

Refinement Exercise: ASMs with Stack Operations

using static
concatenation

ADD(Elem) =
stack := Elem.stack

REMOVE =
if stack = Elem.q
then stack := q
else errmsg := ...

using dynamic head,next

ADD(Elem) =

let pos = new(POS) in
next(pos) := head
head := pos
stack(pos) := Elem

REMOVE =

if head ¹ undef
then head := next(head)
else errmsg := ...

Prove: M2 correctly refines M1: “corresponding” runs have “equiv” stacks
 $e1.e2. \dots en \sim \text{stack}(\text{head})=e1, \dots, \text{stack}(\text{next}^{n-1}(\text{head}))=en$
and execs of ADD resp. REMOVE ops correspond to each other