Formal verification - Tutorial 04

16/03/2026

Communicating finite-state machines

Let S be CFSM with (perfect) transition relation $\rightarrow$.

Exercise 1. *Show that the reachability problem for CFSMs is undecidable.*

Solution. We can simulate the tape of a Turing machine using a single channel. A special symbol is used to mark the position of the head. The head movement are simulated by rotations of the channel contents. □

We consider a model of CFSM comprising a finite set of processes P (each with a finite set of local states) and a finite set of channels C. Each channel is a FIFO queue of messages connecting two processes (point-to-point communication). The *communication topology* of a CFSM is an undirected multigraph where vertices are processes and (undirected) edges are channels.

Exercise 2. *Show that the reachability problem for CFSMs is undecidable when*

1. *there are two processes P and Q and two channels $C = \{c, d\}$, where c connects P to Q and d connects Q to P (i.e., the communication topology is a cycle of length two);*

2. *there are two processes P and Q and two "parallel" channels $C = \{c, d\}$ both connecting P to Q (i.e., the communication topology is a multigraph with two parallel edges).*

Solution. 1. We show how to simulate a single channel e (where the same process can send and receive) by the two channels c, d. Transmissions on e are simulated by transmissions on c. Receptions on e are simulated by receptions on d. Both these are taken care by process P. Process Q, which is fixed, just forwards messages from c to d.

2. We reduce from the *Post correspondence problem* (PCP), which is an undecidable problem. An instance of this problem is given by a finite sequence of pairs of words $(u_1, v_1), \ldots, (u_n, v_n)$ over some alphabet Σ and asks whether there is a sequence of indices $i_1, \ldots, i_k$ such that $u_{i_1} \cdots u_{i_k} = v_{i_1} \cdots v_{i_k}$. Process P guesses a sequence of indices $i_1, \ldots, i_k$ and sends $u_{i_1}, \ldots, u_{i_k}$ on channel c and $v_{i_1}, \ldots, v_{i_k}$ on channel d. Process Q receives messages from both channels and checks that they are the same. □

Exercise 3. *Show that the reachability problem for CFSMs is decidable* over tree communication topologies.

Solution. When the communication topology is a tree, bounded channels suffice to reach all reachable configurations. The idea is that we can always keep the channels to size zero or one, by always executing a transmision immediately followed by the corresponding reception.

Another idea, is as follows. We assume w.l.o.g that the channel alphabets are disjoint. For the leaf processes, we can compute the regular language of messages they can send or receive (but not both). Inductively, consider an internal process p connected to child processes $p_1, \ldots, p_k$. For each we have inductively computed the regular languages $L_1 \subseteq M_1^*, \ldots, L_k \subseteq M_k^*$ of channel actions. We compute the regular language $L \subseteq M$ of channel actions of p to its parent process. Let L' be the shuffle of languages $L_1, \ldots, L_k$ and M^*. Then L is the projection to M^* of the language of all channel actions of p intersected with L'. □

Well-quasi orders

A binary relation $\preceq$ on a set X is **quasi-order** if it is reflexive and transitive. An antichain is a subset of X whose elements are pairwise incomparable w.r.t. $\preceq$.

Exercise 4. *Let $(X, \preceq)$ be a quasi-order. Prove that the following conditions are equivalent.*

(a) Any infinite sequence $a_1, a_2, \ldots$ of elements of X contains a domination *$a_i \preceq a_j$ for some indexes $i < j$.*

(b) X does not contain any infinite antichain and is well-founded *(i.e., there are no infinite strictly decreasing sequences).*

(c) Any infinite sequence $a_1, a_2, \ldots$ of elements of X contains an infinite nondecreasing subsequence, i.e., there are indices $i_1 < i_2 < \ldots$ with $a_{i_1} \preceq a_{i_2} \preceq \ldots$.

(d) Every upward closed set is the upward closure of a finite set. (The upward closure *of a set X is the set of elements that dominate some element of X; X is* upward closed *if it is equal to its upward closure.)*

(e) Every nondecreasing chain of upward closed sets $U_1 \subseteq U_2 \subseteq \cdots \subseteq X$ is finite.

Whenever any of the conditions above holds we call the relation $\preceq$ a **well quasi-order** or **WQO**.

Solution. We show the implication from (b) to (c) using the infinite Ramsey theorem. Consider an infinite sequence $a_1, a_2, \ldots$ of elements of X. We colour the edges of the complete undirected graph on $\{a_1, a_2, \ldots\}$ with three colours $\{A, B, C\}$: we colour the edge $\{a_i, a_j\}$ with $i < j$ with A if $a_i \preceq a_j$, with B if $a_i \succ a_j$, and with C if a_i and a_j are incomparable. By the infinite Ramsey theorem, there is an infinite monochromatic clique, that is a subsequence $a_{i_1}, a_{i_2}, \ldots$ such that all edges $\{a_{i_j}, a_{i_k}\}$ with $j < k$ have the same colour. By assumption (b), this color cannot be B, since otherwise we would have an infinite strictly decreasing sequence. It cannot be C either, since otherwise we would have an infinite antichain. Hence, the color is A and we have an infinite nondecreasing subsequence, as required. □

Exercise 5 (Higman's lemma)**.** *Let $(X, \leq)$ be a WQO and consider the* subword order *(a.k.a.* scattered subsequence order*) on words $\leq^* \subseteq X^* \times X^*$. In other terms, $u \leq^* v$ if u can be obtained from v by deleting some letters and replacing the remaining letters with smaller ones. Prove that $(X^*, \leq^*)$ is a WQO.*

Solution. Call a sequence $u_0, u_1, \ldots$ *bad* if there is no domination $u_i \leq^* u_j$ with $i < j$. By way of contradiction, assume we have a bad sequence as above. We can also assume that the sequence is minimal in the sense that the sequence of lengths $(|u_0|, |u_1|, \ldots)$ is minimal for the lexicographic order. Since no u_n can be empty, we can write $v_n := a_n \cdot u_n$. Consider now the sequence $a_0, a_1, \ldots$ of elements from X. By the well quasi ordering on X, there is an infinite monotone subsequence

$$a_{n_0} \leq a_{n_1} \leq \cdots .$$

Consider now the new sequence

$$u_0, u_1, \ldots, u_{n_0-1}, v_{n_0}, v_{n_1}, \ldots .$$

This sequence is bad, since a domination therein would result in a domination in the original sequence. This contradicts minimality of the original sequence, since v_{n_0} is strictly shorter than u_{n_0}. □

Exercise 6. *Show that every downward-closed language of words (w.r.t. the subword ordering) is regular.*

Lossy channel systems

Let S be a CFSM with (perfect) transition relation $\to$ and lossy transition relation $\Rightarrow$. Recall that $c \Rightarrow d$ if there are configurations $c', d' \in \mathsf{Conf}$ such that $c' \sqsubseteq c$, $c' \to d'$, and $d \sqsubseteq d'$. Consider the following predecessor operators:

$$\mathsf{Pre}_{\to}(T) := \left\{ c \in \mathsf{Conf} \;\middle|\; \exists c' \in T, c \to c' \right\},$$
$$\mathsf{Pre}(T) := \left\{ c \in \mathsf{Conf} \;\middle|\; \exists c' \in T, c \Rightarrow c' \right\},$$

Notice that $\mathsf{Pre}(T)$ can be infinite even when T only contains a single configuration.

Exercise 7. *Let T be a regular set of configurations. Show that the following sets are effectively regular:*

- $\mathsf{Pre}_{\to}(T)$*,*
- $T\uparrow$*,*
- $\mathsf{Pre}(T)$*,*
- $\mathsf{Pre}^*(T)$*.*

Solution. The set $\mathsf{Pre}_{\to}(T)$ can be obtained from T by regularity-preserving operations such as finite unions, concatenations, and right language quotients. From a finite automaton recognising T, we can construct a finite automaton recognising $T\uparrow$ by adding self-loops on all states for all symbols. Straight from the definitions, we have

$$\mathsf{Pre}(T) = \mathsf{Pre}_{\to}(T\uparrow)\uparrow .$$ □