CSE 591: Theoretical Aspects of CPS

Timed automata

References:
Tabuada Ch 7.2, Cassandras & Lafortune Ch 5.6

Instructor: Georgios E. Fainekos

School of Computing, Informatics and Decision System Engineering
Arizona State University
fainekos at asu edu

http://www.public.asu.edu/~gfaineko
Example: Alarm 1

one clock: $d\xi/dt = 1$

$s_0$ with $\xi := 0$

$s_1$ with
- $\xi := 0$
- $\xi \geq 1$

$s_2$ with
- $\xi := 0$ when $0 < \xi < 1$

$s_3$ with $\xi < 1$
Example: Alarm 2

One clock: \( \frac{d\xi}{dt} = 1 \)

- \( s_0 \) to \( s_1 \): \( \xi := 0 \) msg
- \( s_1 \): \( \xi := 0 \) msg
- \( s_1 \) to \( s_2 \): \( \xi \geq 1 \) msg
- \( s_2 \) to \( s_3 \): \( 0 < \xi < 1 \) msg
- \( s_3 \): alarm

\( \xi := 0 \)
Example: Scheduler

- **Sleep**
  - \( \xi_1 = 1, \xi_2 = 1 \)
  - \( 0 \leq \xi_1 \leq 3 \)
  - \( \xi_1 := 0 \)
  - \( \xi_2 := 0 \)

- **Active**
  - \( \dot{\xi}_1 = 1, \dot{\xi}_2 = 1 \)
  - \( 0 \leq \xi_1 \leq 2 \)
  - \( \text{awake: } \xi_1 := 3 \)
  - \( \text{expired: } \xi_1 := 0 \)

- **Starting**
  - \( 0 \leq \xi_1 < 2 \)
  - \( \xi_1 := 0, \xi_2 := 0 \)

- **Execute**
  - \( \dot{\xi}_1 = 1, \dot{\xi}_2 = 1 \)
  - \( 0 \leq \xi_1 \leq 2 \)
  - \( 0 \leq \xi_2 \leq 1 \)
  - \( \text{finished: } 0 < \xi_2 < 1 \)

- **Error**
  - \( \dot{\xi}_1 = 1, \dot{\xi}_2 = 1 \)
  - \( 2 \leq \xi_1 \)
  - \( \text{expired: } \xi_1 := 2 \)


Question

• Subset sum
  • Model the subset sum problem as a reachability problem for a timed automaton
  • We are given 4 positive integers \( K = \{k_1, k_2, k_3, k_4\} \) and a sum \( K_{\text{sum}} \)
  • Does \( \sum k_i = K_{\text{sum}} \)?
Review: Quotient System

Let $S = \{X, X_0, U, \rightarrow, Y, H\}$ be a system and $Q$ be an equivalence relation on $X$ where $(x, x') \in Q$ implies $H(x) = H(x')$. The quotient of $S$ by $Q$ - denoted $S_{/Q}$ - is the system $S_{/Q} = \{X_{/Q}, X_{/Q0}, U, \rightarrow_{/Q}, Y, H_{/Q}\}$, where

1. $X_{/Q} = X/Q$
2. $X_{/Q0} = \{x_{/Q} \in X_{/Q} \mid x_{/Q} \cap X_0 \neq \emptyset\}$
3. $(x_{/Q}, u, x'_{/Q}) \in \rightarrow_{/Q}$ if $\exists (x, u, x') \in \rightarrow$ with $x \in x_{/Q}$ and $x' \in x'_{/Q}$
4. $H_{/Q}(x_{/Q}) = H(x)$ for some $x \in x_{/Q}$

**Theorem:** Let $S = \{X, X_0, U, \rightarrow, Y, H\}$ be a system and $Q$ be an equivalence relation on $X$ where $(x, x') \in Q$ implies $H(x) = H(x')$. The relation

$\Gamma(\pi_Q) = \{(x, x_{/Q}) \in X \times X_{/Q} \mid x_{/Q} = \pi_Q(x)\}$

is a simulation relation from $S$ to $S_{/Q}$.

$\Gamma(\pi_Q)$ is a bisimulation relation between $S$ and $S_{/Q}$ iff $Q$ is bisimulation between $S$ and $S$. 


Review: Bisimulation

- Def. Given $S_a, S_b$ with $Y_a=Y_b$ we say that $S_a$ is **bisimilar** to $S_b$, denoted $S_a \approx_s S_b$, if there exists a relation $R$ satisfying:
  1. $R$ is a simulation relation from $S_a$ to $S_b$
  2. $R^{-1}$ is a simulation relation from $S_b$ to $S_a$

- Let $S_a, S_b$ with $Y_a=Y_b$. A relation $R \subseteq X_a \times X_b$ is a **bisimulation relation** between $S_a$ and $S_b$ if
  1. $\forall x_{a0} \in X_{a0}. \exists x_{b0} \in X_{b0}. (x_{a0}, x_{b0}) \in R$
  2. $\forall x_{b0} \in X_{b0}. \exists x_{a0} \in X_{a0}. (x_{a0}, x_{b0}) \in R$
  3. $\forall (x_a, x_b) \in R. H_a(x_a)=H_b(x_b)$
  4. $\forall (x_a, x_b) \in R.$

  $x_a \xrightarrow{u_a} x'_a$ implies $x_b \xrightarrow{u_b} x'_b$ satisfying $(x'_a, x'_b) \in R$

  $x_b \xrightarrow{u_b} x'_b$ implies $x_a \xrightarrow{u_a} x'_a$ satisfying $(x'_a, x'_b) \in R$
Example: Scheduler

- **Sleep**
  - \( \xi_1 = 1, \xi_2 = 1 \)
  - \( 0 \leq \xi_1 \leq 3 \)
  - \( \xi_1 := 0 \)
  - \( \xi_2 := 0 \)

- **Active**
  - \( \xi_1 = 1, \xi_2 = 1 \)
  - \( 0 \leq \xi_1 \leq 2 \)
  - \( \xi_1 = 3 \)
  - \( \xi_1 := 0 \)

- **Starting**
  - \( 0 \leq \xi_1 < 2 \)
  - \( \xi_2 := 0 \)

- **Error**
  - \( \xi_1 = 1, \xi_2 = 1 \)
  - \( 2 \leq \xi_1 \)
  - \( \xi_1 = 2 \)

- **Execute**
  - \( \xi_1 = 1, \xi_2 = 1 \)
  - \( 0 \leq \xi_1 \leq 2 \)
  - \( 0 \leq \xi_2 \leq 1 \)
  - \( 0 < \xi_2 < 1 \)

- **Awake**
  - \( \xi_1 := 0 \)

- **Expired**
  - \( \xi_1 = 2 \)
2D Continuous state space
Equivalence classes $\mathbb{Q}$
Equivalence classes $Q$
Equivalence classes $Q$
Equivalence classes Q′
Equivalence classes $Q''$
Equivalence classes $Q'''$
Example: Scheduler

- **Sleep**: \( \xi_1 = 1, \xi_2 = 1 \)
  - Conditions: \( 0 \leq \xi_1 \leq 3 \)
  - Actions: \( \xi_1 := 0 \), \( \xi_2 := 0 \)

- **Active**: \( \dot{\xi}_1 = 1, \dot{\xi}_2 = 1 \)
  - Conditions: \( 0 \leq \xi_1 \leq 2 \)
  - Transition: \( \xi_1 := 3 \)

- **Starting**: \( \dot{\xi}_1 = 1, \dot{\xi}_2 = 1 \)
  - Conditions: \( 0 \leq \xi_1 < 2 \)
  - Actions: \( \xi_2 := 0 \)

- **Execute**: \( \dot{\xi}_1 = 1, \dot{\xi}_2 = 1 \)
  - Conditions: \( 0 \leq \xi_1 \leq 2 \)
  - Conditions: \( 0 \leq \xi_2 \leq 1 \)
  - Transition: \( \xi_2 := 0 \)
  - Transition: \( \xi_1 := 2 \)

- **Error**: \( \dot{\xi}_1 = 1, \dot{\xi}_2 = 1 \)
  - Conditions: \( 2 \leq \xi_1 \)
  - Transition: \( \xi_1 := 2 \)

- **Awake**: \( \xi_1 := 0 \)
  - Conditions: \( \xi_1 = 3 \)

- **Expired**: \( \xi_1 := 2 \)
  - Conditions: \( \xi_1 = 2 \)

- **Finished**: \( \xi_1 := 2 \)
  - Conditions: \( 0 < \xi_2 < 1 \)
System trajectories
System trajectories
Example: Alarm 2

What are the regions of interest?

one clock: $d\xi/dt = 1$

$\xi:=0$ to $s_0$

$\xi:=0$ to $s_1$

$0<\xi<1$ to $s_2$

$\xi:=0$ to $s_3$
Example: Alarm 2
Example: Alarm 2
Example: Alarm 2
Timed Automata in Practice

• UPPAAL (http://www.uppaal.com/)
  • Verification
  • Planning and Scheduling
  • Testing real time systems
  • Timed games
  • Probabilistic timed automata
  • Times tool (http://www.timestool.com/)
    • modeling,
    • schedulability analysis
    • synthesis of schedules and executable code
    • worst case reaction time (WCRT) analysis