Symbolic Model Checking

Konkuk University
Department of Computer Science & Engineering
Kunha Kim

Fixed Point

- The set $P(S)$ of all subsets of S forms a lattice under the set inclusion ordering

- Each element of S' of the lattice can also be thought of as a $predicate$ on S, where the predicate is viewed as being $true$ for exactly the states in S'

- The least element in the lattice is the empty set, denoted as $False$, and the greatest element in the lattice is the set S, denoted as $True$

- A function τ that maps $P(S)$ to $P(S)$ will be called a $predicate\ transformer$

Fixed Point

- τ is *monotonic* provided that $P \subseteq Q$ implies $\tau(P) \subseteq \tau(Q)$

- τ is $\cup - continuous$ provided that $P_1 \subseteq P_2 \subseteq \cdots$ implies $\tau(\cup_i P_i) = \cup_i \tau(P_i)$ (Upward Continuous)

- τ is $\cap - continuous$ provided that $P_1 \subseteq P_2 \subseteq \cdots$ implies $\tau(\cap_i P_i) = \cap_i \tau(P_i)$ (Downward Continuous)

- We write $\tau^i(Z)$ to denote i applications of τ to Z ($\tau^0(Z) = Z$, $\tau^{i+1}(Z) = \tau(\tau^i(Z))$)

Fixed Point

- Let $\tau : P(S') \rightarrow P(S')$ be a set valued function and S' a subset of S

- S' is called a fixed point of τ if $\tau(S') = S'$

- S' is called a least fixed point of τ if for all other fixed points U of τ the relation $S' \subseteq U$ is true

- Also denoted as $\mu Z . \tau(Z) = \cap \{Z \,|\, \tau(Z) \subseteq Z\}$ when τ is monotonic

- S' is called a greatest fixed point of τ if for all other fixed points U of τ the relation $U \subseteq S'$ is true

- Also denoted as $\nu Z . \tau(Z) = \cup \{Z \,|\, \tau(Z) \supseteq Z\}$ when τ is monotonic

Finite Fixed Point Lemma

- If S is finite and τ is monotonic, then there is a least fixed point and greatest fixed point
- $\cup_{n\geq 1} \tau^n(\emptyset)$ is a least fixed point of $\tau \cdots$ (a)
- $\cap_{n\geq 1} \tau^n(True)$ is a greatest fixed point of $\tau \cdots$ (b)
- τ is also $\cup - continuous$ and $\cap - continuous \cdots$ (c)

Proof of (c)

- Let $P_1 \subseteq P_2 \subseteq \cdots$ be a sequence of subset of S. Since S is finite, there is j_0 such that for every $j \geq j_0$, $P_j = P_{j_0}$. For every $j < j_0$, $P_j \subseteq P_{j_0}$.

- Thus, $\cup_i P_i = P_{j_0}$ and as a result, $\tau(\cup_i P_i) = \tau(P_{j_0})$

- Because τ is monotonic, $\tau(P_1) \subseteq \tau(P_2) \subseteq \cdots$. Thus, for every $j < j_0$, $\tau(P_j) \subseteq \tau(P_{j_0})$ and for every $j \geq j_0$, $\tau(P_j) = \tau(P_{j_0})$

- Therefore, $\cup_i \tau(P_i) = \tau(P_{j_0})$. It means τ is $\cup - continuous$

- Intuitively, there must be an i such that $\tau^i(\emptyset) = \tau^{i+1}(\emptyset)$ and $\tau^i(\emptyset)$ will be a fixed point of τ

Tarski-Knaster Theorem

- Let $\tau : P(G) \to P(G)$ be a monotone function. Then τ has a least and greatest fixed point
- Note that G not need to be finite

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

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

Procedure for computing least fixed point

```
function Lfp(Tau : PredicateTransformer) : Predicate
    Q := False;
    Q' := Tau(Q);
    while (Q ≠ Q') do
        Q := Q';
        Q' := Tau(Q');
    end while;
    return(Q);
end function
```

Procedure for computing least fixed point

- When the loop does terminates, we will have that $Q = \tau(Q)$ and that $Q \subseteq \mu Z\,.\,\tau(Z)$

- Because Q is also a fix point, $\mu Z\,.\,\tau(Z) \subseteq Q$ and hence $Q = \mu Z\,.\,\tau(Z)$

- The invariant for the while loop in the body of the procedure is given by the assertion $(Q' = \tau(Q)) \wedge (Q' \subseteq \mu Z\,.\,\tau(Z))$

Quantified Boolean Formula

- Given a propositional variable set $V = \{v_0, v_1, \cdots, v_{n-1}\}$, $QBF(V)$ is the smallest set of formulas such that

- Every variable in V is a formula

- If f and g is a formulas, then $\neg f$, $f \vee g$, and $f \wedge g$ are formulas

- If f is a formula and $v \in V$, then $\exists v f$ and $\forall v f$ are formulas

- A truth assignment is a function $\sigma : V \rightarrow \{false, true\}$ and we will equate each QBF formula with the set of truth assignments that satisfy the formulas

- We will use the notation $\sigma < v \leftarrow a >$ for the truth assignment defined by $\sigma < v \leftarrow a > (w) = a$ if $v = w$, otherwise $\sigma(w)$

Some terminologies

- If f is a formula in $QBF(V)$ and σ is a truth assignment, we will write $\sigma \models f$ to denote that f is true under the assignment σ

- $\sigma \models v$ iff $\sigma(v) = 1$

- $\sigma \models \neg f$ iff $\sigma \not\models f$

- $\sigma \models f \vee g$ iff $\sigma \models f$ or $\sigma \models g$

- $\sigma \models f \wedge g$ iff $\sigma \models f$ and $\sigma \models g$

- $\sigma \models \exists v f$ iff $\sigma < v \leftarrow 0 > \models f$ or $\sigma < v \leftarrow 1 > \models f$

- $\sigma \models \forall v f$ iff $\sigma < v \leftarrow 0 > \models f$ and $\sigma < v \leftarrow 1 > \models f$