CS 512 Formal Methods, Spring 2018	Instructor: Assaf Kfoury

Motivating Examples

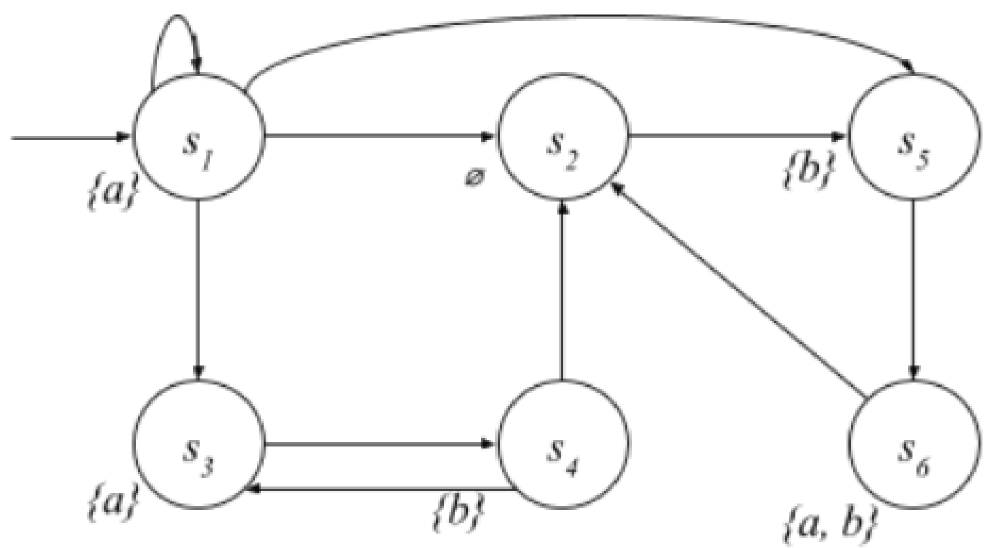
January 25, 2018 Shreya Ramesh

(These lecture notes are **not** proofread and proof-checked by the instructor.)

1 Paths and Traces in Transition Systems

1.1 Example transition system and notation

Below is an example transition system in the form of a graph.



- AP (atomic proposition) $= \{a, b\}$.
- Here, no actions are specified and all steps are silent steps.
- To find traces, we abstract away information and assign variables to the labels. Let us assign $W = \emptyset$, $X = \{a\}$, $Y = \{b\}$, $Z = \{a, b\}$.
- We can now find paths and traces of the transition system by inspection. For larger transition systems, this is not possible and would be calculated with an algorithm.

Paths	Traces
s_1^ω	X^ω
$s_1^+(s_5s_6s_2)^\omega$	$X^+(YZW)^\omega$
$s_1^+(s_3s_4)^+s_2(s_5s_6s_2)^\omega$	$X^+(XY)^+W(YZW)^\omega$
$s_1^+(s_3s_4)^\omega$	$X^+(XY)^\omega$
$s_1^+(s_2s_5s_6)^\omega$	$X^+(WYZ)^\omega$

1.2 Size of set

- Suppose we are given the following expression: $\mathcal{L}(X^\omega)$. We can evaluate it as follows:

$$\begin{gathered}\{a\}^\omega = \\ \{a\}\{a\}\{a\}... = \\ aaa... \subseteq (2^{AP})^\omega.\end{gathered}$$

  2^{AP} is called the "power set."

- We can determine the size of the power set as follows: $|2^{AP}| = 2^{|AP|}$. Since $|AP|$ in this case is 2, we know $|2^{AP}| = 4$.
- How do we calculate $|(2^{AP})^\omega|$? Intuitively, we know that $(2^{AP})^3 = 64$ so it makes sense that $(2^{AP})^\omega = 4^\omega$. This ends up being the size of the real numbers.

2 Propositional Logic

2.1 Review of boolean algebra

- $\wedge$: logical "and"
- $\vee$: logical "or"
- $\neg$: logical "not
- $\wedge$ and $\vee$ are binary connectives, meaning they require two expressions, while $\neg$ is a unary connective.
- Unary connectives bind more tightly than binary connectives e.g. $\neg a \vee b$ is equivalent to $(\neg a) \vee b$ **not** $\neg(a \vee b)$.

2.2 Example

- ϕ is an invariant condition over P.
- Assume $\phi \triangleq \neg a \vee b$ and $X \subseteq AP = \{a, b\}$.
- If $X = \{a\}$ and $a \mapsto$ true, $b \mapsto$ false, then $X \not\models \phi$
- If $X' = \{b\}$ and $a \mapsto$ false, $b \mapsto$ true, then $X \models \phi$.

3 Safety and Liveness Properties

3.1 Definitions

- A **safety property** may specify that an action/behavior/display can occur only after a prior condition is fulfilled. Intuitively, "something bad never happens."
- **Liveness property** is something that requires the system to make progress. Intuitively, "something good eventually happens."

3.2 Example (Problem 2 on HW1)

P (property you are interested in) $= \{A_0A_1... \in (2^{AP})^\omega \mid \exists n \geq 0$ s.t. $a \in A_0, ..., a \in A_{n-1}$ and $\{alb\} = A_n$ and $\overset{\infty}{\exists} j \geq 0$ s.t. $b \in A_j\}$ We can split up the condition as the following:

- Condition 1 (Safety Property): $\exists n \geq 0$ s.t. $a \in A_0, ..., a \in A_{n-1}$ and $\{alb\} = A_n$
- Condition 2 (Liveness property): $\overset{\infty}{\exists} j \geq 0$ s.t. $b \in A_j\}$

Using regular expressions, we can now find prefixes that meet the above conditions. Let us assign $W = \emptyset$, $X = \{a\}$, $Y = \{b\}$, $Z = \{a, b\}$.

- "Bad" prefixes of Condition 1: $(W + X + Y)^*(W + Y)(W + X + Y)^*$
- Possible prefixes that satisfy Condition 2 if $P \leq (2^{AP})^\omega$: $(W + X)^*((Y + Z)(W + X)*)^\omega$