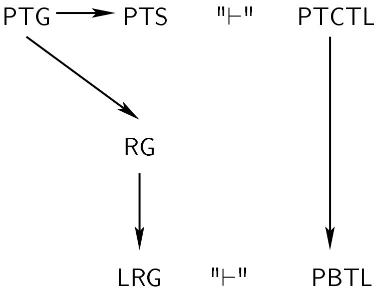
Automatic Verification of Real-time Systems with Discrete Probability Distributions

Talk by Robert Jørgensgaard Olesen

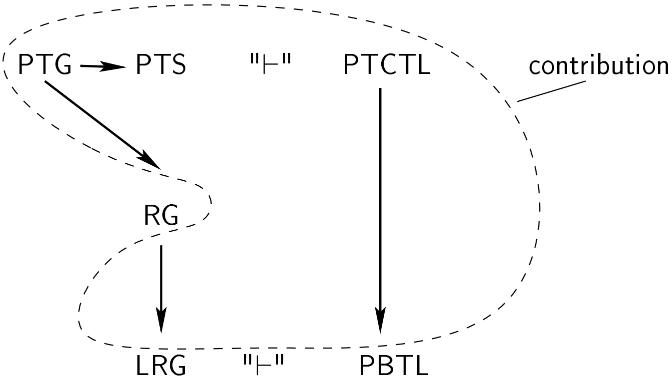
Marta Kwiatkowska Gethin Norman Roberto Segala
Jeremy Sproston

Oktober 2, 2007

The overall idea



PTCTL can be model-checked on PTGs



Agenda

1. Probabilistic Timed Graphs (PTG)
   - Definition
   - Example
   - Semantics
2. Computation Tree Logic
   - Probabilistic Timed Computation Tree Logic (PTCTL)
   - Probabilistic Branching Time Logic (PBTL)
3. Regions
   - Example
   - Region Graph
   - Labelled Region Graph
   - PBTL derived from PTCTL
4. Contribution
   - PTCTL can be model-checked on PTGs

1. Probabilistic Timed Graphs (PTG)
   - Definition
   - Example
   - Semantics
2. Computation Tree Logic
   - Probabilistic Timed Computation Tree Logic (PTCTL)
   - Probabilistic Branching Time Logic (PBTL)
3. Regions
   - Example
   - Region Graph
   - Labelled Region Graph
   - PBTL derived from PTCTL
4. Contribution
   - PTCTL can be model-checked on PTGs

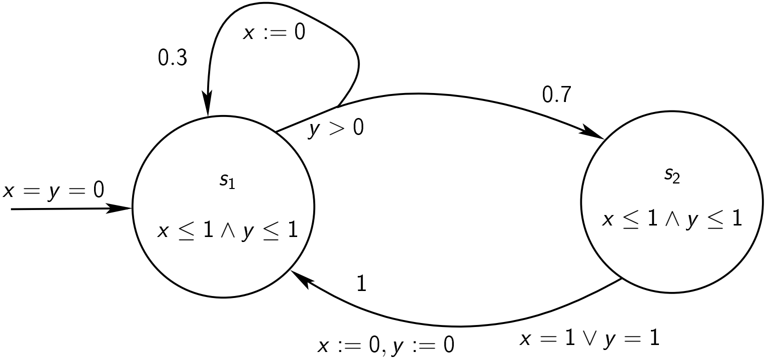
Probabilistic Timed Graphs

Definition

A *probabilistic timed graph* is a tuple
$G = (\mathcal{S}, L, s_{\text{init}}, \mathcal{X}, \text{inv}, \text{prob}, \langle \tau_s \rangle_{s \in S})$, where

- $\mathcal{S}$ is a finite set of nodes,
- $L : \mathcal{S} \rightarrow 2^{AP}$ are the atomic propositions being true in each s,
- s_{init} is the start node,
- $\mathcal{X}$ is a finite set of clocks,
- $\text{inv} : \mathcal{S} \rightarrow AF_{\mathcal{X}}$ are the invariant of each s
- $\text{prob} : \mathcal{S} \rightarrow \mathcal{P}(\mu(\mathcal{S} \times 2^{\mathcal{X}}))$ are the probabilistic transitions for each s, and
- $\tau_s : prob(s) \rightarrow AF_{\mathcal{X}}$ is a guard to each $p \in \text{prob}(s)$, for each s.

Probabilistic Timed Graph Example



Semantics

- The semantics of probabilistic timed graphs are defined in terms of probabilistic timed structures.
- The logic PTCTL is a logic for such structures

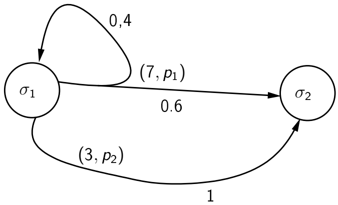
Probabilistic Timed Structure

Definition

A *probabilistic timed structure* $\mathcal{M}$ is a triple (Σ, Tr, End) where

- Σ is a set of states.
- Tr is a function on Σ that returns a set of pairs (t, p) where t is a delay and p is a discrete probability distribution on Σ.
- End is a set of states where time is allowed to increase without bound.

$$Tr(\sigma_1) = \{(7, p_1), (3, p_2)\}$$



Semantics of PTG in terms of PTS

Definition

Let $G = (\mathcal{S}, L, s_{\text{init}}, \mathcal{X}, \text{inv}, \text{prob}, \langle \tau_s \rangle_{s \in S})$ be a probabilistic timed graph.

- A *state of G* is a tuple $\langle s, v \rangle$, where $s \in \mathcal{S}$ and $v \in \Gamma(\mathcal{X})$ s.t. v satisfies $inv(s)$.
- The *probabilistic timed structure of G* is defined as $\mathcal{M}^G = (\Sigma^G, Tr^G, End^G)$ where
  - Σ^G is the set of states of G.
  - $(t, p) \in Tr(\langle s, v \rangle)$ exactly when $\exists p_s \in \texttt{prob}(s)$ s.t.:
    - $v + t$ satisfies $\texttt{inv}(s)$.
    - $v + t'$ satisfies $\tau_s(p_s)$ for all $0 \leq t' \leq t$.
    - $p(\langle s', v' \rangle) = \sum_{C \subseteq \mathcal{X} \wedge (v+t)[C \mapsto 0] = v'} p_s(s', C)$ for all $\langle s', v' \rangle$.
  - $End^G = \{\langle s, v \rangle \mid \forall t \geq 0 \text{ we have } v + t \text{ satisfies } \texttt{inv}(s)\}$.

Recall (slide is skipped at first)

Definition

A *probabilistic timed graph* is a tuple
$G = (\mathcal{S}, L, s_{\text{init}}, \mathcal{X}, \text{inv}, \text{prob}, \langle \tau_s \rangle_{s \in S})$, where

- $\mathcal{S}$ is a finite set of nodes,
- $L : \mathcal{S} \to 2^{AP}$ are the atomic propositions being true in each s,
- s_{init} is the start node,
- $\mathcal{X}$ is a finite set of clocks,
- $\text{inv} : \mathcal{S} \to AF_{\mathcal{X}}$ are the invariant of each s
- $\text{prob} : \mathcal{S} \to \mathcal{P}(\mu(\mathcal{S} \times 2^{\mathcal{X}}))$ are the probabilistic transitions for each s, and
- $\tau_s : prob(s) \to AF_{\mathcal{X}}$ is a guard to each $p \in \text{prob}(s)$, for each s.

Probabilistic Timed Computation Tree Logic

Definition

Let $\mathcal{C}$ be a set of clocks. A set of atomic formulae $AF_{\mathcal{C}}$ is defined inductively by the syntax:

$$\varphi ::= c \leq k \mid k \leq c \mid \neg\varphi \mid \varphi \vee \varphi$$

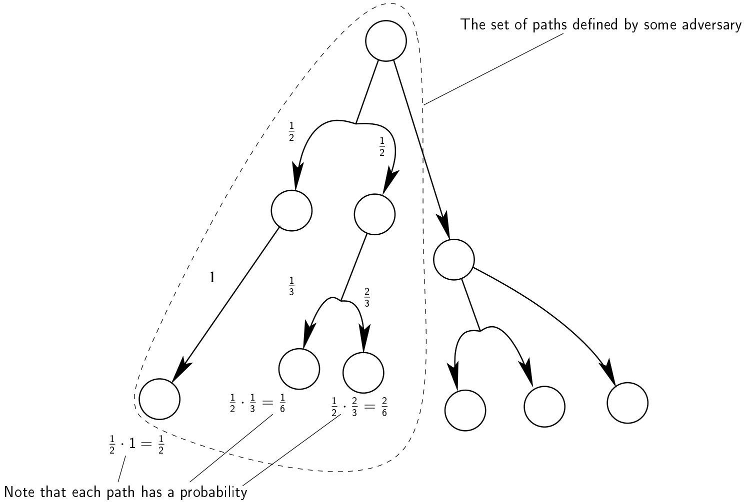
Definition

The syntax of PTCTL is defined as follows:

$$\phi ::= \texttt{true} \mid a \mid \varphi \mid \phi \wedge \phi \mid \neg\phi \mid z.\phi \mid [\phi \exists \mathcal{U} \phi]_{\sqsupseteq \lambda} \mid [\phi \forall \mathcal{U} \phi]_{\sqsupseteq \lambda} \,,$$

where $a \in AP$, $\varphi \in AF_{\mathcal{X} \cup \mathcal{Z}}$, $z \in \mathcal{Z}$, $\lambda \in [0,1]$, and $\sqsupseteq \in \{\geq, >\}$.

Example Adversary



Probabilistic Branching Time Logic

Definition

The syntax of PBTL is defined as follows:

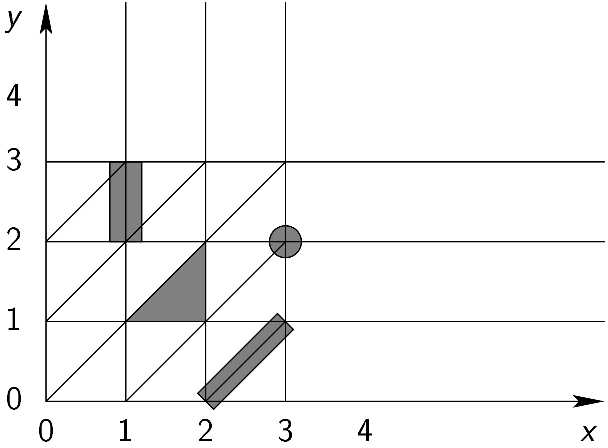
$$\Phi ::= \texttt{true} \mid a | \Phi \wedge \Phi \mid \neg \Phi \mid z.\Phi \mid [\Phi \exists \mathcal{U} \Phi]_{\sqsupseteq \lambda} \mid [\Phi \forall \mathcal{U} \Phi]_{\sqsupseteq \lambda},$$

where $a \in AP^*$, $z \in \mathcal{Z}$, $\lambda \in [0,1]$, and $\sqsupseteq \in \{\geq, >\}$.

$AP^* = AF_\phi \cup AP$ where AF_ϕ is the set of atomic formulae in ϕ.

1. Probabilistic Timed Graphs (PTG)
   - Definition
   - Example
   - Semantics
2. Computation Tree Logic
   - Probabilistic Timed Computation Tree Logic (PTCTL)
   - Probabilistic Branching Time Logic (PBTL)
3. Regions
   - Example
   - Region Graph
   - Labelled Region Graph
   - PBTL derived from PTCTL
4. Contribution
   - PTCTL can be model-checked on PTGs

Example of Regions



Region Graph

Definition (simplified)

Let G be a probabilistic timed graph and ϕ a PTCTL formula. The *region graph* $R(G, \phi)$ is a triple $(V^*, Steps^*, End^*)$ where

- V^* is the set of augmented regions on the form $\langle s, [v, \mathcal{E}]\rangle$.
- $Steps^* : V^* \rightarrow \mathcal{P}(\mu(V^*))$ is a set of probabilistic transitions where time may pass with probability 1, and the state may change with probability

$$p_{\mathrm{succ}}^{s,\alpha}(\langle s', \beta\rangle) = \sum_{\substack{C \subseteq \mathcal{X} \wedge \\ [C \mapsto 0]\alpha = \beta}} p_s(s', C)$$

- $End^* \subseteq V^*$ is the set of end regions.

Labelled Region Graph

Recall that $G = (\mathcal{S}, L, s_{\text{init}}, \mathcal{X}, \text{inv}, \text{prob}, \langle\tau_s\rangle_{s\in S})$ where especially $L : \mathcal{S} \rightarrow 2^{AP}$ are the atomic propositions being true in each s,

Definition

For a region graph $R(G, \phi)$ we define its *associated labelled region graph* by $(R(G, \phi), L^*)$, where $L^* : V^* \rightarrow 2^{AP^*}$ is defined as

$$L^*(\langle s, [v, \mathcal{E}]\rangle) = \{a \in L(s)\} \cap \{a_\varphi \mid [v, \mathcal{E}] \text{ satisfies } \varphi, \varphi \in AF_\phi\}$$

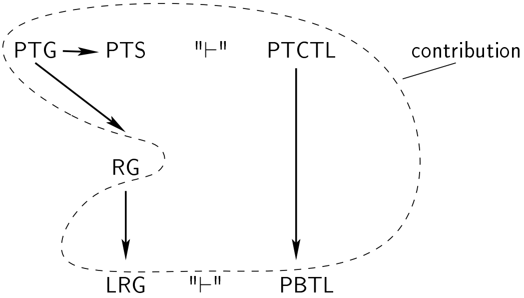
PBTL derived from PTCTL

PTCTL Subformula of ϕ	PBTL Subformula of Φ
`true`	`true`
a	a
φ	a_φ
$\phi_1 \vee \phi_2$	$\Phi_1 \vee \Phi_2$
$\neg\phi$	$\neg\Phi$
$[\phi_1 \exists\mathcal{U} \phi_2]_{\sqsupseteq\lambda}$	$[\Phi_1 \exists\mathcal{U} \Phi_2]_{\sqsupseteq\lambda}$
$[\phi_1 \forall\mathcal{U} \phi_2]_{\sqsupseteq\lambda}$	$[\Phi_1 \forall\mathcal{U} \Phi_2]_{\sqsupseteq\lambda}$

Recall

$$L^*(\langle s, [v, \mathcal{E}]\rangle) = \{a \in L(s)\} \cup \{a_\varphi \mid [v, \mathcal{E}] \text{ satisfies } \varphi, \varphi \in AF_\phi\}$$

PTCTL can be model-checked on PTGs



. . .

. . . THE END