

Before-After Predicates of Event Actions

Events

ML_out
 $n := n + 1$

ML_in
 $n := n - 1$

before-after predicates

$n' = n + 1$

$n' = n - 1$

- Pre-State
- Post-State
- State 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



Semantics

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

PO/VC Rule of Invariant Preservation

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

Axioms

Invariants Satisfied at *Pre-State*

Guards of the Event

\vdash

Invariants Satisfied at *Post-State*

INV