UNIVERSITY OF Southampton

Proof Obligations in Event-B

Proof obligation (PO)

- A Proof obligation (PO) is a formal property to be proved of an Event-B model

- A PO is a sequent of the form Hypotheses $\vdash$ Goal

- This means we should prove the goal while assuming that the hypotheses are true.

- The prover uses properties in the Hypotheses, applies rules and tactics, to prove the Goal

- Example

  $x < MAX \vdash x+1 \leq MAX$

  Prove that $x+1 \leq MAX$ assuming that $x < MAX$

Proof obligations in Event-B

- Well-definedness (WD)
  - e.g, avoid division by zero, partial function application

- Invariant preservation (INV)
  - each event maintains the invariants
    - If the invariant is true before the event,
    - And the guard is true
    - Then the invariant is still true after the actions

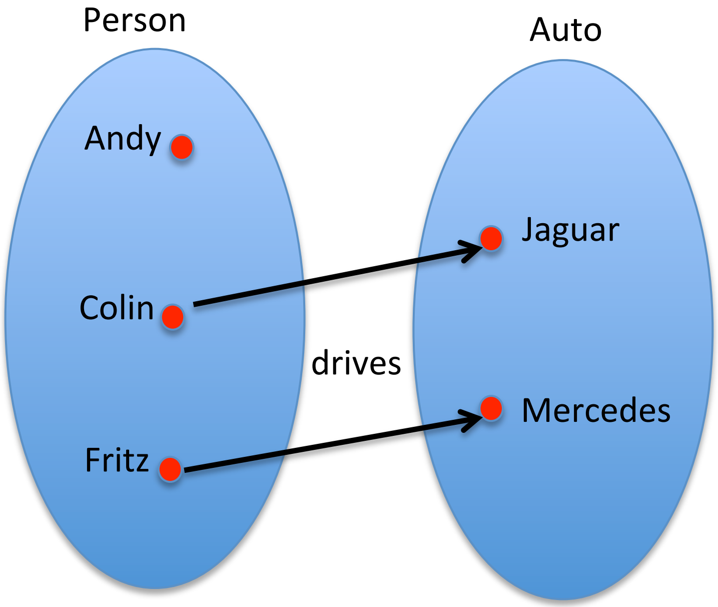
Proof obligations in Event-B

(POs for refinement)

- Simulation (SIM)
  - update of abstract variable correctly simulated by update of concrete variable
- Guard strengthening (GRD)
  - Refined event only possible when abstract event possible
- Convergence (VAR)
  - Ensure convergence of new events using a variant
    - i.e. new events eventually become disabled and allow an old event to occur

Well-definedness PO

(e.g. partial function application)



```
dosomethingtoJaguardrivers =
        any p
        when  p ∈ Person,

                drives(p) = Jaguar
        then
                .....
```

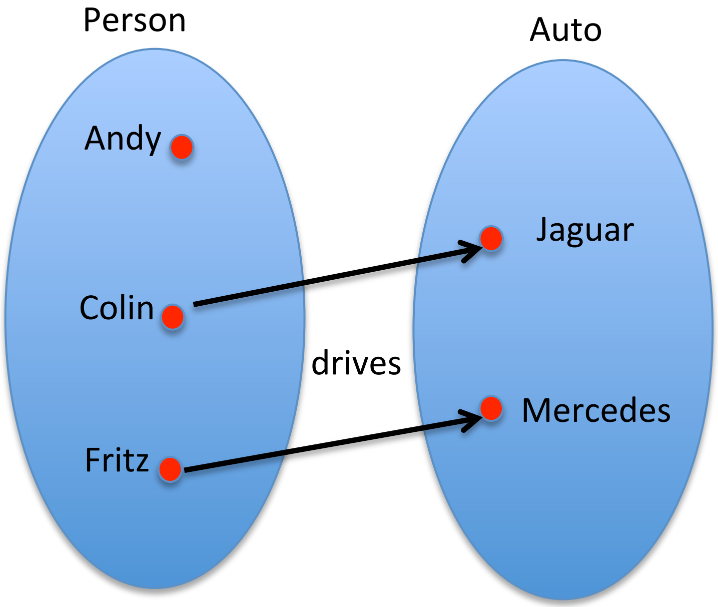
What if p = Andy?

WD PO:

$I, p \in Person \vdash p \in dom(drives)$

Well-definedness PO

(e.g. partial function application)



```
dosomethingtoJaguardrivers =
    any p
    when  p ∈ Person,
          p ∈ dom(drives)
          drives(p) = Jaguar
    then
          .....
```

Add it as a guard

Excludes p = Andy?

WD PO:

I, p : Person, p ∈ dom(drives) ⊢ p ∈ dom(drives)

Event structure

```
E =                         \\  event name
    any
        p1, p2, …           \\  event parameters
    where
        G1                  \\   event guards (predicates)
        G2
        …
    then
        v1 := exp1          \\ event actions
        v2 := exp2
        …
    end
```

Invariant Preservation PO

- Assume: variables v and invariant $I(v)$

- Assume event of this form:

  E = **when** $G(v)$ **then** $v := exp(v)$ **end**

- To prove E preserves $I(v)$:

  INV: $G(v), I(v) \vdash I(exp(v))$

- This is a sequent of the form Hypotheses $\vdash$ Goal

- The sequent is a Proof Obligation (PO) that must be verified

Example

- Invariant: $x \leq MAX$

- Event:

  Inc = **when** $x<MAX$ **then** $x := x+1$ **end**

- To prove Inc preserves $x \leq MAX$ we have this PO:

  INV: $x<MAX , x \leq MAX \quad \vdash \quad x \leq MAX$

Using Event Parameters

- Event has form:

  E = **any** p **where** G(p,v) **then** v := exp(p,v) **end**

INV: $I(v),\ G(p,v) \vdash I(\ exp(p,v)\ )$

Example with parameter

- Invariant: x is even
- Event:

  Inc = **any** p **when** p is even **then** x := x+p **end**

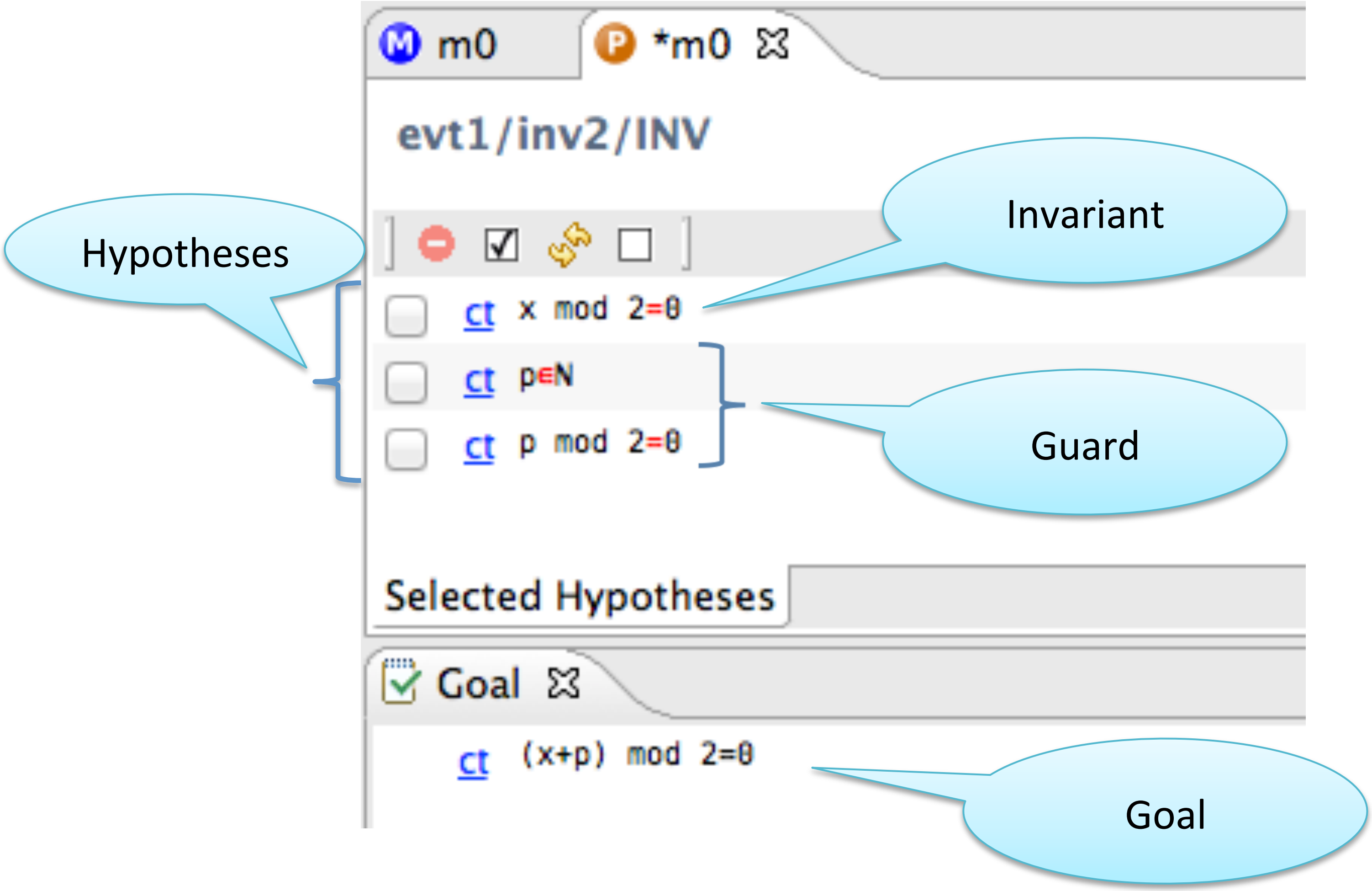
- To prove Inc preserves x is even

- we have this PO:

  INV: p is even, x is even

  $\vdash$ x+p is even

Example PO from Rodin



evt1/inv2/INV

□ ct x mod 2=0

□ ct p∈N

□ ct p mod 2=0

ct (x+p) mod 2=0

Hypotheses

Invariant

Guard

Goal