Under consideration for publication in Formal Aspects of Computing

Parametric Probabilistic Transition Systems for System Design and Analysis[1]

Ruggero Lanotte[1], Andrea Maggiolo-Schettini[2] and Angelo Troina[2]

[1]Dipartimento di Scienze della Cultura, Politiche e dell'Informazione, Università dell'Insubria, Italy
[2]Dipartimento di Informatica, Università di Pisa, Italy

Abstract. We develop a model of Parametric Probabilistic Transition Systems, where probabilities associated with transitions may be parameters. We show how to find instances of the parameters that satisfy a given property and instances that either maximize or minimize the probability of reaching a certain state. As an application, we model a probabilistic non–repudiation protocol with a Parametric Probabilistic Transition System. The theory we develop allows us to find instances that maximize the probability that the protocol ends in a fair state (no participant has an advantage over the others).

Keywords: Discrete–time Markov Chains, Parameters, Reachability, Probabilistic Non-Repudiation Protocol.

1. Introduction

Complex systems may exhibit behaviours depending on decisions that can be taken at each state of the system, based on a probabilistic choice. Therefore, there are properties that should be studied in a probabilistic setting and require suitable description methodologies and verification techniques. This is the case when one wants to study quantitative security, performance and reliability properties of systems of distributed and communicating agents.

Many formalisms have been proposed for analyzing probabilistic systems. The analysis process consists in building a probabilistic model of the system, typically a Discrete–time Markov Chain, a Markov Decision Process or a Continuous Time Markov Chain (see [Bel57, How60, Ros83]), on which analytical, simulation-based and numerical calculations can be performed to obtain the desired quantitative measures. Temporal logics have been adapted to deal with quantitative verification, namely with the problem of determining the probability with which a system satisfies a specification [Alf98, Alf99, BBS95, BK98a, BK98b, Bea02,

Correspondence and offprint requests to: Ruggero Lanotte, Dipartimento di Scienze della Cultura, Politiche e dell'Informazione, Università dell'Insubria, Via Valleggio 11, 22100, Como, Italy, e-mail: ruggero.lanotte@uninsubria.it

[1] A preliminary version of this paper was presented at SEFM'04 [LMT04].

BdA95, CSZ92, DEP98, Han94, JL91, Mal95, SS98, WSS97]. These formalisms are addressed at verifying concrete specifications.

Real specifications, however, are often parametric. Actually, the design of a system may depend on certain parameters of the environment, and concrete instantiations make sense only in the context of a given concrete environment. Moreover, one may want to tune the parameters of a system on the values that allow reaching a desired reliability level, in hardware design, or a security threshold, in protocol design.

In this paper we develop the model of Parametric Probabilistic Transition Systems (PPTSs). Intuitively, PPTSs are Discrete–time Markov Chains in which probabilities associated with transitions may be parameters assuming real values.

It is, in general, undecidable whether there exists a valuation of the parameters appearing in a PPTS that satisfies a given formula. However, we prove that valuations satisfying a given formula can be computed for a subfamily of PPTSs with at most two parameters. Hence, we study the restrictions under which it is possible to compute instantiations of the parameters satisfying a given formula (which may contain also reachability conditions), and we give a syntactical characterization of the PPTSs satisfying those restrictions.

Finally, we propose a technique to compute valuations that maximize or minimize the probability of reaching a certain state of the PPTS.

The class of PPTSs satisfying the restrictions we impose is expressive enough to describe and analyze many real–life systems. One may think, for example, of systems with one or two hardware components which can undermine the reliability of the whole system. If the designer is able to adjust the reliability levels of the components, considered as parameters, our framework allows to analyze and maximize the reliability of the whole system. A similar analysis can be done for the study of reliability and/or security level of probabilistic protocols. In fact, a large class of probabilistic protocols perform just one probabilistic choice, which can be considered as the only parameter of the system. Applications of this type range from academic protocols, e.g. Chaum's dining cryptographers protocol (see [Cha88]) and the probabilistic Non–repudiation protocol introduced in [MR99], to industrial protocols, e.g. the IPv4 Zeroconf protocol as studied in [BSHV03], the Crowds [RR98] and Onion Routing [RSG98] anonymity protocols, etc..

Summing up, the framework we present allows for the parametric analysis of a rich class of systems, e.g., checking whether a formula holds for different values of the parameters, and computing the values of the parameters such that some property is satisfied or the probability of reaching a success (failure) state to be maximized (minimized).

1.1. Related Works

In [AHV93] Alur et al. address the problem of parametric reasoning on the timing properties of real–time systems. *Parametric Timed Automata* are proposed as a generalization of the *Timed Automata* in [AD94]. In particular transition guards on clock formulas are allowed to contain parameters. In this setting, the number of clocks is crucial for the decidability of the emptiness problem: for a subclass of Parametric Timed Automata, where just one clock is parametrically constrained, the emptiness problem is shown to be decidable.

In [TNHH98], a parametric model checking algorithm is proposed for a subclass of Timed Automata called Parametric Time–Interval Automata (PTIA). In a PTIA, one can specify upper- and lower-bounds of the execution time (time–interval) of each transition by using parameter variables. The proposed algorithm takes two inputs, a model described as a PTIA and a property specified as a PTIA accepting all the invalid runs. The algorithm constructs the parallel composition of the PTIAs expressing the model and the property, and checks the emptiness of the language accepted by the product automaton. The output is the weakest condition on the parameters such that the given model never executes the invalid runs.

The interest about parametric real–time properties has also been extended to model checkers for real–time systems. In [HRSV02] Hune et al. introduce an extension of the UPPAAL model checker (see [UPPAAL]) for analyzing Parametric Timed Automata. The authors identify a subclass of Parametric Timed Automata (called L/U automata), for which the emptiness problem is decidable.

With HyTech [HHW97], a tool for model checking Hybrid Automata, Henzinger et al. also consider a parametric analysis. Parametric Hybrid Automata allow the modelling of continuous behaviour by means of linear equations, and, hence, they are more complex than Parametric Timed Automata. As a consequence, the tool cannot cope with too large examples.

While the study of parametric real–time systems has been strongly pursued, parametric analysis of prob-

abilistic systems has not been considered until recent years. In 2004, two studies on parametric probabilistic analysis were brought on independently (see [Daw04, LMT04]).

In [Daw04], Daws presents a language–theoretic approach to symbolic model checking of PCTL formulas over Discrete–time Markov Chains. The probability with which a path formula is satisfied is represented by a regular expression. A recursive evaluation of the regular expression yields an exact rational value when transition probabilities are rational, and rational functions when some probabilities are left unspecified as parameters of the system. This allows for parametric model checking by evaluating the regular expression for different parameter values in the rational domain. In the present paper, which is an extension of [LMT04], we give an in–depth analysis of parametric probabilistic systems, where parameters are real values. We study decidable subclasses of PPTSs and we propose a technique for minimizing/maximizing the probability of reaching certain states under a given condition on the parameters.

1.2. Summary

The remainder of this paper is organized as follows. In Section 2 we recall some basic notions about Discrete–time Markov Chains. In Section 3 we introduce the model of Parametric Probabilistic Transition Systems by extending Markov Chains with parameters. In Section 4 we tackle the problems of the decidability of the existence of instances of parameters that satisfy a given property and we propose a technique to find optimal instances. In Section 5, as an application, we show the model of a probabilistic non-repudiation protocol where some probabilistic choices are modeled with parameters. In Section 6 we draw our conclusions and anticipate some future work.

2. Basic Notions

In this section we recall some basic notions about Discrete–time Markov chains (DTMCs) [Bel57, How60].

2.1. Discrete–time Markov Chains

In this section we recall the definition of Discrete–time Markov chains (DTMCs) [Bel57, How60].

Definition 2.1. A *Discrete–time Markov chain* (DTMC) is a tuple (Q, q_0, δ, π) where:

- Q is a finite set of states;
- $q_0 \in Q$ is the initial state;
- $\delta \subseteq Q \times Q$ is a set of *transitions*;
- $\pi : \delta \to [0,1]$ is a function assigning a probability to each transition. For all states $q \in Q$ it is required that $\sum_{e \in Start(q)} \pi(e) \in \{0,1\}$.

With $Start(q)$ we denote the set of transitions with q as source state, namely $Start(q) = \{(q_i, q_j) \in \delta \mid q_i = q\}$.

Example 2.1. Consider the DTMC M depicted in Figure 1. The set of transitions of M is: $\delta = \{(q_0,q_1),(q_0,q_2),(q_0,q_3),(q_1,q_2),(q_1,q_4),(q_2,q_1),(q_2,q_5),(q_3,q_5)\}$. The probability of a transition appears over the transition. We have, e.g., $\pi((q_0,q_2)) = \frac{1}{12}$ and $\pi((q_2,q_5)) = \frac{1}{2}$.

A *run* of a DTMC $M = (Q, q_0, \delta, \pi)$ is a (possibly infinite) sequence of steps of the form $\omega = q_0 \to q_1 \to \ldots$ where (q_i, q_{i+1}) is in δ and $\pi((q_i, q_{i+1})) > 0$. The length of ω, denoted $|\omega|$, is the number of transitions between states performed by the run and is equal to n if ω is the finite run $q_0 \to q_1 \to \ldots \to q_n$, and ∞ otherwise. With $Path_{fin}(M)$ (resp. $Path_{ful}(M)$) we denote the set of finite (resp. infinite) runs of M.

Let $k \leq |\omega|$; with $\omega(k)$ we denote the state q_k and with $\omega^{(k)}$ we denote the run $q_0 \to q_1 \to \ldots \to q_k$.

If $k = |\omega|$, then we say that ω *is a prefix of* ω' if and only if $length(\omega') \geq k$ and $\omega = (\omega')^{(k)}$. With $last(\omega)$ we denote the state $\omega(k)$.

Assuming the basic notions of probability theory (see e.g. [Hal50]), we may assign a probability to the runs of a DTMC M by following the traditional *Borel σ-algebra* approach of basic cylinders sets (see [KSK66,

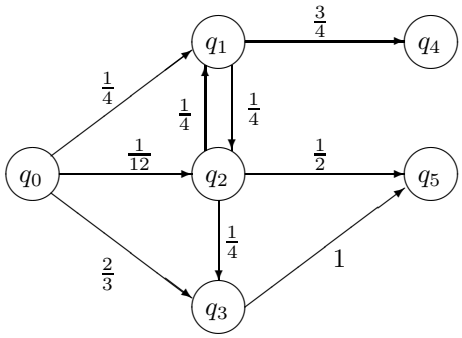

Fig. 1. A Discrete–time Markov Chain.

Wil91]). We denote the probability of a finite run $\omega = q_0 \to q_1 \to \ldots \to q_n$ with $\mu(\omega)$, defined as follows:

$$\mu_M(\omega) = \begin{cases} 1 & \text{if } n = 0 \\ \mu_M(\omega^{(n-1)}) \cdot \pi((q_{n-1}, q_n)) & \text{if } n > 0\,. \end{cases}$$

Finally, we can extend this probability to sets of infinite runs. The probability function μ defined on sets of runs in $Path_{ful}(M)$ is the unique function such that

$$\mu_M(\{\omega' \mid \omega' \in Path_{ful}(M) \ \wedge \ \omega \text{ is a prefix of } \omega'\}) = \mu_M(\omega)$$

for any $\omega \in Path_{fin}(M)$.

In the following we focus on infinite paths. Notice that, in this case, states with no outgoing transitions can be considered by adding a self–loop transition with probability 1.

Definition 2.2. Given a DTMC M and a state q, with $P_M(q)$ we denote the probability of reaching the state q from the initial state of M, more precisely:

$$P_M(q) = \mu(\{\omega \in Path_{ful}(M) \mid \exists k : \omega(k) = q\}).$$

With $Adm(q) \subseteq Q$ we denote the set of states that can be crossed for eventually reaching the state q from the initial state q_0. More precisely,

$$Adm(q) = \{q' \mid q_0 \to \ldots \to q' \to \ldots \to q \in Path_{fin}(M)\}.$$

Moreover, with $AdmTr(q', q) \subseteq \delta$ we denote the set of transitions starting from q' and reaching a state in $Adm(q)$, more precisely

$$AdmTr(q', q) = \{(q', q'') \in \delta \mid q'' \in Adm(q)\}.$$

Example 2.2. Let us consider the DTMC M of the example in Figure 1. We have that $Adm(q_4) = \{q_0, q_1, q_2, q_4\}$. Moreover, we have that $AdmTr(q_1, q_4) = \{(q_1, q_2), (q_1, q_4)\}$ and $AdmTr(q_2, q_4) = \{(q_2, q_1)\}$.

The following proposition has been proved in [HJ94].

Proposition 2.1. Let $M = (Q, q_0, \delta, \pi)$ be a DTMC and $q \in Q$; the probability $P_M(q)$ is equal to the solution of x_{q_0} of the following system of linear equations:

$$\begin{cases} x_q = 1 \\ x_{q'} = \sum_{(q', q'') \in AdmTr(q', q)} \pi((q', q'')) \cdot x_{q''} \quad \forall q' \neq q\,. \end{cases}$$

3. Parametric Probabilistic Transition Systems

In this section we introduce the model of Parametric Probabilistic Transition Systems (PPTSs). Beforehand, we define terms over parameters. Terms can be used as labels for the transitions of a system. Afterwards, we

define formulas over terms. Formulas will be used to describe properties that a term must satisfy. Thus, they can be used as constraints on terms and parameters. Finally, we consider the relationships between PPTSs and DTMCs.

With $\alpha, \beta, \ldots$ we denote *parameters* assuming values in the set $\mathbb{R}$ of real numbers. Given a set of parameters Δ, an *instance* $u : \Delta \to \mathbb{R}$ for Δ is a function assigning a real value to each parameter in Δ.

We define the set $\mathcal{P}(\Delta)$ of *polynomial terms* over parameters in Δ as follows:

$$\tau ::= c \mid \alpha \mid \tau_1 + \tau_2 \mid \tau_1 \cdot \tau_2$$

where $\tau, \tau_1, \tau_2 \in \mathcal{P}(\Delta)$, $c \in \mathbb{R}$ and $\alpha \in \Delta$. Operators $+$ and $\cdot$ represent the classical addition and multiplication operations, hence they satisfy commutativity, associativity, and distributivity of addition over multiplication. Obviously, $\tau_1 \cdot (\tau_2 + \tau_3) = \tau_3 \cdot \tau_1 + \tau_1 \cdot \tau_2$.

We will write α^k to denote the term that is the multiplication of α $k-$times. Obviously, $\alpha^0 = 1$.

An instance u extends to $\mathcal{P}(\Delta)$ as follows: $u(c) = c$, $u(\tau_1+\tau_2) = u(\tau_1)+u(\tau_2)$ and $u(\tau_1 \cdot \tau_2) = u(\tau_1) \cdot u(\tau_2)$.

Definition 3.1 (Normal Form). Let $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ with $\alpha_i \neq \alpha_j$, for any $i \neq j$. A term $\tau \in \mathcal{P}(\Delta)$ is in *normal form* if it is syntactically equivalent to $\tau_1 + \ldots + \tau_m$ where:

- for any i, it holds that $\tau_i = c_i \cdot (\alpha_1)^{k_1^i} \cdot \ldots \cdot (\alpha_n)^{k_n^i}$, where $c \in \mathbb{R}$ and $k_1^i, \ldots, k_n^i$ are natural numbers;
- for any $i \neq j$, there exists h such that $k_h^i \neq k_h^j$.

Each term can be easily put in its normal form, hence, from now on, we suppose that all terms are in normal form.

A polynomial term τ is a *linear term* if there exist $c_1, \ldots, c_{n+1} \in \mathbb{R}$ such $\tau = c_1 \cdot \alpha_1 + \ldots + c_n \cdot \alpha_n + c_{n+1}$.

We define the set $\Phi(\Delta)$ of *formulae* as follows:

$$\phi ::= \tau \sim \tau' \mid \neg\phi_1 \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2$$

where $\phi, \phi_1, \phi_2 \in \Phi(\Delta)$, $\tau, \tau' \in \mathcal{P}(\Delta)$, and $\sim \in \{<, \leq, =, \geq, >\}$.

A formula ϕ in $\Phi(\Delta)$ is *linear* iff all terms $\tau \in \mathcal{P}(\Delta)$ appearing in ϕ are linear.

Let $\phi \in \Phi(\Delta)$ and u be an instance; we say that u *satisfies* ϕ, written $u \models \phi$, iff:

$$\begin{array}{lll} u \models \tau \sim \tau' & \text{iff} & u(\tau) \sim u(\tau') \\ u \models \neg\phi_1 & \text{iff} & u \not\models \phi_1 \\ u \models \phi_1 \vee \phi_2 & \text{iff} & \text{either } u \models \phi_1 \text{ or } u \models \phi_2 \\ u \models \phi_1 \wedge \phi_2 & \text{iff} & \text{both } u \models \phi_1 \text{ and } u \models \phi_2. \end{array}$$

A known property of formulae in Φ is the following (see [Tar51] and [Ren92]).

Theorem 3.1. For each $\phi \in \Phi(\Delta)$, it is decidable in exponential time w.r.t. the number of parameters in ϕ and in polynomial space whether there exists an instance u such that $u \models \phi$.

We introduce now the model of Parametric Probabilistic Transition Systems.

Definition 3.2. A *Parametric Probabilistic Transition System* (PPTS) S is a tuple $(\Delta, Q, q_0, \delta, \lambda)$ where:

- Δ is a finite set of parameters;
- Q is a set of states;
- $q_0 \in Q$ is the initial state;
- $\delta \subseteq Q \times Q$ is a set of *transitions*;
- $\lambda : \delta \to \mathcal{P}(\Delta)$ is a function assigning to each transition (q, q') a polynomial term τ representing the probability of taking that transition.

With $\mathit{Start}(q) \subseteq \delta$ we denote the set of transitions with q as source state, namely the set $\{(q_i, q_j) \in \delta \mid q_i = q\}$. The PPTS S is *linear* if $\lambda(e)$ is linear, for any $e \in \delta$.

Example 3.1. Let us consider the PPTS S of Figure 2. We have parameters $\Delta = \{\alpha_1, \alpha_2\}$, and, as examples, $\mathit{Start}(q_2) = \{(q_2, q_1), (q_2, q_3), (q_2, q_5)\}$ and $\lambda((q_2, q_5)) = \alpha_1 + \alpha_2$.

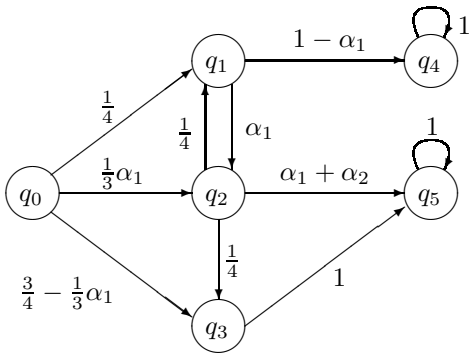

Fig. 2. A Parametric Probabilistic Transition System.

The notions of *run* of a PPTS S and of sets of finite and infinite runs $Path_{fin}(S)$ and $Path_{ful}(S)$, respectively, are defined as for DTMCs.

The following definitions relate instances of parameters to PPTSs.

Definition 3.3 (Instances of PPTSs). Given a PPTS $S = (\Delta, Q, q_0, \delta, \lambda)$ and an instance u, with $S(u)$ we denote the PPTS resulting by instantiating all the variables in Δ according to u. Namely, $S(u) = (\emptyset, Q, q_0, \delta, \lambda')$, where $\lambda'(e) = u(\lambda(e))$ for any $e \in \delta$.

Definition 3.4 (Well Defined Instances). An instance u is *well defined* for a PPTS $S = (\Delta, Q, q_0, \delta, \lambda)$ if and only if for each transition $e \in \delta$ we have that $u(\lambda(e)) \in [0, 1]$, and, for each state $q \in Q$, it holds that $\sum_{e \in Start(q)} u(\lambda(e)) = 1$.

Example 3.2. The instance u_1 such that $u_1(\alpha_1) = u_1(\alpha_2) = \frac{1}{4}$, and the instance u_2 such that $u_2(\alpha_1) = 0$, $u_2(\alpha_2) = \frac{1}{2}$ are well defined for the PPTS S of Figure 2. Note that $S(u_1)$ is the DTMC depicted in Figure 1. The instance u_3 such that $u_3(\alpha_1) = u_3(\alpha_2) = 1$ is not well defined.

Definition 3.5 (Realizability). A PPTS S is *realizable* if and only if there exists a well defined instance for S. Given a formula $\phi \in \Phi(\Delta)$, S is *ϕ–realizable* if and only if there exists a well defined instance u for S, such that $u \models \phi$ (in this case, we say that u *ϕ–realizes* S).

Remark 3.1. Given a well defined instance u for a PPTS S, we have that $S(u)$ is a DTMC.

Note that, as we did for DTMCs by restricting to infinite runs, we assumed that for any well defined instance u, $\sum_{e \in Start(q)} u(\lambda(e)) = 1$. As we have seen, this is not a real limitation, since for every state q_s with no transition to other states, we can add a self–loop transition (q_s, q_s) with $u(\lambda((q_s, q_s))) = 1$ (see states q_4 and q_5 in Figure 2).

We assign probabilities to the runs of a PPTS S for a well defined instance u, as shown in Section 2.1, by considering the DTMC $S(u)$. Thus, given a PPTS S, a state q of S and a well defined instance u, $P_{S(u)}(q)$ returns the probability of reaching the state q for the DTMC $S(u)$.

The following corollary derives from Proposition 2.1.

Corollary 3.1. Given a PPTS $S = (\Delta, Q, q_0, \delta, \lambda)$ a state $q \in Q$ and a well defined instance u, the probability $P_{S(u)}(q)$ of reaching the state q is equal to the solution of x_{q_0} of the following system of linear equations:

$$\begin{cases} x_q = 1 \\ x_{q'} = \sum_{(q',q'') \in AdmTr(q',q)} u(\lambda((q', q''))) \cdot x_{q''} \quad \forall q' \neq q \,. \end{cases}$$

4. ϕ–Realizability of Parametric Probabilistic Transition Systems

In this section we consider the problem of computing the probability of reaching a certain state. We tackle this problem in a parametric setting, and we consider existence, search and optimization of well defined instances.

4.1. The Problem of Existence of an Instance

Given a PPTS, firstly we want to know whether the PPTS is realizable or not. In particular we are interested in the existence of well defined instances for the PPTS. This problem is solved by translation into the satisfiability problem for a formula. The next proposition follows.

Proposition 4.1 (Realizability). It is decidable in exponential time w.r.t. the number of parameters and in polynomial space whether a PPTS S is realizable.

Proof. Given a PPTS $S = (\Delta, Q, q_0, \delta, \lambda)$, we build the formula:

$$\phi_R = (\bigwedge_{e \in \delta} \lambda(e) \in [0,1]) \wedge (\bigwedge_{q' \in Q} \sum_{e \in Start(q')} \lambda(e) = 1) \tag{1}$$

representing the requirements for the realizability of S.

An instance u satisfying the formula ϕ_R ($u \models \phi_R$) is well defined for S. By Theorem 3.1, the existence of an instance u that satisfies ϕ_R is decidable in exponential time. Hence, it is also decidable in exponential time w.r.t. the size of S whether S is realizable. □

We now extend Proposition 4.1 to deal with ϕ–realizability.

Corollary 4.1. It is decidable in exponential time whether a PPTS is ϕ–realizable.

Proof. Given a PPTS $S = (\Delta, Q, q_0, \delta, \lambda)$, and a formula ϕ in $\Phi(\Delta)$, we build the formula:

$$\bar{\phi} = \phi \wedge \phi_R \tag{2}$$

where ϕ_R is the formula of Equation (1).

An instance u satisfying the formula $\bar{\phi}$ is well defined for S and satisfies ϕ. Hence, u ϕ–realizes S. Again, by Theorem 3.1, the existence of an instance u that satisfies $\bar{\phi}$ is decidable in exponential time, and hence it is also decidable in exponential time w.r.t. the size of S whether S is ϕ–realizable. □

Corollary 4.1 can be then extended to deal with the reachability of states of PPTSs.

Corollary 4.2 (Existence). For any PPTS S, state q and formula $\phi \in \Phi(\Delta)$, it is decidable in exponential time w.r.t. the size of S whether there exists an instance u that ϕ–realizes S such that q is reachable in $S(u)$.

Proof. Given a PPTS $S = (\Delta, Q, q_0, \delta, \lambda)$, a state $q \in Q$ and a formula ϕ, we build the formula $\bar{\phi}$ as follows:

$$\bar{\phi} = \phi \ \wedge \ \phi_R \wedge \phi_S \tag{3}$$

where ϕ_R is again the formula in Equation (1) and ϕ_S is the formula:

$$\phi_S = (x_q = 1) \ \wedge \ (\bigwedge_{q' \in Adm(q)} x_{q'} = \sum_{(q',q'') \in AdmTr(q',q)} \lambda((q',q'')) \cdot x_{q''}). \tag{4}$$

Here, formula ϕ_S is such that for any $q' \in Q$, $x_{q'}$ is the polynomial term with variables in Δ modelling the probability of reaching q from q'.

An instance u satisfying the formula $\bar{\phi}$ is such that $u \models \phi \wedge \phi_R$ (hence, for Corollary 4.1, u ϕ–realizes S). Moreover, we have that if $u \models \bar{\phi}$, then x_{q_0} is the polynomial term modelling the probability of reaching state q. By Theorem 3.1, the existence of an instance u that satisfies $\bar{\phi}$ is decidable in exponential time, hence it is also decidable in exponential time w.r.t. the size of S whether there exists an instance u that ϕ–realizes S such that q is reachable in $S(u)$. □

Definition 4.1. With $Set(S, q, \phi) = \{u \,|\, u \models \bar{\phi}\}$, where $\bar{\phi}$ is the formula in Equation (3), we denote the set of well defined instances u such that u ϕ–realizes the PPTS S and the state q is reachable in $S(u)$.

Example 4.1. Let us consider the PPTS S in Figure 2. We want to know whether there exists an instance in the set $Set(S, q_5, (x_{q_0} > \alpha_1 \wedge \alpha_1 > 0))$. Such a set is not empty if and only if the following formula is satisfiable:

$$
\begin{array}{l}
x_{q_0} > \alpha_1 \ \wedge \ \alpha_1 > 0 \\
\alpha_1 \leq 1 \ \wedge \ \alpha_1 + \alpha_2 = \frac{1}{2} \\
\wedge \ x_{q_5} = 1 \\
\wedge \ x_{q_3} = x_{q_5} \\
\wedge \ x_{q_2} = (\alpha_1 + \alpha_2) x_{q_5} + \frac{1}{4} x_{q_3} + \frac{1}{4} x_{q_1} \\
\wedge \ x_{q_1} = \alpha_1 x_{q_2} \\
\wedge \ x_{q_0} = \frac{1}{4} x_{q_1} + \frac{1}{3} \alpha_1 x_{q_2} + (\frac{3}{4} - \frac{1}{3} \alpha_1) x_{q_3} .
\end{array}
$$

Now, the formula above is a formula in $\Phi(\{\alpha_1, \alpha_2\})$, and hence, by Theorem 3.1, its satisfiability is decidable.

4.2. Finding a Solution

Given a PPTS S, a state q and a formula ϕ, we now consider the problem of finding an instance in $Set(S, q, \phi)$ such that the probability of reaching the state q is equal to a certain value $c \in [0, 1]$. Actually, Theorem 4.2 answers the problem of existence of an instance but does not give one. To find an instance u in $Set(S, q, \phi)$ such that $P_{S(u)}(q) = c$, is a harder problem with respect to the problem of existence of an instance. More precisely, to find an instance in $Set(S, q, \phi)$ is in general undecidable.

The following theorem, which derives from Galois' theory, states that it is in general impossible to find the roots of a polynomial of degree higher than 4 (see [Ste89]).

Theorem 4.1. It is impossible to give a general algebraic formula to solve polynomials of degree 5 and higher.

The next proposition follows directly from Theorem 4.1.

Proposition 4.2. Given a PPTS S, a state q and a formula ϕ, the problem of finding an instance u such that $u \in Set(S, q, \phi)$ is in general unsolvable.

Proof. The problem of finding an instance $u \in Set(S, q, \phi)$ is equivalent to the problem of finding the roots of a general polynomial. □

Hence, to have decidability, we must consider some restrictions. In particular, we give a restriction on the degrees of the polynomials generated by a PPTS.

Definition 4.2 (Degree of a Polynomial Term). Let τ be a polynomial term and β be a parameter. The *degree* of τ w.r.t. β, denoted with $dg(\tau, \beta)$, is the maximum natural number n such that α^n appears in τ.

Let $Q = \{q_1, \ldots, q_n\}$ be the states of S such that q_n is equal to q.

By Corollary 3.1, $P_{S(u)}(q)$ is the solution of x_{q_0} in the following system of linear equations:

$$
I = \left\{ \begin{array}{l} x_q = 1 \\ x_{q'} = \sum_{(q', q'') \in AdmTr(q', q)} \lambda((q', q'')) \cdot x_{q''} \quad \forall q' \neq q \, . \end{array} \right.
$$

The system I can be written as $Ax = B$, where x is the vector of the variables $x_{q_1}, \ldots, x_{q_n}$, B is the vector of naturals representing the known terms, and A is the matrix such that the $A[i, j] = \lambda((q_i, q_j))$ if $(q_i, q_j) \in AdmTr(q_i, q)$ and $A[i, j] = 0$ otherwise.

Let A' be the matrix obtained from A by substituting the first column with B.

Let τ_1 be the polynomial computed as the determinant of the matrix A' and τ_2 be the polynomial computed as the determinant of the matrix A.

By using Cramer's rule, we prove the following proposition.

Proposition 4.3. Given a PPTS $S = (\Delta, Q, q_0, \delta, \lambda)$ and a state $q \in Q$, two polynomials $\tau_1, \tau_2 \in \mathcal{P}(\Delta)$ can be found in polynomial time w.r.t. the size of S, such that, for any well defined instance u, it holds that $P_{S(u)}(q) = \frac{u(\tau_1)}{u(\tau_2)}$.

Proof. By Corollary 3.1 and following Equation (4), we have that the possible values that $P_{S(u)}(q)$ can assume for any well defined instance u are those of the variable x_{q_0} of the system of equations

$$x_q = 1 \wedge \bigwedge_{q' \in Adm(q)} x_{q'} = \sum_{(q',q'') \in AdmTr(q',q)} \lambda((q',q'')) \cdot x_{q''}.$$

This can be solved as a system of linear equalities, and hence $x_{q_0} = \frac{\tau_1}{\tau_2}$ for some $\tau_1, \tau_2 \in \mathcal{P}(\Delta)$. □

Example 4.2. Let us consider the PPTS S of example of Figure 2. We have that $P_{S(u)}(q_5) = \frac{u(\tau_1)}{u(\tau_2)}$ where $\tau_1 = 7\alpha_1(\alpha_1 + \alpha_2 + \frac{1}{4}) + (12 - 3\alpha_1)(\frac{3}{4} - \frac{1}{3}\alpha_1)$ and $\tau_2 = 12 - 3\alpha_1$.

We now define the degree of a PPTS S w.r.t. a state and a parameter.

Definition 4.3 (Degree of a PPTS). For a PPTS S, *the degree of S for parameter α and state q* (written $dg(S, \alpha, q)$) is equal to the value $max(dg(\tau_1, \alpha), dg(\tau_2, \alpha))$, where τ_1 and τ_2 are the polynomials of Proposition 4.3.

Example 4.3. Let us consider the PPTS S of example of Figure 2. We have that $dg(S, \alpha_1, q_5) = 2$ and $dg(S, \alpha_2, q_5) = 1$.

4.2.1. One Parameter

Theorem 4.2. Let $S = (\{\alpha\}, Q, q_0, \delta, \lambda)$ be a PPTS and q be a state in Q such that $dg(S, \alpha, q) \leq 4$. Let ϕ be a general formula and $c \in [0, 1]$; a well defined instance u, such that $u \in Set(S, q, \phi)$ and $P_{S(u)}(q) = c$, can be found in polynomial time w.r.t. the size of S.

Proof. By Proposition 4.3 we have that $P_{S(u)}(q) = \frac{u(\tau_1)}{u(\tau_2)}$. Since we are looking for an instance u such that $P_{S(u)}(q) = c$, we must solve the equation $c = \frac{\tau_1}{\tau_2}$, but this is equivalent to $\tau_1 - c \cdot \tau_2 = 0$ when $\tau_2 \neq 0$.

The steps of the proof are the following:

1. $\tau_1 - c \cdot \tau_2 = 0$ is a polynomial of degree 4 and hence one can compute the finite set C of its roots;
2. we can check, for any root r in C, whether r satisfies $\tau_2 \neq 0$, ϕ and the definition of DTMCs.

The set C of roots of the polynomial $\tau_1 - c \cdot \tau_2$ of degree at most 4 on the only parameter α is computable (see [Ste89]). Obviously $|C| \leq dg(S, \alpha, q) \leq 4$. Let U be the set of instances u such that $u(\alpha) \in C$. Obviously $|U| \leq 4$. Let U' be the set of instances $u \in U$ such that $u \models \tau_2 \neq 0 \wedge \phi$; we have that $u \models \tau_2 \neq 0 \wedge \phi$ can be checked in polynomial time on the length of ϕ and τ_2, by using the definition of $\models$. Since $|U| \leq 4$, U' can be computed in polynomial time.

Now, we must look for a $u \in U'$ such that $S(u)$ is a DTMC. To do that it suffices to check whether there exists $u \in U'$ such that

$$u \models \bigwedge_{e \in \delta} \lambda(e) \in [0, 1] \wedge \bigwedge_{q' \in Q} \sum_{e \in Start(q')} \lambda(e) = 1.$$

Obviously, this can be checked in polynomial time on the size of S, by using the definition of $\models$. □

Example 4.4. Consider the PPTS S of Figure 2 where $\alpha_2 = 0$. We look for an instance $u \in Set(S, q_4, \alpha_1 \geq \frac{1}{2})$ such that $P_{S(u)}(q_4) = \frac{1}{6}$. We have that $dg(S, \alpha_1, q) = 2$. Actually, $P_{S(u)}(q_4) = \frac{u(\tau_1)}{u(\tau_2)}$, where $\tau_1 = \alpha_1^2 + 2\alpha_1 - 3$ and $\tau_2 = 3\alpha_1 - 12$.

Hence we must find a value for α_1 such that $\frac{\tau_1}{\tau_2} = \frac{1}{6}$, which is equivalent to solving the equation $6\alpha_1^2 + 9\alpha_1 - 6 = 0$. The solutions are $\alpha_1 = -2$ and $\alpha_1 = \frac{1}{2}$. We must check whether these solutions are admissible. First of all we require that $\alpha_1 \geq \frac{1}{2}$. Hence $\alpha_1 = -2$ is not an admissible solution (note that a valuation with $\alpha_1 = -2$ is also not well defined). Now, it is easy to check that for $\alpha_1 = \frac{1}{2}$ we have that $\lambda(e) \in [0, 1]$, for all transitions e, and $\sum_{e \in Start(q')} \lambda(e) = 1$, for each state q'.

In the following lemma we give a syntactical characterization of PPTSs in terms of $dg(S, \alpha, q)$, allowing to check whether the hypotheses of Theorem 4.2 are satisfied. The idea is that, given a state q of a PPTS S with one only parameter, if the sum on the states q' of S of the maximal degree of polynomials labelling

a transition in $AdmTr(q', q)$ is less than or equal to c, then $dg(S, \alpha, q) \leq c$. Obviously, if $c \leq 4$ Theorem 4.2 can be applied.

As an example, let us consider the PPTS S of Figure 2 with $\alpha_2 = 0$ (S has only one parameter, namely α_1). If we are interested in state q_4, the maximal degree of polynomials labelling a transition in $AdmTr(q_0, q_4)$ is 1, in $AdmTr(q_1, q_4)$ is 1, and in $AdmTr(q_2, q_4)$ is 0. Actually, in Example 4.4 we have already seen that $dg(S, \alpha_1, q) = 2$.

¿From now on, we use $max(\alpha, q', q)$ to denote $max\{dg(\lambda(e), \alpha) | e \in AdmTr(q', q)\}$.

Lemma 4.1. Let $S = (\Delta, Q, q_0, \delta, \lambda)$ be a PPTS, q be a state and $\alpha \in \Delta$ such that $\sum_{q' \in Q} max(\alpha, q', q) \leq c$, for some natural number c, then it holds that $dg(S, \alpha, q) \leq c$.

Proof. The steps of the proof are the following: by Proposition 4.3, τ_1 and τ_2 are computed as the determinants of A' and A, respectively. We compute the determinant of A by rows, hence, by induction on the number of rows in the algorithm for computing the determinant, we prove that $dg(\tau_2, \alpha) \leq c$ and $dg(\tau_1, \alpha) \leq c$, and hence $dg(S, \alpha, q) \leq c$.

Now, the maximal degree that appears in each row i is $max(\alpha, q_i, q)$. By induction on the number of rows in the algorithm for computing the determinant we have that: $dg(\tau_2, \alpha) \leq \sum_{q_i \in Q} max(\alpha, q_i, q) = \sum_{q' \in Q} max(\alpha, q', q) \leq c$.

Hence, $dg(\tau_2, \alpha) \leq c$, and similarly we can prove that $dg(\tau_1, \alpha) \leq c$. Therefore $dg(S, \alpha, q) \leq c$. □

Thus, by Lemma 4.1 and Theorem 4.2, we have the following theorem that gives a syntactical characterization of the PTTSs for which it is possible to find a solution.

Theorem 4.3. Let $S = (\{\alpha\}, Q, q_0, \delta, \lambda)$ be a PPTS and q be a state such that $\sum_{q' \in Q} max(\alpha, q', q) \leq 4$. For any general formula ϕ and $c \in [0, 1]$, a well defined instance u, such that $u \in Set(S, q, \phi)$ and $P_{S(u)}(q) = c$ can be found in polynomial time w.r.t. the size of S.

4.2.2. Two Parameters

We extend the result of Theorem 4.2 to the case of two parameters. To do this, we must restrict to linear formulae and linear PPTS.

Theorem 4.4. Let $S = (\{\alpha_1, \alpha_2\}, Q, q_0, \delta, \lambda)$ be a linear PPTS and q be a state in Q such that $dg(S, \alpha_1, q) \in [1, 3]$ and $dg(S, \alpha_2, q) = 1$. Let ϕ be a linear formula and $c \in [0, 1]$; a well defined instance u, such that $u \in Set(S, q, \phi)$ and $P_{S(u)}(q) = c$, can be found in polynomial time w.r.t. the size of S.

Proof. By Proposition 4.3 we have that $P_{S(u)}(q) = \frac{u(\tau_1)}{u(\tau_2)}$. Since we are looking for an instance u such that $P_{S(u)}(q) = c$, we must solve the equation $c = \frac{\tau_1}{\tau_2}$, but this is equivalent to $\tau_1 - c \cdot \tau_2 = 0$ when $\tau_2 \neq 0$.

The steps of the proof are the following:

1. we compute two polynomials a_1 and a_2 on the only parameter α_1 of degree at most 3 such that $\alpha_2 = -\frac{a_2}{a_1}$;
2. we substitute α_2 with $-\frac{a_2}{a_1}$ in $\tau_2 \neq 0$ and in ϕ. We have now formulae on the only parameter α_1 and with degree less or equal to 4;
3. since it is decidable to find the roots of a polynomial on only one parameter and of degree less or equal to 4, one can find a finite union of intervals expressing the values that α_1 can assume. Hence, fixed α_1, we find α_2 thanks to the expression $\alpha_2 = -\frac{a_2}{a_1}$.

By hypothesis, $\tau_1 - c \cdot \tau_2$ has degree equal to 1 for parameter $\alpha_2 \in \Delta$. Hence, $\tau_1 - c \cdot \tau_2 = 0$ can be written as the polynomial $a_1\alpha_2 + a_2 = 0$ where a_1 and a_2 are two polynomials on the only parameter α_1 of degree at most 3.

As for Theorem 4.2, an instance u must satisfy $\tau_2 \neq 0$, the formula ϕ, and the requirements for S to be realizable (see ϕ_R in Equation (1)). Hence, the following ϕ' must be satisfied:

$$(\tau_2 \neq 0) \wedge \phi \wedge (\bigwedge_{e \in \delta} \lambda(e) \in [0, 1]) \wedge (\bigwedge_{q' \in Q} \sum_{e \in Start(q')} \lambda(e) = 1) .$$

Let ϕ'' be the formula resulting by substituting in the formula ϕ' the parameter α_2 with $-\frac{a_2}{a_1}$. We have

that in ϕ'' only the parameter α_1 appears with degree at most 4. Actually, ϕ' is a linear formula since S and ϕ are linear, and hence, the product between a polynomial of degree 3 with a polynomial of degree 1 returns a polynomial of degree 4.

Given a generic polynomial τ of degree at most 4 on the only parameter α_1, the set C of roots of τ is computable in polynomial time ([Ste89]). Obviously, $|C| \leq dg(S, \alpha_1, q) \leq 4$, hence, $\tau \sim 0$ can be easily translated into a formula of the form $\alpha_1 \in I_1 \cup \ldots \cup I_m$, for some intervals of reals I_j. Therefore, since $\alpha_1 \in I_1 \wedge \alpha_1 \in I_2$ is equivalent to $\alpha_1 \in I_1 \cap I_2$, then ϕ'' can be translated into a formula of the form $\alpha_1 \in I'_1 \cup \ldots \cup I'_k$, for some intervals of reals I'_j.

Thus, given the instance u such that $u(\alpha_1)$ in $I'_1 \cup \ldots \cup I'_k$ and $u(\alpha_2)$ is the value $-\frac{a_2}{a_1}$ where α_1 is substituted with $u(\alpha_1)$, we have that $u \in Set(S, q, \phi)$ and $P_{S(u)}(q) = c$. □

Example 4.5. The PPTS S of Figure 2 is linear. We look for an instance $u \in Set(S, q_5, \alpha_1 + \alpha_2 \geq \frac{1}{2})$ such that $P_{S(u)}(q_5) = \frac{1}{3}$. We have that $dg(S, \alpha_1, q_5) = 3$ and $dg(S, \alpha_2, q_5) = 1$ Actually, $P_{S(u)}(q_4) = \frac{u(\tau_1)}{u(\tau_2)}$, where $\tau_1 = -\frac{13}{16}\alpha_1 + \frac{17}{8}(\alpha_1)^2 + 2\alpha_1\alpha_2 - \frac{1}{4}(\alpha_1)^2\alpha_2 - \frac{1}{4}(\alpha_1)^3$ and $\tau_2 = \alpha_1\left(3 - \frac{3}{4}\right)$.

Hence, we must find a value for α_1 such that $\frac{\tau_1}{\tau_2} = \frac{1}{3}$, which is equivalent to solving the equation

$$\alpha_2 = -\frac{\frac{5}{4} - \frac{9}{16}\alpha_1 + \frac{17}{8}(\alpha_1)^2 - \frac{1}{4}(\alpha_1)^3}{2\alpha_1 - \frac{1}{4}(\alpha_1)^2}.$$

Now, we must substitute α_2 in the formula ϕ' that is equal to

$$\left(2\alpha_1 - \frac{1}{4}(\alpha_1)^2 \neq 0\right) \wedge \alpha_1 + \alpha_2 \geq \frac{1}{2} \wedge \left(\bigwedge_{e \in \delta} \lambda(e) \in [0,1]\right) \wedge \left(\bigwedge_{q' \in Q} \sum_{e \in Start(q')} \lambda(e) = 1\right).$$

We have that in ϕ' the parameter α_1 has a degree of at most 4. As an example, $\alpha_1 + \alpha_2 \geq \frac{1}{2}$ becomes

$$\alpha_1\left(2\alpha_1 - \frac{1}{4}(\alpha_1)^2\right) + \frac{5}{4} - \frac{9}{16}\alpha_1 + \frac{17}{8}(\alpha_1)^2 - \frac{1}{4}(\alpha_1)^3 \geq \frac{1}{2} \geq \frac{1}{2}\left(2\alpha_1 - \frac{1}{4}(\alpha_1)^2\right).$$

Hence, by solving this formula, we can find the intervals to which α_1 must belong.

As a consequence, by Lemma 4.1, we have the following theorem giving a syntactical characterization of PPTSs with two parameters satisfying the hypotheses of Theorem 4.4.

Theorem 4.5. Let $S = (\{\alpha_1, \alpha_2\}, Q, q_0, \delta, \lambda)$ be a linear PPTS and $q \in Q$ such that $\sum_{q' \in Q} max(\alpha_1, q', q) \in [1, 3]$ and $\sum_{q' \in Q} max(\alpha_2, q', q) = 1$. For any ϕ and $c \in [0, 1]$, a well defined instance u, such that $u \in Set(S, q, \phi)$ and $P_{S(u)}(q) = c$, can be found in polynomial time w.r.t. the size of S.

4.2.3. Rational Domain for Parameters

If one is interested in parameters assuming only rational values (as it may often be the case), our results are extended to systems with any degree. Namely, if one considers only rational instances, the following result can be derived by using Ruffini's method.

Corollary 4.3. Let $S = (\{\alpha\}, Q, q_0, \delta, \lambda)$ be a PPTS, q be a state in Q, ϕ be a general formula and $c \in [0, 1]$. A well defined instance u, such that $u \in Set(S, q, \phi)$, $u(\alpha)$ is a rational number and $P_{S(u)}(q) = c$, can be found in polynomial time w.r.t. the size of S.

Proof. Along the lines of the proof of Theorem 4.2 and by Ruffini's method that allows to find rational roots of a polynomial. Hence, the set C of rational roots of the polynomial $\tau_1 - c \cdot \tau_2$ is computable. □

4.3. Finding the Maximum/Minimum Instance

In this section, we consider the case in which one wants either to maximize or to minimize the probability of reaching a certain state. This problem may have interesting applications in practice, as we shall show in the next section.

4.3.1. One Parameter

Theorem 4.6 (Maximizing/Miniminizing). Let $S = (\{\alpha\}, Q, q_0, \delta, \lambda)$ be a PPTS and q be a state in Q such that $dg(S, \alpha, q) \leq 3$. For any formula ϕ, an instance $u \in Set(S, q, \phi)$, such that for each $u' \in Set(S, q, \phi)$ it holds that $P_{S(u)}(q) \geq P_{S(u')}(q)$ (resp. $P_{S(u)}(q) \leq P_{S(u')}(q)$), is computable in polynomial time w.r.t. the size of S.

Proof. The main steps of the proof are:

1. by following the proof of Theorem 4.2, we have to maximize (minimize) the function $\frac{\tau_1}{\tau_2}$;
2. to find the maximum (minimum) we compute the values of α that make null the derivative function of $\frac{\tau_1}{\tau_2}$.

By following the proof of Theorem 4.2 we have that $x_{q_0} = \frac{\tau_1}{\tau_2}$. Now, by mimicking the proof of Theorem 4.2, it is sufficient to maximize (minimize) the function $\frac{\tau_1}{\tau_2}$ in the space ϕ' that is equal to

$$\phi \wedge (\alpha_q \in [0,1]) \wedge (\bigwedge_{e \in \delta} \lambda(e) \in [0,1]) \wedge (\bigwedge_{q' \in Q} \sum_{e \in Start(q')} \lambda(e) = 1).$$

As done for Theorem 4.4, ϕ' can be translated into a formula of the form $\alpha \in I_1 \cup \ldots \cup I_m$, where I_j is an interval of real values.

The maximum of $\frac{\tau_1}{\tau_2}$ is when the derivative function $\frac{d}{d\alpha}\frac{\tau_1}{\tau_2} = 0$.

We have that $\tau_i = a_3^i\alpha^3 + a_2^i\alpha^2 + a_1^i\alpha + a_0^i$, for $i = 1, 2$. Hence, $\frac{d}{d\alpha}\frac{\tau_1}{\tau_2}$ is equal to

$$\frac{(a_3^1a_2^2 - a_2^1a_3^2)\alpha^4 + (2a_3^1a_1^2 - 2a_1^1a_3^2)\alpha^3 + (3a_3^1a_0^2 - 3a_0^1a_3^2 + a_2^1a_1^2 - a_1^1a_2^2)\alpha^2 + (2a_2^1a_0^2 - 2a_0^1a_2^2)\alpha + a_1^1a_0^2 - a_0^1a_1^2}{(\tau_2)^2}.$$

Therefore, the maximum value can be found by studying the function

$$(a_3^1a_2^2 - a_2^1a_3^2)\alpha^4 + (2a_3^1a_1^2 - 2a_1^1a_3^2)\alpha^3 + (3a_3^1a_0^2 - 3a_0^1a_3^2 + a_2^1a_1^2 - a_1^1a_2^2)\alpha^2 + (2a_2^1a_0^2 - 2a_0^1a_2^2)\alpha + a_1^1a_0^2 - a_0^1a_1^2$$

(which is a function of degree 4) in the space $\alpha \in I_1 \cup \ldots \cup I_m$, where I_j is an interval.

Since computing the terms τ_1, τ_2 takes a polynomial time w.r.t. the size of S, the problem of finding a maximal (minimal) solution is polynomial time w.r.t. the size of S. □

As done for Theorem 4.2, we can give a syntactical characterization of the PPTSs satisfying the conditions of Theorem 4.6. Actually, from Lemma 4.1 and Theorem 4.6 we have the following theorem.

Theorem 4.7. Let $S = (\{\alpha\}, Q, q_0, \delta, \lambda)$ be a PPTS and q be a state such that $\sum_{q' \in Q} max(\alpha, q', q) \leq 3$. For any formula ϕ, an instance $u \in Set(S, q, \phi)$, such that for each $u' \in Set(S, q, \phi)$ it holds that $P_{S(u)}(q) \geq P_{S(u')}(q)$ (resp. $P_{S(u)}(q) \leq P_{S(u')}(q)$), is computable in polynomial time w.r.t. the size of S.

4.3.2. Two Parameters

As for the problem of finding a solution, in this section we extend the result of Theorem 4.6 to two parameters. Again, to do that we must restrict to linear formulae and linear PPTS.

Theorem 4.8 (Maximizing/Miniminizing). Let $S = (\{\alpha_1, \alpha_2\}, Q, q_0, \delta, \lambda)$ be a linear PPTS and q be a state in Q such that $dg(S, \alpha_1, q) = dg(S, \alpha_2, q) = 1$. For any linear formula ϕ, an instance $u \in Set(S, q, \phi)$, such that for each $u' \in Set(S, q, \phi)$ it holds that $P_{S(u)}(q) \geq P_{S(u')}(q)$ (resp. $P_{S(u)}(q) \leq P_{S(u')}(q)$), is computable in polynomial time w.r.t. the size of S.

Proof. The main steps of the proof are:

1. by following the proof of Theorem 4.2 we have to maximize (minimize) the function $\frac{\tau_1}{\tau_2}$;
2. to find the maximum (minimum) we compute the values of α_1 and α_2 that make null the derivative function of $\frac{\tau_1}{\tau_2}$.

By following the proof of Theorem 4.2, we have that $x_{q_0} = \frac{\tau_1}{\tau_2}$. Now, by mimicking the proof of Theorem 4.2, it is sufficient to maximize (minimize) the function $\frac{\tau_1}{\tau_2}$ in the space ϕ' that is equal to

$$\phi \wedge (\alpha_q \in [0,1]) \wedge (\bigwedge_{e \in \delta} \lambda(e) \in [0,1]) \wedge (\bigwedge_{q' \in Q} \sum_{e \in Start(q')} \lambda(e) = 1).$$

We have that $\tau_i \equiv a_1^i \alpha_1 \alpha_2 + a_2^i \alpha_1 + a_3^i \alpha_2 + a_4^i$, for $i = 1, 2$. Hence,

$$\frac{d}{d\alpha_1} \frac{\tau_1}{\tau_2} = \frac{(a_1^1 a_3^2 - a_1^2 a_3^1)(\alpha_2)^2 + (a_1^1 a_4^2 + a_2^1 a_3^2 - a_1^2 a_4^1 + a_2^2 a_3^1)\alpha_2 + (a_2^1 a_4^2 - a_2^2 a_4^1)}{(\tau_2)^2}.$$

We note that $(a_1^1 a_3^2 - a_1^2 a_3^1)(\alpha_2)^2 + (a_1^1 a_4^2 + a_2^1 a_3^2 - a_1^2 a_4^1 + a_2^2 a_3^1)\alpha_2 + (a_2^1 a_4^2 - a_2^2 a_4^1)$ is a polynomial of degree 2 on the only parameter α_2. Similarly we can find $\frac{d}{d\alpha_2} \frac{\tau_1}{\tau_2}$. Thus, the maximum can be studied as done in Theorem 4.6. □

Now, as done for Theorem 4.6, from Lemma 4.1 and Theorem 4.8 we have the following theorem giving a syntactical characterization of PPTSs satisfying the hypoteses of Theorem 4.8.

Theorem 4.9. Let $S = (\{\alpha_1, \alpha_2\}, Q, q_0, \delta, \lambda)$ be a linear PPTS with $q \in Q$ such that $\sum_{q' \in Q} max(\alpha_1, q', q) = \sum_{q' \in Q} max(\alpha_2, q', q) = 1$. For any linear formula ϕ, an instance $u \in Set(S, q, \phi)$, such that for each $u' \in Set(S, q, \phi)$ it holds that $P_{S(u)}(q) \geq P_{S(u')}(q)$ (resp. $P_{S(u)}(q) \leq P_{S(u')}(q)$), is computable in polynomial time w.r.t. the size of S.

5. An Application: Probabilistic Non-Repudiation

In this section, as an application, we model and analyze a non-repudiation protocol that employs a probabilistic algorithm to achieve a fairness property. This protocol has been studied, from different points of view, also in [Ald02, LMT03, LMT05].

5.1. A Probabilistic Non-Repudiation Protocol

We consider a protocol that guarantees a non-repudiation service with a certain probability without resorting to a trusted third party [MR99]. In particular, such a probabilistic protocol is fair up to a given tolerance ε decided by the originator. Assume that an authentication phase precedes the protocol. We denote by $Sign_E(M)$ the encryption of message M under the private key of the entity E and with $\{M\}_K$ the encryption of M under the key K. Finally, we use t to denote a time stamp. The protocol can be described as follows (with the notation $R \rightarrow O : Msg$ we denote a message Msg sent by R and received by O):

1.	$R \rightarrow O:$	$Sign_R(request, R, O, t)$	
2.	$O \rightarrow R:$	$Sign_O(\{M\}_K, O, R, t)$	$(= M_1)$
3.	$R \rightarrow O:$	$Sign_R(ack_1)$	
4.			
$a._{1-p}$	$O \rightarrow R:$	$Sign_O(M_r, O, R, t)$	$(= M_i)$
	$R \rightarrow O:$	$Sign_R(ack_i)$	
		goto step 4	
$b._p$	$O \rightarrow R:$	$Sign_O(K, O, R, t)$	$(= M_n)$
5.	$R \rightarrow O:$	$Sign_R(ack_n)$	

The recipient R starts the protocol by sending a signed, timestamped request to the originator O. This sends to R the requested message M ciphered under the key K, and waits for the ack from R (ack_i represents the acknowledgment related to message M_i). At step 4 the originator makes a probabilistic choice according to p. At step $4a$ (taken with probability $1 - p$) O sends to R a random message M_r (i.e. a dummy key), receives the ack and returns to step 4, while at step $4b$ (taken with probability p) O sends to R the key K necessary to decrypt the message $\{M\}_K$. Upon reception of the last ack (ack_n), related to the message containing the key K, the originator terminates the protocol correctly. We suppose that each message ack_i

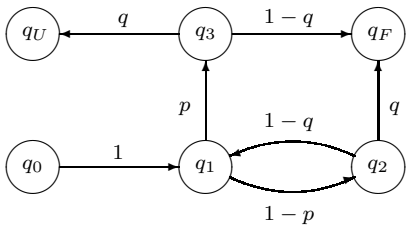

Fig. 3. Parametric Representation of the Protocol.

has the following semantics: "R acknowledges having received message M_i from O". This could be easily obtained, for instance, by assuming that each ack_i message contains an hash of message M_i.

Intuitively, the non-repudiation of origin is guaranteed by the messages M_1 and M_n (signed with the private key of O), while the non repudiation of receipt is given by the last message $Sign_R(ack_n)$. If the protocol terminates after the delivery of the last ack, both parties obtain their expected information, and the protocol is fair. If the protocol terminates before sending the message containing the key K, then neither the originator nor the recipient obtains any valuable information, thus preserving fairness. A strategy for a dishonest recipient consists in guessing the last message containing the key K, verifying whether a received message contains the needed key, and then blocking the transmission of the last ack. Therefore, for the success of the protocol, it is necessary that the ack messages are sent back immediately. The originator decides a deadline for the reception of each ack, after which, if the ack is not received, the protocol is stopped. Obviously, the cryptosystem must be adequately chosen, in such a way that the time needed to verify a key, by deciphering the message, is longer than the transmission time of an ack message. Anyway, as we will see in the next section, a malicious recipient can try to randomly guess the message containing the key K, and in this case the probability for the recipient of guessing the last message depends on the parameter p chosen by the originator.

5.2. Parametric Analysis of the Protocol

In this section we describe the protocol by using the model of PPTSs. In particular we use two parameters, p and q. On the one hand, we assume that the originator follows a Bernoulli distribution with parameter p to decide either to send the real key or to send a dummy key (see step 4 of the protocol). On the other hand, we assume that the recipient follows a Bernoulli distribution with parameter q to decide either to send the ack message or to try to compute M by employing the last received message. In Figure 3 we show a parametric Probabilistic Transition System modelling the communication between the originator and the recipient according to the parameters p and q.

With the transition (q_0, q_1) we model the recipient starting a communication with the originator by sending a request, the originator sending the first ciphered message and the recipient acknowledging such a message. In state q_1 the originator sends, with probability $1-p$, a dummy key reaching state q_2 and, with probability p, sends the last message containing K and reaches state q_3. In state q_2 the recipient sends an ack to the originator with probability $1-q$ going back to state q_1, while with probability q the recipient uses the dummy key in order to decipher the first message, fails and the protocol is stopped. In this case, state q_F is reached. Intuitively, state q_F models a situation in which the protocol ends in a fair way (both participants receive their expected information or neither the originator nor the recipient obtains any valuable information). In state q_3 the recipient sends the last ack with probability $1-q$ and fairly terminates the protocol, and tries to decipher the first message with the last received key (in this case the correct key K) with probability q. In this case, without sending the last ack, the recipient breaks the fairness of the protocol (state q_U represents the situation in which the protocol ends in an unfair way).

Let us assume as S the PPTS of Figure 3 (where we omitted self-loops for states q_U and q_F).

If we are interested in the probability of reaching state q_F we can follow the system of linear equations of Corollary 3.1, and get $x_{q_0} = \frac{p+q-2pq}{p+q-pq}$.

Now, as an example, to find a well defined instance u such that $P_{S(u)}(q_F) = 0.9$ it is sufficient to apply Theorem 4.2. We have that $P_{S(u)}(q_F) = 0.9$ is equivalent to $\frac{1}{10}p + \frac{1}{10}q - \frac{11}{10}pq = 0$. Therefore, we have that

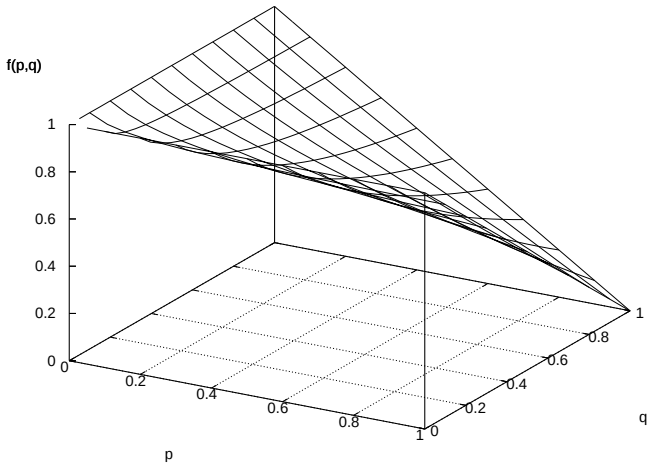

Fig. 4. $f(p,q)$: probability of reaching q_F on the parameters p and q.

$p = \frac{q}{11q-1}$ and $q \in \{0\} \cup (\frac{1}{11}, 1]$. We have a well defined instance for $u(p) = \frac{1}{4}$ and $u(q) = \frac{1}{7}$.

Now, we want to find a well defined instance u such that $\forall u' \in Set(S, q_F, true)\ P_{S(u)}(q_F) \geq P_{S(u')}(q_F)$ and $P_{S(u)}(q_F) \in [0,1]$ (namely, an instance that maximizes the probability of having a fair communication).

Now, we must find the maximum of the function $f(p,q) = \frac{p+q-2pq}{p+q-pq}$. We compute the derivative of f w.r.t. p and q. We have that $\frac{d}{dp}f(p,q) = \frac{-q^2}{(p+q-pq)^2}$ and $\frac{d}{dq}f(p,q) = \frac{-p^2}{(p+q-pq)^2}$. Hence, the function f is decreasing w.r.t. p for q (the point $(0,0)$ is a point of contrary flexure), and therefore, the maximum in the space $[0,1]$ is, indeed, 1 by choosing $q = 0$ or $p = 0$. Notice that the case $u(q) = 0$ models an attacker behaving correctly (he never tries to break the protocol), while the case $u(p) = 1$ models an originator that never sends the last message (hence the protocol cannot be broken).

We may suppose q to be a fixed constant and not a parameter. In this case, we want to find an instance for p (chosen by the originator) that maximizes the probability of reaching state q_F. In this manner the originator can choose the best value for p that minimizes the probability that the protocol ends in an unfair way. Let S' be the PPTS of Figure 3 with $q = \frac{1}{2}$ (namely, the attacker throws a coin to decide whether to decipher the key or not). We want to find a well defined instance u such that $\forall u' \in Set(S', q_F, true)\ P_{S'(u)}(q_F) \geq P_{S'(u')}(q_F)$ (namely, an instance that maximizes the probability of having a fair communication).

For state q_F and with $q = \frac{1}{2}$, we get $x_{q_0} = \frac{1}{1+p}$. Now, we can find the value of p that maximizes the function $\frac{1}{1+p}$, by studying its derivative $\frac{d}{dp}\frac{1}{1+p} = \frac{-1}{(1+p)^2}$. Since such a function is decreasing in $(-\infty, \infty)$ and $p \in [0,1]$, the maximum is for $u(p) = 0$ and, in this case, $P_{S'(u)}(q_F) = 1$. Again, if $p = 0$ the originator will never send the last message containing the correct key, fairness will not be broken, but the protocol will never terminate correctly. Differently, if the originator wants a probability of fair communication equal to 0.999, then it is sufficient to apply Theorem 4.2 which gives $\frac{1}{1+p} = 0.999$, and therefore $p = \frac{0.001}{0.999}$.

A full study of the function $f(p,q)$ is in Figure 4.

Viceversa, we may be interested in studying the value of q (chosen by the attacker) that maximizes the probability of breaking protocol fairness, namely the probability of reaching state q_U. In this case, we have $x_{q_0} = f'(p,q) = \frac{pq}{p+q-pq}$ and $\frac{df'}{dq} = \frac{p^2}{(p+q-pq)^2}$, which is decreasing w.r.t. q and, therefore, the maximum in the space $[0,1]$ is for $q = 1$. Thus, the maximum chance for the attacker of breaking protocol fairness is when choosing $u(q) = 1$, with $P_{S(u)}(q_U) = p$. This guarantees that protocol fairness (once the originator has chosen the parameter p) cannot be broken with probability greater than p, thus allowing the originator to chose the security threshold $1 - p$ for the correct termination of the protocol. Moreover, the probability of a successful attack decreases by choosing a smaller p. In this case, however, the number of dummy messages

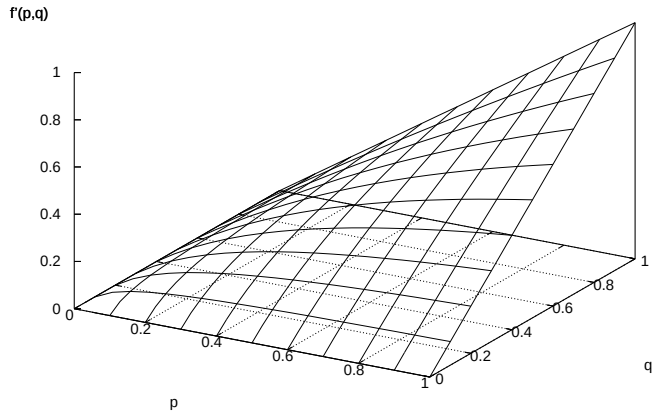

Fig. 5. $f'(p,q)$: probability of reaching state q_U on the parameters p and q.

sent by O, and hence the length of the protocol execution, will increase. Hence, the originator must choose a value for p that guarantees a good security level with the desired performance.

Note that while $f(p,q)$ gives the probability of reaching the fair state q_F, function $f'(p,q)$ gives the complementary probability of reaching the unfair state q_U. Namely, we have that $f'(p,q) = 1 - f(p,q)$.

A full study of the function $f'(p,q)$ is in Figure 5.

6. Conclusions and Future Work

In this paper we have developed a model of Parametric Probabilistic Transition Systems. In this model probabilities associated with transitions may be parameters. We have shown how we can find instances of parameters that satisfy a given property and instances that either maximize or minimize the probability of reaching a given state. As an application we have shown the model of a probabilistic non repudiation protocol.

Our results are obtained under the assumption that the number of parameters is at most two. We have shown that such a class of systems is expressive enough to describe and analyze many real–life systems. However, if one faces systems with more than two parameters, the method we propose can still be useful insofar as the system considered may be studied by fixing the value of all parameters but two. Moreover, it is often possible to decompose the system into independent components with at most two parameters (e.g., see the analysis of the IPv4 zeroconf protocol in [BSHV03]).

As a future work, we plan to extend our study to Probabilistic Labeled Transition Systems, where transitions from state to state are labeled by actions. These are the actions selected by an environment and to which the system reacts. For each label there is a transition probability distribution which gives the probability distribution of the possible final states for a given initial state. In a discrete setting this is the model considered by [LS91]. Models with continuous state space or continuous time (or both) have been considered (see, for instance, [DGJP03]). It would be interesting to define and study parameterized versions also of these formalisms.

An other direction may consist in the defintion of equivalences for PPTSs. To compare probabilistic systems, one may consider the notion of metric, which is a function that associates a real number (distance) to a pair of elements. In [DJGP02, DJGP04, DCPP05] metrics are introduced in order to quantify the similarity of the behavior of probabilistic transitions systems. One may study, for example, how this kind of metrics can be adapted to deal with parametric probabilistic systems.

References

[Ald02] A. Aldini, and R. Gorrieri: *Security Analysis of a Probabilistic Non-repudiation Protocol*. In Proc. of PAPM-PROBMIV'02, Springer LNCS 2399, 2002, 17–36.

[Alf98] L. de Alfaro: *How to specify and verify the long-run average behaviour of probabilistic systems*. In Proc. of LICS'98, IEEE Press, 1998, 454–465.

[Alf99] L. de Alfaro: *Computing minimum and maximum reachability times in probabilistic systems*. In Proc. of CONCUR'99, Springer LNCS 1664, 1999, 66–81.

[AHV93] R. Alur, T. A. Henzinger, and M. Y. Vardi: *Parametric real-time reasoning*. In Proc. of STOC'93, ACM press, 1993, 592–601.

[AD94] R. Alur, D. L. Dill: *A Theory of Timed Automata*. Theoretical Computer Science 126, 1994, 183–235.

[UPPAAL] T. Amnell, G. Behrmann, J. Bengtsson, P. R. D'Argenio, A. David, A. Fehnker, T. Hune, B. Jeannet, K. G. Larsen, M. O. Moeller, P. Pettersson, C. Weise, and W. Yi: *Uppaal-now, next and future*. In Proc. of MOVEP'00, Springer LNCS 2067, 2000, 99–124.

[BBS95] J. C. M. Baeten, J. A. Bergstra, and S. A. Smolka: *Axiomatizing probabilistic processes: ACP with generative probabilities*. Information and Computation 121, 1995, 234–255.

[BK98a] C. Baier, and M. Kwiatkowska: *On the verification of qualitative properties of probabilistic processes under fairness constraints*. Information Processing Letters 66, 1998, 71–79.

[BK98b] C. Baier, and M. Kwiatkowska: *Model checking for probabilistic time logic with fairness*. Distributed Computing 11, 1998, 125–155.

[Bea02] D. Beauquier: *Markov Decision Processes and Buchi Automata*. Fundamenta Informaticae 50, 2002, 1–13.

[Bel57] R. E. Bellman: *Dynamic Programming*. Princeton University Press, 1957.

[BdA95] A. Bianco, and L. de Alfaro: *Model checking of probabilistic and deterministic systems*. In Proc. of 15th Conference on Foundations of Computer Technology and Theoretical Computer Science, Springer LNCS 1026, 1995, 499–513.

[BSHV03] H. Bohnenkamp, P. van der Stok, H. Hermanns, and F. Vaandrager: *Costoptimization of the IPv4 zeroconf protocol*. In Proc. of DSN'03, IEEE Press, 2003, 531–540.

[Cha88] D. L. Chaum: *The dining cryptographers problem: Unconditional sender and recipient untraceability*. Journal of Cryptology 1(1), 1988, 65–75.

[CSZ92] R. Cleaveland, S. A. Smolka, and A. Zwarico: *Testing preorders for probabilistic processes*. In Proc. of ICALP'92, Springer LNCS 623, 1992, 708–719.

[Daw04] C. Daws: *Symbolic and Parametric Model Checking of Discrete-Time Markov Chains*. In Proc. of ICTAC'04, Springer LNCS 3407, 2004, 280–294.

[DCPP05] Y. Deng, T. Chothia, C. Palamidessi and J. Pang: *Metrics for Action-labelled Quantitative Transition Systems*. In Proc. of QAPL'05, Elsevier ENTCS 153(2), 2006, 79–96.

[DJGP02] J. Desharnais, R. Jagadeesan, V. Gupta and P. Panangaden: *The metric analogue of weak bisimulation for probabilistic processes*. In Proc. of LICS'02, IEEE Press, 2002, 413–422.

[DJGP04] J. Desharnais, R. Jagadeesan, V. Gupta and P. Panangaden: *Metrics for labelled Markov processes*. Theoretical Computer Science 318(3), 2004, 323–354.

[DEP98] J. Desharnais, A. Edalat, and P. Panangaden: *A logic characterization of bisimulation for Markov Processes*. In Proc. of LICS'98, IEEE Press, 1998, 478–487.

[DGJP03] J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden: *Approximating Labelled Markov Processes*. Information and Computation 184, 2003, 160–200.

[Hal50] P. R. Halmos: *Measure Theory*. Springer-Verlag, 1950.

[Han94] H. Hansson: *Time and probability in formal design of distributed systems*. Real-Time Safety Critical Systems 1, Elsevier, 1994.

[HJ94] H. Hansson and B. Jonsson: *A Logic for Reasoning about Time and Reliability*. Formal Aspects of Computing 6, 1994, 512–535.

[HHW97] T. A. Henzinger, P.-H. Ho and H. Wong-Toi: *HyTech: A Model Checker for Hybrid Systems*. In Proc. of CAV'97, Springer LNCS 1254, 1997, 460–463.

[How60] H. Howard: *Dynamic Programming and Markov Processes*. MIT Press, 1960.

[HRSV02] T. Hune, J. Romijn, M. Stoelinga and F. W. Vaandrager: *Linear parametric model checking of timed automata*. J. Log. Algebr. Program. 52–53, 1960, 183–220.

[JL91] B. Jonsson, and K. Larsen: *Specification and refinement of probabilistic processes*. In Proc. of LICS'91, IEEE Press, 1991, 266–277.

[KSK66] J. Kemeny, J. Snell and A. Knapp: *Denumerable Markov Chains*. D. Van Nostrand Company Inc., 1966.

[LMT03] R. Lanotte, A. Maggiolo-Schettini, and A. Troina: *Weak Bisimulation for Probabilistic Timed Automata and Applications to Security*. In Proc. of SEFM'03, IEEE Press, 2003, 34–43.

[LMT04] R. Lanotte, A. Maggiolo-Schettini, and A. Troina: *Decidability Results for Parametric Probabilistic Transition Systems with an Application to Security*. In Proc. of SEFM'04, IEEE Press, 2004, 114–121.

[LMT05] R. Lanotte, A. Maggiolo-Schettini, and A. Troina: *Automatic Analysis of a Non-Repudiation Protocol*. In Proc. of QAPL'03, Elsevier ENTCS 112, 2005, 113–129.

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

[Mal95] O. Maler: *A decomposition theorem for probabilistic transition systems*. Theoretical Computer Science 145, 1995, 391–396.

[MR99] O. Markowitch, and Y. Roggeman: *Probabilistic Non-Repudiation without Trusted Third Party*. In Proc. of 2nd Conference on Security in Communication Network, 1999.

[RSG98] M. G. Reed, P. F. Syverson and D. M. Goldschlag: *Anonymous Connections and Onion Routing*. IEEE Journal on Selected Areas in Communications 16(4), 1998, 482–494.

[RR98] M. K. Reiter, and A. D. Rubin: *Crowds: anonymity for Web transactions*. ACM Transactions on Information and System Security 1(1), 1998, 66–92.

[Ren92] J. Renegar: *On the Computational Complexity and Geometry of the First-Order Theory of the Reals, Part I: Introduction. Preliminaries. The Geometry of Semi-Algebraic Sets. The Decision Problem for the Existential Theory of the Reals*. J. Symb. Comput. 13, 1992, 255–300.

[Ros83] S. Ross: *Stochastic Processes*. John-Wiley, 1983.

[SS98] E. Stark, and S. A. Smolka: *Compositional analysis of expected delays in networks of probabilistic I/O automata*. In Proc. of LICS 98, IEEE Press, 1998, 466–477.

[Ste89] I. Stewart: *Galois Theory*. Chapman and Hall, 1989.

[TNHH98] T. Tanimoto, A. Nakata, H. Hashimoto and T. Higashino: *Double Depth First Search Based Parametric Analysis for Parametric Time–Interval Automata*. IEICE Transaction on Fundamentals 11, 2005, 3007–3021.

[Tar51] A. Tarski: *A Decision Method for Elementary Algebra and Geometry*. University of California Press, Second Edition, 1951.

[Wil91] D. Williams: *Probability with Martingales*. Cambridge University press, 1991.

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