Lecture 23: Progress Verification

Huan Zhang
huan@huan-zhang.com

Slides adapted from Prof. Sayan Mitra’s slides in Fall 2021
Homework and final presentations

HW 3 due 4/27

HW 4 due 5/11

Final project presentation slides due 4/30, 8 am (hard deadline, since presentations will start at 11 am)

Final project presentations:

   Tuesday 11 am - 12:20 pm, ECEB 3015 (lecture time)

   Friday 2 pm - 3:30 pm, ECEB 2015

Schedule will be announced by the end of this week. If you cannot present on Friday, please let me and the TA Sanil (schawla7@illinois.edu) know by Thursday (4/25)

Final project report due: 5/11
Visualizing CTL semantics

Path quantifiers
- E: Exists some path
- A: All paths

Temporal operators
- X: Next state
- U: Until
- F: Eventually
- G: Globally (Always)

$q \models EF \text{ red}$
$q \models EG \text{ red}$
$q \models A [\text{red U green}]$
$q \models AX \text{ red}$

$q \models AF \text{ red}$
$q \models AG \text{ red}$
$q \models E [\text{red U green}]$
$q \models EX \text{ red}$

Slides adapted from Prof. Sayan Mitra’s slides in Fall 2021
Progress properties

• Every behavior system $\mathcal{A}$ will eventually reach a goal $\text{goal}$

• CTL: $\text{AF goal}$

• Dijkstra: From any state, (possibly $>1$ tokens) all executions get to a state with 1 token

Invariance/safety

• No behavior of $\mathcal{A}$ goes outside of $\text{unsafe}$

• CTL: $\text{AG unsafe}$

• Dijkstra: Starting a state with a 1 token, all executions have 1 token

• Finding a counterexample to safety does not prove progress
Proving termination for automata

• Automaton $\mathcal{A} = (V, \Theta, D)$
• Recall $D \subseteq \text{val}(V) \times \text{val}(V)$
• Automaton terminates if it does not have any infinite executions

• **Definition:** A **well-founded relation** $<$ on a set $S$ is a binary relation $< \subseteq S \times S$ such that every subset $S' \subseteq S$ has a **least** element.

• In other words, there are no infinite decreasing chains of elements $s_0, s_1, \ldots$, with $s_{i+1} < s_i$.
• Example: totally order set, e.g., $\{1, 2, 3, \ldots\}$ with the usual order
• Example: $S = \mathbb{Z}^+$ $a < b$ iff $a$ divides $b$ and $a \neq b$
• Example: $S = \{0,1\}^*$ $a < b$ iff $a$ is a proper substring of $b$
• Example: $S = \{-1, -2, -3, \ldots\}$, $<$ is the usual order, then $<$ is **not** a well-founded relation
Proving termination for automata

**Theorem.** Automaton $\mathcal{A} = (V, \Theta, D)$ terminates iff there exists a well-founded relation $R$ such that $D \cap \text{Reach}_{\mathcal{A}} \times \text{Reach}_{\mathcal{A}} \subseteq R$.

Proof. If there exists $R$ and automaton does not terminate.
Then there exists an infinite sequence of states $s_0, s_1, \ldots$, with $s_i \not\in D$ $s_{i+1}$. Since these are reachable states, $s_i \not\in R$ $s_{i+1}$. This violates the definition of a well-founded relation.
Suppose $\mathcal{A}$ is terminating, we define

$$R = D \cap \text{Reach}_{\mathcal{A}} \times \text{Reach}_{\mathcal{A}}$$

check that $R$ is indeed well-founded (because $D$ does not permit infinite sequences)
Ranking functions

Often the well-founded relation is defined in terms of a ranking function $f: val(V) \to \mathbb{N}$ such that for any reachable $\nu \in val(V)$ and $\nu'$ such that $(\nu, \nu') \in D$, $f(\nu') < f(\nu)$

Here $<$ is a the usual comparison on integers

Instead of $\mathbb{N}$, the ranking function could use any other range set with a lower bound
```plaintext
Example

<table>
<thead>
<tr>
<th>automaton</th>
<th>UpDown</th>
</tr>
</thead>
<tbody>
<tr>
<td>signature</td>
<td></td>
</tr>
<tr>
<td>internal</td>
<td>up(d: Nat), down</td>
</tr>
<tr>
<td>variables</td>
<td></td>
</tr>
<tr>
<td>internal</td>
<td>x, y: Int</td>
</tr>
<tr>
<td>transitions</td>
<td></td>
</tr>
<tr>
<td>internal</td>
<td>up(d) where d = 1</td>
</tr>
<tr>
<td>pre</td>
<td>x &gt; 0 ∧ y &gt; 0</td>
</tr>
<tr>
<td>eff</td>
<td>x := x - 1</td>
</tr>
<tr>
<td>y := y + d</td>
<td></td>
</tr>
<tr>
<td>internal</td>
<td>down</td>
</tr>
<tr>
<td>pre</td>
<td>y &gt; 0</td>
</tr>
<tr>
<td>eff</td>
<td>y := y - 1</td>
</tr>
</tbody>
</table>
```
Example

Consider the ranking function $f(x, y) = 2x + y$

Check that for any transition $(x, y) \rightarrow (x', y')$

Up(1) $2x' + y' = 2(x - 1) + y + 1 = 2x + y - 1 = f(x, y) - 1 < f(x, y)$

Down: $2x' + y' = 2x + y - 1 = f(x, y) - 1 < f(x, y)$

Hence, the automaton terminates

What if $d > 1$?
Recall Stability

• Time invariant autonomous systems (closed systems, systems without inputs)

\[ \dot{x}(t) = f(x(t)), \quad x_0 \in \mathbb{R}^n, \quad t_0 = 0 \quad \text{(Eq. 1)} \]

• \( \xi(t) \) is the solution

• \( |\xi(t)| \) norm

• \( x^* \in \mathbb{R}^n \) is an equilibrium point if \( f(x^*) = 0 \).

• For analysis we will assume \( 0 \) to be an equilibrium point of (1) with out loss of generality
Lyapunov stability

Lyapunov stability: The system (1) is said to be **Lyapunov stable** (at the origin) if for every $\varepsilon > 0$ there exists $\delta_\varepsilon > 0$ such that for every if $|\xi(0)| \leq \delta_\varepsilon$ then for all $t \geq 0$, $|\xi(t)| \leq \varepsilon$. 
Asymptotically stability

The system (1) is said to be **Asymptotically stable** *(at the origin)* if it is Lyapunov stable and there exists \( \delta_2 > 0 \) such that for every if \( |\xi(0)| \leq \delta_2 \) then \( t \to \infty, \ |\xi(t)| \to 0 \).

If the property holds for any \( \delta_2 \) then **Globally Asymptotically Stable**
Verifying Stability for one dynamical system

**Theorem.** (Lyapunov) Consider the system (1) with state space \( \xi(t) \in \mathbb{R}^n \) and suppose there exists a positive definite, continuously differentiable function \( V: \mathbb{R}^n \to \mathbb{R} \). The system is:

1. Lyapunov stable if \( \dot{V}(\xi(t)) = \frac{\partial V}{\partial x} f(x) \leq 0 \), for all \( x \neq 0 \)
2. Asymptotically stable if \( \dot{V}(\xi(t)) < 0 \), for all \( x \neq 0 \)
3. It is globally AS if \( V \) is also radially unbounded.
   
   \( V \) is radially unbounded if \( ||x|| \to \infty \Rightarrow V(x) \to \infty \)
Defining stability of hybrid systems

- Hybrid automaton: \( A = \langle V, A, D, T \rangle \)
  - \( V = X \cup \{\ell\} \)
- Execution \( \alpha = \tau_0 a_1 \tau_1 a_2 \ldots \)
- Notation \( \alpha(t) \): denotes the valuation \( \beta \cdot lstate \) where \( \beta \) is the longest prefix with \( \beta \cdot ltime = t \)
- \( |\alpha(t)| \): norm of the continuous state \( X \)
- \( A \) is **Lyapunov stable** (at the origin) if for every \( \varepsilon > 0 \) there exists \( \delta_\varepsilon > 0 \) such that for every \( |\alpha(0)| \leq \delta_\varepsilon \) then for all \( t \geq 0 \), \( |\alpha(t)| \leq \varepsilon \).
- **Asymptotically stable** if it is Lyapunov stable and there exists \( \delta_2 > 0 \) such that for every \( |\alpha(0)| \leq \delta_2 \) then \( t \to \infty \), \( |\alpha(t)| \to 0 \).
Question: Stability Verification

- If each mode is asymptotically stable then is \( A \) also asymptotically stable?
Question: Stability Verification

• If each mode is asymptotically stable then is $A$ also asymptotically stable?

• No
Common Lyapunov Function

• If there exists positive definite continuously differentiable function $V: \mathbb{R}^n \to \mathbb{R}$ and a positive definite function $W: \mathbb{R}^n \to \mathbb{R}$ such that for each mode $i$, $\frac{\partial V}{\partial t} f_i(x) \leq -W(x)$ for all $x \neq 0$ then $V$ is called a common Lyapunov function for $A$.

• $V$ is called a common Lyapunov function

• **Theorem.** $A$ is globally asymptotically stable if there exists a common Lyapunov function.
Multiple Lyapunov Functions

• In the absence of a common lyapunov function the stability verification has to rely on the discrete transitions.

• The following theorem gives such a stability in terms of multiple Lyapunov function.

• **Theorem** [Branicky] If there exists a family of positive definite continuously differentiable Lyapunov functions $V_i: \mathbb{R}^n \rightarrow \mathbb{R}$ and a positive definite function $W_i: \mathbb{R}^n \rightarrow \mathbb{R}$ such that for any execution $\alpha$ and for any time $t_1, t_2$

\[
\alpha(t_1).L = \alpha(t_2).L = i \quad \text{and for all time } t \in (t_1, t_2), \alpha(t).L \neq i
\]

• $V_i(\alpha(t_2).x) - V_i(\alpha(t_1).x) \leq -W_i(\alpha(t_1).x)$
Stability Under Slow Switching

- **Average Dwell Time (ADT)** characterizes rate of mode switches
- **Definition:** H has ADT $T$ if there exists a constant $N_0$ such that for every execution $\alpha$, the number of mode switches in $\alpha$:

$$N(\alpha) \leq N_0 + \frac{\text{duration}(\alpha)}{T}.$$
**Stability Under Slow Switching**

```
V_2 \leq \mu \cdot V_1

\frac{\partial V_i}{\partial x} \leq -2\lambda_0 V_i(x)
```

- **Average Dwell Time (ADT)** characterizes rate of mode switches
- **Definition**: H has ADT $T$ if there exists a constant $N_0$ such that for every execution $\alpha$, the number of mode switches in $\alpha$: $N(\alpha) \leq N_0 + \text{duration}(\alpha)/T$.

N($\alpha$): **Theorem [HM`99]** H is asymptotically stable if its modes have a set of Lyapunov functions $(\mu, \lambda_0)$ and $\text{ADT}(H) > \log \frac{\mu}{\lambda_0}$.

- Dwell time is long enough so energy can decrease sufficiently in each mode

"Energy" may increase when switch but up to a factor of $\mu$
Remarks about ADT theorem assumptions

1. If $f_i$ is globally asymptotically stable, then there exists a Lyapunov function $V_i$ that satisfies $\frac{\partial V_i}{\partial x} \leq -2\lambda_i V_i(x)$ for appropriately chosen $\lambda_i > 0$

2. If the set of modes is finite, choose $\lambda_0$ independent of $i$

3. The other assumption restricts the maximum increase in the value of the current Lyapunov functions over any mode switch, by a factor of $\mu$.

4. We will also assume that there exist strictly increasing functions $\beta_1$ and $\beta_2$ such that $\beta_1(|x|) \leq V_i(x) \leq \beta_2(|x|)$

Slides adapted from Prof. Sayan Mitra’s slides in Fall 2021
Proof sketch

Suppose $\alpha$ is any execution of $A$.

Let $T = \alpha.ltime$ and $t_1, \ldots, t_{N(\alpha)}$ be instants of mode switches in $\alpha$.

We will find an upper-bound on the value of $V_{\alpha(T),l}(\alpha(T).x)$

Define $W(t) = e^{2\lambda_0 t}V_{\alpha(t),l}(\alpha(t).x)$

$W$ is non-increasing between mode switches $\left[ \frac{\partial V_i}{\partial x} \leq -2\lambda_0 V_i(x) \right]$

That is, $W(t_{i+1}^-) \leq W(t_i)$

$W(t_{i+1}) \leq \mu W(t_{i+1}^-) \leq \mu W(t_i)$

Iterating this $N(\alpha)$ times: $W(T) \leq \mu^{N(\alpha)}W(0)$

$$e^{2\lambda_0 T}V_{\alpha(T),l}(\alpha(T).x) \leq \mu^{N(\alpha)}V_{\alpha(0),l}(\alpha(0).x)$$

$$V_{\alpha(T),l}(\alpha(T).x) \leq \mu^{N(\alpha)}e^{-2\lambda_0 T}V_{\alpha(0),l}(\alpha(0).x) = e^{-2\lambda_0 T + N(\alpha)\log \mu}V_{\alpha(0),l}(\alpha(0).x)$$

If $\alpha$ has ADT $\tau_\alpha$ then, recall, $N(\alpha) \leq N_0 + T/\tau_\alpha$ and $V_{\alpha(T),l}(\alpha(T).x) \leq e^{-2\lambda_0 T + (N_0 + T/\tau_\alpha)\log \mu}V_{\alpha(0),l}(\alpha(0).x) \leq C e^{T(-2\lambda_0 + \log \mu/\tau_\alpha)}$

If $\tau_\alpha > \log \mu/2\lambda_0$ then second term converges to 0 as $T \to \infty$ then from assumption 4 it follows that $\alpha$ converges to 0.
Our goals in this course

Write programs (tools) that prove correctness

• Understand fundamental limits of creating such tools

• Learn models of CPS at different levels of abstractions

• Gain research experience
What we have learned in this course

• Satisfiability problems:
  • SAT (DPLL)
  • SMT (DPLL-T)
    • Neural network verification (CROWN bound propagation, branch-and-bound)

• Computation Tree Logic
  • CTL model checking

• Dynamical systems (reachability & invariance):
  • Linear/nonlinear systems, LTI systems
  • stability verification, Lyapunov functions

• Verification of hybrid automata and timed automata
  • Abstractions
  • Composition
  • Progress Analysis
  • Common/Multiple Lyapunov functions