CTL Model Checking

Prof. P.H. Schmitt

Institut für Theoretische Informatik
Fakultät für Informatik
Universität Karlsruhe (TH)

Formal Systems II
Fixed Point Theory
Fixed Points Definition

Definition

Let $f : \mathcal{P}(G) \rightarrow \mathcal{P}(G)$ be a set valued function and $Z$ a subset of $G$.

1. $Z$ is called a **fixed point** of $f$ if $f(Z) = Z$.

2. $Z$ is called the **least fixed point** of $f$ if $Z$ is a fixed point and for all other fixed points $U$ of $f$ the relation $Z \subseteq U$ is true.

3. $Z$ is called the **greatest fixed point** of $f$ if $Z$ is a fixed point and for all other fixed points $U$ of $f$ the relation $U \subseteq Z$ is true.
Finite Fixed Point Lemma

Let $G$ be an arbitrary set, Let $\mathcal{P}(G)$ denote the power set of a set $G$. A function $f : \mathcal{P}(G) \rightarrow \mathcal{P}(G)$ is called monotone of for all $X, Y \subseteq G$

$$X \subseteq Y \Rightarrow f(X) \subseteq f(Y)$$

Let $f : \mathcal{P}(G) \rightarrow \mathcal{P}(G)$ be a monotone function on a finite set $G$.

1. There is a least and a greatest fixed point of $f$.
2. $\bigcup_{n \geq 1} f^n(\emptyset)$ is the least fixed point of $f$.
3. $\bigcap_{n \geq 1} f^n(G)$ is the greatest fixed point of $f$. 
Proof of part (2) of the finite fixed point Lemma

Monotonicity of $f$ yields

$$\emptyset \subseteq f(\emptyset) \subseteq f^2(\emptyset) \subseteq \ldots \subseteq f^n(\emptyset) \subseteq \ldots$$

Since $G$ is finite there must be an $i$ such that $f^i(\emptyset) = f^{i+1}(\emptyset)$. Then $Z = \bigcup_{n \geq 1} f^n(\emptyset) = f^i(\emptyset)$ is a fixed point of $f$:

$$f(Z) = f(f^i(\emptyset)) = f^{i+1}(\emptyset) = f^i(\emptyset) = Z$$

Let $U$ be another fixed point of $f$. From $\emptyset \subseteq U$ be infer by monotonicity of $f$ at first $f(\emptyset) \subseteq f(U) = U$. By induction on $n$ we conclude $f^n(\emptyset) \subseteq U$ for all $n$. Thus also $Z = f^i(\emptyset) \subseteq U$. 

[End of proof]
A function $f : \mathcal{P}(G) \rightarrow \mathcal{P}(G)$ is called

1. **∪-continuous** (upward continuous), if for every ascending sequence $M_1 \subseteq M_2 \subseteq \ldots \subseteq M_n \subseteq \ldots$

   $$f\left(\bigcup_{n \geq 1} M_n\right) = \bigcup_{n \geq 1} f(M_n)$$

2. **∩-continuous** (downward continuous), if for every descending sequence $M_1 \supseteq M_2 \supseteq \ldots \supseteq M_n \supseteq \ldots$

   $$f\left(\bigcap_{n \geq 1} M_n\right) = \bigcap_{n \geq 1} f(M_n)$$
Fixed Points For Continuous Functions

Let
\[ f : \mathcal{P}(G) \to \mathcal{P}(G) \]
be an upward continuous functions and
\[ g : \mathcal{P}(G) \to \mathcal{P}(G) \]
a downward continuous function.

The for all \( M, N \in \mathcal{P}(G) \) such that \( M \subseteq f(M) \) and \( g(N) \subseteq N \) the following is true.

1. \( \bigcup_{n \geq 1} f^n(M) \) is the least fixed point of \( f \) containing \( M \),
2. \( \bigcap_{n \geq 1} g^n(M) \) is the greatest fixed point of \( g \) contained in \( M \).
Proof of (1)

By monotonicity we first obtain

\[ M \subseteq f(M) \subseteq f^2(M) \subseteq \ldots \subseteq f^n(M) \subseteq \ldots \]

Let \( P = \bigcup_{n \geq 1} f^n(M) \). This immediately gives \( M \subseteq P \). Furthermore

\[
\begin{align*}
    f(P) &= f\left(\bigcup_{n \geq 1} f^n(M)\right) \\
         &= \bigcup_{n \geq 1} f^{n+1}(M) \quad \text{by continuity} \\
         &= \bigcup_{n \geq 1} f^n(M) \quad \text{since } f(M) \subseteq f^2(M) \\
         &= P
\end{align*}
\]

Assume now that \( Q \) is another fixed point of \( f \) satisfying \( M \subseteq Q \).
By Monotonicity and the fixed point property \( f(M) \subseteq f(Q) = Q \) and furthermore for every \( n \geq 1 \) also \( f^n(M) \subseteq Q \).
Thus we obtain \( P = \bigcup_{n \geq 1} f^n(M) \subseteq Q \).
Knaster-Tarski-Fixed-Points Theorem

Let \( f : \mathcal{P}(G) \to \mathcal{P}(G) \) be a monotone function. Then

\[ f \text{ has a least and a greatest fixed point.} \]

Note, \( G \) need not be finite.
Proof

Fixed Point

Let $L = \{ S \subseteq G \mid f(S) \subseteq S \}$, e.g., $G \in L$.
Let $U = \cap L$. Show $f(U) = U$!

For all $S \in L$ by the property of an intersection: $U \subseteq S$.
By monotonicity and definition of $L$ $f(U) \subseteq f(S) \subseteq S$.
Thus $f(U) \subseteq \cap L = U$ and we have already established half of our claim.

By monotonicity $f(U) \subseteq U$ implies $f(f(U)) \subseteq f(U)$
which yields $f(U) \in L$ and furthermore $U \subseteq f(U)$.

We thus have indeed $U = f(U)$.
Proof

Least Fixed Point

Now assume $W$ is another fixed point of $f$, i.e., $f(W) = W$. This yields $W \in L = \{S \subseteq G \mid f(S) \subseteq S\}$ and 
$U = \bigcap L \subseteq W$. Thus $U$ is the least fixed point of $f$.

Following the same line of argument one can show that 
$\bigcup \{S \subseteq G \mid S \subseteq f(S)\}$ is the greatest fixed point of $f$. 
CTL Model Checking
Algorithm
Two Auxiliary Concepts

Let $\mathcal{T} = (S, R, v)$ be a transition system and $F$ an CTL formula. The set

$$\tau(F) = \{ s \in S \mid s \models F \}$$

is called the characteristic region of $F$ in $\mathcal{T}$.

The universal and existential next step functions $f_{AX}, f_{EX} : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$ are defined by

$$f_{AX}(Z) = \{ s \in S \mid \text{for all } t \text{ with } sRt \text{ we get } t \in Z \}$$
$$f_{EX}(Z) = \{ s \in S \mid \text{there exists a } t \text{ with } sRt \text{ and } t \in Z \}$$
CTL Model Checking Algorithm

Let $\mathcal{T} = (S, R, v)$ be a transition system and $F$ an CTL formula. $\tau(F)$ is computed by the following high-level recursive algorithm:

1. $\tau(p) = \{ s \in S \mid v(s, p) = 1 \}$
2. $\tau(F_1 \land F_2) = \tau(F_1) \cap \tau(F_2)$
3. $\tau(F_1 \lor F_2) = \tau(F_1) \cup \tau(F_2)$
4. $\tau(\neg F_1) = S \setminus \tau(F_1)$
5. $\tau(A(F_1 U F_2)) = \text{lfp}[\tau(F_2) \cup (\tau(F_1) \cap f_{AX}(Z))]$
6. $\tau(E(F_1 U F_2)) = \text{lfp}[\tau(F_2) \cup (\tau(F_1) \cap f_{EX}(Z))]$
7. $\tau(\text{AFF}F_1) = \text{lfp}[\tau(F_1) \cup f_{AX}(Z)]$
8. $\tau(\text{EFF}F_1) = \text{lfp}[\tau(F_1) \cup f_{EX}(Z)]$
9. $\tau(\text{EG}F_1) = \text{gfp}[\tau(F_1) \cap f_{EX}(Z)]$
10. $\tau(\text{AG}F_1) = \text{gfp}[\tau(F_1) \cap f_{AX}(Z)]$
Correctness Proof

Case 10  \( \text{AG} F_1 \)

By definition

\[
\tau(\text{AG} F_1) = \{ s \in S \mid s \in \tau(F_1) \text{ and } h \in \tau(\text{AG} F_1) \text{ for all } h \text{ with } gR h \}\]

Using Definition of the universal next step function:

\[
\tau(\text{AG} F_1) = \tau(F_1) \cap f_{AX}(\tau(\text{AG} F_1))
\]

So, \( \tau(\text{AG} F_1) \) is a fixed point of the function \( \tau(F_1) \cap f_{AX}(Z) \).

It remains to see that it is the greatest fixed point.
Correctness Proof

Case 10  \( \text{AG } F_1 \) (continued)

Let \( H \) be another fixed point, i.e., \( H = \tau(F_1) \cap f_{AX}(H) \).

We need to show \( H \subseteq \tau(\text{AG } F_1) \).

Consider \( g_0 \in H \) with the aim of showing that for all \( n \geq 0 \) and all \( g_i \) satisfying \( g_{i-1} R g_i \) for all \( 1 \leq i \leq n \) we obtain \( g_n \in \tau(F_1) \).

Observe \( H = \tau(F_1) \cap f_{AX}(H) \subseteq \tau(F_1) \).

Thus it suffices to show for all \( n \geq 0 \) that \( g_n \in H \).

For \( n = 0 \) that is true by assumptions.

Assume \( g_{n-1} \in H \).

\( g_{n-1} \in H \subseteq f_{AX}(H) = \{ g \mid \text{ for all } h \text{ with } g R h \text{ we have } h \in H \} \).

Thus \( g_n \in H \).
Correctness Proof

Case 6 $E(F_1 \cup F_2)$

By definition

$$\tau(E(F_1 \cup F_2)) = \{ g \in S \mid s \models F_2 \text{ or } s \models F_1 \text{ and there exists } h \text{ with } gRh \text{ and } h \models F_2 \}$$

Using next step function:

$$\tau(E(F_1 \cup F_2)) = \tau(F_2) \cup (\tau(F_1) \cap f_{EX}(\tau(E(F_1 \cup F_2))))$$

Thus $\tau(E(F_1 \cup F_2))$ is a fixed point of the function

$$\tau(F_2) \cup (\tau(F_1) \cap f_{EX}(Z)).$$

It remains to show that it is the least fixed point.
Correctness Proof

Case 6 $E(F_1 \cup F_2)$ (continued)

Consider $H \subseteq S$ with $H = \tau(F_2) \cup (\tau(F_1) \cap f_{EX}(H))$.

We need $\tau(E(F_1 \cup F_2)) \subseteq H$.

Fix $g_0 \in \tau(E(F_1 \cup F_2))$, try to arrive at $g_0 \in H$.

There is an $n \in \mathbb{N}$ and there are $g_i$ for $1 \leq i \leq n$ satisfying

1. $g_i R g_{i+1}$ for all $0 \leq i < n$.
2. $g_n \in \tau(F_2)$.
3. $g_i \in \tau(F_1)$ for all $0 \leq i < n$.

We set out to prove $g_n \in H$ by induction on $n$.

$n = 0$  Since $H = \tau(F_2) \cup (\tau(F_1) \cap f_{EX}(H)) \supseteq \tau(F_2)$ and $g_0 = g_n \in \tau(F_2)$.

$n - 1 \leadsto n$  By induction hypothesis we have $g_1 \in H$ and
Since $g_0 \in \tau(F_1)$ and $g_0 R g_1$ we obtain $g_0 \in (\tau(F_1) \cap f_{EX}(H)) \subseteq H$

and thus also $g_0 \in H$. 
CTL Model Checking

Example
Transition System
The Task

Check if the following the formula is true in state 1.

\[ F = T_1 \rightarrow \mathbf{AFC}_1 \equiv \neg T_1 \lor \mathbf{AFC}_1 \]
The Set-up

Goal

\[ 1 \models T_1 \rightarrow \text{AF}C_1 \quad \text{i.e.} \quad 1 \models \neg T_1 \lor \text{AF}C_1 \]

We will present the computations starting with the innermost subformulas first, i.e., in the order

\[ \tau(T_1), \tau(C_1), \tau(\neg T_1), \tau(\text{AF}C_1), \text{ and } \tau(F). \]

This will make it much easier to follow the algorithm, since when a recursive call is started, we know already its result.

In the end we check \( 1 \in \tau(F) \).
The First Steps

\[ \tau(T_1) = \{1, 3, 7\} \]  \hspace{1cm} (1)

\[ \tau(C_1) = \{2, 4\} \]  \hspace{1cm} (2)

From which we get easily

\[ \tau(\neg T_1) = \{0, 2, 4, 5, 6\} \]  \hspace{1cm} (3)
Fixed Point Computation

The next step is to compute \( \tau(\text{AF}C_1) \) according to the algorithm this amounts to the computation of the least fixed point of \( f(Z) = \tau(C_1) \cup f_{AX}(Z) = f_{AX}(Z) \cup \{2, 4\} \).

We thus compute \( f(\emptyset) \), \( f^2(\emptyset) \), \( \ldots \) \( f^n(\emptyset) \) till we reach a stationary value, i.e. \( f^n(\emptyset) = f^{n+1}(\emptyset) \).

\[
\begin{align*}
  f^1(\emptyset) &= \{2, 4\} \\
  f^2(\emptyset) &= \{2, 3, 4\} \\
  f^3(\emptyset) &= \{1, 2, 3, 4\} \\
  f^4(\emptyset) &= \{1, 2, 3, 4, 7\} \\
  f^5(\emptyset) &= \{1, 2, 3, 4, 7, 8\} \\
  f^6(\emptyset) &= \{1, 2, 3, 4, 7, 8\}
\end{align*}
\]

Thus

\[
\tau(\text{AF}C_1) = \{1, 2, 3, 4, 7, 8\}
\]
End of the Computation

\[ \tau(F) = \tau(\neg T_1) \cup \tau(\text{AFC}_1) = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = S \]  \hspace{1cm} (5)

Since \(1 \in \tau(F)\) we conclude

\[ s_1 \models F \]  \hspace{1cm} (6)