EEECS3342 System Specification and Refinement (Winter 2022)

Q&A - Week 2 Lecture

Thursday, January 27

Announcements

- Lecture W3 released
- Lab1 Solution released
- Example Questions for Written Test 1 released
- Plan of Returning In-Person (starting Feb. 14)
  + Unchanged
    * Pre-recorded lectures
    * Zoom Weekly Q&A and Office hours in the first instance
    * Zoom Weekly Scheduled labs in the first instance
    * Online Programming & Written tests in the first instance
  + Changed
    * In-Person Exam
  + To be determined:
    * Some (programming and/or written) tests may be in-person, in which case you'll be notified at least one week in advance.

reactive systems.

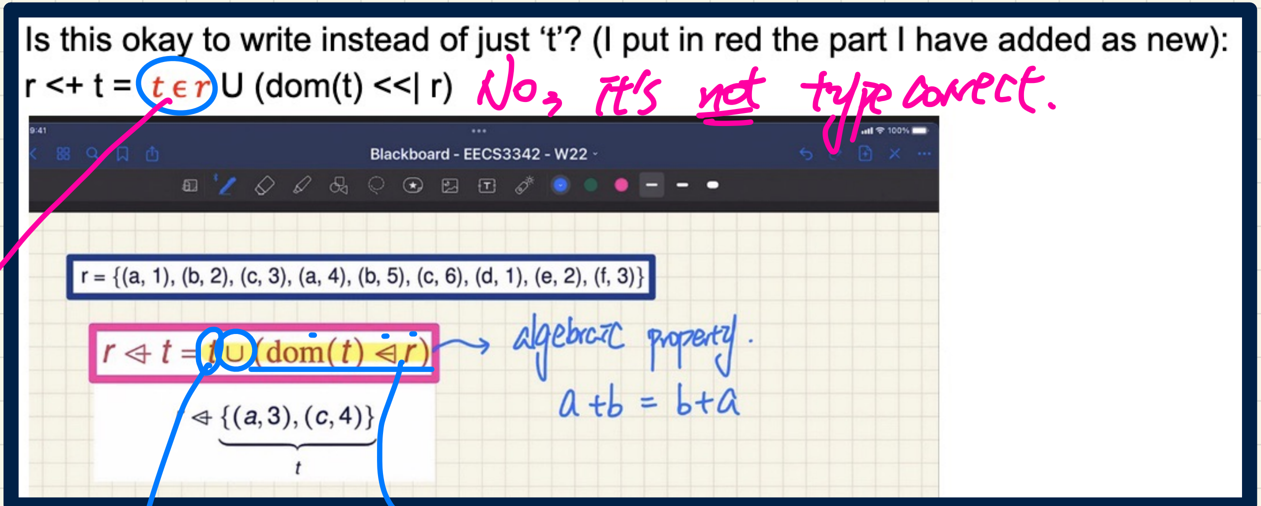
bridge control

WT 1 online

WT 2 ~ 4

ProgTest.

Rewriting Relational Operations



X

set of pairs

set of pairs

disprove

If I want to prove that a function is not bijective, can I simply prove that it's not total, injective or surjective? YES.

Suppose it is not total, do I still need to check if it is injective or surjective?

No, it suffices to disprove that f is bijective by showing that it's not total.

disproving function holding P

↳ give a witness s.t. ¬P.

→ { }.

is_bijective (f) ≜

is_total (f)

∧

is_inj. (f)

∧

is_sur. (f)

App. 1 Not surjective

App. 2 Not injective

$S = \{a, b, c\}$ $T = \{1, 2, 3\}$

$f = \{(a, 1), (b, 2), (c, 1)\}$

Prove or disprove f is bijective.

$\boxed{x ** T}$

$! x . x : INT \Rightarrow x > 0$

not (#

x

)

$\underline{x \circledast y}$

How can we enumerate: $\{1, 2, 3\} \nrightarrow \{a, b\}$

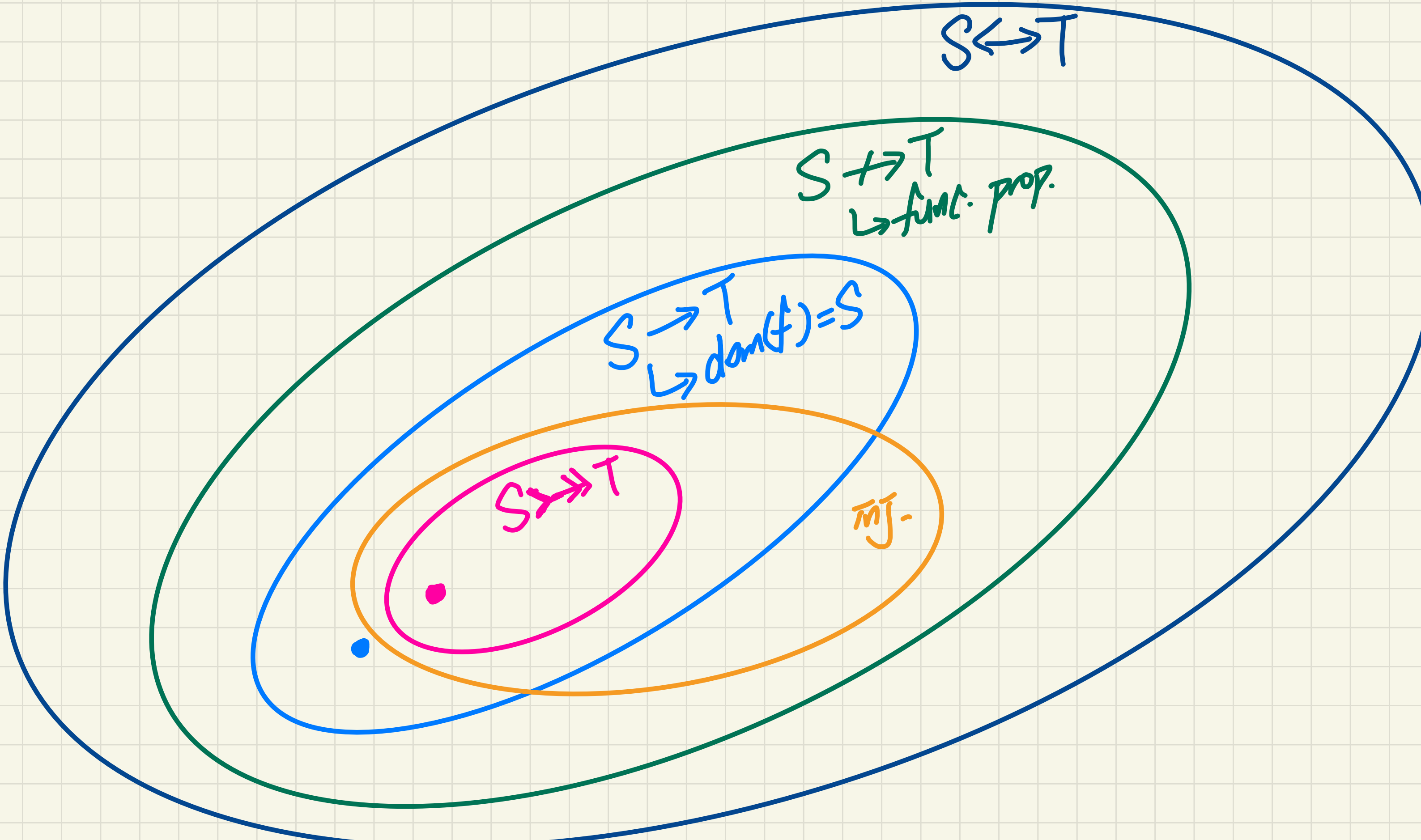
$\{1,2,3\} \leftrightarrow \{a,b\}$

$\{1,2,3\} \nrightarrow \{a,b\}$

relation violating the functional property.

$$
\left\{
\begin{array}{ll}
\# 1 & \emptyset, \\
& \{(1,a)\}, \{(1,b)\}, \\
& \{(2,a)\}, \{(2,b)\}, \\
& \{(3,a)\}, \{(3,b)\}, \\
\# 2 & \cancel{\{(1,a),(1,b)\}} \\
\vdots & \text{Exercise.} \\
\# 6 & \to \cancel{\{1,2,3\} \times \{a,b\}}
\end{array}
\right\}
$$

↳ X function $(1,a), (1,b)$


S ↔ T
S ⇸ T
↳ func. prop.
S → T
↳ dom(f) = S
S ⤖ T
inj.

$$f(n) = 2n^2 + 3n + 4$$

$O(n^2)$

$O(n^3)$

$O(n^4)$

$O(2^n)$

$\boxed{\text{Is every function partial?}}$

→ YES (functional property).

Given two sets S and T, say we write:

- S \/ T for their union
- S /\ T for their intersection
- S \ T for their difference

Pow(______)

What is the **cardinality** of the power set of ({a, b, c, d} \ {a, e}) \/ {a, f}? Enter an integer value (with no spaces).

Answer:

Lab1 Solution: Context

CONTEXT C0

SETS

ACCOUNT carrier set: abstract without the need to enumerate content of the set

PERSON carrier set: details of each member in PERSON are abstracted away (ENV9) - Solution to Exercise 4 of Lab1

CONSTANTS

$-c \leq \underline{\underline{b}}(a) \leq L$

c credit limit (ENV3)

L pre-set upper bound (ENV3) - Solution to Exercise 3 of Lab1

AXIOMS

axm1: $c \in \mathbb{N}_1$

not theorem means an axiom; theorem means a proof is needed. In this case, the typing constraint should be an axiom.

thm1: ⟨theorem⟩ $c > 0$

axm2: $L \in \mathbb{N}_1$

typing constraint of variable L - Solution to Exercise 3 of Lab1

END

Lab1 Solution: Machine (Variables & Invariants)

MACHINE Bank0

// Initial model of the bank system

SEES C0

VARIABLES

b balance (ENV2)

d cash drawer (REQ7)

owner account owner (ENV9) - Solution to Exercise 4 of Lab1

INVARIANTS

inv1: $b \in ACCOUNT \rightarrow\!\!\!\!\!+ \mathbb{Z}$

inv2: $d \in \mathbb{Z}$

inv3: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \geq -c$

(ENV3)

inv4: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \leq L$

(ENV3) - Solution to Exercise 3 of Lab1

inv5: $owner \in ACCOUNT \rightarrow\!\!\!\!\!+ PERSON$

(ENV9) - Solution to Exercise 4 of Lab1

inv6: $dom(b) = dom(owner)$

Consistent domains of the balance and owner functions (ENV9) - Solution to Exercise 4 of Lab1 (Note. If we declared this invariant as a theorem, then it must be provable/derivable from other invariants that are declared as axioms, which is not the case. Instead, we also declare this invariant as an axiom (i.e., not as a theorem) so that proof obligations (POs) will be generated regarding it being established (by INITIALIZATION) and preserved (by other events).)

Lab1 Solution: Machine (INITIALIZATION)

MACHINE Bank0

// Initial model of the bank system

SEES C0

VARIABLES

- b balance (ENV2)
- d cash drawer (REQ7)
- owner account owner (ENV9) - Solution to Exercise 4 of Lab1

INVARIANTS

inv1: $b \in ACCOUNT \nrightarrow \mathbb{Z}$

inv2: $d \in \mathbb{Z}$

inv3: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \geq -c$
(ENV3)

inv4: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \leq L$
(ENV3) - Solution to Exercise 3 of Lab1

inv5: $owner \in ACCOUNT \nrightarrow PERSON$
(ENV9) - Solution to Exercise 4 of Lab1

inv6: $dom(b) = dom(owner)$

Initialisation

begin

act1: $b := \varnothing$

act2:
$d := 0$

(REQ4)

act3: $owner := \varnothing$
Empty bank (ENV9) - Solution to Exercise 4 of Lab1

end

$\varnothing \in ACCOUNT \nrightarrow \mathbb{Z}$

$ACCOUNT \nrightarrow \mathbb{Z}$

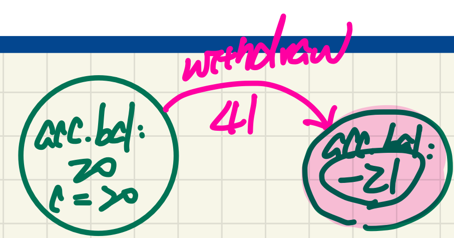
the set of possible partial functions between A. and $\mathbb{Z}$.

Lab1 Solution: Machine (withdraw)

MACHINE Bank0
// Initial model of the bank system
SEES C0
VARIABLES
b balance (ENV2)
d cash drawer (REQ7)
owner account owner (ENV9) - Solution to
INVARIANTS
inv1: $b \in ACCOUNT \rightarrow\!\!\!\!\!+ \mathbb{Z}$
inv2: $d \in \mathbb{Z}$
inv3: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \geq -c$
(ENV3)
inv4: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \leq L$
(ENV3) - Solution to Exercise 3 of Lab1
inv5: $owner \in ACCOUNT \rightarrow\!\!\!\!\!+ PERSON$
(ENV9) - Solution to Exercise 4 of Lab1
inv6: $dom(b) = dom(owner)$

Event withdraw ⟨ordinary⟩ $\widehat{=}$
(REQ6) - Exercise 2 from Lab1: withdraw/inv3/INV cannot be proved.
any
a account to withdraw
v value to withdraw
where
type_of_a: $a \in ACCOUNT$
typing constraint of event parameter a
type_of_v: $v \in \mathbb{N}_1$
typing constraint of event parameter v
wd_for_b(a): $a \in dom(b)$
inv_3: $\boxed{b(a) - v \geq -c}$ ← $\boxed{INV3}$
Solution to Exercise 2 of Lab1
then
act1: $\boxed{b(a) := b(a) - v}$ → $b := b \Leftarrow\!\!+ \{a \mapsto b(a) - v\}$
updates the balance of a
act2: $d := d - v$
updates the cash drawer
end

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



Lab1 Solution: Machine (deposit)

MACHINE Bank0

// Initial model of the bank system

SEES C0

VARIABLES

b balance (ENV2)

d cash drawer (REQ7)

owner account owner (ENV9) - Solution to Exercise 4 of Lab1

INVARIANTS

inv1: $b \in ACCOUNT \rightarrow\!\!\!\!\!+ \mathbb{Z}$

inv2: $d \in \mathbb{Z}$

inv3: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \geq -c$
(ENV3)

inv4: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \leq L$
(ENV3) - Solution to Exercise 3 of Lab1

inv5: $owner \in ACCOUNT \rightarrow\!\!\!\!\!+ PERSON$
(ENV9) - Solution to Exercise 4 of Lab1

inv6: $dom(b) = dom(owner)$

Event deposit ⟨ordinary⟩ $\widehat{=}$

(REQ5) - Solution to Exercise 3 of Lab1

any

a

v

where

grd1: $a \in dom(b)$

grd2: $v \in \mathbb{N}_1$

grd3: $b(a) + v \leq L$

then

act1: $b(a) := b(a) + v$

act2: $d := d + v$

end

Lab1 Solution: Machine (transfer)

MACHINE Bank0

// Initial model of the bank system

SEES C0

VARIABLES

b balance (ENV2)

d cash drawer (REQ7)

owner account owner (ENV9) - Solution to Exerc

INVARIANTS

inv1: $b \in ACCOUNT \rightarrow\!\!\!\!\!\rightarrow \mathbb{Z}$

inv2: $d \in \mathbb{Z}$

inv3: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \geq -c$
(ENV3)

inv4: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \leq L$
(ENV3) - Solution to Exercise 3 of Lab1

inv5: $owner \in ACCOUNT \rightarrow\!\!\!\!\!\rightarrow PERSON$
(ENV9) - Solution to Exercise 4 of Lab1

inv6: $dom(b) = dom(owner)$

Event transfer ⟨ordinary⟩ $\widehat{=}$

(REQ11) - Solution to Exercise 4 of Lab1

any

a1

a2

v

where

grd1: $a1 \in dom(b)$

grd2: $a2 \in dom(b)$

grd3: $a1 \neq a2$

grd4: $b(a1) - v \geq -c$

grd5: $b(a2) + v \leq L$

grd6: $v \in \mathbb{N}_1$

Necessary to make POs related to inv3/inv4 discharged

then

act1: $b := b \lhd\!\!\!- \{a1 \mapsto b(a1) - v, a2 \mapsto b(a2) + v\}$

Note. It's not allowed to have two actions involving the s

:= ...

end

END

withdraw(a1, v)
deposit(a2, v)

$\boxed{b}(a1) := b(a1) - v$
$\boxed{b}(a2) := b(a2) + v$ X

Lab1 Solution: Machine (open/close accounts)

MACHINE Bank0
    // Initial model of the bank system
SEES C0
VARIABLES
    b balance (ENV2)
    d cash drawer (REQ7)
    owner account owner (ENV9) - Solution to Exercise 4
INVARIANTS
    inv1: $b \in ACCOUNT \rightarrow\!\!\!\!\!\rightarrow \mathbb{Z}$
    inv2: $d \in \mathbb{Z}$
    inv3: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \geq -c$
        (ENV3)
    inv4: $\forall a \cdot a \in dom(b) \Rightarrow b(a) \leq L$
        (ENV3) - Solution to Exercise 3 of Lab1
    inv5: $owner \in ACCOUNT \rightarrow\!\!\!\!\!\rightarrow PERSON$
        (ENV9) - Solution to Exercise 4 of Lab1
    inv6: $dom(b) = dom(owner)$

Event open_account ⟨ordinary⟩ $\widehat{=}$
    (REQ4) - Solution to Exercise 4 of Lab1
  any
      p
      a
  where
      grd1: $p \in PERSON$
      grd2: $a \in ACCOUNT$
      grd3: $a \notin dom(owner)$
  then
      act1: $b := b \cup \{a \mapsto 0\}$
        Note. Might need the PP prover
      act2: $owner := owner \cup \{a \mapsto p\}$
  end

Event close_account ⟨ordinary⟩ $\widehat{=}$
    (REQ10) - Solution to Exercise 4 of Lab1
  any
      a
  where
      grd1: $a \in dom(b)$
      grd2: $b(a) = 0$
  then
      act1: $b := \{a\} \lhd\!\!\!\!- b$
      act2: $owner := \{a\} \lhd\!\!\!\!- owner$
  end