Event-B Course

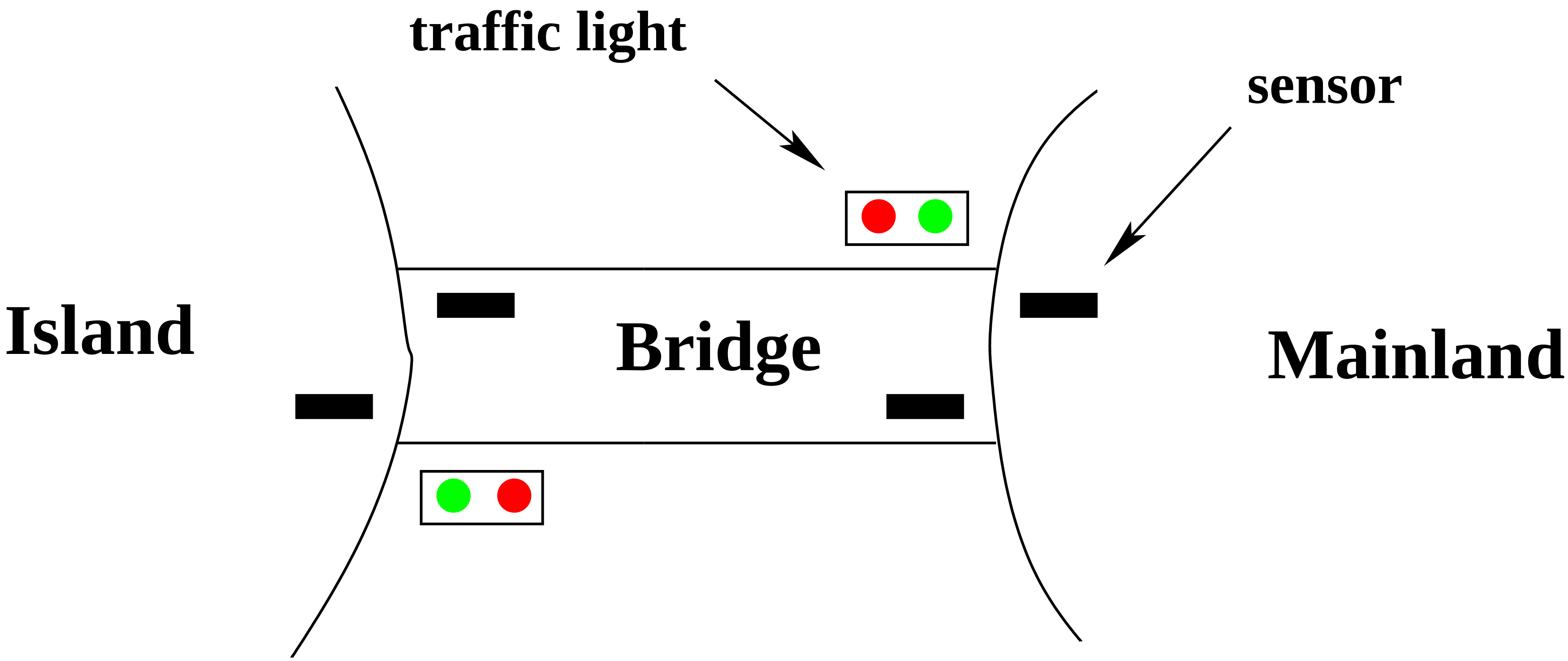
2. Controlling Cars on a Bridge

(summary so far: 9-19-11)

Jean-Raymond Abrial

September-October-November 2011

Environment



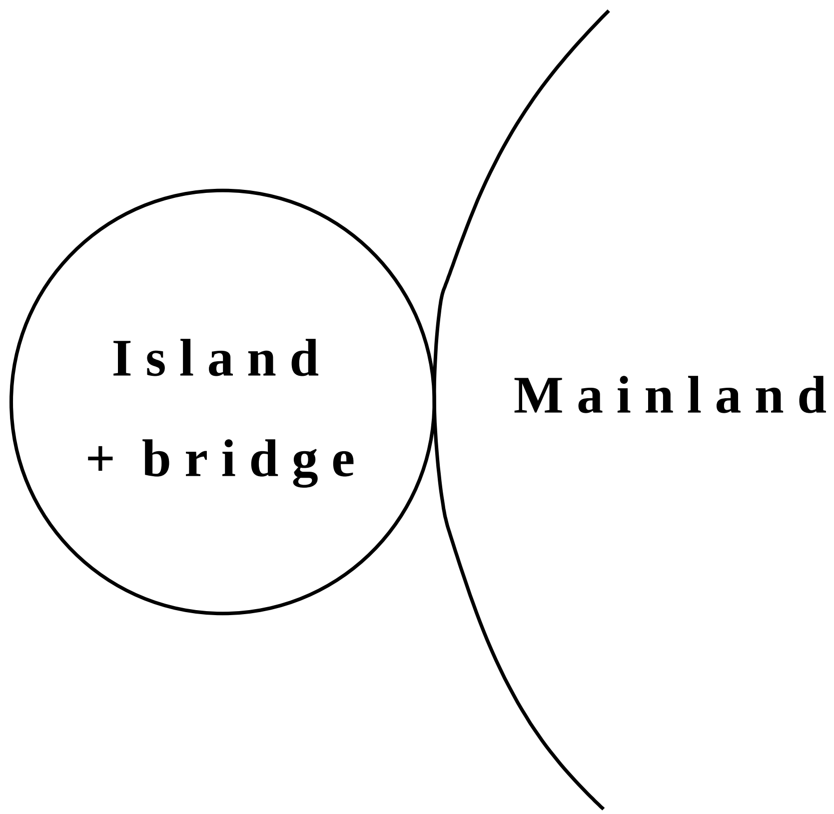
Main Functionalities

The number of cars on the bridge and the island is limited	FUN-2

The bridge is one way or the other, not both at the same time	FUN-3

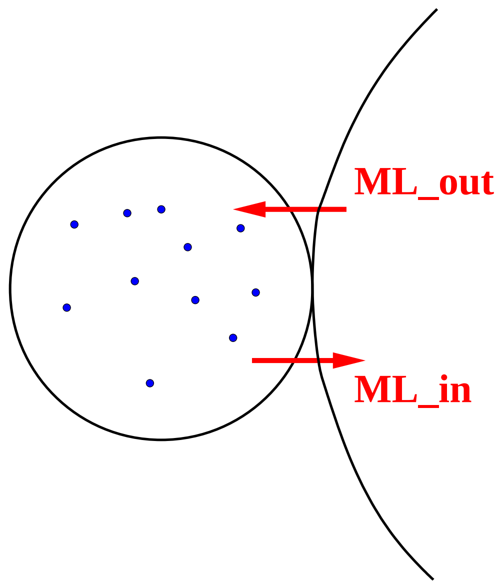
Initial Model

- We do not see the bridge



- We treat FUN-2 (limited number of cars)

Two Events that may be Observed



- We have a single constant d: the maximum number of cars

- We have a single variable n: the number of cars

- We have the invariant: $n \leq d$

Summary of Initial Model

constant: d

variable: n

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

axm0_2: $d > 0$

inv0_1: $n \in \mathbb{N}$

inv0_2: $n \leq d$

init
$n := 0$

ML_out
when
$n < d$
then
$n := n + 1$
end

ML_in
when
$0 < n$
then
$n := n - 1$
end

Proof Obligations for Initial Model

- We have seen three kinds of proof obligations (PO):
  - The Invariant Establishment PO: INV (for initialisation)
  - The Invariant Preservation PO: INV (for other events)
  - The Deadlock Freedom PO (optional): DLF

Proof Obligations for Initial Model (cont'd)

Axioms $\vdash$ Modified Invariant	INV

Axioms Invariants Guard of the event $\vdash$ Modified Invariant	INV

Axiom Invariants $\vdash$ Disjunction of the guards	DLF

Sequents

- A sequent is a formal statement of the following shape:

horizontal

$$\mathbf{H} \vdash \mathbf{G}$$

vertical

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

- **H** denotes a set of predicates: the hypotheses (or assumptions)

- **G** denotes a predicate: the goal (or conclusion)

- The symbol "$\vdash$", called the turnstyle, stands for provability.

  It is read: "Assumptions **H** yield conclusion **G**"

Inference Rules

- Inference rules are used to prove sequents

$$\frac{\mathbf{H}_1 \ \vdash \ \mathbf{G}_1 \qquad \cdots \qquad \mathbf{H}_n \ \vdash \ \mathbf{G}_n}{\mathbf{H} \ \vdash \ \mathbf{G}} \quad \textbf{RULE\_NAME}$$

- Above horizontal line: n sequents called antecedents ($n \geq 0$)

- Below horizontal line: exactly one sequent called consequent

- To prove the consequent, it is sufficient to prove the antecedents

- A rule with no antecedent ($n = 0$) is called an axiom

Example of Inference Rule: Monotonicity

- The rule that removes hypotheses can be stated as follows:

$$\frac{\mathbf{H} \;\vdash\; \mathbf{G}}{\mathbf{H, H'} \;\vdash\; \mathbf{G}} \quad \mathbf{MON}$$

- In order to prove $\mathbf{H, H'} \vdash \mathbf{G}$ it is sufficient to prove $\mathbf{H} \vdash \mathbf{G}$

- It expresses the monotonicity of the hypotheses

Some Arithmetic Rules of Inference

- The Second Peano Axiom

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

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

More Arithmetic Rules of Inference

- Axioms about ordering relations on the integers

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

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

More Arithmetic Inference Rules (cont'd)

- First Peano Axiom

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

- Third Peano Axiom (slightly modified)

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

More Inference Rules: Identity and Equality

- The identity axiom (conclusion holds by hypothesis)

$$\frac{}{\mathbf{P} \ \vdash \ \mathbf{P}} \ \mathbf{HYP}$$

- Rewriting an equality (**EQ_LR**) and reflexivity of equality (**EQL**)

$$\frac{\mathbf{H(F),\ E = F \ \vdash \ P(F)}}{\mathbf{H(E),\ E = F \ \vdash \ P(E)}} \ \mathbf{EQ\_LR}$$

$$\frac{}{\vdash \ \mathbf{E = E}} \ \mathbf{EQL}$$

Other examples of Inference Rules: for Disjunction

- Proof by case analysis

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

- Choice for proving a disjunctive goal

$$\frac{\mathbf{H} \ \vdash \ \mathbf{P}}{\mathbf{H} \ \vdash \ \mathbf{P} \vee \mathbf{Q}} \ \mathsf{OR\_R1}$$

$$\frac{\mathbf{H} \ \vdash \ \mathbf{Q}}{\mathbf{H} \ \vdash \ \mathbf{P} \vee \mathbf{Q}} \ \mathsf{OR\_R2}$$

Proofs

- A proof is a tree of sequents with axioms at the leaves.

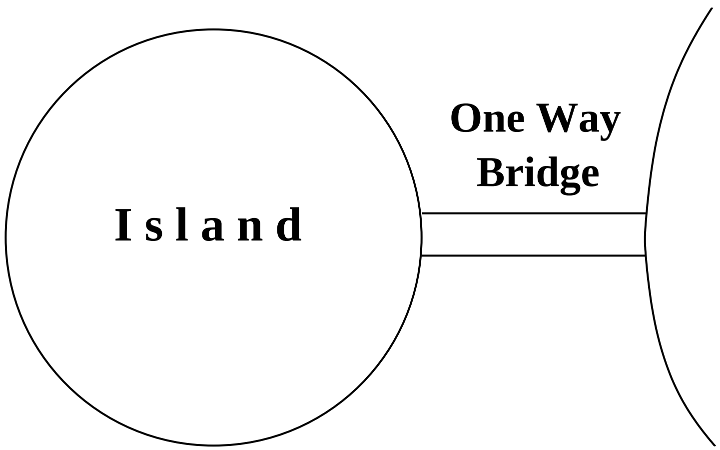
- The rules applied to the leaves are axioms.

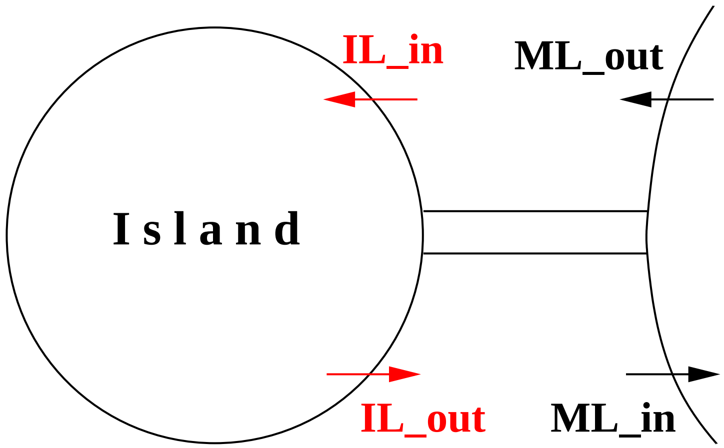
- Each sequent is labeled with (name of) proof rule applied to it.

- The sequent at the root of the tree is called the root sequent.

- The purpose of a proof is to establish the truth of its root sequent.

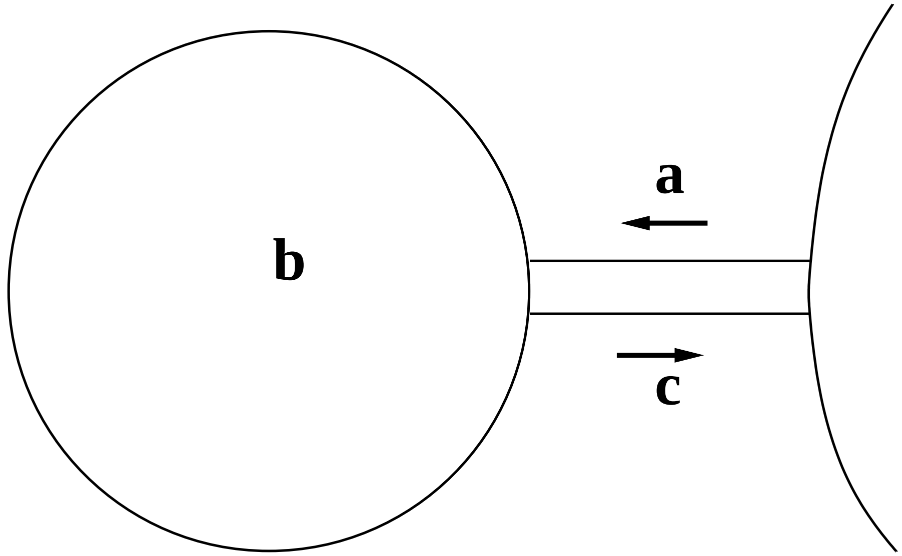
First Refinement: Introducing the one Way Bridge





- We treat FUN-3 (one way bridge)

Introducing Three New Variables: a, b, and c



- We have the following invariant (one way bridge): $\boldsymbol{a = 0 \ \vee \ b = 0}$

- And also the gluing invariant: $\boldsymbol{a + b + c = n}$

- It links the concrete variables $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$ to the abstract one $\boldsymbol{n}$.

State of the First Refinement

constants: d

variables: a, b, c

inv1_1: $a \in \mathbb{N}$

inv1_2: $b \in \mathbb{N}$

inv1_3: $c \in \mathbb{N}$

inv1_4: $a + b + c = n$

inv1_5: $a = 0 \quad \lor \quad c = 0$

Events of the First Refinement (so far)

init
$a := 0$
$b := 0$
$c := 0$

ML_in
when
$0 < c$
then
$c := c - 1$
end

ML_out
when
$a + b < d$
$c = 0$
then
$a := a + 1$
end