A Logic for Reasoning about Time and Reliability

Presentation by Arild Haugstad

Hans Hansson Bengt Jonsson

October 2, 2007

Overview

- PCTL: Probabilistic real time Computation Tree Logic
- Extends CTL
- Discrete time Markov chains

Structure

Assume A a finite set of atomic propositions.

Definition (Structure)

A *structure* is a tuple $\langle S, s^i, \mathcal{T}, L \rangle$ where

- S is a finite set of states,
- $s^i \in S$ is an *initial state*,
- $\mathcal{T}$ as a *transition probability function*, $\mathcal{T} : S \times S \to [0, 1]$ such that for all $s \in S$ we have $\sum_{s' \in S} \mathcal{T}(s, s') = 1$,
- L is a labeling function assigning atomic propositions to states, $L : S \to 2^A$.

Structure

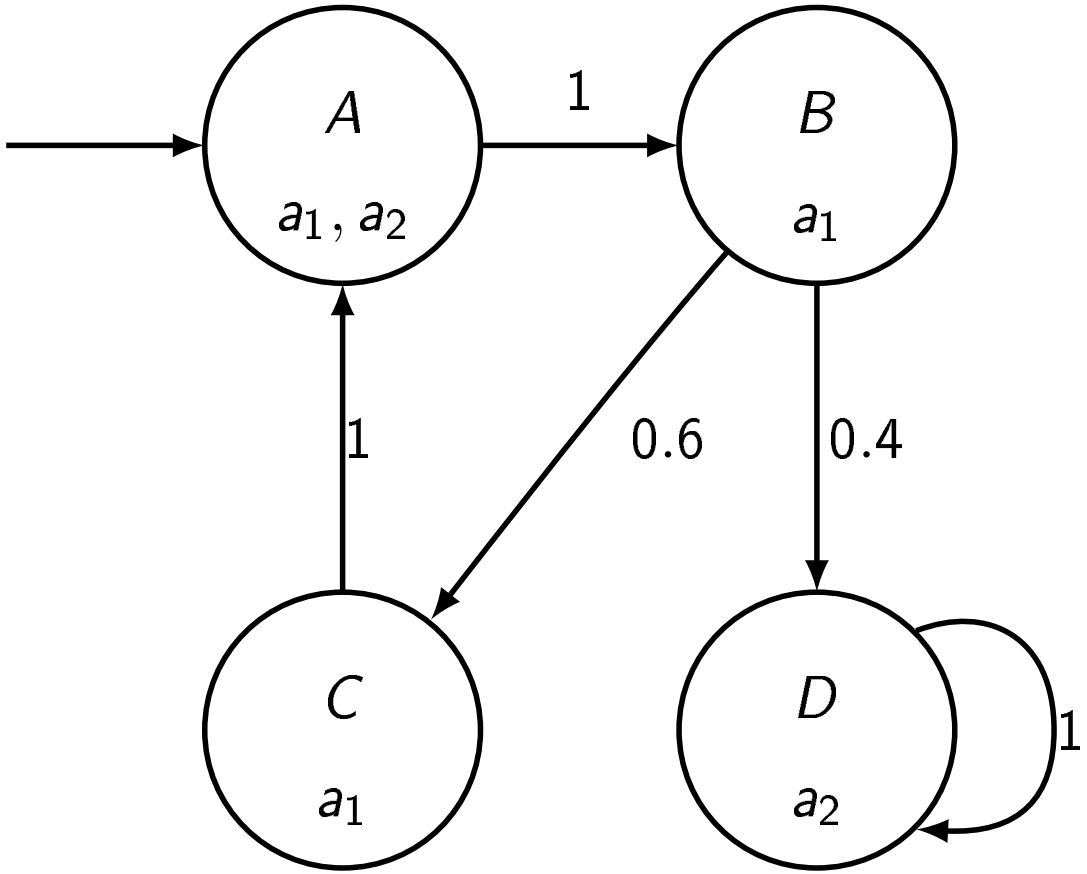

Figure: Sample Structure

PCTL Syntax

The set of PCTL formulas is divided into *path formulas* and *state formulas*:

Definition (PCTL Syntax)

- Each atomic proposition is a state formula,
- If f_1 and f_2 are state formulas, then so are $\neg f_1, (f_1 \wedge f_2), (f_1 \vee f_2), (f_1 \rightarrow f_2)$,
- If f_1 and f_2 are state formulas, and t is a nonnegative integer or ∞, then $(f_1 \, U^{\leq t} \, f_2)$ and $(f_1 \, \mathcal{U}^{\leq t} \, f_2)$ are path formulas,
- If f is a path formula and p is a real number with $0 \leq p \leq 1$, then $[f]_{\geq p}$ and $[f]_{>p}$ are state formulas.

Informal Semantics of PCTL

- A state s satisfies an atomic proposition a if $a \in L(s)$,
- $\neg, \wedge, \vee, \rightarrow$ as expected,
- U is strong until,
- $\mathcal{U}$ is weak until,
- $[f]_{\geq p}$ and $[f]_{>p}$ holds for a state s if the sum of probabilities of paths from s satisfying f is $\geq p$ or $> p$ respectively.

$f_1 \, U^{\leq t}_{\geq p} \, f_2$ and $f_1 \, \mathcal{U}^{\leq t}_{\geq p} \, f_2$ are shorthands for $[f_1 \, U^{\leq t} \, f_2]_{\geq p}$ and $[f_1 \, \mathcal{U}^{\leq t} \, f_2]_{\geq p}$

Some Interesting Properties Expressed in PCTL

- $A\,f \equiv [f]_{\geq 1}$
- $E\,f \equiv [f]_{>0}$
- $G^{\leq t}_{\geq p} f \equiv f\,\mathcal{U}^{\leq t}_{\geq p}\,\mathsf{false}$
- $F^{\leq t}_{\geq p} f \equiv \mathsf{true}\,U^{\leq t}_{\geq p}\,f$
- $AG\,f \equiv f\,\mathcal{U}^{\leq \infty}_{\geq 1}\,\mathsf{false}$
- $AF\,f \equiv \mathsf{true}\,U^{\leq \infty}_{\geq 1}\,f$
- $EG\,f \equiv f\,\mathcal{U}^{\leq \infty}_{>0}\,\mathsf{false}$
- $EF\,f \equiv \mathsf{true}\,U^{\leq \infty}_{>0}\,f$
- $f_1 \overset{\leq t}{\underset{\geq p}{\rightsquigarrow}} f_2 \equiv AG\,[(f_1 \rightarrow F^{\leq t}_{\geq p} f_2)]$

Model Checking: Overall idea

Given structure K and PCTL formula f, to determine whether $\models_K f$:

1. Consider subformulas of f
2. Label each state with true subformulas
3. If s^i is labeled with f, then $\models_K f$

Checking Subformulas

- Atomic from structure
- $\neg$, $\wedge$, $\vee$, $\rightarrow$ from shorter labels
- Modal subformulas?

$t \neq \infty$, checking $f_1 U^{\leq t}_{\geq p} f_2$

For $t < 0$, define $\mathcal{P}(t, s) = 0$, for $t \geq 0$ define

$$\mathcal{P}(t, s) = \text{if } f_2 \in \text{labels}(s) \text{ then } 1$$
$$\text{else if } f_1 \notin \text{labels}(s) \text{ then } 0$$
$$\text{else } \sum_{s' \in S} \mathcal{T}(s, s') \cdot \mathcal{P}(t-1, s')$$

Algorithm for computing $\mathcal{P}$

Algorithm 1: Compute $\mathcal{P}(t, s)$, $\mathcal{O}(t \cdot |S|^2)$

```
1 for i := 0 to t do
2     forall s ∈ S do
3         if f2 ∈ labels(s) then
4             P(i, s) := 1
5         else
6             P(i, s) := 0
7             if f1 ∈ labels(s) then
8                 forall s' ∈ S do
9                     P(i, s) := P(i, s) + T(s, s') · P(i − 1, s')
```

Let $s_1, \ldots, s_N$ be the states in S. Partition S into S_s, S_f, S_i:

S_s : *Success states*; $f_2 \in \text{label}(s)$

S_f : *Failure states*; $f_1, f_2 \notin \text{label}(s)$

S_i : *Inconclusive states*; $f_1 \in \text{label}(s), f_2 \notin \text{label}(s)$

Define the $N \times N$ matrix M by

$$M[s_k, s_l] = \begin{cases} \mathcal{T}(s_k, s_l) & \text{if } s_k \in S_i \\ 1 & \text{if } s_k \notin S_i \wedge k = l \\ 0 & \text{otherwise} \end{cases}$$

Let $\overline{\mathcal{P}}(t)$ be a column vector of size N whose ith element is $\overline{\mathcal{P}}(t)[s_i]$. Let $\overline{\mathcal{P}}(0)[s_i]$ for $s_i \in S_s$ and 0 otherwise. With $\overline{\mathcal{P}}(t) = M^t \cdot \overline{\mathcal{P}}(0)$, we have $\mathcal{P}(s, t) = \overline{\mathcal{P}}(t)[s_i]$.

Algorithm 2: Compute $\overline{\mathcal{P}}(t)$, $\mathcal{O}(\log t \cdot |S|^3)$

```
1 forall s ∈ S do
2     if f_2 ∈ labels(s) then
3         P̄(0)[s] := 1
4     else
5         P̄(0)[s] := 0
6 P̄(t) = M^t · P̄(0)
```

Tricks for Special Cases

- $f_1 U_{>0}^{\leq t} f_2$: Expand t times; some transition to "goal set"
- $f_1 U_{>0}^{\leq \infty} f_2$: True iff $f_1 U_{>0}^{\leq |S_i|} f_2$
- $f_1 U_{\geq p}^{\leq \infty} f_2$: define success and failure states, $\mathcal{P}(\infty, s)$, Gaussian elimination
- $f_1 U_{\geq 1}^{\leq t} f_2$: Expand t times; all transitions to "goal set"
- $f_1 U_{\geq 1}^{\leq \infty} f_2$: True iff $f_1 U_{\geq 1}^{\leq |S_i|} f_2$

Contributions

- PCTL introduced
- Algorithms for checking PCTL introduced and analysed