CS512 - Formal Methods

Thursday, February 1st, 2018

Note-taker: Glib Dolotov

Every invariant property is a regular safety property

$$\Phi : a \to b$$

$$\begin{cases} a = \text{"}fuel < 5\text{"} \\ b = \text{"}warning\ signal\ on\text{"} \end{cases} \quad \text{or} \quad \begin{cases} a = \text{"}smoke\ detected\text{"} \\ b = \text{"}alarm\ buzzer\ on\text{"} \end{cases}$$

$$\Phi : a \to b \equiv \neg a \vee b$$

$$P = \{A_0 A_1 A_2 \cdots \in (2^{AP})^\omega \ |\forall i \geq A_i \vDash \Phi\}$$

A_i	a	b	$\neg a \vee b$
∅	F	F	T
{a}	T	F	F
{b}	F	T	T
{a,b}	T	T	T

The formula from P from above can be rewritten via the chart as:

$$P = \{A_0 A_1 A_2 \cdots \in (2^{AP})^\omega \ |\forall i \geq A_i \in \{M, P, Q\}\}$$

$AP = \{a, b\}$ $\quad 2^{AP} = \{\varnothing,$ {a}, {b}, {a,b}}

M, N, P, Q

AP: What is an example of a property over AP which is ALWAYS TRUE?

$P = \mathscr{L}[M^\omega]$? NO, this can still be false if atomic proposition "a" or "b" is always held (or both).

$P = \mathscr{L}[(M + N + P + Q)^\omega] = (2^{AP})^\omega$? YES

What is an example of a property over AP $[P \subseteq (2^{AP})^\omega]$ which is ALWAYS FALSE?

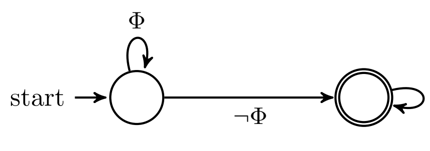
- $P = \emptyset$ (note: $P = \{\emptyset\}$ can be true)
  Since $\emptyset$ is a special type of regular expression, this property is also regular.
- $E \cdot (F)^\omega + \ldots$ where $E \notin \mathscr{L}[F]$

---

n

Some things were added to Handout 04:

A safety property can be defined by its bad prefixes. From there, we want to find the shortest of such prefixes: minimum bad prefix.



The previous diagram shows an automata that will accept bad prefixes to property P.
Φ cooresponds to $\emptyset, \{b\}, \{a, b\}$.
$\neg\Phi$ cooresponds to $\{a\}$.

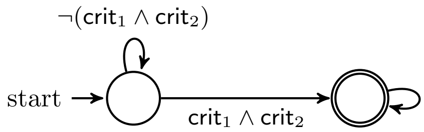
Regular Safety Properties for Mutual Exclusion

$AP = \{\text{crit}_1, \text{crit}_2, \dots\}$ $\qquad 2^{AP} = \{\emptyset, \dots\}$

$$P = \{A_0 A_1 A_2 \cdots \in (2^{AP})^\omega \ | \forall i \geq A_i \not\supseteq \{\text{crit}_1, \text{crit}_2\}\}$$

We use the above because we don't want crit_1 and crit_2 to both occur.

Automata to accept BadPref(P)



Note: by de Morgan's Law: $\neg(\text{crit}_1 \wedge \text{crit}_2) \equiv \text{crit}_1 \wedge \text{crit}_2$.

Example of Safety Property that IS NOT Regular

Safety Property for the Vending Machine:
"the number of inserted dollars $\geq$ the # of dispensed drinks."

$AP = \{\text{pay}, \text{drink}\}$ $\qquad 2^{AP} = \{\underset{\text{M}}{\varnothing}, \ \underset{\text{N}}{\{\text{pay}\}}, \ \underset{\text{P}}{\{\text{drink}\}}, \ \underset{\text{Q}}{\{\text{pay, drink}\}}\}$

$$P = \{A_0 A_1 A_2 \cdots \in (2^{AP})^\omega : \forall i$$
$$|\{j : 0 \leq j \leq i \ \wedge \ \text{pay} \in A_j\}| \geq |\{j : 0 \leq j \leq i \ \wedge \ \text{drink} \in A_j\}|\}$$

i.e. "the number of states in which pay occurs is *geq* the number of states in which drink occurs at any point in the sequence."

Note: we use ":" instead of "—" for "such that" to avoid confusion with the notation for the cardinality of a set ("$|X|$")

Note: There is no standardized way of creating formal models of systems. It is a work in progress. There are different methods that have varying degrees of success.

$$P = \{(M^* Q^* N)^{m_1} (M^* Q^* P)^{n_1} (M^* Q^* N)^{m_2} (M^* Q^* P)^{n_2} \cdots \in (2^{AP})^\omega$$
$$: \forall i \geq 1, m_i \geq 0 \wedge \ n_i \geq 0 \wedge \ m_1 + m_2 + \cdots + m_i \geq n_1 + n_2 + \cdots + n_i\}$$

More broadly: $P = \{((M + Q)^*)^{m_1} \cdots\}$

Note: $\mathscr{L}[(a + b)^*] = \mathscr{L}[(a^* b^*)^*]$

$$\begin{aligned}\text{BadPref}(P) = \{&((M+Q)^*N)^{m_1}((M+Q)^*P)^{n_1}\cdots((M+Q)^*N)^{m_k}((M+Q)^*P)^{n_k}\\ &: \forall k \geq 0, m_1 + \cdots + m_k < n_1 + \cdots + n_k\}\end{aligned}$$

Note: BadPref(P) is a set of <u>finite</u> words. i.e. BadPref(P) $\subseteq (2^{AP})^*$

$a^m b^n a^p b^q : m + n > p + q$ is not a regular expression, it is context-free.
$a^m b^n a^m$ is also not regular.

We concluded lecture with <u>Handout 05 - ω-Regular Properties</u>