

Correctness of LTL Model Checking

Aditya Kanade

EO223, CSA, IISc.

LTL Model Checking

TS $\models \varphi$?

Step	Algorithm	Correctness
1.	LTL \rightarrow GNBA	$L_w(G_{\neg\varphi}) = \text{words}(\neg\varphi)$
2.	GNBA \rightarrow NBA	$L_w(G_{\neg\varphi}) = L_w(A_{\neg\varphi})$
3.	TS \otimes NBA $\models \langle \square \neg F$ (product construction)	Nested DFS

LTL to GNBA

To prove that $Lw(G_\psi) = \text{words}(\psi)$.

\supseteq : Let $\sigma = A_0 A_1 A_2 \dots \in \text{words}(\psi)$.

(a) There exists a run $\bar{\sigma} = B_0 B_1 B_2 \dots$ of G_ψ on σ .

(b) The run $\bar{\sigma}$ is an **accepting run** of G_ψ .

\subseteq : If $\sigma = A_0 A_1 A_2 \dots \in Lw(G_\psi)$ then $\sigma \models \psi$.

$$Lw(\mathcal{G}_\psi) \supseteq \text{words}(\psi)$$

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

(a) Let $B_i = \{ \gamma \in \text{closure}(\psi) \mid A_i A_{i+1} \dots \models \gamma \}$.

- B_i is an elementary set of formulae i.e. $B_i \in \mathcal{Q}$.

- $B_{i+1} \in \mathcal{J}(B_i, A_i)$, for all $i \geq 0$.

- $A_i = B_i \cap AP$

- $\neg \gamma \in B_i$ iff $\gamma \in B_{i+1}$

- $\gamma_1 \cup \gamma_2 \in B_i$ iff $(\gamma_2 \in B_i)$ or $(\gamma_1 \in B_i \text{ and } \gamma_1 \cup \gamma_2 \in B_{i+1})$

(b) Prove that $B_i \in F_{(r_1 \cup r_2)}$, for infinitely many i ,
for all $r_1 \cup r_2 \in \text{closure}(\psi)$.

Let there be finitely many i such that $B_i \in F_{(r_1 \cup r_2)}$.

$B_i \notin F_{(r_1 \cup r_2)} \Rightarrow r_1 \cup r_2 \in B_i$ and $r_2 \notin B_i \dots$ (construction)

Now, $A_i A_{i+1} \dots \in r_1 \cup r_2$ and $A_i A_{i+1} \dots \notin r_2$.

Hence, there exists $k > i$, $A_k A_{k+1} \dots \in r_2$.

Thus, $r_2 \in B_k$. Further, $B_k \in F_{(r_1 \cup r_2)}$
if $B_i \notin F_{(r_1 \cup r_2)}$ for i.m. i then $B_k \in F_{(r_1 \cup r_2)}$ for i.m. k .

Hence, $\bar{\sigma} = B_0 B_1 B_2 \dots$ is an accepting run of G_ψ .

$$Lw(G_\psi) \subseteq \text{words}(\psi)$$

Let $s = A_0 A_1 A_2 \dots \in Lw(G_\psi)$.

Let $B_0 B_1 B_2 \dots$ be the corr. accepting run of G_ψ .

We have $A_i = B_i \cap AP$ and

$$s = (B_0 \cap AP) (B_1 \cap AP) (B_2 \cap AP) \dots \models \psi ?$$

Prove that,

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

$$r \in B_0 \text{ iff } A_0 A_1 A_2 \dots \models r.$$

Proof by structural induction on the structure of r .

Base case: $r \equiv \text{true}$, $r \in AP$

Induction step: $r_1 \wedge r_2$, $O r$, $r_1 \cup r_2$

- If $r_1 \cup r_2 \in B_0$ then $A_0 A_1 A_2 \dots \models r_1 \cup r_2$.

$r_1 \in B_0$ or $r_2 \in B_0$.

* Let $r_2 \notin B_j$, for all $j \geq 0$.

$r_1 \in B_j$ and $r_1 \cup r_2 \in B_j$, for $j \geq 0$ (by induction).

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

Therefore, $B_j \in F_{(r_1 \cup r_2)}$ for $i.m. j \geq 0$.

But, we just showed that,

$$r_2 \notin B_j^* \text{ and } r_1 \cup r_2 \in B_j^{\bullet}$$

iff

$$B_j \notin F_{(r_1 \cup r_2)}, \text{ for all } j.$$

Contradiction.

Hence, $r_1 \in B_i$ and $r_2 \in B_j$.

Thus, $A_0 A_1 A_2 \dots \models r_1 \cup r_2$.

GNBA to NBA

To prove that $L_w(G_\psi) = L_w(A_\psi)$

\supseteq : Let $w \in L_w(A_\psi)$ and ρ be the corr. acc. run.

$\text{Inf}(\rho) \cap F \neq \emptyset$ iff $\text{Inf}(\rho) \cap F_i \neq \emptyset$, for all i .

Thus, $w \in L_w(G_\psi)$.

\subseteq : Let $w \in L_w(G_\psi)$. Suppose $w \notin L_w(A_\psi)$.

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

Thus, $\text{Inf}(\rho) \cap F_i = \emptyset$. Otherwise, you escape.
The run ρ corr. to a run ρ' of G_ψ (on the first comp.).
Contradiction.