

## SOUND APPROXIMATE AND ASYMPTOTIC PROBABILISTIC BISIMULATIONS FOR PCTL

MASSIMO BARTOLETTI <sup>a</sup>, MAURIZIO MURGIA <sup>b</sup>, AND ROBERTO ZUNINO <sup>c</sup>

<sup>a</sup> University of Cagliari, Cagliari, Italy  
*e-mail address:* bart@unica.it

<sup>b</sup> Gran Sasso Science Institute, L'Aquila, Italy  
*e-mail address:* maurizio.murgia@gssi.it

<sup>c</sup> Università degli Studi di Trento, Trento, Italy  
*e-mail address:* roberto.zunino@unitn.it

**ABSTRACT.** We tackle the problem of establishing the soundness of approximate bisimilarity with respect to PCTL and its relaxed semantics. To this purpose, we consider a notion of bisimilarity inspired by the one introduced by Desharnais, Laviolette, and Tracol, and parametric with respect to an approximation error  $\delta$ , and to the depth  $n$  of the observation along traces. Essentially, our soundness theorem establishes that, when a state  $q$  satisfies a given formula up-to error  $\delta$  and steps  $n$ , and  $q$  is bisimilar to  $q'$  up-to error  $\delta'$  and enough steps, we prove that  $q'$  also satisfies the formula up-to a suitable error  $\delta''$  and steps  $n$ . The new error  $\delta''$  is computed from  $\delta, \delta'$  and the formula, and only depends linearly on  $n$ . We provide a detailed overview of our soundness proof.

We extend our bisimilarity notion to families of states, thus obtaining an asymptotic equivalence on such families. We then consider an asymptotic satisfaction relation for PCTL formulae, and prove that asymptotically equivalent families of states asymptotically satisfy the same formulae.

### 1. INTRODUCTION

The behaviour of many real-world systems can be formally modelled as probabilistic processes, e.g. as discrete-time Markov chains. Specifying and verifying properties on these systems requires probabilistic versions of temporal logics, such as PCTL [HJ94]. PCTL allows to express probability bounds using the formula  $\Pr_{\geq\pi}[\psi]$ , which is satisfied by those states starting from which the path formula  $\psi$  holds with probability  $\geq \pi$ . A well-known issue is that real-world systems can have tiny deviations from their mathematical models, while logical properties, such as those written in PCTL, impose sharp constraints on the behaviour. To address this issue, one can use a *relaxed* semantics for PCTL, as in [DAK12]. There, the semantics of formulae is parameterised over the error  $\delta \geq 0$  one is willing to tolerate. While in the standard semantics of  $\Pr_{\geq\pi}[\psi]$  the bound  $\geq \pi$  is *exact*, in relaxed PCTL this bound is weakened to  $\geq \pi - \delta$ . So, the relaxed semantics generalises the standard PCTL semantics of [HJ94], which can be obtained by choosing  $\delta = 0$ . Instead, choosing an error

---

*Key words and phrases:* PCTL, probabilistic processes, approximate bisimulation.

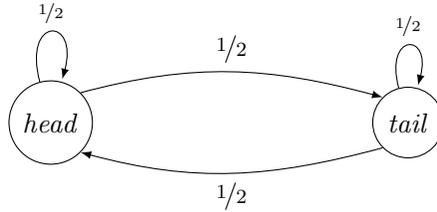


Figure 1: A Markov chain modelling repeated tosses of a fair coin.

$\delta > 0$  effectively provides a way to measure “how much” a state satisfies a given formula: some states might require only a very small error, while others a much larger one.

When dealing with temporal logics such as PCTL, one often wants to study some notion of state equivalence which preserves the semantics of formulae: that is, when two states are equivalent, they satisfy the same formulae. For instance, probabilistic bisimilarities like those in [DGJP10, DEP02, LS91] preserve the semantics of formulae for PCTL and other temporal logics. Although *strict* probabilistic bisimilarity preserves the semantics of relaxed PCTL, it is not *robust* against small deviations in the probability of transitions in Markov chains [GJS90]. A possible approach to deal with this issue is to also relax the notion of probabilistic bisimilarity, by making it parametric with respect to an error  $\delta$  [DAK12]. Relaxing bisimilarity in this way poses a choice regarding which properties of the strict probabilistic bisimilarity are to be kept. In particular, transitivity is enjoyed by the strict probabilistic bisimilarity, but it is *not* desirable for the relaxed notion. Indeed, we could have three states  $q, q'$  and  $q''$  where the behaviour of  $q$  and  $q'$  is similar enough (within the error  $\delta$ ), the behaviour of  $q'$  and  $q''$  is also similar enough (within  $\delta$ ), but the distance between  $q$  and  $q''$  is larger than the allowed error  $\delta$ . At best, we can have a sort of “triangular inequality”, where  $q$  and  $q''$  can still be related but only with a larger error  $2 \cdot \delta$ .

Bisimilarity is usually defined by coinduction, essentially requiring that the relation is preserved along an arbitrarily long sequence of moves. Still, in some settings, observing the behaviour over a very long run is undesirable. For instance, consider the PCTL formula  $\phi = \text{Pr}_{\geq 0.5}[\text{true } U^{\leq n} \text{ a}]$ , which is satisfied by those states from which, with probability  $\geq 0.5$ ,  $\text{a}$  is satisfied within  $n$  steps. In this case, a behavioural equivalence relation that preserves the semantics of  $\phi$  can neglect the long-run behaviour after  $n$  steps. More generally, if all the until operators are *bounded*, as in  $\phi_1 U^{\leq k} \phi_2$ , then each formula has an upper bound of steps  $n$  after which a behavioural equivalence relation can ignore what happens next. Observing the behaviour after this upper bound is unnecessarily strict, and indeed in some settings it is customary to neglect what happens in the very long run. For instance, a real-world player repeatedly tossing a coin is usually considered equivalent to a Markov chain with two states and four transitions with probability  $1/2$  (see Figure 1), even if in the long run the real-world system will diverge from the ideal one (e.g., when the player dies).

Another setting where observing the long-term behaviour is notoriously undesirable is that of cryptography. When studying the security of systems modelling cryptographic protocols, two states are commonly considered equivalent when their behaviour is similar (up to a small error  $\delta$ ) in the short run, even when in the very long run they diverge. For instance, a state  $q$  could represent an ideal system where no attacks can be performed by construction, while another state  $q'$  could represent a real system where an adversary can try to disrupt the cryptographic protocol. In such a scenario, if the protocol is secure, we

would like to have  $q$  and  $q'$  equivalent, since the behaviour of the real system is close to the one of the ideal system. Note that in the real system an adversary can repeatedly try to guess the secret cryptographic keys, and break security in the very long run, with very high probability. Accordingly, standard security definitions require that the behaviour of the ideal and real system are within a small error, but only for a *bounded* number of steps, after which their behaviour could diverge.

**Contributions.** To overcome the above mentioned issues, in this work we introduce a bounded, approximate notion of bisimilarity  $\sim_n^\delta$ , that only observes the first  $n$  steps, and allows for an error  $\delta$ . Unlike standard bisimilarity, our relation is naturally defined by *induction* on  $n$ . We call this looser variant of bisimilarity an *up-to- $n, \delta$*  bisimilarity. We showcase up-to- $n, \delta$  bisimilarity on a running example (Examples 3.6, 4.4, 5.2, and 6.6), comparing an ideal combination padlock against a real one which can be opened by an adversary guessing its combination. We show that the two systems are bisimilar up-to- $n, \delta$ , while they are not bisimilar according to the standard coinductive notion. We then discuss how the two systems satisfy a basic security property expressed in PCTL, with suitable errors. To make our theory amenable to reason about infinite-state systems, such as those usually found when modelling cryptographic protocols, all our results apply to Markov chains with countably many states. In this respect, our work departs from most literature on probabilistic bisimulations [DAK12, SZGN13] and bisimilarity distances [vB17, TvB17, TvB18, TvB16, Fu12, CvBW12, vBSW08], which usually assume *finite*-state Markov chains, as they focus on computing the distances. In Example 4.5 we exploit infinite-state Markov chains to compare a biased random bit generator with an ideal one.

Our first main contribution is a soundness theorem establishing that, when a state  $q$  satisfies a PCTL formula  $\phi$  (up to a given error), any bisimilar state  $q' \sim q$  must also satisfy  $\phi$ , at the cost of a slight increase of the error. More precisely, if  $\phi$  only involves until operators bounded by  $\leq n$ , state  $q$  satisfies  $\phi$  up to some error, and bisimilarity holds for enough steps and error  $\delta$ , then  $q'$  satisfies  $\phi$  with an *additional* asymptotic error  $O(n \cdot \delta)$ .

This asymptotic behaviour is compatible with the usual assumptions of computational security in cryptography. There, models of security protocols include a security parameter  $\eta$ , which affects the length of the cryptographic keys and the running time of the protocol: more precisely, a protocol is assumed to run for  $n(\eta)$  steps, which is polynomially bounded w.r.t.  $\eta$ . As already mentioned above, cryptographic notions of security do not observe the behaviour of the systems after this bound  $n(\eta)$ , since in the long run an adversary can surely guess the secret keys by brute force. Coherently, a protocol is considered to be secure if (roughly) its actual behaviour is *approximately* equivalent to the ideal one for  $n(\eta)$  steps and up to an error  $\delta(\eta)$ , which has to be a negligible function, asymptotically approaching zero faster than any rational function. Under these bounds on  $n$  and  $\delta$ , the asymptotic error  $O(n \cdot \delta)$  in our soundness theorem is negligible in  $\eta$ . Consequently, if two states  $q$  and  $q'$  represent the ideal and actual behaviour, respectively, and they are bisimilar up to a negligible error, they will satisfy the same PCTL formulae with a negligible error.

We formalise this reasoning by providing a notion of *asymptotic equivalence*. We start by considering families of states  $\Xi(\eta)$ , intuitively representing the behaviour of a system depending on a security parameter  $\eta$ . Our asymptotic equivalence  $\Xi_1 \equiv \Xi_2$  holds whenever the behaviour of the two families is  $n, \delta$ -bisimilar within a negligible error whenever we only perform a polynomial number of steps. We further introduce an *asymptotic satisfaction*

relation  $\Xi \models \phi$  which holds whenever the state  $\Xi(\eta)$  satisfies  $\phi$  under similar assumptions on the number of steps and the allowed error. Our second main result is the soundness of the asymptotic equivalence with respect to asymptotic satisfaction. Asymptotically equivalent families asymptotically satisfy the same PCTL formulae.

We provide a detailed overview of the proof of our soundness theorem for  $n, \delta$ -bisimilarity in section 5, deferring the gory technicalities to Appendix A. The proof of asymptotic soundness, which exploits the soundness theorem for  $n, \delta$ -bisimilarity, is given in section 6.

## 2. RELATED WORK

There is a well-established line of research on establishing soundness and completeness of probabilistic bisimulations against various kinds of probabilistic logics [DGJP10, FMM20, HPS<sup>+</sup>11, LS91, MS17, Mio18].

The work closest to ours is that of D’Innocenzo, Abate and Katoen [DAK12], which addresses the model checking problem on a relaxed PCTL differing from ours in a few aspects. First, their syntax allows for an individual bound on the number of steps  $k$  for each until operator  $U^{\leq k}$ , while we assume all such bounds are equal and we make the semantics of PCTL parametrized w.r.t. the number of steps to be considered in until. This approach allows us to simplify the statement of the soundness theorem and the definition of asymptotic satisfaction relation, since the bound is not fixed by the formula, but it is a parameter of the semantics. Dealing with the case where each until in a formula could have its bound seems possible, at the cost of increasing the level of technicalities. Second, their main result shows that bisimilar states up-to a given error  $\epsilon$  satisfy the same formulae  $\psi$ , provided that  $\psi$  ranges over the so-called  $\epsilon$ -robust formulae. Instead, our soundness result applies to *all* PCTL formulae, and ensures that when moving from a state satisfying  $\phi$  to a bisimilar one,  $\phi$  is still satisfied, but at the cost of slightly increasing the error. Third, their relaxed semantics differs from ours. In ours, we relax all the probability bounds by the same amount  $\delta$ . Instead, the relaxation in [DAK12] affects the bounds by a different amount which depends on the error  $\epsilon$ , the until bound  $k$ , and the underlying DTMC.

Desharnais, Laviolette and Tracol [DLT08] use a coinductive approximate probabilistic bisimilarity, up-to an error  $\delta$ . Using such coinductive bisimilarity, [DLT08] establishes the soundness and completeness with respect to a Larsen-Skou logic [LS91] (instead of PCTL). In [DLT08], a bounded, up-to  $n, \delta$  version of bisimilarity is only briefly used to derive a decision algorithm for coinductive bisimilarity under the assumption that the state space is finite. In our work, instead, the bounded up-to  $n, \delta$  bisimilarity is the main focus of study. In particular, our soundness result only assumes  $n, \delta$  bisimilarity, which is strictly weaker than coinductive bisimilarity. Another minor difference is that [DLT08] considers a labelled Markov process, i.e. the probabilistic variant of a labelled transition system, while we instead focus on DTMCs having labels on states.

Bian and Abate [BA17] study bisimulation and trace equivalence up-to an error  $\epsilon$ , and show that  $\epsilon$ -bisimilar states are also  $\epsilon'$ -trace equivalent for a suitable  $\epsilon'$  which depends on  $\epsilon$ . Furthermore, they show that  $\epsilon$ -trace equivalent states satisfy the same formulae in a bounded LTL, up-to a certain error. In our work, we focus instead on the branching logic PCTL.

A related research line is that on *bisimulation metrics* [vB17, vBHMW05, vBW05]. Some of these metrics, like our up-to bisimilarity, take approximations into account [DGJP99, CGT16]. Similarly to our bisimilarity, bisimulation metrics allow to establish two states equivalent up-to a certain error (but usually do not take into account the bound on the

number of steps). Interestingly, Castiglioni, Gebler and Tini [CGT16] introduce a notion of distance between Larsen-Skou formulae, and prove that the bisimulation distance between two processes corresponds to the distance between their mimicking formulae. De Alfaro, Majumdar, Raman and Stoelinga [dAMRS08] elegantly characterise bisimulation metrics with a quantitative  $\mu$ -calculus. Such logic allows to specify interesting properties such as maximal reachability and safety probability, and the maximal probability of satisfying a general  $\omega$ -regular specification, but not full PCTL. Mio [Mio14] characterises a bisimulation metric based on total variability with a more general quantitative  $\mu$ -calculus, dubbed Łukasiewicz  $\mu$ -calculus, able to encode PCTL. Both [dAMRS08] and [Mio14] do not take the number of steps into account, therefore their applicability to the analysis of security protocols is yet to be investigated.

Metrics with discount [DGJP04, dAHM03, BBL<sup>+</sup>21, DCP06, vBSW08] are sometimes used to relate the behaviour of probabilistic processes, weighing less those events that happen in the far future compared to those happening in the first steps. Often, in these metrics each step causes the probability of the next events to be multiplied by a constant factor  $c < 1$ , in order to diminish their importance. Note that this discount makes it so that after  $\eta$  steps, this diminishing factor becomes  $c^\eta$ , which is a negligible function of  $\eta$ . As discussed before, in cryptographic security one needs to consider as important those events happening within polynomially many steps, while neglecting the ones after such a polynomial threshold. Using an exponential discount factor  $c^\eta$  after only  $\eta$  steps goes against this principle, since it would cause a secure system to be at a negligible distance from an insecure one which can be violated after just  $\eta$  steps. For this reason, instead of using a metric with discount, in this paper we resort to a bisimilarity that is parametrized over the number of steps  $n$  and error  $\delta$ , allowing us to obtain a notion which distinguishes between the mentioned secure and insecure systems.

Several works develop algorithms to decide probabilistic bisimilarity, and to compute metrics [vBW14, CvBW12, Fu12, TvB16, TvB17, TvB18]. To this purpose, they restrict to finite-state systems, like e.g. probabilistic automata. Our results, instead, apply also to infinite-state systems.

In [ZD05] a calculus with cryptographic primitives is introduced, together with a semantics where attackers have a probability  $\pi(\eta)$  of guessing encryption keys. It is shown that, assuming that  $\pi(\eta)$  is negligible and that attackers run in polynomial time, some security properties (e.g. secrecy, authentication) are equivalent to the analogous properties with standard Dolev-Yao assumptions (that is, attackers never guess keys but are not restricted to polynomial time). This result can be seen as a special case of our asymptotic soundness theorem.

The interesting work [LG22] proposes a behavioural notion of indistinguishability between session typed probabilistic  $\pi$ -calculus processes, with the aim of providing a formal system for proving security of real cryptographic protocols by comparison with ideal ones. The type system, which is based on bounded linear logic [GSS92, LG16], guarantees that processes terminate in polynomial time. This differs from our approach, where polynomiality appears directly in the equivalence definition (Definition 6.2). Moreover, the calculus of [LG22] is quite restrictive: for instance, it is not possible to specify adversaries that access an oracle a polynomial number of times. By contrast, our abstract model is general enough to represent such adversaries.

**Comparison with [BMZ22].** This paper extends the work [BMZ22] in two directions. First, the current paper includes the proofs of all statements, which were not present in [BMZ22]. Second, in [BMZ22] we hinted at the possible application of soundness to the asymptotic behaviour of systems which depend on a parameter  $\eta$ . Here, we properly develop and formalise that intuition in section 6, providing a new asymptotic soundness result.

### 3. THE PROBABILISTIC TEMPORAL LOGIC PCTL

Assume a set  $\mathcal{L}$  of labels, ranged over by  $l$ , and let  $\delta, \pi$  range over non-negative reals. A *discrete-time Markov chain* (DTMC) is a standard model of probabilistic systems. Throughout this paper, we consider a DTMC having a countable, possibly infinite, set of states  $q$ , each carrying a subset of labels  $\ell(q) \subseteq \mathcal{L}$ .

**Definition 3.1** (Discrete-Time Markov Chain). A (labelled) DTMC is a triple  $(\mathcal{Q}, \text{Pr}, \ell)$  where:

- $\mathcal{Q}$  is a countable set of states;
- $\text{Pr} : \mathcal{Q}^2 \rightarrow [0, 1]$  is a function, named transition probability function;
- $\ell : \mathcal{Q} \rightarrow \mathcal{P}(\mathcal{L})$  is a labelling function

Given  $q \in \mathcal{Q}$  and  $Q \subseteq \mathcal{Q}$ , we write  $\text{Pr}(q, Q)$  for  $\sum_{q' \in Q} \text{Pr}(q, q')$  and we require that  $\text{Pr}(q, \mathcal{Q}) = 1$  for all  $q \in \mathcal{Q}$ .

A *trace* is an infinite sequence of states  $t = q_0 q_1 \dots$ , where we write  $t(i)$  for  $q_i$ , i.e. the  $i$ -th element of  $t$ . A *trace fragment* is a finite, non-empty sequence of states  $\tilde{t} = q_0 \dots q_{n-1}$ , where  $|\tilde{t}| = n \geq 1$  is its length. Given a trace fragment  $\tilde{t}$  and a state  $q$ , we write  $\tilde{t}q^\omega$  for the trace  $\tilde{t}qq\dots$ .

It is well-known that, given an initial state  $q_0$ , the DTMC induces a  $\sigma$ -algebra of measurable sets of traces  $T$  starting from  $q_0$ , i.e. the  $\sigma$ -algebra generated by cylinder sets [BK08]. More in detail, given a trace fragment  $\tilde{t} = q_0 \dots q_{n-1}$ , its *cylinder set*

$$\text{Cyl}(\tilde{t}) = \{t \mid \tilde{t} \text{ is a prefix of } t\}$$

is given probability:

$$\text{Pr}(\text{Cyl}(\tilde{t})) = \prod_{i=0}^{n-2} \text{Pr}(q_i, q_{i+1})$$

As usual, if  $n = 1$  the product is empty and evaluates to 1. Closing the family of cylinder sets under countable unions and complement we obtain the family of measurable sets. The probability measure on cylinder sets then uniquely extends to all the measurable sets.

Given a set of trace fragments  $\tilde{T}$ , all starting from the same state  $q_0$  and having the same length, we let  $\text{Pr}(\tilde{T}) = \text{Pr}(\bigcup_{\tilde{t} \in \tilde{T}} \text{Cyl}(\tilde{t})) = \sum_{\tilde{t} \in \tilde{T}} \text{Pr}(\text{Cyl}(\tilde{t}))$ . Note that using same-length trace fragments ensures that their cylinder sets are disjoint, hence the second equality holds.

Below, we define PCTL formulae. Our syntax is mostly standard, except for the *until* operator. There, for the sake of simplicity, we do not bound the number of steps in the syntax  $\phi_1 \text{U} \phi_2$ , but we do so in the semantics. Concretely, this amounts to imposing the same bound to *all* the occurrences of  $\text{U}$  in the formula. Such bound is then provided as a parameter to the semantics.

**Definition 3.2** (PCTL Syntax). The syntax of PCTL is given by the following grammar, defining *state formulae*  $\phi$  and *path formulae*  $\psi$ :

$$\begin{aligned}\phi &::= l \mid \text{true} \mid \neg\phi \mid \phi \wedge \phi \mid \text{Pr}_{\triangleright\pi}[\psi] & \text{where } \triangleright \in \{>, \geq\} \\ \psi &::= \text{X}\phi \mid \phi \text{ U } \phi\end{aligned}$$

As syntactic sugar, we write  $\text{Pr}_{<\pi}[\psi]$  for  $\neg\text{Pr}_{\geq\pi}[\psi]$ , and  $\text{Pr}_{\leq\pi}[\psi]$  for  $\neg\text{Pr}_{>\pi}[\psi]$ .

Given a PCTL formula  $\phi$ , we define its maximum X-nesting  $\text{X}_{\max}(\phi)$  and its maximum U-nesting  $\text{U}_{\max}(\phi)$  inductively as follows:

**Definition 3.3** (Maximum Nesting). For  $\circ \in \{\text{X}, \text{U}\}$ , we define:

$$\begin{aligned}\circ_{\max}(l) &= 0 & \circ_{\max}(\text{true}) &= 0 & \circ_{\max}(\neg\phi) &= \circ_{\max}(\phi) \\ \circ_{\max}(\phi_1 \wedge \phi_2) &= \max(\circ_{\max}(\phi_1), \circ_{\max}(\phi_2)) & \circ_{\max}(\text{Pr}_{\triangleright\pi}[\psi]) &= \circ_{\max}(\psi) \\ \circ_{\max}(\text{X}\phi) &= \circ_{\max}(\phi) + \begin{cases} 1 & \text{if } \circ = \text{X} \\ 0 & \text{otherwise} \end{cases} \\ \circ_{\max}(\phi_1 \text{ U } \phi_2) &= \max(\circ_{\max}(\phi_1), \circ_{\max}(\phi_2)) + \begin{cases} 1 & \text{if } \circ = \text{U} \\ 0 & \text{otherwise} \end{cases}\end{aligned}$$

We now define a semantics for PCTL where the probability bounds  $\triangleright\pi$  in  $\text{Pr}_{\triangleright\pi}[\psi]$  can be relaxed or strengthened by an error  $\delta$ . Our semantics is parameterized over the *until* bound  $n$ , the error  $\delta \in \mathbb{R}^{\geq 0}$ , and a direction  $r \in \{+1, -1\}$ . Given the parameters, the semantics associates each PCTL state formula with the set of states satisfying it. Intuitively, when  $r = +1$  we relax the semantics of the formula, so that increasing  $\delta$  causes more states to satisfy it. More precisely, the probability bounds  $\triangleright\pi$  in positive occurrences of  $\text{Pr}_{\triangleright\pi}[\psi]$  are decreased by  $\delta$ , while those in negative occurrences are increased by  $\delta$ . Dually, when  $r = -1$  we strengthen the semantics, modifying  $\triangleright\pi$  in the opposite direction. Our semantics is inspired by the relaxed / strengthened PCTL semantics of [DAK12].

**Definition 3.4** (PCTL Semantics). The semantics of PCTL formulae is given below. Let  $n \in \mathbb{N}$ ,  $\delta \in \mathbb{R}^{\geq 0}$  and  $r \in \{+1, -1\}$ .

$$\begin{aligned}[[l]]_{\delta,r}^n &= \{q \in \mathcal{Q} \mid l \in \ell(q)\} \\ [[\text{true}]]_{\delta,r}^n &= \mathcal{Q} \\ [[\neg\phi]]_{\delta,r}^n &= \mathcal{Q} \setminus [[\phi]]_{\delta,-r}^n \\ [[\phi_1 \wedge \phi_2]]_{\delta,r}^n &= [[\phi_1]]_{\delta,r}^n \cap [[\phi_2]]_{\delta,r}^n \\ [[\text{Pr}_{\triangleright\pi}[\psi]]]_{\delta,r}^n &= \{q \in \mathcal{Q} \mid \text{Pr}(\text{Cyl}(q) \cap [[\psi]]_{\delta,r}^n) + r \cdot \delta \triangleright \pi\} \\ [[\text{X}\phi]]_{\delta,r}^n &= \{t \mid t(1) \in [[\phi]]_{\delta,r}^n\} \\ [[\phi_1 \text{ U } \phi_2]]_{\delta,r}^n &= \{t \mid \exists i \in 0..n. t(i) \in [[\phi_2]]_{\delta,r}^n \wedge \forall j \in 0..i-1. t(j) \in [[\phi_1]]_{\delta,r}^n\}\end{aligned}$$

The semantics is mostly standard, except for  $\text{Pr}_{\triangleright\pi}[\psi]$  and  $\phi_1 \text{ U } \phi_2$ . The semantics of  $\text{Pr}_{\triangleright\pi}[\psi]$  adds  $r \cdot \delta$  to the probability of satisfying  $\psi$ , which relaxes or strengthens (depending on  $r$ ) the probability bound as needed. The semantics of  $\phi_1 \text{ U } \phi_2$  uses the parameter  $n$  to bound the number of steps within which  $\phi_2$  must hold.

Our semantics enjoys monotonicity. The semantics of state and path formulae is increasing w.r.t.  $\delta$  if  $r = +1$ , and decreasing otherwise. The semantics also increases when moving from  $r = -1$  to  $r = +1$ .

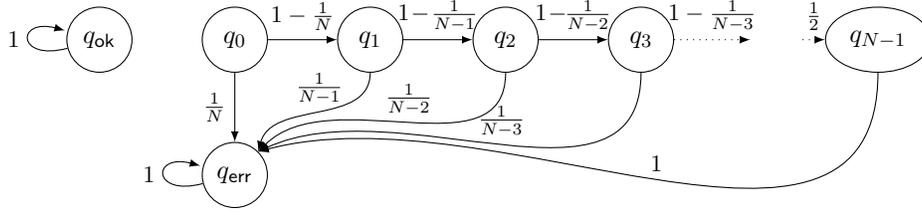


Figure 2: A Markov chain modelling an ideal (left) and a real (right) padlock.

**Lemma 3.5** (Monotonicity). *Whenever  $\delta \leq \delta'$ , we have:*

$$\begin{array}{lll} \llbracket \phi \rrbracket_{\delta,+1}^n \subseteq \llbracket \phi \rrbracket_{\delta',+1}^n & \llbracket \phi \rrbracket_{\delta',-1}^n \subseteq \llbracket \phi \rrbracket_{\delta,-1}^n & \llbracket \phi \rrbracket_{\delta,-1}^n \subseteq \llbracket \phi \rrbracket_{\delta,+1}^n \\ \llbracket \psi \rrbracket_{\delta,+1}^n \subseteq \llbracket \psi \rrbracket_{\delta',+1}^n & \llbracket \psi \rrbracket_{\delta',-1}^n \subseteq \llbracket \psi \rrbracket_{\delta,-1}^n & \llbracket \psi \rrbracket_{\delta,-1}^n \subseteq \llbracket \psi \rrbracket_{\delta,+1}^n \end{array}$$

Note that monotonicity does *not* hold for the parameter  $n$ , i.e. even if  $n \leq n'$ , we can *not* conclude  $\llbracket \phi \rrbracket_{\delta,+1}^n \subseteq \llbracket \phi \rrbracket_{\delta,+1}^{n'}$ . As a counterexample, let  $\mathcal{Q} = \{q_0, q_1\}$ ,  $\ell(q_0) = \emptyset$ ,  $\ell(q_1) = \{\mathbf{a}\}$ ,  $\Pr(q_0, q_1) = \Pr(q_1, q_1) = 1$ , and  $\Pr(q, q') = 0$  elsewhere. Given  $\phi = \Pr_{\leq 0}[\text{true U } \mathbf{a}]$ , we have  $q_0 \in \llbracket \phi \rrbracket_{0,+1}^0$  since in  $n = 0$  steps it is impossible to reach a state satisfying  $\mathbf{a}$ . However, we do *not* have  $q_0 \in \llbracket \phi \rrbracket_{0,+1}^1$  since in  $n' = 1$  steps we always reach  $q_1$ , which satisfies  $\mathbf{a}$ .

**Example 3.6.** We compare an ideal combination padlock to a real one from the point of view of an adversary. The ideal padlock has a single state  $q_{\text{ok}}$ , representing a closed padlock that can not be opened. Instead, the real padlock is under attack from the adversary who tries to open the padlock by repeatedly guessing its 5-digit PIN. At each step the adversary generates a (uniformly) random PIN, different from all the ones which have been attempted so far, and tries to open the padlock with it. The states of the real padlock are  $q_0, \dots, q_{N-1}$  (with  $N = 10^5$ ), where  $q_i$  represents the situation where  $i$  unsuccessful attempts have been made, and an additional state  $q_{\text{err}}$  that represents that the padlock was opened.

Since after  $i$  attempts the adversary needs to guess the correct PIN among the  $N - i$  remaining combinations, the real padlock in state  $q_i$  moves to  $q_{\text{err}}$  with probability  $1/(N - i)$ , and to  $q_{i+1}$  with the complementary probability.

Summing up, we simultaneously model both the ideal and real padlock as a single DTMC with the following transition probability function (see Figure 2):

$$\begin{array}{ll} \Pr(q_{\text{ok}}, q_{\text{ok}}) = 1 & \\ \Pr(q_{\text{err}}, q_{\text{err}}) = 1 & \\ \Pr(q_i, q_{\text{err}}) = 1/(N - i) & 0 \leq i < N \\ \Pr(q_i, q_{i+1}) = 1 - 1/(N - i) & 0 \leq i < N - 1 \\ \Pr(q, q') = 0 & \text{otherwise} \end{array}$$

We label the states with labels  $\mathcal{L} = \{\text{err}\}$  by letting  $\ell(q_{\text{err}}) = \{\text{err}\}$  and  $\ell(q) = \emptyset$  for all  $q \neq q_{\text{err}}$ .

The PCTL formula  $\phi = \Pr_{\leq 0}[\text{true U err}]$  models the expected behaviour of an unbreakable padlock, requiring that the set of traces where the padlock is eventually opened has zero

probability. Formally,  $\phi$  is satisfied by state  $q$  when

$$\begin{aligned}
q \in \llbracket \phi \rrbracket_{\delta,+1}^n &\iff q \in \llbracket \neg \text{Pr}_{>0}[\text{true U err}] \rrbracket_{\delta,+1}^n \\
&\iff q \notin \llbracket \text{Pr}_{>0}[\text{true U err}] \rrbracket_{\delta,-1}^n \\
&\iff \neg(\text{Pr}(\text{Cyl}(q) \cap \llbracket \text{true U err} \rrbracket_{\delta,-1}^n) - \delta > 0) \\
&\iff \text{Pr}(\text{Cyl}(q) \cap \llbracket \text{true U err} \rrbracket_{\delta,-1}^n) \leq \delta
\end{aligned} \tag{3.1}$$

When  $q = q_{\text{ok}}$  we have that  $\text{Cyl}(q_{\text{ok}}) \cap \llbracket \text{true U err} \rrbracket_{\delta,-1}^n = \emptyset$ , hence the above probability is zero, which is surely  $\leq \delta$ . Consequently,  $\phi$  is satisfied by the ideal padlock  $q_{\text{ok}}$ , for all  $n \geq 0$  and  $\delta \geq 0$ .

By contrast,  $\phi$  is not always satisfied by the real padlock  $q = q_0$ , since we have  $q_0 \in \llbracket \phi \rrbracket_{\delta,+1}^n$  only for some values of  $n$  and  $\delta$ . To show why, we start by considering some trivial cases. Choosing  $\delta = 1$  makes equation (3.1) trivially true for all  $n$ . Furthermore, if we choose  $n = 1$ , then  $\text{Cyl}(q_0) \cap \llbracket \text{true U err} \rrbracket_{\delta,-1}^n = \{q_0 q_{\text{err}}^\omega\}$  is a set of traces with probability  $1/N$ . Therefore, equation (3.1) holds only when  $\delta \geq 1/N$ . More in general, when  $n \geq 1$ , we have

$$\text{Cyl}(q_0) \cap \llbracket \text{true U err} \rrbracket_{\delta,-1}^n = \{q_0 q_{\text{err}}^\omega, q_0 q_1 q_{\text{err}}^\omega, q_0 q_1 q_2 q_{\text{err}}^\omega, \dots, q_0 \dots q_{n-1} q_{\text{err}}^\omega\}$$

The probability of the above set is the probability of guessing the PIN within  $n$  steps. The complementary event, i.e. not guessing the PIN for  $n$  times, has probability

$$\frac{N-1}{N} \cdot \frac{N-2}{N-1} \dots \frac{N-n}{N-(n-1)} = \frac{N-n}{N}$$

Consequently, (3.1) simplifies to  $n/N \leq \delta$ , suggesting the least value of  $\delta$  (depending on  $n$ ) for which  $q_0$  satisfies  $\phi$ . For instance, when  $n = 10^3$ , this amounts to claiming that the real padlock is secure, up to an error of  $\delta = n/N = 10^{-2}$ .

#### 4. UP-TO- $n, \delta$ BISIMILARITY

We now define a relation on states  $q \sim_\delta^n q'$  that intuitively holds whenever  $q$  and  $q'$  exhibit similar behaviour for a bounded number of steps. The parameter  $n$  controls the number of steps, while  $\delta$  controls the error allowed in each step. Note that since we only observe the first  $n$  steps, our notion is *inductive*, unlike unbounded bisimilarity which is co-inductive, similarly to [CGT16]. Our notion is also inspired by [DLT08].

**Definition 4.1** (Up-to- $n, \delta$  Bisimilarity). We define the relation  $q \sim_\delta^n q'$  as follows by induction on  $n$ :

- (1)  $q \sim_\delta^0 q'$  always holds
- (2)  $q \sim_\delta^{n+1} q'$  holds if and only if, for all  $Q \subseteq \mathcal{Q}$ :
  - (a)  $\ell(q) = \ell(q')$
  - (b)  $\text{Pr}(q, Q) \leq \text{Pr}(q', \sim_\delta^n(Q)) + \delta$
  - (c)  $\text{Pr}(q', Q) \leq \text{Pr}(q, \sim_\delta^n(Q)) + \delta$

where  $\sim_\delta^n(Q) = \{q' \mid \exists q \in Q. q \sim_\delta^n q'\}$  is the image of the set  $Q$  according to the bisimilarity relation.

We now establish two basic properties of the bisimilarity. Our notion is reflexive and symmetric, and enjoys a triangular property. Furthermore, it is monotonic on both  $n$  and  $\delta$ .

**Lemma 4.2.** *The relation  $\sim$  satisfies:*

$$q \sim_{\delta}^n q \quad q \sim_{\delta}^n q' \implies q' \sim_{\delta}^n q \quad q \sim_{\delta}^n q' \wedge q' \sim_{\delta'}^n q'' \implies q \sim_{\delta+\delta'}^n q''$$

*Proof.* Straightforward induction on  $n$ . □

**Lemma 4.3** (Monotonicity).

$$\begin{aligned} n' \leq n &\implies \sim_{\delta}^n \subseteq \sim_{\delta}^{n'} \\ \delta \leq \delta' &\implies \sim_{\delta}^n \subseteq \sim_{\delta'}^n \end{aligned}$$

**Example 4.4.** We use up-to- $n, \delta$  bisimilarity to compare the behaviour of the ideal padlock  $q_{\text{ok}}$  and the real one, in any of its states, when observed for  $n$  steps. When  $n = 0$  bisimilarity trivially holds, so below we only consider  $n > 0$ .

We start from the simplest case: bisimilarity does not hold between  $q_{\text{ok}}$  and  $q_{\text{err}}$ . Indeed,  $q_{\text{ok}}$  and  $q_{\text{err}}$  have distinct labels ( $\ell(q_{\text{ok}}) = \emptyset \neq \{\text{err}\} = \ell(q_{\text{err}})$ ), hence we do not have  $q_{\text{ok}} \sim_{\delta}^n q_{\text{err}}$ , no matter what  $n > 0$  and  $\delta$  are.

We now compare  $q_{\text{ok}}$  with any  $q_i$ . When  $n = 1$ , both states have an empty label set, i.e.  $\ell(q_{\text{ok}}) = \ell(q_i) = \emptyset$ , hence they are bisimilar for any error  $\delta$ . We therefore can write  $q_{\text{ok}} \sim_{\delta}^1 q_i$  for any  $\delta \geq 0$ .

When  $n = 2$ , we need a larger error  $\delta$  to make  $q_{\text{ok}}$  and  $q_i$  bisimilar. Indeed, if we perform a move from  $q_i$ , the padlock can be broken with probability  $1/(N-i)$ , in which case we reach  $q_{\text{err}}$ , thus violating bisimilarity. Accounting for such probability, we only obtain  $q_{\text{ok}} \sim_{\delta}^2 q_i$  for any  $\delta \geq 1/(N-i)$ .

When  $n = 3$ , we need an even larger error  $\delta$  to make  $q_{\text{ok}}$  and  $q_i$  bisimilar. Indeed, while the first PIN guessing attempt has probability  $1/(N-i)$ , in the second move the guessing probability increases to  $1/(N-i-1)$ . Choosing  $\delta$  equal to the largest probability is enough to account for both moves, hence we obtain  $q_{\text{ok}} \sim_{\delta}^3 q_i$  for any  $\delta \geq 1/(N-i-1)$ . Technically, note that the denominator  $N-i-1$  might be zero, since when  $i = n-1$  the first move always guesses the PIN, and the second guess never actually happens. In such case, we instead take  $\delta = 1$ . More in detail, we verify item (2b) of Definition 4.1 for  $q_{\text{ok}} \sim_{\delta}^3 q_i$ , assuming  $\delta \geq 1/(N-i-1)$ . We must prove that:

$$\Pr(q_{\text{ok}}, Q) \leq \Pr(q_i, \sim_{\delta}^2(Q)) + \delta$$

When  $q_{\text{ok}} \notin Q$  we have  $\Pr(q_{\text{ok}}, Q) = 0$ , hence the inequality holds trivially. Otherwise, if  $q_{\text{ok}} \in Q$  we first observe that  $\Pr(q_{\text{ok}}, Q) = 1$ . From the case  $n = 2$ , we have  $q_{\text{ok}} \sim_{\delta}^2 q_{i+1}$ , since  $\delta \geq 1/(N-(i+1))$ . Hence,  $q_{i+1} \in \sim_{\delta}^2(Q)$  and so:

$$\Pr(q_i, \sim_{\delta}^2(Q)) + \delta \geq \Pr(q_i, \{q_{i+1}\}) + \delta = 1 - \frac{1}{N-i} + \delta \geq 1 - \frac{1}{N-i} + \frac{1}{N-i-1} \geq 1$$

This proves item (2b); the proof for item (2c) is similar.

More in general, for an arbitrary  $n \geq 2$ , we obtain through a similar argument that  $q_{\text{ok}} \sim_{\delta}^n q_i$  for any  $\delta \geq 1/(N-i-n+2)$ . Intuitively,  $\delta = 1/(N-i-n+2)$  is the probability of guessing the PIN in the last attempt (the  $n$ -th), which is the attempt having the highest success probability. Again, when the denominator  $N-i-n+2$  becomes zero (or negative), we instead take  $\delta = 1$ .

Note that the DTMC of the ideal and real padlocks (Example 3.6) has finitely many states. Our bisimilarity notion and results, however, can also deal with DTMCs with a countably infinite set of states, as we show in the next example.

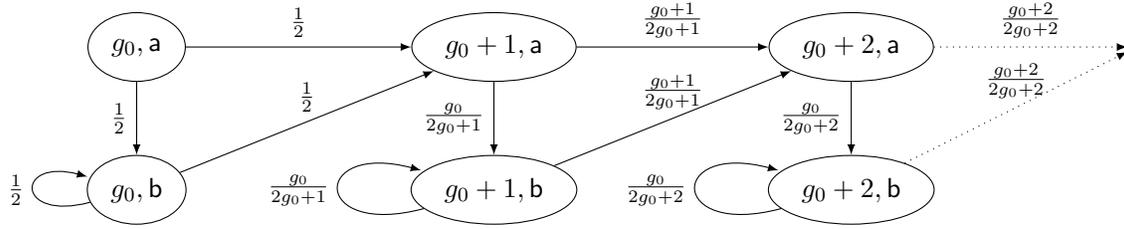


Figure 3: A Markov chain modelling an unfair random generator of bit streams.

**Example 4.5.** We consider an ideal system which randomly generates bit streams in a fair way. We model such a system as having two states  $\{q_a, q_b\}$ , with transition probabilities  $\Pr(x, y) = 1/2$  for any  $x, y \in \{q_a, q_b\}$ , as in Figure 1. We label state  $q_a$  with label **a** denoting bit 0, and state  $q_b$  with label **b** denoting bit 1.

We compare this ideal system with a real system which generates bit streams in an unfair way. At each step, the real system draws a ball from an urn, initially having  $g_0$  **a**-labelled balls and  $g_0$  **b**-labelled balls. After each drawing, the ball is placed back in the urn. However, every time an **a**-labelled ball is drawn, an additional **a**-labelled ball is put in the urn, making the next drawings more biased towards **a**.

We model the real system using the infinite<sup>1</sup> set of states  $\mathbb{N} \times \{\mathbf{a}, \mathbf{b}\}$ , whose first component counts the number of **a**-labelled balls in the urn, and the second component is the label of the last-drawn ball. The transition probabilities are as follows, where  $g_0 \in \mathbb{N}^+$  (see Figure 3):

$$\begin{aligned} \Pr((g, x), (g + 1, \mathbf{a})) &= g/(g + g_0) \\ \Pr((g, x), (g, \mathbf{b})) &= g_0/(g + g_0) \\ \Pr((g, x), (g', x')) &= 0 \quad \text{otherwise} \end{aligned}$$

We label each such state with its second component.

We now compare the ideal system to the real one. Intuitively, the ideal system, when started from state  $q_a$ , produces a sequence of states whose labels are uniform independent random values in  $\{\mathbf{a}, \mathbf{b}\}$ . Instead, the real system slowly becomes more and more biased towards label **a**. More precisely, when started from state  $(g_0, \mathbf{a})$ , in the first drawing the next label is uniformly distributed between **a** and **b**, as in the ideal system. When the sampled state has label **a**, this causes the component  $g$  to be incremented, increasing the probability  $g/(g + g_0)$  of sampling another **a** in the next steps. Indeed, the value  $g$  is always equal to  $g_0$  plus the number of sampled **a**-labelled states so far.

Therefore, unlike the ideal system, on the long run the real system will visit **a**-labelled states with very high probability, since the  $g$  component slowly but steadily increases. While this fact makes the two systems *not* bisimilar according to the standard probabilistic bisimilarity [LS89], if we restrict the number of steps to  $n \ll g_0$  and tolerate a small error  $\delta$ , we can obtain  $q_a \sim_\delta^n (g_0, \mathbf{a})$ .

For instance, if we let  $g_0 = 1000$ ,  $n = 100$  and  $\delta = 0.05$  we have  $q_a \sim_\delta^n (g_0, \mathbf{a})$ . This is because, in  $n$  steps, the first component  $g$  of a real system  $(g, x)$  will at most reach 1100, making the probability of the next step to be  $(g + 1, \mathbf{a})$  to be at most  $1100/2100 \simeq 0.523$ . This differs from the ideal probability 0.5 by less than  $\delta$ , hence bisimilarity holds.

<sup>1</sup>Modelling this behaviour inherently requires an *infinite* set of states, since each number of **a**-labelled balls in the urn leads to a unique transition probability function.

## 5. SOUNDNESS

Our soundness theorem shows that, if we consider any state  $q$  satisfying  $\phi$  (with steps  $n$  and error  $\delta'$ ), and any state  $q'$  which is bisimilar to  $q$  (with enough steps and error  $\delta$ ), then  $q'$  must satisfy  $\phi$ , with the same number  $n$  of steps, at the cost of suitably increasing the error. For a fixed  $\phi$ , the “large enough” number of steps and the increase in the error depend linearly on  $n$ .

**Theorem 5.1** (Soundness). *Let  $k_X = \mathbf{X}_{max}(\phi)$  be the maximum  $\mathbf{X}$ -nesting of a formula  $\phi$ , and let  $k_U = \mathbf{U}_{max}(\phi)$  be the maximum  $\mathbf{U}$ -nesting of  $\phi$ . Then, for all  $n, \delta, \delta'$  we have:*

$$\sim_{\delta}^{\bar{n}} (\llbracket \phi \rrbracket_{\delta', +1}^n) \subseteq \llbracket \phi \rrbracket_{\bar{n} \cdot \delta + \delta', +1}^n \quad \text{where } \bar{n} = n \cdot k_U + k_X + 1$$

**Example 5.2.** We apply Theorem 5.1 to our padlock system in the running example. We take the same formula  $\phi = \text{Pr}_{\leq 0}[\text{true} \cup \text{err}]$  of Example 3.6 and choose  $n = 10^3$  and  $\delta' = 0$ . Since  $\phi$  has only one until operator and no next operators, the value  $\bar{n}$  in the theorem statement is  $\bar{n} = 10^3 \cdot 1 + 0 + 1 = 1001$ . Therefore, from Theorem 5.1 we obtain, for all  $\delta$ :

$$\sim_{\delta}^{1001} (\llbracket \phi \rrbracket_{0, +1}^{1000}) \subseteq \llbracket \phi \rrbracket_{1001 \cdot \delta, +1}^{1000}$$

In Example 3.6 we discussed how the ideal padlock  $q_{\text{ok}}$  satisfies the formula  $\phi$  for any number of steps and any error value. In particular, choosing 1000 steps and zero error, we get  $q_{\text{ok}} \in \llbracket \phi \rrbracket_{0, +1}^{1000}$ .

Moreover, in Example 4.4 we observed that states  $q_{\text{ok}}$  and  $q_0$  are bisimilar with  $\bar{n} = 1001$  and  $\delta = 1/(N - 0 - \bar{n} + 2) = 1/99001$ , i.e.  $q_{\text{ok}} \sim_{\delta}^{\bar{n}} q_0$ .

In such case, the theorem ensures that  $q_0 \in \llbracket \phi \rrbracket_{1001/99001, +1}^{1000}$ , hence the real padlock can be considered unbreakable if we limit our attention to the first  $n = 1000$  steps, up to an error of  $1001/99001 \approx 0.010111$ . Finally, we note that such error is remarkably close to the least value that would still make  $q_0$  satisfy  $\phi$ , which we computed in Example 3.6 as  $n/N = 10^3/10^5 = 0.01$ .

In the rest of this section, we describe the general structure of the proof in a top-down fashion, leaving the detailed proof for Appendix A.

We prove the soundness theorem by induction on the state formula  $\phi$ , hence we also need to deal with path formulae  $\psi$ . Note that the statement of the theorem considers the image of the semantics of the state formula  $\phi$  w.r.t. bisimilarity (i.e.,  $\sim_{\delta}^{\bar{n}} (\llbracket \phi \rrbracket_{\delta', +1}^n)$ ). Analogously, to deal with path formulae we also need an analogous notion on sets of traces. To this purpose, we consider the set of traces in the definition of the semantics:  $T = \text{Cyl}(p) \cap \llbracket \psi \rrbracket_{\delta, r}^n$ . Then, given a state  $q$  bisimilar to  $p$ , we define the set of *pointwise bisimilar traces* starting from  $q$ , which we denote with  $\tilde{R}_{\delta, q}^n(T)$ . Technically, since  $\psi$  can only observe a finite portion of a trace, it is enough to define  $\tilde{R}_{\delta, q}^n(\tilde{T})$  on sets of *trace fragments*  $\tilde{T}$ .

**Definition 5.3.** Write  $F_{q_0}^n$  for the set of all trace fragments of length  $n$  starting from  $q_0$ . Assuming  $p \sim_{\delta}^n q$ , we define  $\tilde{R}_{\delta, q}^n : \mathcal{P}(F_p^n) \rightarrow \mathcal{P}(F_q^n)$  as follows:

$$\tilde{R}_{\delta, q}^n(\tilde{T}) = \{\tilde{u} \in F_q^n \mid \exists \tilde{t} \in \tilde{T}. \forall 0 \leq i < n. \tilde{t}(i) \sim_{\delta}^{n-i} \tilde{u}(i)\}$$

In particular, notice that  $F_q^1 = \{q\}$  (the trace fragment of length 1), and so:

$$\tilde{R}_{\delta, q}^1(\emptyset) = \emptyset \quad \tilde{R}_{\delta, q}^1(\{q\}) = \{q\}$$

The key inequality we exploit in the proof (Lemma 5.4) compares the probability of a set of trace fragments  $\tilde{T}$  starting from  $p$  to the one of the related set of trace fragments

$\tilde{R}_{\delta,q}^m(\tilde{T})$  starting from a  $q$  bisimilar to  $p$ . We remark that the component  $\bar{n}\delta$  in the error that appears in Theorem 5.1 results from the component  $m\delta$  appearing in the following lemma.

**Lemma 5.4.** *If  $p \sim_{\delta}^n q$  and  $\tilde{T}$  is a set of trace fragments of length  $m$ , with  $m \leq n$ , starting from  $p$ , then:*

$$\Pr(\tilde{T}) \leq \Pr(\tilde{R}_{\delta,q}^m(\tilde{T})) + m\delta$$

Lemma 5.4 allows  $\tilde{T}$  to be an infinite set (because the set of states  $\Omega$  can be infinite). We reduce this case to that in which  $\tilde{T}$  is finite. We first recall a basic calculus property: any inequality  $a \leq b$  can be proved by establishing instead  $a \leq b + \epsilon$  for all  $\epsilon > 0$ . Then, since the probability distribution of trace fragments of length  $m$  is discrete, for any  $\epsilon > 0$  we can always take a finite subset of the infinite set  $\tilde{T}$  whose probability differs from that of  $\tilde{T}$  less than  $\epsilon$ . It is then enough to consider the case in which  $\tilde{T}$  is finite, as done in the following lemma.

**Lemma 5.5.** *If  $p \sim_{\delta}^n q$  and  $\tilde{T}$  is a finite set of trace fragments of length  $n > 0$  starting from  $p$ , then:*

$$\Pr(\tilde{T}) \leq \Pr(\tilde{R}_{\delta,q}^n(\tilde{T})) + n\delta$$

We prove Lemma 5.5 by induction on  $n$ . In the inductive step, we partition the traces according to their first move, i.e., on their next state after  $p$  (for the trace fragments in  $T$ ) or  $q$  (for the bisimilar counterparts). A main challenge here is caused by the probabilities of such moves being weakly connected. Indeed, when  $p$  moves to  $p'$ , we might have several states  $q'$ , bisimilar to  $p'$ , such that  $q$  moves to  $q'$ . Worse, when  $p$  moves to another state  $p''$ , we might find that some of the states  $q'$  we met before are also bisimilar to  $p''$ . Such overlaps make it hard to connect the probability of  $p$  moves to that of  $q$  moves.

To overcome these issues, we exploit the technical lemma below. Let set  $A$  represent the  $p$  moves, and set  $B$  represent the  $q$  moves. Then, associate to each set element  $a \in A, b \in B$  a value  $(f_A(a), f_B(b))$  in the lemma) representing the move probability. The lemma ensures that each  $f_A(a)$  can be expressed as a weighted sum of  $f_B(b)$  for the elements  $b$  bisimilar to  $a$ . Here, the weights  $h(a, b)$  make it possible to relate a  $p$  move to a “weighted set” of  $q$  moves. Furthermore, the lemma ensures that no  $b \in B$  has been cumulatively used for more than a unit weight ( $\sum_{a \in A} h(a, b) \leq 1$ ).

**Lemma 5.6.** *Let  $A$  be a finite set and  $B$  be a countable set, equipped with functions  $f_A : A \rightarrow \mathbb{R}_0^+$  and  $f_B : B \rightarrow \mathbb{R}_0^+$ . Let  $g : A \rightarrow 2^B$  be such that  $\sum_{b \in g(a)} f_B(b)$  converges for all  $a \in A$ . If, for all  $A' \subseteq A$ :*

$$\sum_{a \in A'} f_A(a) \leq \sum_{b \in \bigcup_{a \in A'} g(a)} f_B(b) \quad (5.1)$$

*then there exists  $h : A \times B \rightarrow [0, 1]$  such that:*

$$\forall b \in B : \sum_{a \in A} h(a, b) \leq 1 \quad (5.2)$$

$$\forall A' \subseteq A : \sum_{a \in A'} f_A(a) = \sum_{a \in A'} \sum_{b \in g(a)} h(a, b) f_B(b) \quad (5.3)$$

We visualize Lemma 5.6 in Figure 4 through an example. The leftmost graph shows a finite set  $A = \{a_1, a_2, a_3\}$  where each  $a_i$  is equipped with its associated value  $f_A(a_i)$  and,

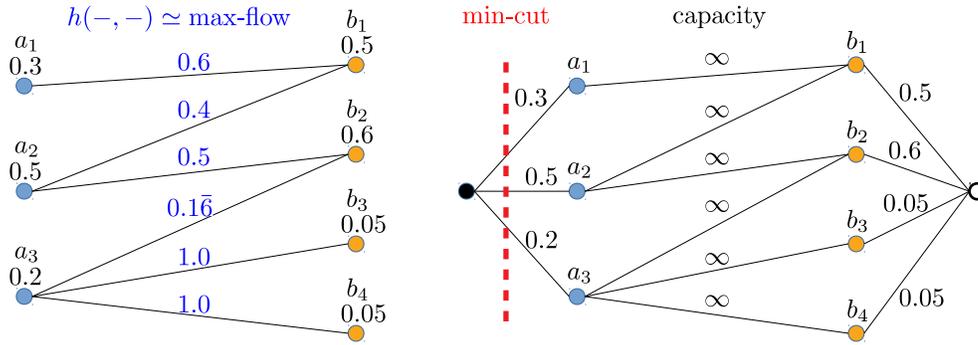


Figure 4: Graphical representation of Lemma 5.6 (left) and its proof (right).

similarly, a finite set  $B = \{b_1, \dots, b_4\}$  where each  $b_i$  has its own value  $f_B(b_i)$ . The function  $g$  is rendered as the edges of the graph, connecting each  $a_i$  with all  $b_j \in g(a_i)$ .

The graph satisfies the hypotheses, as one can easily verify. For instance, when  $A' = \{a_1, a_2\}$  inequality (5.1) simplifies to  $0.3 + 0.5 \leq 0.5 + 0.6$ . The thesis ensures the existence of a weight function  $h(-, -)$  whose values are shown in the graph on the left over each edge.

These values indeed satisfy (5.2): for instance, if we pick  $b = b_2$  the inequality reduces to  $0.5 + 0.1\bar{6} \leq 1$ . Furthermore, (5.3) is also satisfied: for instance, taking  $A' = \{a_2\}$  the equation reduces to  $0.5 = 0.4 \cdot 0.5 + 0.5 \cdot 0.6$ , while taking  $A' = \{a_3\}$  the equation reduces to  $0.2 = 0.1\bar{6} \cdot 0.6 + 1.0 \cdot 0.05 + 1.0 \cdot 0.05$ .

The rightmost graph in Figure 4 instead sketches how our proof devises the desired weight function  $h$ , by constructing a network flow problem, and exploiting the well-known min-cut/max-flow theorem [DF55], following the approach of [Bai98]. We start by adding a source node to the right (white bullet in the figure), connected to nodes in  $B$ , and a sink node to the left, connected to nodes in  $A$ . We write the capacity over each edge: we use  $f_B(b_i)$  for the edges connected to the source,  $f_A(a_i)$  for the edges connected to the sink, and  $+\infty$  for the other edges in the middle.

Then, we argue that the leftmost cut  $C$  shown in the figure is a min-cut. Intuitively, if we take another cut  $C'$  not including some edge in  $C$ , then  $C'$  has to include other edges making  $C'$  not any better than  $C$ . Indeed,  $C'$  can surely not include any edge in the middle, since they have  $+\infty$  capacity. Therefore, if  $C'$  does not include an edge from some  $a_i$  to the sink, it has to include all the edges from the source to each  $b_j \in g(a_i)$ . In this case, hypothesis (5.1) ensures that doing so does not lead to a better cut. Hence,  $C$  is indeed a min-cut.

From the max-flow corresponding to the min-cut, we derive the values for  $h(-, -)$ . Thesis (5.2) follows from the flow conservation law on each  $b_i$ , and the fact that the incoming flow of each  $b_j$  from the source is bounded by the capacity of the related edge. Thesis (5.3) follows from the flow conservation law on each  $a_i$ , and the fact that the outgoing flow of each  $a_i$  to the sink is exactly the capacity of the related edge, since the edge is on a min-cut.

## 6. ASYMPTOTIC EQUIVALENCE

In this section we transport the notion of bisimilarity and the semantics of PCTL to *families* of states, thus reasoning on their asymptotic behaviours. More precisely, given a state-labelled DTMC  $\mathcal{Q}$ , we define a family of states to be an infinite sequence  $\Xi : \mathbb{N} \rightarrow \mathcal{Q}$ . Intuitively,  $\Xi(\eta)$  can describe the behaviour of a probabilistic system depending on a security parameter  $\eta \in \mathbb{N}$ .

When using bisimilarity (Definition 4.1) to relate two given states  $Q_1$  and  $Q_2$ , we have to provide a number of steps  $n$  and a probability error  $\delta$ . By contrast, when relating two families  $\Xi_1$  and  $\Xi_2$  we want to focus on their asymptotic behaviour, and obtain an equivalence that does not depend on specific values of  $n$  and  $\delta$ . To do so, we start by recalling the standard definition of *negligible function*:

**Definition 6.1** (Negligible Function). A function  $f : \mathbb{N} \rightarrow \mathbb{R}$  is said to be negligible whenever

$$\forall c \in \mathbb{N}. \exists \bar{\eta}. \forall \eta \geq \bar{\eta}. |f(\eta)| \leq \eta^{-c}$$

We say that  $\Xi_1$  and  $\Xi_2$  are asymptotically equivalent ( $\Xi_1 \equiv \Xi_2$ ) when the families are asymptotically pointwise bisimilar with a negligible error  $\delta(\eta)$  whenever  $n(\eta)$  is a polynomial.

**Definition 6.2** (Asymptotic Equivalence). Given  $\Xi_1, \Xi_2 : \mathbb{N} \rightarrow \mathcal{Q}$ , we write  $\Xi_1 \equiv \Xi_2$  if and only if for each polynomial  $n(-)$  there exists a negligible function  $\delta(-)$  and  $\bar{\eta} \in \mathbb{N}$  such that for all  $\eta \geq \bar{\eta}$  we have  $\Xi_1(\eta) \sim_{\delta(\eta)}^{n(\eta)} \Xi_2(\eta)$

**Lemma 6.3.**  $\equiv$  is an equivalence relation.

*Proof.* Reflexivity and symmetry are trivial. For transitivity, given a polynomial  $n(-)$ , let  $\delta_1(-), \delta_2(-)$  be the negligible functions resulting from the hypotheses  $\Xi_1 \equiv \Xi_2$  and  $\Xi_2 \equiv \Xi_3$ , respectively. Asymptotically, we obtain

$$\Xi_1(\eta) \sim_{\delta_1(\eta)}^{n(\eta)} \Xi_2(\eta) \quad \wedge \quad \Xi_2(\eta) \sim_{\delta_2(\eta)}^{n(\eta)} \Xi_3(\eta)$$

By the transitivity of  $\sim$ , we get

$$\Xi_1(\eta) \sim_{\delta_1(\eta) + \delta_2(\eta)}^{n(\eta)} \Xi_3(\eta)$$

Hence we obtain the thesis since the sum of negligible functions  $\delta_1(\eta) + \delta_2(\eta)$  is negligible.  $\square$

We now provide an asymptotic semantics for PCTL, by defining its satisfaction relation  $\Xi \models \phi$ . As done above, this notion does not depend on specific values for  $n$  and  $\delta$  (unlike the semantics in Definition 3.4), but instead considers the asymptotic behaviour of the family.

**Definition 6.4** (Asymptotic Satisfaction Relation). We write  $\Xi \models \phi$  when there exists a polynomial  $\bar{n}(-)$  such that for each polynomial  $n(-) \geq \bar{n}(-)$  there exists a negligible function  $\delta(-)$  and  $\bar{\eta} \in \mathbb{N}$  such that for all  $\eta \geq \bar{\eta}$  we have  $\Xi(\eta) \in \llbracket \phi \rrbracket_{\delta(\eta), +1}^{n(\eta)}$

In the above definition, we only consider polynomials greater than a threshold  $\bar{n}(-)$ . This is because a family  $\Xi$  representing, say, a protocol could require a given (polynomial) number of steps to complete its execution. It is reasonable, for instance, that  $\Xi(\eta)$  needs to exchange  $\eta^2$  messages over a network to perform its task. In such cases, we still want to make  $\Xi$  satisfy a formula  $\phi$  stating that the task is eventually completed with high probability. If we quantified over all polynomials  $n(-)$ , we would also allow choosing small polynomials like  $n(\eta) = \eta$  or even  $n(\eta) = 1$ , which would not provide  $\Xi$  enough time to complete. Using a (polynomial) threshold  $\bar{n}(-)$ , instead, we always provide enough time.

We now establish the main result of this section, asymptotic soundness, stating that equivalent families of states asymptotically satisfy the same PCTL formulae. The proof relies on our previous soundness Theorem 5.1.

**Theorem 6.5** (Asymptotic Soundness). *Let  $\Xi_1, \Xi_2$  be families of states such that  $\Xi_1 \equiv \Xi_2$ . For every PCTL formula  $\phi$ :*

$$\Xi_1 \models \phi \iff \Xi_2 \models \phi$$

*Proof.* Assuming  $\Xi_1 \models \phi$  and  $\Xi_1 \equiv \Xi_2$ , we prove  $\Xi_2 \models \phi$ . Let  $k_X = \mathsf{X}_{max}(\phi)$  be the maximum  $\mathsf{X}$ -nesting of  $\phi$ , and let  $k_U = \mathsf{U}_{max}(\phi)$  be the maximum  $\mathsf{U}$ -nesting of  $\phi$ .

Let  $\bar{n}_1(-)$  as in the definition of the hypothesis  $\Xi_1 \models \phi$ . To prove the thesis  $\Xi_2 \models \phi$ , we choose  $\bar{n}_2(-) = \bar{n}_1(-)$ , and we consider an arbitrary  $n_2(-) \geq \bar{n}_2(-) = \bar{n}_1(-)$ . We can then choose  $n_1(-) = n_2(-)$  in the same hypothesis, and obtain a negligible  $\delta_1(-)$  and  $\bar{\eta}_1$ , where for any  $\eta \geq \bar{\eta}_1$  we have

$$\Xi_1(\eta) \in \llbracket \phi \rrbracket_{\delta_1(\eta), +1}^{n_2(\eta)} \quad (6.1)$$

We now exploit the other hypothesis  $\Xi_1 \equiv \Xi_2$ , choosing the polynomial

$$n(\eta) = n_2(\eta) \cdot k_U + k_X + 1 \quad (6.2)$$

and obtaining a negligible  $\delta(-)$  and  $\bar{\eta}$  where for any  $\eta \geq \bar{\eta}$  we have

$$\Xi_1(\eta) \sim_{\delta(\eta)}^{n(\eta)} \Xi_2(\eta) \quad (6.3)$$

To prove the thesis, we finally choose the negligible function  $\delta_2(\eta) = n(\eta) \cdot \delta(\eta) + \delta_1(\eta)$  and  $\bar{\eta}_2 = \max(\bar{\eta}_1, \bar{\eta})$ . By Theorem 5.1 we have that for any  $\eta \geq \bar{\eta}_2$ :

$$\sim_{\delta(\eta)}^{n(\eta)} (\llbracket \phi \rrbracket_{\delta_1(\eta), +1}^{n_2(\eta)}) \subseteq \llbracket \phi \rrbracket_{n(\eta) \cdot \delta(\eta) + \delta_1(\eta), +1}^{n_2(\eta)} \quad \text{where } n(\eta) \text{ is as in (6.2).}$$

Applying this to (6.1) and (6.3) we then have that, for any  $\eta \geq \bar{\eta}_2$ :

$$\Xi_2(\eta) \in \llbracket \phi \rrbracket_{n(\eta) \cdot \delta(\eta) + \delta_1(\eta), +1}^{n_2(\eta)}$$

which is our thesis

$$\Xi_2(\eta) \in \llbracket \phi \rrbracket_{\delta_2(\eta), +1}^{n_2(\eta)} \quad \square$$

**Example 6.6.** We now return to the padlock examples 3.6 and 4.4. We again consider an ideal padlock modelled by a state  $q_{ok}$ , but also a sequence of padlocks having an increasing number of digits  $\eta$ , hence an increasing number  $N = 10^\eta$  of combinations. We assume that state  $q_{i,10^\eta}$  models the state of a padlock having  $\eta$  digits where the adversary has already made  $i$  brute force attempts, following the same strategy as in the previous examples. The transition probabilities are also similarly defined.

In this scenario, we can define two state families. Family  $\Xi_1(\eta) = q_{ok}$  represents a (constant) sequence of ideal padlocks, while family  $\Xi_2(\eta) = q_{0,10^\eta}$  represents a sequence of realistic padlocks with no previous brute force attempt ( $i = 0$ ), in increasing order of robustness. Indeed, as  $\eta$  increases, the padlock becomes harder to break by brute force since the number of combinations  $N = 10^\eta$  grows.

In Example 4.4, we have seen that

$$\Xi_1(\eta) \sim_{\delta(\eta)}^{n(\eta)} \Xi_2(\eta) \quad \text{where } \delta(\eta) = \frac{1}{N - 0 - n(\eta) + 2} = \frac{1}{10^\eta - n(\eta) + 2}$$

and we can observe that the above  $\delta(\eta)$  is indeed negligible when  $n(\eta)$  is a polynomial. This means that  $\Xi_1 \equiv \Xi_2$  holds, hence we can apply Theorem 6.5 and conclude that the families

$\Xi_1$  and  $\Xi_2$  asymptotically satisfy the same PCTL formulae. This is intuitive since, when the adversary can only attempt a polynomial number of brute force attacks, and when the number of combinations increases exponentially, the robustness of the realistic padlocks effectively approaches that of the ideal one.

We now discuss how Theorem 6.5 could be applied to a broad class of systems. Consider the execution of an ideal cryptographic protocol, modelled as a DTMC starting from the initial state  $q_i$ . This model could represent, for instance, the semantics of a formal, symbolic system such as those that can be expressed using process algebras. In this scenario, the underlying cryptographic primitives can be *perfect*, in the sense that ciphertexts reveal no information to whom does not know the decryption key, signatures can never be forged, hash preimages can never be found, and so on, despite the amount of computational resources available to the adversary.

Given such a model, it is then possible to refine it making the cryptographic primitives more realistic, allowing an adversary to attempt attacks such as decryptions and signature forgeries, which however succeed only with negligible probability w.r.t. a security parameter  $\eta$ . This more realistic system can be modelled using a distinct DTMC state  $q_r^\eta$  whose behaviour is similar to that of  $q_i$ : the state transitions are essentially the same, except for the cases in which the adversary is successful in attacking the cryptographic primitives. Therefore, the transition probabilities are almost the same, differing only by a negligible quantity.

Therefore, we can let  $\Xi_1(\eta) = q_i$  and  $\Xi_2(\eta) = q_r^\eta$ , and observe that they are indeed asymptotically equivalent. Note that this holds in general by construction, no matter what is the behaviour of the ideal system  $q_i$  we started from.

Finally, by Theorem 6.5 we can claim that both families  $\Xi_1, \Xi_2$  asymptotically satisfy the same PCTL formulas. This makes it possible, in general, to prove properties on the simpler  $q_i$  system, possibly even using some automatic verification tools, and transfer these results in the more realistic setting  $q_r^\eta$ .

A special case of this fact was originally studied in [ZD05], which however only considered reachability properties. By comparison, Theorem 6.5 is much more general, allowing one to transfer any property that can be expressed using a PCTL formula.

The construction above allows one to refine an ideal system  $q_i$  into a more realistic one  $q_r^\eta$  by taking certain adversaries into account. However, if our goal were to study the security of the system against *all* reasonable adversaries, then the above approach would not be applicable. Indeed, it is easy to find an ideal system and a corresponding realistic refinement, comprising a reasonable adversary, where the asymptotic equivalence does not hold. For instance, consider an ideal protocol where Alice and Bob exchange ten messages, after which Alice randomly chooses and exchanges a single bit. To assess the security of a realistic implementation, we might want to consider the case where Alice is an adversary. In such case, a malicious Alice could exchange the first two messages, then flip a coin  $b \leftarrow \{0, 1\}$  in secret, exchange the other eight messages, and finally send the value  $b$ . The behaviour of such realistic system differs from the ideal one, since the ideal one has a probabilistic choice point only at the end, while the realistic system anticipates it after the first two moves. It is easy to check (and well known) that moving choices to an earlier point makes standard bisimilarity fail, and this is the case also for asymptotic equivalence. The failure of asymptotic equivalence prevents us from applying the asymptotic soundness theorem. In particular, assume that we have proved that the ideal system enjoys certain specifications

expressed as PCTL formulae. We can not exploit the theorem to show that also the realistic system with the adversary enjoys the same specifications.

## 7. CONCLUSIONS

In this paper we studied how the (relaxed) semantics of PCTL formulae interacts with (approximate) probabilistic bisimulation. In the regular, non relaxed case, it is well-known that when a state  $q$  satisfies a PCTL formula  $\phi$ , then all the states that are probabilistic-bisimilar to  $q$  also satisfy  $\phi$  ([DGJP10]). Theorem 5.1 extends this to the relaxed semantics, establishing that when a state  $q$  satisfies a PCTL formula  $\phi$  up-to  $n$  steps and error  $\delta$ , then all the states that are approximately probabilistic bisimilar to  $q$  with error  $\delta'$  (and enough steps) also satisfy  $\phi$  up-to  $n$  steps and suitably increased error. We provide a way to compute the new error in terms of  $n, \delta, \delta'$ . Theorem 6.5 extends such soundness result to the asymptotic behaviour where the error becomes negligible when the number of steps is polynomially bounded.

Our results are a first step towards a novel approach to the security analysis of cryptographic protocols using probabilistic bisimulations. When one is able to prove that a real-world specification of a cryptographic protocol is asymptotically equivalent to an ideal one, then one can invoke Theorem 6.5 and claim that the two models satisfy the same PCTL formulae, essentially reducing the security proof of the cryptographic protocol to verifying the ideal model. A relevant line for future work is to study the applicability of our theory in this setting. As discussed in section 6, our approach is not applicable to all protocols and all adversaries. A relevant line of research could be the study of larger asymptotic equivalences, which allow to transfer properties from ideal to realistic systems. This could be achieved, e.g., by considering weaker logics than PCTL, or moving to linear temporal logics.

Another possible line of research would be investigating proof techniques for establishing approximate bisimilarity and refinement [JL91], as well as devising algorithms for approximate bisimilarity, along the lines of [vBW14, CvBW12, Fu12, TvB16, TvB17, TvB18]. This direction, however, would require restricting our theory to finite-state systems, which contrasts with our general motivation coming from cryptographic security. Indeed, in the analysis of cryptographic protocols, security is usually to be proven against an arbitrary adversary, hence also against infinite-state ones. Hence, model-checking of finite-state systems would not directly be applicable in this setting.

**Acknowledgements.** Massimo Bartoletti is partially supported by Conv. Fondazione di Sardegna & Atenei Sardi project F75F21001220007 *ASTRID*. Maurizio Murgia and Roberto Zunino are partially supported PON *Distributed Ledgers for Secure Open Communities*. Maurizio Murgia is partially supported by MUR PON REACT EU DM 1062/21.

## REFERENCES

- [BA17] Gaoang Bian and Alessandro Abate. On the relationship between bisimulation and trace equivalence in an approximate probabilistic context. In Javier Esparza and Andrzej S. Murawski, editors, *Foundations of Software Science and Computation Structures (FOSSACS)*, volume 10203 of *LNCS*, pages 321–337, 2017. doi:10.1007/978-3-662-54458-7\_19.
- [Bai98] Christel Baier. Algorithmic verification methods for probabilistic systems. Habilitation Thesis, Universität Mannheim, 1998. URL: [https://www.inf.tu-dresden.de/content/institutes/thi/algi/publikationen/texte/15\\_98.pdf](https://www.inf.tu-dresden.de/content/institutes/thi/algi/publikationen/texte/15_98.pdf).

- [BBL<sup>+</sup>21] Giorgio Bacci, Giovanni Bacci, Kim G. Larsen, Radu Mardare, Qiyi Tang, and Franck van Breugel. Computing probabilistic bisimilarity distances for probabilistic automata. *Log. Methods Comput. Sci.*, 17(1), 2021.
- [BK08] Christel Baier and Joost-Pieter Katoen. *Principles of model checking*. MIT Press, 2008.
- [BMZ22] Massimo Bartoletti, Maurizio Murgia, and Roberto Zunino. A sound up-to-n,  $\delta$  bisimilarity for PCTL. In Maurice H. ter Beek and Marjan Sirjani, editors, *Coordination Models and Languages (COORDINATION) 2022*, volume 13271 of *Lecture Notes in Computer Science*, pages 35–52. Springer, 2022. doi:10.1007/978-3-031-08143-9\_3.
- [CGT16] Valentina Castiglioni, Daniel Gebler, and Simone Tini. Logical characterization of bisimulation metrics. In *Workshop on Quantitative Aspects of Programming Languages and Systems (QAPL)*, volume 227 of *EPTCS*, pages 44–62, 2016. doi:10.4204/EPTCS.227.4.
- [CvBW12] Di Chen, Franck van Breugel, and James Worrell. On the complexity of computing probabilistic bisimilarity. In Lars Birkedal, editor, *Foundations of Software Science and Computational Structures (FOSSACS)*, volume 7213 of *LNCS*, pages 437–451. Springer, 2012. doi:10.1007/978-3-642-28729-9\_29.
- [dAHM03] Luca de Alfaro, Thomas A. Henzinger, and Rupak Majumdar. Discounting the future in systems theory. In *International Colloquium on Automata, Languages and Programming (ICALP)*, volume 2719 of *LNCS*, pages 1022–1037. Springer, 2003. doi:10.1007/3-540-45061-0\_79.
- [DAK12] Alessandro D’Innocenzo, Alessandro Abate, and Joost-Pieter Katoen. Robust PCTL model checking. In Thao Dang and Ian M. Mitchell, editors, *Hybrid Systems: Computation and Control (HSCC)*, pages 275–286. ACM, 2012. doi:10.1145/2185632.2185673.
- [dAMRS08] Luca de Alfaro, Rupak Majumdar, Vishwanath Raman, and Mariëlle Stoelinga. Game refinement relations and metrics. *Log. Methods Comput. Sci.*, 4(3), 2008.
- [DCPP06] Yuxin Deng, Tom Chothia, Catuscia Palamidessi, and Jun Pang. Metrics for action-labelled quantitative transition systems. *Electron. Notes Theor. Comput. Sci.*, 153(2):79–96, 2006. doi:10.1016/j.entcs.2005.10.033.
- [DEP02] Josée Desharnais, Abbas Edalat, and Prakash Panangaden. Bisimulation for labelled Markov processes. *Inf. Comput.*, 179(2):163–193, 2002. doi:10.1006/inco.2001.2962.
- [DF55] George Bernard Dantzig and D. R. Fulkerson. *On the Max Flow Min Cut Theorem of Networks*. RAND Corporation, Santa Monica, CA, 1955.
- [DGJP99] Josée Desharnais, Vineet Gupta, Radha Jagadeesan, and Prakash Panangaden. Metrics for labeled Markov systems. In *CONCUR*, volume 1664 of *LNCS*, pages 258–273. Springer, 1999.
- [DGJP04] Josée Desharnais, Vineet Gupta, Radha Jagadeesan, and Prakash Panangaden. Metrics for labelled Markov processes. *Theor. Comput. Sci.*, 318(3):323–354, 2004. doi:10.1016/j.tcs.2003.09.013.
- [DGJP10] Josée Desharnais, Vineet Gupta, Radha Jagadeesan, and Prakash Panangaden. Weak bisimulation is sound and complete for pCTL\*. *Inf. Comput.*, 208(2):203–219, 2010. doi:10.1016/j.ic.2009.11.002.
- [DLT08] Josée Desharnais, François Laviolette, and Mathieu Tracol. Approximate analysis of probabilistic processes: Logic, simulation and games. In *Quantitative Evaluation of Systems (QEST)*, pages 264–273. IEEE Computer Society, 2008. doi:10.1109/QEST.2008.42.
- [FMM20] Robert Furber, Radu Mardare, and Matteo Mio. Probabilistic logics based on Riesz spaces. *Log. Methods Comput. Sci.*, 16(1), 2020. doi:10.23638/LMCS-16(1:6)2020.
- [Fu12] Hongfei Fu. Computing game metrics on Markov decision processes. In Artur Czumaj, Kurt Mehlhorn, Andrew M. Pitts, and Roger Wattenhofer, editors, *Automata, Languages, and Programming (ICALP)*, volume 7392 of *LNCS*, pages 227–238. Springer, 2012. doi:10.1007/978-3-642-31585-5\_23.
- [GJS90] Alessandro Giacalone, Chi-Chang Jou, and Scott A. Smolka. Algebraic reasoning for probabilistic concurrent systems. In Manfred Broy and Cliff B. Jones, editors, *Programming concepts and methods: Proceedings of the IFIP Working Group 2.2, 2.3 Working Conference on Programming Concepts and Methods*, pages 443–458. North-Holland, 1990.
- [GSS92] Jean-Yves Girard, Andre Scedrov, and Philip J. Scott. Bounded linear logic: A modular approach to polynomial-time computability. *Theor. Comput. Sci.*, 97(1):1–66, 1992.
- [HJ94] Hans Hansson and Bengt Jonsson. A logic for reasoning about time and reliability. *Formal Aspects Comput.*, 6(5):512–535, 1994. doi:10.1007/BF01211866.

- [HPS<sup>+</sup>11] Holger Hermanns, Augusto Parma, Roberto Segala, Björn Wachter, and Lijun Zhang. Probabilistic logical characterization. *Inf. Comput.*, 209(2):154–172, 2011. doi:10.1016/j.ic.2010.11.024.
- [JL91] Bengt Jonsson and Kim Guldstrand Larsen. Specification and refinement of probabilistic processes. In *IEEE Symp. on Logic in Computer Science (LICS)*, pages 266–277. IEEE Computer Society Press, 1991.
- [LG16] Ugo Dal Lago and Paolo Di Giamberardino. On session types and polynomial time. *Math. Struct. Comput. Sci.*, 26(8):1433–1458, 2016.
- [LG22] Ugo Dal Lago and Giulia Giusti. On session typing, probabilistic polynomial time, and cryptographic experiments. In *CONCUR*, volume 243 of *LIPICs*, pages 37:1–37:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.
- [LS89] Kim Guldstrand Larsen and Arne Skou. Bisimulation through probabilistic testing. In *ACM Symposium on Principles of Programming Languages (POPL)*, pages 344–352. ACM Press, 1989. doi:10.1145/75277.75307.
- [LS91] Kim Guldstrand Larsen and Arne Skou. Bisimulation through probabilistic testing. *Inf. Comput.*, 94(1):1–28, 1991. doi:10.1016/0890-5401(91)90030-6.
- [Mio14] Matteo Mio. Upper-expectation bisimilarity and Lukasiewicz  $\mu$ -calculus. In *Foundations of Software Science and Computation Structures (FOSSACS)*, volume 8412 of *LNCS*, pages 335–350. Springer, 2014. doi:10.1007/978-3-642-54830-7\_22.
- [Mio18] Matteo Mio. Riesz modal logic with threshold operators. In Anuj Dawar and Erich Grädel, editors, *ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 710–719. ACM, 2018. doi:10.1145/3209108.3209118.
- [MS17] Matteo Mio and Alex Simpson. Lukasiewicz  $\mu$ -calculus. *Fundam. Informaticae*, 150(3-4):317–346, 2017. doi:10.3233/FI-2017-1472.
- [SZGN13] Lei Song, Lijun Zhang, Jens Chr. Godskesen, and Flemming Nielson. Bisimulations meet PCTL equivalences for probabilistic automata. *Logical Methods in Computer Science*, 9(2), 2013. doi:10.2168/LMCS-9(2:7)2013.
- [TvB16] Qiyi Tang and Franck van Breugel. Computing probabilistic bisimilarity distances via policy iteration. In *International Conference on Concurrency Theory (CONCUR)*, volume 59 of *LIPICs*, pages 22:1–22:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016. doi:10.4230/LIPICs.CONCUR.2016.22.
- [TvB17] Qiyi Tang and Franck van Breugel. Algorithms to compute probabilistic bisimilarity distances for labelled Markov chains. In *International Conference on Concurrency Theory (CONCUR)*, volume 85 of *LIPICs*, pages 27:1–27:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017. doi:10.4230/LIPICs.CONCUR.2017.27.
- [TvB18] Qiyi Tang and Franck van Breugel. Deciding probabilistic bisimilarity distance one for labelled Markov chains. In *Computer Aided Verification (CAV)*, volume 10981 of *LNCS*, pages 681–699. Springer, 2018. doi:10.1007/978-3-319-96145-3\_39.
- [vB17] Franck van Breugel. Probabilistic bisimilarity distances. *ACM SIGLOG News*, 4(4):33–51, 2017.
- [vBHMW05] Franck van Breugel, Claudio Hermida, Michael Makkai, and James Worrell. An accessible approach to behavioural pseudometrics. In *Automata, Languages and Programming (ICALP)*, volume 3580 of *LNCS*, pages 1018–1030. Springer, 2005. doi:10.1007/11523468\_82.
- [vBSW08] Franck van Breugel, Babita Sharma, and James Worrell. Approximating a behavioural pseudometric without discount for probabilistic systems. *Log. Methods Comput. Sci.*, 4(2), 2008. doi:10.2168/LMCS-4(2:2)2008.
- [vBW05] Franck van Breugel and James Worrell. A behavioural pseudometric for probabilistic transition systems. *Theor. Comput. Sci.*, 331(1):115–142, 2005. doi:10.1016/j.tcs.2004.09.035.
- [vBW14] Franck van Breugel and James Worrell. The complexity of computing a bisimilarity pseudometric on probabilistic automata. In *Horizons of the Mind. A Tribute to Prakash Panangaden*, volume 8464 of *LNCS*, pages 191–213. Springer, 2014. doi:10.1007/978-3-319-06880-0\_10.
- [ZD05] Roberto Zunino and Pierpaolo Degano. Weakening the perfect encryption assumption in Dolev-Yao adversaries. *Theor. Comput. Sci.*, 340(1):154–178, 2005.

## APPENDIX A. PROOFS

**Proof of Lemma 3.5.** We simultaneously prove the whole statement by induction on the structure of the formulae  $\phi$  and  $\psi$ . The cases  $\phi = l$  and  $\phi = \text{true}$  result in trivial equalities. For the case  $\phi = \neg\phi'$  we need to prove

$$\begin{aligned} \llbracket \neg\phi' \rrbracket_{\delta,+1}^n &\subseteq \llbracket \neg\phi' \rrbracket_{\delta',+1}^n \\ \llbracket \neg\phi' \rrbracket_{\delta',-1}^n &\subseteq \llbracket \neg\phi' \rrbracket_{\delta,-1}^n \\ \llbracket \neg\phi' \rrbracket_{\delta,-1}^n &\subseteq \llbracket \neg\phi' \rrbracket_{\delta,+1}^n \end{aligned}$$

which is equivalent to

$$\begin{aligned} \mathcal{Q} \setminus \llbracket \phi' \rrbracket_{\delta,-1}^n &\subseteq \mathcal{Q} \setminus \llbracket \phi' \rrbracket_{\delta',-1}^n \\ \mathcal{Q} \setminus \llbracket \phi' \rrbracket_{\delta',+1}^n &\subseteq \mathcal{Q} \setminus \llbracket \phi' \rrbracket_{\delta,+1}^n \\ \mathcal{Q} \setminus \llbracket \phi' \rrbracket_{\delta,+1}^n &\subseteq \mathcal{Q} \setminus \llbracket \phi' \rrbracket_{\delta,-1}^n \end{aligned}$$

which, in turn, is equivalent to

$$\begin{aligned} \llbracket \phi' \rrbracket_{\delta',-1}^n &\subseteq \llbracket \phi' \rrbracket_{\delta,-1}^n \\ \llbracket \phi' \rrbracket_{\delta,+1}^n &\subseteq \llbracket \phi' \rrbracket_{\delta',+1}^n \\ \llbracket \phi' \rrbracket_{\delta,-1}^n &\subseteq \llbracket \phi' \rrbracket_{\delta,+1}^n \end{aligned}$$

which is the induction hypothesis.

For the case  $\phi = \phi_1 \wedge \phi_2$  we need to prove

$$\begin{aligned} \llbracket \phi_1 \wedge \phi_2 \rrbracket_{\delta,+1}^n &\subseteq \llbracket \phi_1 \wedge \phi_2 \rrbracket_{\delta',+1}^n \\ \llbracket \phi_1 \wedge \phi_2 \rrbracket_{\delta',-1}^n &\subseteq \llbracket \phi_1 \wedge \phi_2 \rrbracket_{\delta,-1}^n \\ \llbracket \phi_1 \wedge \phi_2 \rrbracket_{\delta,-1}^n &\subseteq \llbracket \phi_1 \wedge \phi_2 \rrbracket_{\delta,+1}^n \end{aligned}$$

which is equivalent to

$$\begin{aligned} \llbracket \phi_1 \rrbracket_{\delta,+1}^n \cap \llbracket \phi_2 \rrbracket_{\delta,+1}^n &\subseteq \llbracket \phi_1 \rrbracket_{\delta',+1}^n \cap \llbracket \phi_2 \rrbracket_{\delta',+1}^n \\ \llbracket \phi_1 \rrbracket_{\delta',-1}^n \cap \llbracket \phi_2 \rrbracket_{\delta',-1}^n &\subseteq \llbracket \phi_1 \rrbracket_{\delta,-1}^n \cap \llbracket \phi_2 \rrbracket_{\delta,-1}^n \\ \llbracket \phi_1 \rrbracket_{\delta,-1}^n \cap \llbracket \phi_2 \rrbracket_{\delta,-1}^n &\subseteq \llbracket \phi_1 \rrbracket_{\delta,+1}^n \cap \llbracket \phi_2 \rrbracket_{\delta,+1}^n \end{aligned}$$

which immediately follows from the induction hypothesis on  $\phi_1$  and  $\phi_2$ . For the case  $\phi = \text{Pr}_{\triangleright\pi}[\psi]$  we need to prove

$$\begin{aligned} \llbracket \text{Pr}_{\triangleright\pi}[\psi] \rrbracket_{\delta,+1}^n &\subseteq \llbracket \text{Pr}_{\triangleright\pi}[\psi] \rrbracket_{\delta',+1}^n \\ \llbracket \text{Pr}_{\triangleright\pi}[\psi] \rrbracket_{\delta',-1}^n &\subseteq \llbracket \text{Pr}_{\triangleright\pi}[\psi] \rrbracket_{\delta,-1}^n \\ \llbracket \text{Pr}_{\triangleright\pi}[\psi] \rrbracket_{\delta,-1}^n &\subseteq \llbracket \text{Pr}_{\triangleright\pi}[\psi] \rrbracket_{\delta,+1}^n \end{aligned}$$

The first inclusion follows from

$$\begin{aligned} \llbracket \text{Pr}_{\triangleright\pi}[\psi] \rrbracket_{\delta,+1}^n &= \{q \in \mathcal{Q} \mid \text{Pr}(\text{Cyl}(q) \cap \llbracket \psi \rrbracket_{\delta,+1}^n) + \delta \triangleright \pi\} \\ &\subseteq \{q \in \mathcal{Q} \mid \text{Pr}(\text{Cyl}(q) \cap \llbracket \psi \rrbracket_{\delta',+1}^n) + \delta' \triangleright \pi\} \\ &= \llbracket \text{Pr}_{\triangleright\pi}[\psi] \rrbracket_{\delta',+1}^n \end{aligned}$$

where we exploited  $\delta \leq \delta'$ , the induction hypothesis  $\llbracket \psi \rrbracket_{\delta,+1}^n \subseteq \llbracket \psi \rrbracket_{\delta',+1}^n$ , the monotonicity of  $\Pr(-)$ , and the fact that  $\geq \circ \triangleright \subseteq \triangleright$ . The second inclusion follows from an analogous argument:

$$\begin{aligned} \llbracket \Pr_{\triangleright \pi}[\psi] \rrbracket_{\delta',-1}^n &= \{q \in \mathcal{Q} \mid \Pr(\text{Cyl}(q) \cap \llbracket \psi \rrbracket_{\delta',-1}^n) - \delta' \triangleright \pi\} \\ &\subseteq \{q \in \mathcal{Q} \mid \Pr(\text{Cyl}(q) \cap \llbracket \psi \rrbracket_{\delta,-1}^n) - \delta \triangleright \pi\} \\ &= \llbracket \Pr_{\triangleright \pi}[\psi] \rrbracket_{\delta,-1}^n \end{aligned}$$

where we exploited  $-\delta' \leq -\delta$ , the induction hypothesis  $\llbracket \psi \rrbracket_{\delta',-1}^n \subseteq \llbracket \psi \rrbracket_{\delta,-1}^n$ , the monotonicity of  $\Pr(-)$ , and the fact that  $\geq \circ \triangleright \subseteq \triangleright$ .

For  $\psi = X\phi$ , we can observe that  $\llbracket X\phi \rrbracket_{\delta,r}^n = f(\llbracket \phi \rrbracket_{\delta,r}^n)$  where  $f$  is a monotonic function mapping sets of states to sets of traces, which does not depend on  $\delta, r, n$ . Hence, the thesis follows from the set inclusions about the semantics of  $\phi$  in the induction hypothesis.

Similarly, for  $\psi = \phi_1 \cup \phi_2$ , we can observe that  $\llbracket \phi_1 \cup \phi_2 \rrbracket_{\delta,r}^n = g_n(\llbracket \phi_1 \rrbracket_{\delta,r}^n, \llbracket \phi_2 \rrbracket_{\delta,r}^n)$  where  $g_n$  is a monotonic function mapping pairs of sets of states to sets of traces, which does not depend on  $\delta, r$  (but only on  $n$ ). Hence, the thesis follows from the set inclusions about the semantics of  $\phi_1$  and  $\phi_2$  in the induction hypothesis.  $\square$

**Proof of Lemma 4.3.** The statement follows by induction on  $n - n'$  from the following properties:

$$\delta \leq \delta' \wedge p \sim_{\delta}^n q \implies p \sim_{\delta'}^n q \quad (\text{A.1})$$

$$p \sim_{\delta}^{n+1} q \implies p \sim_{\delta}^n q \quad (\text{A.2})$$

To prove (A.1) we proceed by induction on  $n$ . In the base case  $n = 0$  the thesis trivially follows by the first case of Definition 4.1.

For the inductive case, we assume (A.1) holds for  $n$ , and prove it for  $n + 1$ . Therefore, we assume  $p \sim_{\delta}^{n+1} q$  and prove  $p \sim_{\delta'}^{n+1} q$ .

To prove the thesis, we must show that all the items of Definition 4.1 hold. Item (2a) directly follows from the hypothesis. For item (2b) we have

$$\Pr(p, Q) \leq \Pr(q, \sim_{\delta}^n(Q)) + \delta \leq \Pr(q, \sim_{\delta'}^n(Q)) + \delta'$$

where the first inequality follows from the hypothesis  $p \sim_{\delta}^{n+1} q$ , while the second one follows from the induction hypothesis (which implies  $\sim_{\delta}^n(Q) \subseteq \sim_{\delta'}^n(Q)$ ) and  $\delta \leq \delta'$ . Item (2c) is analogous.

We now prove (A.2), proceeding by induction on  $n$ . In the base case  $n = 0$ , the thesis trivially follows by the first case of Definition 4.1. For the inductive case, we assume the statement holds for  $n$ , and we prove it for  $n + 1$ . Therefore, we assume  $p \sim_{\delta}^{n+2} q$  and prove  $p \sim_{\delta}^{n+1} q$ .

To prove the thesis, we must show that all the items of Definition 4.1 hold. Item (2a) directly follows from the hypothesis. For item (2b) of the thesis we have

$$\Pr(p, Q) \leq \Pr(q, \sim_{\delta}^{n+1}(Q)) + \delta \leq \Pr(q, \sim_{\delta}^n(Q)) + \delta$$

where the first inequality follows from the hypothesis  $p \sim_{\delta}^{n+2} q$ , while the second one follows from the induction hypothesis (which implies  $\sim_{\delta}^{n+1}(Q) \subseteq \sim_{\delta}^n(Q)$ ). Item (2c) is analogous.  $\square$

**Lemma A.1.** *Let  $a, b \in \mathbb{R}$ . If  $\forall \epsilon > 0 : a \leq b + \epsilon$  then  $a \leq b$ .*

*Proof.* If  $a > b$ , taking  $\epsilon = (a - b)/2$  contradicts the hypothesis.  $\square$

**Proof of Lemma 5.4.** By Lemma 4.3 we have that  $p \sim_{\delta}^m q$ . If  $T$  is finite the thesis follows from Lemma 5.5. If  $T$  is infinite, it must be countable: this follows by the fact that Markov chains states are countable and the length of the traces in  $T$  is finite. So, let  $\tilde{t}_0 \tilde{t}_1 \dots$  be an enumeration of  $T$ . By definition of infinite sum, we have that:

$$\Pr(T) = \lim_{k \rightarrow \infty} \sum_{i=0}^k \Pr(\tilde{t}_i)$$

By definition of limit of a sequence, we have that for all  $\epsilon > 0$  there exists  $v \in \mathbb{N}$  such that for all  $k > v$ :

$$\left| \Pr(T) - \sum_{i=0}^k \Pr(\tilde{t}_i) \right| < \epsilon$$

Since  $\Pr(\tilde{t}_i) \geq 0$  for all  $i$ , we can drop the absolute value and we get:

$$\Pr(T) - \sum_{i=0}^k \Pr(\tilde{t}_i) < \epsilon \tag{A.3}$$

By Lemma A.1 it suffice to show  $\Pr(T) \leq \Pr(\tilde{R}_{\delta,q}^m(T)) + \delta m + \epsilon$  for all  $\epsilon > 0$ , or equivalently:

$$\Pr(T) - \epsilon \leq \Pr(\tilde{R}_{\delta,q}^m(T)) + \delta m$$

So, let  $\epsilon > 0$  and let  $k$  be such that Lemma A.3 holds. Then we have:

$$\Pr(T) - \epsilon < \sum_{i=0}^k \Pr(\tilde{t}_i)$$

Let  $T' = \{\tilde{t}_i \mid i \leq k\}$ . Since  $\sum_{i=0}^k \Pr(\tilde{t}_i) = \Pr(T')$  and  $T'$  is finite, by Lemma 5.5 we have:

$$\sum_{i=0}^k \Pr(\tilde{t}_i) \leq \Pr(\tilde{R}_{\delta,q}^m(T')) + \delta m$$

Since  $\tilde{R}_{\delta,q}^m(T') \subseteq \tilde{R}_{\delta,q}^m(T)$  we have that:

$$\Pr(\tilde{R}_{\delta,q}^m(T')) + \delta m \leq \Pr(\tilde{R}_{\delta,q}^m(T)) + \delta m$$

Summing up, we have that  $\Pr(T) - \epsilon \leq \Pr(\tilde{R}_{\delta,q}^m(T)) + \delta m$  for all  $\epsilon > 0$ . By Lemma A.1 it follows that  $\Pr(T) \leq \Pr(\tilde{R}_{\delta,q}^m(T)) + \delta m$  as required.  $\square$

**Proof of Lemma 5.6.** Without loss of generality, we prove the statement under the following additional assumptions:

$$\forall b \in B : f_B(b) > 0 \tag{A.4}$$

$$\forall b \in B : \{a \in A \mid b \in g(a)\} \neq \emptyset \quad \text{and} \tag{A.5}$$

$$\forall b_1, b_2 \in B : \{a \in A \mid b_1 \in g(a)\} = \{a \in A \mid b_2 \in g(a)\} \implies b_1 = b_2$$

If  $B$  does not satisfy Equation A.4, just remove from  $B$  the elements  $b$  such that  $f_B(b) = 0$  adjust  $g$  accordingly, and set  $h(a, b) = 0$ . Equation 5.1 still holds since we removed only elements whose value is zero. If  $B$  does not satisfy Equation A.5, it can be transformed to a set that does. To see why, let  $\equiv \subseteq B \times B$  be defined as:

$$b \equiv b' \text{ iff } \{a \in A \mid b \in g(a)\} = \{a \in A \mid b' \in g(a)\}$$

Let  $\hat{B}$  be the set of equivalence classes w.r.t.  $\equiv$ . For an equivalence class  $[b]$ , define:

$$f_{\hat{B}}([b]) = \sum_{b' \in [b]} f_B(b') \quad g'(a) = \{[b] \mid b \in g(a)\}$$

It is easy to verify that (A.5) is satisfied. Notice that  $\sum_{[b] \in g'(a)} f_{\hat{B}}([b])$  converges, since:

$$\sum_{[b] \in g'(a)} f_{\hat{B}}([b]) = \sum_{[b] \in g'(a)} \sum_{b' \in [b]} f_B(b') = \sum_{b \in g(a)} f_B(b)$$

We now show that  $A, \hat{B}$  and  $g'$  satisfy Equation 5.1. We have that, for all  $b \in B$ ,  $f_B(b) \leq f_{\hat{B}}([b])$  and  $b \in g(a) \implies [b] \in g'(a)$ . Therefore, for all  $A' \subseteq A$ :

$$\sum_{a \in A'} f_A(a) \leq \sum_{b \in \bigcup_{a \in A'} g(a)} f_B(b) \leq \sum_{[b] \in \bigcup_{a \in A'} g'(a)} f_{\hat{B}}([b])$$

From a function  $h'$  satisfying Equation 5.2 and Equation 5.3 for  $A, \hat{B}$  and  $g'$  we can easily obtain a function  $h$  for  $A, B$  and  $g$ : e.g., set  $h(a, b) = h'(a, [b]) \frac{f_B(b)}{f_{\hat{B}}([b])}$ . Notice that  $f_{\hat{B}}([b]) > 0$  by Equation A.4, and that if  $B$  satisfies Equation A.5 it then holds that  $|B| < 2^{|A|}$ , and so  $B$  is finite. That said, we show that the thesis holds by reducing to the max-flow problem [DF55]. Assume w.l.o.g. that  $A$  and  $B$  are disjoint. Let  $N = (V, E)$  be a directed graph, where  $V = A \cup B \cup \{s, t\}$  with  $s, t \notin A \cup B$  and:

$$E = \{(s, b) \mid b \in B\} \cup \{(b, a) \mid a \in A, b \in g(a)\} \cup \{(a, t) \mid a \in A\}$$

Define edge capacity  $w : E \rightarrow \mathbb{R}_0^+ \cup \{\infty\}$  as follows:

$$w(s, b) = f_B(b) \quad w(b, a) = \infty \quad w(a, t) = f_A(a)$$

Consider the cut  $C = \{(a, t) \mid a \in A\}$  associated with partition  $(V \setminus \{t\}, \{t\})$ . Such cut has capacity  $\sum_{a \in A} f_A(a)$  and we argue it is minimum. Take a cut  $C'$  of the network. First notice that if  $C'$  contains edges of the form  $(b, a)$  its capacity would be infinite. We can therefore consider only cuts whose elements are of the form  $(s, b)$  or  $(a, t)$ , and thus for all  $a \in A$  we have that  $a$  and the elements of  $g(a)$  are in the same partition. In other words,  $s$  partition is of the form  $A' \cup \bigcup_{a \in A'} g(a) \cup \{s\}$ ,  $t$  partition is of the form  $A \setminus A' \cup \bigcup_{a \in (A \setminus A')} g(a) \cup \{t\}$ , where  $A' \subseteq A$ . So capacity of  $C'$  is  $\sum_{a \in A'} f_A(a) + \sum_{b \in g(A \setminus A')} f_B(b)$ . Now, capacity of  $C$  is  $\sum_{a \in A'} f_A(a) + \sum_{a \in (A \setminus A')} f_A(a)$ . Since  $\sum_{a \in (A \setminus A')} f_A(a) \leq \sum_{b \in g(A \setminus A')} f_B(b)$  by assumption Equation 5.1, we have that capacity of  $C$  is minimal. By the min-cut max-flow theorem [DF55], we have that the max flow of the network has capacity  $\sum_{a \in A} f_A(a)$ .

Let  $flow : E \rightarrow \mathbb{R}_0^+$  be the a flow associated to such cut. Consequently, we have that  $flow(a, t) = f_A(a)$  for all  $a \in A$ . Define:

$$h(a, b) = \begin{cases} \frac{flow(b, a)}{f_B(b)} & \text{if } b \in g(a) \\ 0 & \text{otherwise} \end{cases}$$

We have to show that  $h$  satisfies Equation 5.2 and Equation 5.3. Let  $A' \subseteq A$ . We have that:

$$\begin{aligned} \sum_{a \in A'} \sum_{b \in g(a)} h(a, b) f_B(b) &= \sum_{a \in A'} \sum_{b \in g(a)} \frac{flow(b, a)}{f_B(b)} f_B(b) \\ &= \sum_{a \in A'} \sum_{b \in g(a)} flow(b, a) \end{aligned}$$

By the conservation of flow constraint, we have that:

$$\begin{aligned} \sum_{a \in A'} \sum_{b \in g(a)} flow(b, a) &= \sum_{a \in A'} flow(a, t) \\ &= \sum_{a \in A'} f_A(a) \end{aligned}$$

So summing up we have that:

$$\sum_{a \in A'} \sum_{b \in g(a)} h(a, b) f_B(b) = \sum_{a \in A'} f_A(a)$$

For the remaining part, let  $b \in B$ . We have that:

$$\begin{aligned} \sum_{a \in A} h(a, b) &= \sum_{a \in \{a' \mid b \in g(a')\}} h(a, b) \\ &= \sum_{a \in \{a' \mid b \in g(a')\}} \frac{flow(b, a)}{f_B(b)} \\ &= \frac{1}{f_B(b)} \sum_{a \in \{a' \mid b \in g(a')\}} flow(b, a) \\ &\leq \frac{f_B(b)}{f_B(b)} \\ &= 1 \end{aligned} \quad \square$$

**Proof of Lemma 5.5.** By induction on  $n$ . The base case ( $n = 1$ ) is trivial as  $T = \{p\}$  and  $\tilde{R}_{\delta, q}^n(T) = \{q\}$ , or  $T = \emptyset$  and  $\tilde{R}_{\delta, q}^n(T) = \emptyset$ . Therefore,  $\Pr(T) = \Pr(\tilde{R}_{\delta, q}^n(T)) = |T|$ . For the inductive case, first notice that:

$$\Pr(T) = \sum_{\tilde{t} \in T} \Pr(p, \tilde{t}(1)) \Pr(\tilde{t}(1..n-1))$$

Referring to Lemma 5.6, let  $A = \{\tilde{t}(1) \mid \tilde{t} \in T\}$ ,  $B = \{q' \mid p' \sim_{\delta}^{n-1} q' \text{ for some } p' \in A\} \cup \{D\}$ , where  $D$  is a special element not occurring in  $A \cup B$ . Let  $f_A(p') = \Pr(p, p')$ ,  $f_B(q') = \Pr(q, q')$  and  $f_B(D) = \delta$ . Finally, let  $g(p') = \sim_{\delta}^{n-1}(p') \cup \{D\}$ .

By Definition 4.1, we have that  $A, B, f_A, f_B$  and  $g$  satisfy Equation 5.1 of Lemma 5.6. Indeed, for all  $A' \subseteq A$ , we have that:

$$\sum_{a \in A'} f_A(a) = \Pr(p, A') \leq \Pr(q, \sim_\delta^{n-1}(A')) + \delta = \sum_{b \in \bigcup_{a \in A'} g(a)} f_B(b)$$

We can then conclude that there exist  $h$  such that, for all  $A' \subseteq A$ :

$$\Pr(p, A') = \sum_{p' \in A'} \left( h(p', D) \delta + \sum_{q' \in \sim_\delta^{n-1}(p')} h(p', q') \Pr(q, q') \right)$$

Let  $T_P = \{\tilde{t}(1..n-1) \mid \tilde{t} \in T \wedge \tilde{t}(1) \in P\}$  where  $P \subseteq A$ . We simply write  $T_{p'}$  if  $P = \{p'\}$ . So, we have that:

$$\begin{aligned} \Pr(T) &= \sum_{\tilde{t} \in T} \Pr(p, \tilde{t}(1)) \Pr(\tilde{t}(1..n-1)) \\ &= \sum_{p' \in A} \Pr(p, p') \Pr(T_{p'}) \\ &= \sum_{p' \in A} \Pr(T_{p'}) \left( h(p', D) \delta + \sum_{q' \in \sim_\delta^{n-1}(p')} h(p', q') \Pr(q, q') \right) \\ &\leq \delta + \sum_{p' \in A} \Pr(T_{p'}) \sum_{q' \in \sim_\delta^{n-1}(p')} h(p', q') \Pr(q, q') \\ &= \delta + \sum_{p' \in A} \sum_{q' \in \sim_\delta^{n-1}(p')} h(p', q') \Pr(q, q') \Pr(T_{p'}) \\ &\leq \delta + \sum_{p' \in A} \sum_{q' \in \sim_\delta^{n-1}(p')} h(p', q') \Pr(q, q') \left( \Pr(\tilde{R}_{\delta, q'}^{n-1}(T_{p'})) + \delta(n-1) \right) \\ &= \delta + s_1 + s_2 \end{aligned}$$

where:

$$\begin{aligned} s_1 &= \sum_{p' \in A} \sum_{q' \in \sim_\delta^{n-1}(p')} h(p', q') \Pr(q, q') \delta(n-1) \\ s_2 &= \sum_{p' \in A} \sum_{q' \in \sim_\delta^{n-1}(p')} h(p', q') \Pr(q, q') \Pr(\tilde{R}_{\delta, q'}^{n-1}(T_{p'})) \end{aligned}$$

Now:

$$\begin{aligned} s_1 &= \delta(n-1) \sum_{p' \in A} \sum_{q' \in \sim_\delta^{n-1}(p')} h(p', q') \Pr(q, q') \\ &\leq \delta(n-1) \Pr(p, A) \\ &\leq \delta(n-1) \end{aligned}$$

Therefore  $\delta + s_1 \leq \delta n$ . It remains to show that  $s_2 \leq \Pr(\tilde{R}_{\delta, q}^n(T))$ . First notice that  $s_2$  can be rewritten as follows by a simple reordering of terms:

$$s_2 = \sum_{q' \in \sim_\delta^{n-1}(A)} \sum_{p' \in A \cap \sim_\delta^{n-1}(q')} h(p', q') \Pr(q, q') \Pr(\tilde{R}_{\delta, q'}^{n-1}(T_{p'}))$$

So:

$$\begin{aligned}
s_2 &= \sum_{q' \in \sim_{\delta}^{n-1}(A)} \sum_{p' \in A \cap \sim_{\delta}^{n-1}(q')} h(p', q') \Pr(q, q') \Pr(\tilde{R}_{\delta, q'}^{n-1}(T_{p'})) \\
&\leq \sum_{q' \in \sim_{\delta}^{n-1}(A)} \sum_{p' \in A \cap \sim_{\delta}^{n-1}(q')} h(p', q') \Pr(q, q') \Pr(\tilde{R}_{\delta, q'}^{n-1}(T_{A \cap \sim_{\delta}^{n-1}(q')})) \\
&\leq \sum_{q' \in \sim_{\delta}^{n-1}(A)} \Pr(q, q') \Pr(\tilde{R}_{\delta, q'}^{n-1}(T_{A \cap \sim_{\delta}^{n-1}(q')})) \sum_{p' \in A \cap \sim_{\delta}^{n-1}(q')} h(p', q') \\
&\leq \sum_{q' \in \sim_{\delta}^{n-1}(A)} \Pr(q, q') \Pr(\tilde{R}_{\delta, q'}^{n-1}(T_{A \cap \sim_{\delta}^{n-1}(q')})) \\
&= \Pr(\tilde{R}_{\delta, q}^n(T))
\end{aligned}$$

The last equality follows by partitioning  $\tilde{R}_{\delta, q}^n(T)$  according to the second state of each trace  $q'$ . The set of all such second states is the set of those bisimilar to (some state of)  $A$ , namely  $\sim_{\delta}^{n-1}(A)$ . Given any such  $q'$ , the probability of its partition is  $\Pr(q, q') \Pr(U_{q'})$  where  $U_{q'}$  is the set of the *tails* of  $\tilde{R}_{\delta, q}^n(T)$  starting from  $q'$ . Since this set is defined taking pointwise bisimilar traces, we can equivalently express  $U_{q'}$  by first taking the tails of  $T$  (i.e.,  $T_A$ ), and then considering the bisimilar traces: in other words, we have  $U_{q'} = \tilde{R}_{\delta, q'}^{n-1}(T_A)$ . Note that the states in  $A$  which are not bisimilar to  $q'$  do not contribute to  $\tilde{R}_{\delta, q'}^{n-1}(T_A)$  in any way, so we can also write the desired  $U_{q'} = \tilde{R}_{\delta, q'}^{n-1}(T_{A \cap \sim_{\delta}^{n-1}(q')})$ .  $\square$

**Lemma A.2.** *Let  $T = \{t \mid t(0) = p \wedge t \models_{\delta, r}^n \mathbf{X}\phi\}$  for some  $p, \phi$ , and let  $m \geq 2$ . Then:*

$$\Pr(T) = \Pr(\{\tilde{t} \mid |\tilde{t}| = m \wedge \tilde{t}(0) = p \wedge \tilde{t} \models_{\delta, r}^n \mathbf{X}\phi\})$$

*Proof.* Trivial.  $\square$

**Lemma A.3.** *Let  $T = \{t \mid t(0) = p \wedge t \models_{\delta, r}^n \phi_1 \mathbf{U} \phi_2\}$  for some  $p, \phi_1, \phi_2$ , and let  $m \geq n + 1$ . Then:*

$$\Pr(T) = \Pr(\{\tilde{t} \mid |\tilde{t}| = m \wedge \tilde{t}(0) = p \wedge \tilde{t} \models_{\delta, r}^n \phi_1 \mathbf{U} \phi_2\})$$

*Proof.* (Sketch) Let  $\tilde{T} = \{\tilde{t} \mid |\tilde{t}| = m \wedge \tilde{t}(0) = p \wedge \tilde{t} \models_{\delta, r}^n \phi_1 \mathbf{U} \phi_2\}$ . The thesis follows from the fact that  $T = \bigcup_{\tilde{t} \in \tilde{T}} \text{Cyl}(\tilde{t})$ .  $\square$

For notational convenience, hereafter we will often write  $q \models_{\delta, r}^n \phi$  instead of  $q \in \llbracket \phi \rrbracket_{\delta, r}^n$ .

**Lemma A.4.** *Let  $k$  and  $n$  be, respectively, the maximum nesting level of  $\mathbf{U}$  and of  $\mathbf{X}$  in  $\phi$ , and let  $p \sim_{\delta_1}^{mk+n+1} q$ . Then:*

- (1)  $p \models_{\delta_2, +1}^m \phi \implies q \models_{\delta_2 + \delta_1(mk+n+1), +1}^m \phi$
- (2)  $p \not\models_{\delta_2, -1}^m \phi \implies q \not\models_{\delta_2 + \delta_1(mk+n+1), -1}^m \phi$

*Proof.* By induction on  $\phi$ . The cases **true** and **a** are trivial.

- $\neg\phi'$ . We only show item 1 as the other item is similar. So, suppose  $p \models_{\delta_2, +1}^m \neg\phi'$ . Then,  $p \not\models_{\delta_2, -1}^m \phi$ . By the induction hypothesis we have that  $q \not\models_{\delta_2 + \delta_1(mk+n+1), -1}^m \phi$ , and hence  $q \models_{\delta_2 + \delta_1(mk+n+1), +1}^m \neg\phi'$  as required.

- $\phi_1 \wedge \phi_2$ . We only show item 1 as the other item is similar. So, suppose  $p \models_{\delta_2,+1}^m \phi_1 \wedge \phi_2$ . Then  $p \models_{\delta_2,+1}^m \phi_1$  and  $p \models_{\delta_2,+1}^m \phi_2$ . By the induction hypothesis  $q \models_{\delta_2+\delta_1(mk+n+1),+1}^m \phi_1$  and  $q \models_{\delta_2+\delta_1(mk+n+1),+1}^m \phi_2$ . Therefore  $q \models_{\delta_2+\delta_1(mk+n+1),+1}^m \phi_1 \wedge \phi_2$  as required.
- $\Pr_{\triangleright\pi}[\psi]$ . For item 1, suppose that  $p \models_{\delta_2,+1}^m \Pr_{\triangleright\pi}[\psi]$ . We only deal with the case  $\triangleright = \geq$ , since the case  $\triangleright = >$  is analogous. Let:

$$T = \{\tilde{t} \mid |\tilde{t}| = mk + n + 1 \wedge \tilde{t}(0) = p \wedge \tilde{t} \models_{\delta_2,+1}^m \psi\}$$

We start by proving that:

$$\forall \tilde{u} \in \tilde{R}_{\delta_1,q}^{mk+n+1}(T) \quad : \quad \tilde{u} \models_{\delta_2+\delta_1(mk+n+1),+1}^m \psi \quad (\text{A.6})$$

Let  $\tilde{u} \in \tilde{R}_{\delta_1,q}^{mk+n+1}(T)$ . Then, there is  $\tilde{t} \in T$  such that, for all  $0 \leq i < mk + n + 1$ :

$$\tilde{t}(i) \sim_{\delta_1}^{mk+n+1-i} \tilde{u}(i)$$

We proceed by cases on  $\psi$ .

- $\phi_1 \mathbf{U} \phi_2$ . First notice that  $mk + n + 1 \geq m + 1$ , and hence by Lemma A.3 we have that:

$$\Pr(T) = \Pr(\{t \mid t(0) = p \wedge t \models_{\delta_2,+1}^m \phi_1 \mathbf{U} \phi_2\})$$

We then have  $\Pr(T) + \delta_2 \geq \pi$ . Since  $\tilde{t} \models_{\delta_2,+1}^m \phi_1 \mathbf{U} \phi_2$ , we have that:

$$\exists i \leq m : \tilde{t}(i) \models_{\delta_2,+1}^m \phi_2 \wedge \forall j < i : \tilde{t}(j) \models_{\delta_2,+1}^m \phi_1$$

Let  $n'$  be the maximum nesting level of  $\mathbf{X}$  in  $\phi_2$ . We know that:

$$\tilde{t}(i) \sim_{\delta_1}^{mk+n+1-i} \tilde{u}(i) \wedge mk + n + 1 - i > m(k-1) + n' + 1$$

Then, by Lemma 4.3 (monotonicity of  $\sim$ ), we have that:

$$\tilde{t}(i) \sim_{\delta_1}^{m(k-1)+n'+1} \tilde{u}(i)$$

Then, by the induction hypothesis, we have that:

$$\tilde{u}(i) \models_{\delta_2+\delta_1(m(k-1)+n'+1),+1}^m \phi_2$$

By Lemma 3.5 (monotonicity of  $\models$ ) it follows that:

$$\tilde{u}(i) \models_{\delta_2+\delta_1(mk+n+1),+1}^m \phi_2$$

With a similar argument we can conclude that, for all  $j < i$ :

$$\tilde{u}(j) \models_{\delta_2+\delta_1(mk+n+1),+1}^m \phi_1$$

Hence Equation A.6 holds.

- $\mathbf{X}\phi_1$ . First notice that  $mk + n + 1 \geq 2$ , and hence by Lemma A.2 we have that:

$$\Pr(T) = \Pr(\{t \mid t(0) = p \wedge t \models_{\delta_2,+1}^m \mathbf{X}\phi_1\})$$

Then,  $\Pr(T) + \delta_2 \geq \pi$ . Since  $\tilde{t} \models_{\delta_2,+1}^m \mathbf{X}\phi_1$ , we have that  $\tilde{t}(1) \models_{\delta_2,+1}^m \phi_1$ . We know that  $\tilde{u}(1) \sim_{\delta_1}^{mk+n} \tilde{t}(1)$ . By the induction hypothesis,  $\tilde{u}(1) \models_{\delta_2+\delta_1(mk+n),+1}^m \phi_1$ . By Lemma 3.5 (monotonicity of  $\models$ ) it follows that:  $\tilde{u}(i) \models_{\delta_2+\delta_1(mk+n+1),+1}^m \phi_1$ . Hence, (A.6) holds.

Back to the main statement, we have that, by Lemma 5.4:

$$\Pr(\tilde{R}_{\delta_1, q}^{mk+n+1}(T)) + \delta_2 + \delta_1(mk + n + 1) \geq \Pr(T) + \delta_2$$

So, summing up:

$$\begin{aligned} & \Pr(\{t \mid t(0) = q \wedge t \models_{\delta_2 + \delta_1(mk+n+1), +1}^m \psi\}) + \delta_2 + \delta_1(mk + n + 1) \\ = & \Pr(\{\tilde{t} \mid |\tilde{t}| = mk + n + 1 \wedge \tilde{t}(0) = q \wedge \tilde{t} \models_{\delta_2 + \delta_1(mk+n+1), +1}^m \psi\}) \\ & + \delta_2 + \delta_1(mk + n + 1) \\ \geq & \Pr(\tilde{R}_{\delta_1, q}^{mk+n+1}(T)) + \delta_2 + \delta_1(mk + n + 1) \\ \geq & \Pr(T) + \delta_2 \\ \geq & \pi \end{aligned}$$

Therefore,  $q \models_{\delta_2 + \delta_1(mk+n), +1}^m \Pr_{\geq \pi}[\psi]$ .

For item 2, suppose that  $p \not\models_{\delta_2, -1}^m \Pr_{\geq \pi}[\psi]$ . Then:

$$\Pr(\{t \mid t(0) = p \wedge t \models_{\delta_2, -1}^m \psi\}) - \delta_2 < \pi$$

From the above, by a case analysis on  $\psi$ , and exploiting Lemma A.3 and Lemma A.2, we conclude that  $\Pr(T) - \delta_2 < \pi$ , where:

$$T = \{\tilde{t} \mid |\tilde{t}| = mk + n + 1 \wedge t(0) = p \wedge t \models_{\delta_2, -1}^m \psi\}$$

Let:

$$\bar{T} = \{\tilde{t} \mid |\tilde{t}| = mk + n + 1 \wedge t(0) = p \wedge \tilde{t} \not\models_{\delta_2, -1}^m \psi\}$$

We have that  $1 - \Pr(\bar{T}) = \Pr(T)$ . We start by proving that:

$$\forall \tilde{u} \in \tilde{R}_{\delta_1, q}^{mk+n+1}(\bar{T}) : \tilde{u} \not\models_{\delta_2 + \delta_1(mk+n+1), -1}^m \psi$$

Let  $\tilde{u} \in \tilde{R}_{\delta_1, q}^{mk+n+1}(\bar{T})$ . Then, there exist  $\tilde{t} \in \bar{T}$  such that, for all  $0 \leq i < mk + n + 1$ :

$$\tilde{t}(i) \sim_{\delta_1}^{mk+n-i} \tilde{u}(i)$$

We proceed by cases on  $\psi$ .

–  $\phi_1 \cup \phi_2$ . Since  $\tilde{t} \not\models_{\delta_2, -1}^m \phi_1 \cup \phi_2$ , we have that:

$$\forall i \leq m : \tilde{t}(i) \not\models_{\delta_1, -1}^m \phi_2 \vee \exists j < i : \tilde{t}(j) \not\models_{\delta_2, -1}^m \phi_1$$

Take  $i \leq m$ . Let  $n'$  be the maximum nesting level of  $X$  in  $\phi_2$ . If  $\tilde{t}(i) \not\models_{\delta_1, -1}^m \phi_2$ , since

$$\tilde{t}(i) \sim_{\delta_1}^{mk+n+1-i} \tilde{u}(i) \wedge mk + n + 1 - i > m(k-1) + n' + 1$$

by Lemma 4.3 (monotonicity of  $\sim$ ) we have that:

$$\tilde{t}(i) \sim_{\delta_1}^{m(k-1)+n'+1} \tilde{u}(i)$$

By the induction hypothesis we have that:

$$\tilde{u}(i) \not\models_{\delta_2 + \delta_1(m(k-1)+n'+1), -1}^m \phi_2$$

By Lemma 3.5 (monotonicity of  $\models$ ) it follows:

$$\tilde{u}(i) \not\models_{\delta_2 + \delta_1(mk+n+1), -1}^m \phi_2$$

If  $\tilde{t}(j) \not\models_{\delta_1, -1}^m \phi_1$  for some  $j < i$ , with a similar argument we can conclude that:

$$\tilde{u}(j) \not\models_{\delta_2 + \delta_1(m(k-1)+n+1), -1}^m \phi_1$$

–  $X\phi_1$ . Since  $\tilde{t} \not\models_{\delta_2, -1}^m X\phi_1$ , we have that:  $\tilde{t}(1) \not\models_{\delta_2, -1}^m \phi_1$ . Since  $\tilde{t}(1) \sim_{\delta_1}^{mk+n} \tilde{u}(1)$ , by the induction hypothesis we have  $\tilde{u}(i) \not\models_{\delta_2+\delta_1(mk+n), -1}^m \phi_1$ . By Lemma 3.5 it follows that:

$$\tilde{u}(i) \not\models_{\delta_2+\delta_1(mk+n+1), -1}^m \phi_1$$

Back to the main statement, by Lemma 5.4 we have that:

$$\Pr(\bar{T}) \leq \Pr(\tilde{R}_{\delta_1, q}^{mk+n+1}(\bar{T})) + \delta_1(mk + n + 1)$$

Summing up, we have that:

$$\begin{aligned} & \Pr(\{t \mid t(0) = q \wedge t \models_{\delta_2+\delta_1(mk+n+1), -1}^m \psi\}) - \delta_2 - \delta_1(mk + n + 1) \\ &= \Pr(\{\tilde{t} \mid |\tilde{t}| = |\tilde{t}| = mk + n + 1 \wedge \tilde{t}(0) = q \wedge \tilde{t} \models_{\delta_2+\delta_1(mk+n+1), -1}^m \psi\}) \\ & \quad - \delta_2 - \delta_1(mk + n + 1) \\ &= 1 - \Pr(\{\tilde{t} \mid |\tilde{t}| = mk + n + 1 \wedge \tilde{t}(0) = q \wedge \tilde{t} \not\models_{\delta_2+\delta_1(mk+n+1), -1}^m \psi\}) \\ & \quad - \delta_2 - \delta_1(mk + n + 1) \\ &\leq 1 - \Pr(\tilde{R}_{\delta_1, q}^{mk+n}(\bar{T})) - \delta_2 - \delta_1(mk + n + 1) \\ &\leq 1 - \Pr(\bar{T}) - \delta_2 \\ &= \Pr(T) - \delta_2 < \pi \end{aligned}$$

Therefore,  $q \not\models_{\delta_2+\delta_1(mk+n), -1}^m \Pr_{\geq \pi}[\psi]$ . □

**Proof of Theorem 5.1.** Immediate consequence of Lemma A.4. □