \langle\, p_0, t_0 \,\rangle) \xrightarrow{\tau, \pi_1} \cdots \xrightarrow{\tau, \pi_i} (\langle\, p_i, t_0 \,\rangle = \langle\, q, t_0 \,\rangle)\}$$

Note that $W_{p,i,q,\mathcal{T}(s)}$ is independent for any p, i, q and s. We now have the following.

Lemma A.5 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$, $s = \langle d, \alpha \rangle s'$, and $p, q \in P$. Then*

$$W_{\mathcal{P}}(p, i, q, d) = \mathsf{Pr}(W_{p,i,q,\mathcal{T}(s)}).$$

Proof: The proof is by induction on i.

(Base case): In this case $i = 0$. Then

$$W_{\mathcal{P}}(p, 0, q, d) = \begin{cases} 1 & \text{if } p = q \\ 0 & \text{otherwise} \end{cases}$$

while

$$\mathsf{Pr}(W_{p,0,q,\mathcal{T}(s)}) = \begin{cases} 1 & \text{if } p = q \text{ (since } W_{p,0,p,\mathcal{T}(s)} = \{\langle p, t_0 \rangle\} \text{ and } \mathsf{Pr}(\langle p, t_0 \rangle) = 1) \\ 0 & \text{otherwise (since } W_{p,0,q,\mathcal{T}(s)} = \emptyset) \end{cases}$$

(Induction step): Assume the result holds for k; we must show that it holds for $i = k + 1$. We need to consider the following two cases.

- $\nu(p, d) = 0$. By the definition of $W_{\mathcal{P}}$, $W_{\mathcal{P}}(p, k+1, q, d) = 0$, while $\mathsf{Pr}(W_{p,k+1,q,\mathcal{T}(s)}) = 0$ since $W_{p,k+1,q,\mathcal{T}(s)} = \emptyset$.
- $\nu(p, d) \neq 0$. In this case,

$$\begin{aligned}
& W_{\mathcal{P}}(p, k + 1, q, d) \\
= \ & \frac{1}{\nu(p, d)} \cdot \sum_{p' \in P} \mu_P(p, \tau, p') \cdot W_{\mathcal{P}}(p', k, q, d) \\
= \ & \frac{1}{\nu(p, t_0)} \cdot \sum_{p' \in P} \mu_P(p, \tau, p') \cdot \mathsf{Pr}(W_{p',k,q,\mathcal{T}(s)}) \qquad \text{(by Lemma A.3 and IH)} \\
= \ & \sum_{p' \in P} \frac{\mu_P(p, \tau, p')}{\nu(p, t_0)} \cdot \mathsf{Pr}(W_{p',k,q,\mathcal{T}(s)}) \\
= \ & \sum_{p' \in P} \mu_{\mathcal{P} \| \mathcal{T}(s)}(\langle p, t_0 \rangle, \tau, \langle p', t_0 \rangle) \cdot \mathsf{Pr}(W_{p',k,q,\mathcal{T}(s)}) \\
& \qquad \text{(by the definition of } \mu_{\mathcal{P} \| \mathcal{T}(s)}) \\
= \ & \sum_{p' \in P} \mathsf{Pr}(W_{p,1,p',\mathcal{T}(s)}) \cdot \mathsf{Pr}(W_{p',k,q,\mathcal{T}(s)}) \qquad \text{(by the definition of } W_{p,i,q,\mathcal{T}(s)}) \\
= \ & \mathsf{Pr}(W_{p,k+1,q,\mathcal{T}(s)}) \qquad \text{(by the definitions of } W_{p,i,q,\mathcal{T}(s)} \text{ and } \mathsf{Pr})
\end{aligned}$$

■

Lemma A.6 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$, $s = \langle d, \alpha \rangle s'$, and $p, q \in P$. Then*

$$W_{\mathcal{P},\varepsilon}(p, q, d) = \mathsf{Pr}(W_{p,q,\mathcal{T}(s)})$$

where $W_{p,q,\mathcal{T}(s)} = \bigcup_{i=0}^{\infty} W_{p,i,q,\mathcal{T}(s)}$.

Proof: This result follows directly from Lemma A.5 and the definitions of Pr and $W_{\mathcal{P},\varepsilon}$. Note that $W_{p,q,\mathcal{T}(s)}$ is independent for any p, q and s, since $\mathcal{P}$ is divergence-free. ■

The next lemma presents a recursive characterization for $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle p, t_0 \rangle))$ when s is of the form $s = \langle d, \alpha \rangle s'$.

Lemma A.7 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$, $s = \langle d, \alpha \rangle s'$, and t_0 be the start state of $\mathcal{T}(s)$, with t_1 the next state on the spine of $\mathcal{T}(s)$. Then for any $p \in P$*

$$\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle p, t_0 \rangle)) = \sum_{p' \in P} \sum_{\{q \in P | \nu(q,d) > 0\}} W_{\mathcal{P},\varepsilon}(p, q, d) \cdot \frac{d(\alpha)}{\nu(q, d)} \cdot \mu_P(q, \alpha, p') \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle)).$$

Proof:

$$\begin{aligned}
&\sum_{p' \in P} \sum_{\{q \in P | \nu(q,d) > 0\}} W_{\mathcal{P},\varepsilon}(p, q, d) \cdot \frac{d(\alpha)}{\nu(q, d)} \cdot \mu_P(q, \alpha, p') \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle)) \\
&= \sum_{p' \in P} \sum_{\{q \in P | \nu(q,t_0) > 0\}} \mathsf{Pr}(W_{p,q,\mathcal{T}(s)}) \cdot \frac{\mu_{T(s)}(t_0, \alpha, t_1) \cdot \mu_P(q, \alpha, p')}{\nu(q, t_0)} \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle)) \\
&\quad \text{(by Lemmas A.3 and A.6 and the definition of } \mathcal{T}(s)) \\
&= \sum_{p' \in P} \sum_{\{q \in P | \nu(q,t_0) > 0\}} \mathsf{Pr}(W_{p,q,\mathcal{T}(s)}) \cdot \mu_{\mathcal{P}\|\mathcal{T}(s)}(\langle q, t_0 \rangle, \alpha, \langle p', t_1 \rangle) \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle)) \\
&\quad \text{(by the definition of } \mu_{\mathcal{P}\|\mathcal{T}(s)}) \\
&= \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle p, t_0 \rangle)) \quad \text{(by the definition of } W_{p,q,\mathcal{T}(s)} \text{ and } \mathsf{Pr})
\end{aligned}$$

Here the subexpression $[\sum_{\{q \in P | \nu(q,t_0) > 0\}} \mathsf{Pr}(W_{p,q,\mathcal{T}(s)}) \cdot \mu_{\mathcal{P}\|\mathcal{T}(s)}(\langle q, t_0 \rangle, \alpha, \langle p', t_1 \rangle)]$ gives the probability that from configuration $\langle p, t_0 \rangle$ process $\mathcal{P}$ performs some internal transitions, reaches state $\langle q, t_0 \rangle$, and then synchronizes with test $\mathcal{T}(s)$ on action α to arrive at state $\langle p', t_1 \rangle$. In essence, this may be seen as a weak α transition from $\langle p, t_0 \rangle$ to $\langle p', t_1 \rangle$ in $\mathcal{P}\|\mathcal{T}(s)$ (note that throughout this weak transition, the interaction system stays in test states that are on the spine of $\mathcal{T}(s)$). ■

Finally, we prove the main result (Lemma 4.6) by induction on the length of s.

Proof:

(Base case): $s = \epsilon$

In this case, $\mathcal{T}(s)$ consists of a single (successful) state t_0 and no transitions. As $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(\epsilon)}(\langle p, t_0 \rangle)) = 1$ by the definition of Pr and $M_{\mathcal{P}}(p, \epsilon) = 1$ by the definition of $M_{\mathcal{P}}$, we have that $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle p, t_0 \rangle)) = M_{\mathcal{P}}(p, s)$.

(Induction step): $s = \langle d, \alpha \rangle s'$. Then

$$\begin{array}{ll} & \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle p, t_0 \rangle)) \\ = & \sum_{p' \in P} \sum_{\{q \in P | \nu(q,d) > 0\}} W_{\mathcal{P},\varepsilon}(p, q, d) \cdot \frac{d(\alpha)}{\nu(q,d)} \cdot \mu_P(q, \alpha, p') \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle)) \\ & \text{(by Lemma A.7)} \\ = & \sum_{p' \in P} \sum_{\{q \in P | \nu(q,d) > 0\}} W_{\mathcal{P},\varepsilon}(p, q, d) \cdot \frac{d(\alpha)}{\nu(q,d)} \cdot \mu_P(q, \alpha, p') \cdot M_{\mathcal{P}}(p', s') \quad \text{(by IH)} \\ = & \sum_{p' \in P} N_{\mathcal{P}}(p, \alpha, p', d) \cdot M_{\mathcal{P}}(p', s') \quad \text{(by the definition of } N_{\mathcal{P}}) \\ = & M_{\mathcal{P}}(p, s) \quad \text{(by the definition of } M_{\mathcal{P}}). \end{array}$$

■

Proof of Lemma 4.9

We again prove a stronger result: for any $p \in P$, $t \in T$ and $e = (t = t_0) \xrightarrow{\alpha_1, \pi_1} \cdots \xrightarrow{\alpha_n, \pi_n} t_n$, $\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p, t \rangle | e)) = v \cdot M_{\mathcal{P}}(p, s)$, where $s = tr(e)$ and $v = \prod_{1 \leq i \leq |e|} \frac{\mu_T(t_{i-1}, \alpha_i, t_i)}{\mu_T(t_{i-1}, \alpha_i)}$. The proof is by induction on $|e|$.

(Base case): $e = t$. The result follows from (the proof of) Lemma 2.8 and the fact that $\prod_{1 \leq i \leq 0} x_i = 1$ for any quantities x_i.

(Induction step): $e = (t = t_0) \xrightarrow{\alpha_1, \pi_1} e'$, where $e' = t_1 \xrightarrow{\alpha_2, \pi_2} \cdots \xrightarrow{\alpha_n, \pi_n} t_n$, $s' = tr(e')$ and $v' = \prod_{2 \leq i \leq n} \frac{\mu_T(t_{i-1}, \alpha_i, t_i)}{\mu_T(t_{i-1}, \alpha_i)}$. Also let $d_1 = \mu_T(t)$. We now have the following.

$$\begin{array}{ll} & \mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p, t \rangle | e)) \\ = & \sum_{p' \in P} \sum_{\{q \in P | \nu(q,d_1) > 0\}} W_{\mathcal{P},\varepsilon}(p, q, d_1) \cdot \frac{\pi_1}{\nu(q,d_1)} \cdot \mu_P(q, \alpha_1, p') \cdot \mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle p', t_1 \rangle | e')) \\ & \text{(follows from definition of } \mathsf{Pr}) \\ = & \sum_{p' \in P} \sum_{\{q \in P | \nu(q,d_1) > 0\}} W_{\mathcal{P},\varepsilon}(p, q, d_1) \cdot \frac{\pi_1}{d_1(\alpha_1)} \cdot \frac{d_1(\alpha_1)}{\nu(q,d_1)} \cdot \mu_P(q, \alpha_1, p') \cdot v' \cdot M_{\mathcal{P}}(p', s') \\ & \text{(by induction hypothesis)} \\ = & \frac{\pi_1}{d_1(\alpha_1)} \cdot v' \cdot \sum_{p' \in P} \sum_{\{q \in P | \nu(q,d_1) > 0\}} W_{\mathcal{P},\varepsilon}(p, q, d_1) \cdot \frac{d_1(\alpha_1)}{\nu(q,d_1)} \cdot \mu_P(q, \alpha_1, p') \cdot M_{\mathcal{P}}(p', s') \\ = & \frac{\mu_T(t_0, \alpha_1, t_1)}{\mu_T(t_0, \alpha_1)} \cdot v' \cdot \sum_{p' \in P} N_{\mathcal{P}}(p, \alpha_1, p', d_1) \cdot M_{\mathcal{P}}(p', s') \\ & \text{(by definition of } N_{\mathcal{P}}) \\ = & v \cdot M_{\mathcal{P}}(p, s) \quad \text{(by definition of } M_{\mathcal{P}} \text{ and } v) \end{array}$$

Proof of Lemma 4.19

We prove, by induction on the length of s, a stronger result, namely, that for all $p \in P$, $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle p, t_0 \rangle)) = M_{\tau,\mathcal{P}}(p, s)$ (recall that t_0 is the start state of $\mathcal{T}(s)$). Before proceeding with the proof, we state and prove a number of sublemmas. The first of these sublemmas shows the correspondence between the two normalization functions, namely, $\nu : P \times T \to [0, 1]$ (defined in Section 2.2), and $\nu : P \times D_{Act_\tau} \to [0, 1]$ (defined in Section 4.2.1).

Lemma A.8 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$, $s = \langle\, d, \alpha \,\rangle s'$, and $q \in P$. Then $\nu(q, d) = \nu(q, t_0)$, where t_0 is the start state of $\mathcal{T}(s)$.*

Proof:

$$\begin{aligned}
\nu(q,d) &= (\textstyle\sum_{\beta \in Act} \mu_P(q,\beta) \cdot d(\beta)) + \mu_P(q,\tau) + d(\tau) - \mu_P(q,\tau) \cdot d(\tau) \\
&= (\textstyle\sum_{\beta \in Act} \mu_P(q,\beta) \cdot \mu_{T(s)}(t_0,\beta)) + \mu_P(q,\tau) + \mu_{T(s)}(t_0,\tau) - \mu_P(q,\tau) \cdot \mu_{T(s)}(t_0,\tau) \\
&= \nu(q, t_0)
\end{aligned}$$

■

The next sublemma shows the correspondence between the functions $W_{\tau,\mathcal{P}} : P \times N \times P \times D_{Act_\tau} \to [0,1]$, and $\mathsf{Pr} : 2^{\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(P \times T)} \to [0,1]$. Note that $W_{p,i,q,\mathcal{T}(s)}$ is introduced in Definition A.4.

Lemma A.9 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$, $s = \langle\, d, \alpha \,\rangle s'$, and $p, q \in P$. Then*

$$W_{\tau,\mathcal{P}}(p, i, q, d) = \mathsf{Pr}(W_{p,i,q,\mathcal{T}(s)}).$$

Proof: The proof is by induction on i.

(Base case): $i = 0$. Then

$$W_{\tau,\mathcal{P}}(p,0,q,d) = \begin{cases} 1 & \text{if } p = q \\ 0 & \text{otherwise} \end{cases}$$

while

$$\mathsf{Pr}(W_{p,0,q,\mathcal{T}(s)}) = \begin{cases} 1 & \text{if } p = q \text{ (since } W_{p,0,p,\mathcal{T}(s)} = \{\langle\, p, t_0 \,\rangle\} \text{ and } \mathsf{Pr}(\langle\, p, t_0 \,\rangle) = 1) \\ 0 & \text{otherwise (since } W_{p,0,q,\mathcal{T}(s)} = \emptyset) \end{cases}$$

(Induction step): Assume the result holds for k; we must show that it holds for $i = k+1$. We need to consider the following two cases.

- $\nu(p,d) = 0$. Then by the definition of $W_{\tau,\mathcal{P}}$, $W_{\tau,\mathcal{P}}(p, k+1, q, d) = 0$, while $\mathsf{Pr}(W_{p,k+1,q,\mathcal{T}(s)}) = 0$ since $W_{p,k+1,q,\mathcal{T}(s)} = \emptyset$.
- $\nu(p,d) \neq 0$. In this case,

$$\begin{aligned}
&W_{\tau,\mathcal{P}}(p, k+1, q, d) \\
&= \frac{1 - d(\tau)}{\nu(p,d)} \cdot \sum_{p' \in P} \mu_P(p,\tau,p') \cdot W_{\tau,\mathcal{P}}(p', k, q, d) \\
&= \frac{1 - \mu_{T(s)}(t_0,\tau)}{\nu(p,t_0)} \cdot \sum_{p' \in P} \mu_P(p,\tau,p') \cdot \mathsf{Pr}(W_{p',k,q,\mathcal{T}(s)}) \qquad \text{(by Lemma A.8 and IH)} \\
&= \sum_{p' \in P} \frac{\mu_P(p,\tau,p') \cdot (1 - \mu_{T(s)}(t_0,\tau))}{\nu(p,t_0)} \cdot \mathsf{Pr}(W_{p',k,q,\mathcal{T}(s)}) \\
&= \sum_{p' \in P} \mu_{\mathcal{P}\|\mathcal{T}(s)}(\langle\, p, t_0 \,\rangle, \tau, \langle\, p', t_0 \,\rangle) \cdot \mathsf{Pr}(W_{p',k,q,\mathcal{T}(s)}) \qquad \text{(by the definition of } \mu_{\mathcal{P}\|\mathcal{T}(s)}) \\
&= \sum_{p' \in P} \mathsf{Pr}(W_{p,1,p',\mathcal{T}(s)}) \cdot \mathsf{Pr}(W_{p',k,q,\mathcal{T}(s)}) \qquad \text{(by the definition of } W_{p,i,q,\mathcal{T}(s)}) \\
&= \mathsf{Pr}(W_{p,k+1,q,\mathcal{T}(s)}) \qquad \text{(by the definitions of } W_{p,i,q,\mathcal{T}(s)} \text{ and } \mathsf{Pr})
\end{aligned}$$

$\blacksquare$

Lemma A.10 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$, $s = \langle d, \alpha \rangle s'$, and $p, q \in P$. Then*

$$W_{\tau,\mathcal{P},\varepsilon}(p, q, d) = \mathsf{Pr}(W_{p,q,\mathcal{T}(s)})$$

where $W_{p,q,\mathcal{T}(s)} = \bigcup_{i=0}^{\infty} W_{p,i,q,\mathcal{T}(s)}$.

Proof: This result follows directly from Lemma A.9 and the definitions of Pr and $W_{\tau,\mathcal{P},\varepsilon}$. $\blacksquare$

The next lemma presents a recursive characterization for $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle p, t_0 \rangle))$ when s is of the form $s = \langle d, \alpha \rangle s'$.

Lemma A.11 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$, $s = \langle d, \alpha \rangle s'$, and t_0 be the start state of $\mathcal{T}(s)$, with t_1 the next state on the spine of $\mathcal{T}(s)$. Then for any $p \in P$ we have the following.*

$$\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle p, t_0 \rangle)) =$$

$$\begin{cases} \sum_{p' \in P} \sum_{\{q \in P | \nu(q,d) > 0\}} W_{\tau,\mathcal{P},\varepsilon}(p, q, d) \cdot \frac{d(\alpha)}{\nu(q,d)} \cdot \mu_P(q, \alpha, p') \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle)) & \text{if } \alpha \neq \tau \\ \sum_{p' \in P} (\sum_{\{q \in P | \nu(q,d) > 0\}} W_{\tau,\mathcal{P},\varepsilon}(p, q, d) \cdot \frac{d(\tau)}{\nu(q,d)} \cdot \mu_P(q, \tau, p') \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle)) & \\ \quad + \sum_{\{ p' \in P | \nu(p',d) > 0 \}} W_{\tau,\mathcal{P},\varepsilon}(p, p', d) \cdot \frac{d(\tau)}{\nu(p',d)} \cdot (1 - \mu_P(p', \tau)) \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle))) & \text{if } \alpha = \tau \end{cases}$$

Proof: We need to consider the following two cases:

- $\alpha \neq \tau$. This case is similar to Lemma A.7 and is omitted.
- $\alpha = \tau$. In this case

$$\begin{aligned} & \sum_{p' \in P} (\sum_{\{q \in P | \nu(q,d) > 0\}} W_{\tau,\mathcal{P},\varepsilon}(p, q, d) \cdot \frac{d(\tau)}{\nu(q, d)} \cdot \mu_P(q, \tau, p') \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle)) \\ & \quad + \sum_{\{ p' \in P | \nu(p',d) > 0 \}} W_{\tau,\mathcal{P},\varepsilon}(p, p', d) \cdot \frac{d(\tau)}{\nu(p', d)} \cdot (1 - \mu_P(p', \tau)) \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle))) \\ = & \sum_{p' \in P} (\sum_{\{q \in P | \nu(q,t_0) > 0\}} \mathsf{Pr}(W_{p,q,\mathcal{T}(s)}) \cdot \frac{\mu_{\mathcal{T}(s)}(t_0, \tau, t_1) \cdot \mu_P(q, \tau, p')}{\nu(q, t_0)} \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle)) \\ & \quad + \sum_{\{ p' \in P | \nu(p',t_0) > 0 \}} \mathsf{Pr}(W_{p,p',\mathcal{T}(s)}) \cdot \frac{\mu_{\mathcal{T}(s)}(t_0, \tau, t_1) \cdot (1 - \mu_P(p', \tau))}{\nu(p', t_0)} \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle))) \\ & \quad \text{(by Lemmas A.8 and A.10, and the definition of } \mathcal{T}(s)) \\ = & \sum_{p' \in P} (\sum_{\{q \in P | \nu(q,t_0) > 0\}} \mathsf{Pr}(W_{p,q,\mathcal{T}(s)}) \cdot \mu_{\mathcal{P}\|\mathcal{T}(s)}(\langle q, t_0 \rangle, \tau, \langle p', t_1 \rangle) \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle p', t_1 \rangle) + \end{aligned}$$

$$\sum_{\{\,p'\in P|\nu(p',t_0)>0\,\}} \mathsf{Pr}(W_{p,p',\mathcal{T}(s)}) \cdot \mu_{\mathcal{P}\|\mathcal{T}(s)}(\langle\, p', t_0\,\rangle, \tau, \langle\, p', t_1\,\rangle) \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle\, p', t_1\,\rangle))))$$

(by the definition of $\mu_{\mathcal{P}\|\mathcal{T}(s)}$)

$$= \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle\, p, t_0\,\rangle)) \qquad \text{(by the definition of } W_{p,q,\mathcal{T}(s)} \text{ and } \mathsf{Pr})$$

The subexpression

$$[\sum_{\{q\in P|\nu(q,t_0)>0\}} \mathsf{Pr}(W_{p,q,\mathcal{T}(s)}) \cdot \mu_{\mathcal{P}\|\mathcal{T}(s)}(\langle\, q, t_0\,\rangle, \tau, \langle\, p', t_1\,\rangle)]$$

gives the probability that from configuration $\langle\, p, t_0\,\rangle$ process $\mathcal{P}$ performs some internal transitions, reaches state $\langle\, q, t_0\,\rangle$, and then synchronizes with test $\mathcal{T}(s)$ on a τ to arrive at state $\langle\, p', t_1\,\rangle$. Similarly, the subexpression

$$[\sum_{\{\,p'\in P|\nu(p',t_0)>0\,\}} \mathsf{Pr}(W_{p,p',\mathcal{T}(s)}) \cdot \mu_{\mathcal{P}\|\mathcal{T}(s)}(\langle\, p', t_0\,\rangle, \tau, \langle\, p', t_1\,\rangle)]$$

reflects the probability that from configuration $\langle\, p, t_0\,\rangle$ process $\mathcal{P}$ performs some internal transitions and reaches state $\langle\, p', t_0\,\rangle$, whence test $\mathcal{T}(s)$ performs a τ to arrive at state $\langle\, p', t_1\,\rangle$. The sum of these two subexpressions gives the probability of evolving from $\langle\, p, t_0\,\rangle$ to $\langle\, p', t_1\,\rangle$ in $\mathcal{P}\|\mathcal{T}(s)$ through a weak τ transition (note that throughout this weak transition, the interaction system stays in test states that are on the spine of $\mathcal{T}(s)$).

■

Finally, we prove the main result (Lemma 4.19) by induction on the length of s.

Proof:

(Base case): $s = \epsilon$

In this case, $\mathcal{T}(s)$ consists of a single (successful) state (t_0) and no transitions. As $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(\epsilon)}(\langle\, p, t_0\,\rangle)) = 1$ by the definition of Pr and $M_{\tau,\mathcal{P}}(p, \epsilon) = 1$ by the definition of $M_{\tau,\mathcal{P}}$, we have that $\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle\, p, t_0\,\rangle)) = M_{\tau,\mathcal{P}}(p, s)$.

(Induction step): $s = \langle\, d, \alpha\,\rangle s'$. We must consider the following two cases.

- $\alpha \neq \tau$. Then

$$\begin{aligned}
&\mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle\, p, t_0\,\rangle)) \\
=\;& \textstyle\sum_{p'\in P} \sum_{\{\,q\in P|\nu(q,d)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p, q, d) \cdot \frac{d(\alpha)}{\nu(q,d)} \cdot \mu_P(q, \alpha, p') \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle\, p', t_1\,\rangle)) \\
& \text{(by Lemma A.11)} \\
=\;& \textstyle\sum_{p'\in P} \sum_{\nu(q,d)>0} W_{\tau,\mathcal{P},\varepsilon}(p, q, d) \cdot \frac{d(\alpha)}{\nu(q,d)} \cdot \mu_P(q, \alpha, p') \cdot M_{\tau,\mathcal{P}}(p', s') \qquad \text{(by IH)} \\
=\;& \textstyle\sum_{p'\in P} N_{\tau,\mathcal{P}}(p, \alpha, p', d) \cdot M_{\tau,\mathcal{P}}(p', s') \qquad \text{(by the definition of } N_{\tau,\mathcal{P}}) \\
=\;& M_{\tau,\mathcal{P}}(p, s) \qquad \text{(by the definition of } M_{\tau,\mathcal{P}}).
\end{aligned}$$

- $\alpha = \tau$. Then

$$
\begin{array}{ll}
& \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s)}(\langle\, p, t_0\,\rangle)) \\
= & \sum_{p' \in P}(\sum_{\{\, q \in P | \nu(q,d)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,q,d) \cdot \frac{d(\tau)}{\nu(q,d)} \cdot \mu_P(q,\tau,p') \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle\, p', t_1\,\rangle)) \\
& \qquad + \sum_{\{\, p' \in P | \nu(p',d)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,p',d) \cdot \frac{d(\tau)}{\nu(p',d)} \cdot (1-\mu_P(p',\tau)) \cdot \mathsf{Pr}(\mathsf{S}_{\mathcal{P}\|\mathcal{T}(s')}(\langle\, p', t_1\,\rangle))) \\
& \quad \text{(by Lemma A.11)} \\
= & \sum_{p' \in P}(\sum_{\{\, q \in P | \nu(q,d)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,q,d) \cdot \frac{d(\tau)}{\nu(q,d)} \cdot \mu_P(q,\tau,p') \cdot M_{\tau,\mathcal{P}}(p',s') \\
& \qquad + \sum_{\{\, p' \in P | \nu(p',d)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,p',d) \cdot \frac{d(\tau)}{\nu(p',d)} \cdot (1-\mu_P(p',\tau)) \cdot M_{\tau,\mathcal{P}}(p',s')) \quad \text{(by IH)} \\
= & \sum_{p' \in P} N_{\tau,\mathcal{P}}(p,\tau,p',d) \cdot M_{\tau,\mathcal{P}}(p',s') \quad \text{(by the definition of } N_{\tau,\mathcal{P}}) \\
= & M_{\tau,\mathcal{P}}(p,s) \quad \text{(by the definition of } M_{\tau,\mathcal{P}}).
\end{array}
$$

■

Proof of Lemma 4.22

As in Lemma 4.9, we prove that $\mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle\, p,t\,\rangle|e)) = v \cdot M_{\tau,\mathcal{P}}(p,s)$ for all $p \in P$ and $t \in T$ where P is the set of states of $\mathcal{P}$, T is the set of states of $\mathcal{T}$, e has the form $t = t_0 \xrightarrow{\alpha_1,\pi_1} \cdots \xrightarrow{\alpha_n,\pi_n} t_n$, and $v = \prod_{1 \le i \le |e|} \frac{\mu_T(t_{i-1},\alpha_i,t_i)}{\mu_T(t_{i-1},\alpha_i)}$ where $\alpha_i = \lambda(s,i)$. We prove this fact by induction on $|e|$. The proof of the base case follows exactly the same lines as the proof of Lemma 4.9 and is omitted. In addition, if the label of the first transition of e is not τ, the proof is the same as the proof of Lemma 4.9. Here we just show the case of τ. Let $d_1 = \mu_T(t)$.

(Induction step): Let $e = (t = t_0) \xrightarrow{\alpha_1,\pi_1} e'$ where $\alpha_1 = \tau$ and $e' = t_1 \xrightarrow{\alpha_2,\pi_2} \cdots \xrightarrow{\alpha_n,\pi_n} t_n$. Also let $s' = tr(e')$ and $v' = \prod_{2 \le i \le |e|} \frac{\mu_T(t_{i-1},\alpha_i,t_i)}{\mu_T(t_{i-1},\alpha_i)}$.

$$
\begin{array}{ll}
& \mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle\, p,t\,\rangle|e)) \\
= & \sum_{p' \in P}(\sum_{\{\, q \in P | \nu(q,d_1)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,q,d_1) \cdot \frac{\pi_1}{\nu(q,d_1)} \cdot \mu_P(q,\tau,p') \cdot \mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle\, p',t_1\,\rangle|e')) \\
& + \sum_{\{\, p' \in P | \nu(p',d_1)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,p',d_1) \cdot \frac{\pi_1}{\nu(p',d_1)} \cdot (1-\mu_P(p',\tau)) \cdot \mathsf{Pr}(\mathsf{C}_{\mathcal{P}\|\mathcal{T}}(\langle\, p',t_1\,\rangle|e'))) \\
= & \sum_{p' \in P}(\sum_{\{\, q \in P | \nu(q,d_1)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,q,d_1) \cdot \frac{\pi_1}{\nu(q,d_1)} \cdot \mu_P(q,\tau,p') \cdot v' \cdot M_{\tau,\mathcal{P}}(p',s') \\
& + \sum_{\{\, p' \in P | \nu(p',d_1)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,p',d_1) \cdot \frac{\pi_1}{\nu(p',d_1)} \cdot (1-\mu_P(p',\tau)) \cdot v' \cdot M_{\tau,\mathcal{P}}(p',s')) \quad \text{(by IH)} \\
= & \sum_{p' \in P}(\sum_{\{\, q \in P | \nu(q,d_1)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,q,d_1) \cdot \frac{\pi_1}{d_1(\tau)} \cdot \frac{d_1(\tau)}{\nu(q,d_1)} \cdot \mu_P(q,\tau,p') \cdot v' \cdot M_{\tau,\mathcal{P}}(p',s') \\
& + \sum_{\{\, p' \in P | \nu(p',d_1)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,p',d_1) \cdot \frac{\pi_1}{d_1(\tau)} \cdot \frac{d_1(\tau)}{\nu(p',d_1)} \cdot (1-\mu_P(p',\tau)) \cdot v' \cdot M_{\tau,\mathcal{P}}(p',s')) \\
= & \frac{\pi_1}{d_1(\tau)} \cdot \sum_{p' \in P}(\sum_{\{\, q \in P | \nu(q,d_1)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,q,d_1) \cdot \frac{d_1(\tau)}{\nu(q,d_1)} \cdot \mu_P(q,\tau,p') \cdot v' \cdot M_{\tau,\mathcal{P}}(p',s') \\
& + \sum_{\{\, p' \in P | \nu(p',d_1)>0\,\}} W_{\tau,\mathcal{P},\varepsilon}(p,p',d_1) \cdot \frac{d_1(\tau)}{\nu(p',d_1)} \cdot (1-\mu_P(p',\tau)) \cdot v' \cdot M_{\tau,\mathcal{P}}(p',s')) \\
= & \frac{\mu_T(t,\tau,t_1)}{\mu_T(t,\tau)} \cdot v' \cdot \sum_{p' \in P} N_{\tau,\mathcal{P}}(p,\tau,p',d_1) \cdot M_{\tau,\mathcal{P}}(p',s') \\
= & \prod_{1 \le i \le |e|} \frac{\mu_T(t_{i-1},\alpha_i,t_i)}{\mu_T(t_{i-1},\alpha_i)} \cdot M_{\tau,\mathcal{P}}(p,s)
\end{array}
$$

Proof of Lemma 4.27

We prove the contrapositive of this statement, namely, that $\mathcal{P} \not\ll \mathcal{Q}$ implies $\mathcal{P} \not\ll^{NB} Q$. Suppose $\mathcal{P} \not\ll \mathcal{Q}$. Then there exists a probabilistic trace s such that $M_{\tau,\mathcal{P}}(p_S,s) > M_{\tau,\mathcal{Q}}(q_S,s)$.

If s is non-blocking, then it follows directly that $\mathcal{P} \not\ll^{NB} \mathcal{Q}$. If s is blocking, we show how to construct a non-blocking probabilistic trace s' such that $M_{\tau,\mathcal{P}}(p_S, s') > M_{\tau,\mathcal{Q}}(q_S, s')$ to show that $\mathcal{P} \not\ll^{NB} \mathcal{Q}$. We first give some definitions that will be used in the proof.

Definition A.12 *Given a probabilistic trace s, let $s(\pi)$ be the probabilistic trace such that $\lambda(s(\pi)) = \lambda(s)$ and*

$$\delta(s(\pi), i)(\alpha) = \begin{cases} \delta(s,i)(\alpha) & \text{if } \delta(s,i)(\tau) \neq 0 \\ (1-\pi)\cdot\delta(s,i)(\alpha) & \text{if } \delta(s,i)(\tau) = 0 \text{ and } \alpha \neq \tau \\ \pi & \text{if } \delta(s,i)(\tau) = 0 \text{ and } \alpha = \tau \end{cases}$$

where π is in the interval $[0,1]$.

$s(\pi)$ is the probabilistic trace obtained by attaching a τ-transition with non-zero probability π if $\delta(s,i)(\tau) = 0$. The probabilities of transitions other than τ are factored by $(1-\pi)$. Clearly, $s(0) = s$, and if $\pi \neq 0$, $s(\pi)$ is non-blocking.

Definition A.13 *Let $d \in D_{Act_\tau}$, $\pi \in [0,1]$. Then $d(\pi)$ is the probability distribution over Act_τ defined as:*

$$d(\pi)(\alpha) = \begin{cases} d(\alpha) & \text{if } d(\tau) \neq 0 \\ (1-\pi)\cdot d(\alpha) & \text{if } d(\tau) = 0 \text{ and } \alpha \neq \tau \\ \pi & \text{if } d(\tau) = 0 \text{ and } \alpha = \tau \end{cases}$$

Definition A.14 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$, $s \in Tr_{Act_\tau}$, $p \in P$, and $\pi \in [0,1]$. Then $f_{\mathcal{P},p,s}(\pi) : [0,1] \to [0,1]$ is defined as follows.*

$$f_{\mathcal{P},p,s}(\pi) = M_{\tau,\mathcal{P}}(p, s(\pi)).$$

We now have the following.

Lemma A.15 *Let $\mathcal{P} = (P, Act, \mu_P, p_S)$, $p \in P$, and $s \in Tr_{Act_\tau}$. Then $f_{\mathcal{P},p,s}(\pi)$ is continuous for $0 \leq \pi \leq 1$.*

Proof: First we state the following facts. Assume that $\mathcal{P} = (P, Act, \mu_P, p_S)$ is given.

1. For a given $d \in D_{Act_\tau}$ and $\alpha \in Act_\tau$, $d(\pi)(\alpha)$ interpreted as a function of π is continuous over $[0,1]$.
   This fact follows directly from Definition A.13.

2. For any $p \in P$ and $d \in D_{Act_\tau}$, $\nu(p, d(\pi))$ interpreted as a function of π is continuous over $[0,1]$.
   This fact follows from the definitions of $d(\pi)$ and ν and the continuity of $+, -$ and $\cdot$.

3. For any $p, p' \in P$, $i \in N$, and $d \in D_{Act_\tau}$, $W_{\tau,\mathcal{P}}(p, i, p', d(\pi))$ interpreted as a function of π is continuous over $[0, 1]$.
   This fact follows from the definitions of $d(\pi)$ and $W_{\tau,\mathcal{P}}(p, i, p', d)$.

4. For any $p, p' \in P$ and $d \in D_{Act_\tau}$, $W_{\tau,\mathcal{P},\varepsilon}(p, p', d(\pi))$ interpreted as a function of π is continuous over $[0, 1]$.
   This fact follows directly from the previous fact.

5. For any $p, p' \in P$, $\alpha \in Act_\tau$, and $d \in D_{Act_\tau}$, $N_{\tau,\mathcal{P}}(p, \alpha, p', d(\pi))$ interpreted as a function of π is continuous over $[0, 1]$.
   This fact follows from the definition of $N_{\tau,\mathcal{P}}(p, \alpha, p', d(\pi))$.

Now we prove the claim by induction on the length of s.

(Base case): $s = \epsilon$.
In this case, $f_{\mathcal{P},p,s}(\pi) = M_{\tau,\mathcal{P}}(p, \epsilon)$ since $\epsilon(\pi) = \epsilon$; moreover, $M_{\tau,\mathcal{P}}(p, \epsilon) = 1$ by the definition of $M_{\tau,\mathcal{P}}(p, s)$. Therefore $f_{\mathcal{P},p,s}(\pi)$ is continuous.

(Induction step): $s = \langle\, d, \alpha \,\rangle s'$.
First note that if $s = \langle\, d, \alpha \,\rangle s'$, then $s(\pi) = \langle\, d(\pi), \alpha \,\rangle s'(\pi)$.
In this case, $f_{\mathcal{P},p,s}(\pi) = M_{\tau,\mathcal{P}}(p, s(\pi)) = \sum_{p' \in P} N_{\tau,\mathcal{P}}(p, \alpha, p', d(\pi)) \cdot M_{\tau,\mathcal{P}}(p', s'(\pi))$.
For any p', $f_{\mathcal{P},p',s'}(\pi) = M_{\tau,\mathcal{P}}(p', s'(\pi))$ is continuous over $[0, 1]$ by the induction hypothesis, and $N_{\tau,\mathcal{P}}(p, \alpha, p', d(\pi))$ is continuous over $[0, 1]$ by fact 5. The desired result now follows.

■

Using this result we can prove the main lemma. Let s be a blocking probabilistic trace such that $M_{\tau,\mathcal{P}}(p, s) > M_{\tau,\mathcal{Q}}(q, s)$. This implies $M_{\tau,\mathcal{P}}(p, s) - M_{\tau,\mathcal{Q}}(q, s) > 0$. At $\pi = 0$,

$$M_{\tau,\mathcal{P}}(p, s(\pi)) - M_{\tau,\mathcal{Q}}(q, s(\pi)) = M_{\tau,\mathcal{P}}(p, s) - M_{\tau,\mathcal{Q}}(q, s)$$

so

$$M_{\tau,\mathcal{P}}(p, s(0)) - M_{\tau,\mathcal{Q}}(q, s(0)) > 0$$

Since $f_{\mathcal{P},p,s}$ and $f_{\mathcal{Q},q,s}$ are continuous over $[0, 1]$, so is

$$(f_{\mathcal{P},p,s} - f_{\mathcal{Q},q,s})(\pi) = M_{\tau,\mathcal{P}}(p, s(\pi)) - M_{\tau,\mathcal{Q}}(q, s(\pi)).$$

So there must be a π_0 in the interval $(0, 1]$ such that $M_{\tau,\mathcal{P}}(p, s(\pi_0)) - M_{\tau,\mathcal{Q}}(q, s(\pi_0)) > 0$, and this implies there is a non-blocking probabilistic trace s' $(= s(\pi_0))$ for which $M_{\tau,\mathcal{P}}(p_S, s') > M_{\tau,\mathcal{Q}}(q_S, s')$. Therefore $\mathcal{P} \not\ll^{NB} Q$.

Proof of Lemma 4.30

We prove a slightly stronger statement: for any non-blocking probabilistic trace s, $M_{\tau,\mathcal{P}}(p, s) + \Sigma_{s' \in s^{-1}} M_{\tau,\mathcal{P}}(p, s') = 1$ for all $\mathcal{P}$ and $p \in P$.

We begin by establishing the following.

Lemma A.16 *Let $d \in D_{Act_\tau}$ be such that $d(\tau) > 0$. Then for any $p \in P$,*

$$\Sigma_{\alpha \in Act} \Sigma_{p' \in P} N_{\tau,\mathcal{P}}(p, \alpha, p', d) + \Sigma_{p' \in P} N_{\tau,\mathcal{P}}(p, \tau, p', d) = 1.$$

Proof: First note that $\nu(p,d) \neq 0$ if $d(\tau) > 0$. For $p \in P$, let $\tau(p)$ be recursively defined as follows:

$$\tau(p) = \begin{cases} 0 & \text{if } \mu_P(p,\tau) = 0 \\ max\{\tau(p') \mid \mu_P(p,\tau,p') > 0\} + 1 & \text{otherwise} \end{cases}$$

$\tau(p)$ represents the length of the maximal sequence of τ-transitions from p. Since $\mathcal{P}$ is divergence-free, $\tau(p)$ is defined for all $p \in P$. From the definition of $W_{\tau,\mathcal{P},\varepsilon}$,

$$\tau(p) = n \text{ implies } W_{\tau,\mathcal{P},\varepsilon}(p,q,d) = \Sigma_{i=0}^{n} W_{\tau,\mathcal{P}}(p,i,q,d) \qquad (\dagger)$$

The proof follows by induction on $\tau(p)$.

(Base case): $\tau(p) = 0$.

Here $\mu_P(p,\tau) = 0$, and thus for $\alpha \neq \tau$,

$$\begin{aligned} \Sigma_{p' \in P} N_{\tau,\mathcal{P}}(p,\alpha,p',d) &= \Sigma_{p' \in P} \frac{d(\alpha)}{\nu(p,d)} \cdot \mu_P(p,\alpha,p') \\ &\qquad \text{(by definition of } N_{\tau,\mathcal{P}}\text{, since } \mu_P(p,\tau) = 0) \\ &= \frac{d(\alpha)}{\nu(p,d)} \cdot \mu_P(p,\alpha) \end{aligned}$$

Moreover, since $\mu_P(p,\tau) = 0$ we know that $\Sigma_{p' \in P} N_{\tau,\mathcal{P}}(p,\tau,p',d) = \frac{d(\tau)}{\nu(p,d)}$. We may now derive the following.

$$\begin{aligned} &\Sigma_{\alpha \in Act} \Sigma_{p' \in P} N_{\tau,\mathcal{P}}(p,\alpha,p',d) + \Sigma_{p' \in P} N_{\tau,\mathcal{P}}(p,\tau,p',d) \\ &= \Sigma_{\alpha \in Act} \frac{d(\alpha) \cdot \mu_P(p,\alpha)}{\nu(p,d)} + \frac{d(\tau)}{\nu(p,d)} \\ &= 1 \quad \text{(by definition of } \nu(p,d)\text{, since } \mu(p,\tau) = 0) \end{aligned}$$

(Induction step): The induction hypothesis states that the result holds for p such that $\tau(p) = n$; we must prove it for $p \in P$ such that $\tau(p) = n+1$. To do so, we show that $\Sigma_{p' \in P} N_{\tau,\mathcal{P}}(p,\alpha,p',d)$ may be expressed in terms of $N_{\tau,\mathcal{P}}(q,\alpha,p',d)$, where q is a state such that $\mu_P(p,\tau,q) > 0$ and hence $\tau(q) \leq n$.

When $\alpha \neq \tau$, we have the following.

$$\begin{aligned} &N_{\tau,\mathcal{P}}(p,\alpha,p',d) \\ &= \Sigma_{q \in P} W_{\tau,\mathcal{P},\varepsilon}(p,q,d) \cdot \frac{d(\alpha)}{\nu(q,d)} \cdot \mu_P(q,\alpha,p') \quad \text{(definition of } N_{\tau,\mathcal{P}}) \end{aligned}$$

$$
\begin{aligned}
&= \Sigma_{i=0}^{n+1}\Sigma_{q\in P}W_{\tau,\mathcal{P}}(p,i,q,d)\cdot\frac{d(\alpha)}{\nu(q,d)}\cdot\mu_P(q,\alpha,p') \quad \text{by } (\dagger)\\
&= \Sigma_{q\in P}W_{\tau,\mathcal{P}}(p,0,q,d)\cdot\frac{d(\alpha)}{\nu(q,d)}\cdot\mu_P(q,\alpha,p')\\
&\quad +\Sigma_{i=0}^{n}\Sigma_{q\in P}W_{\tau,\mathcal{P}}(p,i+1,q,d)\cdot\frac{d(\alpha)}{\nu(q,d)}\cdot\mu_P(q,\alpha,p')\\
&= \frac{d(\alpha)}{\nu(p,d)}\cdot\mu_P(p,\alpha,p')\\
&\quad +\frac{1-d(\tau)}{\nu(p,d)}\Sigma_{q'\in P}\mu_P(p,\tau,q')\Sigma_{q\in P}\Sigma_{i=0}^{n}W_{\tau,\mathcal{P}}(q',i,q,d)\cdot\frac{d(\alpha)}{\nu(q,d)}\cdot\mu_P(q,\alpha,p')\\
&\quad\quad \text{(by definition of } W_{\tau,\mathcal{P}})\\
&= \frac{d(\alpha)}{\nu(p,d)}\cdot\mu_P(p,\alpha,p')\\
&\quad +\frac{1-d(\tau)}{\nu(p,d)}\Sigma_{q'\in P}\mu_P(p,\tau,q')\Sigma_{q\in P}W_{\tau,\mathcal{P},\varepsilon}(q',q,d)\cdot\frac{d(\alpha)}{\nu(q,d)}\cdot\mu_P(q,\alpha,p') \qquad (1)\\
&\quad\quad \text{(by definition of } W_{\tau,\mathcal{P}} \text{ and } \dagger)
\end{aligned}
$$

We now use (1) to calculate $\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\alpha,p',d)$ as follows.

$$
\begin{aligned}
&\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\alpha,p',d)\\
&= \frac{d(\alpha)}{\nu(p,d)}\cdot\mu_P(p,\alpha)\\
&\quad +\frac{1-d(\tau)}{\nu(p,d)}\Sigma_{q'\in P}\mu_P(p,\tau,q')\Sigma_{p'\in P}\Sigma_{q\in P}W_{\tau,\mathcal{P},\varepsilon}(q',q,d)\cdot\frac{d(\alpha)}{\nu(q,d)}\cdot\mu_P(q,\alpha,p')\\
&= \frac{d(\alpha)\cdot\mu_P(p,\alpha)}{\nu(p,d)}+\frac{1-d(\tau)}{\nu(p,d)}\Sigma_{q\in P}\mu_P(p,\tau,q)\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(q,\alpha,p',d) \qquad (2)\\
&\quad\quad \text{(by definition of } N_{\tau,\mathcal{P}})
\end{aligned}
$$

For τ, we get the following.

$$
\begin{aligned}
&N_{\tau,\mathcal{P}}(p,\tau,p',d)\\
&= \Sigma_{q\in P}W_{\tau,\mathcal{P},\varepsilon}(p,q,d)\cdot\frac{d(\tau)}{\nu(q,d)}\cdot\mu_P(q,\tau,p')+W_{\tau,\mathcal{P},\varepsilon}(p,p',d)\cdot\frac{d(\tau)}{\nu(p',d)}\cdot(1-\mu_P(p',\tau))\\
&\quad\quad \text{(by definition of } N_{\tau,\mathcal{P}})\\
&= \frac{d(\tau)}{\nu(p,d)}\cdot\mu_P(p,\tau,p')\\
&\quad +\frac{1-d(\tau)}{\nu(p,d)}\Sigma_{q\in P}\mu_P(p,\tau,q)\Sigma_{q'\in P}\Sigma_{i=0}^{n}W_{\tau,\mathcal{P}}(q,i,q',d)\cdot\frac{d(\tau)}{\nu(q',d)}\cdot\mu_P(q',\tau,p')\\
&\quad +W_{\tau,\mathcal{P},\varepsilon}(p,p',d)\cdot\frac{d(\tau)}{\nu(p',d)}\cdot(1-\mu_P(p',\tau))
\end{aligned}
$$

(by definition of $W_{\tau,\mathcal{P},\epsilon}$ and $\dagger$)

$$
\begin{aligned}
= \ & \frac{d(\tau)}{\nu(p,d)} \cdot \mu_P(p,\tau,p') \\
& + \frac{1-d(\tau)}{\nu(p,d)} \Sigma_{q\in P}\mu_P(p,\tau,q)\Sigma_{q'\in P}W_{\tau,\mathcal{P},\varepsilon}(q,q',d) \cdot \frac{d(\tau)}{\nu(q',d)} \cdot \mu_P(q',\tau,p') \\
& + W_{\tau,\mathcal{P},\varepsilon}(p,p',d) \cdot \frac{d(\tau)}{\nu(p',d)} \cdot (1-\mu_P(p',\tau)) \qquad (3)
\end{aligned}
$$

(by definition of $W_{\tau,\mathcal{P},\epsilon}$ and $\dagger$)

We now use (3) to calculate $\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\tau,p',d)$ as follows.

$$
\begin{aligned}
& \Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\tau,p',d) \\
= \ & \frac{d(\tau)\cdot\mu_P(p,\tau)}{\nu(p,d)} \\
& + \frac{1-d(\tau)}{\nu(p,d)} \Sigma_{q\in P}\mu_P(p,\tau,q)\Sigma_{p'\in P}\Sigma_{q'\in P}\Sigma_{i=0}^{n}W_{\tau,\mathcal{P}}(q,i,q',d) \cdot \frac{d(\tau)}{\nu(q',d)} \cdot \mu_P(q',\tau,p') \\
& + \frac{d(\tau)}{\nu(p,d)}(1-\mu_P(p,\tau)) \\
& + \frac{1-d(\tau)}{\nu(p,d)} \Sigma_{q\in P}\mu_P(p,\tau,q)\Sigma_{p'\in P}\Sigma_{i=0}^{n}W_{\tau,\mathcal{P}}(q,i,p',d) \cdot \frac{d(\tau)}{\nu(p',d)} \cdot (1-\mu_P(p',\tau)) \\
= \ & \frac{d(\tau)\cdot\mu_P(p,\tau)}{\nu(p,d)} + \frac{d(\tau)}{\nu(p,d)}(1-\mu_P(p,\tau)) \\
& \frac{1-d(\tau)}{\nu(p,d)} \Sigma_{q\in P}\mu_P(p,\tau,q)\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(q,\tau,p',d) \qquad (4)
\end{aligned}
$$

(by $\dagger$ and definition of $N_{\tau,\mathcal{P}}$)

Adding (2) and (4), we obtain the following.

$$
\begin{aligned}
& \Sigma_{\alpha\in Act}\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\alpha,p',d) + \Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\tau,p',d) \\
= \ & \Sigma_{\alpha\in Act}\frac{d(\alpha)\cdot\mu_P(p,\alpha)}{\nu(p,d)} \\
& + \frac{1-d(\tau)}{\nu(p,d)} \Sigma_{q\in P}\mu_P(p,\tau,q)\Sigma_{\alpha\in Act}\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(q,\alpha,p',d) \\
& + \frac{d(\tau)\cdot\mu_P(p,\tau)}{\nu(p,d)} \\
& + \frac{d(\tau)}{\nu(p,d)}(1-\mu_P(p,\tau)) \\
& + \frac{1-d(\tau)}{\nu(p,d)} \Sigma_{q\in P}\mu_P(p,\tau,q)\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(q,\tau,p',d) \\
= \ & \Sigma_{\alpha\in Act}\frac{d(\alpha)\cdot\mu_P(p,\alpha)}{\nu(p,d)} + \frac{d(\tau)}{\nu(p,d)}(1-\mu_P(p,\tau)) + \frac{d(\tau)\cdot\mu_P(p,\tau)}{\nu(p,d)}
\end{aligned}
$$

$$+\frac{1-d(\tau)}{\nu(p,d)}\Sigma_{q\in P}\mu_P(p,\tau,q)(\Sigma_{\alpha\in Act}\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(q,\alpha,p',d)+\Sigma_{q'\in P}N_{\tau,\mathcal{P}}(q,\tau,q',d))$$

Since $\tau(q)\leq n$ for all q such that $\mu(p,\tau,q)>0$, the induction hypothesis guarantees that

$$\Sigma_{\alpha\in Act}\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(q,\alpha,p',d)+\Sigma_{q'\in P}N_{\tau,\mathcal{P}}(q,\tau,q',d)=1.$$

Therefore, by the definition of $\nu(p,d)$,

$$\begin{aligned}
&\Sigma_{\alpha\in Act}\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\alpha,p',d)+\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\tau,p',d)\\
&= \Sigma_{\alpha\in Act}\frac{d(\alpha)\cdot\mu_P(p,\alpha)}{\nu(p,d)}+\frac{d(\tau)\cdot\mu_P(p,\tau)}{\nu(p,d)}+\frac{d(\tau)}{\nu(p,d)}(1-\mu_P(p,\tau))+\frac{1-d(\tau)}{\nu(p,d)}\cdot\mu_P(p,\tau)\\
&= 1.
\end{aligned}$$

■

We now turn to the proof that $M_{\tau,\mathcal{P}}(p,s)+\Sigma_{s'\in s^{-1}}M_{\tau,\mathcal{P}}(p,s')=1$.

(Base case): $s=\epsilon$

Since $s^{-1}=\emptyset$,

$M_{\tau,\mathcal{P}}(p,\epsilon)+\Sigma_{s'\in\epsilon^{-1}}M_{\tau,\mathcal{P}}(p,s')=M_{\tau,\mathcal{P}}(p,\epsilon)=1$

(Induction step): Let $s=\langle d,\alpha\rangle s'$. Then, since $s^{-1}=\{\langle d,\beta\rangle|\beta\neq\alpha,d(\beta)>0\}\cup\{\langle d,\alpha\rangle s''|s''\in s'^{-1}\}$, we have the following.

$$\begin{aligned}
&M_{\tau,\mathcal{P}}(p,\langle d,\alpha\rangle s')+\Sigma_{u\in s'^{-1}}M_{\tau,\mathcal{P}}(p,u)\\
&= M_{\tau,\mathcal{P}}(p,\langle d,\alpha\rangle s')+\Sigma_{\beta\in Act_\tau-\{\alpha\}}M_{\tau,\mathcal{P}}(p,\langle d,\beta\rangle)+\Sigma_{s''\in s'^{-1}}M_{\tau,\mathcal{P}}(p,\langle d,\alpha\rangle s'') \qquad (5)
\end{aligned}$$

The sum of the first term and the third terms on the right-hand side of (5) may be rewritten as follows.

$$\begin{aligned}
&M_{\tau,\mathcal{P}}(p,\langle d,\alpha\rangle s')+\Sigma_{s''\in s'^{-1}}M_{\tau,\mathcal{P}}(p,\langle d,\alpha\rangle s'')\\
&= \Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\alpha,p',d)\cdot M_{\tau,\mathcal{P}}(p',s')\\
&\quad+\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\alpha,p',d)\cdot\Sigma_{s''\in s'^{-1}}M_{\tau,\mathcal{P}}(p',s'')\\
&\qquad\text{(by the definition of } M_{\tau,\mathcal{P}})\\
&= \Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\alpha,p',d)(M_{\tau,\mathcal{P}}(p',s')+\Sigma_{s''\in s'^{-1}}M_{\tau,\mathcal{P}}(p',s''))\\
&= \Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\alpha,p',d)\\
&\qquad\text{(by the IH)}
\end{aligned}$$

From the definition of $M_{\tau,\mathcal{P}}$ we know that

$$\Sigma_{\beta\in Act_\tau-\{\alpha\}}M_{\tau,\mathcal{P}}(p,\langle d,\beta\rangle) = \Sigma_{\beta\in Act_\tau-\{\alpha\}}\Sigma_{p'\in P}N_{\tau,\mathcal{P}}(p,\beta,p',d).$$

Therefore, we may derive the following.

$$\begin{aligned}
&M_{\tau,\mathcal{P}}(p,\langle\, d,\alpha\,\rangle s') + \Sigma_{\beta\in Act_\tau-\{\alpha\}} M_{\tau,\mathcal{P}}(p,\langle\, d,\beta\,\rangle) + \Sigma_{s''\in s'^{-1}} M_{\tau,\mathcal{P}}(p,\langle\, d,\alpha\,\rangle s'')\\
&= \Sigma_{p'\in P} N_{\tau,\mathcal{P}}(p,\alpha,p',d) + \Sigma_{\beta\in Act_\tau-\{\alpha\}} \Sigma_{p'\in P} N_{\tau,\mathcal{P}}(p,\beta,p',d)\\
&= 1\\
&\qquad \text{(by Lemma A.16)}
\end{aligned}$$

Example 4.37

To simplify notation, we write $V_i(\alpha)$ for $\frac{d_i(\alpha)}{d_i(\alpha)+d_i(\tau)}$ and $U_{i,j}(\alpha)$ for $\prod_{i<k\leq j}\frac{d_k(\tau)}{d_k(\alpha)+d_k(\tau)}$. Intuitively $V_i(\alpha)$ is the probability of the environment participating in an α-transition from configuration $\langle\, p,t_i\,\rangle$, and $U_{i,j}(\alpha)$ is the probability of evolving from $\langle\, p,t_i\,\rangle$ to $\langle\, p,t_j\,\rangle$ via τ-transitions where α is the only action the process can execute.

(Case 1) $\widehat{\lambda(s)} = \varepsilon$
Let $s = \langle\, d_1,\tau\,\rangle\cdots\langle\, d_i,\tau\,\rangle$. Then, $M_{\tau,\mathcal{P}_3}(p_S,s) = M_{\tau,\mathcal{Q}_3}(q_S,s) = U_{0,i}(a)$

(Case 2) $\widehat{\lambda(s)} = a$
Let $s = \langle\, d_1,\tau\,\rangle\cdots\langle\, d_i,\tau\,\rangle\langle\, d_{i+1},a\,\rangle s_1$, and $s_1 = \langle\, d_{i+2},\tau\,\rangle\cdots\langle\, d_{i+j+1},\tau\,\rangle$

$$\begin{aligned}
M_{\tau,\mathcal{P}_3}(p_S,s) &= U_{0,i}(a)\cdot(\tfrac{1}{2}\cdot V_{i+1}(a)\cdot M_{\tau,\mathcal{P}_3}(p_1,s_1) + \tfrac{1}{2}\cdot V_{i+1}(a)\cdot M_{\tau,\mathcal{P}_3}(p_2,s_1))\\
M_{\tau,\mathcal{P}_3}(p_1,s_1) &= U_{i+1,i+j+1}(b)\\
M_{\tau,\mathcal{P}_3}(p_2,s_1) &= U_{i+1,i+j+1}(b)
\end{aligned}$$

$$\begin{aligned}
M_{\tau,\mathcal{Q}_3}(q_S,s) &= U_{0,i}(a)\cdot V_{i+1}(a)\cdot M_{\tau,\mathcal{Q}_3}(q_1,s_1)\\
M_{\tau,\mathcal{Q}_3}(q_1,s_1) &= U_{i+1,i+j+1}(b)
\end{aligned}$$

Thus,

$$\begin{aligned}
M_{\tau,\mathcal{P}_3}(p_S,s) &= U_{0,i}(a)\cdot(\tfrac{1}{2}\cdot V_{i+1}(a)\cdot U_{i+1,i+j+1}(b) + \tfrac{1}{2}\cdot V_{i+1}(a)\cdot U_{i+1,i+j+1}(b))\\
&= U_{0,i}(a)\cdot V_{i+1}(a)\cdot U_{i+1,i+j+1}(b)\\
&= M_{\tau,\mathcal{Q}_3}(q_S,s)
\end{aligned}$$

(Case 3) $\widehat{\lambda(s)} = ab$
Let $s = \langle\, d_1,\tau\,\rangle\cdots\langle\, d_i,\tau\,\rangle\langle\, d_{i+1},a\,\rangle s_1$, $s_1 = \langle\, d_{i+2},\tau\,\rangle\cdots\langle\, d_{i+j+1},\tau\,\rangle\langle\, d_{i+j+2},b\,\rangle s_2$, and $s_2 = \langle\, d_{i+j+3},\tau\,\rangle\cdots\langle\, d_{i+j+k+2},\tau\,\rangle$.

$$\begin{aligned}
M_{\tau,\mathcal{P}_3}(p_S,s) &= U_{0,i}(a)\cdot(\tfrac{1}{2}\cdot V_{i+1}(a)\cdot M_{\tau,\mathcal{P}_3}(p_1,s_1) + \tfrac{1}{2}\cdot V_{i+1}(a)\cdot M_{\tau,\mathcal{P}_3}(p_2,s_1))\\
M_{\tau,\mathcal{P}_3}(p_1,s_1) &= U_{i+1,i+j+1}(b)\cdot V_{i+j+2}(b)\cdot M_{\tau,\mathcal{P}_3}(p_3,s_2)\\
M_{\tau,\mathcal{P}_3}(p_2,s_1) &= U_{i+1,i+j+1}(b)\cdot V_{i+j+2}(b)\cdot M_{\tau,\mathcal{P}_3}(p_4,s_2)\\
M_{\tau,\mathcal{P}_3}(p_3,s_2) &= U_{i+j+2,i+j+k+2}(c)\\
M_{\tau,\mathcal{P}_3}(p_4,s_2) &= U_{i+j+2,i+j+k+2}(d)
\end{aligned}$$

$$\begin{array}{rcl}
M_{\tau,\mathcal{Q}_3}(q_S,s) & = & U_{0,i}(a)\cdot V_{i+1}(a)\cdot M_{\tau,\mathcal{Q}_3}(q_1,s_1)\\
M_{\tau,\mathcal{Q}_3}(q_1,s_1) & = & U_{i+1,i+j+1}(b)\cdot(\frac{1}{2}\cdot V_{i+j+2}(b)\cdot M_{\tau,\mathcal{Q}_3}(q_2,s_2)+\frac{1}{2}\cdot V_{i+j+2}(b)\cdot M_{\tau,\mathcal{Q}_3}(q_3,s_2))\\
M_{\tau,\mathcal{Q}_3}(q_2,s_2) & = & U_{i+j+2,i+j+k+2}(c)\\
M_{\tau,\mathcal{Q}_3}(q_3,s_2) & = & U_{i+j+2,i+j+k+2}(d)
\end{array}$$

Thus,

$$\begin{array}{rcl}
M_{\tau,\mathcal{P}_3}(p_S,s) & = & \frac{1}{2}\cdot U_{0,i}(a)\cdot V_{i+1}(a)\cdot U_{i+1,i+j+1}(b)\cdot V_{i+j+2}(b)\cdot U_{i+j+2,i+j+k+2}(c)\\
& & +\frac{1}{2}\cdot U_{0,i}(a)\cdot V_{i+1}(a)\cdot U_{i+1,i+j+1}(b)\cdot V_{i+j+2}(b)\cdot U_{i+j+2,i+j+k+2}(d)\\
& = & U_{0,i}(a)\cdot V_{i+1}(a)\cdot U_{i+1,i+j+1}(b)\cdot(\frac{1}{2}\cdot V_{i+j+2}(b)\cdot U_{i+j+2,i+j+k+2}(c)\\
& & \qquad +\frac{1}{2}\cdot V_{i+j+2}(b)\cdot U_{i+j+2,i+j+k+2}(d))\\
& = & M_{\tau,\mathcal{Q}_3}(q_S,s)
\end{array}$$

(Case 4) $\widehat{\lambda(s)}=abc$. Let $s=\langle\, d_1,\tau\,\rangle\cdots\langle\, d_i,\tau\,\rangle\langle\, d_{i+1},a\,\rangle s_1$,
$s_1=\langle\, d_{i+2},\tau\,\rangle\cdots\langle\, d_{i+j+1},\tau\,\rangle\langle\, d_{i+j+2},b\,\rangle s_2$,
$s_2=\langle\, d_{i+j+3},\tau\,\rangle\cdots\langle\, d_{i+j+k+2},\tau\,\rangle\langle\, d_{i+j+k+3},c\,\rangle s_3$, and
$s_3=\langle\, d_{i+j+k+4},\tau\,\rangle\cdots\langle\, d_{i+j+k+l+3},\tau\,\rangle$

$$\begin{array}{rcl}
M_{\tau,\mathcal{P}_3}(p_S,s) & = & \frac{1}{2}\cdot U_{0,i}(a)\cdot V_{i+1}(a)\cdot M_{\tau,\mathcal{P}_3}(p_1,s_1)\\
M_{\tau,\mathcal{P}_3}(p_1,s_1) & = & U_{i+1,i+j+1}(b)\cdot V_{i+j+2}(b)\cdot M_{\tau,\mathcal{P}_3}(p_3,s_2)\\
M_{\tau,\mathcal{P}_3}(p_3,s_2) & = & U_{i+j+2,i+j+k+2}(c)\cdot V_{i+j+k+3}(c)\cdot M_{\tau,\mathcal{P}_3}(p_5,s_3)\\
M_{\tau,\mathcal{P}_3}(p_5,s_3) & = & 1
\end{array}$$

$$\begin{array}{rcl}
M_{\tau,\mathcal{Q}_3}(q_S,s) & = & U_{0,i}(a)\cdot V_{i+1}(a)\cdot M_{\tau,\mathcal{Q}_3}(q_1,s_1)\\
M_{\tau,\mathcal{Q}_3}(q_1,s_1) & = & \frac{1}{2}\cdot U_{i+1,i+j+1}(b)\cdot V_{i+j+2}(b)\cdot M_{\tau,\mathcal{Q}_3}(q_2,s_2)\\
M_{\tau,\mathcal{Q}_3}(q_2,s_2) & = & U_{i+j+2,i+j+k+2}(c)\cdot V_{i+j+k+3}(c)\cdot M_{\tau,\mathcal{Q}_3}(q_4,s_3)\\
M_{\tau,\mathcal{Q}_3}(q_4,s_3) & = & 1
\end{array}$$

Thus $M_{\tau,\mathcal{P}_3}(p_S,s)=M_{\tau,\mathcal{Q}_3}(q_S,s)$.

(Case 5) $\widehat{s}=abd$
Similar to case 4.