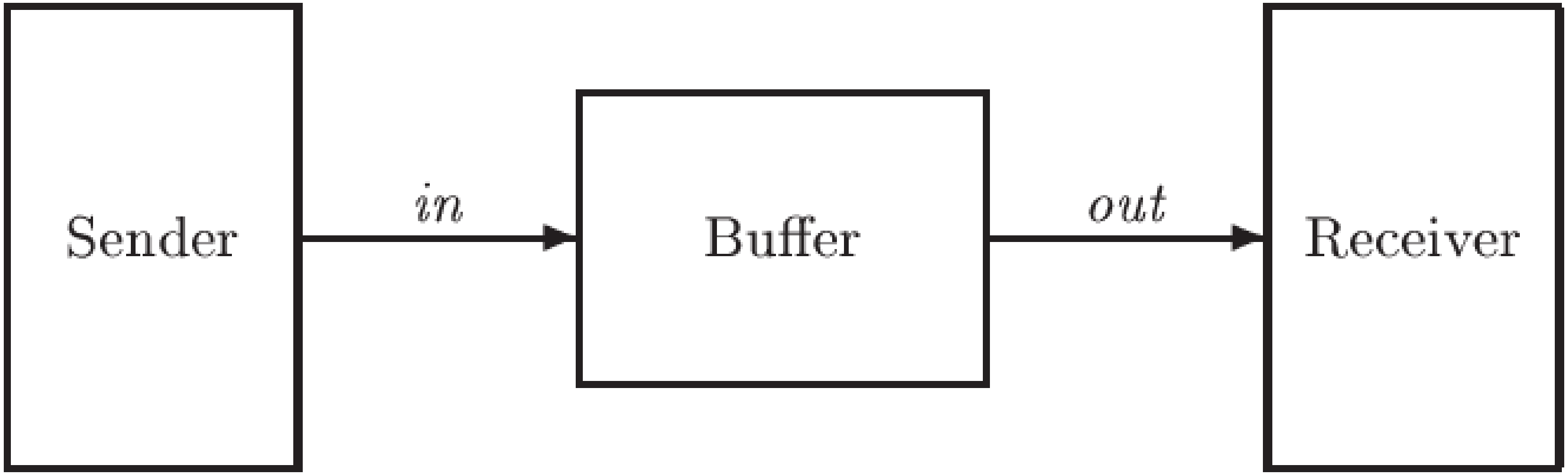
Faculty of Computer Systems & Software Engineering

Formal methods.

Specification of FIFO

Vitaliy Mezhuyev

FIFO



1. We have Sender and Receiver, like in Async Interface
2. They communicate via Buffer by ***in*** and ***out*** lines.
3. Communication is asynchronous, because Buffer can store data in FIFO.

Modeling FIFO buffer

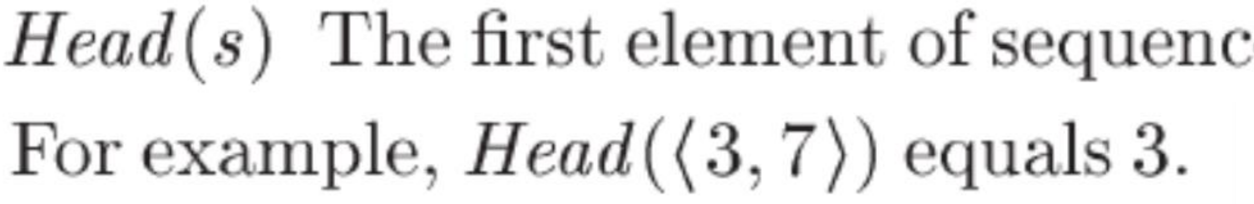
1. We will model FIFO buffer as a sequence of messages.

2. For it we need use (keyword **EXTENDS**) module **Sequences** (together with module Naturals).

3. The Sequences module defines operations on finite sequences of ordered elements (tuples).

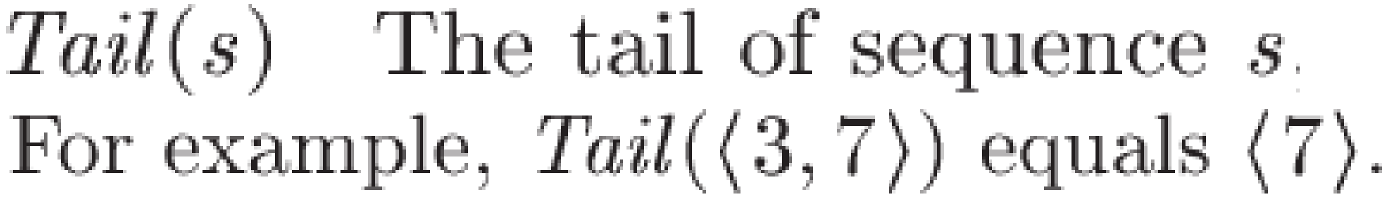
4. Tuple is represented with << >>

The basic operations of Sequences module



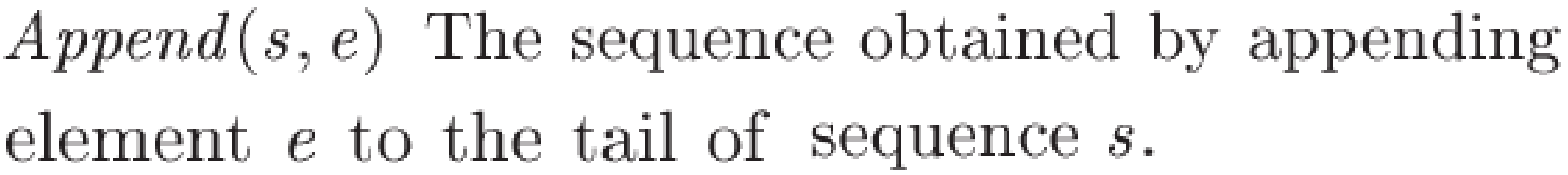
$Head(s)$ The first element of sequence s.

For example, $Head(\langle 3, 7 \rangle)$ equals 3.



$Tail(s)$ The tail of sequence s.

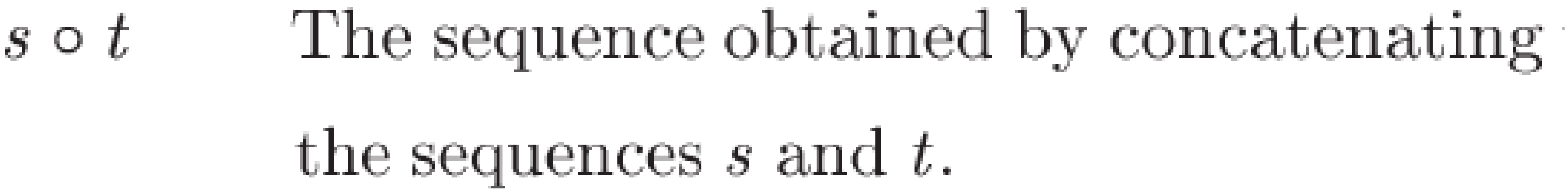
For example, $Tail(\langle 3, 7 \rangle)$ equals $\langle 7 \rangle$.



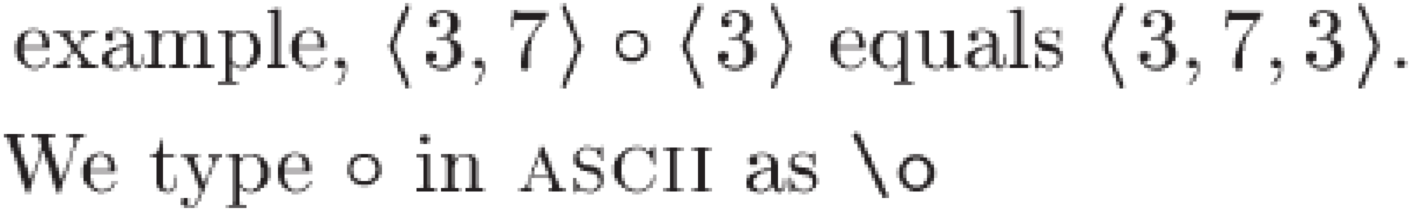
$Append(s, e)$ The sequence obtained by appending element e to the tail of sequence s.

For example, $Append(\langle 3, 7 \rangle, 3)$ equals $\langle 3, 7, 3 \rangle$.

Work with Sequences

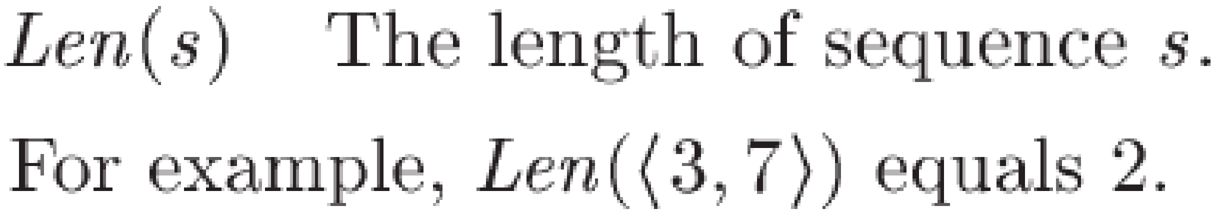


$s \circ t$ The sequence obtained by concatenating the sequences s and t.



example, $\langle 3, 7 \rangle \circ \langle 3 \rangle$ equals $\langle 3, 7, 3 \rangle$.

We type $\circ$ in ASCII as \o



$Len(s)$ The length of sequence s.

For example, $Len(\langle 3, 7 \rangle)$ equals 2.

Specification of constants and variables

- Constant **Data** represents the set of all messages that can be sent

- Variable Buf represents the queue (FIFO buffer) of messages.

- The value of Buf is the sequence of messages that have been sent by the **Sender** but not yet received by the **Receiver**.

Send and Receive actions

Send – there is exists an element in Data set, such that we will *append* to the Buf

\E d \in Data : Buf' = Append (Buf, d)

Receive - the next state of the Buf will be the *tail* of Buf in old state

Buf' = Tail (Buf)

Definition of Bounded FIFO

- We have specified an unbounded FIFO, that can hold an any number of messages.
- Any real system has a finite amount of resources, so FIFO can contain only a limited number of messages.
- So, action Send is enabled if there are fewer than N messages in the buffer, i.e. Len(Buf) is less than N.
- N is a const – a positive natural number.

Liveness properties

- Specification of a bounded FIFO was its safety property

A possible liveness property

- Buffer is eventually often full or eventually often empty

  []<> (Len (Buf) = 0 \/ Len (Buf) = N)

Questions

1. What is FIFO?
2. How to specify sequences in TLA?
3. How to add element to the end of a sequence?
4. How to get head and tail of a sequence?
5. How to concatenate two sequences?
6. How to find a length of a sequence?
7. Describe the possible actions of FIFO
8. How to specify a bounded FIFO?
9. What are the possible liveness properties for a FIFO protocol?

Thank you for your attention!
Please ask questions