Lecture 3: Model checking

Zak Kincaid

September 26, 2016

Model Checking Problem: given a Kripke structure K and an LTL formula φ, do we have $K \models \varphi$?

Model Checking, as an algorithmic discipline: exhaustively explore all possible behaviours of the system, searching for a violation. Many tools for doing this efficiently (SPIN, nuSMV).

1 Automata over infinite words

Fix a set of propositions P.

- For any Kripke structure K, define $\mathcal{L}(K) = \{L(\pi) : \pi \in \mathit{Path}(K)\}$
- For any LTL formula φ, define $\mathcal{L}(\varphi) \triangleq \{\pi \in (2^P)^\omega : \pi \models \varphi\}$ to be the set of paths that satisfy φ.

Idea: $K \models \varphi$ exactly when $\mathcal{L}(K) \subseteq \mathcal{L}(\varphi)$.

If K is finite, then the model checking problem is decidable by reduction to inclusion testing for Büchi automata: there is a Büchi automaton that recognizes both $\mathcal{L}(K)$ and $\mathcal{L}(\varphi)$, and inclusion checking is decidable.

Definition 1.1 (Büchi automaton)**.** *A (non-deterministic) Büchi automaton* $A = \langle Q, \Sigma, \Delta, I, F\rangle$ *where*

- Q *is a finite set of states*
- Σ *is a finite alphabet*
- $\Delta \subseteq Q \times \Sigma \times Q$ *is a transition relation*

- *$I \subseteq Q$ is a set of initial states*

- *$F \subseteq Q$ is a set of final states*

A word $w = w_0 w_1 w_2 ... \in \Sigma^\omega$ is accepted by a Büchi automaton $A = \langle Q, \Sigma, \Delta, I, F \rangle$ if there exists an *accepting run* $q_0 q_1 q_2 ...$ consisting of an infinite sequence of states such that:

- $q_0 \in Q$ is initial

- for each i, $\langle q_i, w_i, q_{i+1} \rangle \in \Delta$

- The set $\{i : q_i \in F\}$ is infinite

Proposition 1.2. *Let K be a Kripke structure. There is a Büchi automaton $A(K)$ such that $\mathcal{L}(A(K)) = \mathcal{L}(K)$.*

Proof. Let $K = \langle K_S, K_I, K_R, K_L \rangle$ be a Kripke structure over a set of propositions P (for simplicity, suppose K_R is total). Define $A(K) = \{A_K, A_\Sigma, A_\Delta, A_I, A_F\}$ where

- $A_Q = K_S$

- $A_\Sigma = 2^P$

- $A_\Delta = \{\langle s, K_L(s), t \rangle : s \; K_R \; t\}$

- $A_I = K_I$

- $A_F = K_S$

□

Proposition 1.3. *For any Büchi automata A and B, there is an automaton that recognizes $\mathcal{L}(A) \cap \mathcal{L}(B)$.*

Proof. Construct as follows:

- $Q = A_Q \times B_Q \times \{A, B\}$

- $\Sigma = A_\Sigma$

- The transition relation Δ is defined to be the set of all $\langle (a, b, c), \sigma, (a', b', c) \rangle$ such that:

- $\langle a, \sigma, a' \rangle \in \Delta_A$,
- $\langle b, \sigma, b' \rangle \in \Delta_B$,
- $c = A, a \in A_F$ implies $c' = B$
- $c = B, b \in B_F$ implies $c' = A$
- $c = A \wedge a \notin A_F$ or $c = B \wedge b \notin B_F$ implies $c' = c$.
- $A_I = \{(a, b, A) : a \in A_I, b \in B_I\}$
- $A_F = \{\langle a, b, B \rangle : b \in F\}$

$\square$

Proposition 1.4. *For any Büchi automaton A, there is an automaton that recognizes* $\bar{(}\mathcal{L}A)$

- However, this is complicated and can be avoided: rather than checking $\mathcal{L}(A(K)) \cap \overline{\mathcal{L}(A(\varphi))} = \emptyset$, we check $\mathcal{L}(A(K)) \cap \mathcal{L}(A(\neg\varphi)) = \emptyset$.

2 LTL tableaux

Automata are *local* in the sense that they make decisions based on the next letter of the sequence. Let's localize LTL semantics so that satisfaction $\pi \models \varphi$ is expressed only in terms of π, π_0, and $\pi[1...]$. Most are already local:

$$\begin{aligned} \pi \models p &\iff \pi_0 \models p \\ \pi \models \varphi \vee \psi &\iff \pi \models \varphi \vee \pi \models \psi \\ \pi \models \neg\varphi &\iff \pi \not\models \varphi \\ \pi \models \mathbf{X}\varphi &\iff \pi[1...] \models \varphi \end{aligned}$$

The one that is not is $\varphi \, \mathbf{U} \, \psi$. However, we can take

$$\pi \models \varphi \, \mathbf{U} \, \psi \iff \pi \models \psi \text{ or } \pi \models (\varphi \wedge (\varphi \, \mathbf{U} \, \psi))$$

Thus, the evaluation of an LTL formula can be expressed in terms of its sub-formulas:

$$\begin{aligned} sub(p) &= \{p\} \\ sub(\varphi_1 \vee \varphi_2) &= \{\varphi_1 \vee \varphi_2\} \cup sub(\varphi_1) \cup sub(\varphi_2) \\ sub(\neg\varphi) &= \{\neg\varphi\} \cup sub(\varphi) \\ sub(\mathbf{X}\varphi) &= \{\mathbf{X}\varphi\} \cup sub(\varphi) \\ sub(\varphi \mathbf{U} \psi) &= \{\varphi \mathbf{U} \psi, \mathbf{X}(\varphi \mathbf{U} \psi)\} \cup sub(\varphi) \cup sub(\psi) \end{aligned}$$

Note: $|sub(\varphi)| \leq 2|\varphi|$.

Definition 2.1. *A set $\Phi \subseteq sub(\varphi)$ is* consistent *if:*

- *for all $\varphi_1 \vee \varphi_2 \in sub(\varphi)$, $\varphi_1 \vee \varphi_2 \in \Phi \iff \varphi_1 \in sub(\varphi)$ or $\varphi_2 \in \Phi$*
- *for all $\neg\psi \in sub(\varphi)$, $\neg\psi \in \Phi \iff \psi \notin \Phi$*
- *for all $\psi_1 \mathbf{U} \psi_2 \in sub(\varphi)$, $\psi_1 \mathbf{U} \psi_2 \in \Phi \iff \psi_2 \in \Phi$ or both $\psi_1 \in \Phi$ and $\mathbf{X}(\psi_1 \mathbf{U} \psi_2) \in \Phi$.*

Definition 2.2 (Generalized Büchi automaton)**.** *A* Generalized Büchi automaton *(GBA) is a Büchi automaton equipped with a* set $\mathcal{F}$ *of sets of final states. A word is accepted by a GBA if there is an accepting run such that each $F \in \mathcal{F}$ is visited infinitely often.*

Proposition 2.3. *For any generalized Büchi automaton A, there is a Büchi automaton that accepts the same language.*

Proof. The construction is similar to the one for intersection. Let $A = \langle A_Q, A_\Sigma, A_\Delta, A_I, A_\mathcal{F}\rangle$ be a GBA. Write $A_\mathcal{F}$ as $A_\mathcal{F} = \{F_0, ..., F_n\}$

- $Q = A_Q \times \{0, ..., n\}$
- $\Sigma = A_\Sigma$
- $\Delta = \{\langle (a,i), \sigma, (a', i')\rangle : \langle a, \sigma, a'\rangle \in \Delta_A, i' = i + 1_{a \in F_i} \mod (n+1)\}$ where $1_{a\in F_i} = \begin{cases} 1 & \text{if } a \in F_i \\ 0 & \text{otherwise} \end{cases}$
- $A_I = \{(a, 0) : a \in A_I\}$
- $A_F = \{\langle a, n\rangle : a \in F_n\}$

□

Definition 2.4 (LTL tableau)**.** *Let φ be an LTL formula. Its* tableau *is a generalized Büchi automaton $A(\varphi) = \langle Q, \Sigma, \Delta, I, \mathcal{F}\rangle$ where*

- $Q = \{\Phi \in 2^{sub(\varphi)} : \Phi \textit{ is consistent}\}$
- $\Sigma = 2^P$
- $\Delta = \{\langle \Phi, \sigma, \Psi\rangle : \forall \mathbf{X}\varphi \in sub(\varphi), \mathbf{X}\varphi \in \Phi \iff \varphi \in \Psi, \sigma = P \cap \Phi\}$
- $I = \{\Phi \in Q : \varphi \in I\}$
- *For each $\varphi\ \mathbf{U}\ \psi \in sub(\varphi)$, define $F_{\varphi \mathbf{U} \psi} \triangleq \{\Phi \in Q : \varphi\ \mathbf{U}\ \psi \notin \Phi \vee \psi \in \Phi\}$. Define $\mathcal{F} = \{F_{\varphi\mathbf{U}\psi} : \varphi\ \mathbf{U}\ \psi \in sub(\varphi)\}$.*

Theorem 2.5. $\mathcal{L}(\varphi) = \mathcal{L}(A(\varphi))$.

Proof. For any path π, define $sat_\varphi(\pi) \triangleq \{\psi \in sub(\varphi) : \pi \models \varphi\}$. Clearly, $sat_\varphi(\pi)$ is consistent for any π.

"$\mathcal{L}(\varphi) \subseteq \mathcal{L}(A(\varphi))$". Prove that for any $\pi \in \mathcal{L}(\varphi)$ we have $\pi \in \mathcal{L}(A(\varphi))$. We want to show that

$$sat_\varphi(\pi) sat_\varphi(\pi[1...]) sat_\varphi(\pi[2...])$$

is an accepting run. To show that this is a run of $A(\varphi)$, we must show that for any π, $\langle sat_\varphi(\pi), \pi_0, sat_\varphi(\pi[1...])\rangle \in \Delta$. This follows directly from the definitions. To show that this is an *accepting* run, we must show that it meets each $F_{\psi_1 \mathbf{U} \psi_2}$ infinitely often. It must be the case that either

- $\psi_1\ \mathbf{U}\ \psi_2$ is satisfied infinitely often, and so ψ_2 must also be satisfied infinitely often (and so $sat_\varphi(\pi[i...])$ contains ψ_2 infinitely often), or
- $\psi_1\ \mathbf{U}\ \psi_2$ is not satisfied infinitely often (and so $sat_\varphi(\pi[i...])$ doesn't contain $\psi_1\ \mathbf{U}\ \psi_2$ infinitely often).

"$\mathcal{L}(A(\varphi)) \subseteq \mathcal{L}(\varphi)$" We prove that for all $\psi \in sub(\varphi)$, for all consistent Φ and all $\pi \in \mathcal{L}(\Phi)$, $\psi \in \Phi \iff \pi \models \psi$. Since the accepting states of $A(\varphi)$ all contain φ this implies that $\mathcal{L}(A(\varphi)) \subseteq \mathcal{L}(\varphi)$. We prove the result by induction on ψ. Let Φ be a consistent set and let $\pi \in \mathcal{L}(\Phi)$.

- Case $p \in P$: $\pi \in \mathcal{L}(\Phi)$ implies that $\pi_0 = P \cap \Phi$ (by def'n of Δ). $\pi \models p \iff \pi_0 \models p \iff p \in \Phi$.
- Case $\psi_1 \vee \psi_2$: By consistency, $\psi_1 \vee \psi_2 \in \Phi \iff \psi_1 \in \Phi \vee \psi_2 \in \Phi$. By the induction hypothesis, $\psi_1 \in \Phi \iff \pi \models \psi_1$ and $\psi_2 \in \Phi \iff \pi \models \psi_2$, so $\psi_1 \vee \psi_2 \in \Phi \iff \pi \models \psi_1 \vee \pi \models \psi_2 \iff \pi \models \psi_1 \vee \psi_2$.

- Case $\neg\psi$: By consistency, $\neg\psi \in \Phi \iff \psi \notin \varphi$. By induction hypothesis, $\psi \notin \Phi \iff \pi \not\models \varphi$. So $\not\psi \in \Phi \iff \pi \notin \varphi \iff \pi \models \not\varphi$.
- Case $\mathbf{X}\psi$: Since $\pi \in \mathcal{L}(\Phi)$, there is some Φ' such that $\pi[1...] \in \mathcal{L}(\Phi')$ and $\langle \Phi, \pi_0, \Phi' \rangle \in \Delta$. By def'n, $\mathbf{X}\psi \in \Phi \iff \psi \in \Phi'$ By the induction hypothesis, $\pi[1...] \in \mathcal{L}(\Phi')$ entails that $\varphi \in \Phi' \iff \pi[1...] \models \psi$. So $\mathbf{X}\psi \in \Phi \iff \pi \models \mathbf{X}\psi$.
- Case $\psi_1 \mathbf{U} \psi_2$: Let $\Phi_0\Phi_1...$ be an accepting run for π.
  - $\pi \models \psi_1 \mathbf{U} \psi_2$: There exists some *least* i such that $\pi[j...] \models \psi_2$ and $\pi[i...] \models \psi_1$ for all $j < i$. By the induction hypothesis, $\psi_2 \in \Phi_i$ and $\psi_1 \in \Phi_j$ for all $j < i$. We may prove by induction that $\psi_1 \mathbf{U} \psi_2 \in \Phi_j$ for all $j \leq i$, so $\psi_1 \mathbf{U} \psi_2 \in \Phi$.
  - $\pi \not\models \psi_1 \mathbf{U} \psi_2$:
    * Case $\pi[i...] \models \psi_1$ for all i, and $\pi[i...] \not\models \psi_2$ for all i. By IH, $\psi_1 \in \Phi_i$ for all i and $\psi_2 \notin \Phi_i$ for all i. For a contradiction, suppose that $\psi_1 \mathbf{U} \psi_2 \in \Phi$. Prove by induction that $\psi_1 \mathbf{U} \psi_2 \in \Phi_i$ for all i. This contradicts the fact that infinitely many Φ_i must be in $F_{\psi_1 \mathbf{U} \psi_2}$.
    * Case there exists some *least* i such that $\pi[i...] \not\models \psi_1$, $\pi[i...] \not\models \psi_2$, and $\pi[j...] \models \psi_1$ for all $j < i$. By the induction hypothesis, $\psi_1 \in \Phi_j$ for all $j < i$, and $\psi_1, \psi_2 \notin \Phi_j$. Prove by induction that for all $j \leq i$, $\psi_1 \mathbf{U} \psi_2 \notin \Phi_j$.

$\square$