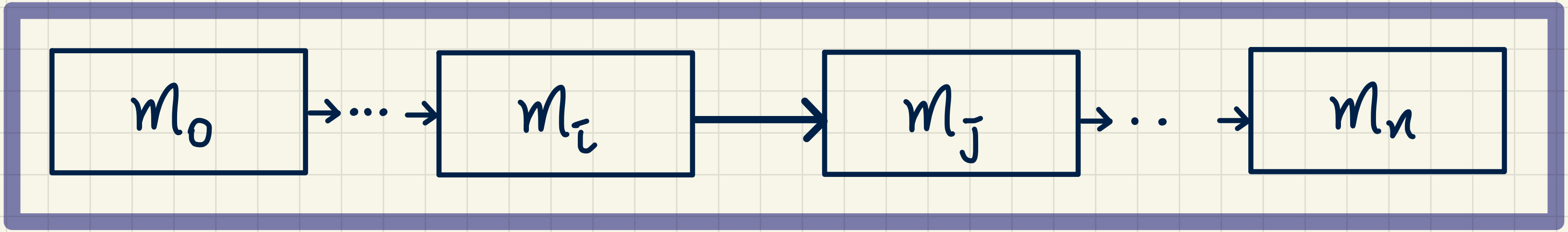
Formalizing Arrays as Functions

```
String[] names = {"alan", "mark", "tom"};
```

Correct by Construction



State Space of a Model

Definition: The state space of a model is
the set of all possible valuations of its declared constants and variables, subject to declared constraints.

Say an initial model of a bank system with two constants and a variable:

$c \in \mathbb{N}1 \wedge L \in \mathbb{N}1 \wedge accounts \in String \nrightarrow \mathbb{Z}$ /* typing constraint */

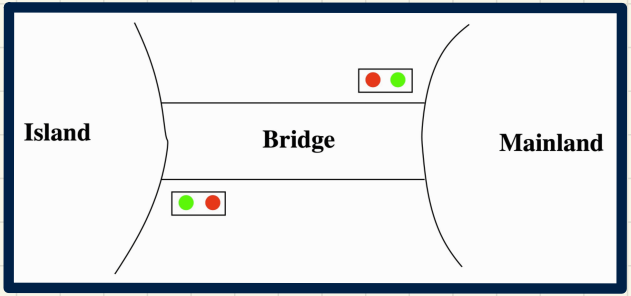
$\forall id \bullet id \in \mathrm{dom}(accounts) \Rightarrow -c \leq accounts(id) \leq L$ /* desired property */

Q1. Give some example configurations of this initial model's state space.

Q2. How large exactly is this initial model's state space?

Bridge Controller:

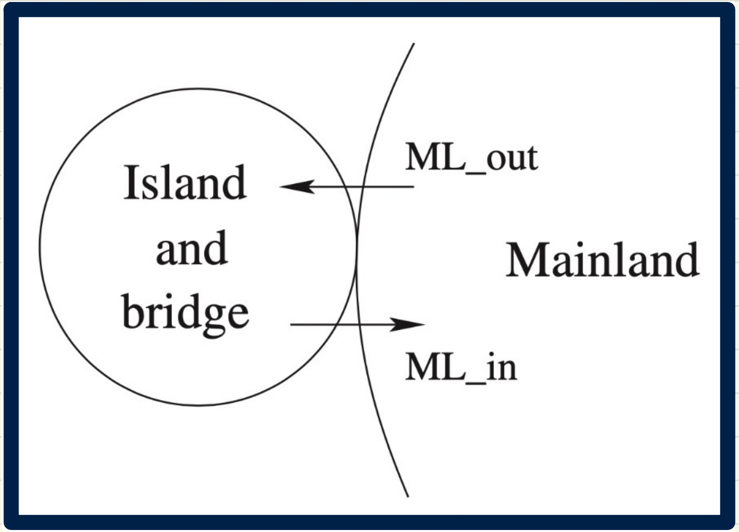
Requirements Document



ENV1	The system is equipped with two traffic lights with two colors: green and red.
ENV2	The traffic lights control the entrance to the bridge at both ends of it.
ENV3	Cars are not supposed to pass on a red traffic light, only on a green one.
ENV4	The system is equipped with four sensors with two states: on or off.
ENV5	The sensors are used to detect the presence of a car entering or leaving the bridge: "on" means that a car is willing to enter the bridge or to leave it.
REQ1	The system is controlling cars on a bridge connecting the mainland to an island.
REQ2	The number of cars on bridge and island is limited.
REQ3	The bridge is one-way or the other, not both at the same time.

Bridge Controller: Abstraction in the Initial Model

REQ2	The number of cars on bridge and island is limited.



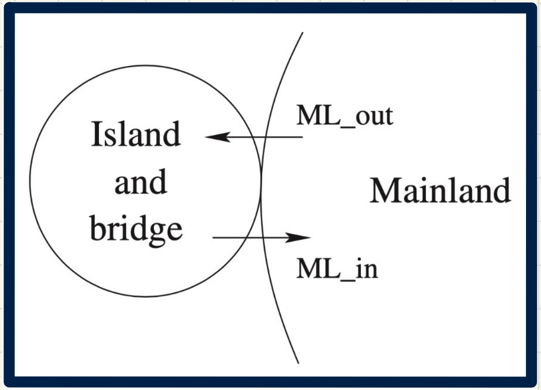
Bridge Controller: State Space of the Initial Model

REQ2	The number of cars on bridge and island is limited.

Static Part of Model

constants: d

axioms:
axm0_1 : $d \in \mathbb{N}$



Dynamic Part of Model

variables: n

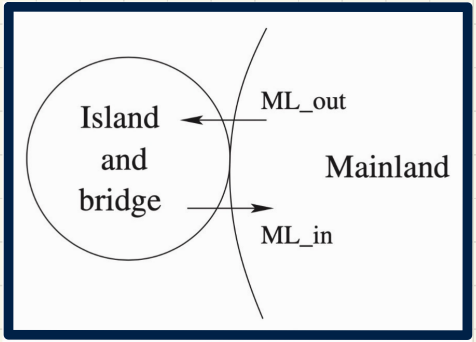
invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

Bridge Controller: State Transitions of the Initial Model

REQ2	The number of cars on bridge and island is limited.

constants: d

axioms:
axm0_1 : $d \in \mathbb{N}$



variables: n

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

ML_out
begin
$n := n + 1$
end

ML_in
begin
$n := n - 1$
end

State Transition Diagram on an Example Configuration

d = 2

n initialized to 0

d = 2
n =

Before-After Predicates of Event Actions

Events	ML_out	ML_in
	$n := n + 1$	$n := n - 1$
before–after predicates	$n' = n + 1$	$n' = n - 1$

- Pre-State
- Post-State
- Sate Transition

Exercise: Event Actions vs. Before-After Predicates

Q. Are the following event actions suitable for a swap between x and y?

```
swap
  begin
    temp := x
    x := y
    y := temp
  end
```

Design of Events: Invariant Preservation

variables: n

```
ML_out
  begin
    n := n + 1
  end
```

```
ML_in
  begin
    n := n − 1
  end
```

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

Sequents: Syntax and Semantics

Syntax

$$H \vdash G$$

$$\begin{array}{c} H \\ \vdash \\ G \end{array}$$

Semantics

Q. What does it mean when H is empty/absent?

PO/VC Rule of Invariant Preservation

constants: d

variables: n

ML_out
begin
$n := n + 1$
end

axioms:
axm0_1 : $d \in \mathbb{N}$

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

ML_in
begin
$n := n - 1$
end

Axioms *Invariants* Satisfied at ***Pre-State*** Guards of the Event $\vdash$ *Invariants* Satisfied at ***Post-State***	INV

PO/VC Rule of Invariant Preservation: Components

constants: d

variables: n

ML_out
begin
$n := n + 1$
end

axioms:
axm0_1 : $d \in \mathbb{N}$

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

ML_in
begin
$n := n - 1$
end

c: list of constants

A(c): list of axioms

v and v′: variables in pre- and post-state

I(c, v): list of invariants

G(c, v): guards of an event's

E(c, v): effect of an event's actions

v′ = E(c, v): BAP of an event's actions

PO/VC Rule of Invariant Preservation: Sequents

constants: d	**variables:** n	ML_out **begin** $n := n + 1$ **end**
axioms: **axm0_1** : $d \in \mathbb{N}$	**invariants:** **inv0_1** : $n \in \mathbb{N}$ **inv0_2** : $n \leq d$	ML_in **begin** $n := n - 1$ **end**

$$A(c)$$
$$I(c, v)$$
$$G(c, v)$$
$$\vdash$$
$$I_i(c, E(c, v))$$

Q. How many PO/VC rules for model m0?

PO/VC Rule of Invariant Preservation: Sequents

constants: d

variables: n

axioms:
axm0_1 : $d \in \mathbb{N}$

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

ML_out
begin
$n := n + 1$
end

ML_in
begin
$n := n - 1$
end

$$A(c)$$
$$I(c, \mathbf{v})$$
$$G(c, \mathbf{v})$$
$$\vdash$$
$$I_i(c, \mathbf{E(c, v)})$$

Inference Rule: Syntax and Semantics

Syntax

$$\frac{A}{C}\ L$$

Semantics

Q. What does it mean when **A** is empty/absent?

Examples

Proof of Sequent: Steps and Structure

Outstanding Sequent to Prove

$$d \in \mathbb{N}$$
$$n \in \mathbb{N}$$
$$n \leq d$$
$$\vdash$$
$$n + 1 \in \mathbb{N}$$

ML_out/inv0_1/INV

Known Inference Rules

$$\frac{H1 \vdash G}{H1, H2 \vdash G} \quad \textbf{MON}$$

$$\frac{}{n \in \mathbb{N} \vdash n + 1 \in \mathbb{N}} \quad \textbf{P2}$$

Understanding Inference Rule: OR_L

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \lor Q \vdash R} \ \textbf{OR\_L}$$

Justifying Inference Rule: OR_L

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \vee Q \vdash R}\ \textbf{OR\_L}$$

Example Inference Rules

$$\frac{}{\vdash 0 \in \mathbb{N}} \; \textbf{P1}$$

$$\frac{}{n \in \mathbb{N} \vdash n+1 \in \mathbb{N}} \; \textbf{P2}$$

$$\frac{}{n < m \vdash n+1 \leq m} \; \textbf{INC}$$

$$\frac{}{0 < n \vdash n-1 \in \mathbb{N}} \; \textbf{P2'}$$

$$\frac{}{n \leq m \vdash n-1 < m} \; \textbf{DEC}$$

$$\frac{}{n \in \mathbb{N} \vdash 0 \leq n} \; \textbf{P3}$$

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \vee Q \vdash R} \; \textbf{OR\_L}$$

$$\frac{H \vdash P}{H \vdash P \vee Q} \; \textbf{OR\_R1}$$

$$\frac{H \vdash Q}{H \vdash P \vee Q} \; \textbf{OR\_R2}$$

$$\frac{H1 \vdash G}{H1, H2 \vdash G} \; \textbf{MON}$$

Discharging POs of original m0: Invariant Preservation

ML_out/inv0_1/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$\vdash$
$n + 1 \in \mathbb{N}$

ML_in/inv0_1/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$\vdash$
$n - 1 \in \mathbb{N}$

ML_out/inv0_2/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$\vdash$
$n + 1 \leq d$

ML_in/inv0_2/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$\vdash$
$n - 1 \leq d$

$$\frac{H \vdash P}{H \vdash P \vee Q} \quad \text{OR\_R1}$$

$$\frac{H1 \vdash G}{H1, H2 \vdash G} \quad \text{MON}$$

$$\frac{}{n \leq m \vdash n - 1 < m} \quad \text{DEC}$$

$$\frac{}{n \in \mathbb{N} \vdash n + 1 \in \mathbb{N}} \quad \text{P2}$$

PO/VC Rule of Invariant Preservation: Revised M0

constants: d

variables: n

axioms:
axm0_1 : $d \in \mathbb{N}$

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

ML_out
begin
$n := n + 1$
end

ML_in
begin
$n := n - 1$
end

$$A(c)$$
$$I(c, v)$$
$$G(c, v)$$
$$\vdash$$
$$I_i(c, E(c, v))$$

Q. How many PO/VC rules for model m0?

Discharging POs of revised m0: Invariant Preservation

ML_out/inv0_1/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$n < d$
$\vdash$
$n + 1 \in \mathbb{N}$

ML_in/inv0_1/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$n > 0$
$\vdash$
$n - 1 \in \mathbb{N}$

ML_out/inv0_2/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$n < d$
$\vdash$
$n + 1 \leq d$

ML_in/inv0_2/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$n > 0$
$\vdash$
$n - 1 \leq d$

$$\frac{H \vdash P}{H \vdash P \lor Q} \quad \textbf{OR\_R1}$$

$$\frac{H1 \vdash G}{H1, H2 \vdash G} \quad \textbf{MON}$$

$$\frac{}{n \leq m \vdash n - 1 < m} \quad \textbf{DEC}$$

$$\frac{}{n < m \vdash n + 1 \leq m} \quad \textbf{INC}$$

$$\frac{}{n \in \mathbb{N} \vdash n + 1 \in \mathbb{N}} \quad \textbf{P2}$$

$$\frac{}{0 < n \vdash n - 1 \in \mathbb{N}} \quad \textbf{P2'}$$

Initializing the System

$$d \in \mathbb{N},\ n \in \mathbb{N},\ n \leq d,\ n < d \vdash n+1 \in \mathbb{N}$$

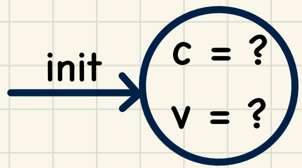
$$d \in \mathbb{N},\ n \in \mathbb{N},\ n \leq d,\ n < d \vdash n+1 \leq d$$

$$d \in \mathbb{N},\ n \in \mathbb{N},\ n \leq d,\ n > 0 \vdash n-1 \in \mathbb{N}$$

$$d \in \mathbb{N},\ n \in \mathbb{N},\ n \leq d,\ n > 0 \vdash n-1 \leq d$$

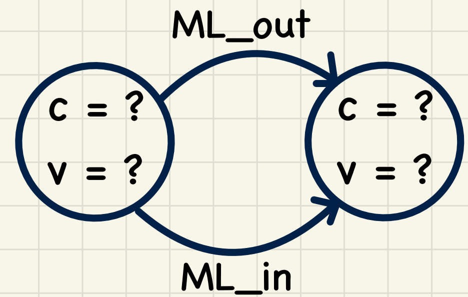
Analogy to Induction:

Base Cases ≈ Establishing Invariants



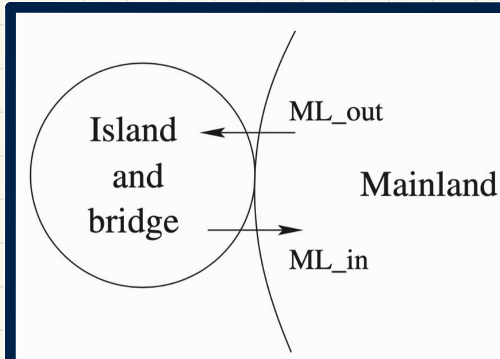
Analogy to Induction:

Inductive Cases ≈ Preserving Invariants



The Initialization Event

```
init
  begin
    n := 0
  end
```



PO of Invariant Establishment

constants: d	variables: n	init **begin** $n := 0$ **end**
axioms: **axm0_1** : $d \in \mathbb{N}$	**invariants:** **inv0_1** : $n \in \mathbb{N}$ **inv0_2** : $n \leq d$	

Components

K(c): effect of init's actions

v′ = K(c): BAP of init's actions

Rule of Invariant Establishment

$$\frac{A(c) \vdash I_i(c, K(c))}{}\ \text{INV}$$

$A(c)$

$\vdash$

$I_i(c, K(c))$ — INV

Exercise:

Generate Sequents from the INV rule.

Discharging PO of Invariant Establishment

$$d \in \mathbb{N} \vdash 0 \in \mathbb{N}$$

init/inv0_1/INV

$$d \in \mathbb{N} \vdash 0 \leq d$$

init/inv0_2/INV

$$\frac{H1 \vdash G}{H1, H2 \vdash G} \text{ MON}$$

$$\frac{}{\vdash 0 \in \mathbb{N}} \text{ P1}$$

$$\frac{}{n \in \mathbb{N} \vdash 0 \leq n} \text{ P3}$$