Tarski's Fixed-point Lemma

Recall:

- We identify a predicate with the set of states in which the predicate is true.
- Predicates are ordered via set inclusion.
- X is a fixed point of τ iff $\tau(X) = X$.
- A predicate transformer τ is *monotonic* iff $P \subseteq Q$ implies $\tau(P) \subseteq \tau(Q)$.
- A predicate transformer τ is $\cup$-*continuous* iff $P_1 \subseteq P_2 \subseteq \ldots$ implies $\tau(\cup_i P_i) = \cup_i \tau(P_i)$.
- A predicate transformer τ is $\cap$-*continuous* iff $P_1 \supseteq P_2 \supseteq \ldots$ implies $\tau(\cap_i P_i) = \cap_i \tau(P_i)$.

Lemma. $\mathbf{lfp}\, Z \left[\tau(Z)\right] = \cap\{Z \mid \tau(Z) = Z\}$ whenever τ is monotonic.

Proof. We in fact prove that $\mathbf{lfp}\, Z \left[\tau(Z)\right] = \cap\{Z \mid \tau(Z) \subseteq Z\}$, since it has a simpler proof.

Define $L = \{Z \mid \tau(Z) \subseteq Z\}$, we first prove that $\cap L$ is a fixpoint of τ, and we shall proceed by showing that $\tau(\cap L) \subseteq \cap L$ and $\tau(\cap L) \supseteq \cap L$. Recall that $\cap L$ is the greatest lower bound of L. We now reason

$Z \in L$	
$\Rightarrow$	$\cap L$ lower bound of L
$\cap L \subseteq Z$	
$\Rightarrow$	τ monotonic
$\tau(\cap L) \subseteq \tau(Z)$	
$\Rightarrow$	$Z \in L$ iff $\tau(Z) \subseteq Z$
$\tau(\cap L) \subseteq Z$	
$\Rightarrow$	$\cap L$ greatest lower bound of L
$\boxed{\tau(\cap L) \subseteq \cap L}$	
$\Rightarrow$	τ monotonic
$\tau(\tau(\cap L)) \subseteq \tau(\cap L)$	
$\Rightarrow$	definition of L
$\tau(\cap L) \in L$	
$\Rightarrow$	$\cap L$ lower bound of L
$\boxed{\cap L \subseteq \tau(\cap L)}$	

so we conclude $\cap L = \tau(\cap L)$.

We now prove that $\cap L$ is the least fixpoint. Suppose X is an arbitrary fixpoint of τ, then it is $X \in L$. But $\cap L$ is a lower bound of L, so it must be $\cap L \subseteq X$. $\square$

Lemma. $\textbf{lfp}\, Z \left[\tau(Z)\right] = \cup_i \tau^i(\mathit{False})$ whenever τ is $\cup$-continuous.

Proof. For any predicate P and $i \in \mathbb{N}$, $\tau^i(P)$ is defined inductively as: $\tau^0(P) = P$ and $\tau^i(P) = \tau(\tau^{i-1}(P))$ for $i > 0$. We first show that $\cup_i \tau^i(\mathit{False})$ is a fixpoint of τ. We reason

$$
\begin{aligned}
& \tau(\cup_{i=0}^{\infty} \tau^i(\mathit{False})) \\
= \quad & \text{τ $\cup$-continuous} \\
& \cup_{i=0}^{\infty} \tau(\tau^i(\mathit{False})) \\
= \quad & \text{definition of } \tau^i \\
& \cup_{i=0}^{\infty} \tau^{i+1}(\mathit{False}) \\
= \quad & \text{algebra} \\
& \cup_{i=1}^{\infty} \tau^i(\mathit{False}) \\
= \quad & P \cup \emptyset = P \\
& \cup_{i=1}^{\infty} \tau^i(\mathit{False}) \cup \emptyset \\
= \quad & \mathit{False} = \emptyset \text{ and definition of } \tau^0 \\
& \cup_{i=1}^{\infty} \tau^i(\mathit{False}) \cup \tau^0(\mathit{False}) \\
= \quad & \text{algebra} \\
& \cup_{i=0}^{\infty} \tau^i(\mathit{False})
\end{aligned}
$$

and we have showed that $\cup_i \tau^i(\mathit{False})$ is a fixpoint of τ. We now prove that it is the least fixpoint. Suppose X is an arbitrary fixpoint of τ. It must be $\mathit{False} \subseteq X$ and since τ is monotonic we have $\tau(\mathit{False}) \subseteq \tau(X) = X$. By induction one can prove (Exercise) that

$$\forall i \in \mathbb{N} \quad \tau^i(\mathit{False}) \subseteq X$$

which implies that $\cup_{i=0}^{\infty} \tau^i(\mathit{False}) \subseteq X$. $\square$

Lemma Suppose the set of states is finite. Then $\mathbf{E}[f_1 \mathbf{U} f_2]$ is the least fixpoint of the transformer $\tau(Z) = f_2 \vee (f_1 \wedge \mathbf{EX}\, Z)$.

Proof. The proof strategy, as per Lemma 13 (page 64 of the textbook), is the following:

1. prove that τ is monotonic;
2. since the state space is finite and τ is monotonic, observe that $\textbf{lfp}\, Z \left[\tau(Z)\right] = \cup_i \tau^i(\mathit{False})$;

3. prove that $\mathbf{E}[f_1 \mathbf{U} f_2] = \cup_i \tau^i(\mathit{False})$, and conclude that $\mathbf{E}[f_1 \mathbf{U} f_2] = \mathbf{lfp}\, Z \left[\tau(Z)\right]$.

Here we only prove step 1, since steps 2 and 3 are covered in the textbook. We shall also prove that $\mathbf{E}[f_1 \mathbf{U} f_2]$ is a fixpoint of τ, which is needed in step 3 but it is not detailed in the textbook.

We begin with step 1. Lemma 9 (page 64 of the textbook) shows that the transformer $\alpha(Z) = f_1 \wedge \mathbf{EX}\, Z$ is monotonic. We thus need to prove that $\tau(Z) = f_2 \vee \alpha(Z)$ is monotonic. Let us consider any two predicates $P_1 \subseteq P_2$, then

$s \in \tau(P_1)$

$\Leftrightarrow$ definition of τ, semantics of $\vee$

$s \models f_2$ or $s \in \alpha(P_1)$

$\Rightarrow$ α monotonic, i.e., $\alpha(P_1) \subseteq \alpha(P_2)$

$s \models f_2$ or $s \in \alpha(P_2)$

$\Leftrightarrow$ semantics of $\vee$, definition of τ

$s \in \tau(P_2)$

and we have therefore shown that $\tau(P_1) \subseteq \tau(P_2)$.

We now prove that $\mathbf{E}[f_1 \mathbf{U} f_2]$ is a fixpoint of τ, i.e., that $\tau(\mathbf{E}[f_1 \mathbf{U} f_2]) = \mathbf{E}[f_1 \mathbf{U} f_2]$. For a path π we denote by π^i the suffix of π starting at the i-th state (the first state has index 0). We reason:

$s_0 \in \tau(\mathbf{E}[f_1 \mathbf{U} f_2])$

$\Leftrightarrow$ definition of τ, semantics of $\wedge, \vee$

$s_0 \models f_2$ or ($s_0 \models f_1$ and $s_0 \models \mathbf{EX}\, \mathbf{E}[f_1 \mathbf{U} f_2]$)

$\Leftrightarrow$ semantics of $\mathbf{E}$

$s_0 \models f_2$ or ($s_0 \models f_1$ and $\exists \pi = s_0, s_1, \ldots\ \pi \models \mathbf{X}\, \mathbf{E}[f_1 \mathbf{U} f_2]$)

$\Leftrightarrow$ semantics of $\mathbf{X}$

$s_0 \models f_2$ or ($s_0 \models f_1$ and $\exists \pi = s_0, s_1, \ldots\ \pi^1 \models \mathbf{E}[f_1 \mathbf{U} f_2]$)

$\Leftrightarrow$ s_1 is the first state of π^1

$s_0 \models f_2$ or ($s_0 \models f_1$ and $\exists \pi = s_0, s_1, \ldots\ s_1 \models \mathbf{E}[f_1 \mathbf{U} f_2]$)

$\Leftrightarrow$ semantics of $\mathbf{E}$

$s_0 \models f_2$ or ($s_0 \models f_1$ and $\exists \pi = s_0, s_1, \ldots\ \exists \sigma = s_1, t_1, t_2, \ldots\ \sigma \models f_1 \mathbf{U} f_2$)

$\Leftrightarrow$ semantics of $\mathbf{U}$

$s_0 \models f_2$ or ($s_0 \models f_1$ and $\exists \pi = s_0, s_1, \ldots\ \exists \sigma = s_1, t_1, t_2, \ldots\ \exists k \geqslant 0\ (\sigma^k \models f_2$ and $\forall i < k\ \sigma^i \models f_1))$

$\Leftrightarrow$ logic - eliminate double quantifier

$s_0 \models f_2$ or ($s_0 \models f_1$ and $\exists \pi = s_0, s_1, \ldots\ \exists k \geqslant 1\ (\pi^k \models f_2$ and $\forall\, 1 \leqslant i < k\ \ \pi^i \models f_1))$

$\Leftrightarrow$ logic - include $s_0 \models f_1$ in existential quantifier

$s_0 \models f_2$ or $(\exists \pi = s_0, s_1, \ldots\ \exists k \geqslant 1\ (\pi^k \models f_2$ and $\forall\, 0 \leqslant i < k\ \ \pi^i \models f_1))$

$\Leftrightarrow$ logic - include $s_0 \models f_2$ in existential quantifier

$\exists \pi = s_0, s_1, \ldots\ \exists k \geqslant 0\ (\pi^k \models f_2$ and $\forall\, 0 \leqslant i < k\ \ \pi^i \models f_1)$

$\Leftrightarrow$ semantics of $\mathbf{U}$

$\exists \pi = s_0, s_1, \ldots\ \pi \models f_1 \mathbf{U} f_2$

$\Leftrightarrow$ semantics of $\mathbf{E}$

$s_0 \in \mathbf{E}[f_1 \mathbf{U} f_2]$

and we have shown that $\tau(\mathbf{E}[f_1 \mathbf{U} f_2]) = \mathbf{E}[f_1 \mathbf{U} f_2]$. $\square$