Decidability Results for Parametric Probabilistic Transition Systems with an Application to Security

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

Andrea Maggiolo-Schettini and Angelo Troina
Dipartimento di Informatica - Università di Pisa
Via Buonarroti 2, 56127 Pisa, Italy
{maggiolo,troina}@di.unipi.it

Abstract

We develop a model of Parametric Probabilistic Transition Systems. In this model probabilities associated with transitions may be parameters, and we show how to find instances of parameters that satisfy a given property and instances that either maximize or minimize the probability of reaching a given state. We show, as an application, the model of a probabilistic non repudiation protocol. 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).

1 Introduction

Many formalisms have been proposed to specify and verify systems in which the behavior is controlled by decisions that can be taken at each state of the system, based on a probabilistic choice [2, 3, 4, 5, 6, 7, 8, 9, 10, 13, 14, 18, 20, 21]. Such frameworks have been used to describe and analyze fault tolerant systems, randomized algorithms and communication protocols. To model systems of this kind it may be useful to represent probabilities as parameters which can be instantiated such that the system enjoys some given property.

In this paper we develop a model of Parametric Probabilistic Transition Systems and we show how to find instances of parameters that satisfy a given property and instances that either maximize or minimize the probability of reaching a given state.

In Section 2 we recall some basic notions. In Section 3 we introduce Parametric Probabilistic Transition Systems. In Section 4 we tackle the problem of existence of instances of parameters which satisfy a given property and of finding optimal instances. In Section 5, as an application, we show the model of a probabilistic non-repudiation protocol. In Section 6 we anticipate some future work.

2 Basic notions

With $\alpha, \beta, \ldots$ we denote *parameters* assuming real values. An $instance$ u is a function assigning a real value to each parameter.

We define the set $\mathcal{P}$ of *polynomial terms* over parameters as follows:

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

where $\tau, \tau_1, \tau_2 \in \mathcal{P}$, $c \in \mathbb{R}$ and α is a parameter. A polynomial term is a *linear term* if it is constructed without operation $\tau_1 \cdot \tau_2$. With $Par(\tau)$ we denote the set of parameters appearing in the term τ.

An instance u extends to $\mathcal{P}$ as follows:

$$\begin{array}{rcl} u(c) & = & c \\ u(c \cdot \alpha) & = & c \cdot u(\alpha) \\ u(\tau_1 + \tau_2) & = & u(\tau_1) + u(\tau_2) \\ u(\tau_1 \cdot \tau_2) & = & u(\tau_1) \cdot u(\tau_2). \end{array}$$

We define the set Φ 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 ϕ, ϕ_1, ϕ_2 range over Φ, τ, τ' are in $\mathcal{P}$, and $\sim \in \{<, \leq, =, \geq, >\}$. A formula in Φ is *linear* iff all terms $\tau \in \mathcal{P}$ appearing in ϕ are linear. With $Par(\phi)$ we denote the set of parameters appearing in ϕ.

Let $\phi \in \Phi$ 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.

Theorem 2.1 *For each $\phi \in \Phi$, it is decidable in exponential time w.r.t. the size of ϕ whether there exists an instance u such that $u \models \phi$.*

3 Parametric Probabilistic Transition Systems

Definition 3.1 *A* Parametric Probabilistic Transition System *S is a quadruple (Q, q_0, Tr, λ) such that:*

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

If q is a state, then with $Start(q)$ we denote the set of transitions with source q in S, namely the set $\{(q_i, q_j) \in Tr \mid q_i = q\}$. Moreover, with $Par(S)$ we denote the set of parameters appearing in the terms assigned by λ to transitions.

Example 3.2 *Consider the Parametric Probabilistic Transition System of Figure 1. As an example, we have $\lambda((q_2, q_5)) = \alpha_1 + \alpha_2$, $Start(q_2) = \{(q_2, q_1), (q_2, q_3), (q_2, q_5)\}$, and $Par(S) = \{\alpha_1, \alpha_2\}$.*

A *run* of S is a possible infinite sequence of steps of the form $\omega = q_0 \to q_1 \to \ldots$ where (q_i, q_{i+1}) is in Tr. The length of ω, denoted $length(\omega)$, represents the number of transition between states performed by the run and is equal to n if ω is the finite run $q_0 \to q_1 \to \cdots \to q_n$, and ∞ otherwise. With $Path_{fin}(S)$ (resp. $Path_{ful}(S)$) we denote the set of finite (resp. infinite) runs of S.

Let $k \leq length(\omega)$; with $\omega(k)$ we denote the state q_k and with $\omega^{(k)}$ we denote the run q_0 if $k = 0$, and the run $q_0 \to q_1 \to \cdots \to q_k$, otherwise.

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

Definition 3.3 *An instance u is* well defined *for a Parametric Probabilistic Transition System S if and only if for each transition e of S we have that $u(\lambda(e)) \in [0, 1]$, and, for each state q of S, it holds that $\sum_{e \in Start(q)} u(\lambda(e)) = 1$.*

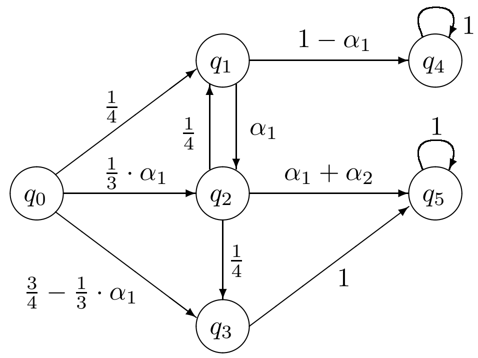

Figure 1. A Parametric Probabilistic Transition System.

Example 3.4 *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 Parametric Probabilistic Transition System of Figure 1. The instance u_3 such that $u_3(\alpha_1) = u_3(\alpha_2) = 1$ is not well defined.*

If ω is a finite run $q_0 \to q_1 \to \cdots \to q_n$ and u is a well defined instance for S, then we denote with $\overline{\mu}(\omega, u)$ the probability of ω according to u and we compute $\overline{\mu}(\omega, u)$ as follows:

$$\overline{\mu}(\omega, u) = \begin{cases} 1 & \text{if } n = 0 \\ \overline{\mu}(\omega^{(n-1)}, u) \cdot u(\lambda((q_{n-1}, q_n))) & \text{if } n > 0 \end{cases}$$

Assuming the basic notions of probability theory (see e.g. [12]), the measure μ^u defined on the set $Path_{ful}(S)$ is the unique measure such that

$$\mu^u(\{\omega \mid \omega \in Path_{ful}(S) \wedge \omega' \text{ is a prefix of } \omega\}) = \overline{\mu}(\omega', u)$$

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

4 Reachability Problem and Decidability Results

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

Let q be a state of S and u be a well defined instance for S. With $P^u(q, S)$ we denote the probability of reaching the state q with the instance u, more precisely

$$P^u(q, S) = \mu^u(\{\omega \in Path_{ful}(S) \mid \exists k : \omega(k) = q\}).$$

We note that the set $\{\omega \in Path_{ful}(S) \mid \exists k : \omega(k) = q\}$ is measurable, and hence the probability $P^u(q, S)$ is well defined.

With $Adm(q) \subset Q$ we denote the set of states that can be crossed for reaching the state q from the initial state q_0 of S. We assume that $q \notin Adm(q)$. Moreover with $AdmTr(q, q') \subset Tr$ we denote the set of transitions starting from q' and reaching a state in $Adm(q) \cup \{q\}$, more precisely the set

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

Example 4.1 *Let us consider the Parametric Probabilistic Transition System S of the example in Figure 1. We have that $Adm(q_4) = \{q_0, q_1, q_2\}$. Moreover, we have that $AdmTr(q_4, q_1) = \{(q_1, q_2), (q_1, q_4)\}$ and $AdmTr(q_4, q_2) = \{(q_2, q_1)\}$.*

Proposition 4.2 *$P^u(q, S)$ is equal to the solution of x_{q_0} of the following system of linear equations:*

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

Proof. By induction on the length of runs of S, and from the fact that

$$P^u(q, S) = \sum_{(q_0, q') \in Start(q_0)} u(\lambda((q_0, q'))) \cdot P^u(q, S_{q'})$$

where $S_{q'}$ is S with q' as initial state, and since $P^u(q, S) = 0$ if q is not reachable from the initial state of S. □

4.1 The Problem of existence of an instance

Let S be a Parametric Probabilistic Transition System, q be a state of S, α_q be a parameter not in $Par(S)$ and ϕ be a formula such that $Par(\phi) = Par(S) \cup \{\alpha_q\}$. With $Set(S, q, \phi)$ we denote the set of well defined instances u such that $u \models \phi$ and $u(\alpha_q) = P^u(q, S)$. The parameter α_q appearing in ϕ represents the value of the probability $P^u(q, S)$.

Theorem 4.3 (Existence) *For any Parametric Probabilistic Transition System S, state q and formula ϕ, it is decidable whether $Set(S, q, \phi) \neq \emptyset$ in exponential time w.r.t. the size of S.*

Proof. Given a Parametric Probabilistic Transition System $S = (Q, q_0, Tr, \lambda)$, a state $q \in Q$ and a formula ϕ we build the formula $\bar{\phi}$ as follows:

$$\bar{\phi} = \phi \ \wedge \ \alpha_q = x_{q_0} \wedge \phi_1 \wedge \phi_2 \wedge \phi_3$$

where ϕ_1 is the formula

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

and ϕ_2 is the formula

$$\bigwedge_{e \in Tr} \lambda(e) \in [0, 1]$$

and ϕ_3 is the formula

$$\bigwedge_{q' \in Q} \sum_{e \in Start(q')} \lambda(e) = 1.$$

An instance u satisfying the formula $\bar{\phi}$ is such that $u \models \phi$, $u(\alpha_q) = P^u(q, S)$ and u is well defined for S. As a consequence $Set(S, q, \phi) = \{u \mid u \models \bar{\phi}\}$. By Theorem 2.1 it is decidable in exponential time to check the existence of an instance u that satisfies $\bar{\phi}$, hence, it is also decidable in exponential time w.r.t. the size of S to check whether $Set(S, q, \phi) \neq \emptyset$. □

Example 4.4 *Let us suppose the Parametric Probabilistic Transition System S of example of Figure 1. We want to know whether there exists an instance in the set*

$$Set(S, q_5, (\alpha_{q_5} > \alpha_1 \wedge \alpha_1 > 0)).$$

This set is not empty if and only if the following formula is satisfiable:

$$\begin{aligned}
&\alpha_{q_5} > \alpha_1 \\
&\wedge \ \alpha_1 > 0 \\
&\wedge \ \alpha_{q_5} = x_{q_0} \\
&\wedge \ x_{q_5} = 1 \\
&\wedge \ x_{q_3} = x_{q_5} \\
&\wedge \ x_{q_2} = (\alpha_1 + \alpha_2) \cdot x_{q_5} + \tfrac{1}{4} \cdot x_{q_3} + \tfrac{1}{4} \cdot x_{q_1} \\
&\wedge \ x_{q_1} = \alpha_1 \cdot x_{q_2} \\
&\wedge \ x_{q_0} = \tfrac{1}{4} \cdot x_{q_1} + \tfrac{1}{3} \cdot \alpha_1 \cdot x_{q_2} + (\tfrac{3}{4} - \tfrac{1}{3} \cdot \alpha_1) \cdot x_{q_3}.
\end{aligned}$$

But the formula above is a formula in Φ, and so, by Theorem 2.1, it is decidable to check its satisfiability.

4.2 Finding a solution

We consider now the problem of finding an instance in $Set(S, q, \phi)$ such that $u(\alpha_q) = c$, for a given value $c \in [0, 1]$. Actually, Theorem 4.3 answers the problem of existence of an instance but does not give one. To find an instance in $Set(S, q, \phi)$ is a harder problem with respect to the problem of existence of an instance. Hence, to have decidability, we must consider some restrictions. More precisely, we consider Parametric Probabilistic Transition

System S with at most one parameter.

Let τ be a term such that $Par(\tau) = \{\beta\}$, for some β. the *degree* of τ, denoted with $dg(\tau)$, is the maximum natural n such that $\tau = c_n \cdot \beta^n + \cdots + c_1 \cdot \beta + c_0$ and $c_n \neq 0$.

Definition 4.5 *A Parametric Probabilistic Transition System S has degree at most k for q if and only if $|Par(S)| \leq 1$, $dg(\lambda(e)) \leq k$, for any $e \in Tr$, and*

$$\left(\sum_{q' \in Adm(q)} \max\{dg(\lambda(e)) \mid e \in AdmTr(q,q')\} \right) \leq k.$$

Hence, a Parametric Probabilistic Transition System S has degree at most k for q if and only if

1. S has at most one parameter,
2. Each term labeling a transition has degree at most k, and
3. The sum of the degrees of the terms with maximum degree appearing in the admissible transitions of each state in $Adm(q)$ are less or equal to k.

Example 4.6 *Let us consider the Parametric Probabilistic Transition System S of example of Figure 1 such that $\alpha_2 = \frac{1}{4}$. We have that S has degree at most 2 for q_4. Actually, $Par(S) = \{\alpha_1\}$, each transition has a label with degree equal to either 1 or 0, and*

$$\max\{dg(\lambda(e)) \mid e \in AdmTr(q_4, q_0)\} = 1,$$

$$\max\{dg(\lambda(e)) \mid e \in AdmTr(q_4, q_1)\} = 1,$$

and

$$\max\{dg(\lambda(e)) \mid e \in AdmTr(q_4, q_2)\} = 0.$$

Actually, there exist terms appearing in admissible transitions of q_0 and q_1 with degree equal to 1, and no parameter appears in the unique admissible transition of q_2. Therefore, we have that $1 + 1 + 0 = 2$ and hence S has degree at most 2 for q_4. In the same manner, S has degree at most 3 for q_5. Moreover, if we do not instantiate the parameter α_2, the Parametric Probabilistic Transition System S has no degree at most k, for any k.

Theorem 4.7 *For each Parametric Probabilistic Transition System S with degree at most 2 for q, and for each linear formula ϕ and a value $c \in [0,1]$, a well defined instance u, such that $u \in Set(S,q,\phi)$ and $u(\alpha_q) = c$, can be found in polynomial time w.r.t. the size of S.*

Proof. First of all, by proposition 4.2, we have that the possible values that x_{q_0} can assume are those expressed by the system of equations Eq that is equal to

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

We prove that, if S is a Parametric Probabilistic Transition System with degree at most 2 for q and $Par(S) = \{\beta\}$, then there exist two terms τ_1 and τ_2 such that $Par(\tau_i) = \{\beta\}$ and $dg(\tau_i) \leq 2$, for $i = 1, 2$, and the set of solutions of x_{q_0} is expressed by $\frac{\tau_1}{\tau_2}$.

Actually, Eq is of the form $Ax = b$, where A is the matrix of coefficients of Eq, x is the vector of variables $x_{q'}$, for $q' \in Adm(q)$, and b is a vector with value 1 for the element at the position of x_q and value 0 for the elements at the other positions. Therefore, the solution of x_{q_0} is equal to the $\frac{A_q}{A_S}$, where A_q is the determinant of the matrix A where the column of position x_q is replaced with b, and A_S is the determinant of the matrix A.

By induction on the computation of the determinant, we have that $x_{q_0} = \frac{\tau_1}{\tau_2}$, for some terms τ_1 and τ_2 such that $Par(\tau_i) = \{\beta\}$ and $dg(\tau_i) \leq 2$, for $i = 1, 2$.

Now, we must consider the case that $c = \frac{\tau_1}{\tau_2}$ but this is equivalent to $\tau_1 - c \cdot \tau_2 = 0$. Hence, by solving the polynomial $\tau_1 - c \cdot \tau_2$ of degree 2 we have two cases. The polynomial has not solution in the interval $[0,1]$ and therefore $Set(S,q,\phi)$ is empty. The polynomial has at least a solution in the interval $[0,1]$. Let c' and c'' be the solutions in $[0,1]$ (if there exist only one solution, then we suppose that $c' = c''$). Hence, we must find a solution in the space

$$(\beta \in \{c', c''\}) \wedge \bigwedge_{e \in Tr} \lambda(e) \in [0,1] \wedge \bigwedge_{q' \in Q} \sum_{e \in Start(q')} \lambda(e) = 1$$

where β is the unique parameter in $Par(S)$.

Now each occurrence of $\lambda(e)$ is at most a polynomial of degree 2 and so

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

can be substituted with a liner formula by resolving the polynomials of degree 2. Actually, each formula $c_2 \cdot \beta^2 + c_1 \cdot \beta + c_0 \sim 0$, where $c_2, c_1, c_0 \in \mathbb{R}$, can be written as a finite (at most 2) disjunction of formulae of the form $\beta \in I$, where I is an interval.

Hence, the resulting formula is linear, and therefore finding a solution is decidable. Moreover, since computing the determinant takes a polynomial time, the same holds for finding a solution. $\square$

Example 4.8 *Consider the Parametric Probabilistic Transition System S of Figure 1. We look for an instance u such* *that $P^u(S, q_4, \alpha_1 \geq \frac{1}{2})$ is equal to $\frac{1}{6}$. Now, by solving the system of linear equations introduced in Proposition 4.2, we have that*

$$\alpha_{q_4} = x_{q_0} = \frac{\alpha_1^2 + 2 \cdot \alpha_1 - 3}{3 \cdot \alpha_1 - 12} = \frac{1}{6}.$$

So we must find a value for α_1 such that $6\alpha_1^2 + 9\alpha_1 - 6 = 0$. The solutions are $\alpha_1 \in \{-2, \frac{1}{2}\}$. We must check whether these solutions are admissible. First of all we require that $\alpha_1 \geq \frac{1}{2}$. Hence -2 is not an admissible solution[1]. 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'.

4.3 The Problem of finding the Maximum/Minimum instance

Now 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 an interesting application in practice, as we shall show.

Theorem 4.9 (Maximizing/Miniminizing) *For any Parametric Probabilistic Transition System S having degree at most 1 for q and linear formula ϕ, it is decidable in polynomial time w.r.t. the size of S to find an instance u such that, for each $u' \in Set(S, q, \phi)$, it holds that $u(\alpha_q) \geq u'(\alpha_q)$ (resp. $u(\alpha_q) \leq u'(\alpha_q)$).*

Proof. By following the proof of Theorem 4.7 we have that $x_{q_0} = \frac{\tau_1}{\tau_2}$ where both τ_1 and τ_2 have degree less or equal to 1.

Now by mimicking the proof of Theorem 4.3 it is sufficient to maximize (minimize) the function $\frac{\tau_1}{\tau_2}$ in the space ϕ' that is equal to

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

Since $\alpha_q = \frac{\tau_1}{\tau_2}$ we can substitute in ϕ' each occurrence of α_q with $\frac{\tau_1}{\tau_2}$.

Each atomic formula of ϕ' is of the form $c_1 \cdot \frac{\tau_1}{\tau_2} + c_2 \cdot \beta \sim c_3$ where β is the unique parameter of S and $Par(\tau_i) = \{\beta\}$, for $i = 1, 2$. Hence this formula is equivalent to $(c_1 \cdot \tau_1 + c_2 \cdot \tau_2 \cdot \beta \sim c_3 \cdot \tau_2 \wedge \tau_2 > 0) \vee (c_3 \cdot \tau_2 \sim c_1 \cdot \tau_1 + c_2 \cdot \tau_2 \cdot \beta \wedge \tau_2 < 0)$.

Since $dg(\tau_i) \leq 1$, for $i = 1, 2$, then the formula above is a formula with terms of degree at most 2.

Hence ϕ' can be expressed as the composition of formulae of the form, $c'' \cdot \beta^2 + c' \cdot \beta + c \sim 0$, which can be substituted with a linear formula by resolving the polynomial $c_2 \cdot \beta^2 + c_1 \cdot \beta + c_0$.

[1] Note that a valuation with $\alpha_1 = -2$ is also not well defined.

Therefore, ϕ' is equivalent to a disjunction of formulae of the form $\beta \in I$, where I is an interval.

Now the maximum (resp. minimum) of $\frac{\tau_1}{\tau_2}$ in a space which is a finite disjunction of formulae of the form $\beta \in I$, where I is an interval, can be easily found.

Actually, the maximum of $\frac{\tau_1}{\tau_2}$ is when $\frac{d}{d\beta}\frac{\tau_1}{\tau_2} = 0$ but, since $dg(\tau_1) \leq 1$ and $dg(\tau_2) \leq 1$, we have that

$$\frac{d}{d\beta}\frac{\tau_1}{\tau_2} = \frac{c_1 \cdot \beta + c_2}{(\tau_2)^2},$$

for some $c_1, c_2 \in \mathbb{R}$.

Therefore, if $c_1 > 0$, then $\frac{\tau_1}{\tau_2}$ is increasing in $(-\infty, -\frac{c_2}{c_1})$, decreasing in $(-\frac{c_2}{c_1}, \infty)$, and the point $-\frac{c_2}{c_1}$ is the maximum. Moreover, if $c_1 < 0$, then $\frac{\tau_1}{\tau_2}$ is decreasing in $(-\infty, -\frac{c_2}{c_1})$, increasing in $(\frac{c_2}{c_1}, \infty)$, and the point $-\frac{c_2}{c_1}$ is the minimum. Finally, if $c_1 = 0$, then $\frac{\tau_1}{\tau_2}$ is always either increasing or decreasing (depending on the sign of c_2).

Since computing the determinant takes a polynomial time w.r.t. the size of S, the same holds for the problem of finding a maximal (minimal) solution.

□

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 [1, 15, 16].

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 [19]. 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 $R \to O : Msg$ we denote a message Msg sent by R and received by O):

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

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 ack_i message carries 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 Parametric Probabilistic Transition System. 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 2 we show a parametric Probabilistic Transition System modelling the communication between the originator and the recipient according to the parameters p and q.

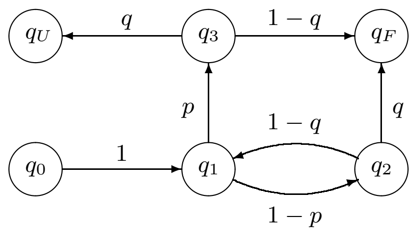

Figure 2. Parametric Representation of the Protocol.

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).

We suppose q to be a fixed constant and not a parameter, we want to find an instance for p (chosen by the originator) that maximizes the probability of reaching state q_F and minimizes the probability of reaching state q_U. In this manner the originator can choose the best value for p that minimizes the probability that the protocol ends in an unfair way.

Assuming S the Parametric Probabilistic Transition System of Figure 2, and assuming $q = \frac{1}{2}$ (namely, the attacker throws a coin to decide whether decipher the key or not). We want to find a well defined instance u such that $\forall u' \in Set(S, q_F, true)\ u(\alpha_{q_F}) \geq u'(\alpha_{q_F})$ (namely, an instance that maximizes the probability of having a fair communication).

Actually, given $q = \frac{1}{2}$ the Parametric Probabilistic Transition System of figure 2 has degree at most 1 for q_F. Following the proof of Theorem 4.9 and the system of linear equations of Proposition 4.2, we get $x_{q_0} = \frac{1}{1+p}$. Now, we must find the maximum of the function $\frac{1}{1+p}$, that one has for the value of p such that

$$\frac{d}{dp}\frac{1}{1+p} = \frac{-1}{(1+p)^2} = 0$$

But $-1 < 0$ and then the function is decreasing in $(-\infty, \infty)$. Hence the maximum is for $p = 0$ and $P^{(p=0)}(S, q_F, true) = 1$. Therefore the probability of an attack decreases if the number of messages sent by R is big. Hence the originator must choose a value of p small enough. As an example, if the originator wants a probability of fair communication equal to 0.999, then it is sufficient to apply Theorem 4.7 which gives $\frac{1}{1+p} = 0.999$, and therefore $p = \frac{0.001}{0.999}$.

6 Conclusions and Future Works

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.

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 [17]. Models with continuous state space or continuous time (or both) have been considered (see, for instance, [11]). We want to define and study parameterized versions of these formalisms.

References

[1] 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.

[2] 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.

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

[4] 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.

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

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

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

[8] 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.

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

[10] 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.

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

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

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

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

[15] 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.

[16] R. Lanotte, A. Maggiolo-Schettini, and A. Troina, ”Automatic Analysis of a Non-Repudiation Protocol”, In Proc. of QAPL’03, Elsevier ENTCS, to appear.

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

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

[19] O. Markowitch, and Y. Roggeman, “Probabilistic Non-Repudiation without Trusted Third Party”, 2nd Conference on Security in Communication Network, 1999.

[20] 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.

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