Model Checking III
Basic Fixpoint Theorems

Edmund M. Clarke, Jr.
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
Let $M = (S, R, L)$ be an arbitrary finite Kripke structure.

$Pred(S)$ is the lattice of predicates over $S$. Each predicate is identified with the set of states that make it true. The ordering is set inclusion.

Thus, the least element in the lattice is the empty set, denoted by $False$, and the greatest element in the lattice is the set of all states, denoted by $True$.

A functional $F : Pred(S) \rightarrow Pred(S)$ is called a **predicate transformer**.

Let $\tau : \text{Pred}(S) \rightarrow \text{Pred}(S)$ be a predicate transformer, then

1. $\tau$ is \textit{monotonic} provided that $P \subseteq Q$ implies $\tau[P] \subseteq \tau[Q]$;

2. $\tau$ is $\cup$-\textit{continuous} provided that $P_1 \subseteq P_2 \subseteq \ldots$ implies $\tau[\bigcup_i P_i] = \bigcup_i \tau[P_i]$;

3. $\tau$ is $\cap$-\textit{continuous} provided that $P_1 \supseteq P_2 \supseteq \ldots$ implies $\tau[\bigcap_i P_i] = \bigcap_i \tau[P_i]$. 


Basic Fixpoint Theorems

If \( \tau \) is monotonic, then it has a least fixpoint, \( \text{lfp} \ Z \left[ \tau(Z) \right] \), and a greatest fixpoint, \( \text{gfp} \ Z \left[ \tau(Z) \right] \).

\[
\text{lfp} \ Z \left[ \tau(Z) \right] = \cap \{ Z \mid \tau(Z) = Z \} \quad \text{whenever} \quad \tau \text{ is monotonic.}
\]

\[
\text{lfp} \ Z \left[ \tau(Z) \right] = \cup_i \tau^i(False) \quad \text{whenever} \quad \tau \text{ is also } \cup\text{-continuous;}
\]

\[
\text{gfp} \ Z \left[ \tau(Z) \right] = \cup \{ Z \mid \tau(Z) = Z \} \quad \text{whenever} \quad \tau \text{ is monotonic.}
\]

\[
\text{gfp} \ Z \left[ \tau(Z) \right] = \cap_i \tau^i(True) \quad \text{whenever} \quad \tau \text{ is also } \cap\text{-continuous.}
\]
Let \( M \) be a finite Kripke structure and let \( \tau \) be a monotonic predicate transformer on \( S \).

1. The functional \( \tau \) is both \( \cup \)-continuous and \( \cap \)-continuous.
2. For every \( i \), \( \tau^i(False) \subseteq \tau^{i+1}(False) \) and \( \tau^i(True) \supseteq \tau^{i+1}(True) \).
3. There is an integer \( i_0 \) such that for every \( j \geq i_0 \),
   \( \tau^j(False) = \tau^{i_0}(False) \).
   There is an integer \( j_0 \) such that for every \( j \geq j_0 \),
   \( \tau^j(True) = \tau^{j_0}(True) \).
4. There is an integer \( i_0 \) such that \( \text{lfp} \ Z \left[ \tau(Z) \right] \) is \( \tau^{i_0}(False) \).
   There is an integer \( j_0 \) such that \( \text{gfp} \ Z \left[ \tau(Z) \right] \) is \( \tau^{j_0}(True) \).
As a consequence of the preceding lemmas, if $\tau$ is monotonic, its least fixpoint can be computed by the following program.

```plaintext
function Lfp($\tau$ : PredicateTransformer)
begin
    $Q$ := False;
    $Q'$ := $\tau$(Q);
    while ($Q \neq Q'$) do
        begin
            $Q$ := $Q'$;
            $Q'$ := $\tau$(Q')
        end;
    return $Q$
end
```
Correctness of Algorithm

The invariant for the while loop is given by the assertion

\[(Q' = \tau[Q]) \land (Q' \subseteq \text{lfp } Z [\tau(Z)])\]

It is easy to see that at the beginning of the \(i\)-th iteration, \(Q = \tau^{i-1}(\text{False})\) and \(Q' = \tau^i(\text{False})\). Lemma 2 implies that

\[\text{False} \subseteq \tau(\text{False}) \subseteq \tau^2(\text{False}) \subseteq \ldots\]

So, the number of iterations before the loop terminates is bounded by the cardinality of \(S\).

When the loop terminates, we have \(Q = \tau[Q]\) and \(Q \subseteq \text{lfp } Z [\tau(Z)]\).

It follows directly that \(Q = \text{lfp } Z [\tau(Z)]\) and that the value returned is the least fixpoint.
The greatest fixpoint of $\tau$ may be computed in a similar manner. Essentially the same argument can be used to show that the procedure terminates and that the value it returns is $\text{gfp} \ Z \ [\tau(Z)]$.

```
function Gfp(Tau : PredicateTransformer)
begin
    Q := True;
    Q' := Tau(Q);
    while (Q ≠ Q') do
        begin
            Q := Q';
            Q' := Tau(Q')
        end;
    return(Q)
end
```
Each CTL operator can be characterized as a least or greatest fixpoint of a predicate transformer:

- $\mathbf{A}[f_1 U f_2] = \text{lfp} \ Z [f_2 \lor (f_1 \land AX \ Z)]$
- $\mathbf{E}[f_1 U f_2] = \text{lfp} \ Z [f_2 \lor (f_1 \land EX \ Z)]$
- $\mathbf{AF} f_1 = \text{lfp} \ Z [f_1 \lor AX \ Z]$
- $\mathbf{EF} f_1 = \text{lfp} \ Z [f_1 \lor EX \ Z]$
- $\mathbf{AG} f_1 = \text{gfp} \ Z [f_1 \land AX \ Z]$
- $\mathbf{EG} f_1 = \text{gfp} \ Z [f_1 \land EX \ Z]$

We will only prove the characterization for $\mathbf{EU}$. 
Fixpoint Characterization of $EU$

**Lemma**

$E[f_1 U f_2]$ is the least fixpoint of the functional $\tau(Z) = f_2 \lor (f_1 \land EX Z)$.

**Proof:**

It is straightforward to prove that $E[f_1 U f_2]$ is a fixpoint of $\tau(Z)$.

Additional steps are required to show that $E[f_1 U f_2]$ is the least such fixpoint.

1. Prove that $\tau(Z) = f_2 \lor (f_1 \land EX Z)$ is monotonic.

2. Observe that $\tau$ is $\cup$-continuous and that
   \[
   \text{lfp } Z \left[ \tau(Z) \right] = \cup_i \tau^i(False).
   \]

3. Show that $E[f_1 U f_2] = \cup_i \tau^i(False)$. See next page.

4. Conclude from steps 2 and 3 that $E[f_1 U f_2]$ is the least fixpoint of $\tau(Z) = f_2 \lor (f_1 \land EX Z)$. $\Box$
Next, we show that \( E[f_1 \cup f_2] = \bigcup_i \tau^i(False) \). We break this step into two parts:

- First, show that \( \bigcup_i \tau^i(False) \subseteq E[f_1 \cup f_2] \).
  
  Hint: Prove by induction that for all \( i \), \( \tau^i(False) \subseteq E[f_1 \cup f_2] \). Use the fact that \( E[f_1 \cup f_2] \) is a fixpoint of \( \tau(Z) \).

- Next, show that \( E[f_1 \cup f_2] \subseteq \bigcup_i \tau^i(False) \).
  
  Hint: If \( s_1 \models E[f_1 \cup f_2] \), then there is a path \( \pi = s_1, \ldots, s_j, \ldots \) such that \( s_j \models f_2 \) and for all \( l < j \), \( s_l \models f_1 \). Show that \( s_1 \in \tau^j(False) \).
The next four figures show how $E[p \ U \ q]$ may be computed for a simple Kripke structure.

In this case the functional $\tau$ is given by

$$\tau(Z) = q \lor (p \land EX \ Z).$$

The figures demonstrate that the sequence of approximations $\tau^i(False)$ converges to $E[p \ U \ q]$.

$$E[p \ U \ q] = \tau^3(False) \text{ since } \tau^3(False) = \tau^4(False).$$
Simple Example for $E[p U q]$ (Cont.)

$M, s_0 \models E[p U q]$?
Simple Example for $E[p \ U \ q]$ (Cont.)

$M, s_0 \models E[p \ U \ q]?$

$\tau^1(\text{False})$
Simple Example for $E[p \ U \ q]$ (Cont.)

$M, s_0 \models E[p \ U \ q]$?

$\tau^2(False)$
$M, s_0 \models E[p \mathbf{U} q]?$

$\tau^3(False)$