jpf-ctl: CTL Model Checking of Java Code

Parssa Khazra, Anto Nanah Ji, Matt Walker, Hongru Wang, and Franck van Breugel
Department of Electrical Engineering and Computer Science, York University, Toronto

November 26, 2021

Abstract

Although several attempts have been made to extend *Java PathFinder* (JPF) to support model checking of linear temporal logic (LTL), we are not aware of any extension of JPF that provides *computation tree logic* (CTL) model checking. Our extension, named jpf-ctl, extends JPF so it can check whether a Java app satisfies a property expressed in CTL.

1 The Syntax of Computation Tree Logic

Computation tree logic (CTL) was introduced by Turing award winners Clarke and Emerson [3]. The formulas of this logic consist of the constants `true` and `false` and so-called atomic propositions which are combined by means of several operators that we will discuss below. The *atomic propositions* are used to express basic facts about the states of the system. That is, these atomic propositions are state predicates. In the next section, we provide some concrete examples of atomic propositions in the context of Java code.

CTL contains the operators

- negation, denoted $\neg$,
- conjunction, denoted by $\wedge$,
- disjunction, denoted $\vee$,
- implication, denoted $\rightarrow$, and
- equivalence, denoted $\leftrightarrow$.

Furthermore, it contains

- universal quantification, denoted $\forall$, and
- existential quantification, denoted $\exists$.

Finally, it contains the so-called temporal operators

- next, denoted $\bigcirc$,
- until, denoted U,
- always, denoted $\Box$, and
- eventually, denoted $\Diamond$.

Let us formally define the syntax of CTL. Let AP be the set of atomic propositions. The set of CTL formulas is defined by the following grammar.

$$\begin{aligned}\varphi ::= &(\varphi) \mid a \\ &\mid \texttt{true} \mid \texttt{false} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \rightarrow \varphi \mid \varphi \leftrightarrow \varphi \\ &\mid \forall \bigcirc \varphi \mid \exists \bigcirc \varphi \mid \forall \varphi \,\mathsf{U}\, \varphi \mid \exists \varphi \,\mathsf{U}\, \varphi \mid \forall \Box \varphi \mid \exists \Box \varphi \mid \forall \Diamond \varphi \mid \exists \Diamond \varphi\end{aligned}$$

where $a \in AP$.

In order to make sense of a CTL formula such as

$$\forall \bigcirc a \rightarrow b \rightarrow c$$

we need to define the precedence of the operators. Furthermore, we need to specify whether the binary operators are left or right associative. For the order of precedence, we use the commonly accepted order (from highest to lowest): $\neg$, $\wedge$, $\vee$, $\rightarrow$, and $\leftrightarrow$. According to Baier and Katoen [1], U takes precedence over $\wedge$, $\vee$, and $\rightarrow$ (they do not consider $\leftrightarrow$). Usually, unary operators have higher precedence than binary ones. Hence, the operators, listed from highest to lowest precedence, are

$$\begin{array}{l}\neg \\ \forall\bigcirc, \exists\bigcirc, \forall\Box, \exists\Box, \forall\Diamond, \exists\Diamond \\ \forall\mathsf{U}, \exists\mathsf{U} \\ \wedge \\ \vee \\ \rightarrow \\ \leftrightarrow\end{array}$$

The binary operators $\wedge$, $\vee$ and $\leftrightarrow$ are (left) associative. Usually, $\rightarrow$ is considered right associative. According to Baier and Katoen [1], U is also right associative.

Using the above specified precedence and associativity rules, the above CTL formula is interpreted as

$$(\forall \bigcirc a) \rightarrow (b \rightarrow c)$$

To express the CTL formulas in ASCII, we use the following grammar.

$$\begin{aligned}\varphi ::= &(\varphi) \mid a \\ &\mid \texttt{true} \mid \texttt{false} \mid \texttt{!}\varphi \mid \varphi \texttt{ \&\& } \varphi \mid \varphi \texttt{ || } \varphi \mid \varphi \texttt{ -> } \varphi \mid \varphi \texttt{ <-> } \varphi \\ &\mid \texttt{AX}\,\varphi \mid \texttt{EX}\,\varphi \mid \varphi \texttt{ AU } \varphi \mid \varphi \texttt{ EU } \varphi \mid \texttt{AG}\,\varphi \mid \texttt{EG}\,\varphi \mid \texttt{AF}\,\varphi \mid \texttt{EF}\,\varphi\end{aligned}$$

The ASCII representation of $\neg$, $\wedge$, and $\vee$ is taken from Java. It is common practice to use `A` and `E` for universal (for *a*ll) and existential (*e*xists) quantification. In the seminal paper by Turing award winner Pnueli [10], the temporal operators $\bigcirc$, U, $\Box$, and $\Diamond$ are represented as `X` (ne*x*t), `U` (*u*ntil), `G` (*g*lobally), and `F` (*f*uture). The above CTL formula is represented in ASCII as follows.

```
AX a -> b -> c
```

2 The Syntax of Computation Tree Logic for Java

The next operator $\bigcirc$ expresses that something holds in the next state. For Java code, if one were to define the notion of next state, it would probably be the state after the next bytecode instruction has been executed. However, expressing properties of Java code in terms to steps taken at the bytecode level seems of limited, if any, use. Therefore, we do not consider the next operator $\bigcirc$.

Recall that atomic propositions are used to express basic facts about the states. For now, we restrict our attention to static Boolean fields. Such an atomic proposition holds in those states in which the field has the value true. In Java, static Boolean fields are of the form

- ⟨package name⟩ . ⟨class name⟩ . ⟨field name⟩ or
- ⟨class name⟩ . ⟨field name⟩.

For example, the package `java.awt` contains the classes `AWTEvent` and `InvocationEvent`. The former contains the static field `consumed` and the latter contains `catchExceptions`. Hence, the static Boolean field `java.awt.AWTEvent.consumed` is an atomic proposition, as is `java.awt.InvocationEvent.catchExceptions`. Those fields are used as atomic propositions in the following CTL formula.

```
AG (java.awt.AWTEvent.consumed
    || EF !java.awt.event.InvocationEvent.catchExceptions)
```

As can be seen in the above example, the atomic propositions often clutter the CTL formula. Therefore, we allow aliases to be introduced for these atomic propositions. These aliases, which are meant to be less verbose than the atomic propositions, can be used in the CTL formula. For example, consider the following.

```
consumed: java.awt.AWTEvent.consumed
caught: java.awt.event.InvocationEvent.catchExceptions

AG (consumed || EF !caught)
```

By using the aliases `consumed` and `caught` for the atomic propositions `java.awt.AWTEvent.consumed` and `java.awt.event.InvocationEvent.catchExceptions`, the CTL formula becomes easier to read.

3 A Lexer and Parser for CTL Formulas

A lexer and parser for CTL formulas have been developed using ANTLR [9]. The above described grammar can be specified in ANTLR format as folows.

```
formula
  : '(' formula ')'                          #Bracket
  | ALIAS                                    #Alias
  | 'true'                                   #True
  | 'false'                                  #False
  | '!' formula                              #Not
  | 'AG' formula                             #ForAllAlways
  | 'AF' formula                             #ForAllEventually
  | 'EG' formula                             #ExistsAlways
  | 'EF' formula                             #ExistsEventually
  | <assoc=right> formula 'AU' formula       #ForAllUntil
  | <assoc=right> formula 'EU' formula       #ExistsUntil
  | <assoc=left> formula '&&' formula        #And
  | <assoc=left> formula '| |' formula       #Or
  | <assoc=right> formula '->' formula       #Implies
  | <assoc=left> formula '<->' formula       #Iff
```

The operators `AU`, `EU`, and `->` are specified as right associative. The other binary operators are left associative. The second column of the above rule contains the labels of the alternatives (see [9, Section 8.2]). We will discuss their role below.

The order of the alternatives is consistent with the precedence of the operators (if an operator has higher precedence, then its alternative occurs earlier). As a consequence, we had to order the operators `AU` and `EU`. We gave `AU` higher precedence than `EU`. Assume that a, b, and c are atomic propositions. The formula a `AU` b `AU` c is equivalent to a `AU` `(`b `AU` c`)` since `AU` is right associative. The formula a `AU` b `EU` c is equivalent to `(`a `AU` b`)` `EU` c since `AU` binds stronger than `EU`. For the same reason, the formula a `EU` b `AU` c is equivalent to a `EU` `(`b `AU` c`)`.

To keep aliases simple, we only allow Java identifiers. Recall that the atomic propositions are static attributes. To specify these, we also used relevant snippets of the ANTLR grammar for Java[1]. Whitespace, that is, spaces, tabs, form feeds, and returns are skipped.

4 From Parse Tree to Abstract Syntax Tree

Next, we translate a parse tree, generated by the lexer and parser, to an abstract syntax tree. An abstract syntax tree for CTL is represented by an object of type `Formula`, which is part of the package `ctl`. A UML diagram with the classes of the `ctl` package can be found in Figure 1. The CTL formula

```
AG (consumed || EF !caught)
```

[1] See github.com/antlr/grammars-v4/tree/master/java/java8.

is represented by the following `Formula` object.

```
Formula formula =
  new ForAllAlways(
    new Or(
      new Alias("consumed"),
      new ExistsEventually(
        new Not(
          new Alias("caught")
        )
      )
    )
  );
```

To implement this translation, we use the visitor design pattern. ANTLR supports this design pattern (see [9, Section 7.3]). From the CTL grammar, ANTLR generates a `CTLVisitor` interface. This interface contains a visit method for each alternative. For example, for the alternative labelled `ExistsAlways`, the interface contains the method `visitExistsAlways`.

ANTLR also generates the `CTLBaseVisitor` class. This adapter class provides a default implementation for all the methods of the `CTLVisitor` interface. We implement our translation by extending this class and overriding methods. For example, when we visit a node of the parse tree corresponding to the alternative labelled `And`, we first visit the left child and obtain the `Formula` object corresponding to the translation of the parse tree rooted at that left child. Next, we visit the right child and obtain the `Formula` object for the parse tree rooted at that right child. Finally, we create an `And` object from those two `Formula` objects.

```
@Override
public Formula visitAnd(AndContext context) {
  Formula left = (Formula) visit(context.formula(0));
  Formula right = (Formula) visit(context.formula(1));
  return new And(left, right);
}
```

Since the implication operator is right associative, in the `visitImplies` method we visit the right child first.

```
@Override
public Formula visitImplies(ImpliesContext context) {
  Formula right = (Formula) visit(context.formula(1));
  Formula left = (Formula) visit(context.formula(0));
  return new Implies(left, right);
}
```

5 Testing the Lexer, the Parser, and the Translation

We have developed a number of JUnit test classes that each test the lexer, the parser, and the translation of a parse tree to the corresponding abstract syntax tree. A UML diagram of these classes can be found in Figure 2.

The `BaseTest` class contains the `parse` method that, given a string, returns the corresponding abstract syntax tree. The `Formula` class contains the `random` method that returns the abstract syntax tree of a random CTL formula.

```
/**
 * Tests that the or operator is left associative.
 */
@RepeatedTest(TIMES)
public void testOr() {
  // generate three random abstract syntax trees
  Formula first = Formula.random();
  Formula second = Formula.random();
  Formula third = Formula.random();
  // combine the three
  Formula expected = new Or(new Or(first, second), third);
  // create its string representation without parentheses
  String formula = first + " || " + second + " || " + third;
  // obtain the abstract syntax tree
  Formula actual = parse(formula);
  assertEquals(expected, actual);
}
```

6 Non-serial transition relations

For technical convenience, in the literature it is often assumed that the transition relation is serial, that is, every state has outgoing transitions. However, the transition systems generated by JPF may have states without any outgoing transitions. Below, we revisit the definition of path fragments and paths of a transition system [1, Definition 3.4 and 3.6], the satisfaction relation for CTL [1, Definition 6.4], and the characterization of the satisfaction sets for CTL [1, Theorem 6.23] for systems with non-serial transition relations.

We denote the set of nonempty and finite sequences of states in S by S^* and the set of infinite sequences of states in S by $\mathcal{S}^\omega$.

Definition 1. Let $\mathcal{T} = (S, \to, AP, L)$ be a transition system.

- The nonempty and finite sequence $s_0 \dots s_n$ in S^*, where $n \geq 0$, is a path if $s_i \to s_{i+1}$ for all $0 \leq i < n$ and $s_n \not\to$.
- The infinite sequence $s_0 s_1 \dots$ in S^ω is a path if $s_i \to s_{i+1}$ for all $i \geq 0$.

We denote the set of paths that start in state s by $Paths_{\mathcal{T}}(s)$.

Definition 2. Let $\mathcal{T} = (S, \to, AP, L)$ be a transition system.

- The nonempty and finite sequence $s_0 \dots s_n$ in S^*, where $n \geq 0$, is a path fragment if $s_i \to s_{i+1}$ for all $0 \leq i < n$.

We denote the set of path fragments that start in state s by $PathFrag_{\mathcal{T}}(s)$. We denote the length of a path π by $|\pi|$. If the path π is infinite, then $|\pi| = \omega$. The satisfaction relation is defined as follows (see [1, Remark 6.11]).

Definition 3. Let $\mathcal{T} = (S, \to, AP, L)$ be a transition system. The relation $\models_{\mathcal{T}} \subseteq S \times CTL$ is defined by

- $s \models_{\mathcal{T}} a$ if $a \in L(s)$
- $s \models_{\mathcal{T}} \neg\varphi$ if $s \not\models_{\mathcal{T}} \varphi$
- $s \models_{\mathcal{T}} \varphi \wedge \psi$ if $s \models_{\mathcal{T}} \varphi \wedge s \models_{\mathcal{T}} \psi$
- $s \models_{\mathcal{T}} \exists \bigcirc \varphi$ if $\exists \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \wedge \pi[1] \models_{\mathcal{T}} \varphi$
- $s \models_{\mathcal{T}} \forall \bigcirc \varphi$ if $\forall \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \wedge \pi[1] \models_{\mathcal{T}} \varphi$
- $s \models_{\mathcal{T}} \exists \Box \varphi$ if $\exists \pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \varphi$
- $s \models_{\mathcal{T}} \forall \Box \varphi$ if $\forall \pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \varphi$
- $s \models_{\mathcal{T}} \exists \Diamond \varphi$ if $\exists \pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \varphi$
- $s \models_{\mathcal{T}} \forall \Diamond \varphi$ if $\forall \pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \varphi$
- $s \models_{\mathcal{T}} \exists \varphi \,\mathsf{U}\, \psi$ if $\exists \pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \psi \wedge \forall 0 \leq k < j : \pi[k] \models_{\mathcal{T}} \varphi$
- $s \models_{\mathcal{T}} \forall \varphi \,\mathsf{U}\, \psi$ if $\forall \pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \psi \wedge \forall 0 \leq k < j : \pi[k] \models_{\mathcal{T}} \varphi$

Recall that $\pi[0]$ the first state of a path π and $\pi[|\pi| - 1]$ is its last state. We use $\pi[\dots j]$ to denote $\pi[0] \dots \pi[j]$.

As defined in [1, Definition 6.12], CTL formulas φ and ψ are equivalent, denoted $\varphi \equiv \psi$, if for every transition system $\mathcal{T}$ and for each state s of $\mathcal{T}$, we have that $s \models_{\mathcal{T}} \varphi$ if and only if $s \models_{\mathcal{T}} \psi$. As we will show below, most equivalences found in [1, Figure 6.5] also hold for non-serial transition relations. However, the equivalence $\forall \bigcirc \varphi \equiv \neg\exists \bigcirc \neg\varphi$ does not hold in this setting.

Proposition 1. *For all $\varphi \in CTL$, $\forall \bigcirc \varphi \not\equiv \neg\exists \bigcirc \neg\varphi$*

Proof. Let $\varphi \in CTL$. Consider the transition system $\mathcal{T}$ consisting of a single state s without any transitions or labels. Note that $Paths_{\mathcal{T}}(s) = \{s\}$. Since

$$\begin{aligned} s \models_{\mathcal{T}} \neg\exists \bigcirc \neg\varphi \text{ iff } & s \not\models_{\mathcal{T}} \exists \bigcirc \neg\varphi \\ \text{iff } & \neg(\exists \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \wedge \pi[1] \models_{\mathcal{T}} \neg\varphi) \\ \text{iff } & \forall \pi \in Paths_{\mathcal{T}}(s) : |\pi| \leq 1 \vee \pi[1] \not\models_{\mathcal{T}} \neg\varphi \\ \text{iff } & \forall \pi \in Paths_{\mathcal{T}}(s) : |\pi| \leq 1 \vee \pi[1] \models_{\mathcal{T}} \varphi \end{aligned}$$

we can conclude that $s \models_{\mathcal{T}} \neg\exists \bigcirc \neg\varphi$. But $s \not\models_{\mathcal{T}} \forall \bigcirc \varphi$. □

Theorem 1. *For all $\varphi, \psi \in CTL$,*

- $\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$
- $\varphi \Rightarrow \psi \equiv \neg\varphi \vee \psi$
- $\varphi \Leftrightarrow \psi \equiv \varphi \Rightarrow \psi \wedge \psi \Rightarrow \varphi$
- $\forall\Box\varphi \equiv \neg\exists\Diamond\neg\varphi$
- $\exists\Diamond\varphi \equiv \exists \mathtt{true}\, \mathsf{U}\, \varphi$
- $\forall\Diamond\varphi \equiv \neg\exists\Box\neg\varphi$
- $\forall\varphi\, \mathsf{U}\, \psi \equiv \neg\exists(\neg\psi\, \mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \neg\exists\Box\neg\psi$

Proof. Let $\varphi, \psi \in CTL$. Let s be a state of the transition system $\mathcal{T}$.

- $$\begin{aligned} s \models_{\mathcal{T}} \varphi \vee \psi \text{ iff } & s \models_{\mathcal{T}} \varphi \vee s \models_{\mathcal{T}} \psi \\ \text{iff } & s \not\models_{\mathcal{T}} \neg\varphi \vee s \not\models_{\mathcal{T}} \neg\psi \\ \text{iff } & s \not\models_{\mathcal{T}} \neg\varphi \wedge \neg\psi \\ \text{iff } & s \models_{\mathcal{T}} \neg(\neg\varphi \wedge \neg\psi) \end{aligned}$$
- The equivalences for $\varphi \Rightarrow \psi$ and $\varphi \Leftrightarrow \psi$ are proved similarly.
- $$\begin{aligned} s \models_{\mathcal{T}} \forall\Box\varphi \text{ iff } & \forall \pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \varphi \\ \text{iff } & \forall \pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \not\models_{\mathcal{T}} \neg\varphi \\ \text{iff } & \neg(\exists \pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \neg\varphi) \\ \text{iff } & s \not\models_{\mathcal{T}} \exists\Diamond\neg\varphi \\ \text{iff } & s \models_{\mathcal{T}} \neg\exists\Diamond\neg\varphi \end{aligned}$$

- $s \models_{\mathcal{T}} \exists\Diamond\varphi$ iff $\exists\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \varphi$
  iff $\exists\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \varphi \wedge \forall 0 \leq k < j : \pi[k] \models_{\mathcal{T}} \mathtt{true}$
  iff $s \models_{\mathcal{T}} \exists \mathtt{true}\ \mathsf{U}\ \varphi$

- $s \models_{\mathcal{T}} \forall\Diamond\varphi$ iff $\forall\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \varphi$
  iff $\forall\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq i < |\pi| : \pi[i] \not\models_{\mathcal{T}} \neg\varphi$
  iff $\neg(\exists\pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \neg\varphi)$
  iff $s \not\models_{\mathcal{T}} \exists\Box\neg\varphi$
  iff $s \models_{\mathcal{T}} \neg\exists\Box\neg\varphi$

- $s \models_{\mathcal{T}} \forall\varphi\ \mathsf{U}\ \psi$ iff $\forall\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \psi \wedge \forall 0 \leq k < j : \pi[k] \models_{\mathcal{T}} \varphi$
  iff $\forall\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \psi \wedge$
  $\forall 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} (\varphi \vee \psi) \vee \exists 0 \leq k < j : \pi[k] \models_{\mathcal{T}} \psi$
  iff $\forall\pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} (\varphi \vee \psi) \vee \exists 0 \leq k < j : \pi[k] \models_{\mathcal{T}} \psi \wedge$
  $\forall\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \psi$
  iff $\forall\pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq j < |\pi| : \pi[j] \not\models_{\mathcal{T}} (\neg\varphi \wedge \neg\psi) \vee \exists 0 \leq k < j : \pi[k] \not\models_{\mathcal{T}} \neg\psi \wedge$
  $\forall\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq i < |\pi| : \pi[i] \not\models_{\mathcal{T}} \neg\psi$
  iff $\neg(\exists\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} (\neg\varphi \wedge \neg\psi) \wedge \forall 0 \leq k < j : \pi[k] \models_{\mathcal{T}} \neg\psi) \wedge$
  $\neg(\exists\pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \neg\psi)$
  iff $s \not\models_{\mathcal{T}} \exists(\neg\psi\ \mathsf{U}\ (\neg\varphi \wedge \neg\psi)) \wedge s \not\models_{\mathcal{T}} \exists\Box\neg\psi$
  iff $s \models_{\mathcal{T}} \neg\exists(\neg\psi\ \mathsf{U}\ (\neg\varphi \wedge \neg\psi)) \wedge s \models_{\mathcal{T}} \neg\exists\Box\neg\psi$
  iff $s \models_{\mathcal{T}} \neg\exists(\neg\psi\ \mathsf{U}\ (\neg\varphi \wedge \neg\psi)) \wedge \neg\exists\Box\neg\psi$

□

In the proof of Theorem 3 we use the following definition.

Definition 4. For $\pi, \rho \in Paths(s)$, $\pi \sqsubseteq \rho$ if $|\pi| \leq |\rho|$ and for all $0 \leq i < |\pi|$, $\pi[i] = \rho[i]$.

We use 2^S to denote the powerset of S. A function $\mathcal{F} : 2^S \to 2^S$ is monotone if for all U, $V \in 2^S$, $U \subseteq V$ implies $\mathcal{F}(U) \subseteq \mathcal{F}(V)$. The following result is known as the Knaster-Tarski theorem [8, 11]. Also this result is used in the proof of Theorem 3.

Theorem 2. *If $\mathcal{F} : 2^S \to 2^S$ is monotone then*

(a) there exists a smallest $U \in 2^S$ with $U \supseteq \mathcal{F}(U)$, which we denote by $\mu\mathcal{F}$,

(b) there exists a largest $U \in 2^S$ with $U \subseteq \mathcal{F}(U)$, which we denote by $\nu\mathcal{F}$,

(c) $\mu\mathcal{F} = \mathcal{F}(\mu\mathcal{F})$,

(d) $\nu\mathcal{F} = \mathcal{F}(\nu\mathcal{F})$,

(e) if S is finite then there exists $M \in \mathbb{N}$ such that for all $m \geq M$, $\mu\mathcal{F} = \mathcal{F}^m(\emptyset)$, and

(f) if S is finite then there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $\nu\mathcal{F} = \mathcal{F}^n(S)$.

(g) if $\bigcup_{m\in\mathbb{N}} \mathcal{F}^m(\emptyset) \supseteq \mathcal{F}(\bigcup_{m\in\mathbb{N}} \mathcal{F}^m(\emptyset))$ then $\mu\mathcal{F} = \bigcup_{m\in\mathbb{N}} \mathcal{F}^m(\emptyset)$.

(h) if $\bigcap_{n\in\mathbb{N}} \mathcal{F}^n(S) \subseteq \mathcal{F}(\bigcap_{n\in\mathbb{N}} \mathcal{F}^n(S))$ then $\nu\mathcal{F} = \bigcap_{n\in\mathbb{N}} \mathcal{F}^n(S)$.

Proof.

(a) See, for example, [5, Theorem 2.35].

(b) See, for example, [5, Theorem 2.35].

(c) See, for example, [5, Theorem 2.35].

(d) See, for example, [5, Theorem 2.35].

(e) See, for example, [4, Lemma 8].

(f) See, for example, [4, Lemma 8].

(g) For all $n \in \mathbb{N}$, $\mathcal{F}^n(\emptyset) \subseteq \bigcup_{m\in\mathbb{N}} \mathcal{F}^m(\emptyset)$. Since $\mathcal{F}$ is monotone by assumption, $\mathcal{F}^{n+1}(\emptyset) \subseteq \mathcal{F}(\bigcup_{m\in\mathbb{N}} \mathcal{F}^m(\emptyset))$. Hence, $\bigcup_{n\in\mathbb{N}} \mathcal{F}^n(\emptyset) \subseteq \mathcal{F}(\bigcup_{m\in\mathbb{N}} \mathcal{F}^m(\emptyset))$. From the other assumption, namely $\bigcup_{m\in\mathbb{N}} \mathcal{F}^m(\emptyset) \supseteq \mathcal{F}(\bigcup_{m\in\mathbb{N}} \mathcal{F}^m(\emptyset))$, we can deduce that $\bigcup_{n\in\mathbb{N}} \mathcal{F}^n(\emptyset) = \mathcal{F}(\bigcup_{m\in\mathbb{N}} \mathcal{F}^m(\emptyset))$. This captures that $\mathcal{F}$ is continuous. Then, according to [5, Theorem 8.15], we have that $\mu\mathcal{F} = \bigcup_{m\in\mathbb{N}} \mathcal{F}^m(\emptyset)$.

(h) Similar to the previous case.

□

Theorem 3. *Let $\mathcal{T} = (S, \rightarrow, AP, L)$ be a transition system. For all $a \in AP$ and $\varphi, \psi \in CTL$,*

- $Sat_{\mathcal{T}}(a) = \{\, s \in S \mid a \in L(s) \,\}$
- $Sat_{\mathcal{T}}(\neg\varphi) = S \setminus Sat_{\mathcal{T}}(\varphi)$
- $Sat_{\mathcal{T}}(\varphi \wedge \psi) = Sat_{\mathcal{T}}(\varphi) \cap Sat_{\mathcal{T}}(\psi)$
- $Sat_{\mathcal{T}}(\exists \bigcirc \varphi) = \{\, s \in S \mid post_{\mathcal{T}}(s) \cap Sat_{\mathcal{T}}(\varphi) \neq \emptyset \,\}$
- $Sat_{\mathcal{T}}(\forall \bigcirc \varphi) = \{\, s \in S \mid post_{\mathcal{T}}(s) \neq \emptyset \wedge post_{\mathcal{T}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \,\}$

- $Sat_{\mathcal{T}}(\exists\Box\varphi)$ *is the largest* $U \subseteq S$ *satisfying*

$$U \subseteq \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) = \emptyset \vee post_{\mathcal{T}}(s) \cap U \neq \emptyset \,\}$$

- $Sat_{\mathcal{T}}(\exists\varphi \,\mathsf{U}\, \psi)$ *is the smallest* $U \subseteq S$ *satisfying*

$$U \supseteq Sat_{\mathcal{T}}(\psi) \cup \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) \cap U \neq \emptyset \,\}$$

Proof.

- Consider the CTL formula a. Then

$$\begin{aligned} Sat_{\mathcal{T}}(a) =& \{\, s \in S \mid s \models_{\mathcal{T}} a \,\} \\ =& \{\, s \in S \mid a \in L(s) \,\} \end{aligned}$$

- Consider the CTL formula $\neg\varphi$. Then

$$\begin{aligned} Sat_{\mathcal{T}}(\neg\varphi) =& \{\, s \in S \mid s \models_{\mathcal{T}} \neg\varphi \,\} \\ =& \{\, s \in S \mid s \not\models_{\mathcal{T}} \varphi \,\} \\ =& S \setminus \{\, s \in S \mid s \models_{\mathcal{T}} \varphi \,\} \\ =& S \setminus Sat_{\mathcal{T}}(\varphi) \end{aligned}$$

- Consider the CTL formula $\varphi \wedge \psi$. Then

$$\begin{aligned} Sat_{\mathcal{T}}(\varphi \wedge \psi) =& \{\, s \in S \mid s \models_{\mathcal{T}} \varphi \wedge \psi \,\} \\ =& \{\, s \in S \mid s \models_{\mathcal{T}} \varphi \wedge s \models_{\mathcal{T}} \psi \,\} \\ =& \{\, s \in S \mid s \models_{\mathcal{T}} \varphi \,\} \cap \{\, s \in S \mid s \models_{\mathcal{T}} \psi \,\} \\ =& Sat_{\mathcal{T}}(\varphi) \cap Sat_{\mathcal{T}}(\psi) \end{aligned}$$

- Consider the CTL formula $\exists \bigcirc \varphi$. Then

$$\begin{aligned} Sat_{\mathcal{T}}(\exists \bigcirc \varphi) =& \{\, s \in S \mid s \models_{\mathcal{T}} \exists \bigcirc \varphi \,\} \\ =& \{\, s \in S \mid \exists \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \wedge \pi[1] \models_{\mathcal{T}} \varphi \,\} \\ =& \{\, s \in S \mid \exists s' \in post_{\mathcal{T}}(s) : s' \models_{\mathcal{T}} \varphi \,\} \\ =& \{\, s \in S \mid \exists s' \in post_{\mathcal{T}}(s) : s' \in Sat_{\mathcal{T}}(\varphi) \,\} \\ =& \{\, s \in S \mid post_{\mathcal{T}}(s) \cap Sat_{\mathcal{T}}(\varphi) \neq \emptyset \,\} \end{aligned}$$

- Consider the CTL formula $\forall \bigcirc \varphi$. Then

$$\begin{aligned} Sat_{\mathcal{T}}(\forall \bigcirc \varphi) =& \{\, s \in S \mid s \models_{\mathcal{T}} \forall \bigcirc \varphi \,\} \\ =& \{\, s \in S \mid \forall \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \wedge \pi[1] \models_{\mathcal{T}} \varphi \,\} \\ =& \{\, s \in S \mid post_{\mathcal{T}}(s) \neq \emptyset \wedge \forall s' \in post_{\mathcal{T}}(s) : s' \models_{\mathcal{T}} \varphi \,\} \\ =& \{\, s \in S \mid post_{\mathcal{T}}(s) \neq \emptyset \wedge \forall s' \in post_{\mathcal{T}}(s) : s' \in Sat_{\mathcal{T}}(\varphi) \,\} \\ =& \{\, s \in S \mid post_{\mathcal{T}}(s) \neq \emptyset \wedge post_{\mathcal{T}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \,\} \end{aligned}$$

- Consider the CTL formula $\exists\Box\varphi$. Given the CTL formula φ, the function

$$\mathcal{F}_{\mathcal{T},\varphi} : 2^S \to 2^S$$

is defined by

$$\mathcal{F}_{\mathcal{T},\varphi}(U) = \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) = \emptyset \vee post_{\mathcal{T}}(s) \cap U \neq \emptyset \,\}.$$

Next, we show that the function $\mathcal{F}_{\mathcal{T},\varphi}$ is monotone, that is, for all $U, V \in 2^S$, if $U \subseteq V$ then $\mathcal{F}_{\mathcal{T},\varphi}(U) \subseteq \mathcal{F}_{\mathcal{T},\varphi}(V)$. Let $U, V \in 2^S$ and assume that $U \subseteq V$. Let $s \in \mathcal{F}_{\mathcal{T},\varphi}(U)$. To conclude that $\mathcal{F}_{\mathcal{T},\varphi}(U) \subseteq \mathcal{F}_{\mathcal{T},\varphi}(V)$, it remains to show that $s \in \mathcal{F}_{\mathcal{T},\varphi}(V)$. Since $s \in \mathcal{F}_{\mathcal{T},\varphi}(U)$, we have that $s \in Sat_{\mathcal{T}}(\varphi)$ and either $post_{\mathcal{T}}(s) = \emptyset$ or $post_{\mathcal{T}}(s) \cap U \neq \emptyset$. Since $U \subseteq V$, we can conclude that $post_{\mathcal{T}}(s) \cap U \neq \emptyset$ implies $post_{\mathcal{T}}(s) \cap V \neq \emptyset$. Hence, $s \in \mathcal{F}_{\mathcal{T},\varphi}(V)$. From Theorem 2(b) we can conclude that there exists a largest $U \in 2^S$ satisfying $U \subseteq \mathcal{F}_{\mathcal{T},\varphi}(U)$.

Since

$$\begin{aligned}
Sat_{\mathcal{T}}(\exists\Box\varphi) =& \{\, s \in S \mid s \models_{\mathcal{T}} \exists\Box\varphi \,\} \\
=& \{\, s \in S \mid \exists \pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \varphi \,\} \\
=& \{\, s \in S \mid s \models_{\mathcal{T}} \varphi \wedge post_{\mathcal{T}}(s) = \emptyset \,\} \cup \\
& \{\, s \in S \mid s \models_{\mathcal{T}} \varphi \wedge \exists s' \in post_{\mathcal{T}}(s) : \exists \pi \in Paths_{\mathcal{T}}(s') : \forall 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \varphi \,\} \\
=& \{\, s \in S \mid s \models_{\mathcal{T}} \varphi \wedge post_{\mathcal{T}}(s) = \emptyset \,\} \cup \\
& \{\, s \in S \mid s \models_{\mathcal{T}} \varphi \wedge \exists s' \in post_{\mathcal{T}}(s) : s' \models_{\mathcal{T}} \exists\Box\varphi \,\} \\
=& \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) = \emptyset \vee post_{\mathcal{T}}(s) \cap Sat_{\mathcal{T}}(\exists\Box\varphi) \neq \emptyset \,\} \\
=& \mathcal{F}_{\mathcal{T},\varphi}(Sat_{\mathcal{T}}(\exists\Box\varphi))
\end{aligned}$$

we can conclude that $Sat_{\mathcal{T}}(\exists\Box\varphi) \subseteq \mathcal{F}_{\mathcal{T},\varphi}(Sat_{\mathcal{T}}(\exists\Box\varphi))$.

Let $U \in 2^S$ satisfying $U \subseteq \mathcal{F}_{\mathcal{T},\varphi}(U)$. It remains to show that $U \subseteq Sat_{\mathcal{T}}(\exists\Box\varphi)$. First, we will show that for all $s \in U$ and $n \in \mathbb{N}$,

(a1) $\exists \pi_n \in Paths_{\mathcal{T}}(s) : |\pi_n| \leq n + 1$ or

(a2) $\exists \pi_n \in PathFrag_{\mathcal{T}}(s) : |\pi_n| = n + 1$

and

(b) $\forall 0 \leq i < |\pi_n| : \pi_n[i] \in U$ and

(c) $\forall 0 \leq i < j \leq n : \pi_i \sqsubseteq \pi_j$.

We prove this by induction on n. Let $s \in U$. We distinguish the following two cases.

- Let $n = 0$ (base case). We distinguish the following two cases.
  - If $post_{\mathcal{T}}(s) = \emptyset$ then $s \in Paths_{\mathcal{T}}(s)$ and (a1), (b) and (c) are satisfied.

* Otherwise, $post_{\mathcal{T}}(s) \neq \emptyset$. Then $s \in PathFrag_{\mathcal{T}}(s)$ and (a2), (b) and (c) are satisfied.

– Otherwise, $n > 0$ (induction step). By induction, (a1) or (a2), and (b), and (c) hold for $n-1$. We distinguish the following two cases.

  * Assume (a1), (b), and (c) hold for $n-1$. That is, $\exists \pi_{n-1} \in Paths_{\mathcal{T}}(s) : |\pi_{n-1}| \leq n$ and $\forall 0 \leq i < |\pi_{n-1}| : \pi_{n-1}[i] \in U$ and $\forall 0 \leq i < j \leq n-1 : \pi_i \sqsubseteq \pi_j$. Then we choose $\pi_n = \pi_{n-1}$. Then (a1), (b), and (c) hold for n.
  * Otherwise, (a2), (b), and (c) hold for $n-1$. That is, $\exists \pi_{n-1} \in PathFrag_{\mathcal{T}}(s) : |\pi_{n-1}| = n$ and $\forall 0 \leq i < |\pi_{n-1}| : \pi_{n-1}[i] \in U$ and $\forall 0 \leq i < j \leq n-1 : \pi_i \sqsubseteq \pi_j$. Let $s' = \pi_{n-1}[n-1]$. Then $s' \in U$. Since $U \subseteq \mathcal{F}_{\mathcal{T},\varphi}(U)$ by assumption, we have that $s' \in \mathcal{F}_{\mathcal{T},\varphi}(U)$. Hence, by definition,

$$s' \in Sat_{\mathcal{T}}(\varphi) \wedge (post_{\mathcal{T}}(s') = \emptyset \vee post_{\mathcal{T}}(s') \cap U \neq \emptyset). \tag{1}$$

    We distinguish the following two cases.

    · If $post_{\mathcal{T}}(s') = \emptyset$ then $\pi_{n-1} \in Paths_{\mathcal{T}}(s)$. We choose $\pi_n = \pi_{n-1}$. Then (a1), (b), and (c) hold for n.

    · Otherwise, $post_{\mathcal{T}}(s') \neq \emptyset$. From (1) we can conclude that $post_{\mathcal{T}}(s') \cap U \neq \emptyset$. Let $s'' \in post_{\mathcal{T}}(s') \cap U$. In this case, we choose $\pi_n = \pi_{n-1}s''$. Then (a2), (b), and (c) hold for n.

From the above we can conclude $U \subseteq Sat_{\mathcal{T}}(\exists\Box\varphi)$ as follows. Let $s \in U$. Then either for some $n \in \mathbb{N}$, (a1) and (b) hold, that is,

$$\exists n \in \mathbb{N} : \exists \pi_n \in Paths_{\mathcal{T}}(s) : |\pi_n| \leq n+1 \wedge \forall 0 \leq i < |\pi_n| : \pi_n[i] \in U$$

or for all $n \in \mathbb{N}$, (a2), (b) and (c) hold, that is

$$\forall n \in \mathbb{N} : \exists \pi_n \in PathFrag_{\mathcal{T}}(s) : |\pi_n| = n+1 \wedge \forall 0 \leq i < |\pi_n| : \pi_n[i] \in U \wedge \\ \forall 0 \leq i < j \leq n : \pi_i \sqsubseteq \pi_j.$$

In the latter case, for $\pi_\omega \in S^\omega$ with $\pi_\omega[i] = \pi_i[i]$ we have that

$$\pi_\omega \in Paths_{\mathcal{T}}(s) \wedge \forall 0 \leq i < |\pi_\omega| : \pi_\omega[i] \in U.$$

Hence, in both cases,

$$\exists \pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \in U.$$

Since $U \subseteq \mathcal{F}_{\mathcal{T},\varphi}(U)$ and $\mathcal{F}_{\mathcal{T},\varphi}(U) \subseteq Sat_{\mathcal{T}}(\varphi)$, we have that

$$\exists \pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \in Sat_{\mathcal{T}}(\varphi)$$

and, therefore, $s \in Sat_{\mathcal{T}}(\exists\Box\varphi)$.

- Consider the CTL formula $\exists\varphi \,\mathsf{U}\, \psi$. Given the CTL formulas φ and ψ, the function

$$\mathcal{G}_{\mathcal{T},\varphi,\psi} : 2^S \to 2^S$$

is defined by

$$\mathcal{G}_{\mathcal{T},\varphi,\psi}(U) = Sat_{\mathcal{T}}(\psi) \cup \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) \cap U \neq \emptyset \,\}.$$

Next, we show that the function $\mathcal{G}_{\mathcal{T},\varphi,\psi}$ is monotone, that is, for all $U, V \in 2^S$, if $U \subseteq V$ then $\mathcal{G}_{\mathcal{T},\varphi,\psi}(U) \subseteq \mathcal{G}_{\mathcal{T},\varphi,\psi}(V)$. Let $U, V \in 2^S$ and assume that $U \subseteq V$. Let $s \in \mathcal{G}_{\mathcal{T},\varphi,\psi}(U)$. To conclude that $\mathcal{G}_{\mathcal{T},\varphi,\psi}(U) \subseteq \mathcal{G}_{\mathcal{T},\varphi,\psi}(V)$, it remains to show that $s \in \mathcal{G}_{\mathcal{T},\varphi,\psi}(V)$. Since $s \in \mathcal{G}_{\mathcal{T},\varphi,\psi}(U)$, we have that $s \in Sat_{\mathcal{T}}(\varphi)$, or $s \in Sat_{\mathcal{T}}(\varphi)$ and $post_{\mathcal{T}}(s) \cap U \neq \emptyset$. Since $U \subseteq V$, we can conclude that $post_{\mathcal{T}}(s) \cap U \neq \emptyset$ implies $post_{\mathcal{T}}(s) \cap V \neq \emptyset$. Hence, $s \in \mathcal{G}_{\mathcal{T},\varphi,\psi}(V)$. From Theorem 2(a) we can conclude that there exists a smallest $U \in 2^S$ satisfying $U \supseteq \mathcal{G}_{\mathcal{T},\varphi,\psi}(U)$.

Since

$$\begin{aligned}
&Sat_{\mathcal{T}}(\exists\varphi \,\mathsf{U}\, \psi)\\
=&\{\, s \in S \mid s \models_{\mathcal{T}} \exists\varphi \,\mathsf{U}\, \psi \,\}\\
=&\{\, s \in S \mid \exists\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \psi \wedge \forall 0 \leq k < j : \pi[k] \models_{\mathcal{T}} \varphi \,\}\\
=&\{\, s \in S \mid \exists\pi \in Paths_{\mathcal{T}}(s) : \pi[0] \models_{\mathcal{T}} \psi \vee \exists 1 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \psi \wedge \pi[0] \models_{\mathcal{T}} \varphi \wedge \forall 1 \leq k < j : \pi[k] \models
\end{aligned}$$

$$\begin{aligned}
=&\{\, s \in S \mid s \models_{\mathcal{T}} \psi \vee (s \models_{\mathcal{T}} \varphi \wedge \exists\pi \in Paths_{\mathcal{T}}(s) : \exists 1 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \psi \wedge \forall 1 \leq k < j : \pi[k] \models_{\mathcal{T}} \varphi)\\
=&Sat_{\mathcal{T}}(\psi) \cup \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid \exists s' \in post_{\mathcal{T}}(s) : \exists\pi' \in Paths_{\mathcal{T}}(s') : \exists 0 \leq j < |\pi'| : \pi'[j] \models_{\mathcal{T}} \psi \wedge \forall 0 \leq k <\\
=&Sat_{\mathcal{T}}(\psi) \cup \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid \exists s' \in post_{\mathcal{T}}(s) : s' \models_{\mathcal{T}} \exists\varphi \,\mathsf{U}\, \psi \,\})\\
=&Sat_{\mathcal{T}}(\psi) \cup \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) \cap Sat_{\mathcal{T}}(\exists\varphi \,\mathsf{U}\, \psi) \neq \emptyset \,\})\\
=&\mathcal{G}_{\mathcal{T},\varphi,\psi}(Sat_{\mathcal{T}}(\exists\varphi \,\mathsf{U}\, \psi))
\end{aligned}$$

we can conclude that $Sat_{\mathcal{T}}(\exists\varphi \,\mathsf{U}\, \psi) \supseteq \mathcal{G}_{\mathcal{T},\varphi,\psi}(Sat_{\mathcal{T}}(\exists\varphi \,\mathsf{U}\, \psi))$.

Let $U \in 2^S$ satisfying $U \supseteq \mathcal{G}_{\mathcal{T},\varphi,\psi}(U)$. It remains to show that $U \supseteq Sat_{\mathcal{T}}(\exists\varphi \,\mathsf{U}\, \psi)$. First, we will show that for all $s \notin U$ and $n \in \mathbb{N}$,

$$\forall\pi_n \in Paths_{\mathcal{T}}(s) \cup PathFrag_{\mathcal{T}}(s) : |\pi_n| \leq n{+}1 \Rightarrow \forall 0 \leq j < |\pi_n| : \pi_n[j] \not\models_{\mathcal{T}} \psi \vee \exists 0 \leq k < j : \pi_n[k] \not\models_{\mathcal{T}} \varphi \tag{2}$$

We prove this by induction on n. Let $s \notin U$. Since $U \supseteq \mathcal{G}_{\mathcal{T},\varphi,\psi}(U)$ by assumption, we have that $s \notin \mathcal{G}_{\mathcal{T},\varphi,\psi}(U)$ and, hence, by definition

$$s \notin Sat_{\mathcal{T}}(\psi) \wedge (s \notin Sat_{\mathcal{T}}(\varphi) \vee post_{\mathcal{T}}(s) \cap U = \emptyset). \tag{3}$$

We distinguish two cases.

- Let $n = 0$ (base case). Since $\pi_0 = s$ and $s \notin Sat_{\mathcal{T}}(\psi)$, we can conclude $\pi_0[0] \not\models_{\mathcal{T}} \psi$, which implies (2).

– Otherwise, $n > 0$ (inductive step). Let $\pi_n \in Paths_{\mathcal{T}}(s) \cup PathFrag_{\mathcal{T}}(s)$. We distinguish the following two cases.
  * If $|\pi_n| \leq n$ then (2) holds by induction.
  * Otherwise, $|\pi_n| = n + 1$. Recall from (3) that $s \notin Sat_{\mathcal{T}}(\psi)$. We distinguish two cases.
    · If $s \notin Sat_{\mathcal{T}}(\varphi)$ then $\pi_n[0] \not\models_{\mathcal{T}} \psi$ and $\pi_n[0] \not\models_{\mathcal{T}} \varphi$ and, therefore, (2).
    · Otherwise, $s \in Sat_{\mathcal{T}}(\varphi)$. From (3) we can conclude that $post_{\mathcal{T}}(s) \cap U = \emptyset$. Since $|\pi_n| = n + 1$, we have that $\pi_n = s\pi_{n-1}$, where $\pi_{n-1} \in Paths_{\mathcal{T}}(s') \cup PathFrag_{\mathcal{T}}(s')$ for some $s' \in post_{\mathcal{T}}(s)$. Because $post_{\mathcal{T}}(s) \cap U = \emptyset$, we have that $s' \notin U$. By induction, (2) holds for π_{n-1}. Furthermore, from $s \notin Sat_{\mathcal{T}}(\psi)$ we can conclude that $\pi_n[0] \not\models_{\mathcal{T}} \psi$. Combining these two fact, we can conclude that (2) holds for π_n.

From (2) we can conclude $U \supseteq Sat_{\mathcal{T}}(\exists\varphi \,\mathsf{U}\, \psi)$ as follows. Towards a contradiction, assume that $s \in Sat_{\mathcal{T}}(\exists\varphi \,\mathsf{U}\, \psi)$ and $s \notin U$. Then

$$\exists\pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \psi \wedge \forall 0 \leq k < j : \pi[k] \models_{\mathcal{T}} \varphi \tag{4}$$

We distinguish two cases.

– Let $\pi \in S^*$. Then $|\pi| = n + 1$ for some $n \in \mathbb{N}$. Hence, (4) contradicts (2).
– Let $\pi \in S^\omega$. Then $\pi[\ldots j] \in PathFrag_{\mathcal{T}}(s)$ with $\pi[\ldots j][j] \models_{\mathcal{T}} \psi$ and $\forall 0 \leq k < j : \pi[\ldots j][k] \models_{\mathcal{T}} \varphi$, also contradicting (2).

□

7 Lower- and upperbounds

Regularly, JPF runs out of memory. Sometimes, we stop JPF as it is taking too much time. In both cases, JPF does not produce the complete transition system, but only a part of it. We model this as a partial transition system.

Definition 5. A partial transition system is a tuple $(S, F, \rightarrow, AP, L)$ consisting of

- a finite set S of *states*,
- a set $F \subseteq S$ of *fully explored states*,
- a transition relation $\rightarrow \subseteq S \times S$,
- a set AP of *atomic propositions*, and
- a *labelling function* $L : S \rightarrow 2^{AP}$.

The difference between a partial transition system and an ordinary transition system is the set F of fully explored states. A transition system is called partial because the states $S \setminus F$ are not fully explored yet, that is, these states *have* transitions that have not been explored yet, that is, they are not part of $\rightarrow$.

Recall that for a transition system $\mathcal{T} = (S', \rightarrow', AP, L')$ and a state $s \in S$, the set $post_{\mathcal{T}}(s)$ is defined by

$$post_{\mathcal{T}}(s) = \{\, s' \in S \mid s \rightarrow s' \,\}$$

This notion carries over to partial transition systems.

Definition 6. Transition system $\mathcal{T} = (S', \rightarrow', AP, L')$ completes the partial transition system $\mathcal{P} = (S, F, \rightarrow, AP, L)$ if

- $S \subseteq S'$,
- for all $s \in F$, $post_{\mathcal{P}}(s) = post_{\mathcal{T}}(s)$,
- for all $s \in S \setminus F$, $post_{\mathcal{P}}(s) \subsetneqq post_{\mathcal{T}}(s)$, and
- $L' \restriction S = L$.

All the states of the partial transition system $\mathcal{P}$ are also part of the transition system $\mathcal{T}$. If a state in $\mathcal{P}$ is fully explored, then it has the same outgoing transitions in $\mathcal{P}$ and $\mathcal{T}$. Otherwise, it has more outgoing transitions in $\mathcal{T}$ than in $\mathcal{P}$.

Given a partial transition system $\mathcal{P}$, a state s of that system, and a CTL formula φ, we want to determine if φ holds in s. Note that all transition systems which complete $\mathcal{P}$ contain state s. We distinguish the following three cases:

- for all transition systems which complete $\mathcal{P}$ the formula φ holds in s,
- for none of the transition systems which complete $\mathcal{P}$ the formula φ holds in s, and
- for some transition systems which complete $\mathcal{P}$ the formula φ holds in s and for some transition systems which complete $\mathcal{P}$ the formula φ does not hold in s.

In the first case, formula φ holds in state s of the partial transition system $\mathcal{P}$. In the second case, φ does not hold in s. In the third case, there is insufficient information to determine whether φ holds in s.

Recall that for CTL formula φ the set $Sat_{\mathcal{T}}(\varphi)$ is defined as

$$Sat_{\mathcal{T}}(\varphi) = \{\, s \in S' \mid s \models_{\mathcal{T}} \varphi \,\}$$

Then φ holds in all states in S that belong to

$$\bigcap \{\, Sat_{\mathcal{T}}(\varphi) \mid \mathcal{T} \text{ completes } \mathcal{P} \,\}$$

and φ does not hold in all states in S that do *not* belong to

$$\bigcup \{\, Sat_{\mathcal{T}}(\varphi) \mid \mathcal{T} \text{ completes } \mathcal{P} \,\}$$

Since there are in general infinitely many transition systems that complete $\mathcal{P}$, we will approximate these two sets. We will approximate the former from below, that is, we will give a lowerbound, and the latter from above, that is, we give an upperbound. Next, we will define the sets $Sat^{\ell}_{\mathcal{P}}(\varphi)$ and $Sat^{u}_{\mathcal{P}}(\varphi)$. As we will show in Theorem 5,

$$Sat^{\ell}_{\mathcal{P}}(\varphi) \subseteq Sat_{\mathcal{T}}(\varphi) \cap S \subseteq Sat^{u}_{\mathcal{P}}(\varphi)$$

for all $\mathcal{T}$ that complete $\mathcal{P}$. As a consequence, if $s \in Sat^{\ell}_{\mathcal{P}}(\varphi)$ then φ holds in s. Furthermore, if $s \notin Sat^{u}_{\mathcal{P}}(\varphi)$ then φ does not hold in s.

Definition 7. Let $\mathcal{P} = (S, F, \rightarrow, AP, L)$ be a partial transition system. For all $a \in AP$ and φ, $\psi \in CTL$,

- $Sat^{\ell}_{\mathcal{P}}(a) = \{\, s \in S \mid a \in L(s) \,\}$
- $Sat^{u}_{\mathcal{P}}(a) = \{\, s \in S \mid a \in L(s) \,\}$
- $Sat^{\ell}_{\mathcal{P}}(\neg\varphi) = S \setminus Sat^{u}_{\mathcal{P}}(\varphi)$
- $Sat^{u}_{\mathcal{P}}(\neg\varphi) = S \setminus Sat^{\ell}_{\mathcal{P}}(\varphi)$
- $Sat^{\ell}_{\mathcal{P}}(\varphi \wedge \psi) = Sat^{\ell}_{\mathcal{P}}(\varphi) \cap Sat^{\ell}_{\mathcal{P}}(\psi)$
- $Sat^{u}_{\mathcal{P}}(\varphi \wedge \psi) = Sat^{u}_{\mathcal{P}}(\varphi) \cap Sat^{u}_{\mathcal{P}}(\psi)$
- $Sat^{\ell}_{\mathcal{P}}(\exists \bigcirc \varphi) = \{\, s \in S \mid post_{\mathcal{P}}(s) \cap Sat^{\ell}_{\mathcal{P}}(\varphi) \neq \emptyset \,\}$
- $Sat^{u}_{\mathcal{P}}(\exists \bigcirc \varphi) = (S \setminus F) \cup \{\, s \in F \mid post_{\mathcal{P}}(s) \cap Sat^{u}_{\mathcal{P}}(\varphi) \neq \emptyset \,\}$
- $Sat^{\ell}_{\mathcal{P}}(\forall \bigcirc \varphi) = \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat^{\ell}_{\mathcal{P}}(\varphi) \,\}$
- $Sat^{u}_{\mathcal{P}}(\forall \bigcirc \varphi) = (S \setminus F) \cup \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat^{u}_{\mathcal{P}}(\varphi) \,\}$
- $Sat^{\ell}_{\mathcal{P}}(\exists\Box\varphi)$ is the largest $U \subseteq S$ satisfying

$$U \subseteq \{\, s \in Sat^{\ell}_{\mathcal{P}}(\varphi) \mid (s \in F \wedge post_{\mathcal{P}}(s) = \emptyset) \vee post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\}$$

- $Sat^{u}_{\mathcal{P}}(\exists\Box\varphi)$ is the largest $U \subseteq S$ satisfying

$$U \subseteq \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \vee post_{\mathcal{P}}(s) = \emptyset \vee post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\}$$

- $Sat^{\ell}_{\mathcal{P}}(\exists\varphi \,\mathsf{U}\, \psi)$ is the smallest $U \subseteq S$ satisfying

$$U \supseteq Sat^{\ell}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{\ell}_{\mathcal{P}}(\varphi) \mid post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\}$$

- $Sat^{u}_{\mathcal{P}}(\exists\varphi \,\mathsf{U}\, \psi)$ is the smallest $U \subseteq S$ satisfying

$$U \supseteq Sat^{u}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \vee post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\}$$

Given the CTL formula φ, the functions

$$\mathcal{F}^{\ell}_{\mathcal{P},\varphi}, \mathcal{F}^{u}_{\mathcal{P},\varphi} : 2^S \to 2^S$$

are defined by

$$\begin{aligned}\mathcal{F}^{\ell}_{\mathcal{P},\varphi}(U) =& \{\, s \in Sat^{\ell}_{\mathcal{P}}(\varphi) \mid (s \in F \wedge post_{\mathcal{P}}(s) = \emptyset) \vee post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\} \\ \mathcal{F}^{u}_{\mathcal{P},\varphi}(U) =& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \vee post_{\mathcal{P}}(s) = \emptyset \vee post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\}\end{aligned}$$

Given the CTL formulas φ and ψ, the functions

$$\mathcal{G}^{\ell}_{\mathcal{P},\varphi,\psi}, \mathcal{G}^{u}_{\mathcal{P},\varphi,\psi} : 2^S \to 2^S$$

are defined by

$$\begin{aligned}\mathcal{G}^{\ell}_{\mathcal{P},\varphi,\psi}(U) =& Sat^{\ell}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{\ell}_{\mathcal{P}}(\varphi) \mid post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\} \\ \mathcal{G}^{u}_{\mathcal{P},\varphi,\psi}(U) =& Sat^{u}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \vee post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\}\end{aligned}$$

As in the proof of Theorem 3, we can show that these functions are monotone.

We assume that the transition systems are finitely branching, that is, each state has finitely many outgoing transitions. That is, for each $s \in S$, the set $post_{\mathcal{T}}(s)$ is finite.

In our development, we use the following theorem that is known as Cantor's intersection theorem.

Theorem 4. *Assume that the sequence of sets $(U_n)_{n\in\mathbb{N}}$ is decreasing, that is, for all $n \in \mathbb{N}$, $U_n \supseteq U_{n+1}$. If U_n is nonempty and finite for all $n \in \mathbb{N}$, then $\bigcap_{n\in\mathbb{N}} U_n$ is nonempty.*

Proof. See, for example, [6, Theorem 4.3.9]. □

Theorem 5. *For each partial transition system $\mathcal{P} = (S, F, \to, AP, L)$ and transition system $\mathcal{T}$ that completes $\mathcal{P}$ and $\varphi \in CTL$,*

$$Sat^{\ell}_{\mathcal{P}}(\varphi) \subseteq Sat_{\mathcal{T}}(\varphi) \cap S \subseteq Sat^{u}_{\mathcal{P}}(\varphi).$$

Proof. We prove this theorem by structural induction on φ. We distinguish the following cases.

- Consider the CTL formula a. Then

$$\begin{aligned}Sat^{\ell}_{\mathcal{P}}(a) =& \{\, s \in S \mid a \in L(s) \,\} \\ =& Sat_{\mathcal{T}}(a) \cap S \\ =& \{\, s \in S \mid a \in L(s) \,\} \\ =& Sat^{u}_{\mathcal{P}}(a).\end{aligned}$$

- Consider the CTL formula $\neg\varphi$. Then

$$\begin{aligned}
Sat^{\ell}_{\mathcal{P}}(\neg\varphi) =& S \setminus Sat^{u}_{\mathcal{P}}(\varphi) \\
\subseteq& S \setminus (Sat_{\mathcal{T}}(\varphi) \cap S) && \text{[induction]} \\
=& Sat_{\mathcal{T}}(\neg\varphi) \cap S \\
=& S \setminus (Sat_{\mathcal{T}}(\varphi) \cap S) \\
\subseteq& S \setminus Sat^{\ell}_{\mathcal{P}}(\varphi) && \text{[induction]} \\
=& Sat^{u}_{\mathcal{P}}(\neg\varphi).
\end{aligned}$$

- Consider the CTL formula $\varphi \wedge \psi$. Then

$$\begin{aligned}
Sat^{\ell}_{\mathcal{P}}(\varphi \wedge \psi) =& Sat^{\ell}_{\mathcal{P}}(\varphi) \cap Sat^{\ell}_{\mathcal{P}}(\psi) \\
\subseteq& (Sat_{\mathcal{T}}(\varphi) \cap S) \cap (Sat_{\mathcal{T}}(\psi) \cap S) && \text{[induction]} \\
=& Sat_{\mathcal{T}}(\varphi \wedge \psi) \cap S \\
=& (Sat_{\mathcal{T}}(\varphi) \cap S) \cap (Sat_{\mathcal{T}}(\psi) \cap S) \\
\subseteq& Sat^{u}_{\mathcal{P}}(\varphi) \cap Sat^{u}_{\mathcal{P}}(\psi) && \text{[induction]} \\
=& Sat^{u}_{\mathcal{P}}(\varphi \wedge \psi).
\end{aligned}$$

- Consider the CTL formula $\exists \bigcirc \varphi$. Then

$$\begin{aligned}
Sat^{\ell}_{\mathcal{P}}(\exists \bigcirc \varphi) =& \{\, s \in S \mid post_{\mathcal{P}}(s) \cap Sat^{\ell}_{\mathcal{P}}(\varphi) \neq \emptyset \,\} \\
\subseteq& \{\, s \in S \mid post_{\mathcal{P}}(s) \cap Sat_{\mathcal{T}}(\varphi) \cap S \neq \emptyset \,\} && \text{[induction]} \\
=& \{\, s \in S \mid post_{\mathcal{P}}(s) \cap Sat_{\mathcal{T}}(\varphi) \neq \emptyset \,\} && [post_{\mathcal{P}}(s) \subseteq S] \\
\subseteq& \{\, s \in S \mid post_{\mathcal{T}}(s) \cap Sat_{\mathcal{T}}(\varphi) \neq \emptyset \,\} && [post_{\mathcal{P}}(s) \subseteq post_{\mathcal{T}}(s)] \\
=& Sat_{\mathcal{T}}(\exists \bigcirc \varphi) \cap S \\
=& \{\, s \in S \mid post_{\mathcal{T}}(s) \cap Sat_{\mathcal{T}}(\varphi) \neq \emptyset \,\} \\
=& \{\, s \in F \mid post_{\mathcal{T}}(s) \cap Sat_{\mathcal{T}}(\varphi) \neq \emptyset \,\} \cup \\
& \{\, s \in S \setminus F \mid post_{\mathcal{T}}(s) \cap Sat_{\mathcal{T}}(\varphi) \neq \emptyset \,\} \\
\subseteq& \{\, s \in F \mid post_{\mathcal{T}}(s) \cap Sat_{\mathcal{T}}(\varphi) \neq \emptyset \,\} \cup \\
& S \setminus F \\
=& \{\, s \in F \mid post_{\mathcal{P}}(s) \cap Sat_{\mathcal{T}}(\varphi) \neq \emptyset \,\} \cup && [post_{\mathcal{P}}(s) = post_{\mathcal{T}}(s)] \\
& S \setminus F \\
=& \{\, s \in F \mid post_{\mathcal{P}}(s) \cap Sat_{\mathcal{T}}(\varphi) \cap S \neq \emptyset \,\} \cup && [post_{\mathcal{P}}(s) \subseteq S] \\
& S \setminus F \\
\subseteq& \{\, s \in F \mid post_{\mathcal{P}}(s) \cap Sat^{u}_{\mathcal{P}}(\varphi) \neq \emptyset \,\} \cup && \text{[induction]} \\
& S \setminus F \\
=& Sat^{u}_{\mathcal{P}}(\exists \bigcirc \varphi).
\end{aligned}$$

- Consider the CTL formula $\forall \bigcirc \varphi$. Then

$$\begin{aligned}
Sat^{\ell}_{\mathcal{P}}(\forall \bigcirc \varphi) =& \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat^{\ell}_{\mathcal{P}}(\varphi) \,\} \\
\subseteq& \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \cap S \,\} && \text{[induction]} \\
=& \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \,\} \\
\subseteq& \{\, s \in F \mid post_{\mathcal{T}}(s) \neq \emptyset \wedge post_{\mathcal{T}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \,\} && [post_{\mathcal{P}}(s) = post_{\mathcal{T}}(s)] \\
=& Sat_{\mathcal{T}}(\forall \bigcirc \varphi) \cap S \\
=& \{\, s \in S \mid post_{\mathcal{T}}(s) \neq \emptyset \wedge post_{\mathcal{T}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \,\} \\
=& \{\, s \in F \mid post_{\mathcal{T}}(s) \neq \emptyset \wedge post_{\mathcal{T}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \,\} \cup \\
& \{\, s \in S \setminus F \mid post_{\mathcal{T}}(s) \neq \emptyset \wedge post_{\mathcal{T}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \,\} \\
\subseteq& \{\, s \in F \mid post_{\mathcal{T}}(s) \neq \emptyset \wedge post_{\mathcal{T}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \,\} \cup \\
& S \setminus F \\
=& \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \,\} \cup && [post_{\mathcal{P}}(s) = post_{\mathcal{T}}(s)] \\
& S \setminus F \\
=& \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat_{\mathcal{T}}(\varphi) \cap S \,\} \cup && [post_{\mathcal{P}}(s) \subseteq S] \\
& S \setminus F \\
\subseteq& \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat^{u}_{\mathcal{P}}(\varphi) \,\} \cup && \text{[induction]} \\
& S \setminus F \\
=& Sat^{u}_{\mathcal{P}}(\exists \bigcirc \varphi).
\end{aligned}$$

- Consider the CTL formula $\exists \Box \varphi$. Assume that $\mathcal{T}$ has S' as its set of states. First, we show that for all $n \in \mathbb{N}$,

$$(\mathcal{F}^{\ell}_{\mathcal{P},\varphi})^n(S) \subseteq (\mathcal{F}_{\mathcal{T},\varphi})^n(S') \cap S \subseteq (\mathcal{F}^{u}_{\mathcal{P},\varphi})^n(S)$$

by induction on n. It obviously holds for $n = 0$ (base case). Assume that $n > 0$ (induction

step). Then

$$
\begin{aligned}
(\mathcal{F}^{\ell}_{\mathcal{P},\varphi})^n(S) =& \{\, s \in Sat^{\ell}_{\mathcal{P}}(\varphi) \mid (s \in F \wedge post_{\mathcal{P}}(s) = \emptyset) \vee post_{\mathcal{P}}(s) \cap (\mathcal{F}^{\ell}_{\mathcal{P},\varphi})^{n-1}(S) \neq \emptyset \,\} \\
\subseteq& \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid (s \in F \wedge post_{\mathcal{P}}(s) = \emptyset) \vee post_{\mathcal{P}}(s) \cap (\mathcal{F}^{\ell}_{\mathcal{P},\varphi})^{n-1}(S) \neq \emptyset \,\} \cap S \\
& [Sat^{\ell}_{\mathcal{P}}(\varphi) \subseteq Sat_{\mathcal{T}}(\varphi) \cap S \text{ by induction}] \\
\subseteq& \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid (s \in F \wedge post_{\mathcal{P}}(s) = \emptyset) \vee post_{\mathcal{T}}(s) \cap (\mathcal{F}^{\ell}_{\mathcal{P},\varphi})^{n-1}(S) \neq \emptyset \,\} \cap S \\
& [post_{\mathcal{P}}(s) \subseteq post_{\mathcal{T}}(s)] \\
\subseteq& \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid (s \in F \wedge post_{\mathcal{P}}(s) = \emptyset) \vee post_{\mathcal{T}}(s) \cap (\mathcal{F}_{\mathcal{T},\varphi})^{n-1}(S') \neq \emptyset \,\} \cap S \\
& [\text{by induction } (\mathcal{F}^{\ell}_{\mathcal{P},\varphi})^{n-1}(S) \subseteq (\mathcal{F}_{\mathcal{T},\varphi})^{n-1}(S') \cap S \subseteq (\mathcal{F}_{\mathcal{T},\varphi})^{n-1}(S')] \\
\subseteq& \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) = \emptyset \vee post_{\mathcal{T}}(s) \cap (\mathcal{F}_{\mathcal{T},\varphi})^{n-1}(S') \neq \emptyset \,\} \cap S \\
& [post_{\mathcal{P}}(s) = post_{\mathcal{T}}(s) \text{ for all } s \in F] \\
=& (\mathcal{F}_{\mathcal{T},\varphi})^n(S') \cap S \\
=& \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) = \emptyset \vee post_{\mathcal{T}}(s) \cap (\mathcal{F}_{\mathcal{T},\varphi})^{n-1}(S') \neq \emptyset \,\} \cap S \\
\subseteq& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid post_{\mathcal{T}}(s) = \emptyset \vee post_{\mathcal{T}}(s) \cap (\mathcal{F}_{\mathcal{T},\varphi})^{n-1}(S') \neq \emptyset \,\} \\
& [Sat_{\mathcal{T}}(\varphi) \cap S \subseteq Sat^{u}_{\mathcal{P}}(\varphi) \text{ by induction}] \\
\subseteq& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \,\} \cup \\
& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in F \wedge (post_{\mathcal{T}}(s) = \emptyset \vee post_{\mathcal{T}}(s) \cap (\mathcal{F}_{\mathcal{T},\varphi})^{n-1}(S') \neq \emptyset) \,\} \\
=& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \,\} \cup \\
& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in F \wedge (post_{\mathcal{P}}(s) = \emptyset \vee post_{\mathcal{P}}(s) \cap (\mathcal{F}_{\mathcal{T},\varphi})^{n-1}(S') \neq \emptyset) \,\} \\
& [post_{\mathcal{P}}(s) = post_{\mathcal{T}}(s) \text{ for all } s \in F] \\
\subseteq& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \,\} \cup \\
& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in F \wedge (post_{\mathcal{P}}(s) = \emptyset \vee post_{\mathcal{P}}(s) \cap (\mathcal{F}^{u}_{\mathcal{P},\varphi})^{n-1}(S) \neq \emptyset) \,\} \\
& [post(s) \subseteq S \text{ and } (\mathcal{F}_{\mathcal{T},\varphi})^{n-1}(S') \cap S \subseteq (\mathcal{F}^{u}_{\mathcal{P},\varphi})^{n-1}(S) \text{ by induction}] \\
=& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \vee (s \in F \wedge (post_{\mathcal{P}}(s) = \emptyset \vee post_{\mathcal{P}}(s) \cap (\mathcal{F}^{u}_{\mathcal{P},\varphi})^{n-1}(S)) \neq \emptyset)) \,\} \\
=& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \vee post_{\mathcal{P}}(s) = \emptyset \vee post_{\mathcal{P}}(s) \cap (\mathcal{F}^{u}_{\mathcal{P},\varphi})^{n-1}(S) \neq \emptyset \,\} \\
=& (\mathcal{F}^{u}_{\mathcal{P},\varphi})^n(S).
\end{aligned}
$$

Next, we show that

$$\bigcap_{n\in\mathbb{N}} (\mathcal{F}_{\mathcal{T},\varphi})^n(S') \subseteq \mathcal{F}_{\mathcal{T},\varphi}(\bigcap_{n\in\mathbb{N}} (\mathcal{F}_{\mathcal{T},\varphi})^n(S')). \tag{5}$$

Let $s \in \bigcap_{n\in\mathbb{N}} (\mathcal{F}_{\mathcal{T},\varphi})^n(S')$. Then $s \in (\mathcal{F}_{\mathcal{T},\varphi})^n(S')$ for all $n \in \mathbb{N}$. Hence, $s \in Sat_{\mathcal{T}}(\varphi)$ and either $post_{\mathcal{T}}(s) = \emptyset$ or $post_{\mathcal{T}}(s) \cap (\mathcal{F}_{\mathcal{T},\varphi})^n(S') \neq \emptyset$. We distinguish the following two cases.

- Assume $post_{\mathcal{T}}(s) = \emptyset$. Since $s \in Sat_{\mathcal{T}}(\varphi)$, we have that $s \in \mathcal{F}_{\mathcal{T},\varphi}(\bigcap_{n\in\mathbb{N}} (\mathcal{F}_{\mathcal{T},\varphi})^n(S'))$.
- Otherwise, $post_{\mathcal{T}}(s) \neq \emptyset$. Hence, $s \in Sat_{\mathcal{T}}(\varphi)$ and for all $n \in \mathbb{N}$, $post_{\mathcal{T}}(s) \cap (\mathcal{F}_{\mathcal{T},\varphi})^n(S') \neq \emptyset$. Note that the sequence of sets $((\mathcal{F}_{\mathcal{T},\varphi})^n(S'))_{n\in\mathbb{N}}$ is decreasing as

the function $\mathcal{F}_{\mathcal{T},\varphi}$ is monotone. Since the set $post_{\mathcal{T}}(s)$ is finite, the sets $post_{\mathcal{T}}(s) \cap (\mathcal{F}_{\mathcal{T},\varphi})^n(S')$ are finite as well. According to Theorem 4, $\bigcap_{n\in\mathbb{N}} post_{\mathcal{T}}(s) \cap (\mathcal{F}_{\mathcal{T},\varphi})^n(S') \neq \emptyset$. Therefore, $post_{\mathcal{T}}(s) \cap \bigcap_{n\in\mathbb{N}} (\mathcal{F}_{\mathcal{T},\varphi})^n(S') \neq \emptyset$ and, hence, $s \in \mathcal{F}_{\mathcal{T},\varphi}(\bigcap_{n\in\mathbb{N}} (\mathcal{F}_{\mathcal{T},\varphi})^n(S'))$.

Since the set S is finite and the function $\mathcal{F}^{\ell}_{\mathcal{P},\varphi}$ is monotone, according to Theorem 2(f), $Sat^{\ell}_{\mathcal{P}}(\exists\Box\varphi) = (\mathcal{F}^{\ell}_{\mathcal{P},\varphi})^n(S)$ for all $n \geq N$ for some $N \in \mathbb{N}$. Hence, $Sat^{\ell}_{\mathcal{P}}(\exists\Box\varphi) = \bigcap_{n\in\mathbb{N}} (\mathcal{F}^{\ell}_{\mathcal{P},\varphi})^n(S)$. Similarly, $Sat^{u}_{\mathcal{P}}(\exists\Box\varphi) = \bigcap_{n\in\mathbb{N}} (\mathcal{F}^{u}_{\mathcal{P},\varphi})^n(S)$. Since $\mathcal{F}_{\mathcal{T},\varphi}$ is monotone and (5), we can conclude from Theorem 2(h) that $Sat_{\mathcal{T}}(\exists\Box\varphi) = \bigcap_{n\in\mathbb{N}} (\mathcal{F}_{\mathcal{T},\varphi})^n(S')$.

$$
\begin{aligned}
Sat^{\ell}_{\mathcal{P}}(\exists\Box\varphi) &= \bigcap_{n\in\mathbb{N}} (\mathcal{F}^{\ell}_{\mathcal{P},\varphi})^n(S) \\
&\subseteq \bigcap_{n\in\mathbb{N}} (\mathcal{F}_{\mathcal{T},\varphi})^n(S') \cap S \\
&= Sat_{\mathcal{T}}(\exists\Box\varphi) \cap S \\
&= \bigcap_{n\in\mathbb{N}} (\mathcal{F}_{\mathcal{T},\varphi})^n(S') \cap S \\
&\subseteq \bigcap_{n\in\mathbb{N}} (\mathcal{F}^{u}_{\mathcal{P},\varphi})^n(S) \\
&= Sat^{u}_{\mathcal{P}}(\exists\Box\varphi).
\end{aligned}
$$

- Consider the CTL formula $\exists\varphi \,\mathsf{U}\, \psi$. First, we show that for all $n \in \mathbb{N}$,

$$(\mathcal{G}^{\ell}_{\mathcal{P},\varphi,\psi})^n(\emptyset) \subseteq (\mathcal{G}_{\mathcal{T},\varphi,\psi})^n(\emptyset) \cap S \subseteq (\mathcal{G}^{u}_{\mathcal{P},\varphi,\psi})^n(\emptyset)$$

by induction on n. It obviously holds for $n = 0$ (base case). Assume that $n > 0$ (inductive

step). Then

$$
\begin{aligned}
(\mathcal{G}^{\ell}_{\mathcal{P},\varphi,\psi})^n(\emptyset) =& Sat^{\ell}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{\ell}_{\mathcal{P}}(\varphi) \mid post_{\mathcal{P}}(s) \cap (\mathcal{G}^{\ell}_{\mathcal{P},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\} \\
\subseteq& (Sat_{\mathcal{T}}(\psi) \cup \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{P}}(s) \cap (\mathcal{G}^{\ell}_{\mathcal{P},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\}) \cap S \\
& [Sat^{\ell}_{\mathcal{P}}(\varphi) \subseteq Sat_{\mathcal{T}}(\varphi) \cap S \text{ and } Sat^{\ell}_{\mathcal{P}}(\psi) \subseteq Sat_{\mathcal{T}}(\psi) \cap S \text{ by induction}] \\
\subseteq& (Sat_{\mathcal{T}}(\psi) \cup \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) \cap (\mathcal{G}^{\ell}_{\mathcal{T},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\}) \cap S \\
& [post_{\mathcal{P}}(s) \subseteq post_{\mathcal{T}}(s)] \\
\subseteq& (Sat_{\mathcal{T}}(\psi) \cup \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) \cap (\mathcal{G}_{\mathcal{T},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\}) \cap S \\
& [\text{by induction } (\mathcal{G}^{\ell}_{\mathcal{P},\varphi,\psi})^{n-1}(\emptyset) \subseteq (\mathcal{G}_{\mathcal{T},\varphi})^{n-1}(\emptyset) \cap S \subseteq (\mathcal{G}_{\mathcal{T},\varphi})^{n-1}(\emptyset)] \\
=& (\mathcal{G}_{\mathcal{T},\varphi,\psi})^n(\emptyset) \cap S \\
=& (Sat_{\mathcal{T}}(\psi) \cup \{\, s \in Sat_{\mathcal{T}}(\varphi) \mid post_{\mathcal{T}}(s) \cap (\mathcal{G}_{\mathcal{T},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\}) \cap S \\
=& Sat^{u}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid post_{\mathcal{T}}(s) \cap (\mathcal{G}_{\mathcal{T},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\} \\
& [Sat_{\mathcal{T}}(\varphi) \cap S \subseteq Sat^{u}_{\mathcal{P}}(\varphi) \text{ and } Sat_{\mathcal{T}}(\psi) \cap S \subseteq Sat^{u}_{\mathcal{P}}(\psi) \text{ by induction}] \\
=& Sat^{u}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in S \setminus F \wedge post_{\mathcal{T}}(s) \cap (\mathcal{G}_{\mathcal{T},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\} \cup \\
& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in F \wedge post_{\mathcal{T}}(s) \cap (\mathcal{G}_{\mathcal{T},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\} \\
\subseteq& Sat^{u}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in S \setminus F \,\} \cup \\
& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in F \wedge post_{\mathcal{T}}(s) \cap (\mathcal{G}_{\mathcal{T},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\} \\
=& Sat^{u}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in S \setminus F \,\} \cup \\
& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in F \wedge post_{\mathcal{P}}(s) \cap (\mathcal{G}_{\mathcal{T},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\} \\
& [post_{\mathcal{P}}(s) = post_{\mathcal{T}}(s) \text{ for all } s \in F] \\
=& Sat^{u}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in S \setminus F \,\} \cup \\
& \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in F \wedge post_{\mathcal{P}}(s) \cap (\mathcal{G}^{u}_{\mathcal{P},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\} \\
& [post_{\mathcal{P}}(s) \subseteq S \text{ and } (\mathcal{G}_{\mathcal{T},\varphi,\psi})^{n-1}(\emptyset) \cap S \subseteq (\mathcal{G}^{u}_{\mathcal{P},\varphi,\psi})^{n-1}(\emptyset) \text{ by induction}] \\
\subseteq& Sat^{u}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \vee post_{\mathcal{P}}(s) \cap (\mathcal{G}^{u}_{\mathcal{P},\varphi,\psi})^{n-1}(\emptyset) \neq \emptyset \,\} \\
=& (\mathcal{G}^{u}_{\mathcal{P},\varphi,\psi})^n(\emptyset).
\end{aligned}
$$

Next, we show that

$$\bigcup_{n\in\mathbb{N}} (\mathcal{G}_{\mathcal{T},\varphi,\psi})^n(\emptyset) \supseteq \mathcal{G}_{\mathcal{T},\varphi,\psi}(\bigcup_{n\in\mathbb{N}} (\mathcal{G}_{\mathcal{T},\varphi,\psi})^n(\emptyset)) \tag{6}$$

Let $s \in \mathcal{G}_{\mathcal{T},\varphi,\psi}(\bigcup_{n\in\mathbb{N}} (\mathcal{G}_{\mathcal{T},\varphi,\psi})^n(\emptyset))$. We distinguish two cases.

- Assume that $s \in Sat_{\mathcal{T}}(\psi)$. Then $s \in \mathcal{G}_{\mathcal{T},\varphi,\psi}(\emptyset)$ and, hence, $s \in \bigcup_{n\in\mathbb{N}} (\mathcal{G}_{\mathcal{T},\varphi,\psi})^n(\emptyset)$.
- Otherwise, $s \in Sat_{\mathcal{T}}(\varphi)$ and $post_{\mathcal{T}}(s) \cap \bigcup_{n\in\mathbb{N}} (\mathcal{G}_{\mathcal{T},\varphi,\psi})^n(\emptyset) \neq \emptyset$. Therefore, $post_{\mathcal{T}}(s) \cap (\mathcal{G}_{\mathcal{T},\varphi,\psi})^n(\emptyset) \neq \emptyset$ for some $n \in \mathbb{N}$. Hence, $s \in \bigcup_{n\in\mathbb{N}} (\mathcal{G}_{\mathcal{T},\varphi,\psi})^n(\emptyset)$.

The remainder of the proof is similar to the previous case.

□

Corollary 1. *For each partial transition system $\mathcal{P} = (S, F, \to, AP, L)$ and transition system $\mathcal{T}$ that completes $\mathcal{P}$ and $\varphi, \psi \in CTL$, if $\varphi \equiv \psi$ then*

$$Sat^{\ell}_{\mathcal{P}}(\varphi) \subseteq Sat_{\mathcal{T}}(\psi) \cap S \subseteq Sat^{u}_{\mathcal{P}}(\varphi).$$

Proof. Immediate consequence of Theorem 5. □

As a consequence, if the CTL formulas φ and ψ are equivalent, then we can use the lower- and upperbounds of φ for ψ as well.

In some cases, we can characterize $Sat_{\mathcal{T}}$ without any reference to $\mathcal{T}$.

Proposition 2. *For each partial transition system $\mathcal{P} = (S, F, \to, AP, L)$ and transition system $\mathcal{T}$ that completes $\mathcal{P}$,*

(a) $Sat_{\mathcal{T}}(\exists \bigcirc \mathtt{true}) \cap S = (S \setminus F) \cup \{ s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \}$

(b) $Sat_{\mathcal{T}}(\exists \bigcirc \mathtt{false}) \cap S = \emptyset$

(c) $Sat_{\mathcal{T}}(\forall \bigcirc \mathtt{true}) \cap S = (S \setminus F) \cup \{ s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \}$

(d) $Sat_{\mathcal{T}}(\forall \bigcirc \mathtt{false}) \cap S = \emptyset$

(e) $Sat_{\mathcal{T}}(\exists \Box \mathtt{true}) \cap S = S$

(f) $Sat_{\mathcal{T}}(\exists \Box \mathtt{false}) \cap S = \emptyset$

(g) $Sat_{\mathcal{T}}(\exists \varphi \,\mathsf{U}\, \mathtt{true}) \cap S = S$

(h) $Sat_{\mathcal{T}}(\exists \varphi \,\mathsf{U}\, \mathtt{false}) \cap S = \emptyset$

Proof.

(a)

$$\begin{aligned}
Sat_{\mathcal{T}}(\exists \bigcirc \mathtt{true}) \cap S &= \{ s \in S \mid s \models_{\mathcal{T}} \exists \bigcirc \mathtt{true} \} \\
&= \{ s \in S \mid \exists \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \wedge \pi[1] \models_{\mathcal{T}} \mathtt{true} \} \\
&= \{ s \in S \mid \exists \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \} \\
&= \{ s \in S \mid post_{\mathcal{T}}(s) \neq \emptyset \} \\
&= \{ s \in S \setminus F \mid post_{\mathcal{T}}(s) \neq \emptyset \} \cup \{ s \in F \mid post_{\mathcal{T}}(s) \neq \emptyset \} \\
&= (S \setminus F) \cup \{ s \in F \mid post_{\mathcal{T}}(s) \neq \emptyset \} \qquad [\text{for all } s \in S \setminus F, \emptyset \subseteq post_{\mathcal{P}}(s) \subsetneqq post_{\mathcal{T}} \\
&= (S \setminus F) \cup \{ s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \} \qquad [\text{for all } s \in F, post_{\mathcal{P}}(s) = post_{\mathcal{T}}(s)]
\end{aligned}$$

(b)

$$\begin{aligned}
Sat_{\mathcal{T}}(\exists \bigcirc \mathtt{false}) \cap S &= \{ s \in S \mid s \models_{\mathcal{T}} \exists \bigcirc \mathtt{false} \} \\
&= \{ s \in S \mid \exists \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \wedge \pi[1] \models_{\mathcal{T}} \mathtt{false} \} \\
&= \emptyset
\end{aligned}$$

(c)

$$\begin{aligned}
Sat_{\mathcal{T}}(\forall \bigcirc \texttt{true}) \cap S =& \{\, s \in S \mid s \models_{\mathcal{T}} \forall \bigcirc \texttt{true} \,\} \\
=& \{\, s \in S \mid \forall \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \wedge \pi[1] \models_{\mathcal{T}} \texttt{true} \,\} \\
=& \{\, s \in S \mid \forall \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \,\} \\
=& \{\, s \in S \mid post_{\mathcal{T}}(s) \neq \emptyset \,\} \\
=& \{\, s \in S \setminus F \mid post_{\mathcal{T}}(s) \neq \emptyset \,\} \cup \{\, s \in F \mid post_{\mathcal{T}}(s) \neq \emptyset \,\} \\
=& (S \setminus F) \cup \{\, s \in F \mid post_{\mathcal{T}}(s) \neq \emptyset \,\} \qquad [\text{for all } s \in S \setminus F, \emptyset \subseteq post_{\mathcal{P}}(s) \subsetneqq post_{\mathcal{T}} \\
=& (S \setminus F) \cup \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \,\} \qquad [\text{for all } s \in F, post_{\mathcal{P}}(s) = post_{\mathcal{T}}(s)]
\end{aligned}$$

(d)

$$\begin{aligned}
Sat_{\mathcal{T}}(\forall \bigcirc \texttt{false}) \cap S =& \{\, s \in S \mid s \models_{\mathcal{T}} \forall \bigcirc \texttt{false} \,\} \\
=& \{\, s \in S \mid \forall \pi \in Paths_{\mathcal{T}}(s) : |\pi| > 1 \wedge \pi[1] \models_{\mathcal{T}} \texttt{false} \,\} \\
=& \emptyset
\end{aligned}$$

(e)

$$\begin{aligned}
Sat_{\mathcal{T}}(\exists \Box \texttt{true}) \cap S =& \{\, s \in S \mid s \models_{\mathcal{T}} \exists \Box \texttt{true} \,\} \\
=& \{\, s \in S \mid \exists \pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \texttt{true} \,\} \\
=& S
\end{aligned}$$

(f)

$$\begin{aligned}
Sat_{\mathcal{T}}(\exists \Box \texttt{false}) \cap S =& \{\, s \in S \mid s \models_{\mathcal{T}} \exists \Box \texttt{false} \,\} \\
=& \{\, s \in S \mid \exists \pi \in Paths_{\mathcal{T}}(s) : \forall 0 \leq i < |\pi| : \pi[i] \models_{\mathcal{T}} \texttt{false} \,\} \\
=& \emptyset
\end{aligned}$$

(g)

$$\begin{aligned}
Sat_{\mathcal{T}}(\exists \varphi \,\mathsf{U}\, \texttt{true}) \cap S =& \{\, s \in S \mid s \models_{\mathcal{T}} \exists \varphi \,\mathsf{U}\, \texttt{true} \,\} \\
=& \{\, s \in S \mid \exists \pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \texttt{true} \wedge \forall 0 \leq i < j : \pi[i] \models \\
=& S \qquad [\pi[0] \models_{\mathcal{T}} \texttt{true}]
\end{aligned}$$

(h)

$$\begin{aligned}
Sat_{\mathcal{T}}(\exists \varphi \,\mathsf{U}\, \texttt{false}) \cap S =& \{\, s \in S \mid s \models_{\mathcal{T}} \exists \varphi \,\mathsf{U}\, \texttt{false} \,\} \\
=& \{\, s \in S \mid \exists \pi \in Paths_{\mathcal{T}}(s) : \exists 0 \leq j < |\pi| : \pi[j] \models_{\mathcal{T}} \texttt{false} \wedge \forall 0 \leq i < j : \pi[i \\
=& \emptyset
\end{aligned}$$

□

The above also holds for any formula $\exists \bigcirc \varphi$ where $\varphi \equiv \texttt{true}$. Deciding that $\varphi \equiv \texttt{true}$ is the same as checking whether φ is valid, which in turn is the same as checking that $\neg\varphi$ is not satisfiable. However, the satisfiability problem for CTL is not easy to solve: it is EXPTIME-complete [7]. Therefore, we will only use the above characterization and not its generalization.

As we show next, if a system is fully explored then the lower- and upperbounds coincide.

Proposition 3. *For each partial transition system $\mathcal{P} = (S, F, \rightarrow, AP, L)$, if $F = S$ then*

$$Sat^{\ell}_{\mathcal{P}}(\varphi) = Sat^{u}_{\mathcal{P}}(\varphi).$$

Proof. We prove this proposition by structural induction on φ. We distinguish the following cases.

- Consider the CTL formula a. Then

  $$Sat^{\ell}_{\mathcal{P}}(a) = \{\, s \in S \mid a \in L(s) \,\} = Sat^{u}_{\mathcal{P}}(a).$$

  Consider the CTL formula $\neg\varphi$. Then

  $$\begin{aligned} Sat^{\ell}_{\mathcal{P}}(\neg\varphi) =& S \setminus Sat^{u}_{\mathcal{P}}(\varphi) \\ =& S \setminus Sat^{\ell}_{\mathcal{P}}(\varphi) && \text{[induction]} \\ =& Sat^{u}_{\mathcal{P}}(\neg\varphi). \end{aligned}$$

- Consider the CTL formula $\varphi \wedge \psi$. Then

  $$\begin{aligned} Sat^{\ell}_{\mathcal{P}}(\varphi \wedge \psi) =& Sat^{\ell}_{\mathcal{P}}(\varphi) \cap Sat^{\ell}_{\mathcal{P}}(\psi) \\ =& Sat^{u}_{\mathcal{P}}(\varphi) \cap Sat^{u}_{\mathcal{P}}(\psi) && \text{[induction]} \\ =& Sat^{u}_{\mathcal{P}}(\varphi \wedge \psi). \end{aligned}$$

- Consider the CTL formula $\exists \bigcirc \varphi$. Then

  $$\begin{aligned} Sat^{\ell}_{\mathcal{P}}(\exists \bigcirc \varphi) =& \{\, s \in S \mid post_{\mathcal{P}}(s) \cap Sat^{\ell}_{\mathcal{P}}(\varphi) \neq \emptyset \,\} \\ =& \{\, s \in F \mid post_{\mathcal{P}}(s) \cap Sat^{u}_{\mathcal{P}}(\varphi) \neq \emptyset \,\} \cup && \text{[induction]} \\ & S \setminus F \qquad [F = S] \\ =& Sat^{u}_{\mathcal{P}}(\exists \bigcirc \varphi). \end{aligned}$$

- Consider the CTL formula $\forall \bigcirc \varphi$. Then

  $$\begin{aligned} Sat^{\ell}_{\mathcal{P}}(\forall \bigcirc \varphi) =& \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat^{\ell}_{\mathcal{P}}(\varphi) \,\} \\ =& \{\, s \in S \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat^{\ell}_{\mathcal{P}}(\varphi) \,\} && [F = S] \\ =& \{\, s \in S \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat^{u}_{\mathcal{P}}(\varphi) \,\} && \text{[induction]} \\ =& (S \setminus F) \cup \{\, s \in F \mid post_{\mathcal{P}}(s) \neq \emptyset \wedge post_{\mathcal{P}}(s) \subseteq Sat^{u}_{\mathcal{P}}(\varphi) \,\} && [F = S] \\ =& Sat^{u}_{\mathcal{P}}(\forall \bigcirc \varphi). \end{aligned}$$

- Consider the CTL formula $\exists\Box\varphi$. Let $U \in 2^S$. Then

$$\begin{aligned}
&\mathcal{F}^{\ell}_{\mathcal{P},\varphi}(U)\\
=&\{\, s \in Sat^{\ell}_{\mathcal{P}}(\varphi) \mid (s \in F \wedge post_{\mathcal{P}}(s) = \emptyset) \vee post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\}\\
=&\{\, s \in Sat^{\ell}_{\mathcal{P}}(\varphi) \mid post_{\mathcal{P}}(s) = \emptyset \vee post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\} \qquad [F = S]\\
=&\{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \vee post_{\mathcal{P}}(s) = \emptyset \vee post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\} \qquad [F = S]\\
=&\mathcal{F}^{u}_{\mathcal{P},\varphi}(U)
\end{aligned}$$

  Therefore, $Sat^{\ell}_{\mathcal{P}}(\exists\Box\varphi) = Sat^{u}_{\mathcal{P}}(\exists\Box\varphi)$.

- Consider the CTL formula $\exists\varphi \,\mathsf{U}\, \psi$. Let $U \in 2^S$. Then

$$\begin{aligned}
&\mathcal{G}^{\ell}_{\mathcal{P},\varphi,\psi}(U)\\
=&Sat^{\ell}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{\ell}_{\mathcal{P}}(\varphi) \mid post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\}\\
=&Sat^{u}_{\mathcal{P}}(\psi) \cup \{\, s \in Sat^{u}_{\mathcal{P}}(\varphi) \mid s \in (S \setminus F) \vee post_{\mathcal{P}}(s) \cap U \neq \emptyset \,\} \qquad [F = S]\\
=&\mathcal{G}^{u}_{\mathcal{P},\varphi,\psi}(U)
\end{aligned}$$

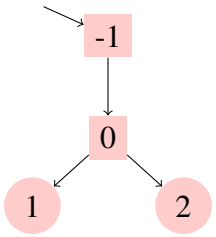
  Therefore, $Sat^{\ell}_{\mathcal{P}}(\exists\varphi \,\mathsf{U}\, \psi) = Sat^{u}_{\mathcal{P}}(\exists\varphi \,\mathsf{U}\, \psi)$.

□

8 JPF Listener that Writes a Partial Transition System to File

A listener for Java PathFinder (JPF) writes its partial transition system to file. In [2, Section 7.3], a listener that writes a transition system to file has been developed. This listener is extended to the setting of partial transition systems.

Consider the following partial transition system.



State -1 is the initial state. The states -1 and 0 are fully explored, and states 1 and 2 are not fully explored. The listener produces a file, the name of which is the name of the system under test with ".tra" as suffix (see [2, Section 7.4]), with the following content.

```
-1 -> 0
0 -> 1
0 -> 2
1 2
```

The first three lines describe the transitions. Each line contains the source of the transition followed by the target of the transition. The last line contains the states that are not fully explored yet.

9 Counterexamples and Witnesses

References

[1] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking*. MIT Press, Cambridge, MA, USA, 2008.

[2] Franck van Breugel. Java PathFinder: a tool to detect bugs in Java code. 2020.

[3] Edmund M. Clarke and E. Allen Emerson. Design and synthesis of synchronization skeletons using branching-time temporal logic. In Dexter Kozen, editor, *Proceedings of the 3rd Workshop on Logics of Programs*, volume 131 of *Lecture Notes in Computer Science*, pages 52–71, Yorktown Heights, NY, USA, May 1981. Springer-Verlag.

[4] Edmund M. Clarke, Orna Grumberg, and Doron Peleg. *Model Checking*. MIT Press, Cambridge, MA, USA, 1999.

[5] Brian A. Davey and Hilary A. Priestley. *Introduction to Lattice and Order*. Cambridge University Press, Cambridge, UK, 2002.

[6] Ryszard Engelking. *General Topology*. Heldermann Verlag, Berlin, Germany, 1989.

[7] Michael J. Fischer and Richard E. Ladner. Propositional dynamic logic of regular programs. *Journal of Computer and System Sciences*, 18(2):194–211, April 1979.

[8] Bronisław Knaster. Un théorème sur les fonctions d'ensembles. *Annales de la Société Polonaise de Mathématique*, 6:133–134, 1928.

[9] Terence Parr. *The Definitive ANTLR 4 Reference*. The Pragmatic Bookshelf, Dallas, TX, USA, 2013.

[10] Amir Pnueli. The temporal logic of programs. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, pages 46–57, Providence, RI, USA, October/November 1977. IEEE.

[11] Alfred Tarski. A lattice-theoretic fixed point theorem and its applications. *Pacific Journal of Mathematics*, 5(2):285–309, June 1955.

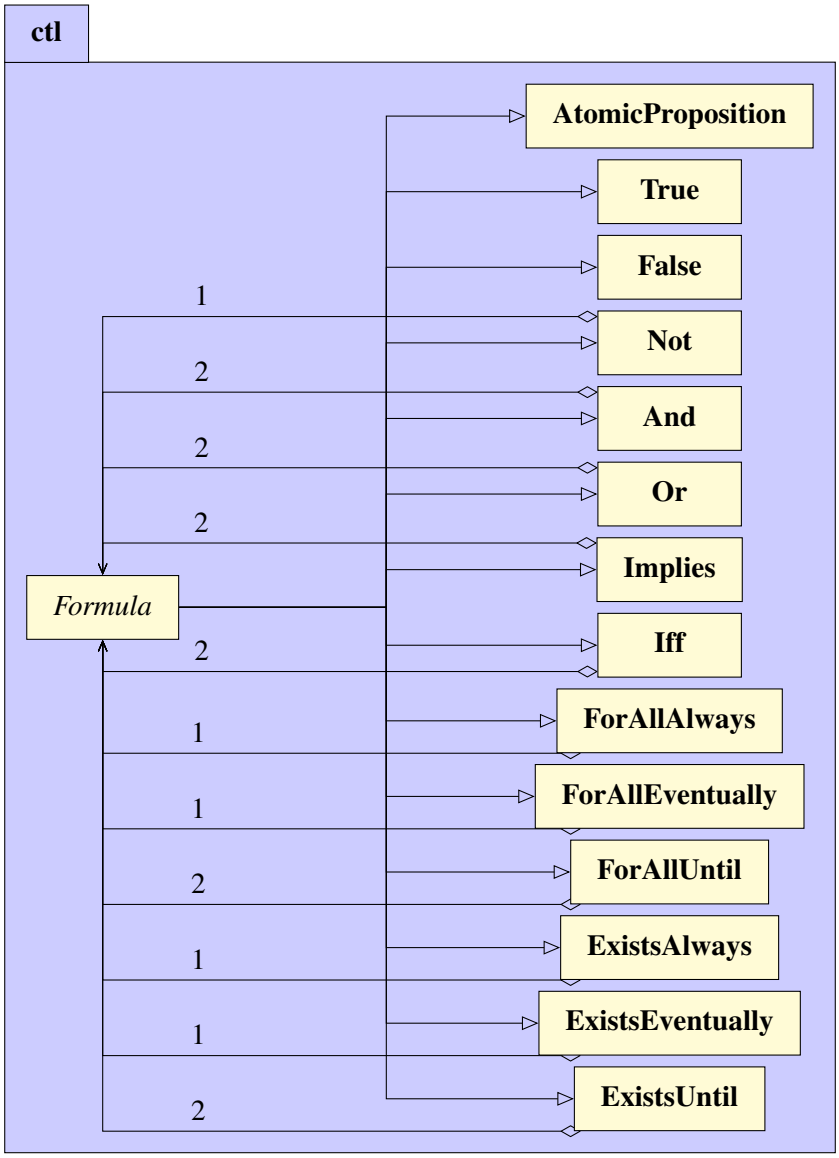


Figure 1: UML class diagram of the abstract syntax classes.

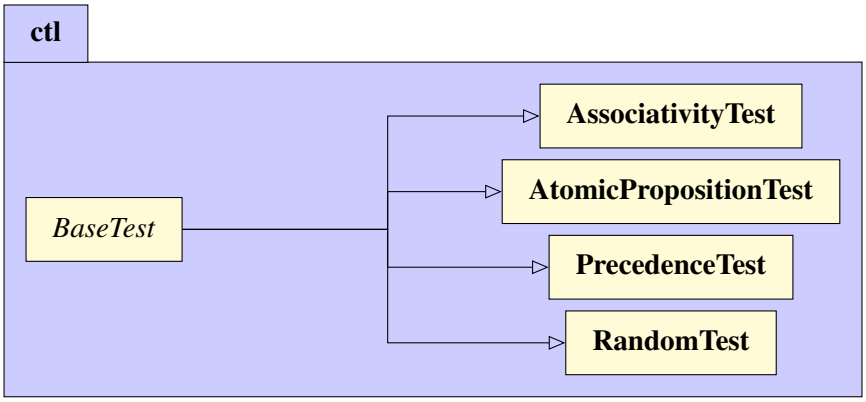


Figure 2: UML class diagram of the test classes.