Symbolic Model Checking of Probabilistic Timed Automata Using Backwards Reachability*

Marta Kwiatkowska, Gethin Norman and Jeremy Sproston
University of Birmingham, Birmingham B15 2TT, United Kingdom
{M.Z.Kwiatkowska,G.Norman,J.Sproston}@cs.bham.ac.uk

January 26, 2000

Abstract

We consider probabilistic timed automata of [13], an extension of the timed automata model of [2] with discrete probability distributions. In contrast to timed automata, which model real-time systems purely in terms of nondeterminism, our model allows to express the likelihood of the system making certain transitions, and is thus appropriate for modelling fault-tolerance and probabilistic failures. We present a symbolic model checking algorithm for the existential fragment of the logic PTCTL of [13] based on backward reachability as in [12]. The logic allows us to specify properties such as "with probability 0.99 or greater, it is possible to correctly deliver a data packet within 5 time units", or "with probability 0.87 or greater, the system never enters an error state".

1 Introduction

Much progress has been made recently with formal methods and tools for the verification of real-time systems, to mention the *timed automata* model [2] and the associated tools such as UPPAAL [4] and KRONOS [6]. With the help of these, the modelling and automated analysis of systems is possible in the presence of dense real-time by means of reduction of timed automata to finite quotient structures.

The timed automata model describes the system events purely in terms of nondeterminism. However, it may be desirable to express the relative likelihood of the system exhibiting certain behaviour. For example, we may wish to model a system for which the target node of a transition is not uniquely determined, but instead is given *probabilistically*; for example, a transition can result in success with probability 0.9, and otherwise

*The first two authors are supported in part by EPSRC grant GR/M04617.

Technical Report CSR-00-1, School of Computer Science, University of Birmingham, January 2000.

an error state is entered. Another example could be a communications protocol, which delivers data over unreliable medium; thus, a message is lost with probability 0.05 each time a communication channel is used. In such cases, *quantitative* estimates of the *likelihood* of properties being satisfied or violated are called for. For example, we might wish to establish the minimal/maximal probability of never entering an error state in the gear box controller [15], or the probability of the message being delivered correctly within t time units in the bounded retransmission protocol [7]. Minimal/maximal probabilities are obtained instead of exact ones because of nondeterminism. There exist established methods for model checking of untimed probabilistic systems against reachability problems and temporal logic specifications such as PBTL [5, 3, 8].

This paper is a contribution in the area of automatic verification of *probabilistic timed automata*. This model was introduced in [13], where a model checking method for the logic PTCTL (a synthesis of TCTL of [1] and PBTL of [3]) has also been presented. Unfortunately, the method of [13] is not practical, as it relies on the construction of the full region graph of the automaton (exponential in the number of clocks). Here we propose an improvement, a *symbolic* method based on backward reachability, for the existential fragment of the logic PTCTL. Our starting point is the non-probabilistic, real-time, model checking algorithm of [12], which we adapt to our setting through a judicious combination with the maximal probability reachability algorithm of [9].

Due to the presence of quantitative probabilities, the unstructured aggregation of backwards reachable states in a single set featured in the method of [12] is insufficient. Instead, for a given 'until' formula, we generate a certain quotient transition system on this state set, then solve a corresponding linear programming problem to establish the probability of the formula being satisfied. Another improvement of the approach of [13], for the more restricted case of probabilistic reachability properties via forward reachability, has been proposed in [14].

2 Concurrent Probabilistic Systems

We assume some familiarity with Markov chains and probability theory, see e.g. [16]. Let S be a finite set. A probability subdistribution (distribution) on S is a function $p : S \to [0,1]$ such that $\sum_{s \in S} p(s) \leq 1$ $(= 1)$. Since our results generalise to the case of subdistributions, by abuse of notation we refer to subdistributions as distributions. The set of distributions over S is denoted by $\mu(S)$. A *concurrent probabilistic system* is a pair $\mathcal{C} = (S, \mathit{Steps})$ where S is a finite set of states and *Steps* a function which assigns to each state $s \in S$ a finite, non-empty set $\mathit{Steps}(s)$ of probability distributions on S. Elements of $\mathit{Steps}(s)$ are called *transitions*. Execution of $\mathcal{C}$ results in *paths*, which arise by first resolving nondeterminism in a given state, and then moving to the target state according to the selected probability distribution. A path of the system $\mathcal{C} = (S, \mathit{Steps})$ is a non-empty, finite or infinite sequence, $\pi = s_0 \xrightarrow{p_0} s_1 \xrightarrow{p_1} s_2 \xrightarrow{p_2} \cdots$ where $s_i \in S$, $p_i \in \mathit{Steps}(s_i)$ with $p_i(s_{i+1}) > 0$ for all $0 \leq i \leq |\pi|$, $|\pi|$ length of path π. We use $\pi(i)$ to refer to the ith state of π, and $\mathit{last}(\pi)$ to its last state. We let $\mathit{Path}_{\mathit{ful}}(s)$ denote the set of infinite paths of $\mathcal{C}$ starting in $s \in S$.

The selection of a probability distribution is made by an *adversary*, a function A mapping every finite path ρ of $\mathcal{C}$ to a distribution $A(\rho)$ on S such that $A(\rho) \in Steps(last(\rho))$ is a transition in $\mathcal{C}$. The subset of infinite paths starting in s and corresponding to the choices of an adversary A is denoted by $Path^A_{ful}(s)$. With each adversary one can associate a sequential Markov chain whose states are finite paths of $\mathcal{C}$, together with the induced probability measure $Prob$ on subsets of $Path_{ful}(s)$; see [3] for more details. We rely on the following known result.

Theorem 1 [8] *Let $\mathcal{C} = (S, Steps)$ be a concurrent probabilistic system, $R \subseteq S$. Define $ReachE(s,R)$ as the maximal probability of reaching the set of states R in $\mathcal{C}$. The linear programming problem over the set $\{x_s \mid s \in S \setminus R\}$ of variables: minimize $\sum_{s \in S\setminus R} x_s$ subject to*

$$x_s \geq \sum_{s' \in S \setminus R} p(s') \cdot x_{s'} + \sum_{s' \in R} p(s') \quad p \in Steps(s) \text{ and } s \in S \setminus R$$

admits exactly one optimal solution vector $\mathbf{x}$, and for all $s \in S \setminus R : \mathbf{x}_s = ReachE(s,R)$.

The linear programming problem of Theorem 1 can be solved iteratively or in polynomial time with e.g. the ellipsoid method. It can be optimized by pre-computing the set of states that are reachable with positive probability [5] or with probability 1 [9], often resulting in a reduction in the number of unknowns.

3 Probabilistic Timed Automata

We follow the notation of [2, 13], and only recall the basic notions. A *clock* $x \in \mathcal{X}$ is a real-valued variable which increases at the same rate as real-time. A *clock valuation* $\nu : \mathcal{X} \to \mathbb{R}$, ranging over $\mathbb{R}^{\mathcal{X}}$, is a function assigning a real value to each clock in $\mathcal{X}$. If $X \subseteq \mathcal{X}$, we write $\nu[X := 0]$ for the valuation that assigns 0 to clocks in X and agrees with ν on all the remaining clocks in $\mathcal{X}$, and $\nu + t$ for the valuation whose clocks take the value $\nu(x) + t$ where $t \in \mathbb{R}$.

The set of *zones* of $\mathcal{X}$, written $\mathbf{Z}_{\mathcal{X}}$, is defined inductively by the syntax:

$$\zeta ::= \mathtt{true} \mid x \sim k \mid x - y \sim k \mid \zeta \vee \zeta \mid \zeta \wedge \zeta$$

where $x, y \in \mathcal{X}$, $\sim \in \{<, \leq, \geq, >\}$ and $k \in \mathbb{N}$. We only consider canonical zones which ensures equality between syntactic and semantic (as subsets of $\mathbb{R}^{\mathcal{X}}$) representation of zones. This enables us to use the above syntax interchangeably with set-theoretic operations. Let $\zeta \in \mathbf{Z}_{\mathcal{X}}$ and $\nu \in \mathbb{R}^{\mathcal{X}}$. Then $\zeta[\nu]$ is the boolean value obtained by replacing each occurrence of a clock $x \in \mathcal{X}$ in ζ by $\nu(x)$. If $\zeta[\nu] = \mathtt{true}$ then we say that ν *satisfies* ζ, also denoted by $\nu \in \zeta$.

We shall require the following operations on zones. For any zones $\zeta, \zeta' \in \mathbf{Z}_{\mathcal{X}}$ and subset $X \subseteq \mathcal{X}$ of clocks let:

$$[X := 0]\zeta \stackrel{\text{def}}{=} \{\nu \mid \nu[X := 0] \in \zeta\}$$
$$\swarrow_{\zeta'} \zeta \stackrel{\text{def}}{=} \{\nu \mid \exists t \geq 0 \,.(\nu + t \in \zeta \ \wedge \ \forall t' \leq t \,.(\nu + t' \in \zeta \vee \zeta'))\}.$$

A *timed automaton* is an ordinary automaton extended with clocks. Its nodes and transitions are labelled with zones, known as *invariants* and *enabling conditions* respectively. The automaton may only stay in a node, letting time pass, if the clocks satisfy the invariant. When an enabling condition is satisfied, the corresponding transition can be taken. Transitions are instantaneous, and are additionally labelled with *clock resets* of the form $X := 0$, which reset the clocks $x \in X$ to zero upon entering the target node.

Probabilistic timed automata generalise timed automata in the following sense. Transitions no longer have a single target node but possibly several, which are chosen *probabilistically*. We associate every such transition with a single enabling condition, and allow its *edges* to be labelled with their own probability values and clock resets. The probabilities labelling the edges of any transition must sum up to no more than one, and hence can be viewed as a discrete probability distribution. Several transitions may be simultaneously enabled, with the choice between them (and letting time elapse if the invariant would not be violated) resolved *nondeterministically*.

Definition 2 (Probabilistic Timed Automaton [13]) *A probabilistic timed automaton is a tuple* $G = (\mathcal{S}, L, \bar{s}, \mathcal{X}, inv, prob, \langle \tau_s \rangle_{s \in \mathcal{S}})$ *which contains:*

- *a finite set* $\mathcal{S}$ *of nodes,*
- *a function* $L : \mathcal{S} \longrightarrow 2^{\mathrm{AP}}$ *assigning to each node of the automaton the set of atomic propositions that are true in that node,*
- *a start node* $\bar{s} \in \mathcal{S}$*,*
- *a finite set* $\mathcal{X}$ *of clocks,*
- *a function* $inv : \mathcal{S} \longrightarrow \mathbf{Z}_{\mathcal{X}}$ *assigning to each node an invariant condition,*
- *a function* $prob : \mathcal{S} \longrightarrow \mathcal{P}_{fn}(\mu(\mathcal{S} \times 2^{\mathcal{X}}))$ *assigning to each node a (finite, non-empty) set of discrete probability distributions on* $\mathcal{S} \times 2^{\mathcal{X}}$*, and*
- *a family of functions* $\langle \tau_s \rangle_{s \in \mathcal{S}}$ *where, for any* $s \in \mathcal{S}$*,* $\tau_s : prob(s) \longrightarrow \mathbf{Z}_{\mathcal{X}}$ *assigns to each* $p \in prob(s)$ *an enabling condition.*

An *edge* e of G is a tuple of the form $(s, s', p, X) \in \mathcal{S}^2 \times \mu(\mathcal{S} \times 2^{\mathcal{X}}) \times 2^{\mathcal{X}}$. We define the *set E of edges* of the probabilistic timed automaton G such that $(s, s', p, X) \in E$ if and only if $p \in prob(s)$ and $p(s', X) > 0$. If $s \in \mathcal{S}$, the set $\mathsf{in}(s)$ contains all edges of the form $(\_, s, \_, \_)$. For any $e = (s, s', X, p)$ define the following functions: $\mathsf{type}(e) = p$, and $\mathsf{source}(e) = s$.

Example 1 An example of a probabilistic timed automaton H modelling a simple probabilistic communication protocol is included in Figure 1. Its nodes represent the following states: *ii* (sender, receiver both idle); *hi* (sender has data, receiver idle); *si* (sender sent data, receiver idle; and *sr* (sender sent data, receiver received). It starts in the state *ii*, and moves to *hi* as soon as the data is received. While in *hi*, after between 1 and 2 time units have elapsed, it can make a probabilistic transition either to *sr* with probability 0.9

(data received), or to si with probability 0.1 (data lost). In si the protocol will attempt to resend the data after 2 to 3 time units, which again can be lost, this time with probability 0.05.

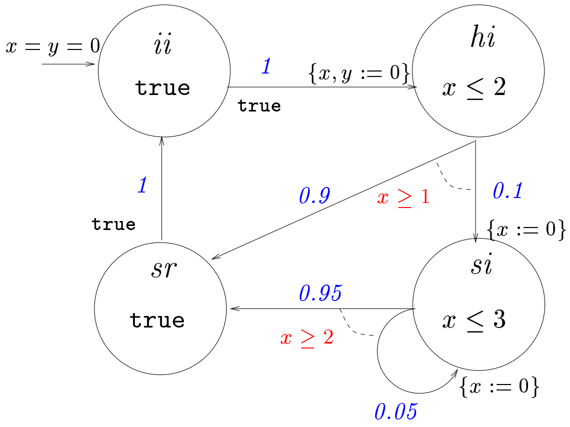

Figure 1: A probabilistic timed automaton H modelling a probabilistic protocol

An underlying model for probabilistic timed automata are *probabilistic timed structures*, a suitable combination of the timed structures of [11] and concurrent probabilistic systems described in Section 2. Define a *state* as a pair $\langle s, \nu \rangle$ consisting of a node and a clock valuation. Formally, a *probabilistic timed structure* is a pair $\mathcal{M} = (Q, \mathit{TSteps})$ where Q is a set of states, and TSteps a function which assigns to each state $q \in Q$ a set $\mathit{TSteps}(q)$ of pairs of the form (t, p) where $t \in \mathbb{R}$ and $p \in \mu(Q)$. Thus, each transition (t, p) contains both information about *time duration* as well as *probability*: the meaning of $(t, p) \in \mathit{TSteps}(q)$ is that, when in state q, then, after t time units have elapsed, the system moves to state q' with probability $p(q')$.

We can derive the notions of a path, adversary and probability measure $Prob^T$ as for concurrent probabilistic systems, except that we must take account of the additional labelling of steps with time duration (see [13] for precise details). Let $\mathcal{M} = (Q, \mathit{TSteps})$ be a probabilistic timed structure. Its paths are of the form $\omega = q_0 \xrightarrow{t_0, p_0} q_1 \xrightarrow{t_1, p_1} q_2 \xrightarrow{t_2, p_2} \cdots$ where $q_i \in Q$, $(t_i, p_i) \in \mathit{TSteps}(q_i)$ and $p_i(q_{i+1}) > 0$ for all $0 \leq i \leq |\omega|$. An *adversary* (or scheduler) of $\mathcal{M} = (Q, \mathit{TSteps})$ is a function A mapping every finite path ω of $\mathcal{M}$ to a pair (t, p) such that $A(\omega) \in \mathit{TSteps}(\mathit{last}(\omega))$.

In what follows we fix the set AP of atomic propositions and a labelling function L and omit them if clear from the context. The probabilistic timed structure arising from G with respect to the labelling L is as follows.

Definition 3 *For any probabilistic timed automaton G, let $\mathcal{M}_G = (Q_G, \mathit{TSteps}_G)$ be the probabilistic timed structure given by:*

- $Q_G = \{\langle s, \nu \rangle \mid s \in \mathcal{S},\ \nu \in \mathbb{R}^{\mathcal{X}}$ *and ν satisfies $inv(s)$*$\}$, *with the interpretation of propositions induced from the labelling function L of G.*

- *Take any* $\langle s,\nu\rangle \in Q_G$*. Then* $(t,\tilde{p}) \in \mathit{TSteps}_G\langle s,\nu\rangle$*, where* $t \in \mathbb{R}$ *and* $\tilde{p} \in \mu(\mathcal{S} \times \mathbb{R}^{\mathcal{X}})$*, iff there exists* $p \in \mathit{prob}(s)$ *such that*
  - *the clock valuation* $\nu + t$ *satisfies* $\tau_s(p)$*;*
  - $(\nu + t')$ *satisfies the invariant condition* $\mathit{inv}(s)$ *for all* $0 \leq t' \leq t$*;*
  - *for any* $\langle s',\nu'\rangle$*:*

$$\tilde{p}\langle s',\nu'\rangle = \sum_{\substack{X \subseteq \mathcal{X}\, \& \\ (\nu+t)[X:=0]=\nu'}} p(s',X) \; .$$

  Let $\mathsf{type}(\tilde{p}) = p$*.*

- *Take any* $\langle s,\nu\rangle \in Q_G$*. If* $\nu + t$ *satisfies* $\mathit{inv}(s)$ *for all* $t \in \mathbb{R}$*, then* $(1, p_{\mathrm{div}}^{\langle s,\nu\rangle}) \in \mathit{TSteps}_G\langle s,\nu\rangle$ *where* $p_{\mathrm{div}}^{\langle s,\nu\rangle}\langle s',\nu'\rangle = 1$ *iff* $\langle s',\nu'\rangle = \langle s,\nu\rangle$*. Let* $\mathsf{type}(p_{\mathrm{div}}^{\langle s,\nu\rangle}) = \perp$*. (This is to model letting time diverge in states where it is possible.)*

In common with the usual practice in real-time systems we disallow *divergent* paths (i.e. those which do not permit time passage beyond some bound) since they do not correspond to realisable behaviour [13]. We let Adv ($\mathit{Adv}_{\mathit{div}}$) denote the set of all (all divergent) adversaries of $\mathcal{M}_G$.

For simplicity, we assume the following restriction. Let $\mathcal{M}_G = (Q_G, \mathit{TSteps}_G)$ be a probabilistic timed structure of G, then for every $q \in Q_G$ there exists an adversary A of $\mathcal{M}_G$ such that $\mathit{Prob}^T\{\omega \,|\, \omega \in \mathit{Path}^A_{\mathit{ful}}(q) \text{ and } \omega \text{ is divergent}\} = 1$. In other words, the automata we consider must allow time divergence, possibly through transitions, with probability 1 in every state.

4 The logic PTCTL$_\exists$

We now describe the existential fragment, PTCTL$_\exists$, of the probabilistic real-time logic PTCTL (Probabilistic Timed Computation Tree Logic) [13]. PTCTL combines TCTL [1, 12] (in particular, the reset quantifier $z.\phi$ and the facility to refer directly to clock values) and the existential fragment of probabilistic temporal logic PBTL [3] similar to pCTL of [5].

As with TCTL, we enlarge the set of clock variables with the set of *formula clocks*, $\mathcal{Z}$, which is disjoint from $\mathcal{X}$. A *formula clock valuation* is denoted by $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$ and used in the same way as standard clock valuations.

Definition 4 (Syntax of PTCTL$_\exists$**)** *The syntax is:*

$$\phi ::= \mathtt{true} \;|\; a \;|\; \zeta \;|\; \phi \wedge \phi \;|\; \neg\phi \;|\; z.\phi \;|\; [\phi \,\exists\mathcal{U}\, \phi]_{\sqsupseteq\lambda}$$

where $a \in \mathrm{AP}$ *is an* atomic proposition*,* $\zeta \in \mathbf{Z}_{\mathcal{X}\cup\mathcal{Z}}$ *is a* zone*,* $z \in \mathcal{Z}$*,* $\lambda \in [0,1]$*, and* $\sqsupseteq$ *is either* $\geq$ *or* $>$*.*

PTCTL is interpreted over probabilistic timed structures. Before we give the formal semantics, we introduce some notation. Given a state q and a formula clock valuation $\mathcal{E}$, we denote by $\zeta[q, \mathcal{E}]$ the boolean value obtained by replacing each occurrence of a system clock $x \in \mathcal{X}$, resp. formula clock $z \in \mathcal{Z}$, in ζ by $q(x)$, resp. $\mathcal{E}(z)$. Consider a path ω of $\mathcal{M}$. A *position* of ω is a pair (i, t'), where $i \in \mathbb{N}$ and $t' \in \mathbb{R}$ such that $0 \leq t' \leq t_i$. The *state at position* (i, t'), denoted by $q_i + t'$, assigns $q_i(a)$ to each proposition a in AP, and $q_i(x) + t'$ to each clock x in $\mathcal{X}$. Given a path ω, $i, j \in \mathbb{N}$ and $t, t' \in \mathbb{R}$ such that $i \leq |\omega|$, $t \leq t_i$ and $t' \leq t_j$, we say that the position (j, t') *precedes* the position (i, t), written $(j, t') \prec (i, t)$, iff $j < i$, or $j = i$ and $t' < t$.

Definition 5 (Satisfaction Relation for PTCTL$_\exists$**)** *Given a probabilistic timed structure $\mathcal{M}$ and a set $\mathcal{A}$ of adversaries of $\mathcal{M}$, then for any state q of $\mathcal{M}$, formula clock valuation $\mathcal{E}$, and* PTCTL$_\exists$ *formula ϕ, the satisfaction relation $q, \mathcal{E} \models_{\mathcal{A}} \phi$ is defined inductively as follows:*

$$
\begin{array}{lll}
q, \mathcal{E} \models_{\mathcal{A}} \texttt{true} & & \text{for all } q \text{ and } \mathcal{E} \\
q, \mathcal{E} \models_{\mathcal{A}} a & \Leftrightarrow & q(a) = \texttt{true} \\
q, \mathcal{E} \models_{\mathcal{A}} \zeta & \Leftrightarrow & \zeta[q, \mathcal{E}] = \texttt{true} \\
q, \mathcal{E} \models_{\mathcal{A}} \phi_1 \wedge \phi_2 & \Leftrightarrow & q, \mathcal{E} \models_{\mathcal{A}} \phi_1 \text{ and } q, \mathcal{E} \models_{\mathcal{A}} \phi_2 \\
q, \mathcal{E} \models_{\mathcal{A}} \neg\phi & \Leftrightarrow & q, \mathcal{E} \not\models_{\mathcal{A}} \phi \\
q, \mathcal{E} \models_{\mathcal{A}} z.\phi & \Leftrightarrow & q, \mathcal{E}[z := 0] \models_{\mathcal{A}} \phi \\
q, \mathcal{E} \models_{\mathcal{A}} [\phi_1 \, \exists\mathcal{U} \, \phi_2]_{\sqsupseteq\lambda} & \Leftrightarrow & \mathit{Prob}(\{\omega \mid \omega \in \mathit{Path}^A_{\mathit{ful}}(q) \;\&\; \omega, \mathcal{E} \models_{\mathcal{A}} \phi_1 \, \mathcal{U} \, \phi_2\}) \sqsupseteq \lambda \\
& & \text{for some } A \in \mathcal{A} \\
\omega, \mathcal{E} \models_{\mathcal{A}} \phi_1 \, \mathcal{U} \, \phi_2 & \Leftrightarrow & \text{there exists a position } (i, t) \text{ of } \omega \text{ such that} \\
& & \omega(i) + t, \mathcal{E} + \mathcal{D}_\omega(i) + t \;\models_{\mathcal{A}}\; \phi_2, \text{ and} \\
& & \text{for all positions } (j, t') \text{ of } \omega \text{ such that } (j, t') \prec (i, t), \\
& & \omega(j) + t', \mathcal{E} + \mathcal{D}_\omega(j) + t' \;\models_{\mathcal{A}}\; \phi_1 \vee \phi_2 \\
& & \text{where } \mathcal{D}_\omega(i) \text{ is the total elapsed time up to step } i.
\end{array}
$$

The above defines a family of satisfaction relations for classes of adversaries, typically $\models_{\mathit{Adv}_{\mathit{div}}}$. We note that the restriction on automata G imposed in Section 2 ensures that for PTCTL$_\exists$ we obtain that $\models_{\mathit{Adv}}$ coincides with $\models_{\mathit{Adv}_{\mathit{div}}}$.

An example of a property expressible in PTCTL$_\exists$ is "with probability 0.99 or greater, it is possible to correctly deliver a data packet within 5 time units", which is written as $z.[\texttt{true} \; \exists\mathcal{U} \; \texttt{delivered} \wedge (z \leq 5)]_{\geq 0.99}$. Due to the presence of negation, by duality our logic includes a form of universal quantification over adversaries, for example, $\neg[\texttt{true} \; \exists\mathcal{U} \; \texttt{error}]_{>1-0.87}$ expresses "with probability 0.87 or greater, the system never enters an error state".

For the remainder of this paper we fix automaton $G = (S, L, \bar{s}, \mathcal{X}, \mathit{inv}, \mathit{prob}, \langle\tau_s\rangle_{s\in S})$ with the underlying timed probabilistic structure $\mathcal{M}_G = (Q_G, \mathit{TSteps}_G)$.

5 Model Checking Existential 'Until': A First Attempt

In [13] an algorithm for model checking full PTCTL was proposed. It is based on the construction of the full region graph, and thus has high complexity since the region graph is exponential in the number of clocks. Here we turn our attention to the *symbolic* method of [12] for nonprobabilistic existential 'until', and work with zones instead of regions. Given a formula $[\phi\ \exists\mathcal{U}\ \psi]_{\sqsupseteq\lambda}$, the idea is to first compute the set of node-zone pairs satisfying ψ, and then traverse the edges $e = (s', s, p, X)$ of G backwards from ψ-states s, continuously satisfying ϕ. We refer to node-zone pairs as *symbolic states*. Assume we have computed the sets $[\![\phi]\!], [\![\psi]\!] \subseteq \mathcal{S} \times \mathbf{Z}_{\mathcal{X}\cup\mathcal{Z}}$ of symbolic states such that, for any state $\langle s, \nu\rangle \in Q_G$ and formula clock evaluation $\mathcal{E}$, $\langle s,\nu\rangle, \mathcal{E} \models \phi$, resp. ψ, iff there exists $\langle s, \zeta\rangle \in [\![\phi]\!]$, resp. $[\![\psi]\!]$, such that $[\nu, \mathcal{E}] \in \zeta$.

Let $\mathsf{zone} : S \times \mathrm{PTCTL}_{\exists} \to \mathbf{Z}_{\mathcal{X}\cup\mathcal{Z}}$ be the function $\mathsf{zone}(s,\theta) \stackrel{\text{def}}{=} \bigcup_{\langle s,\zeta\rangle\in[\![\theta]\!]} \zeta$. We extend the time and discrete predecessor functions $\mathsf{time\_pre}$ and $\mathsf{disc\_pre}$ of [17] as follows:

$$\begin{aligned}
\mathsf{time_pre}_{\phi}(\langle s,\zeta\rangle) &\stackrel{\text{def}}{=} \langle s, \swarrow_{\mathsf{zone}(s,\phi)} \zeta \cap inv(s)\rangle \\
\mathsf{disc_pre}_{\phi}((s', s, p, X), \langle s,\zeta\rangle) &\stackrel{\text{def}}{=} \langle s', \tau_{s'}(p) \cap ([X := 0]\zeta) \cap \mathsf{zone}(s',\phi)\rangle
\end{aligned}$$

(note that by construction $\mathsf{zone}(s',\phi) \subseteq inv(s')$) and lift $\mathsf{time\_pre}_{\phi}$ to sets $T \subseteq \mathcal{S} \times \mathbf{Z}_{\mathcal{X}\cup\mathcal{Z}}$ in the usual way.

Combining the above with the approach of [12] yields an algorithm for finding all states from which one can reach a ψ-state with *positive probability* without leaving ϕ-states, shown in Figure 2. Note the use of $\mathsf{disc\_pre}_{\phi}(e, \mathsf{time\_pre}_{\phi}\langle s,\nu\rangle)$, rather than $\mathsf{time\_pre}_{\phi}(\mathsf{disc\_pre}_{\phi}(e, \langle s,\nu\rangle))$, to ensure the detection of symbolic states for which the edge e is enabled *throughout*.

ExistsUntil$^{>0}(\phi,\psi)$**{**
$Z := \mathsf{time\_pre}_{\phi}([\![\psi]\!])$
$Z' := S$
while $Z' \neq Z$ **do**
  $Z' := Z$
  for all $(s,\zeta) \in Z$
    for all $e \in \mathsf{in}(s)$
      $Z := Z \cup \{\mathsf{disc\_pre}_{\phi}(e, \mathsf{time\_pre}_{\phi}\langle s,\nu\rangle)\}$
    end for all
  end for all
end while
return Z

Figure 2: Algorithm for finding all states satisfying $[\phi\ \exists\mathcal{U}\ \psi]_{>0}$

It might seem that simply generating edges between symbolic states and calculating the probabilities labelling these edges would enable us to construct a concurrent probabilistic transition system quotient of the automaton, then use the reduction to the linear programming problem of Theorem 1 to establish $[\phi\ \exists\mathcal{U}\ \psi]_{\sqsupseteq\lambda}$ for arbitrary λ. Unfortunately, this is not the case, as we now demonstrate.

Example 2 Consider the automaton H in Figure 1 and PTCTL$_{\exists}$ formula $[(y < 6)\ \exists\mathcal{U} sr]_{\sqsupseteq\lambda}$ (for any λ) meaning "y stays below 6 until a data packet has been received (in sr)". The concurrent probabilistic system quotient corresponding to the automaton H is shown in Figure 3.

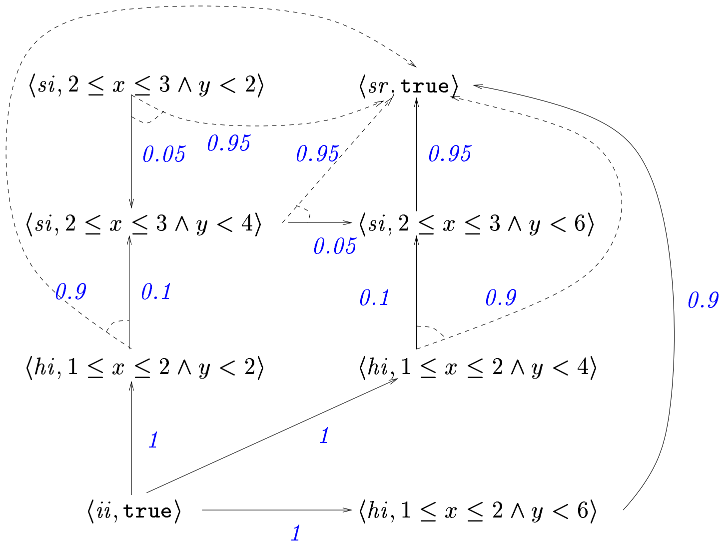

Figure 3: The concurrent probabilistic system for the automaton H in Figure 1

We overload the notation by referring to *edges* both when considering G (where they connect nodes) and the concurrent probabilistic system quotient (where they connect symbolic states). The problem with the algorithm in Figure 2 is that it fails to detect all edges; in particular, the dotted edges in Figure 3 would not be found. In general, we may compute symbolic states $\langle s, \zeta\rangle, \langle s, \zeta'\rangle$ via different edges e_1, e_2 belonging to *the same* distribution $p \in \mu(S \times 2^{\mathcal{X}})$, i.e. having the same type. Then, if $\zeta \cap \zeta' \neq \emptyset$, in the state $\langle s, \zeta \cap \zeta'\rangle$ *both* these edges are *relevant*, i.e. enabled throughout $\zeta \cap \zeta'$. We must explicitly consider all the relevant *intersections* of zones, together with the additional induced edges. The notion of relevance is captured by the function below. Assume the existence of sets $Z \subseteq \mathcal{S} \times \mathbf{Z}_{\mathcal{X}\cup\mathcal{Z}}$ of symbolic states and E of edges between them, then define:

$$\mathsf{relevant}(p, \langle s', \zeta'\rangle) \stackrel{\text{def}}{=}$$
$$\{\langle s', \zeta''\rangle \mid \langle s', \zeta''\rangle \in Z \wedge \zeta' \cap \zeta'' \neq \emptyset \wedge \exists e \in E\ .\ \mathsf{source}(e) = \langle s', \zeta''\rangle \wedge \mathsf{type}(e) = p\}.$$

Finally, note that our algorithm must also allow for situations where *nondeterministic* choice between probability distributions arises, e.g. in symbolic state $\langle ii, \mathtt{true}\rangle$ in Figure 3.

6 Symbolic Model Checking Algorithm for $\mathrm{PTCTL}_{\exists}$

We are now ready to give a symbolic model checking procedure for the existential fragment of PTCTL. Given a probabilistic timed automaton G and a $\mathrm{PTCTL}_{\exists}$ formula θ, the algorithm proceeds by building the parse tree of the formula, and traverses it bottom-up, inductively computing the set of node-zone pairs satisfying subformulae θ' as they are encountered. For all subformulae θ' which are not of the form $[\phi\, \exists\mathcal{U}\psi]_{\sqsupseteq\lambda}$, the corresponding set $[\![\theta']\!]$ can be computed simply by appropriate operations on zones. For the subformula $\theta' = [\phi\, \exists\mathcal{U}\psi]_{\sqsupseteq\lambda}$, however, a probabilistic concurrent system $\mathcal{C}_{\phi,\psi} = (S_{\phi,\psi}, \mathit{Steps}_{\phi,\psi})$ is computed by means of the algorithm **ExistsUntil**. The solution to the linear programming problem of Theorem 1 over $\mathcal{C}_{\phi,\psi}$ yields the set of symbolic states which satisfy $[\phi\, \exists\mathcal{U}\psi]_{\sqsupseteq\lambda}$.

Formally, if θ is a $\mathrm{PTCTL}_{\exists}$ formula, define $[\![\theta]\!]$ by induction as follows:

1. $[\![\mathtt{true}]\!] \stackrel{\text{def}}{=} \{\langle s, inv(s)\rangle \mid s \in \mathcal{S}\}$

2. $[\![a]\!] \stackrel{\text{def}}{=} \{\langle s, inv(s)\rangle \mid s \in \mathcal{S} \text{ and } a \in L(s)\}$

3. $[\![\zeta]\!] \stackrel{\text{def}}{=} \{\langle s, inv(s) \cap \zeta\rangle \mid s \in \mathcal{S}\}$

4. $[\![\phi \wedge \psi]\!] \stackrel{\text{def}}{=} \{\langle s, \zeta \cap \zeta'\rangle \mid \langle s, \zeta\rangle \in [\![\phi]\!] \text{ and } \langle s, \zeta'\rangle \in [\![\psi]\!]\}$

5. $[\![\neg\phi]\!] \stackrel{\text{def}}{=} \{\langle s, inv(s) \setminus \{\zeta \mid \langle s, \zeta\rangle \in [\![\phi]\!]\}\rangle \mid s \in \mathcal{S}\}$

6. $[\![z.\phi]\!] \stackrel{\text{def}}{=} \{\langle s, [z := 0]\zeta\rangle \mid \langle s, \zeta\rangle \in [\![\phi]\!]\}$

7. $[\![[\phi\, \exists\mathcal{U}\, \psi]_{\sqsupseteq\lambda}]\!] \stackrel{\text{def}}{=} \{\mathsf{time\_pre}_{\phi}\langle s, \mathsf{zone}(T_s)\rangle \mid s \in \mathcal{S}\}$
   where $T_s = \bigcup\{\zeta \mid \zeta \in \mathbf{Z}_{\mathcal{X}\cup\mathcal{Z}},\ \langle s, \zeta\rangle \in S_{\phi,\psi} \text{ and } \mathit{ReachE}(\langle s, \zeta\rangle, [\![\psi]\!]) \sqsupseteq \lambda\}$.

The algorithm **ExistsUntil** is shown in Figure 4.

It consists of two phases: generation of all symbolic states $Z_{\phi,\psi}$ and a subset of edges $E_{\phi,\psi}$ between them, followed by the construction of the probabilistic concurrent system $\mathcal{C}_{\phi,\psi} = (S_{\phi,\psi}, \mathit{Steps}_{\phi,\psi})$ where $S_{\phi,\psi} = Z_{\phi,\psi}$, at which stage the missing edges are added.

The following summarises the construction of the set $\mathit{Steps}_{\phi,\psi}$. Let ϕ, ψ be fixed and assume the existence of sets $Z \subseteq \mathcal{S} \times \mathbf{Z}_{\mathcal{X}\cup\mathcal{Z}}$ of symbolic states and E of edges (we elide the subscripts ϕ, ψ for clarity). For $\langle s, \zeta\rangle \in Z$, define $E\langle s, \zeta\rangle \stackrel{\text{def}}{=} \{e \mid (\langle s, \hat{\zeta}\rangle, \_, \_, \_) \in E \wedge \zeta \subseteq \hat{\zeta}\}$; $\mathsf{dist}\langle s, \zeta\rangle \stackrel{\text{def}}{=} \{p \mid (\langle s, \hat{\zeta}\rangle, \_, p, \_) \in E\langle s, \zeta\rangle\}$; and $\mathsf{choices}(\langle s, \zeta\rangle, p) \stackrel{\text{def}}{=} \{(s', X) \mid (\langle s, \hat{\zeta}\rangle, \langle s', \zeta'\rangle, p, X) \in E\langle s, \zeta\rangle\}$ where $p \in \mathsf{dist}\langle s, \zeta\rangle$. Now for any $p \in \mathsf{dist}\langle s, \zeta\rangle$ and $(s', X) \in \mathsf{choices}(\langle s, \zeta\rangle, p)$ put:

$$\mathsf{targets}(\langle s, \zeta\rangle, p, (s', X)) \stackrel{\text{def}}{=} \{(\langle s', \zeta'\rangle, X) \mid (\langle s, \hat{\zeta}\rangle, \langle s', \zeta'\rangle, p, X) \in E\langle s, \zeta\rangle\}$$

$$\mathsf{supports}(\langle s, \zeta\rangle, p) = \prod_{(s', X) \in \mathsf{choices}(\langle s, \zeta\rangle, p)} \mathsf{targets}(\langle s, \zeta\rangle, p, (s', X))$$

ExistsUntil(ϕ, ψ)**{**

  $Z := \emptyset$

  $E := \emptyset$

  $\mathit{Fringe} := [\![\psi]\!]$

  while $\mathit{Fringe} \neq \emptyset$ **do**

    for all $\langle s, \zeta \rangle \in \mathit{Fringe}$

      $Z := Z \cup \{\langle s, \zeta \rangle\}$

      $\mathit{Fringe} := \mathit{Fringe} \setminus \{\langle s, \zeta \rangle\}$

      for all $e = (s', s, p, X) \in \mathsf{in}(s)$

        $\langle s', \zeta_{\text{new}} \rangle := \mathsf{disc\_pre}_\phi(e, \mathsf{time\_pre}_\phi\langle s, \zeta \rangle)$

        if $\langle s', \zeta_{\text{new}} \rangle \notin Z \ \wedge \ \zeta_{\text{new}} \neq \emptyset$

          $\mathit{Fringe} := \mathit{Fringe} \cup \{\langle s', \zeta_{\text{new}} \rangle\}$

        end if

        if $\langle s', \zeta_{\text{new}} \rangle \notin \mathsf{time\_pre}_\phi([\![\psi]\!]) \ \wedge \ \zeta_{\text{new}} \neq \emptyset$ **then**

          $E := E \cup \{(\langle s', \zeta_{\text{new}} \rangle, \langle s, \zeta \rangle, p, X)\}$

          for all $\langle s', \zeta_{\text{old}} \rangle \in \mathsf{relevant}(p, \langle s', \zeta_{\text{new}} \rangle)$

            if $\langle s', \zeta_{\text{new}} \cap \zeta_{\text{old}} \rangle \notin Z$

              $\mathit{Fringe} := \mathit{Fringe} \cup \{\langle s', \zeta_{\text{new}} \cap \zeta_{\text{old}} \rangle\}$

            end if

          end for all

        end if

      end for all

    end for all

  end while

  return $\mathcal{C} = (Z, \mathit{Steps}(Z, E))$

}

Figure 4: Algorithm for $[\phi \ \exists\mathcal{U} \ \psi]_{\sqsupseteq\lambda}$

The set *Steps for the sets* Z and E can now be defined as follows: $\hat{p} \in \mathit{Steps}\langle s, \zeta \rangle$ iff there exists $p \in \mathsf{dist}\langle s, \zeta \rangle$ and $\mathit{support} \in \mathsf{supports}(\langle s, \zeta \rangle, p)$ such that for any $\langle s', \zeta' \rangle \in Z$:

$$\hat{p}\langle s', \zeta' \rangle = \sum_{(\langle s', \zeta' \rangle, X) \in \mathit{support}} p(s', X)$$

where we consider $(\langle s', \zeta' \rangle, X) \in \mathit{support}$ by abuse of notation.

We now state the formal correctness of our model checking procedure.

Theorem 6 *For any state* $\langle s, \nu \rangle \in Q_G$*,* PTCTL$_\exists$ *formula* θ *and* $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$*:*

$$\langle s, \nu \rangle, \mathcal{E} \models \theta \text{ if and only if } [\nu, \mathcal{E}] \in \mathsf{zone}(s, [\![\theta]\!]).$$

Proof. The proof is given in the Appendix. □

Proposition 7 *The algorithm* **ExistsUntil** *terminates for any formula* $[\phi\ \exists\mathcal{U}\ \psi]_{\sqsupseteq\lambda}$.

Before we give the proof we require the following definition. Given a probabilistic real-time graph G and PTCTL formula θ let $c_{\theta,G}$ be the largest integer constant appearing in the invariant and enabling conditions of G and in the formula θ.

Proof. We first prove by induction on $\theta \in$ PTCTL that, for any $s \in S$, the maximum constant appearing in $\mathsf{zone}(s, [\![\psi]\!]) \in \mathbf{Z}_{\mathcal{X}\cup\mathcal{Z}}$ it is less than or equal to $c_{\theta,G}$. In all cases except $\theta = [\phi\ \exists\mathcal{U}\ \psi]_{\sqsupseteq\lambda}$ this follows by definition.

In the case for $\theta = [\phi\ \exists\mathcal{U}\ \psi]_{\sqsupseteq\lambda}$, since $c_{\theta,G} = \max\{c_{\phi,G}, c_{\psi,G}\}$, it is straightforward to show if the maximum constant appearing in ζ it is less than $c_{\theta,G}$, $\langle s, \zeta' \rangle = \mathsf{time\_pre}_\phi \langle s, \zeta \rangle$ and $\langle s', \zeta'' \rangle = \mathsf{disc\_pre}_\phi(\langle s, \zeta' \rangle, e)$ for some $e \in \mathsf{in}(s)$, then the maximum constant appearing in ζ' and ζ'' is less than $c_{\theta,G}$. Furthermore, if the maximum constant appearing in ζ and ζ' is less than $c_{\theta,G}$, then so is the maximum constant appearing in $\zeta \cap \zeta'$. It then follows that at any point during the algorithm **ExistUntil**, if $\langle s, \zeta \rangle \in Z$ then the maximum constant appearing in ζ it is less than $c_{\theta,G}$.

Finally, since there are only finitely many states and finitely many $\zeta \in \mathbf{Z}_{\mathcal{X}\cup\mathcal{Z}}$ such that the maximum constant appearing ζ is less than $c_{\theta,G}$, it follows that the algorithm must terminate. □

7 Conclusion

We conclude with some observations of the complexity of our method. Though in the worst case the size of the quotient is proportional to the number of regions, we expect that in practice it will result in significantly smaller structures. Future work will address extending the method of [18] for computing the coarsest bisimilarity quotient to our setting. While this should allow for model checking of full PTCTL, the method proposed here can result in a smaller system since it generates a quotient for a particular formula.

References

[1] R. Alur, C. Courcoubetis, and D. Dill. Model-checking in dense real-time. *Information and Computation*, 104(1), 1993.

[2] R. Alur and D. Dill. A theory of timed automata. *Theoretical Computer Science*, 126, 1994.

[3] C. Baier and M. Kwiatkowska. Model checking for a probabilistic branching time logic with fairness. *Distributed Computing*, 11, 1998.

[4] J. Bengtsson, K. Larsen, F. Larsson, P. Pettersson, W. Yi, and C. Weise. New Generation of UPPAAL. In *Int. Workshop on Software Tools for Technology Transfer*, 1998.

[5] A. Bianco and L. de Alfaro. Model checking of probabilistic and nondeterministic systems. In *Proc. FST&TCS'95*, volume 1026 of *Lect. Notes in Comp. Sci.* Springer-Verlag, 1995.

[6] M. Bozga, C. Daws, O. Maler, A. Olivero, S. Tripakis, and S. Yovine. Kronos: a model-checking tool for real-time systems. In *Proc. CAV'98*. Springer Verlag, 1998.

[7] P. D'Argenio, J.-P. Katoen, T. Ruys, and J. Tretmans. The bounded retransmission protocol must be on time! In *Proc. TACAS'97*, volume 1217 of *Lect. Notes in Comp. Sci.* Springer-Verlag, 1997.

[8] L. de Alfaro. *Formal verification of probabilistic systems*. PhD thesis, Stanford University, Department of Computer Science, 1997.

[9] L. de Alfaro. Computing minimum and maximum reachability times in probabilistic systems. In *Proc. CONCUR'99*, volume 1664 of *Lect. Notes in Comp. Sci.* Springer Verlag, 1999.

[10] H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing*, 6(4):512–535, 1994.

[11] T. Henzinger and O. Kupferman. From quantity to quality. In *Proc. HART'97*, Lect. Notes in Comp. Sci. 1201. Springer-Verlag, 1997.

[12] T. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model checking for real-time systems. *Information and Computation*, 111(2), 1994.

[13] M. Kwiatkowska, G. Norman, R. Segala, and J. Sproston. Automatic verification of real-time systems with discrete probability distributions. In *Proc. ARTS'99*, volume 1601 of *Lect. Notes in Comp. Sci.* Springer-Verlag, 1999.

[14] M. Kwiatkowska, G. Norman, R. Segala, and J. Sproston. Automatic verification of real-time systems with discrete probability distributions. Technical Report CSR-00-2, University of Birmingham, 2000.

[15] M. Lindahl, P. Pettersson, and W. Yi. Formal Design and Analysis of a Gear-Box Controller. In *Proc. TACAS'98*, number 1384 in Lect. Notes in Comp. Sci. Springer–Verlag, 1998.

[16] W. Stewart. *Introduction to the Numerical Solution of Markov Chains*. Princeton University Press, 1994.

[17] S. Tripakis. *L'Analyse Formelle des Systèmes Temporisés en Pratique*. PhD thesis, Université Joseph Fourier, 1998.

[18] S. Tripakis and S. Yovine. Analysis of timed systems based on time-abstracting bisimulations. In *Proc. CAV'96*, volume 1102 of *Lect. Notes in Comp. Sci.* Springer-Verlag, 1996.

Appendix (Proof of Theorem 6)

For simplicity we fix a probabilistic timed automaton G and PTCTL formula $[\phi\ \exists\mathcal{U}\ \psi]_{\sqsupseteq\lambda}$. To ease notation, we denote the probabilistic timed structure $\mathcal{M}_G = (Q_G, \mathit{TSteps}_G)$ associated with G by $\mathcal{M} = (Q, \mathit{TSteps})$ and the probabilistic concurrent system $\mathcal{C}_{\phi,\psi} = (Z_{\phi,\psi}, \mathit{Steps}_{\phi,\psi})$ and set of edges $E_{\phi,\psi}$ generated by the algorithm **ExistsUntil**(ϕ, ψ) by $\mathcal{C} = (Z, \mathit{Steps})$ and E respectively.

Before we give the proof of Theorem 6 we introduce the following definitions. For any state $\langle s, \nu\rangle \in Q$ and $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$, we say:

$$\langle s, \nu\rangle, \mathcal{E} \in \mathsf{time\_pre}_\phi\langle s, \zeta\rangle \text{ if } [\nu, \mathcal{E}] \in \zeta' \text{ where } \langle s, \zeta'\rangle = \mathsf{time\_pre}_\phi\langle s, \zeta\rangle.$$

Next, for any adversary A of $\mathcal{M}$ we introduce the sequence of functions $(\mathbf{P}^A_n)_{n\in\mathbb{N}}$. Intuitively, for a state $\langle s, \nu\rangle \in Q$ and $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$, the value $\mathbf{P}^A_n(\langle s, \nu\rangle, \mathcal{E})$ equals the probability of reaching from $\langle s, \nu\rangle$, under the adversary A, a state which satisfies ψ in *at most* n discrete transitions, under the restriction of passing through only ϕ states, and with respect to the formula clock valuation $\mathcal{E}$. Since adversaries can choose on the basis of history, we define $\mathbf{P}^A_n$ over paths, then restrict to the case of single states (paths of length 0).

Definition 8 *For any adversary $A \in \mathit{Adv}_{\mathcal{M}}$, $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$ and finite path $\omega \in \mathit{Path}^A_{\mathit{fin}}$ such that $\mathit{last}(\omega) = \langle s, \nu\rangle$ and $A(\omega) = (t, \tilde{p})$:*

- *if there exists $t' \leq t$ such that $\langle s, \nu + t'\rangle, \mathcal{E} + t' \models \psi$ and $\langle s, \nu + t''\rangle, \mathcal{E} + t'' \models \phi \vee \psi$ for all $t'' \leq t'$, let $\mathbf{P}^A_0(\omega, \mathcal{E}) = 1$*
- *otherwise, let $\mathbf{P}^A_0(\omega, \mathcal{E}) = 0$*

and for any $n \geq 0$:

- *if there exists $t' \leq t$ such that $\langle s, \nu + t'\rangle, \mathcal{E} + t' \models \psi$ and $\langle s, \nu + t''\rangle, \mathcal{E} + t'' \models \phi \vee \psi$ for all $t'' \leq t'$, let $\mathbf{P}^A_{n+1}(\omega, \mathcal{E}) = 1$*
- *if $\langle s, \nu + t'\rangle, \mathcal{E} + t' \models \phi \wedge \neg\psi$ for all $t' \leq t$, let*

$$\mathbf{P}^A_{n+1}(\omega, \mathcal{E}) = \sum_{\langle s', \nu'\rangle \in Q} \tilde{p}\langle s', \nu'\rangle \cdot \mathbf{P}^A_n(\omega \xrightarrow{t,\tilde{p}} \langle s', \nu'\rangle, \mathcal{E} + t)$$

- *otherwise, let $\mathbf{P}^A_{n+1}(\omega, \mathcal{E}) = 0$.*

Lemma 9 *For any $\langle s, \nu\rangle \in Q$ and $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$:*

$$\sup_{A\in \mathit{Adv}_{\mathcal{M}}} \mathit{Prob}\{\omega \mid \omega \in \mathit{Path}^A_{\mathit{ful}}\langle s, \nu\rangle \ \&\ \omega, \mathcal{E} \models \phi\ \mathcal{U}\ \psi\} = \sup_{A\in \mathit{Adv}_{\mathcal{M}}} \lim_{n\to\infty} \mathbf{P}^A_n(\langle s, \nu\rangle, \mathcal{E}).$$

Proof. The lemma is proved by showing for any $\langle s, \nu \rangle \in Q$, $A \in Adv_{\mathcal{M}}$ and $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$:

$$Prob\{\omega \,|\, \omega \in Path^{A}_{ful}\langle s, \nu \rangle \text{ and } \omega, \mathcal{E} \models \phi \,\mathcal{U}\, \psi\} = \lim_{n \to \infty} \mathbf{P}^{A}_{n}(\langle s, \nu \rangle, \mathcal{E})$$

which follows from the fact that we can associate with A a Markov chain whose states are finite paths of $\mathcal{M}$ and the iterative method for PCTL until formulas for Markov chains (see for example [10]). $\square$

Next, for any adversary B of $\mathcal{C}$, we define a sequence of functions $(\mathbf{P}^{B}_{n})_{n \in \mathbb{N}}$. Intuitively, for any state $\langle s, \zeta \rangle$, $\mathbf{P}^{B}_{n}\langle s, \zeta \rangle$ equals the probability, of reaching from state $\langle s, \nu \rangle$ under the adversary B, a state in $[\![\psi]\!]$ in at most n transitions.

Definition 10 *For any adversary $B \in Adv_{\mathcal{C}}$ and $\pi \in Path^{B}_{fin}$, if $last(\pi) = \langle s, \zeta \rangle$, let:*

$$\mathbf{P}^{B}_{0}(\pi) = \begin{cases} 1 & \text{if } \langle s, \zeta \rangle \in \mathsf{time\_pre}_{\phi}[\![\psi]\!] \\ 0 & \text{otherwise} \end{cases}$$

and for any $n \geq 0$, if $B(\pi) = \hat{p}$:

$$\mathbf{P}^{B}_{n+1}(\pi) = \begin{cases} 1 & \text{if } \langle s, \zeta \rangle \in \mathsf{time\_pre}_{\phi}[\![\psi]\!] \\ \sum_{\langle s', \zeta' \rangle \in Z} \hat{p}\langle s', \zeta' \rangle \cdot \mathbf{P}^{B}_{n}(\pi \xrightarrow{\hat{p}} \langle s', \zeta' \rangle) & \text{otherwise.} \end{cases}$$

Lemma 11 *For any $\langle s, \zeta \rangle \in Z$:*

$$ReachE(\langle s, \zeta \rangle, [\![\psi]\!]) = \sup_{B \in Adv_{\mathcal{C}}} \lim_{n \to \infty} \mathbf{P}^{B}_{n}\langle s, \zeta \rangle.$$

Proof. The proof follows similarly to that of Lemma 9. $\square$

We now give the proof of the theorem.

Proof (of Theorem 6)**.** The proof is by induction on $\theta \in \mathrm{PTCTL}_{\exists}$. The cases for $\theta = \texttt{true}$, $\theta \in \mathrm{AP}$, $\theta \in \mathbf{Z}_{\mathcal{X} \cup \mathcal{Z}}$, $\theta = \phi \wedge \psi$, $\theta = \neg\phi$ and $\theta = z.\phi$ follow by definition of $[\![\cdot]\!]$ and $\models$.

In the case of $\theta = [\phi \,\exists\mathcal{U}\, \psi]_{\sqsupseteq\lambda}$, by induction on θ we have:

$$\langle s, \nu \rangle, \mathcal{E} \models \xi \text{ if and only if } [\nu, \mathcal{E}] \in \mathsf{zone}(s, [\![\xi]\!]) \text{ for } \xi \in \{\phi, \psi\}. \tag{1}$$

The remainder of the proof in this case is subdivided into properties **(a)**, **(b)**, **(c)** and **(d)** successively shown below. We first prove that the following holds.

Property **(a)**. For all $(\langle s, \zeta \rangle, \langle s', \zeta' \rangle, p, X) \in E$ if $\nu \in \mathbb{R}^{\mathcal{X}}$, $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$ and $[\nu, \mathcal{E}] \in \zeta$, then there exists $t \in \mathbb{R}$ such that

- $\langle s, \nu \rangle, \mathcal{E} \models \phi$
- ν satisfies $inv(s)$ and $\tau_s(p)$

- $\langle s', \nu[X := 0] + t' \rangle, \mathcal{E} + t' \models \phi \vee \psi$ for all $0 \leq t' \leq t$
- $[\nu, \mathcal{E}][X := 0] + t \in \zeta'$.

Proof of **(a)**. Follows by induction on $\langle s', \zeta' \rangle \in Z$.

- In the base step $\langle s', \zeta' \rangle \in [\![\psi]\!]$, in which case by definition of $\mathsf{time\_pre}_\phi$ and (1), if $\langle s', \nu' \rangle, \mathcal{E} \in \mathsf{time\_pre}_\phi \langle s', \zeta' \rangle$, then there exists $t \in \mathbb{R}$ such that:

$$\langle s', \nu' + t \rangle, \mathcal{E} + t \models \psi \text{ and } \langle s', \nu' + t' \rangle, \mathcal{E} + t' \models \phi \vee \psi \text{ for all } t' \leq t.$$

  Now consider any $(\langle s, \zeta \rangle, \langle s', \zeta' \rangle, p, X) \in E$, then by definition

$$\langle s, \zeta \rangle = \mathsf{disc\_pre}_\phi(e, \mathsf{time\_pre}_\phi \langle s', \zeta' \rangle)$$

  and $e = (s, s', p, X) \in \mathsf{in}(s')$. Property **(a)** then follows by definition of $\mathsf{disc\_pre}_\phi$, (1) and from above.

- For the inductive step, $(\langle s', \zeta' \rangle, \langle s'', \zeta'' \rangle, p', X') \in E$ for some $\langle s'', \zeta'' \rangle \in Z$ and in this case by induction if $[\nu', \mathcal{E}'] \in \zeta'$, then $\langle s', \zeta' \rangle, \mathcal{E}' \models \phi$, and hence $\langle s', \zeta' \rangle, \mathcal{E}' \models \phi \vee \psi$. The remainder of the proof of **(a)** now follows similarly to the base case.

Next we prove the following.

Property **(b)**. For any $\langle s, \nu \rangle \in Q$ and $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$:

$$\langle s, \nu \rangle, \mathcal{E} \models [\phi \, \exists \mathcal{U} \, \psi]_{>0} \;\Leftrightarrow\; \exists \, \langle s, \zeta \rangle \in Z \text{ such that } [\nu, \mathcal{E}] \in \mathsf{time\_pre}_\phi(\zeta).$$

Proof of **(b)**. Follows from **(a)** and since:

- for any $\langle s, \nu \rangle \in Q$ and $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$, $\langle s, \nu \rangle, \mathcal{E} \models [\phi \, \exists \mathcal{U} \, \psi]_{>0}$ if and only if there exists a path $\omega \in \mathit{Path}_{\mathit{ful}} \langle s, \nu \rangle$ and a position (i, t) of ω such that $\omega(i) + t, \mathcal{E} + \mathcal{D}_\omega(i) + t \models_{\mathcal{A}} \phi_2$, and for all positions (j, t') of ω such that $(j, t') \prec (i, t)$, $\omega(j) + t', \mathcal{E} + \mathcal{D}_\omega(j) + t' \models_{\mathcal{A}} \phi_1 \vee \phi_2$ where $\mathcal{D}_\omega(i)$ is the total elapsed time up to step i.

- $\langle s, \zeta \rangle \in Z$ if and only if there exists $\pi \in \mathit{Path}_{\mathit{ful}} \langle s, \zeta \rangle$ such that $\pi(i) \in [\![\psi]\!]$ for some $i \in \mathbb{N}$, which follows by construction of $\mathcal{C}$.

Finally, we show a correspondence between the probability values of $\mathbf{P}_n^A$ for adversaries A of the probabilistic timed structure $\mathcal{M}$ and $\mathbf{P}_n^B$ for adversaries B of the constructed concurrent probabilistic system $\mathcal{C}$. Since $\mathcal{C}$ contains only the portion corresponding to the satisfaction of the formula $[\phi \, \exists \mathcal{U} \, \psi]_{\sqsupseteq \lambda}$, we only consider the adversaries A of $\mathcal{M}$ which satisfy:

$$\mathit{Prob}\{\omega \mid \omega \in \mathit{Path}_{\mathit{ful}}^A \langle s, \nu \rangle \text{ and } \omega, \mathcal{E} \models \phi \, \mathcal{U} \, \psi\} > 0.$$

Formally, we will show the following correspondence. For all $n \in \mathbb{N}$, $\langle s, \nu\rangle \in Q$ and $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$ such that $\langle s, \nu\rangle, \mathcal{E} \models [\phi \, \exists \mathcal{U} \, \psi]_{>0}$, it is the case that:

Property **(c)**. If $B \in Adv_{\mathcal{C}}$, $\langle s, \zeta\rangle \in Z$ and $\langle s, \nu\rangle, \mathcal{E} \in \mathsf{time\_pre}_{\phi}\langle s, \zeta\rangle$, then there exists $A \in Adv_{\mathcal{M}}$ such that $\mathbf{P}^A_n(\langle s, \nu\rangle, \mathcal{E}) \geq \mathbf{P}^B_n\langle s, \zeta\rangle$

Property **(d)**. If $A \in Adv_{\mathcal{M}}$ and $Prob\{\omega \,|\, \omega \in Path^A_{ful}\langle s, \nu\rangle$ and $\omega, \mathcal{E} \models \phi \, \mathcal{U} \, \psi\} > 0$, then there exists $\langle s, \zeta\rangle \in Z$ such that $\langle s, \nu\rangle, \mathcal{E} \in \mathsf{time\_pre}_{\phi}\langle s, \zeta\rangle$ and $B \in Adv_{\mathcal{C}}$ such that $\mathbf{P}^B_n\langle s, \zeta\rangle \geq \mathbf{P}^A_n(\langle s, \nu\rangle, \mathcal{E})$.

It follows from **(b)**, Lemma 9 and Lemma 11 that to prove Theorem 6 it is sufficient to show that **(c)** and **(d)** hold.

Proof of **(c)**, **(d)** (base case). We now prove **(c)** and **(d)** by induction on $n \in \mathbb{N}$. The case for $n = 0$ for both **(c)** and **(d)** is proved by showing: if $\langle s, \nu\rangle \in Q$, $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$, $A \in Adv_{\mathcal{M}}$, $\langle s, \zeta\rangle \in Z$ such that $\langle s, \nu\rangle \in \mathsf{time\_pre}_{\phi}\langle s, \zeta\rangle$ and $B \in Adv_{\mathcal{C}}$ then:

$$
\begin{array}{rcll}
\mathbf{P}^A_0(\langle s, \nu\rangle, \mathcal{E}) > 0 & \Leftrightarrow & \mathbf{P}^A_0(\langle s, \nu\rangle, \mathcal{E}) = 1 & \text{by Definition 8} \\
& \Leftrightarrow & \langle s, \nu\rangle, \mathcal{E} \in \mathsf{time\_pre}_{\phi}[\![\psi]\!] & \text{by induction} \\
& \Leftrightarrow & \mathbf{P}^B_0\langle s, \zeta\rangle = 1 & \text{by Definition 10.}
\end{array}
$$

Next, suppose the property holds for some $n \in \mathbb{N}$ and consider any $\langle s, \nu\rangle \in Q$ and $\mathcal{E} \in \mathbb{R}^{\mathcal{Z}}$ such that $\langle s, \nu\rangle, \mathcal{E} \models [\phi \, \exists \mathcal{U} \, \psi]_{>0}$. If $\langle s, \nu + t\rangle, \mathcal{E} + t \models \psi$ for some $t \in \mathbb{R}$ and $\langle s, \nu + t'\rangle, \mathcal{E} + t' \models \phi$ for all $t' \leq t$, then the result follows similarly to the case when $n = 0$ and we are left to consider when $\langle s, \nu + t\rangle, \mathcal{E} + t \not\models \psi$ for all $t \in \mathbb{R}$.

Proof of **(c)** (induction step). Let $B \in Adv_{\mathcal{C}}$ and $\langle s, \zeta\rangle \in Z$ such that $\langle s, \nu\rangle, \mathcal{E} \in \mathsf{time\_pre}_{\phi}\langle s, \zeta\rangle$. By construction, $B\langle s, \zeta\rangle = \hat{p}$ for some $\hat{p} \in Steps\langle s, \zeta\rangle$, and there exists $p \in prob(s)$ and $support \in \mathsf{supports}(\langle s, \zeta\rangle, p)$ such that for any $\langle s', \zeta'\rangle \in Z$:

$$
\hat{p}\langle s', \zeta'\rangle = \sum_{(\langle s', \zeta'\rangle, X) \in support} p(s', X).
$$

Furthermore, supposing B' is the adversary of $\mathcal{C}$ such that

$$
\mathbf{P}^{B'}_n(\langle s', \zeta'\rangle) = \mathbf{P}^B_n(\langle s, \zeta\rangle \xrightarrow{\hat{p}} \langle s', \zeta'\rangle),
$$

if $(\langle s', \zeta'\rangle, X) \in support$ for some $X \subseteq \mathcal{X}$, then by Definition 10:

$$
\mathbf{P}^B_{n+1}\langle s, \zeta\rangle = \sum_{(\langle s', \zeta'\rangle, X) \in support} p(s', X) \cdot \mathbf{P}^{B'}_n\langle s', \zeta'\rangle. \tag{2}
$$

Moreover, by construction of *Steps*: $(\langle s', \zeta'\rangle, X) \in support$ if and only if $(\langle s, \hat{\zeta}\rangle, \langle s', \zeta'\rangle, p, X) \in E$ for some $\hat{\zeta} \supseteq \zeta$. Also, for any $t \in \mathbb{R}$ such that $\langle s, \nu + t\rangle, \mathcal{E} + t \in \langle s, \zeta\rangle$, if $(\langle s', \zeta'\rangle, X) \in support$, then $\langle s', (\nu + t)[X := 0]\rangle, \mathcal{E} + t \in \mathsf{time\_pre}_{\phi}\langle s', \zeta'\rangle$ by construction of E.

Now, by construction of *support*, for any $(s', X) \in \mathsf{support}(p)$, either $(\langle s', \zeta' \rangle, X) \notin$ *support* for all $\langle s', \zeta' \rangle \in Z$, or there exists a unique $\langle s', \zeta' \rangle \in Z$ such that $(\langle s', \zeta' \rangle, X) \in$ *support*. Considering the adversary A such that $A\langle s, \nu \rangle = (t, \tilde{p})$, $\mathsf{type}(\tilde{p}) = p$ and for all $(\langle s', \zeta' \rangle, X) \in$ *support*:

$$\mathbf{P}^{A}_{n}(\langle s, \nu \rangle \xrightarrow{t,\tilde{p}} \langle s, \nu + t[X := 0] \rangle, \mathcal{E} + t) \geq \mathbf{P}^{B'}_{n} \langle s', \zeta' \rangle \tag{3}$$

(which exists by induction on **(c)**), then letting $\nu^t_X = (\nu + t)[X := 0]$ and $\mathcal{E}^t = \mathcal{E} + t$ to ease notation, by Definition 8 we have:

$$\begin{aligned}
\mathbf{P}^{A}_{n+1}(\langle s, \nu \rangle, \mathcal{E}) &= \sum_{\langle s', \nu' \rangle \in Q} \tilde{p}\langle s', \nu' \rangle \cdot \mathbf{P}^{A}_{n}(\langle s, \nu \rangle \xrightarrow{t,\tilde{p}} \langle s', \nu' \rangle, \mathcal{E}^t) \\
&= \sum_{(s', X) \in \mathsf{support}(p)} p(s', X) \cdot \mathbf{P}^{A}_{n}(\langle s, \nu \rangle \xrightarrow{t,\tilde{p}} \langle s', \nu^t_X \rangle, \mathcal{E}^t) && \text{by definition of } \tilde{p} \\
&\geq \sum_{(\langle s', \zeta' \rangle, X) \in \mathit{support}} p(s', X) \cdot \mathbf{P}^{A}_{n}(\langle s, \nu \rangle \xrightarrow{t,\tilde{p}} \langle s', \nu^t_X \rangle, \mathcal{E}^t) && \text{from above} \\
&\geq \sum_{(\langle s', \zeta' \rangle, X) \in \mathit{support}} p(s', X) \cdot \mathbf{P}^{B'}_{n} \langle s', \zeta' \rangle && \text{by (3)} \\
&= \mathbf{P}^{B}_{n+1} \langle s, \zeta \rangle && \text{by (2)}
\end{aligned}$$

and since $\langle s, \zeta \rangle$ and B are arbitrary, **(c)** holds by induction.

Proof of **(d)** (induction step). For the proof in this case consider any adversary $A \in \mathit{Adv}_{\mathcal{M}}$ such that $\mathit{Prob}\{\omega \,|\, \omega \in \mathit{Path}^{A}_{\mathit{ful}}\langle s, \nu \rangle \text{ and } \omega, \mathcal{E} \models \phi \,\mathcal{U}\, \psi\} > 0$. Now, by definition $A\langle s, \nu \rangle = (t, \tilde{p})$ for some $t \in \mathbb{R}$ and $\tilde{p} \in \mu(Q)$, and by definition of $\models$ and $\mathcal{M}$:

- $\nu + t'$ satisfies $\mathit{inv}(s)$ for all $0 \leq t' \leq t$
- $\nu + t$ satisfies $\tau_s(\mathsf{type}(\tilde{p}))$
- $\langle s, \nu + t' \rangle, \mathcal{E} + t' \models \phi$ for all $0 \leq t' \leq t$.

Also, supposing $\mathsf{type}(\tilde{p}) = p$, then it is straightforward to show:

$$\mathbf{P}^{A}_{n+1}(\langle s, \nu \rangle, \mathcal{E}) = \sum_{(s', X) \in \mathsf{support}(p)} p(s, X) \cdot \mathbf{P}^{A'}_{n}(\langle s', (\nu + t)[X := 0] \rangle, \mathcal{E} + t) \tag{4}$$

for some $A' \in \mathit{Adv}_{\mathcal{M}}$. Now consider any $(s', X) \in \mathsf{support}(p)$ such that

$$\mathbf{P}^{A'}_{n} \langle s', (\nu + t)[X := 0] \rangle, \mathcal{E} + t) > 0,$$

then by definition $(s, s', p, X) \in \mathsf{in}(s')$ and by induction there exists $\langle s', \zeta'_{s',X} \rangle \in Z$ and adversary B' such that

$$\mathbf{P}^{B'}_{n} \langle s', \zeta'_{s',X} \rangle \geq \mathbf{P}^{A'}_{n}(\langle s', (\nu + t)[X := 0] \rangle, \mathcal{E} + t)$$

and $\langle s', (\nu + t)[X := 0] \rangle, \mathcal{E} + t \in \mathsf{time\_pre}_{\phi}\langle s', \zeta'_{s',X} \rangle$. Letting:

$$\langle s, \zeta_{s',X} \rangle = \mathsf{disc\_pre}_{\phi}((s, s', X, p), \mathsf{time\_pre}_{\phi}\langle s', \zeta'_{s',X} \rangle),$$

it follows that

- $\langle s, \zeta_{s',X} \rangle, \langle s', \zeta'_{s',X} \rangle \in Z$
- $\langle s, \nu + t \rangle, \mathcal{E} + t \in \langle s, \zeta_{s',X} \rangle$
- $\langle s, (\nu + t)[X := 0] \rangle, \mathcal{E} + t \in \mathsf{time\_pre}_{\phi} \langle s', \zeta'_{s',X} \rangle$
- $(\langle s, \zeta_{s',X} \rangle, \langle s', \zeta'_{s',X} \rangle, p, X) \in E$.

It then follows by construction of Z that $\langle s, \zeta \rangle \in Z$ where

$$\zeta = \cap \{ \zeta_{s',X} \mid (s', X) \in \mathsf{support}(p) \ \& \ \langle s', (\nu + t)[X := 0] \rangle, \mathcal{E} + t \models [\phi \ \exists\mathcal{U} \ \psi]_{>0} \}$$

and from above $[\nu, \mathcal{E}] + t \in \zeta$. Furthermore, by construction of *Steps* there exists $\hat{p} \in$ *Steps*$\langle s, \zeta \rangle$ such that for any $\langle s', \zeta' \rangle \in Z$:

$$\hat{p}\langle s', \zeta' \rangle \geq \sum_{\substack{(s',X) \in \mathsf{support}(p), \ \zeta' = \zeta_{s',X} \\ \& \, \mathbf{P}_n^{A'} \langle s', (\nu+t)[X:=0] \rangle, \mathcal{E}+t) > 0}} p(s, X). \tag{5}$$

Now, define B as the adversary of $\mathcal{C}$ such that $B\langle s, \zeta \rangle = \hat{p}$ and whose behaviour is exactly as B' in $\langle s, \zeta \rangle \xrightarrow{\hat{p}} \langle s', \zeta'_{s',X} \rangle$. Let $\nu_X^t = (\nu + t)[X := 0]$, $\mathcal{E}^t = \mathcal{E} + t$ and $\theta' = [\phi \ \exists\mathcal{U} \ \psi]_{>0}$ to ease notation. By Definition 10, we have:

$$\begin{array}{lll}
\mathbf{P}_{n+1}^{B} \langle s, \zeta \rangle = & \displaystyle\sum_{\langle s', \zeta' \rangle \in Z} \hat{p}\langle s', \zeta' \rangle \cdot \mathbf{P}_n^B(\langle s, \zeta \rangle \xrightarrow{\hat{p}} \langle s', \zeta' \rangle) & \\
\geq & \displaystyle\sum_{\substack{(s',X) \in \mathsf{support}(p) \, \& \\ \mathbf{P}_n^{A'} \langle s', \nu_X^t \rangle, \mathcal{E}^t) > 0}} p(s, X) \cdot \mathbf{P}_n^B(\langle s, \zeta \rangle \xrightarrow{\hat{p}} \langle s', \zeta'_{s',X} \rangle) & \text{by (5)} \\
\geq & \displaystyle\sum_{\substack{(s',X) \in \mathsf{support}(p) \, \& \\ \mathbf{P}_n^{A'} \langle s', \nu_X^t \rangle, \mathcal{E}^t) > 0}} p(s, X) \cdot \mathbf{P}_n^{A'}(\langle s', \nu_X^t \rangle, \mathcal{E}^t) & \text{by construction of } B \\
= & \displaystyle\sum_{(s',X) \in \mathsf{support}(p)} p(s, X) \cdot \mathbf{P}_n^{A'}(\langle s, \nu_X^t \rangle, \mathcal{E}^t) & \text{rearranging} \\
= & \mathbf{P}_{n+1}^{A}(\langle s, \nu \rangle, \mathcal{E}) & \text{by (4)}
\end{array}$$

as required. $\square$