Model Checking CTMCs Against Timed Automata

Taolue Chen[1] Tingting Han[2,3]
Joost-Pieter Katoen[2,3] Alexandru Mereacre[2]

[1]CWI, The Netherlands
[2]RWTH Aachen University, Germany
[3]University of Twente, The Netherlands

Summerschool on Model Checking, Beijing, October 13, 2010

Verifying Markov chains

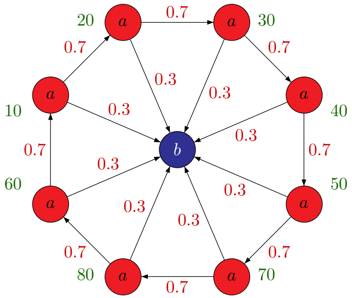
<table>
<tr><td></td><td colspan="2">branching time</td><td colspan="3">linear time</td></tr>
<tr><td rowspan="3">discrete-
time
(DTMC $\mathcal{D}$)</td><td colspan="2">PCTL</td><td colspan="3">LTL</td></tr>
<tr><td colspan="2">linear equations
[HJ94] $(\star)$</td><td colspan="2">automata-based
[V85,CSS03] $(\star\star)$</td><td>tableau-based
[CY95]</td></tr>
<tr><td colspan="2">PTIME</td><td colspan="3">PSPACE-C</td></tr>
<tr><td rowspan="3">continuous-
time
(CTMC $\mathcal{C}$)</td><td>untimed
PCTL</td><td>real-time
CSL</td><td>untimed
LTL</td><td colspan="2"></td></tr>
<tr><td>$emb(\mathcal{C})$
$(\star)$</td><td>integral equations
[BHHK03]</td><td>$emb(\mathcal{C})$
$(\star\star)$</td><td colspan="2"></td></tr>
<tr><td>PTIME</td><td>PTIME</td><td>PSPACE-C</td><td colspan="2"></td></tr>
</table>

Our contribution

<table>
<tr><td></td><td colspan="2">branching time</td><td colspan="2">linear time</td></tr>
<tr><td rowspan="3">discrete-time
(DTMC $\mathcal{D}$)</td><td colspan="2">PCTL</td><td colspan="2">LTL</td></tr>
<tr><td colspan="2">linear equations
[HJ94] ($\star$)</td><td>automata-based
[V85,CSS03] ($\star\star$)</td><td>tableau-based
[CY95]</td></tr>
<tr><td colspan="2">PTIME</td><td colspan="2">PSPACE-C</td></tr>
<tr><td rowspan="3">continuous-time
(CTMC $\mathcal{C}$)</td><td>untimed
PCTL</td><td>real-time
CSL</td><td>untimed
LTL</td><td rowspan="3">real-time
DTA
integral equations
of second type (PDPs)</td></tr>
<tr><td>$emb(\mathcal{C})$
($\star$)</td><td>integral equations
[BHHK03]</td><td>$emb(\mathcal{C})$
($\star\star$)</td></tr>
<tr><td>PTIME</td><td>PTIME</td><td>PSPACE-C</td></tr>
</table>

Continuous-time Markov chain

A *Continuous-Time Markov Chain* is a tuple $\mathcal{C} = (S, \mathrm{AP}, L, \alpha, \mathbf{P}, E)$:

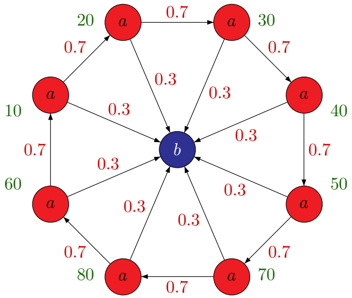


- S - finite set of *states*;
- AP - set of *atomic propositions*;
- $L : S \rightarrow 2^{\mathrm{AP}}$ - *labeling function*;
- $\alpha \in \mathit{Distr}(S)$ - *initial distribution*;
- $\mathbf{P} : S \times S \rightarrow [0, 1]$ - *transition probability matrix*;
- $E : S \rightarrow \mathbb{R}_{\geqslant 0}$ - *exit rate function*

A CTMC is a Kripke structure with random delays!

Continuous-time Markov chain

A *Continuous-Time Markov Chain* is a tuple $\mathcal{C} = (S, \mathrm{AP}, L, \alpha, \mathbf{P}, E)$:



- S - finite set of *states*;
- AP - set of *atomic propositions*;
- $L : S \to 2^{\mathrm{AP}}$ - *labeling function*;
- $\alpha \in Distr(S)$ - *initial distribution*;
- $\mathbf{P} : S \times S \to [0, 1]$ - *transition probability matrix*;
- $E : S \to \mathbb{R}_{\geqslant 0}$ - *exit rate function*

A CTMC is a Kripke structure with random delays!

CTMC semantics

Let $\mathcal{C} = (S, \mathrm{AP}, L, \alpha, \mathbf{P}, E)$ be a CTMC

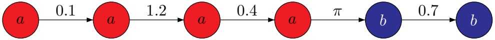
State residence time distribution

$1 - e^{-E(s)\cdot d}$ is the probability to leave state s in interval $[0, d]$

Jump behaviour

$\left(1 - e^{-E(s)\cdot d}\right) \cdot \mathbf{P}(s, s')$ is the probability to take $s \rightarrow s'$ in $[0, d]$

Paths are alternating sequences of states and positive reals



$\mathrm{Pr}^{\mathcal{C}}$ denotes the probability measure on CTMC paths

σ-algebra of $\mathcal{C}$ is generated by cylinder sets over finite paths

Properties are specified over CTMC paths

Properties: branching time (CTL, PCTL, CSL) and linear time (LTL)

Today: linear real-time properties = deterministic timed automata

Properties are specified over CTMC paths

Properties: branching time (CTL, PCTL, CSL) and linear time (LTL)

Today: linear real-time properties = deterministic timed automata

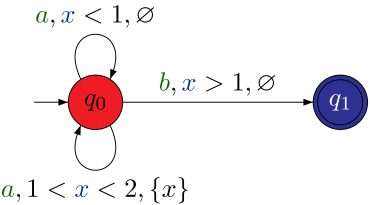
Properties are specified over CTMC paths

Properties: branching time (CTL, PCTL, CSL) and linear time (LTL)

Today: linear real-time properties = deterministic timed automata

Deterministic Timed Automata

A *Deterministic Timed Automaton* is a tuple $\mathcal{A} = (\Sigma, \mathcal{X}, Q, q_0, Q_F, \rightarrow)$:

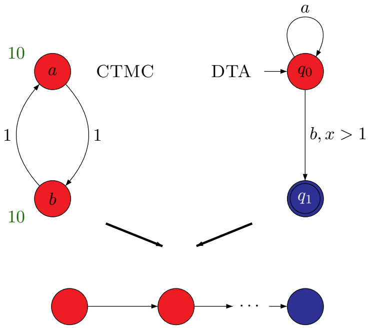


- Σ - *alphabet*;
- $\mathcal{X}$ - finite set of *clocks*;
- Q - finite set of *locations*;
- $q_0 \in Q$ - *initial location*;
- $Q_F \subseteq Q$ - *accept locations*;
- $\rightarrow \in Q \times \Sigma \times \mathcal{B}(\mathcal{X}) \times 2^{\mathcal{X}} \times Q$ - *transition relation*;

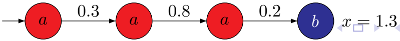
Determinism: $q \xrightarrow{a,g,X} q'$ and $q \xrightarrow{a,g',X'} q''$ implies $g \cap g' = \varnothing$

Problem statement

Given a $\mathrm{CTMC}\ \mathcal{C}$ and a $\mathrm{DTA}\ \mathcal{A}$ compute the probability of all paths in $\mathcal{C}$ which satisfy (accepting path) the property $\mathcal{A}$



Example accepting CTMC path:



Measurability and zenoness

Measurability theorem

For CTMC $\mathcal{C}$ and DTA $\mathcal{A}$, $Paths^{\mathcal{C}}(\mathcal{A})$ is measurable

Zeno behaviours

The set of Zeno (i.e., time-convergent) paths in CTMC $\mathcal{C}$ has measure zero

Automata-based approaches

model	automaton	product	property
LTS TS	Nondet. Büchi $\mathcal{A}$	LTS $TS \otimes \mathcal{A}$	$\Box \Diamond acc$
DTMC $\mathcal{D}$	Deter. Rabin $\mathcal{A}$	DTMC $\mathcal{D} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC_{acc})
MDP $\mathcal{M}$	Deter. Rabin $\mathcal{A}$	MDP $\mathcal{M} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC_{acc})
CTMC $\mathcal{C}$	Deter. Rabin $\mathcal{A}$	CTMC $\mathcal{C} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC_{acc})

Combining a CTMC with a DTA

For $\underbrace{\mathcal{C} = (S, \mathrm{AP}, L, s_0, \mathbf{P}, E)}_{\text{a CTMC}}$ and $\underbrace{\mathcal{A} = (2^{\mathrm{AP}}, \mathcal{X}, Q, q_0, Q_F, \rightarrow)}_{\text{a DTA}}$,

let the product $\mathcal{C} \otimes \mathcal{A} = (Loc, \mathcal{X}, \ell_0, Loc_F, E, \rightsquigarrow)$ be defined by:

- $Loc := S \times Q$;
- $\ell_0 := \langle s_0, q_0 \rangle$;
- $Loc_F := S \times Q_F$;
- $E(\langle s, q \rangle) := E(s)$;
- $\rightsquigarrow$ is defined as:

$$\frac{\mathbf{P}(s, s') > 0 \ \wedge \ q \xrightarrow{L(s), g, X} q'}{\langle s, q \rangle \overset{g, X}{\rightsquigarrow} \zeta} \quad \text{where } \zeta(\langle s', q' \rangle) = \mathbf{P}(s, s')$$

Standard automata-based approach

model	automaton	product	property
LTS TS	Nondet. Büchi $\mathcal{A}$	LTS $TS \otimes \mathcal{A}$	$\Box\Diamond acc$
DTMC $\mathcal{D}$	Deter. Rabin $\mathcal{A}$	DTMC $\mathcal{D} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC_{acc})
MDP $\mathcal{M}$	Deter. Rabin $\mathcal{A}$	MDP $\mathcal{M} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC_{acc})
CTMC $\mathcal{C}$	Deter. Rabin $\mathcal{A}$	CTMC $\mathcal{C} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC_{acc})
CTMC $\mathcal{C}$	DTA $\mathcal{A}$	~~CTMC~~ $\mathcal{C} \otimes \mathcal{A}$	

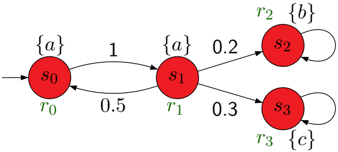
Standard automata-based approach

model	automaton	product	property
LTS TS	Nondet. Büchi $\mathcal{A}$	LTS $TS \otimes \mathcal{A}$	$\Box \Diamond acc$
DTMC $\mathcal{D}$	Deter. Rabin $\mathcal{A}$	DTMC $\mathcal{D} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC$_{acc}$)
MDP $\mathcal{M}$	Deter. Rabin $\mathcal{A}$	MDP $\mathcal{M} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC$_{acc}$)
CTMC $\mathcal{C}$	Deter. Rabin $\mathcal{A}$	CTMC $\mathcal{C} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC$_{acc}$)
CTMC $\mathcal{C}$	DTA $\mathcal{A}$	DMTA $\mathcal{C} \otimes \mathcal{A}$	

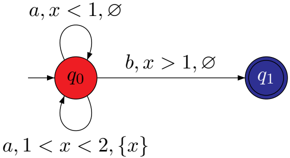
Standard automata-based approach

model	automaton	product	property
LTS TS	Nondet. Büchi $\mathcal{A}$	LTS $TS \otimes \mathcal{A}$	$\Box \Diamond acc$
DTMC $\mathcal{D}$	Deter. Rabin $\mathcal{A}$	DTMC $\mathcal{D} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC_{acc})
MDP $\mathcal{M}$	Deter. Rabin $\mathcal{A}$	MDP $\mathcal{M} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC_{acc})
CTMC $\mathcal{C}$	Deter. Rabin $\mathcal{A}$	CTMC $\mathcal{C} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC_{acc})
CTMC $\mathcal{C}$	DTA $\mathcal{A}$	DMTA $\mathcal{C} \otimes \mathcal{A}$	?

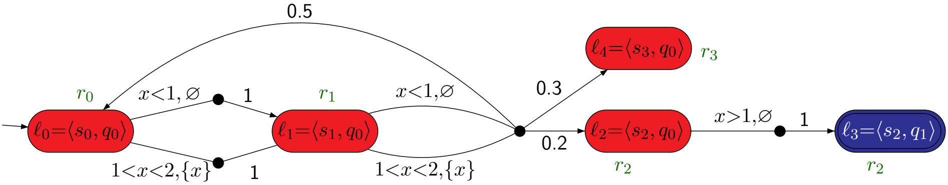
Let's consider a small example



(a) CTMC $\mathcal{C}$



(b) DTA $\mathcal{A}$

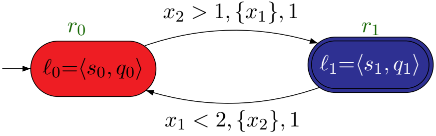


(c) the product $\mathcal{C} \otimes \mathcal{A}$

$\mathcal{C} \otimes \mathcal{A}$ is a deterministic Markovian timed automaton (DMTA)

Deterministic Markovian Timed Automaton

A DMTA is a tuple $(Loc, \mathcal{X}, \ell_0, Loc_F, E, \rightsquigarrow)$ with:



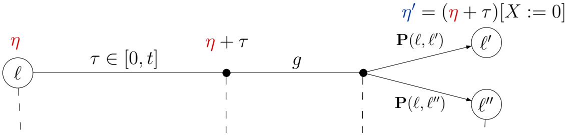
- Loc - finite set of *locations*;
- $\mathcal{X}$ - finite set of *clocks*;
- $\ell_0 \in Loc$ - *initial location*;
- $Loc_F \subseteq Loc$ - *accept locations*;
- $E : Loc \rightarrow \mathbb{R}_{\geqslant 0}$ - *exit rates*;

$$\rightsquigarrow \subseteq Loc \times \mathcal{B}(\mathcal{X}) \times 2^{\mathcal{X}} \times Distr(Loc) \text{ - } \textit{edge relation}$$

Determinism: $\ell \overset{g,X}{\rightsquigarrow} \zeta$ and $\ell \overset{g',X'}{\rightsquigarrow} \zeta'$ implies $g \cap g' = \varnothing$

DMTA semantics

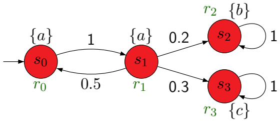
The probability to take $\ell \xrightarrow[\mathbf{P}(\ell,\ell')]{g,X} \ell'$ in $[0,t]$ given clock valuation η is:



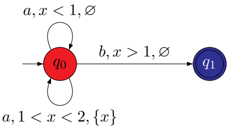
$$p_{\eta}(\ell, \ell', t) \quad = \quad \int_0^t \underbrace{E(\ell) \cdot e^{-E(\ell)\tau}}_{\textit{density to leave } \ell \textit{ at } \tau} \quad \cdot \quad \underbrace{\mathbf{1}_g(\eta + \tau)}_{\eta+\tau \models g?} \quad \cdot \quad \mathbf{P}(\ell, \ell') \quad d\tau$$

η is the clock valuation on entering ℓ

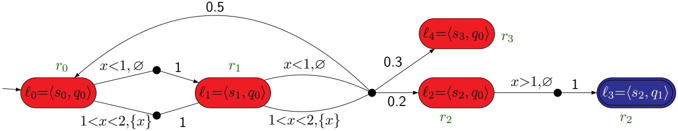
Equivalent measures



(d) CTMC $\mathcal{C}$



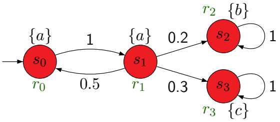
(e) DTA $\mathcal{A}$



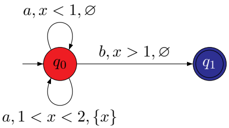
(f) the product $\mathcal{C} \otimes \mathcal{A}$

Theorem: $\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right) = \Pr_0^{\mathcal{C}\otimes\mathcal{A}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond Loc_F)\right)$

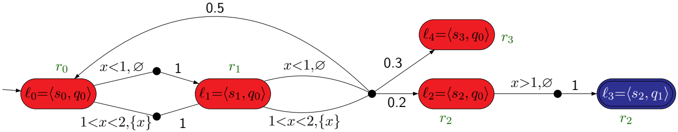
Equivalent measures



(g) CTMC $\mathcal{C}$



(h) DTA $\mathcal{A}$



(i) the product $\mathcal{C} \otimes \mathcal{A}$

Theorem: $\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right) = \Pr^{\mathcal{C}\otimes\mathcal{A}}_{\vec{0}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond Loc_F)\right)$

Roadmap

$$\text{CTMC } \mathcal{C} + \text{DTA } \mathcal{A} \qquad \Pr{}^{\mathcal{C}}\big(\mathit{Paths}^{\mathcal{C}}(\mathcal{A})\big)$$

$$\downarrow \qquad\qquad\qquad ||$$

$$\text{DMTA } \mathcal{C} \otimes \mathcal{A} \qquad \Pr{}^{\mathcal{C}\otimes\mathcal{A}}_{\vec{0}}\big(\mathit{Paths}^{\mathcal{C}\otimes\mathcal{A}}(\Diamond\, \mathit{Loc}_F)\big)$$

But how to effectively compute these probabilities?

Roadmap

$$\text{CTMC } \mathcal{C} + \text{DTA } \mathcal{A} \qquad \Pr^{\mathcal{C}}\left(\mathit{Paths}^{\mathcal{C}}(\mathcal{A})\right)$$

$$\downarrow \qquad\qquad\qquad\qquad ||$$

$$\text{DMTA } \mathcal{C} \otimes \mathcal{A} \qquad \Pr^{\mathcal{C}\otimes\mathcal{A}}_{\vec{0}}\left(\mathit{Paths}^{\mathcal{C}\otimes\mathcal{A}}(\Diamond\, \mathit{Loc}_F)\right)$$

But how to effectively compute these probabilities?

Calculating reachability probabilities in PDPs

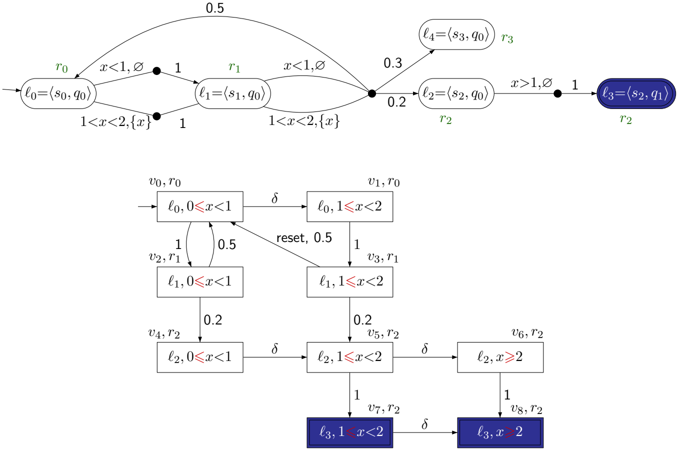
$\text{CTMC } \mathcal{C} + \text{DTA } \mathcal{A}$	$\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right)$
$\downarrow$	$\vert\vert$
$\text{DMTA } \mathcal{C} \otimes \mathcal{A}$	$\Pr_{\vec{0}}^{\mathcal{C}\otimes\mathcal{A}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond\, Loc_F)\right)$
$\downarrow$	$\downarrow$
region graph $= \text{PDP } \mathcal{Z}$	reachability probabilities
$\downarrow$	$\downarrow$
embedded $\text{DTMP } emb(\mathcal{Z})$	$\Pr^{emb(\mathcal{Z})}\left((v_0, \vec{0}), (V_F, \cdot)\right)$
	$\downarrow$
	partial differential equations

Region graph

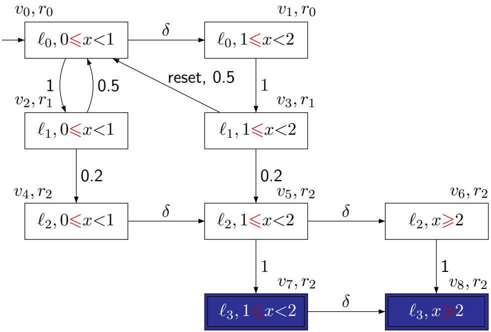
The region graph $\mathcal{G}(\mathcal{M}) = (V, v_0, V_F, \Lambda, \hookrightarrow)$ of DMTA $\mathcal{M}$ is given by:

- $V := Loc \times \mathcal{B}(\mathcal{X})$ - set of *vertices*, consisting of a location and a region;
- $v_0 = (\ell_0, \vec{0})$ - *initial vertex*;
- $V_F := \{v \mid v\downharpoonleft_1 \in Loc_F\}$ - set of *accepting vertices*;
- $\Lambda : V \to \mathbb{R}_{\geqslant 0}$ - *exit rate function* where $\Lambda(v) := E(v\downharpoonleft_1)$;
- $\hookrightarrow \subseteq V \times \big(([0,1] \times 2^{\mathcal{X}}) \cup \{\delta\}\big) \times V$ - *transition (edge) relation*
  - $v \overset{\delta}{\hookrightarrow} v'$ - delay transition
  - $v \overset{p,X}{\hookrightarrow} v'$ - Markovian transition

Region graph example



This is a piecewise deterministic Markov process!



Piecewise Deterministic Markov Processes [Davis84]

A Piecewise-Deterministic (Markov) Process is a tuple

$$\mathcal{Z} = (Z, \mathcal{X}, Inv, \phi, \Lambda, \mu)$$

- Z and $\mathcal{X}$ - finite sets of *locations* and *variables*;
- $Inv : Z \to \mathcal{B}_c(\mathcal{X})$ - *invariant function*; e.g., $x < 2$
- $\phi : Z \times \mathcal{V}(\mathcal{X}) \times \mathbb{R} \to \mathcal{V}(\mathcal{X})$ - *flow function*; η now, $\phi(z, \eta, t)$ in t time
- $\Lambda : \mathbb{S} \to \mathbb{R}_{>0}$ - *exit rate function*;
- $\mu : \mathbb{S} \cup \partial\mathbb{S} \to Distr(\mathbb{S})$ - *transition probability function*;

Piecewise Deterministic Markov Processes [Davis84]

A Piecewise-Deterministic (Markov) Process is a tuple

$$\mathcal{Z} = (Z, \mathcal{X}, Inv, \phi, \Lambda, \mu)$$

- Z and $\mathcal{X}$ - finite sets of *locations* and *variables*;
- $Inv : Z \to \mathcal{B}_o(\mathcal{X})$ - *invariant function*; e.g., $x<2$
  - $\mathbb{S} = \{\xi = (z, \eta) \mid z \in Z, \eta \in Inv(z)\}$ is the state space;
  - $\partial\mathbb{S} = \bigcup_{z \in Z}(\{z\} \times \partial Inv(z))$ the boundary of $\mathbb{S}$ $(z, x=2)$
- $\phi : Z \times \mathcal{V}(\mathcal{X}) \times \mathbb{R} \to \mathcal{V}(\mathcal{X})$ - *flow function*; η now, $\phi(z, \eta, t)$ in t time
- $\Lambda : \mathbb{S} \to \mathbb{R}_{>0}$ - *exit rate function*;
- $\mu : \mathbb{S} \cup \partial\mathbb{S} \to Distr(\mathbb{S})$ - *transition probability function*;

Piecewise Deterministic Markov Processes [Davis84]

A Piecewise-Deterministic (Markov) Process is a tuple

$$\mathcal{Z} = (Z, \mathcal{X}, Inv, \phi, \Lambda, \mu)$$

- Z and $\mathcal{X}$ - finite sets of *locations* and *variables*;
- $Inv : Z \rightarrow \mathcal{B}_o(\mathcal{X})$ - *invariant function*; e.g., $x<2$
  - $\mathbb{S} = \{\xi = (z, \eta) \mid z \in Z, \eta \in Inv(z)\}$ is the state space;
  - $\partial\mathbb{S} = \bigcup_{z \in Z}(\{z\} \times \partial Inv(z))$ the boundary of $\mathbb{S}$ $(z, x=2)$
- $\phi : Z \times \mathcal{V}(\mathcal{X}) \times \mathbb{R} \rightarrow \mathcal{V}(\mathcal{X})$ - *flow function*; η now, $\phi(z, \eta, t)$ in t time
- $\Lambda : \mathbb{S} \rightarrow \mathbb{R}_{\geq 0}$ - *exit rate function*;
- $\mu : \mathbb{S} \cup \partial\mathbb{S} \rightarrow Distr(\mathbb{S})$ - *transition probability function*;

Piecewise Deterministic Markov Processes [Davis84]

A Piecewise-Deterministic (Markov) Process is a tuple

$$\mathcal{Z} = (Z, \mathcal{X}, Inv, \phi, \Lambda, \mu)$$

- Z and $\mathcal{X}$ - finite sets of *locations* and *variables*;
- $Inv : Z \to \mathcal{B}_o(\mathcal{X})$ - *invariant function*; e.g., $x<2$
  - $\mathbb{S} = \{\xi = (z, \eta) \mid z \in Z, \eta \in Inv(z)\}$ is the state space;
  - $\partial\mathbb{S} = \bigcup_{z \in Z}(\{z\} \times \partial Inv(z))$ the boundary of $\mathbb{S}$ $(z, x{=}2)$
- $\phi : Z \times \mathcal{V}(\mathcal{X}) \times \mathbb{R} \to \mathcal{V}(\mathcal{X})$ - *flow function*; η now, $\phi(z, \eta, t)$ in t time
- $\Lambda : \mathbb{S} \to \mathbb{R}_{>0}$ - *exit rate function*;
- $\mu : \mathbb{S} \cup \partial\mathbb{S} \to Distr(\mathbb{S})$ - *transition probability function*;

Piecewise Deterministic Markov Processes [Davis84]

A Piecewise-Deterministic (Markov) Process is a tuple

$$\mathcal{Z} = (Z, \mathcal{X}, Inv, \phi, \Lambda, \mu)$$

- Z and $\mathcal{X}$ - finite sets of *locations* and *variables*;
- $Inv : Z \to \mathcal{B}_o(\mathcal{X})$ - *invariant function*; e.g., $x<2$
  - $\mathbb{S} \; = \; \{\xi = (z, \eta) \mid z \in Z, \eta \in Inv(z)\}$ is the state space;
  - $\partial\mathbb{S} \; = \; \bigcup_{z \in Z}(\{z\} \times \partial Inv(z))$ the boundary of $\mathbb{S}$ $(z, x{=}2)$
- $\phi : Z \times \mathcal{V}(\mathcal{X}) \times \mathbb{R} \to \mathcal{V}(\mathcal{X})$ - *flow function*; η now, $\phi(z, \eta, t)$ in t time
- $\Lambda : \mathbb{S} \to \mathbb{R}_{>0}$ - *exit rate function*;
- $\mu : \mathbb{S} \cup \partial\mathbb{S} \to Distr(\mathbb{S})$ - *transition probability function*;

Piecewise Deterministic Markov Processes [Davis84]

A Piecewise-Deterministic (Markov) Process is a tuple

$$\mathcal{Z} = (Z, \mathcal{X}, Inv, \phi, \Lambda, \mu)$$

- Z and $\mathcal{X}$ - finite sets of *locations* and *variables*;
- $Inv : Z \to \mathcal{B}_o(\mathcal{X})$ - *invariant function*; e.g., $x<2$
  - $\mathbb{S} \;=\; \{\xi = (z, \eta) \mid z \in Z, \eta \in Inv(z)\}$ is the state space;
  - $\partial\mathbb{S} \;=\; \bigcup_{z \in Z}(\{z\} \times \partial Inv(z))$ the boundary of $\mathbb{S}$ $\quad (z, x{=}2)$
- $\phi : Z \times \mathcal{V}(\mathcal{X}) \times \mathbb{R} \to \mathcal{V}(\mathcal{X})$ - *flow function*; η now, $\phi(z, \eta, t)$ in t time deterministic!
- $\Lambda : \mathbb{S} \to \mathbb{R}_{>0}$ - *exit rate function*;
- $\mu : \mathbb{S} \cup \partial\mathbb{S} \to Distr(\mathbb{S})$ - *transition probability function*;

Piecewise Deterministic Markov Processes [Davis84]

A Piecewise-Deterministic (Markov) Process is a tuple

$$\mathcal{Z} = (Z, \mathcal{X}, Inv, \phi, \Lambda, \mu)$$

- Z and $\mathcal{X}$ - finite sets of *locations* and *variables*;
- $Inv : Z \rightarrow \mathcal{B}_o(\mathcal{X})$ - *invariant function*; e.g., $x<2$
  - $\mathbb{S} \;=\; \{\xi = (z, \eta) \mid z \in Z, \eta \in Inv(z)\}$ is the state space;
  - $\partial\mathbb{S} \;=\; \bigcup_{z \in Z}(\{z\} \times \partial Inv(z))$ the boundary of $\mathbb{S}$ $(z, x{=}2)$
- $\phi : Z \times \mathcal{V}(\mathcal{X}) \times \mathbb{R} \rightarrow \mathcal{V}(\mathcal{X})$ - *flow function*; η now, $\phi(z, \eta, t)$ in t time deterministic!
- $\Lambda : \mathbb{S} \rightarrow \mathbb{R}_{\geqslant 0}$ - *exit rate function*;
- $\mu : \mathbb{S} \cup \partial\mathbb{S} \rightarrow Distr(\mathbb{S})$ - *transition probability function*;

Piecewise Deterministic Markov Processes [Davis84]

A Piecewise-Deterministic (Markov) Process is a tuple

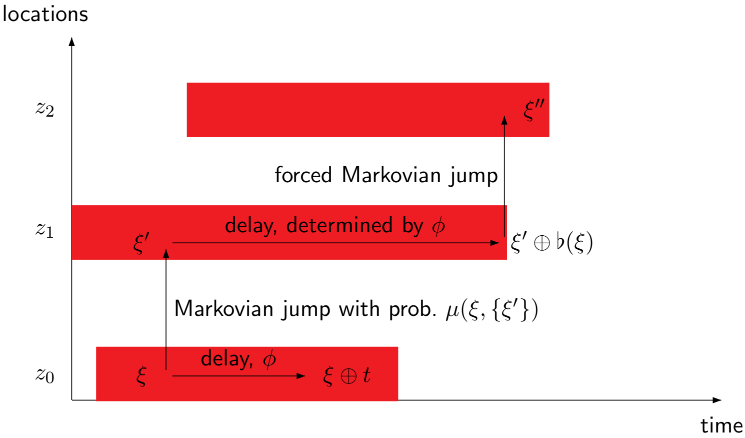
$$\mathcal{Z} = (Z, \mathcal{X}, Inv, \phi, \Lambda, \mu)$$

- Z and $\mathcal{X}$ - finite sets of *locations* and *variables*;
- $Inv : Z \to \mathcal{B}_o(\mathcal{X})$ - *invariant function*; e.g., $x<2$
  - $\mathbb{S} = \{\xi = (z, \eta) \mid z \in Z, \eta \in Inv(z)\}$ is the state space;
  - $\partial\mathbb{S} = \bigcup_{z \in Z}(\{z\} \times \partial Inv(z))$ the boundary of $\mathbb{S}$ $(z, x=2)$
- $\phi : Z \times \mathcal{V}(\mathcal{X}) \times \mathbb{R} \to \mathcal{V}(\mathcal{X})$ - *flow function*; η now, $\phi(z, \eta, t)$ in t time deterministic!
- $\Lambda : \mathbb{S} \to \mathbb{R}_{\geqslant 0}$ - *exit rate function*;
- $\mu : \mathbb{S} \cup \partial\mathbb{S} \to Distr(\mathbb{S})$ - *transition probability function*;

PDP semantics

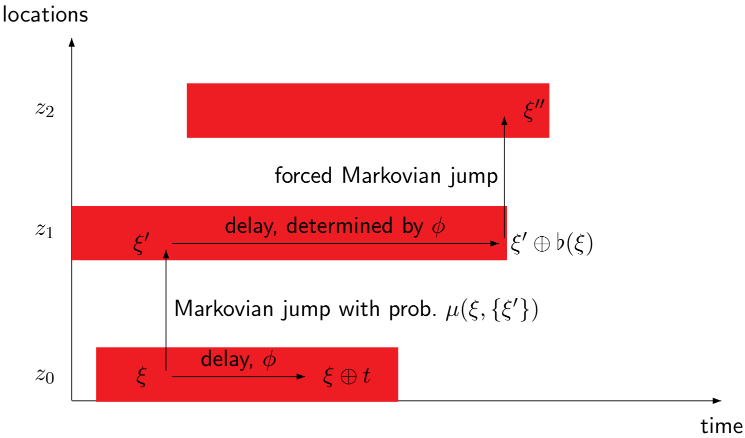
- A PDP may reside in state (z, η) as long as $\eta \models \mathit{Inv}(z)$ holds
- In state $\xi = (z, \eta)$ the PDP can delay or jump probabilistically
- Delay to $(z, \eta \oplus t) \in \mathbb{S} \cup \partial\mathbb{S}$ where
  - $\eta \oplus t$ updates the variable according to flow function ϕ
  - and the target variable valuation $\eta \oplus t \models \mathit{Inv}(z)$
- Markovian jump to state $\xi' \in \mathbb{S}$ with probability $\mu(\xi, \{\xi'\})$
- On hitting the “boundary” of $\mathit{Inv}(z)$ take a forced Markovian jump
  - from state ξ to $\xi' \in \mathbb{S}$ with probability $\mu(\xi, \{\xi'\})$

PDP semantics



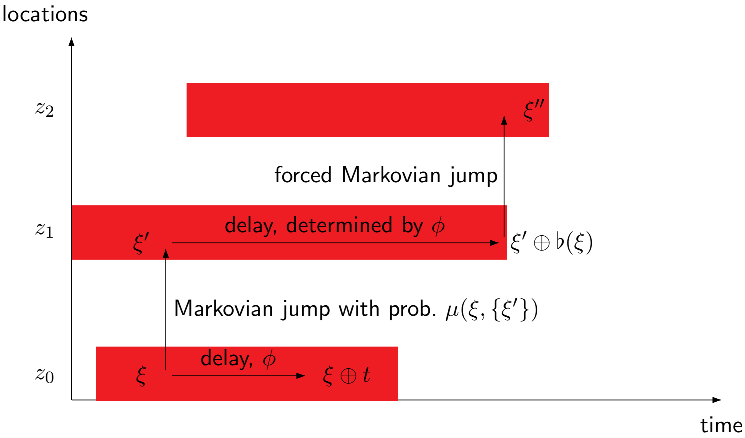
A PDP-state $\xi = (z, \eta)$ with $\eta \models Inv(z)$

PDP semantics



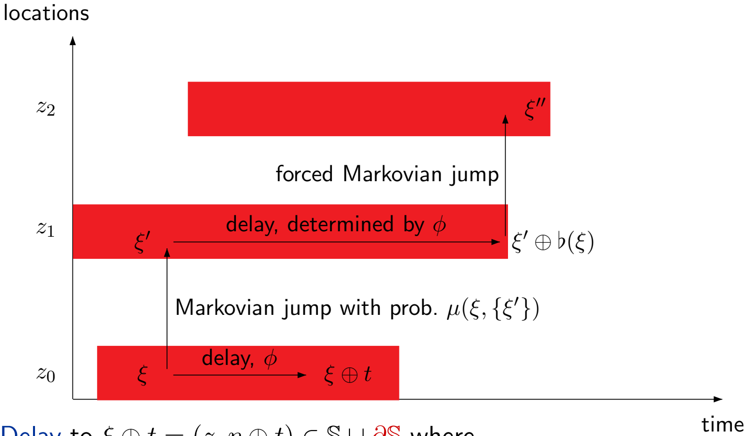
In state ξ, the PDP can delay or take a Markovian jump

PDP semantics



Markovian jump to state $\xi' \in \mathbb{S}$ with probability $\mu(\xi, \{\xi'\})$

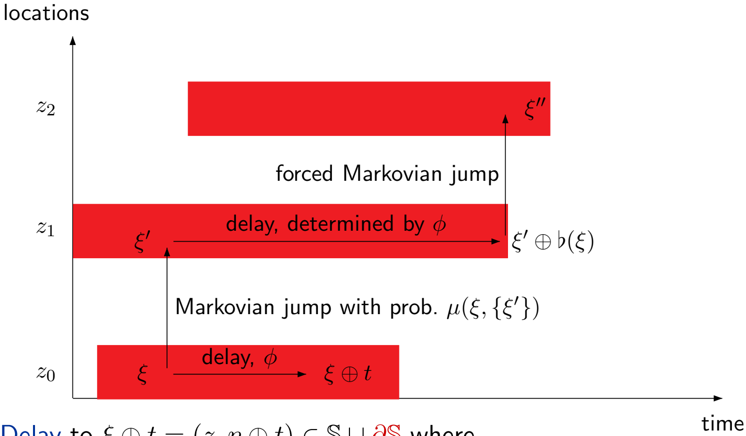
PDP semantics



Delay to $\xi \oplus t = (z, \eta \oplus t) \in \mathbb{S} \cup \partial\mathbb{S}$ where

- $\eta \oplus t$ updates the variable according to flow function ϕ
- if hitting the "boundary" of $Inv(z)$ take a forced Markovian jump

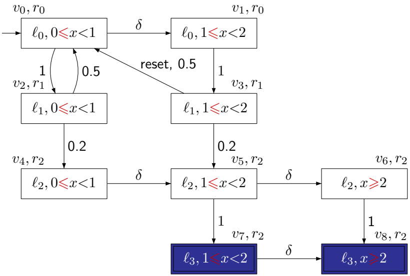
PDP semantics



Delay to $\xi \oplus t = (z, \eta \oplus t) \in \mathbb{S} \cup \partial\mathbb{S}$ where

- $\eta \oplus t$ updates the variable according to flow function ϕ
- if hitting the "boundary" of $Inv(z)$ take a forced Markovian jump

The region graph of $\mathcal{C} \otimes \mathcal{A}$ is indeed a PDP!



- Z - set of *locations*; the set of vertices
- $\mathcal{X}$ - set of *variables*; the set of clocks
- $Inv : Z \to \mathcal{B}_o(\mathcal{X})$ - *invariant function*; regions
- $\phi : Z \times \mathcal{V}(\mathcal{X}) \times \mathbb{R} \to \mathcal{V}(\mathcal{X})$ - *flow function*; simply $\dot{x} = 1$
- $\Lambda : \mathbb{S} \to \mathbb{R}_{\geqslant 0}$ - *exit rate function*; simply $\Lambda(v, t) = \Lambda(v)$
- $\mu : \mathbb{S} \cup \partial\mathbb{S} \to Distr(\mathbb{S})$ - *transition probability function*; the distribution in $\hookrightarrow$

Discrete transition probabilities [Costa & Davis'88]

The one -jump probability from state ξ to set $A \subseteq \mathbb{S}$ of states:

$$\hat{\mu}(\xi, A) = \int_0^{\flat(\xi)} \underbrace{(\mathcal{Q}\mathbf{1}_A)(\xi \oplus t)}_{\text{trans. prob. } \xi \oplus t \to A} \cdot \underbrace{\Lambda(\xi \oplus t) \cdot e^{-\int_0^t \Lambda(\xi \oplus \tau)\, d\tau}\, dt}_{\text{density at time } t}$$

$$+ \underbrace{(\mathcal{Q}\mathbf{1}_A)(\xi \oplus \flat(\xi)) \cdot e^{-\int_0^{\flat(\xi)} \Lambda(\xi \oplus \tau)\, d\tau}}_{\text{probability to take forced transition}}$$

where $\flat(\xi) = \inf\{ t > 0 \mid \xi \oplus t \in \partial\mathbb{S} \}$ is the minimal time to hit the boundary

These are the transition probabilities of the embedded DTMP *emb*$(\mathcal{Z})$

Main results

Recall that:

$$\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right) \;=\; \Pr_{\vec{0}}^{\mathcal{C}\otimes\mathcal{A}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond Loc_F)\right)$$

We now have in addition that:

$$\Pr_{\vec{0}}^{\mathcal{C}\otimes\mathcal{A}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond Loc_F)\right) \;=\; \Pr^{emb(\mathcal{Z})}\left((v_0,\vec{0}),(V_F,\cdot)\right)$$

Thus:

$$\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right) \;=\; \Pr^{emb(\mathcal{Z})}\left((v_0,\vec{0}),(V_F,\cdot)\right)$$

The probability that CTMC $\mathcal{C}$ satisfies DTA $\mathcal{A}$ reduces to computing simple reachability probabilities in a PDP

Main results

Recall that:

$$\boxed{\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right) \;=\; \Pr^{\mathcal{C}\otimes\mathcal{A}}_{\vec{0}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond Loc_F)\right)}$$

We now have in addition that:

$$\boxed{\Pr^{\mathcal{C}\otimes\mathcal{A}}_{\vec{0}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond Loc_F)\right) \;=\; \Pr^{\mathit{emb}(\mathcal{Z})}\left((v_0,\vec{0}),(V_F,\cdot)\right)}$$

Thus:

$$\boxed{\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right) \;=\; \Pr^{\mathit{emb}(\mathcal{Z})}\left((v_0,\vec{0}),(V_F,\cdot)\right)}$$

The probability that CTMC $\mathcal{C}$ satisfies DTA $\mathcal{A}$ reduces to computing simple reachability probabilities in a PDP

Main results

Recall that:

$$\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right) = \Pr_{\vec{0}}^{\mathcal{C}\otimes\mathcal{A}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond Loc_F)\right)$$

We now have in addition that:

$$\Pr_{\vec{0}}^{\mathcal{C}\otimes\mathcal{A}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond Loc_F)\right) = \Pr^{\textsf{emb}(\mathcal{Z})}\left((v_0,\vec{0}),(V_F,\cdot)\right)$$

Thus:

$$\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right) = \Pr^{\textsf{emb}(\mathcal{Z})}\left((v_0,\vec{0}),(V_F,\cdot)\right)$$

The probability that CTMC $\mathcal{C}$ satisfies DTA $\mathcal{A}$ reduces to computing simple reachability probabilities in a PDP

Main results

Recall that:

$$\boxed{\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right) \;=\; \Pr_{\vec{0}}^{\mathcal{C}\otimes\mathcal{A}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond Loc_F)\right)}$$

We now have in addition that:

$$\boxed{\Pr_{\vec{0}}^{\mathcal{C}\otimes\mathcal{A}}\left(Paths^{\mathcal{C}\otimes\mathcal{A}}(\Diamond Loc_F)\right) \;=\; \Pr^{\mathit{emb}(\mathcal{Z})}\left((v_0, \vec{0}), (V_F, \cdot)\right)}$$

Thus:

$$\boxed{\Pr^{\mathcal{C}}\left(Paths^{\mathcal{C}}(\mathcal{A})\right) \;=\; \Pr^{\mathit{emb}(\mathcal{Z})}\left((v_0, \vec{0}), (V_F, \cdot)\right)}$$

The probability that CTMC $\mathcal{C}$ satisfies DTA $\mathcal{A}$ reduces to computing simple reachability probabilities in a PDP

Characterizing reachability probabilities

Reachability probabilities of untimed events in a $\mathrm{PDP}\ \mathcal{Z}$ can be characterised in the embedded DTMP *emb*$(\mathcal{Z})$ as follows:

- for the delay transition $v \overset{\delta}{\hookrightarrow} v'$,

$$Prob^{\mathcal{D}}_{v,\delta}(\eta) = e^{-\Lambda(v)\flat(v,\eta)} \cdot Prob^{\mathcal{D}}_{v'}\big(\eta + \flat(v,\eta)\big)$$

- for the Markovian transition $v \overset{p,X}{\hookrightarrow} v'$,

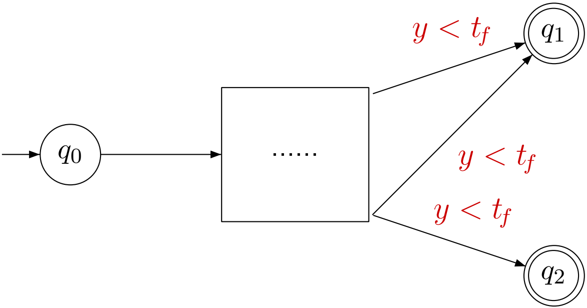
$$Prob^{\mathcal{D}}_{v,v'}(\eta) = \int_0^{\flat(v,\eta)} p{\cdot}\Lambda(v){\cdot}e^{-\Lambda(v)\tau}{\cdot}Prob^{\mathcal{D}}_{v'}\big((\eta+\tau)[X := 0]\big)\ d\tau$$

- for each vertex $v \in V$, we obtain:

$$Prob^{\mathcal{D}}_{v}(\eta) = \begin{cases} Prob^{\mathcal{D}}_{v,\delta}(\eta) + \sum_{v \overset{p,X}{\hookrightarrow} v'} Prob^{\mathcal{D}}_{v,v'}(\eta), & \text{if } v \notin V_F \\ 1, & \text{otherwise} \end{cases}$$

Approximating reachability probabilities

Augment the DTA $\mathcal{A}$ with a new clock y and with guard $y < t_f$, and get $\mathcal{A}[t_f]$:



$$Paths^{\mathcal{C}}(\mathcal{A}[t_f]) \subseteq Paths^{\mathcal{C}}(\mathcal{A})$$

$$\lim_{t_f \to \infty} \Pr^{\mathcal{C}}\big(Paths^{\mathcal{C}}(\mathcal{A}[t_f])\big) = \Pr^{\mathcal{C}}\big(Paths^{\mathcal{C}}(\mathcal{A})\big)$$

PDEs as reachability probabilities

Approximate $\Pr^{\mathcal{C}}\big(Paths^{\mathcal{C}}(\mathcal{A})\big)$ by solving the following system of PDEs:

- For $v \in V \setminus V_F$:

$$\frac{\partial \hbar_v(y,\eta)}{\partial y} + \sum_{i=1}^{|\mathcal{X}|} \frac{\partial \hbar_v(y,\eta)}{\partial \eta^{(i)}} + \Lambda(v)\cdot \sum_{v \overset{p,X}{\hookrightarrow} v'} p\cdot(\hbar_{v'}(y,\eta[X:=0]) - \hbar_v(y,\eta)) = 0$$

- For $v \in V_F$:

$$\frac{\partial \hbar_v(y,\eta)}{\partial y} + \sum_{i=1}^{|\mathcal{X}|} \frac{\partial \hbar_v(y,\eta)}{\partial \eta^{(i)}} + 1 = 0$$

$\hbar_v(y,\eta)$ is the probability to reach $(V_F,\cdot)$ starting from (v,η,y) with $y \leq t_f$

Generalization for ω-regular properties

model	automaton	product	property
LTS TS	Nondet. Büchi $\mathcal{A}$	LTS $TS \otimes \mathcal{A}$	$\Box \Diamond acc$
DTMC $\mathcal{D}$	Deter. Rabin $\mathcal{A}$	DTMC $\mathcal{D} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC$_{acc}$)
MDP $\mathcal{M}$	Deter. Rabin $\mathcal{A}$	MDP $\mathcal{M} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC$_{acc}$)
CTMC $\mathcal{C}$	Deter. Rabin $\mathcal{A}$	CTMC $\mathcal{C} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC$_{acc}$)
CTMC $\mathcal{C}$	DTA $\mathcal{A}$	DMTA $\mathcal{C} \otimes \mathcal{A}$	Prob($\Diamond\, acc$) in a PDP
CTMC $\mathcal{C}$	DTA$^{\omega}$ $\mathcal{A}$	DMTA$^{\omega}$ $\mathcal{C} \otimes \mathcal{A}^{\omega}$	Prob($\Diamond$ BSCC$_{acc}$) in a PDP

Generalization for ω-regular properties

model	automaton	product	property
LTS TS	Nondet. Büchi $\mathcal{A}$	LTS $TS \otimes \mathcal{A}$	$\Box \Diamond acc$
DTMC $\mathcal{D}$	Deter. Rabin $\mathcal{A}$	DTMC $\mathcal{D} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC$_{acc}$)
MDP $\mathcal{M}$	Deter. Rabin $\mathcal{A}$	MDP $\mathcal{M} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC$_{acc}$)
CTMC $\mathcal{C}$	Deter. Rabin $\mathcal{A}$	CTMC $\mathcal{C} \otimes \mathcal{A}$	Prob($\Diamond$ BSCC$_{acc}$)
CTMC $\mathcal{C}$	DTA $\mathcal{A}$	DMTA $\mathcal{C} \otimes \mathcal{A}$	Prob($\Diamond\, acc$) in a PDP
CTMC $\mathcal{C}$	DTA$^{\omega}$ $\mathcal{A}$	DMTA$^{\omega}$ $\mathcal{C} \otimes \mathcal{A}^{\omega}$	Prob($\Diamond$ BSCC$_{acc}$) in a PDP

Related work

- PTCTL model checking of PTA (Kwiatkowska *et el.* TCS 2002)
- CSL with regular expressions (Baier *et al.* IEEE TSE 2007)
- CSL with single-clock DTA as time constraints (Donatelli *et al.* IEEE TSE 2009)
  - our results coincide with Donatelli's for single-clock DTA
  - ... but we obtain the results in a different manner
- Probabilistic semantics of TA (Baier *et al.* LICS 2008)
- Quantitative model checking of such TA (Bertrand *et al.* QEST 2008)
- Optimal stopping times in PDPs (Costa & Davis MCSS 1988)

Epilogue

- Problem: verifying a CTMC $\mathcal{C}$ against a deterministic TA $\mathcal{A}$

- Main result:

  The probability that $\mathcal{C}$ satisfies $\mathcal{A}$ coincides with a simple reachability probability in a PDP

- Approximate solutions are obtained by solving a system of PDEs

- For single clock DTA this reduces to a system of linear equations
  - whose coefficients are obtained by solving a system of ODEs

- Results generalize to DTA with ω-regular acceptance conditions