Note Title 3/12/2010

Soundness of LTL Model Checking

Aditya Kanade

E0223, CSA, IISc.

Note Title 3/12/2010

LTL Model Checking

TS $\models \varphi$?

Step	Algorithm	Soundness
1.	LTL $\rightarrow$ GNBA	$L_\omega(G_{\neg\varphi}) = \text{words}(\neg\varphi)$
2.	GNBA $\rightarrow$ NBA	$L_\omega(G_{\neg\varphi}) = L_\omega(A_{\neg\varphi})$
3.	TS $\otimes$ A	Product construction
4.	TS $\otimes$ A $\models \Diamond\Box\neg F$ (persistence checking)	Nested DFS

LTL to GNBA

To prove that $L_\omega(G_\varphi) = \text{words}(\varphi)$.

$\subseteq$: Let $\sigma = A_0 A_1 A_2 \cdots \in \text{words}(\varphi)$.

(a) There exists a run $\overline{\sigma} = B_0 B_1 B_2 \cdots$ of G_φ on σ.

(b) The run $\overline{\sigma}$ is an accepting run of G_φ.

$\supseteq$: If $\sigma = A_0 A_1 A_2 \cdots \in L_\omega(G_\varphi)$ then $\sigma \models \varphi$.

$L_\omega(G_\varphi) \supseteq \text{words}(\varphi)$

Let $\sigma = A_0 A_1 A_2 \cdots \in \text{words}(\varphi)$.

(a) Let $B_i = \{ \psi \in \text{closure}(\varphi) \mid A_i A_{i+1} \cdots \vdash \psi \}$.

- B_i is an elementary set of formulae i.e. $B_i \in \wp$.
- $B_{i+1} \in \delta(B_i, A_i)$, for all $i \geq 0$.
  - $A_i = B_i \cap AP \Rightarrow \delta(B_i, A_i) \neq \emptyset$
  - $\bigcirc \psi \in B_i$ iff $\psi \in B_{i+1}$ $\approx$ Def. of δ in the construction
  - $\psi_1 \cup \psi_2 \in B_i$ iff $(\psi_2 \in B_i)$ or $(\psi_1 \in B_i$ and $\psi_1 \cup \psi_2 \in B_{i+1})$
    $\approx$ Def. of δ in the construction

[This part is not discussed in the additional slides]

(b) Prove that $B_i \in F_{(\psi_1 U \psi_2)}$, for infinitely many i, for all $\psi_1 U \psi_2 \in$ closure(φ).

Let there be finitely many j such that $B_j \in F_{(\psi_1 U \psi_2)}$.

$B_i \notin F_{(\psi_1 U \psi_2)} \Rightarrow \psi_1 U \psi_2 \in B_i$ and $\psi_2 \notin B_i$ .... (construction)

Now, $A_i A_{i+1} \cdots \models \psi_1 U \psi_2$ and $A_i A_{i+1} \cdots \not\models \psi_2$ ... (Def. of B_i)

Hence, there exists $k > i$, $A_k A_{k+1} \cdots \models \psi_2$.

Thus, $\psi_2 \in B_k$. Further, $B_k \in F_{(\psi_1 U \psi_2)}$.

If $B_i \notin F_{(\psi_1 U \psi_2)}$ for i.m. i then $B_k \in F_{(\psi_1 U \psi_2)}$ for i.m. k.

Hence, $\overline{G} = B_0 B_1 B_2 \cdots$ is an accepting run of G_φ.

$$L_\omega(G_\varphi) \subseteq \text{words}(\varphi)$$

Let $\sigma = A_0 A_1 A_2 \ldots \in L_\omega(G_\varphi)$.

Let $B_0 B_1 B_2 \ldots$ be the corr. accepting run of G_φ.

We have $A_i = B_i \cap AP$. and

$$\sigma = (B_0 \cap AP)(B_1 \cap AP)(B_2 \cap AP) \ldots \models \varphi \ ?$$

Prove that,

for all $\psi \in \text{closure}(\varphi)$,

$\psi \in B_0$ iff $A_0 A_1 A_2 \ldots \models \psi$.

Proof by structural induction on the structure of ψ.

Base case: $\psi \equiv true^*$, $\psi \in AP^*$ (* Ref. to additional slides)

Induction step: $\psi_1 \wedge \psi_2^*$, $O\psi^*$, $\psi_1 \cup \psi_2$

1. If $\psi_1 \cup \psi_2 \in B_0$ then $A_0 A_1 A_2 \ldots \models \psi_1 \cup \psi_2$.

   $\psi_1 \in B_0$ or $\psi_2 \in B_0$.

   * Let $\psi_2 \notin B_j$, for all $j \geq 0$.

     $\psi_1 \in B_j$ and $\psi_1 \cup \psi_2 \in B_j$, for $j \geq 0$ (by construction).

   However, $B_0 B_1 B_2 \ldots$ is accepting.

Therefore, $B_j \in F_{(\psi_1 \cup \psi_2)}$ for $i.m.\ j \geq 0$.

But, we just showed that,

$\psi_2 \notin B_j$ * and $\psi_1 \cup \psi_2 \in B_j$ •

iff

$B_j \notin F_{(\psi_1 \cup \psi_2)}$, for all j ---(by construction)

Contradiction.

Hence, $\psi_2 \in B_j$ and $\psi_1 \in B_i$, $0 \leq i < j$ --(by construction)

By hypothesis, $A_j \cdots \models \psi_2$, $A_i \cdots \models \psi_1$, $0 \leq i < j$.

Hence, $A_0 A_1 \cdots \models \psi_1 \cup \psi_2$.

2. If $A_0 A_1 \cdots \models \psi_1 \cup \psi_2$ then $\psi_1 \cup \psi_2 \in B_0$.

Let $A_0 A_1 \cdots \models \psi_1 \cup \psi_2$. There exists a j s.t.

$A_j A_{j+1} \cdots \models \psi_2 \implies \psi_2 \in B_j$ (by induction hypothesis)

$A_i A_{i+1} \cdots \models \psi_2 \implies \psi_1 \in B_i$, $0 \leq i < j$

By the definition of elementary sets:

$\psi_1 \cup \psi_2 \in B_j$

$\psi_1 \cup \psi_2 \in B_i \cdots 0 \leq i < j$.

Hence, proved.

GNBA to NBA

To prove that $L_\omega(G_\varphi) = L_\omega(A_\varphi)$

Let F be the acc. set of A_φ and $F_1, \ldots, F_k$ be acc. sets of G_φ.

$\supseteq$: Let $w \in L_\omega(A_\varphi)$ and ρ be the corr. acc. run.

$Inf(\rho) \cap F \neq \phi$ iff $Inf(\rho) \cap F_i \neq \phi$, for all i.

Thus, $w \in L_\omega(G_\varphi)$.

$\subseteq$: Let $w \in L_\omega(G_\varphi)$. Suppose $w \notin L_\omega(A_\varphi)$.

Let the run ρ of A on w be stuck in an i'th copy.

Thus, $Inf(\rho) \cap F_i = \phi$. Otherwise, you escape.

the run ρ corr. to a run ρ' of G_φ (on the first comp.).

Contradiction.

Soundness of Nested DFS

To prove that the nested DFS does not miss a cycle containing $s \not\in a$ (even though we ignore the states visited in previous calls to CYCLE_CHECK.)

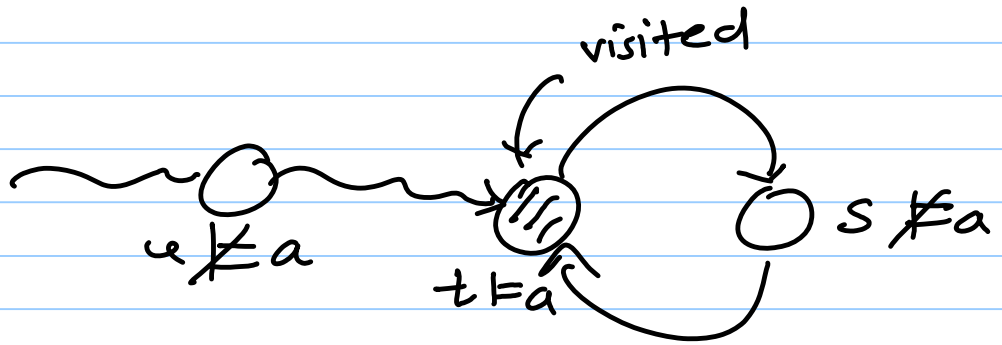
To prove that upon calling CYCLE_CHECK(s), there is no cycle of the form $s\, t_1 \cdots t_k\, s$ such that some $t_i \in V$, $1 \leq i \leq k$.

V: global set of visited states

Suppose there is some $t_i = t$ s.t. $t \in V$.

There must be some $u \not\models a$ s.t. t was visited during a call CYCLE_CHECK(u) < CYCLE_CHECK(s)*.

We therefore have the following reachability relations:



(a) Let u precede s in the Outer DFS.

Hence, CYCLE-CHECK(s) < CYCLE-CHECK(u).

Contradiction with *

(b) Let s precede u in the Outer DFS.

Hence, u is reachable from s ... (as s was on the stack.)

Already, t is reachable from u and

s is reachable from t

$\Rightarrow$ s is reachable from u.

This (or some other) cycle containing u should be detected @ no call of CYCLE-CHECK(s).