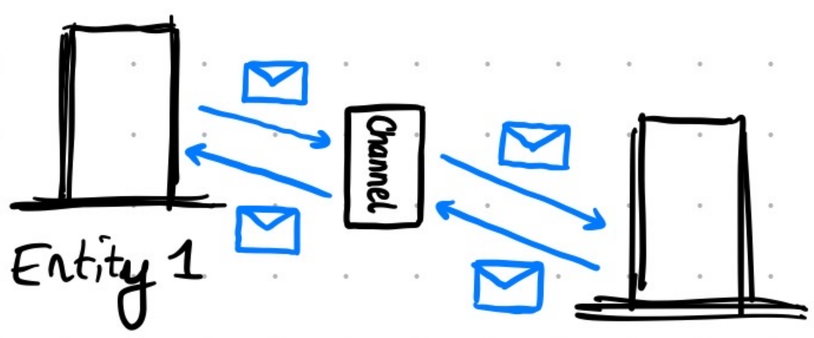
Lossy Channel Systems and the Subsequence Ordering

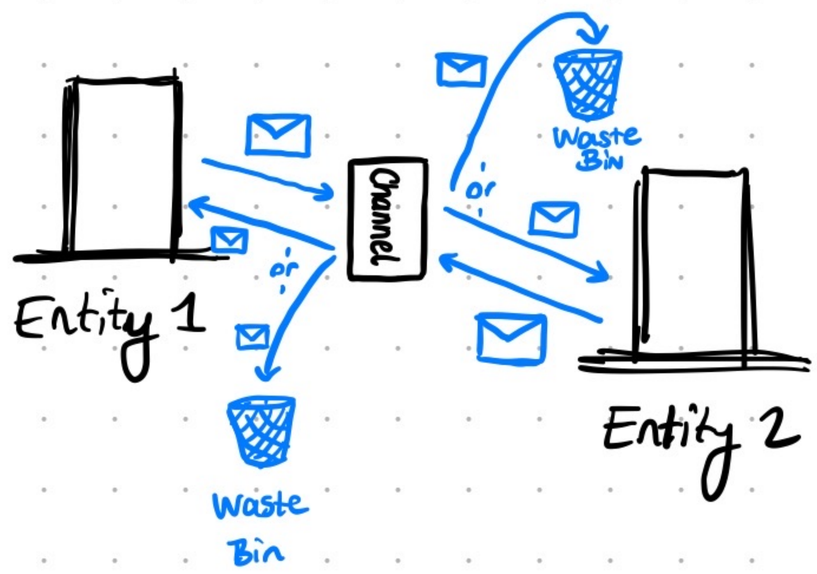
Goal: Learn about a WSTS-model used to model & verify network communications.

Idea: Communication over FIFO (First-in-first-out) channels via asynchronous message transfer



Problem: A FIFO channel (i.e. a list-like data structure) may be used to simulate the tape of a Turing Machine ⇒ VERY UNDECIDABLE!

However: Over-the-network communication must be able to deal with package losses



Assuming arbitrary package losses, we get a very different data structure:

the configurations form a wqo (as we will see) for which the transition relation is MONOTONOUS: A WSTS!

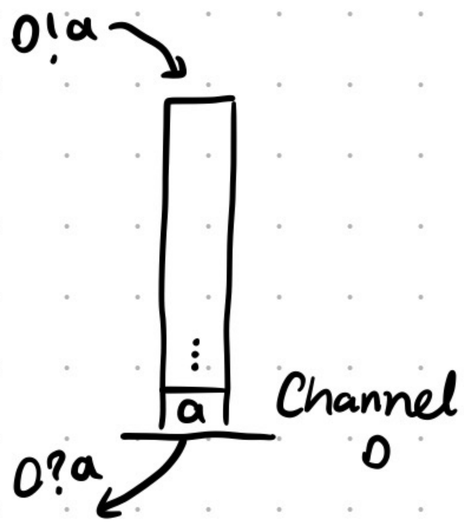
Lossy Channel Systems

A lossy channel system (LCS) $L = (Q, q_0, C, M, \rightarrow)$ consists of

- A finite set of states Q
- An initial state $q_0 \in Q$
- A finite set of channels C
- A finite message alphabet M
- And a transition relation $\rightarrow \subseteq Q \times OP \times Q$ that performs an operation in $OP = C \times \{!, ?\} \times M$

  e.g. $0!a$: append $a \in M$ to channel 0
  $0?a$: pop $a \in M$ from the head of channel 0

Idea:



we write $p \xrightarrow{i!a} q$ or $(p \xrightarrow{i?a} q)$ to denote
$(p, i!a, q) \in \rightarrow$ or $(p, i?a, q) \in \rightarrow$.

We use one set of states Q to model the communication over multiple automata.
This is not a problem because we can use the product
(States of Entity 1) x ... x (States of Entity k)

Let $L = (Q, q_0, C, M, \rightarrow)$ be an LCS for the rest of this lecture.
The operational semantics (the runtime behaviour) of the LCS is defined as a transition system $\mathcal{U}_L = (Cf, \{(q_0, (\varepsilon, \dots, \varepsilon))\}, \rightarrow)$ with

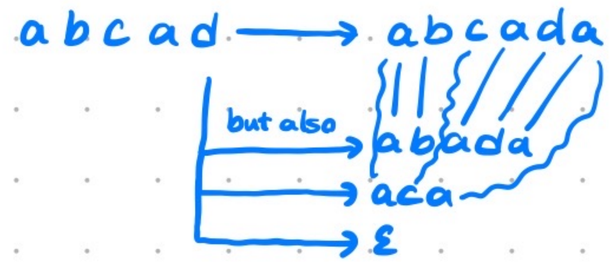
- the set of configurations $Cf = \{(q, W) \mid q \in Q, W : C \to M^*\}$.
- the initial configuration $(q_0, (\underbrace{\varepsilon, \dots, \varepsilon}_{\text{all channels empty}}))$
- the transition relation $\rightarrow \subseteq Cf \times Cf$ as the smallest relation with (we use the same arrow "$\rightarrow$" for the transition system, but the arrow we mean should be clear from the context: $\rightarrow \subseteq Q \times OP \times Q$ vs. $\rightarrow \subseteq Cf \times Cf$)

$(q_1, W) \longrightarrow (q_2, W')$ if $q_1 \xrightarrow{c!a} q_2$ and $W'(d) = W(d)$ if $d \neq c$
$W'(c) = W(c).a$

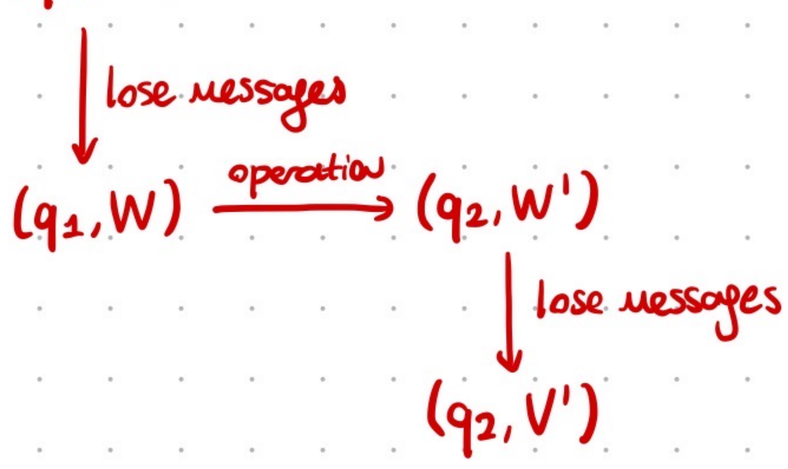
$(q_1, W) \longrightarrow (q_2, W')$ if $q_1 \xrightarrow{c?a} q_2$ and $W(d) = W'(d)$ if $d \neq c$
$W(c) = a.W'(c)$.

$(q_1, V) \longrightarrow (q_2, V')$ if $(q_1, W) \to (q_2, W')$ and $V(c) \geq W(c)$ and $V'(c) \leq W'(c)$ for all $c \in C$, under the subsequence ordering

→ recall the ordering over symbols in $(M, =)$)
$x_0 \dots x_k \geq x_{i_0} \dots x_{i_\ell}$ where $0 \leq i_0 < i_1 < \dots < i_\ell \leq k$
e.g. theoreuprover ≥ oreo
→ this encodes the "loss"



Picture



Now we show that $\mathcal{U}_L = (Cf, \preceq, \{(q_0, (\varepsilon, \dots, \varepsilon))\}, \rightarrow)$ is a WSTS under the ordering

$(q, W) \preceq (q', W')$ if $q = q'$ and $W(c) \leq W'(c)$ for all $c \in C$ under the subsequence ordering over the alphabet $(M, =)$.

LCS are WSTS

We need to show two properties:

(1) $\rightarrow$ is monotonous wrt. $\preceq$
(2) $(Cf, \preceq)$ is a wqo.

We first show monotonity.

Lemma: Let $(q,W), (p,V), (p';V') \in Cf$ with $(p,V) \rightarrow (p';V')$ and $(p,V) \leq (q,W)$
Then there is a $(q';W') \in Cf$ with $(q,W) \rightarrow (q';W')$ and $(p';V') \leq (q',W')$

Proof: The result follows from the definitions:

The relation $(q,W) \geq (p,V)$ implies $q=p$ and $W(c) \geq V(c)$ for all $c \in C$.
Since $(p,V) \rightarrow (p',V')$, it follows from the $\rightarrow$ definition that $(q,W) = (p,W) \rightarrow (p';V')$.
We let $(q';W') = (p';V')$ and get $(q,W) \rightarrow (q,W')$, completing the proof.

It remains to show that $(Cf, \preceq)$ is a wqo.
Note that $(Cf, \preceq)$ is the product order of $(Q, =)$ with $|C|$ copies of $(M^*, \leq)$.
So, if $(M^*, \leq)$ is a wqo, we get that $(Cf, \preceq)$ is a wqo by repeatedly applying Dickson's Lemma.
We do something more general and show (as promised last week) that applying the subsequence ordering to a wqo results in a wqo.

Theorem (Higman's Lemma): If $(Q, \leq)$ is a wqo, then so is $(Q^*, \leq)$.

(Proof on the next page)

Proof: Suppose there are infinite sequences that are bad.

Overview

We construct an infinite bad sequence that is made up of words that are as small as possible.
We do this by inductively choosing the next word such that we can still extend it to an infinite bad sequence.
We will derive a contradiction by finding an even "smaller" infinite bad sequence.

The Proof

First, we construct $(w_i)_{i\in\mathbb{N}}$ that is (1) bad and (2) all sequences $(v_i)_{i\in\mathbb{N}}$ with a $k\in\mathbb{N}$ where $v_j = w_j$ for all $j<k$ and $|v_k|<|w_k|$, are good.

For the base case, we choose a shortest word $w_0 \in Q^*$ that can be extended to a bad sequence (We can make such a choice because the set of lengths $\mathbb{N}$ is well founded).
For the inductive case, we have the bad sequence $w_0, w_1, \dots, w_i$ with the property (2) that can be extended to an infinite bad sequence. (restricted to $k\leq i$)
We extend it by choosing the shortest word $w_{i+1} \in Q^*$ such that $w_0, w_1, \dots, w_{i+1}$ can be extended to an infinite bad sequence.

Since subsequences of bad sequences are also bad, $w_0, w_1, \dots, w_{i+1}$ is bad.

The property (2) also holds: Let $(v_i)_{i\in\mathbb{N}}$ with $k\leq i+1$ where $v_j = w_j$ for all $j<k$ and $|v_j|<|w_j|$.
If $k\leq i$, the result follows from applying the induction hypothesis ((2)) to $w_0, \dots, w_i$.
If $k=i+1$, $|v_{i+1}|<|w_{i+1}|$ holds. Since $(v_i)_{i\in\mathbb{N}}$ is bad, we would have chosen v_{i+1} instead of w_{i+1}.
It can easily be verified that the full sequence $(w_i)_{i\in\mathbb{N}}$ is bad and has (2).

Since $(w_i)_{i\in\mathbb{N}}$ is bad, no element is ε, since ε is the smallest element.
Now consider the first letters $a_0, a_1, \dots$ of the words $w_0, w_1, \dots$. Let $w_i = a_i \cdot w_i'$ for all $i\in\mathbb{N}$.
The sequence $(a_i)_{i\in\mathbb{N}}$ is in Q. Since Q is a wqo, there must be an increasing subsequence $(a_{\varphi(i)})_{i\in\mathbb{N}}$.
We construct the sequence

$$(v_i)_{i\in\mathbb{N}} = \underbrace{w_0, w_1, w_2, \dots, w_{\varphi(0)-1}}_{\text{from } (w_i)_{i\in\mathbb{N}}}, \underbrace{w'_{\varphi(0)}, w'_{\varphi(1)}, w'_{\varphi(2)}, \dots}_{\text{from } (w'_{\varphi(i)})_{i\in\mathbb{N}}}$$

The first $\varphi(0)$ elements are the same as $(w_i)_{i\in\mathbb{N}}$ but the $(\varphi(0)+1)$-th element is shorter.
So, $(v_i)_{i\in\mathbb{N}}$ must be good. Then there are two indices $i<j$ with $v_i \leq v_j$.
We show that this contradicts the badness of $(w_i)_{i\in\mathbb{N}}$.

Case $i,j < \varphi(0)$: We get $w_i \leq w_j$ since both indices are in the blue part of the sequence. ↯

Case $i<\varphi(0)$ and $j\geq\varphi(0)$: Then $v_j = w_{\varphi(\ell)}$ for some $\ell\in\mathbb{N}$. We have $w_i \leq w'_{\varphi(\ell)} \leq a_{\varphi(\ell)} \cdot w'_{\varphi(\ell)} = w_{\varphi(\ell)}$ ↯

Case $i,j\geq\varphi(0)$: Then $v_i = w'_{\varphi(\ell)}$, and $v_j = w'_{\varphi(m)}$ for $\ell<m$. We have $a_{\varphi(\ell)} \leq a_{\varphi(m)}$.
Combined with $w'_{\varphi(\ell)} \leq w'_{\varphi(m)}$, we get $w_{\varphi(\ell)} = a_{\varphi(\ell)} \cdot w'_{\varphi(\ell)} \leq a_{\varphi(m)} \cdot w'_{\varphi(m)} = w_{\varphi(m)}$. ↯ □

Corollary

(Abdulla+WSTS): Upward closed reachability is decidable for LCS.