COL750: Foundations of Automatic Verification (Jan-May 2023)

Extra Lecture (LTL Model Checking)[1]

Kumar Madhukar

madhukar@cse.iitd.ac.in

March 6th

[1] to make-up for the one cancelled on Feb 13th

LTL to Büchi Automata

- Construction
- Correctness

Construction

Here is the reference material for the construction and the correctness proof:

https://www.cmi.ac.in/~madhavan/papers/pdf/isical97.pdf (see Section 3)

Correctness

Let α be an LTL formula.

Let $Voc(\alpha)$ be the set of atomic propositions used in α.

Let M $(= P_0, P_1, \ldots)$ be an infinite word over $2^{Voc(\alpha)}$.

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k)$ *iff* $M, 0 \models \alpha$

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \to M, 0 \vDash \alpha$

Let $A_0, A_1, \ldots$ be an accepting run of $\mathcal{A}_\alpha$ on M.

For all $\beta \in \mathrm{CL}(\alpha)$ and for every $i \geq 0$, we show that

$M, i \vDash \beta \;\; \textit{iff} \;\; \beta \in A_i$

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \vDash \alpha$

Induction (on structure of β).

If β is an atomic proposition p,

$M, i \vDash p$ *iff* $p \in P_i$ *iff* $p \in A_i$

Proof

$\beta = \neg\gamma$

$M, i \models \beta$ *iff* $M, i \models \neg\gamma$
iff (by the induction hypothesis) $\gamma \notin A_i$
iff (by the definition of an atom) $\neg\gamma \in A_i$
iff $\beta \in A_i$

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \models \alpha$

$\beta = \gamma \vee \delta$

Exercise.

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \vDash \alpha$

$\beta = X\gamma$

$M, i \vDash \beta$ *iff* $M, i+1 \vDash \gamma$
iff (by the induction hypothesis) $\gamma \in A_{i+1}$
iff (because $A_i \longrightarrow A_{i+1}$) $X\gamma \in A_i$
iff $\beta \in A_i$

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \vDash \alpha$

$\beta = \gamma U \delta$

(forward) $M, i \vDash \beta \;\rightarrow\; \beta \in A_i$

From the semantics of until, we know that

$M, k \vDash \delta$, for some $k \geq i$, and for all $i \leq j < k$, $M, j \vDash \gamma$

We show $\beta \in A_i$ by a second induction on $k - i$

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \to M, 0 \models \alpha$

(forward) $M, i \models \beta \;\to\; \beta \in A_i$

We show $\beta \in A_i$ by a second induction on $k - i$

Base case: $(k - i = 0)$

$M, i \models \delta$ implies $\delta \in A_i$ (main induction hypothesis), implies $\beta \in A_i$ (definition of atoms)

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \to M, 0 \vDash \alpha$

Induction step: $(k - i > 0)$

$M, i \vDash \gamma$, and $M, (i+1) \vDash \gamma U \delta$

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \vDash \alpha$

Induction step: $(k - i > 0)$

$M, i \vDash \gamma$, and $M, (i+1) \vDash \gamma U \delta$

$\gamma U \delta \in A_{i+1}$ (secondary induction hypothesis)

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \vDash \alpha$

Induction step: $(k - i > 0)$

$M, i \vDash \gamma$, and $M, (i+1) \vDash \gamma U \delta$

$\gamma U \delta \in A_{i+1}$ (secondary induction hypothesis)

$X(\gamma U \delta) \in A_i$ (the way transitions have been set up)

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \models \alpha$

Induction step: $(k - i > 0)$

$M, i \models \gamma$, and $M, (i+1) \models \gamma U \delta$

$\gamma U \delta \in A_{i+1}$ (secondary induction hypothesis)

$X(\gamma U \delta) \in A_i$ (the way transitions have been set up)

$\gamma \in A_i$ (main induction hypothesis)

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \vDash \alpha$

Induction step: $(k - i > 0)$

$M, i \vDash \gamma$, and $M, (i+1) \vDash \gamma U \delta$

$\gamma U \delta \in A_{i+1}$ (secondary induction hypothesis)

$X(\gamma U \delta) \in A_i$ (the way transitions have been set up)

$\gamma \in A_i$ (main induction hypothesis)

$\gamma U \delta \in A_i$ (definition of atoms)

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \vDash \alpha$

(reverse) $\beta \in A_i \;\rightarrow\; M, i \vDash \beta$

Let m be the index of the until formula β.

Since $A_0, A_1, \ldots$ is an accepting run of $(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k)$, there must exist a $k \geq i$ such that $A_k \in G_m$. Take the least such k.

Induction on $(k - i)$.

Base case: $k = i$.

$A_i \in G_m$. But $\gamma U \delta \in A_i$. So, $\delta \in A_i$.
$M, i \vDash \delta$ (main induction hypothesis)
$M, i \vDash \gamma U \delta$

Proof

Induction step: $(k - i > 0)$

Since $A_i \notin G_m$, $\delta \notin A_i$.

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \models \alpha$

Induction step: $(k - i > 0)$

Since $A_i \notin G_m$, $\delta \notin A_i$.

$\gamma, X(\gamma U \delta) \in A_i$

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \models \alpha$

Induction step: $(k - i > 0)$

Since $A_i \notin G_m$, $\delta \notin A_i$.

$\gamma, X(\gamma U \delta) \in A_i$

Because there is a transition from A_i to A_{i+1}, $\gamma U \delta \in A_{i+1}$

Proof

Induction step: $(k - i > 0)$

Since $A_i \notin G_m$, $\delta \notin A_i$.

$\gamma, X(\gamma U \delta) \in A_i$

Because there is a transition from A_i to A_{i+1}, $\gamma U \delta \in A_{i+1}$

$M, (i+1) \vDash \gamma U \delta$ (secondary induction hypothesis)

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \vDash \alpha$

Induction step: $(k - i > 0)$

Since $A_i \notin G_m$, $\delta \notin A_i$.

$\gamma, X(\gamma U \delta) \in A_i$

Because there is a transition from A_i to A_{i+1}, $\gamma U \delta \in A_{i+1}$

$M, (i+1) \vDash \gamma U \delta$ (secondary induction hypothesis)
$M, i \vDash \gamma$ (main induction hypothesis)

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \rightarrow M, 0 \vDash \alpha$

Induction step: $(k - i > 0)$

Since $A_i \notin G_m$, $\delta \notin A_i$.

$\gamma, X(\gamma U \delta) \in A_i$

Because there is a transition from A_i to A_{i+1}, $\gamma U \delta \in A_{i+1}$

$M, (i+1) \vDash \gamma U \delta$ (secondary induction hypothesis)
$M, i \vDash \gamma$ (main induction hypothesis)
$M, i \vDash \gamma U \delta$ (semantics of until)

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \leftarrow M, 0 \vDash \alpha$

Suppose, $M = P_0, P_1, \ldots$, such that $M, 0 \vDash \alpha$

For each $i \geq 0$, define A_i to be the set $\{\beta \in \text{CL}(\alpha) \mid M, i \vDash \beta\}$

Claim: each A_i is an atom, two consecutive atoms are connected by a transition in our construction, and A_0 is in an initial state. (exercise: verify these claims)

Claim: $A_0, A_1, \ldots$ is an accepting run.

Proof

$M \in \mathcal{L}(\mathcal{A}_\alpha, G_1, G_2, \ldots, G_k) \leftarrow M, 0 \vDash \alpha$

Suppose not.

Let G_m is the one not visited infinitely often. There is a k such that for all $j \geq k$, $A_j \notin G_m$.

$\gamma_m U \delta_m \in A_j$, $\delta_m \notin A_j$

But the way A_k has been constructed, $M, k \vDash \gamma_m U \delta_m$.

This conflicts with the fact that δ_m is not true any time in the future!

Counting and Non-counting Languages

A language $A \subseteq \Sigma^\omega$ is said to be non-counting if there is a number n_0 such that for every $n \geq n_0$ and for every $u, v \in \Sigma^\star$ and $\alpha \in \Sigma^\omega$,

$$uv^n\alpha \in A \quad \text{iff} \quad uv^{n+1}\alpha \in A$$

A is said to be counting if it is not non-counting.

Counting and Non-counting Languages

- $\{a, b\}^\omega$ is non-counting.
- $a^\star b\{a, b\}^\omega$ is also non-counting. Why? Exercise.
- $(aa)^\star b^\omega$ is counting. Why? Exercise.
- LTL can only define non-counting languages. (proof not in scope; not discussed in class)

LTL Model Checking with fairness

- no special treatment required
- the fairness constraints can be expressed in the LTL formula itself
- to restrict to paths where ϕ is true infinitely often, while verifying ψ, we instead verify $GF\phi \rightarrow \psi$

LTL Model Checking using CTL Model Checking

- the existence of an infinite path can be checked with EG $\top$
- the acceptance criteria can be given as fairness constraints '`FAIRNESS` $\neg(\delta U \gamma) \vee \gamma$'
- this constraint essentially says that it should hold infinitely often that if $\delta U \gamma$ is true, then γ is also true
- such a fairness constraint is added for every until formula is the closure

Thank you!