Universitetet i Oslo
Institutt for Informatikk

PMA

Einar Broch Johnsen, Martin Steffen

INF 4140: Models of Concurrency

Høst 2014 **Series 9** 10. 11. 2014

Topic: Histories (Exercises with hints for solution)

Issued: 10. 11. 2014

Exercise 1 (History functions) Using the techniques on the slides from lecture 10, define the following functions over histories:

1. a Boolean function $\_\textbf{endswith}\_ : Hist \times Set \to Bool$ such that h **endswith** s is *true* if h is nonempty and ends with an event in the set s. For instance, $[a, b, c, d]$ **endswith** $\{b, c\}$ is *false*, ε **endswith** $\{b, c\}$ is *false*, and $[a, b, c, d]$ **endswith** $\{b, d\}$ is *true*.

2. a Boolean function $\_\textbf{beginswith}\_ : Hist \times Set \to Bool$ such that h **beginswith** s is *true* if h is nonempty and begins with an event in the set s. For instance, $[a, b, c, d]$ **beginswith** $\{b, c\}$ is *false*, ε **beginswith** $\{b, c\}$ is *false*, and $[a, b, c, d]$ **beginswith** $\{b, a\}$ is *true*.

3. a Boolean function testing if one history is a subsequence of another history, $\_ \sqsubseteq \_ : Hist \times Hist \to Bool$. For instance, $[b, d, e] \sqsubseteq [a, b, c, d, e]$, but not $[b, e, d] \sqsubseteq [a, b, c, d, e]$.

4. a function $\_ \setminus \_ : Hist \times Set \to Hist$ such that $h \setminus s$ is the subsequence of h consisting of all events not in the set s. For instance, $[a, b, c, b, d, a] \setminus \{d, c\}$ is $[a, b, b, a]$.

5. a function $pending : Hist \to Hist$ such that $pending(h)$ is the sequence of all send messages that not yet have been received. For instance, $pending([A \uparrow B : m_1, A \uparrow B : m_2, A \uparrow B : m_1, A \downarrow B : m_1])$ is $[A \uparrow B : m_1, A \uparrow B : m_2]$. (In case there are several identical send messages, and some but not all of these have been received, you may choose the order of the remaining ones as you wish. For instance, the example above could give the result $[A \uparrow B : m_2, A \uparrow B : m_1]$.) Hint: here you need to distinguish between send and receive events in the definition, and you may need to introduce an additional function.

Solution:

1. ε **ew** $s = false$
   $h; x$ **ew** $s = x \in s$

2. ε **bw** $s = false$
   $\varepsilon; x$ **bw** $s = x \in s$
   $h; x$ **bw** $s = h$ **bw** s

3. $\varepsilon \sqsubseteq h = true$
   $h; x \sqsubseteq \varepsilon = false$
   $h; x \sqsubseteq h'; x' =$ **if** $x = x'$ **then** $h \sqsubseteq h'$ **else** $h; x \sqsubseteq h'$

4. $\varepsilon \backslash s = \varepsilon$
   $h; x \backslash s =$ **if** $x \in s$ **then** $h \backslash s$ **else** $(h \backslash s); x$

5. $pending(\varepsilon) = \varepsilon$
   $pending(h; A{\uparrow}B : m) = pending(h); A{\uparrow}B : m$
   $pending(h; A{\downarrow}B : m) = pending(rem(h, A{\uparrow}B : m))$ using an additional function, $rem : Hist \times Event \to Hist$, for removing an occurrence of an event from a history (we remove the rightmost, which is easiest):

   $rem(\varepsilon, x) = \varepsilon$
   $rem(h; x', x) =$ **if** $x = x'$ **then** h **else** $rem(h, x); x'$

Exercise 2 (Coin Machine Users) Consider the coin machine in lecture 10, where the history invariant for the coin machine C is defined over the global history H by:

$$I_C(H/\alpha_C) = 0 \leq sum(H/\downarrow C) - sum(H/C\uparrow) < 15$$

In the lecture, a coin machine agent C was composed with a user agent U with exact change. We will here consider the composition of C with two different users, U_1 and U_2.

(a) User U_1 inserts only "5 krone" coins, i.e., U_1 only sends five messages. The user is specified by the following invariant:

$$I_{U_1}(H/\alpha_{U_1}) = H/\{U_1\uparrow: one\} = \varepsilon \land sum(H/U_1\uparrow) - sum(H/\downarrow U_1) = 0 \ \lor 5 \ \lor 10$$

where the formula $P = a \ \lor b \ \lor c$ is an abbreviation for $P = a \ \lor P = b \ \lor P = c$.

Write down the global invariant for the system consisting of C and U_1. Is it possible to use the legal function to simplify this invariant? For instance, may we say something more precise about the difference $sum(H/\downarrow C) - sum(H/C\uparrow)$ compared to what we know from I_C?

(b) User U_2 sends both five and one messages to the coin machine, but U_2 never cares about collecting the coins returned by the machine. User U_2 is specified by the following invariant:

$$I_{U_2}(H/\alpha_{U_2}) = 0 \leq sum(H/U_2\uparrow) \land sum(H/\downarrow U_2) = 0$$

Write down the global invariant for the system consisting of C and U_2. Is it possible to use the legal function to simplify this global invariant?

Solution:

(a) Global invariant:

$$I(H) = legal(H) \land I_C(H/\alpha_C) \land I_{U_1}(H/\alpha_{U_1})$$

Since H is legal, we know that C cannot receive any *one* messages, i.e.,

$$H/(\downarrow C : one) = \varepsilon$$

Thus, we have $sum(H/\downarrow C) = 0 \lor 5 \lor 10 \lor \dots$
Furthermore, $sum(H/C\uparrow) = 0 \lor 10 \lor 20 \lor \dots$
Combining these with I_C, we get

$$sum(H/\downarrow C) - sum(H/C\uparrow) = 0 \lor 5 \lor 10$$

(b) Global invariant:

$$I(H) = legal(H) \land I_C(H/\alpha_C) \land I_{U_2}(H/\alpha_{U_2})$$

An important thing to realize here is that even though U_2 never collects the returned coins, the machine will return them (maintaining I_C). Thus, events $C\uparrow U_2$ will appear on H, but $C\downarrow U_2$ will not appear:

$$\begin{aligned} I(H) = \ & legal(H) \land 0 \leq sum(H/U_2\uparrow C) \land sum(H/C\downarrow U_2) = 0 \\ & \land\ 0 \leq sum(H/U_2\downarrow C) - sum(H/C\uparrow U_2) < 15 \end{aligned}$$