Modeling and Verification of Probabilistic Systems

Joost-Pieter Katoen

Lehrstuhl für Informatik 2
Software Modeling and Verification Group

http://moves.rwth-aachen.de/teaching/ws-1819/movep18/

November 5, 2018

Overview

1. Introduction
2. Qualitative PCTL
3. Computation Tree Logic
4. CTL versus qualitative PCTL
5. Fair CTL versus qualitative PCTL
6. Repeated reachability and persistence
7. Summary

Summary of previous lecture

Probabilistic CTL

- Allows for path properties, such as (bounded) until and next.
- State formulas include propositional logic + the operator $\mathbb{P}_J(\varphi)$
- $s \models \mathbb{P}_J(\varphi)$ if the probability of all paths starting in s fulfilling φ is in J
- Model checking is done by a recursive descent over the formula
- This yields a polynomial-time algorithm (linear in $|\Phi|$).

Aim of this lecture

- Is PCTL, restricted to $\mathbb{P}_{=1}(\varphi)$, equally expressive as CTL?
- What is the expressive power of PCTL? Can repeated reachability be expressed?

Set up of this lecture

1. Qualitative PCTL versus CTL.
2. Qualitative PCTL versus CTL with fairness.
3. Repeated reachability probabilities in PCTL.

Overview

1. Introduction
2. Qualitative PCTL
3. Computation Tree Logic
4. CTL versus qualitative PCTL
5. Fair CTL versus qualitative PCTL
6. Repeated reachability and persistence
7. Summary

PCTL syntax

Probabilistic Computation Tree Logic: Syntax

PCTL consists of state- and path-formulas.

- PCTL *state formulas* over the set AP obey the grammar:

$$\Phi \ ::= \ \text{true} \ \Big| \ a \ \Big| \ \Phi_1 \wedge \Phi_2 \ \Big| \ \neg\Phi \ \Big| \ \mathbb{P}_J(\varphi)$$

where $a \in AP$, φ is a path formula and $J \subseteq [0,1]$ is an interval.

- PCTL *path formulae* are formed according to the following grammar:

$$\varphi \ ::= \ \bigcirc\Phi \ \Big| \ \Phi_1 \, \mathsf{U} \, \Phi_2 \ \Big| \ \Phi_1 \, \mathsf{U}^{\leqslant n} \, \Phi_2$$

where Φ, Φ_1, and Φ_2 are state formulae and $n \in \mathbb{N}$.

Qualitative PCTL

Qualitative PCTL

State formulae in the *qualitative fragment* of PCTL (over AP):

$$\Phi ::= \text{true} \ \Big| \ a \ \Big| \ \Phi_1 \wedge \Phi_2 \ \Big| \ \neg\Phi \ \Big| \ \mathbb{P}_{>0}(\varphi) \ \Big| \ \mathbb{P}_{=1}(\varphi)$$

where $a \in AP$, and φ is a path formula formed according to the grammar:

$$\varphi ::= \bigcirc\Phi \ \Big| \ \Phi_1 \, \mathsf{U} \, \Phi_2.$$

Remark

The probability bounds $= 0$ and < 1 can be derived:

$$\mathbb{P}_{=0}(\varphi) \equiv \neg\mathbb{P}_{>0}(\varphi) \quad \text{and} \quad \mathbb{P}_{<1}(\varphi) \equiv \neg\mathbb{P}_{=1}(\varphi)$$

So, in qualitative PCTL, there is no bounded until, and only > 0, $= 0$, > 1 and $= 1$ are allowed thresholds.

Qualitative PCTL

Qualitative PCTL

State formulae in the *qualitative fragment* of PCTL (over AP):

$$\Phi ::= \text{true} \ \Big| \ a \ \Big| \ \Phi_1 \wedge \Phi_2 \ \Big| \ \neg\Phi \ \Big| \ \mathbb{P}_{>0}(\varphi) \ \Big| \ \mathbb{P}_{=1}(\varphi)$$

where $a \in AP$, and φ is a path formula formed according to the grammar:

$$\varphi ::= \bigcirc\Phi \ \Big| \ \Phi_1 \, \mathsf{U} \, \Phi_2.$$

Examples

$\mathbb{P}_{=1}(\lozenge\mathbb{P}_{>0}(\bigcirc a))$ and $\mathbb{P}_{<1}(\mathbb{P}_{>0}(\lozenge a) \, \mathsf{U} \, b)$ are qualitative PCTL formulas.

Overview

1. Introduction
2. Qualitative PCTL
3. Computation Tree Logic
4. CTL versus qualitative PCTL
5. Fair CTL versus qualitative PCTL
6. Repeated reachability and persistence
7. Summary

Computation Tree Logic [Clarke & Emerson, 1981]

Computation Tree Logic: Syntax

CTL consists of state- and path-formulas.

- CTL *state formulas* over the set AP obey the grammar:

$$\Phi \ ::= \ \text{true} \ \Big| \ a \ \Big| \ \Phi_1 \wedge \Phi_2 \ \Big| \ \neg\Phi \ \Big| \ \exists\varphi \ \Big| \ \forall\varphi$$

where $a \in AP$ and φ is a path formula formed by the grammar:

$$\varphi \ ::= \ \bigcirc\Phi \ \Big| \ \Phi_1 \,\mathsf{U}\, \Phi_2$$

Remark

No bounded until, and only universal and existential path quantifiers.

Examples

$\forall\lozenge\exists\bigcirc\ a$ and $\exists(\forall\lozenge a)\,\mathsf{U}\, b$ are CTL formulas.

Computation Tree Logic [Clarke & Emerson, 1981]

Computation Tree Logic: Syntax

CTL consists of state- and path-formulas.

- CTL *state formulas* over the set AP obey the grammar:

$$\Phi \ ::= \ \text{true} \ \Big| \ a \ \Big| \ \Phi_1 \wedge \Phi_2 \ \Big| \ \neg\Phi \ \Big| \ \exists\varphi \ \Big| \ \forall\varphi$$

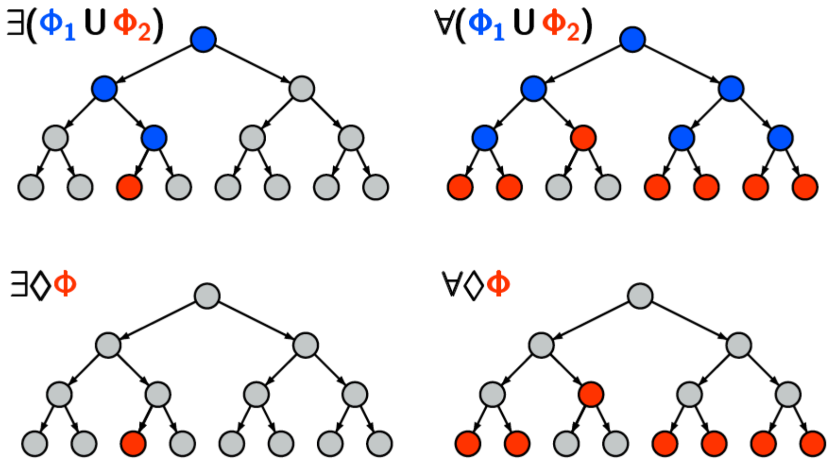
where $a \in AP$ and φ is a path formula $\varphi \ ::= \ \bigcirc\Phi \ \Big| \ \Phi_1 \,\mathsf{U}\, \Phi_2$

Intuition

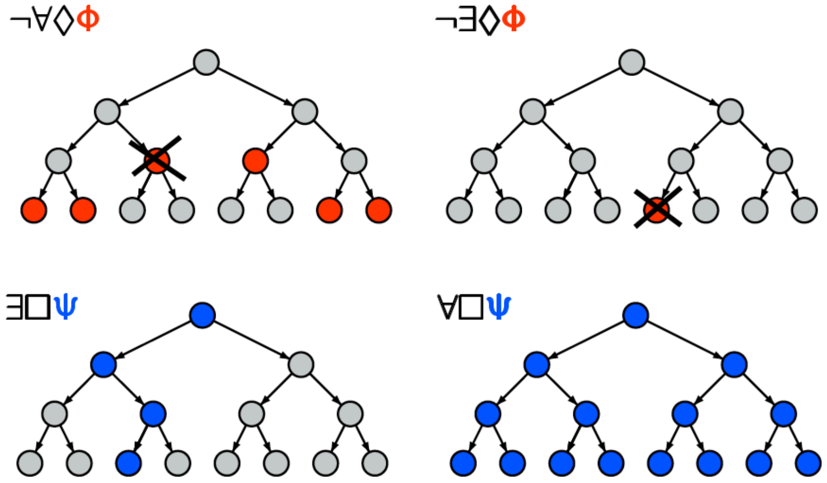
- $s \models \forall\varphi$ if all paths starting in s fulfill φ
- $s \models \exists\varphi$ if some path starting in s fulfill φ

Question: are CTL and qualitative PCTL equally expressive? No.

CTL semantics


$\exists(\Phi_1\,\mathsf{U}\,\Phi_2)$
$\forall(\Phi_1\,\mathsf{U}\,\Phi_2)$
$\exists\lozenge\Phi$
$\forall\lozenge\Phi$

CTL semantics



CTL semantics (1)

Notation

$\mathcal{D}, s \models \Phi$ if and only if state-formula Φ holds in state s of (possibly infinite) DTMC $\mathcal{D}$. As $\mathcal{D}$ is known from the context we simply write $s \models \Phi$.

Satisfaction relation for state formulas

The satisfaction relation $\models$ is defined for CTL state formulas by:

$$\begin{array}{lll}
s \models a & \text{iff} & a \in L(s) \\
s \models \neg\,\Phi & \text{iff} & \text{not } (s \models \Phi) \\
s \models \Phi \,\wedge\, \Psi & \text{iff} & (s \models \Phi) \text{ and } (s \models \Psi) \\
s \models \exists\varphi & \text{iff} & \text{there exists } \pi \in \mathit{Paths}(s). \pi \models \varphi \\
s \models \forall\varphi & \text{iff} & \text{for all } \pi \in \mathit{Paths}(s). \pi \models \varphi
\end{array}$$

where the semantics of CTL path-formulas is the same as for PCTL path-formulas.

Overview

1 Introduction

2 Qualitative PCTL

3 Computation Tree Logic

4 CTL versus qualitative PCTL

5 Fair CTL versus qualitative PCTL

6 Repeated reachability and persistence

7 Summary

CTL versus qualitative PCTL

Equivalence of PCTL and CTL Formulae

The PCTL formula Φ is *equivalent* to the CTL formula Ψ, denoted $\Phi \equiv \Psi$, if $\mathit{Sat}(\Phi) = \mathit{Sat}(\Psi)$ for each DTMC $\mathcal{D}$.

Example

The simplest such cases are path formulae involving the next-step operator:

$$\begin{array}{lll}
\mathbb{P}_{=1}(\bigcirc a) & \equiv & \forall\bigcirc a \\
\mathbb{P}_{>0}(\bigcirc a) & \equiv & \exists\bigcirc a
\end{array}$$

And for $\exists\Diamond$ and $\forall\Box$ we have:

$$\begin{array}{lll}
\mathbb{P}_{>0}(\Diamond a) & \equiv & \exists\Diamond a \\
\mathbb{P}_{=1}(\Box a) & \equiv & \forall\Box a.
\end{array}$$

CTL versus qualitative PCTL

(1) $\mathbb{P}_{>0}(\Diamond a) \;\equiv\; \exists\Diamond a$ and (2) $\mathbb{P}_{=1}(\Box a) \;\equiv\; \forall\Box a$.

Proof:

(1) Consider the first statement.

$\Rightarrow$ Assume $s \models \mathbb{P}_{>0}(\Diamond a)$. By the PCTL semantics, $Pr(s \models \Diamond a) > 0$. Thus, $\{\, \pi \in Paths(s) \mid \pi \models \Diamond a \,\} \neq \varnothing$, and hence, $s \models \exists\Diamond a$.

$\Leftarrow$ Assume $s \models \exists\Diamond a$, i.e., there is a finite path $\hat{\pi} = s_0\, s_1 \ldots s_n$ with $s_0 = s$ and $s_n \models a$. It follows that all paths in the cylinder set $Cyl(\hat{\pi})$ fulfill $\Diamond a$. Thus:

$$Pr(s \models \Diamond a) \;\geqslant\; Pr_s(Cyl(s_0\, s_1 \ldots s_n)) \;=\; \mathbf{P}(s_0 s_1 \ldots s_n) \;>0.$$

So, by the PCTL semantics we have: $s \models \mathbb{P}_{>0}(\Diamond a)$.

(2) The second statement follows by duality.

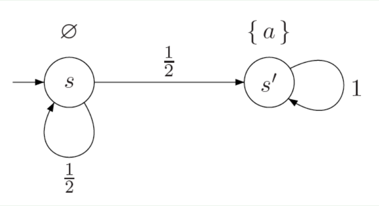
CTL versus qualitative PCTL

(1) $\mathbb{P}_{>0}(\Diamond a) \;\equiv\; \exists\Diamond a$ and (2) $\mathbb{P}_{=1}(\Box a) \;\equiv\; \forall\Box a$.

(3) $\mathbb{P}_{>0}(\Box a) \;\not\equiv\; \exists\Box a$ and (4) $\mathbb{P}_{=1}(\Diamond a) \;\not\equiv\; \forall\Diamond a$.

Example

Consider the second statement (4). Let s be a state in a (possibly infinite) DTMC. Then: $s \models \forall\Diamond a$ implies $s \models \mathbb{P}_{=1}(\Diamond a)$. The reverse direction, however, does not hold. Consider the example DTMC:



$s \models \mathbb{P}_{=1}(\Diamond a)$ as the probability of path s^ω is zero. However, the path s^ω is possible and violates $\Diamond a$. Thus, $s \not\models \forall\Diamond a$.

Statement (3) follows by duality.

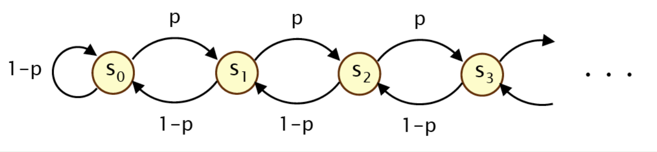
Almost-sure-reachability not in CTL

Almost-sure-reachability not in CTL

1. There is no CTL formula that is equivalent to $\mathbb{P}_{=1}(\Diamond a)$.
2. There is no CTL formula that is equivalent to $\mathbb{P}_{>0}(\Box a)$.

Proof:

We provide the proof of 1.; 2. follows by duality: $\mathbb{P}_{>0}(\Box a) \equiv \neg\mathbb{P}_{=1}(\Diamond\neg a)$. By contraposition. Assume $\Phi \equiv \mathbb{P}_{=1}(\Diamond a)$. Consider the infinite DTMC $\mathcal{D}_p$:



The value of p does affect reachability: $Pr(s \models \Diamond\, s_0) = \begin{cases} 1 & \text{if } p \leqslant \frac{1}{2} \\ <1 & \text{if } p > \frac{1}{2} \end{cases}$

Almost-sure-reachability not in CTL

There is no CTL formula that is equivalent to $\mathbb{P}_{=1}(\Diamond a)$.

Proof:

We have: $Pr(s \models \Diamond\, s_0) = \begin{cases} 1 & \text{if } p \leqslant \frac{1}{2} \\ <1 & \text{if } p > \frac{1}{2} \end{cases}$

Thus, in $\mathcal{D}_{\frac{1}{4}}$ we have $s \models \mathbb{P}_{=1}(\Diamond s_0)$ for all states s, while in $\mathcal{D}_{\frac{3}{4}}$, e.g., $s_1 \not\models \mathbb{P}_{=1}(\Diamond s_0)$. Hence: $s_1 \in Sat_{\mathcal{D}_{\frac{1}{4}}}(\,\mathbb{P}_{=1}(\Diamond s_0)\,)$ but $s_1 \notin Sat_{\mathcal{D}_{\frac{3}{4}}}(\,\mathbb{P}_{=1}(\Diamond s_0)\,)$. For CTL-formula Φ —by assumption $\Phi \equiv \mathbb{P}_{=1}(\Diamond s_0)$— we have:

$$Sat_{\mathcal{D}_{\frac{1}{4}}}(\Phi) \;=\; Sat_{\mathcal{D}_{\frac{3}{4}}}(\Phi).$$

Hence, state s_1 either fulfills the CTL formula Φ in both DTMCs or in none of them. This, however, contradicts $\Phi \equiv \mathbb{P}_{=1}(\Diamond s_0)$.

Remark

The proof relies on the fact that the satisfaction of $\mathbb{P}_{=1}(\Diamond a)$ for infinite DTMCs may depend on the precise value of the transition probabilities, while CTL just refers to the underlying graph of a DTMC. For finite DTMCs, the previous result does not hold.

For each finite DTMC $\mathcal{D}$ it holds that:

$$\mathbb{P}_{=1}(\Diamond a) \quad \equiv \quad \forall(\,(\exists\Diamond a)\,\mathsf{W}\,a\,)$$

where W is the weak until operator defined by $\Phi\,\mathsf{W}\,\Psi = (\Phi\,\mathsf{U}\,\Psi) \;\vee\; \Box\Phi$.

Proof:

Exercise.

$\forall\Diamond$ is not expressible in qualitative PCTL

1. There is no qualitative PCTL formula that is equivalent to $\forall\Diamond a$.
2. There is no qualitative PCTL formula that is equivalent to $\exists\Box a$.

Proof:

Proof of the first claim on the black board. The second claim follows by duality since $\forall\Diamond a \equiv \neg\exists\Box\neg a$.

$\forall\Diamond$ is not expressible in qualitative PCTL

Qualitative PCTL versus CTL

Incomparable expressiveness

Qualitative PCTL and CTL have incomparable expressiveness; e.g., $\forall\Diamond a$ cannot be expressed in qualitative PCTL and $\mathbb{P}_{=1}(\Diamond a)$ cannot be expressed in CTL.

Overview

1. Introduction
2. Qualitative PCTL
3. Computation Tree Logic
4. CTL versus qualitative PCTL
5. Fair CTL versus qualitative PCTL
6. Repeated reachability and persistence
7. Summary

Fairness

Remark

The existence of unfair computations is vital (in particular s_n^ω in the proof of the result that $\forall\Diamond$ is not expressible in qualitative PCTL.) In fact, under appropriate fairness constraints, we yield $\forall\Diamond a \equiv \mathbb{P}_{=1}(\Diamond a)$.

Strong fairness

Assume $\mathcal{D}$ is a finite DTMC and that any state s in $\mathcal{D}$ is uniquely characterized by an atomic proposition, say s. The *(strong) fairness* constraint *fair* is defined by:

$$fair \;=\; \bigwedge_{s \in S} \;\; \bigwedge_{t \,\in\, Post(s)} (\Box\Diamond s \rightarrow \Box\Diamond t).$$

It asserts that when a state s is visited infinitely often, then every of its direct successors is visited infinitely often too.

Fair CTL

Fair paths

In fair CTL, path formulas are interpreted over fair infinite paths, i.e., paths π that satisfy

$$fair \;=\; \bigwedge_{s \in S} \;\; \bigwedge_{t \,\in\, Post(s)} (\Box\Diamond s \rightarrow \Box\Diamond t).$$

A path π such that $\pi \models fair$ is called fair. Let $Paths_{fair}(s)$ be the set of fair paths starting in s.

Fair CTL semantics

The fair semantics of CTL is defined by the satisfaction $\models_{fair}$ which is defined as $\models$ for the CTL semantics, except that:

$$
\begin{array}{lll}
s \models_{fair} \exists\varphi & \text{iff} & \text{there exists } \pi \in Paths_{fair}(s).\, \pi \models_{fair} \varphi \\
s \models_{fair} \forall\varphi & \text{iff} & \text{for all } \pi \in Paths_{fair}(s).\, \pi \models_{fair} \varphi.
\end{array}
$$

Fairness theorem

Qualitative PCTL versus fair CTL theorem

Let s be an arbitrary state in a finite DTMC. Then:

$$
\begin{array}{lll}
s \models \mathbb{P}_{=1}(\Diamond a) & \text{iff} & s \models_{fair} \forall\Diamond a \\
s \models \mathbb{P}_{>0}(\Box a) & \text{iff} & s \models_{fair} \exists\Box a \\
s \models \mathbb{P}_{=1}(a \,\mathsf{U}\, b) & \text{iff} & s \models_{fair} \forall(a \,\mathsf{U}\, b) \\
s \models \mathbb{P}_{>0}(a \,\mathsf{U}\, b) & \text{iff} & s \models_{fair} \exists(a \,\mathsf{U}\, b)
\end{array}
$$

Proof:

Using the fairness theorem (cf. Lecture 4): for (possibly infinite) DTMC $\mathcal{D}$ and s, t states in $\mathcal{D}$:

$$Pr(s \models \Box\Diamond t) \;=\; Pr(s \models \bigwedge_{u \in Post^*(t)} \Box\Diamond u).$$

In addition, we use that from every reachable state at least one fair path starts. Similar arguments hold for infinite DTMCs (where *fair* is interpreted as infinitary conjunction.)

Qualitative PCTL versus fair CTL

Comparable expressiveness

Qualitative PCTL and fair CTL are equally expressive for finite Markov chains.

Overview

1. Introduction
2. Qualitative PCTL
3. Computation Tree Logic
4. CTL versus qualitative PCTL
5. Fair CTL versus qualitative PCTL
6. Repeated reachability and persistence
7. Summary

Almost sure repeated reachability

Almost sure repeated reachability is PCTL-definable

For finite DTMC $\mathcal{D}$, state $s \in S$ and $G \subseteq S$:

$$s \models \mathbb{P}_{=1}(\Box \mathbb{P}_{=1}(\Diamond G)) \quad \text{iff} \quad Pr_s\{\pi \in Paths(s) \mid \pi \models \Box\Diamond G\} = 1.$$

We abbreviate $\mathbb{P}_{=1}(\Box \mathbb{P}_{=1}(\Diamond G))$ by $\mathbb{P}_{=1}(\Box\Diamond G)$.

Proof:

On the blackboard.

Remark:

For CTL, universal repeated reachability properties can be formalized by the combination of the modalities $\forall\Box$ and $\forall\Diamond$:

$$s \models \forall\Box\forall\Diamond G \quad \text{iff} \quad \pi \models \Box\Diamond G \text{ for all } \pi \in Paths(s).$$

Repeated reachability probabilities

Repeated reachability probabilities are PCTL-definable

For finite DTMC $\mathcal{D}$, state $s \in S$, $G \subseteq S$ and interval $J \subseteq [0,1]$ we have:

$$s \models \underbrace{\mathbb{P}_J(\Diamond \mathbb{P}_{=1}(\Box \mathbb{P}_{=1}(\Diamond G)))}_{=\mathbb{P}_J(\Box\Diamond G)} \quad \text{if and only if} \quad Pr(s \models \Box\Diamond G) \in J.$$

Proof:

By the long run theorem (cf. Lecture 4), almost surely a BSCC T will be reached and each of its states will be visited infinitely often. Thus, the probabilities for $\Box\Diamond G$ agree with the probability to reach a BSCC T that contains a state in G.

Remark:

By the above theorem, $\mathbb{P}_{>0}(\Box\Diamond G)$ is PCTL definable. Note that $\exists\Box\Diamond G$ is not CTL-definable (but definable in a combination of CTL and LTL, called CTL*).

Almost sure persistence

Almost sure persistence is PCTL-definable

For finite DTMC $\mathcal{D}$, state $s \in S$ and $G \subseteq S$:

$$s \models \mathbb{P}_{=1}\,(\,\Diamond\,\mathbb{P}_{=1}(\Box G)\,) \quad \text{iff} \quad Pr_s\{\,\pi \in Paths(s) \mid \pi \models \Diamond\Box G\,\} \;=\; 1.$$

We abbreviate $\mathbb{P}_{=1}\,(\,\Diamond\,\mathbb{P}_{=1}(\Box G))$ by $\mathbb{P}_{=1}\,(\,\Diamond\Box G)$.

Proof:

Left as an exercise.

Remark:

Note that $\forall\Diamond\Box G$ is not CTL-definable. $\Diamond\Box G$ is a well-known example formula in LTL that cannot be expressed in CTL. But by the above theorem it can be expressed in PCTL.

Persistence probabilities

Persistence probabilities are PCTL-definable

For finite DTMC $\mathcal{D}$, state $s \in S$, $G \subseteq S$ and interval $J \subseteq [0,1]$ we have:

$$s \models \underbrace{\mathbb{P}_J(\Diamond\mathbb{P}_{=1}(\Box G))}_{=\mathbb{P}_J(\Diamond\Box G)} \quad \text{if and only if} \quad Pr(s \models \Diamond\Box G) \in J.$$

Proof:

Left as an exercise. Hint: use the long run theorem (cf. Lecture 4).

Overview

1. Introduction
2. Qualitative PCTL
3. Computation Tree Logic
4. CTL versus qualitative PCTL
5. Fair CTL versus qualitative PCTL
6. Repeated reachability and persistence
7. Summary

Summary

- Qualitative PCTL only allow the probability bounds > 0 and $= 1$.
- There is no CTL formula that is equivalent to $\mathbb{P}_{=1}(\Diamond a)$.
- There is no PCTL formula that is equivalent to $\forall\Box a$.
- These results do not apply to finite DTMCs.
- $\mathbb{P}_{=1}(\Diamond a)$ and $\forall\Diamond a$ are equivalent under strong fairness.
- Repeated reachability probabilities are PCTL definable.

Take-home messages

Qualitative PCTL and CTL have incomparable expressiveness. Qualitative and fair CTL are equally expressive. Repeated reachability and persistence probabilities are PCTL definable. Their qualitative counterparts are not all expressible in CTL.