CS 512, Spring 2018, Handout 21

Probabilistic Computation-Tree Logic (PCTL)

Assaf Kfoury

April 12, 2018

Minimal presentation of PCTL

- **Syntax of PCTL:**

$$\varphi \;::=\; \texttt{true} \mid \texttt{false} \mid p \mid \neg\varphi \mid \varphi \wedge \varphi' \mid \mathbb{P}_J(\Psi) \qquad \text{(\textit{state} formulas)}$$

$$\Psi \;::=\; \varphi \,\mathbb{U}\, \varphi' \mid \varphi \,\mathbb{U}^{\leqslant n}\, \varphi' \qquad \text{(\textit{path} formulas)}$$

where p ranges over a finite set AP of atomic propositions,
n ranges over $\mathbb{N}$, and
J ranges over intervals with rational bounds between 0 and 1, *i.e.*,

$$J = [q_1, q_2] \quad \text{or} \quad J =]q_1, q_2] \quad \text{or} \quad J = [q_1, q_2[\quad \text{or} \quad J =]q_1, q_2[$$

for some $0 \leqslant q_1 \leqslant q_2 \leqslant 1$.

Minimal presentation of PCTL

- **Syntax of PCTL:**

$$\varphi ::= \mathtt{true} \mid \mathtt{false} \mid p \mid \neg\varphi \mid \varphi \wedge \varphi' \mid \mathbb{P}_J(\Psi) \qquad \text{(\textit{state} formulas)}$$

$$\Psi ::= \varphi \ \mathbb{U} \ \varphi' \mid \varphi \ \mathbb{U}^{\leqslant n} \ \varphi' \qquad \text{(\textit{path} formulas)}$$

where p ranges over a finite set AP of atomic propositions,
n ranges over $\mathbb{N}$, and
J ranges over intervals with rational bounds between 0 and 1, *i.e.*,

$$J = [q_1, q_2] \quad \text{or} \quad J =]q_1, q_2] \quad \text{or} \quad J = [q_1, q_2[\quad \text{or} \quad J =]q_1, q_2[$$

for some $0 \leqslant q_1 \leqslant q_2 \leqslant 1$.

Remark: We use only *until* "$\mathbb{U}$" and *bounded until* "$\mathbb{U}^{\leqslant n}$" as temporal connectives in this version of PCTL.

- Informal meaning of $(\varphi_1 \ \mathbb{U}^{\leqslant n} \ \varphi_2)$:

"φ_2 will hold within at most n steps while

φ_1 holds in all the states that are visited before a φ_2-state is reached"

Minimal presentation of PCTL

- **Syntax of PCTL – some shorthands:**

  If $J = [q_1, q_2]$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 \leqslant p \leqslant q_2}(\Psi)$, which asserts that path formula Ψ holds with a probability p between q_1 and q_2.

  If $J =]q_1, q_2]$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 < p \leqslant q_2}(\Psi)$.

  If $J = [q_1, q_2[$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 \leqslant p < q_2}(\Psi)$.

  If $J =]q_1, q_2[$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 < p < q_2}(\Psi)$.

Minimal presentation of PCTL

- **Syntax of PCTL – some shorthands:**

  If $J = [q_1, q_2]$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 \leqslant p \leqslant q_2}(\Psi)$, which asserts that path formula Ψ holds with a probability p between q_1 and q_2.

  If $J =]q_1, q_2]$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 < p \leqslant q_2}(\Psi)$.

  If $J = [q_1, q_2[$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 \leqslant p < q_2}(\Psi)$.

  If $J =]q_1, q_2[$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 < p < q_2}(\Psi)$.

- If $J = [q_1, q_2]$ and $q_1 = 0$, we can read $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{\leqslant q_2}(\Psi)$.

  If $J = [q_1, q_2]$ and $q_2 = 1$, we can read $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{\geqslant q_1}(\Psi)$.

  If $J = [q_1, q_2]$ and $q_1 = q_2 = q$, we can read $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{=q}(\Psi)$.

- And similarly, if $J =]q_1, q_2]$ or $J = [q_1, q_2[\quad \ldots .$

Minimal presentation of PCTL

- **Syntax of PCTL – some shorthands:**

  If $J = [q_1, q_2]$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 \leqslant p \leqslant q_2}(\Psi)$, which asserts that path formula Ψ holds with a probability p between q_1 and q_2.

  If $J =]q_1, q_2]$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 < p \leqslant q_2}(\Psi)$.

  If $J = [q_1, q_2[$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 \leqslant p < q_2}(\Psi)$.

  If $J =]q_1, q_2[$ we can read the formula $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{q_1 < p < q_2}(\Psi)$.

- If $J = [q_1, q_2]$ and $q_1 = 0$, we can read $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{\leqslant q_2}(\Psi)$.

  If $J = [q_1, q_2]$ and $q_2 = 1$, we can read $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{\geqslant q_1}(\Psi)$.

  If $J = [q_1, q_2]$ and $q_1 = q_2 = q$, we can read $\mathbb{P}_J(\Psi)$ as $\mathbb{P}_{=q}(\Psi)$.
- And similarly, if $J =]q_1, q_2]$ or $J = [q_1, q_2[$ $\quad \ldots .$

- If $J = [q_1, 1]$ and $\Psi = (\varphi_1 \ \mathbb{U} \ \varphi_2)$ we can read $\mathbb{P}_J(\Psi)$ as $(\varphi_1 \ \mathbb{U}^{\geqslant q_1} \ \varphi_2)$.
- Etc. $\quad \ldots .$

Minimal presentation of PCTL

- **Semantics of PCTL:**

$$
\begin{array}{lll}
\mathcal{M}, s & \models \mathtt{true} & \\
\mathcal{M}, s & \models p & \text{iff} \quad p \in L(s) \\
\mathcal{M}, s & \models \neg\varphi & \text{iff} \quad \mathcal{M}, s \not\models \varphi \\
\mathcal{M}, s & \models \varphi_1 \wedge \varphi_2 & \text{iff} \quad \mathcal{M}, s \models \varphi_1 \text{ and } \mathcal{M}, s \models \varphi_2 \\
\mathcal{M}, s & \models \mathbb{P}_J(\Psi) & \text{iff} \quad \Pr(\mathcal{M}, s \models \Psi) \in J
\end{array}
$$

where $\Pr(\mathcal{M}, s \models \Psi) := \Pr\{\, \pi \in$ **Paths**$(s) \mid \mathcal{M}, \pi \models \Psi \,\}$ with:

$$
\begin{array}{lll}
\mathcal{M}, \pi & \models \varphi_1 \ \mathbb{U}\ \varphi_2 & \text{iff} \quad \text{there is } j \geqslant 0 \text{ such } \pi[j..] \models \varphi_2 \text{ and} \\
 & & \qquad \pi[i..] \models \varphi_1 \text{ for every } 0 \leqslant i < j \\
\mathcal{M}, \pi & \models \varphi_1 \ \mathbb{U}^{\leqslant n}\ \varphi_2 & \text{iff} \quad \text{there is } 0 \leqslant j \leqslant n \text{ such } \pi[j..] \models \varphi_2 \text{ and} \\
 & & \qquad \pi[i..] \models \varphi_1 \text{ for every } 0 \leqslant i < j
\end{array}
$$

where $\pi = s_0 s_1 s_2 \cdots$ is an ω-infinite execution path in $\mathcal{M}$.

Minimal presentation of PCTL

- **Definitions of other temporal connectives in terms of $\mathbb{U}$ and $\mathbb{U}^{\leqslant n}$.**

  1. $\Diamond\, \varphi \triangleq (\mathbf{true}\ \mathbb{U}\ \varphi)$
  2. $\Diamond^{\leqslant n}\, \varphi \triangleq (\mathbf{true}\ \mathbb{U}^{\leqslant n}\ \varphi)$,

     a path satisfies $(\Diamond^{\leqslant n}\, \varphi)$ if it reaches a φ-state within n steps
  3. Can you define $(\Box^{\leqslant n}\, \varphi) \triangleq \neg(\Diamond^{\leqslant n} \neg\varphi)$?

     a path satisfies $(\Box^{\leqslant n}\, \varphi)$ if each of its first $n+1$ states satisfies φ
  4. How about defining $\bigcirc\, \varphi \triangleq (\neg\varphi\ \mathbb{U}^{\leqslant 1}\ \varphi) \vee (\mathbf{true}\ \mathbb{U}^{\leqslant 1}\ \varphi)$?
  5. $\mathbb{P}_{\leqslant p}(\Box\, \varphi) \triangleq \mathbb{P}_{\geqslant 1-p}(\Diamond\, \neg\varphi)$
  6. $\mathbb{P}_{]p,q]}(\Box^{\leqslant n}\, \varphi) \triangleq \mathbb{P}_{[1-q,1-p[}(\Diamond^{\leqslant n}\, \neg\varphi)$
  7. $\mathbb{P}_J(\Box^{\leqslant n}\, \varphi) \triangleq \mathbb{P}_J(\varphi\, \mathsf{W}^{\leqslant n}\, \bot)$
  8. Etc. $\ldots$

Examples of modeling with PCTL

1. $\bigcirc^{\leqslant 0.2} \varphi$

   "φ is true in the next state with probability $\leqslant 0.2$"

2. $\big(\varphi_1 \, \mathbb{U}^{\leqslant 0.3} \, \varphi_2\big)$

   "probability of reaching a φ_2-state via a φ_1-path $\leqslant 0.3$"

3. $\mathbb{P}_{\leqslant 0.4}\big(\varphi_1 \, \mathbb{U}^{\leqslant 10} \, \varphi_2\big)$ or also $\big(\varphi_1 \, \mathbb{U}^{\leqslant 10}_{\leqslant 0.4} \, \varphi_2\big)$

   "probability of reaching a φ_2-state via a φ_1-path in at most 10 steps $\leqslant 0.4$"

The two next formulas are equivalent (why?):

4. $\mathbb{P}_{\leqslant 0.001}\big(\Diamond^{\leqslant 50} \text{error}\big)$

   "probability of an error to occur within 50 steps $\leqslant 0.001$"

5. $\mathbb{P}_{\geqslant 0.999}\big(\Box^{\leqslant 50} \neg\text{error}\big)$

   "probability of **no** error to occur within 50 steps $\geqslant 0.999$"

Examples of modeling with PCTL

6. In a transition system $\mathcal{M}$ where, along every ω-infinite execution path a 6-sided die is repeatedly cast, the following PCTL formula:

   $$\bigwedge_{1 \leqslant i \leqslant 6} \mathbb{P}_{=1/6}(\Diamond\, a_i)$$

   expresses that "each of the 6 possible outcomes is equally probable", where $a_1, \ldots, a_6$ are atomic propositions representing 6 sides of the die.

Examples of modeling with PCTL

7. $\mathbb{P}_{=1}(\Diamond \text{delivered})$

   "with probability $= 1$ the message will be eventually delivered"

8. $\mathbb{P}_{=1}\Big(\Box \big(\text{try\_to\_send} \to \mathbb{P}_{\geqslant 0.99}(\Diamond^{\leqslant 3} \text{delivered})\big)\Big)$

   "with probability $= 1$ every attempt to send the message will result

   in its delivery in at most 3 steps with probability $\geqslant 0.99$"

   Combining the two preceding formulas:

9. $\mathbb{P}_{=1}(\Diamond \text{delivered}) \;\wedge\; \mathbb{P}_{=1}\Big(\Box \big(\text{try\_to\_send} \to \mathbb{P}_{\geqslant 0.99}(\Diamond^{\leqslant 3} \text{delivered})\big)\Big)$

   "with probability $= 1$ the message will . . .   and

   with probability $= 1$ every attempt to send . . ."

Exercise: Check that all the formulas on pages 9, 10, and 11, are valid in the formal syntax of PCTL on page 2.

Hint: Consult the equivalences on page 8.

(THIS PAGE INTENTIONALLY LEFT BLANK)