Lecture 3

Part A

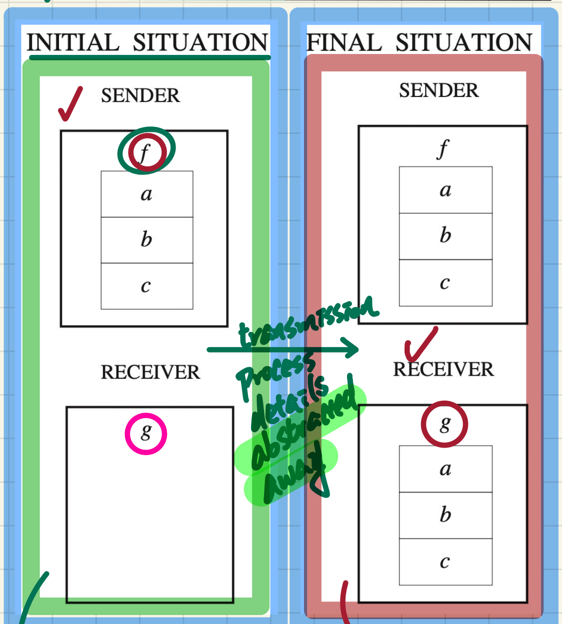
Case Study on Distributed Programs -
File Transfer Protocol
Initial Model: State and Events

FTP: Abstraction and State Space in the Initial Model

REQ1	The protocol ensures the copy of a file from the sender to the receiver.

e.g. $n=3$ $f \in 1..\cancel{n}\,3 \to D$ $d1, d2, d3, \ldots$ $f = \{(1, d2), (2, d1), (3, d3)\}$

Synchronous Transmission



$b = FALSE \Rightarrow g = \emptyset$ $b = TRUE \Rightarrow g = f$

Static Part of Model

carrier sets: membership abstracted away

sets: D $BOOLEAN$

data item

constants: n f

f → file of sender

n → max size of file

axioms:

axm0_1 : $n > 0$

axm0_2 : $f \in 1\,..\,n \to D$ total function

axm0_3 : $BOOLEAN = \{TRUE, FALSE\}$

Dynamic Part of Model

e.g. $n=3$, $g \in 1..\cancel{n}\,3 \to D$ $d1, d2, d3$

variables: g, b

b: whether or not the transmission has been completed

invariants:

inv0_1a : $g \in g \in 1\,..\,n \nrightarrow D$ partial function

inv0_1b : $b \in BOOLEAN$

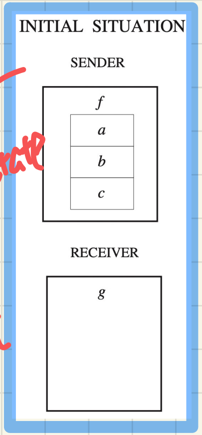
inv0_2 : * ??

inv0_3 : ** ??

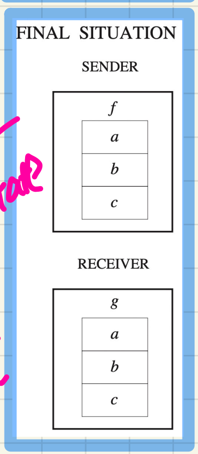
conditional invariants

$g = \{(1, d2), (3, d3)\}$

FTP: Events of Initial Model



post-state of init event



post-state of final event

sets: $D, BOOLEAN$

constants: n, f

axioms:
- **axm0_1** : $n > 0$
- **axm0_2** : $f \in 1 .. n \to D$
- **axm0_3** : $BOOLEAN = \{TRUE, FALSE\}$

variables: g, b

invariants:
- **inv0_1a** : $g \in g \in 1 .. n \nrightarrow D$
- **inv0_1b** : $b \in BOOLEAN$
- **inv0_2** : $b = FALSE \Rightarrow g = \varnothing$
- **inv0_3** : $b = TRUE \Rightarrow g = f$

init:

sender's file ready for transmission

init
  begin
    ??
  end

$g := \varnothing$

$b := FALSE$

enables

final:

sender's file transmitted to receiver

final
  when
    ??
  then
    ??
  end

$b = FALSE$

$g := f$

$b := TRUE$

before transmission can be completed, it must have not been started

PO of Invariant Establishment

sets: $D, BOOLEAN$

constants: n, f

axioms:
- **axm0_1** : $n > 0$
- **axm0_2** : $f \in 1\,..\,n \rightarrow D$
- **axm0_3** : $BOOLEAN = \{TRUE, FALSE\}$

variables: g, b

invariants:
- **inv0_1a** : $g \in 1\,..\,n \mathrel{+\!\!\!\rightarrow} D$
- **inv0_1b** : $b \in BOOLEAN$
- **inv0_2** : $b = FALSE \Rightarrow g = \varnothing$
- **inv0_3** : $b = TRUE \Rightarrow g = f$

init
  begin
    $g := \varnothing$
    $b := FALSE$
  end

BAP: $g' = \varnothing \wedge b' = FALSE$

Rule of Invariant Establishment

$$\frac{A(c) \vdash I_i(c, K(c))}{} \quad \text{INV}$$

<u>Components</u>

K(c): effect of init's actions

v' = K(c): BAP of init's actions

Exercise: Generate Sequents from the INV rule.

init/inv0_1a/INV

$n > 0$

$f \in 1..n \rightarrow D$

$BOOLEAN = \{TRUE, FALSE\}$

$\vdash$

$\underbrace{\boxed{g'}}_{\varnothing} \in 1..n \mathrel{+\!\!\!\rightarrow} D$

init/inv0_2/INV

$n > 0$

$f \in 1..n \rightarrow D$

$BOOLEAN = \{TRUE, FALSE\}$

$\vdash$

$\underbrace{\boxed{b'}}_{FALSE} = FALSE \Rightarrow \underbrace{\boxed{g'}}_{\varnothing} = \varnothing$

Discharging PO of Invariant Establishment

$$
\begin{array}{l}
n > 0 \\
f \in 1 \,..\, n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
\vdash \\
\boxed{\varnothing \in 1 \,..\, n \mathrel{+\!\!\!\!\rightarrow} D}
\end{array}
$$

init/inv0_1a/INV

ARI

$$
\boxed{
\begin{array}{l}
n > 0 \\
f \in 1 \,..\, n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
\vdash T \ \cancel{TRUE}
\end{array}
}
$$

TRUE_R

∅ is always a partial function whose domain & range are ∅

$$
\begin{array}{l}
n > 0 \\
f \in 1 \,..\, n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
\vdash \\
FALSE \in BOOLEAN
\end{array}
$$

init/inv0_1b/INV

$$
\begin{array}{l}
n > 0 \\
f \in 1 \,..\, n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
\vdash \\
FALSE = FALSE \Rightarrow \varnothing = \varnothing
\end{array}
$$

init/inv0_2/INV

MON

$$
\boxed{
\begin{array}{l}
\vdash \\
FALSE = FALSE \Rightarrow \varnothing = \varnothing
\end{array}
}
$$

ARI

$$
\boxed{
\begin{array}{l}
\vdash \\
\quad T
\end{array}
}
$$

TRUE_R

① $FALSE = FALSE \equiv T$

② $\varnothing = \varnothing \equiv T$

③ $T \Rightarrow T \equiv T$

$$
\begin{array}{l}
n > 0 \\
f \in 1 \,..\, n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
\vdash \\
FALSE = TRUE \Rightarrow \varnothing = f
\end{array}
$$

init/inv0_3/INV

PO of Invariant Preservation

sets: $D, BOOLEAN$

constants: n, f

axioms:
- **axm0_1** : $n > 0$
- **axm0_2** : $f \in 1 \,..\, n \rightarrow D$
- **axm0_3** : $BOOLEAN = \{TRUE, FALSE\}$

variables: g, b

invariants:
- ✓ **inv0_1a** : $g \in 1 \,..\, n \mathrel{+\!\!\!\!\rightarrow} D$
- ✓ **inv0_1b** : $b \in BOOLEAN$
- ✓ **inv0_2** : $b = FALSE \Rightarrow g = \varnothing$
- ✓ **inv0_3** : $b = TRUE \Rightarrow g = f$

final
  when
    $\boxed{b = FALSE}$
  then
    $g := f$
    $b := TRUE$
  end

BAP: $g' = f \land b' = FALSE$

Rule of Invariant Preservation

$\boxed{A(c)}$
$\boxed{I(c, v)}$
$\boxed{G(c, v)}$
$\vdash$
$I_i(c, E(c, v))$

Exercise: Generate Sequents from the INV rule.

final/inv0_1a/INV

$n > 0$
$f \in 1 \,..\, n \rightarrow D$
$BOOLEAN = \{TRUE, FALSE\}$
$g \in 1 \,..\, n \mathrel{+\!\!\!\!\rightarrow} D$
$b \in BOOLEAN$
$b = FALSE \Rightarrow g = \varnothing$
$b = TRUE \Rightarrow g = f$
$b = FALSE$
$\vdash$ *

* $\cancel{g}\ f \in 1 \,..\, n \mathrel{+\!\!\!\!\rightarrow} D$

final/inv0_2/INV

$n > 0$
$f \in 1 \,..\, n \rightarrow D$
$BOOLEAN = \{TRUE, FALSE\}$
$g \in 1 \,..\, n \mathrel{+\!\!\!\!\rightarrow} D$
$b \in BOOLEAN$
$b = FALSE \Rightarrow g = \varnothing$
$b = TRUE \Rightarrow g = f$
b FALSE
$\vdash$ **

** $\cancel{b}\ FALSE = TRUE \Rightarrow \cancel{g}\ f = f$

Discharging POs of m0: Invariant Preservation

final/inv0_1a/INV

$$
\begin{array}{l}
n > 0 \\
f \in 1 \,..\, n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
g \in 1 \,..\, n \nrightarrow D \\
b \in BOOLEAN \\
b = FALSE \Rightarrow g = \varnothing \\
b = TRUE \Rightarrow g = f \\
b = FALSE \\
\vdash \\
f \in 1 \,..\, n \nrightarrow D
\end{array}
$$

✓

MON

$$
\boxed{\begin{array}{l} f \in 1..n \rightarrow D \\ \vdash \\ f \in 1..n \nrightarrow D \end{array}}
$$

ARI

① a total fun. is a special case of partial fun.

② But a partial fun is not necessarily a total fun.

final/inv0_1b/INV

$$
\begin{array}{l}
n > 0 \\
f \in 1 \,..\, n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
g \in 1 \,..\, n \nrightarrow D \\
b \in BOOLEAN \\
b = FALSE \Rightarrow g = \varnothing \\
b = TRUE \Rightarrow g = f \\
b = FALSE \\
\vdash \\
TRUE \in BOOLEAN
\end{array}
$$

final/inv0_2/INV

$$
\begin{array}{l}
n > 0 \\
f \in 1 \,..\, n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
g \in 1 \,..\, n \nrightarrow D \\
b \in BOOLEAN \\
b = FALSE \Rightarrow g = \varnothing \\
b = TRUE \Rightarrow g = f \\
b = FALSE \\
\vdash \\
TRUE = FALSE \Rightarrow f = \varnothing
\end{array}
$$

MON

$$
\boxed{\begin{array}{l} \vdash \\ TRUE = FALSE \Rightarrow f = \varnothing \end{array}}
$$

ARI

$$
\boxed{\vdash \top}
$$

TRUE_R

① $TRUE = FALSE \equiv \bot$

② $\bot \Rightarrow P \equiv \top$

final/inv0_3/INV

$$
\begin{array}{l}
n > 0 \\
f \in 1 \,..\, n \rightarrow D \\
BOOLEAN = \{TRUE, FALSE\} \\
g \in 1 \,..\, n \nrightarrow D \\
b \in BOOLEAN \\
b = FALSE \Rightarrow g = \varnothing \\
b = TRUE \Rightarrow g = f \\
b = FALSE \\
\vdash \\
TRUE = TRUE \Rightarrow f = f
\end{array}
$$

Summary of the Initial Model: Provably Correct

sets: $D, BOOLEAN$

constants: n, f

axioms:
- **axm0_1** : $n > 0$
- **axm0_2** : $f \in 1 \,..\, n \rightarrow D$
- **axm0_3** : $BOOLEAN = \{TRUE, FALSE\}$

variables: g, b

invariants:
- **inv0_1a** : $g \in 1 \,..\, n \twoheadrightarrow D$
- **inv0_1b** : $b \in BOOLEAN$
- **inv0_2** : $b = FALSE \Rightarrow g = \varnothing$
- **inv0_3** : $b = TRUE \Rightarrow g = f$

init
  begin
    $g := \varnothing$
    $b := FALSE$
  end

final
  when
    $b = FALSE$
  then
    $g := f$
    $b := TRUE$
  end

Correctness Criteria:
- + Invariant Establishment
- + Invariant Preservation
- + Deadlock Freedom