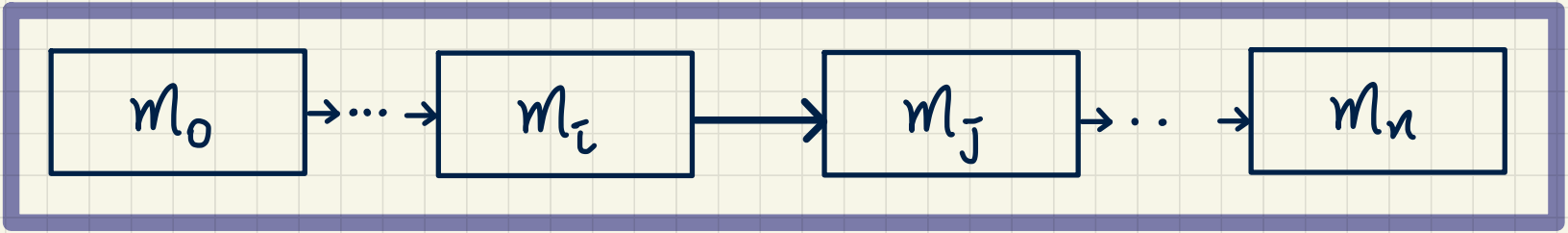
Formalizing Arrays as Functions

```
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:

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

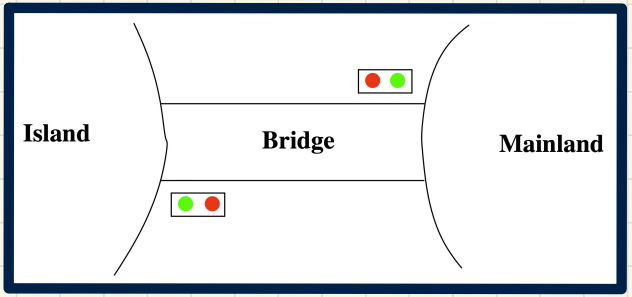
$\forall id \bullet id \in \mathrm{dom}(accounts) \Rightarrow -c \leq accounts(id) \leq L$ /* desired property */

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:

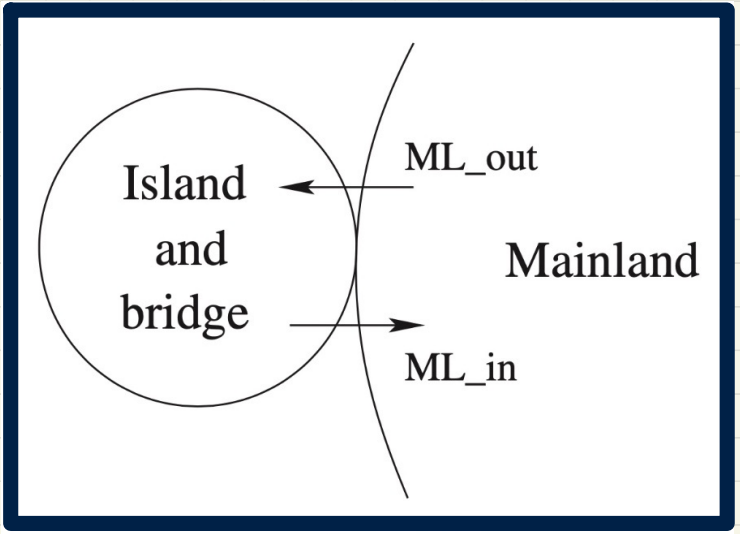
Requirements Document



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.



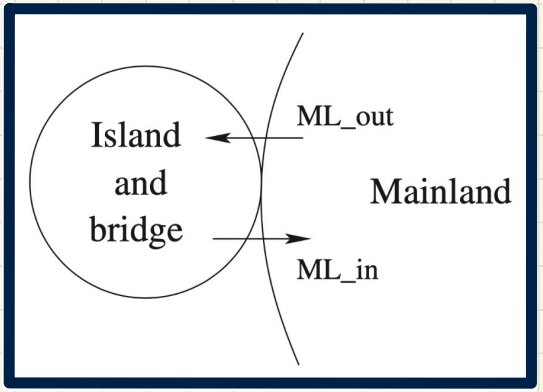
Bridge Controller: State Space of the Initial Model

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

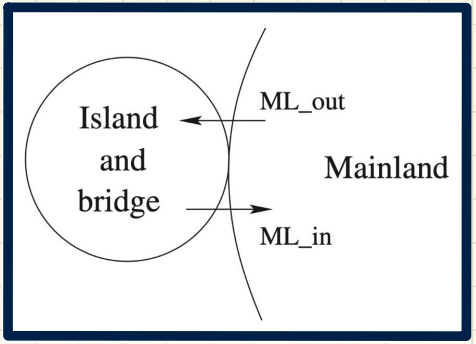
REQ2	The number of cars on bridge and island is limited.

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 =