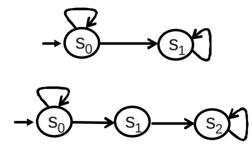
Algorithmic Verification

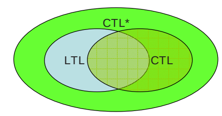
Comp4151
Lecture 4-B
Ansgar Fehnker

Overview

Modelling
- Finite automata
- Büchi automata
- Kripke structures



Specification
- Linear Time Logic
- Computation Tree Logic
- CTL*



Overview

Model checking
- Explicit state CTL model checking
- Labelling states with sub-formulas
- Bottom-up along the parse tree of the CTL formula
- Complexity linear in the size of the Kripke structure and length of the formula.

However
- Size of the Kripke structure exponential in the number of components.

Symbolic Model Checking

Basic Idea
- Define model checking in terms of sets of states
- Use a compact symbolic representation for sets of states
- Use efficient algorithms to operate on this representation

Today
- The fixpoint characterization of CTL

Sets

Preliminaries

Given a Kripke structure $M=(S, s_0, \rightarrow, \mu)$ and a CTL formula ϕ over a set of atomic propositions AP.
$[| \phi |]$ denotes the set of states s with $M,s \models \phi$

- $[| p |] = \{ s \mid p \in \mu(s) \}$
- $[|true|] = S$
- $[|false|] = \varnothing$
- $[| \neg \phi |] = S \setminus [| \phi |]$
- $[| \phi \wedge \psi |] = [| \phi |] \cap [| \psi |]$
- $[| \phi \vee \psi |] = [| \phi |] \cup [| \psi |]$

What about the temporal operators?

Sets

Exist Next

Set of states that satisfies EX ϕ

$[| EX\ \phi |] = \{ s \mid \exists (s,s') \in \rightarrow \text{ such that } s' \in [| \phi |] \}$

$\Rightarrow$ We can compute $[| EX\ \phi |]$, given set $[| \phi |]$ ✓

Sets

Exist Until

Set of states that satisfies $E\ \phi\ U\ \psi$

$$[| E\ \phi\ U\ \psi |] = [| \psi \vee (\phi \wedge EX\ E\ \phi\ U\ \psi)|]$$
$$= [| \psi |] \cup ([| \phi |] \cap [| EX\ E\ \phi\ U\ \psi |])$$

with

$[| EX\ E\ \phi\ U\ \psi |] = \{ s \mid \exists (s,s') \in \rightarrow \text{ s.t. } s' \in [| E\ \phi\ U\ \psi |] \}$

$\Rightarrow$ We can compute $[|E\ \phi\ U\ \psi|]$, given $[|E\ \phi\ U\ \psi|]$ **???**

Sets

Exist Globally

Set of states that satisfies EG ϕ

$$[| EG\ \phi |] = [| \phi \wedge EX\ EG\ \phi |]$$
$$= [| \phi |] \cap [| EX\ EG\ \phi |])$$
$$= [| \phi |] \cap \{ s \mid \exists (s,s') \in \rightarrow \text{ s.t. } s' \in [| EG\ \phi |] \}$$

$\Rightarrow$ We can compute $[|EG\ \phi|]$, given $[|EG\ \phi|]$ **???**

Feels like circular reasoning

Monotonic Functions

A short diversion

Monotonic Functions

Definition

Let S be a set of states S and f: $2^S \rightarrow 2^S$ a function from sets of states to sets of states.

- Function f is called *monotonic* if $P \subseteq Q$ implies $f(P) \subseteq f(Q)$
- A subset P of S is called a *fixpoint* of f if $f(P) = P$
- A fixpoint P is a *least fixpoint* if $P \subseteq Q$ for all fixpoints Q
- A fixpoint P is a *greatest fixpoint* if $P \supseteq Q$ for all fixpoints Q
- We define $f^1(P) := f(P)$ and $f^{n+1}(P) := f(f^n(P))$

Monotonic Functions

Examples

Let $S:=\{0,1,2,3\}$

> There exist non-monotonic functions without fixpoint.

> There exist functions with fixpoint, but no least or greatest fixpoint.

$f(P) := P \cup \{2\}$

- monotonic with fixpoints {2}, {0,2}, {1,2}, {3,2}, {0,1,2}, {1,2,3}, {0,2,3}, {0,1,2,3}.

$f(P) := P \setminus \{2\}$

- monotonic with fixpoints ∅, {0}, {1}, {3}, {0,1}, {1,3}, {0,3}, {0,1,3}.

$f(P) := \{s+1 \bmod 4 \mid s \notin P\}$

- not monotonic, but fixpoints {0,2}, {1,3}

Monotonic Functions

Knaster-Tarski Theorem

Let S be a *finite* set with n elements. If f: $2^S \rightarrow 2^S$ is a *monotonic* function then

- $f^n(\emptyset)$ is the *least fixpoint* of f
- $f^n(S)$ is the *greatest fixpoint* of f

> Guarantees existence of least and greatest fixpoints for *monotonic functions* **and** tells even how to compute them.

Monotonic Functions

Proof for $f^n(\emptyset)$ is the *least* *fixpoint* of f

- Since $\emptyset \subseteq f(\emptyset)$, show by induction $f^k(\emptyset) \subseteq f^{k+1}(\emptyset)$
- If $f^k(\emptyset) = f^{k+1}(\emptyset)$ for some k, then
  $f^l(\emptyset) = f^{l+1}(\emptyset)$ for all $l > k$
- If $f^k(\emptyset) \subsetneq f^{k+1}(\emptyset)$, then $f^{k+1}(\emptyset)$ must contain at least one element more than $f^k(\emptyset)$

$\Rightarrow f^k(\emptyset) \subsetneq f^{k+1}(\emptyset)$ for at most n k's
$\Rightarrow f^n(\emptyset) = f^{n+1}(\emptyset)$ is a *fixpoint*

Monotonic Functions

Proof for $f^n(\emptyset)$ is the *least fixpoint* of f

- Given another fixpoint P, we have $\emptyset \subseteq P$
- Hence $f(\emptyset) \subseteq f(P)$, hence $f(\emptyset) \subseteq P$ (P is fixpoint)
- By induction $f^k(\emptyset) \subseteq P$ for all k>0
- In particular $f^n(\emptyset) \subseteq P$

$\Rightarrow f^n(\emptyset)$ is the *least fixpoint*

Similar proof for greatest fixpoint

Monotonic Functions

Examples

Let S:={0,1,2,3}

f(P) := $P \cup \{2\}$
- fixpoints {2}, {0,2}, {1,2}, {3,2}, {0,1,2}, {1,2,3}, {0,2,3}, {0,1,2,3}.
- $f(\emptyset)$={2}, f({2})={2} $\Rightarrow$ least fixpoint {2}
- f(S) = S $\Rightarrow$ greatest fixpoint S

f(P) := P \ {2}
- fixpoints $\emptyset$, {0}, {1}, {3}, {0,1}, {1,3}, {0,3}, {0,1,3}.
- $f(\emptyset)$= …
- f(S) = …

Fixpoint Characterization

We have

- Knaster-Tarski Theorem, which gives us a way to compute least and greatest fixpoints.
- And the following equalities
  - [| EG ϕ |] = { s | $\exists$ (s,s') $\in \rightarrow$ s.t. s' $\in$ [| EG ϕ |] }
  - [| E ϕ U ψ |]= [| ψ |] $\cup$ ([| ϕ |] $\cap$ {s| …})

[| EG ϕ |] and [| E ϕ U ψ |] are fixpoints !!!

Fixpoint Characterization

Exist globally

[| EG ϕ |] is a fixpoint of

$f_{EG}(P) = [| \phi |] \cap \{ s \mid \exists (s,s') \in \rightarrow \text{ s.t. } s' \in P \}$

Theorem:

- f_{EG} is monotonic
- [| EG ϕ |] is the greatest fix-point
- [| EG ϕ |] = $f^{n}_{EG}(S)$

Fixpoint Characterization

Proof: f is monotonic

Suppose $P \subseteq Q$, then

$$
\begin{aligned}
f_{EG}(P) &= [| \phi |] \cap \{ s \mid \exists (s,s') \in \rightarrow \text{ s.t. } s' \in P \} \\
&\subseteq [| \phi |] \cap \{ s \mid \exists (s,s') \in \rightarrow \text{ s.t. } s' \in Q \} \quad // P \subseteq Q \\
&= f_{EG}(Q)
\end{aligned}
$$

Fixpoint Characterization

Proof: [| EG ϕ |] is the greatest fix-point

Let P be fixpoint of f. Let $s_0 \in P$. Show $s_0 \in$ [| EG ϕ |].

- We have $s_0 \in f_{EG}(P) = [|\phi|] \cap \{ s \mid \exists (s,s') \in \rightarrow \text{ s.t. } s' \in P \}$
- Hence M, $s_0 \models \phi$, and there exists $s_1 \in P$ with $(s_0, s_1') \in \rightarrow$
- By induction, show there exists for all $k \geq 0$ a state s_k with M, $s_k \models \phi$ and $(s_k, s_{k+1}') \in \rightarrow$
- There exists an infinite path $s_0, s_1, \ldots$ with M,$s_i \models \phi$ for all $i \geq 0$

$\Rightarrow$ M, $s_0 \models$ EG ϕ

$\Rightarrow$ $s_0 \in$ [| EG ϕ |].

Fixpoint Characterization

Proof: [| EG ϕ |] = $f^{n}_{EG}(S)$

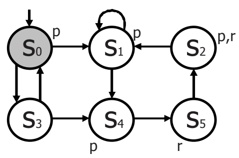
Follows directly from Knaster-Tarski Theorem.

Fixpoint Characterization

Example: EG p

$f_{EG}(P) = [| \; p \; |] \cap \{ s \mid \exists (s,s') \in \rightarrow \text{ s.t. } s' \in P \}$

$S = \{s_0, s_1, s_2, s_3, s_4, s_5\}$
$f_{EG}^1(S) = \{s_0, s_1, s_2, s_4\}$
$f_{EG}^2(S) = \{s_0, s_1, s_2\}$
$f_{EG}^3(S) = \{s_0, s_1, s_2\}$



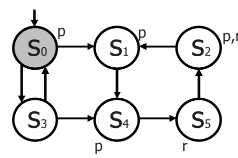
$\Rightarrow [|EG \; p|] = \{s_0, s_1, s_2\}$

Fixpoint Characterization

Example: EG p

$f_{EG}(P) = [| \; p \; |] \cap \{ s \mid \exists (s,s') \in \rightarrow \text{ s.t. } s' \in P \}$

$S = \{s_0, s_1, s_2, s_3, s_4, s_5\}$
$f_{EG}^1(S) = \{s_0, s_1, s_2, s_4\}$
$f_{EG}^2(S) = \{s_0, s_1, s_2\}$
$f_{EG}^3(S) = \{s_0, s_2\}$
$f_{EG}^4(S) = \emptyset$
$\Rightarrow [|EG \; p|] = \emptyset$



Fixpoint Characterization

Exist globally

$[| \; E \; \phi \; U \; \psi \; |]$= is a fixpoint of

$f_{EU}(P) = [|\psi|] \cup ([|\phi|] \cap \{ s \mid \exists (s,s') \in \rightarrow \text{ s.t. } s' \in P \})$

Theorem:

- f_{EU} is monotonic
- $[| \; E \; \phi \; U \; \psi \; |]$= is the least fix-point
- $[| \; E \; \phi \; U \; \psi \; |] = f_{EU}^{\,n}(\emptyset)$

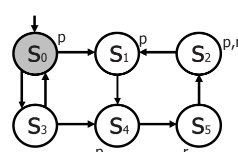
Without proof

Fixpoint Characterization

Example: E p U r

$f_{EU}(P) = [|r|] \cup ([|p|] \cap \{ s \mid \exists (s,s') \in \rightarrow \text{ s.t. } s' \in P \})$

$f_{EG}^1(\emptyset) = \{s_2, s_5\}$
$f_{EG}^2(\emptyset) = \{s_2, s_4, s_5\}$
$f_{EG}^3(\emptyset) = \{s_1, s_2, s_4, s_5\}$
$f_{EG}^4(\emptyset) = \{s_0, s_1, s_2, s_4, s_5\}$
$f_{EG}^5(\emptyset) = \{s_0, s_1, s_2, s_4, s_5\}$



$\Rightarrow [| \; E \; p \; U \; r \; |] = \{s_0, s_1, s_2, s_4, s_5\}$

Summary

Semantic of CTL with fixpoints

Given Kripke structure M=(S, s_0, →, μ), with n states, and ϕ in ENF over atomic propositions AP.

- [|true|] = S
- [|false|] = ∅
- [| p |] = { s | p ∈ μ(s) }
- [|¬ ϕ |] = S \ [| ϕ |]
- [| ϕ ∧ ψ |] = [| ϕ |] ∩ [| ψ |]
- [| E ϕ U ψ |]= $f_{EU}^n(\emptyset)$
- [| EG ϕ |] = $f_{EG}^n(S)$

- Translates to an algorithm based on sets
- Sets of states as unordered list lists are inefficient
- We need
  - Compact set representation
  - Efficient operations on sets

Outlook

Next Week

- OBDDs
- Symbolic CTL model checking
- SMV

Comp4151 Ansgar Fehnker