

Lecture 12 - Oct 21

Bridge Controller

***Before-After Predicate, Inv. Preservation
Formal Model Components
WrittenTest1 Review***

Announcements/Reminders

- Today's class: [notes template](#) posted
- **ProgTest** being graded
- **WrittenTest1** (Oct 22) tomorrow

Transition of an Event

✓
Withdraw

$a : \text{Account}$

$v : \mathbb{N}$

where

$a \in \text{dom}(b)$

begin

b

only
ncr. modified

$b \Leftarrow \{ a \mapsto b(a) - v \}$

end

BAP: $b' = \{ a \mapsto b(a) - v \}$

$b : \text{Account} \mapsto \mathbb{Z}$

$I : \forall a. a \in \text{dom}(b) \Rightarrow b(a) \geq -C$
Invariant



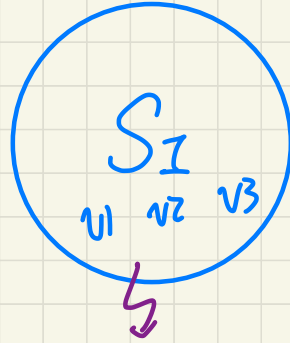
withdraw
guard
evals to true.
effect of event.

post-state
Invariant maintained
(I')

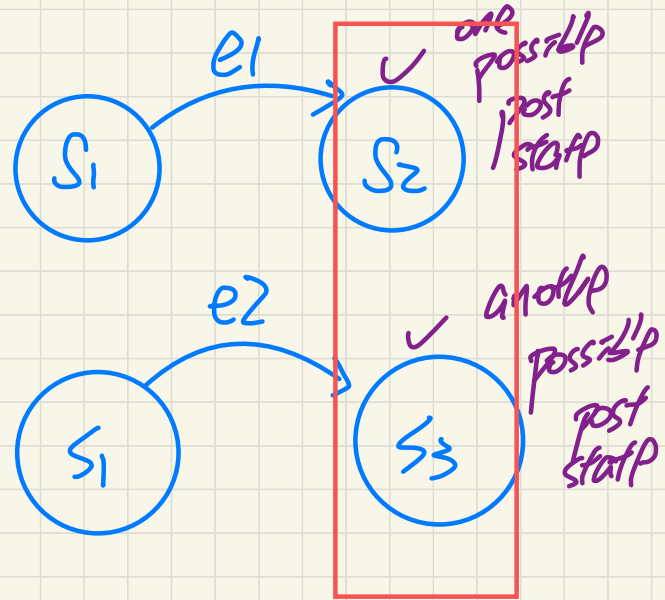
Axiom
 $a \in \text{dom}(b) \rightarrow \text{guard of withdraw}$

$I \forall a. a \in \text{dom}(b) \Rightarrow b(a) \geq -C$

$\neg I'$
 $b \notin \{ \dots \}$
 $\forall a. a \in \text{dom}(b) \Rightarrow b(a) \geq -C$
 $b \notin \{ \dots \}$

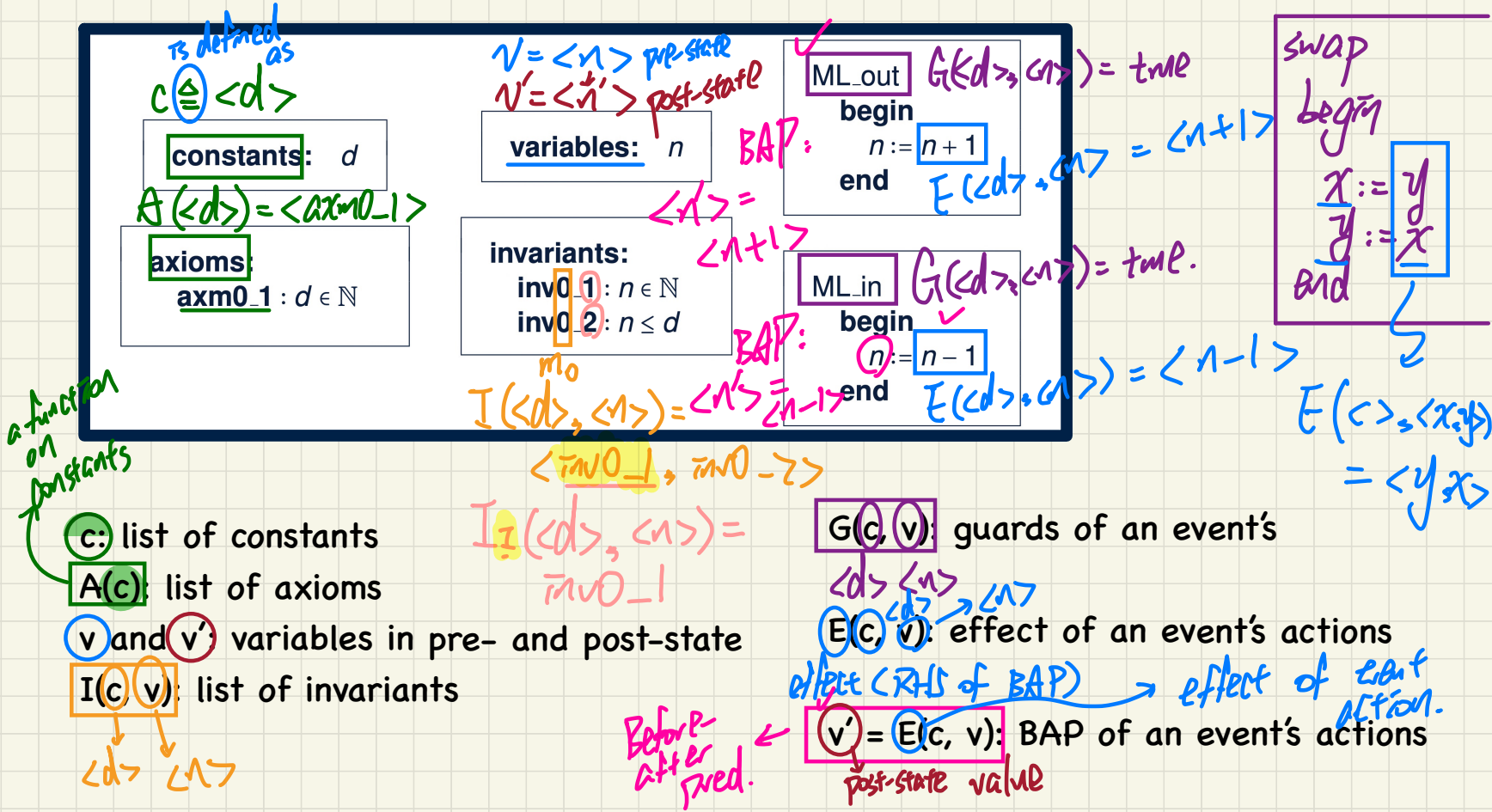


say: e_1, e_2
are enabled
~ only one event
can happen
at a time.



↓
all possible
poststates
must maintain
the invariant.

PO/VC Rule of Invariant Preservation: Components



$axm0$ — 1

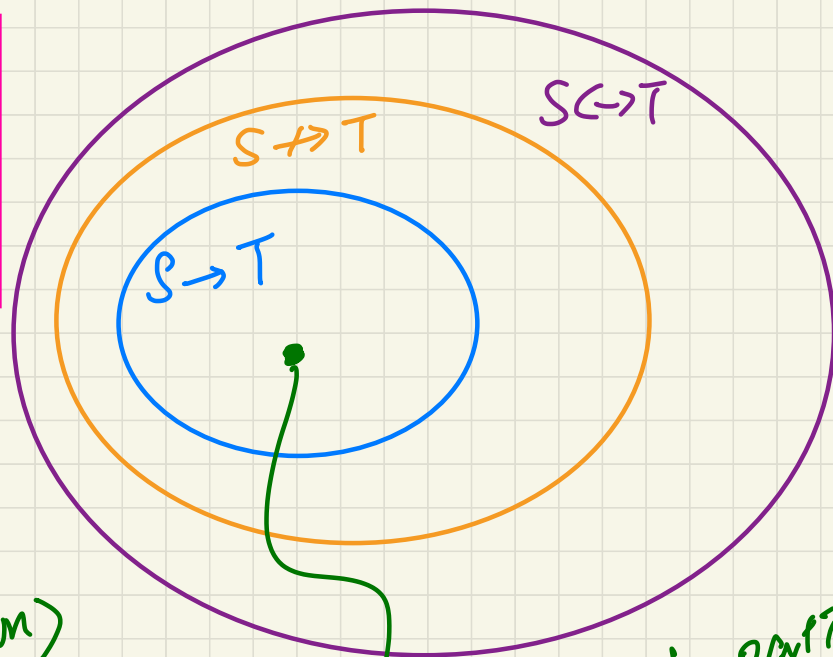
↓
model
No

↳
index
of axioms.

Correct

least accurate

most accurate



Event-B summary
↳ placed desktop

↳ print copy
(bring your own)

↓
not to be
sketched

Correct: total = partial, rel
most accurate: $S \rightarrow T$
least accurate: $S \leftrightarrow T$

$$a : \mathbb{N} \mapsto \mathbb{Z}$$

set of all integers

$$a : \mathbb{N} \mapsto \text{Int}$$

↓
the set of 32-bit ints (in Java)

$$a : \mathbb{N} \rightarrow ?$$

(not feasible)

$$a : \mathbb{N} \mapsto \mathbb{Z}$$

(not feasible)

$$a : \mathbb{N} \mapsto \text{Int}$$

(feasible).

Well-defined
expressions

$$\frac{x}{y} \quad \text{WD if } y \neq 0$$

$$\frac{\frac{\neg \lambda}{\neg \lambda}}{\neg \lambda} \Rightarrow$$

$$r : S \leftrightarrow T$$

$$\frac{S = \{a, b, c\}}{T = \{1, 2\}}$$

↳ a valid relation contains members from S and T only.

$$r = \{(a, 1), (b, 2), (a, 2)\} \quad r[\{c\}] = \emptyset$$

$$r[\{a\}] \rightarrow \emptyset \quad \text{not well-defined.}$$