Lecture

Distributed System: File Transfer Protocol

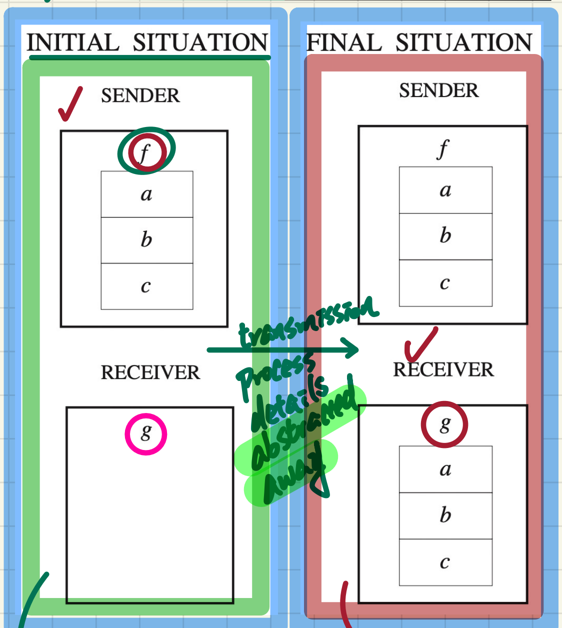
Initial Model: State and Events

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

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** : $f \in 1 \,..\, n \rightarrow D$ total function
- **axm0_3** : $BOOLEAN = \{TRUE, FALSE\}$

Dynamic Part of Model

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

variables: g, b

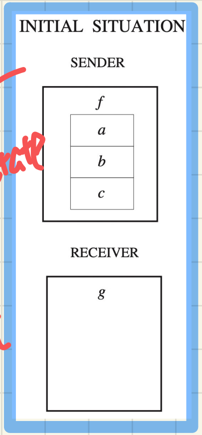
b: whether or not the transmission has been completed

invariants:
- **inv0_1a** : $g \in g \in 1 \,..\, n \nrightarrow D$ partial function
- **inv0_1b** : $b \in BOOLEAN$
- **inv0_2** : * ??
- **inv0_3** : ** ??

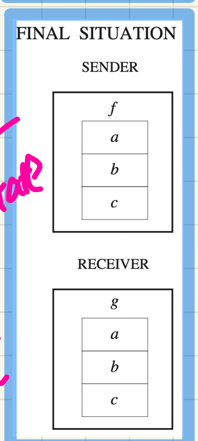
conditional invariants

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

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** : $g \in 1\,..\,n \nrightarrow D$
- **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: $g' = \varnothing \land b' = FALSE$

Rule of Invariant Establishment

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

Components

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

$n > 0$

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

$BOOLEAN = \{TRUE, FALSE\}$

$\vdash$

$\boxed{g'} \in 1..n \nrightarrow D$

$\varnothing$

init/inv0_2/INV

$n > 0$

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

$BOOLEAN = \{TRUE, FALSE\}$

$\vdash$

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

FALSE $\qquad$ $\varnothing$

Discharging PO of Invariant Establishment

Art

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

init/inv0_1a/INV

ARI

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

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

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

ARI

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

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

variables: g, b

axioms:
- $axm0\_1 : n > 0$
- $axm0\_2 : f \in 1\,..\,n \rightarrow D$
- $axm0\_3 : BOOLEAN = \{TRUE, FALSE\}$

invariants:
- ✓ $inv0\_1a : g \in 1\,..\,n \nrightarrow D$
- ✓ $inv0\_1b : b \in BOOLEAN$
- ✓ $inv0\_2 : b = FALSE \Rightarrow g = \varnothing$
- ✓ $inv0\_3 : b = TRUE \Rightarrow g = f$

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

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

Rule of Invariant Preservation

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

Exercise: Generate Sequents from the INV rule.

final/inv0_1a/INV

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

* $\cancel{g} \in 1..n \nrightarrow D$
f

final/inv0_2/INV

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

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

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

① $TRUE = FALSE \equiv \bot$

② $\bot \Rightarrow P \equiv \top$

$$
\boxed{\begin{array}{l} \vdash \\ \top \end{array}}
$$

TRUE_R

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** : $g \in 1 \,..\, n \nrightarrow D$
- **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

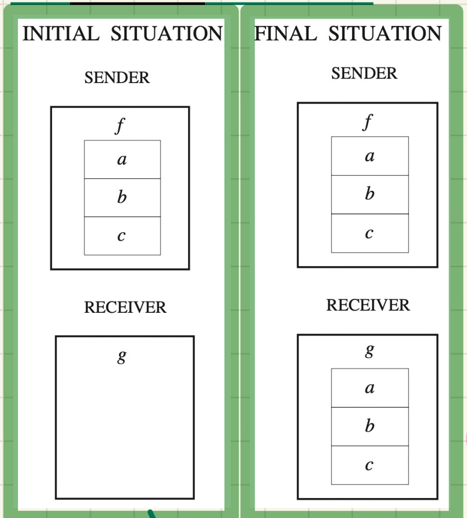
Lecture

Distributed System: File Transfer Protocol

1st Refinement: State, Events, Proofs

FTP: Abstraction in the 1st Refinement

m0: most abstract

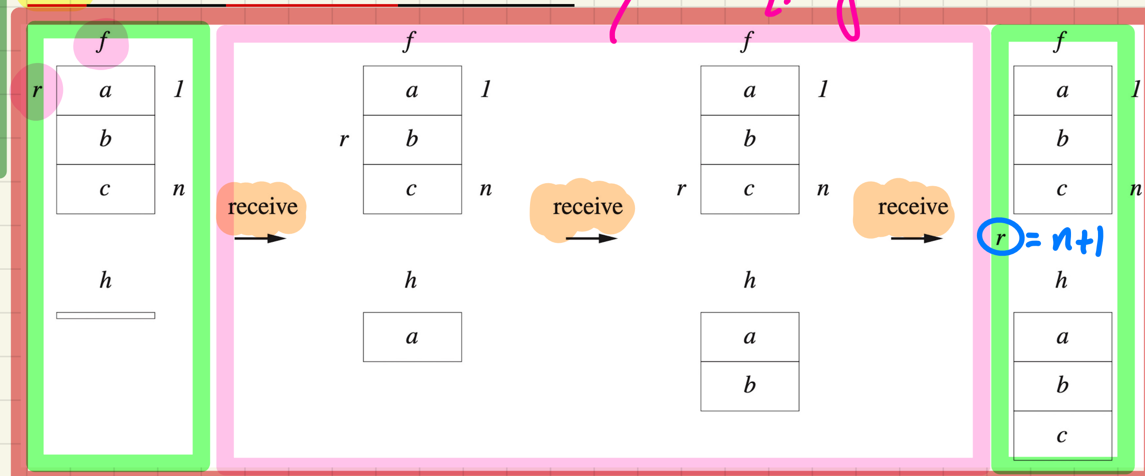


synchronous & instantaneous

REQ2	The file is supposed to be made of a sequence of items.
REQ3	The file is sent piece by piece between the two sites.

refinement:
1. asynchronous
2. gradual

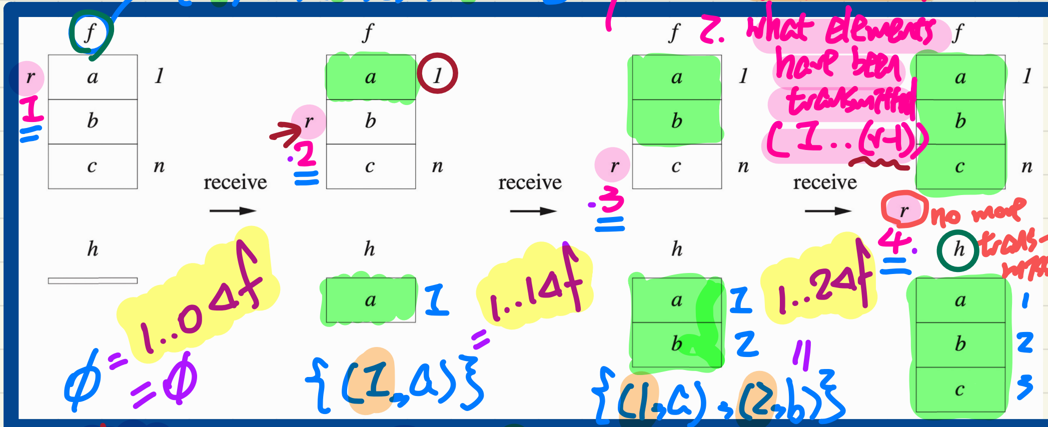
m1: more concrete than m0



FTP: State Space of the 1st Refinement

r value indicates:
1. which element to be transmitted
2. what elements have been transmitted $(1..(r-1))$

$\{(1,a),(2,b),(3,c)\}$



Static Part of Model

sets: $D, BOOLEAN$

constants: n, f

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

Dynamic Part of Model

variables: b, h, r

invariants:
- **inv1_1** : $r \in 1..n+1$
- **inv1_2** : ?? *
- **inv1_3** : ?? **
- **thm1_1** : ?? ***

to be proved for establishment & preservation

1. need not be proved for establishment & preservation
2. to be proved as derivable from invariants

$* \; h = (1..(r-1)) \lhd f$

$\{1, 2, \ldots, r-1\}$

$1..0 = \phi$

$** \; b = TRUE \Rightarrow r = n+1$

$*** \; b = TRUE \Rightarrow h = f$

$\{(1,a),(2,b),(3,c)\}$

$= \underline{1..4} \lhd f$

dom(f)

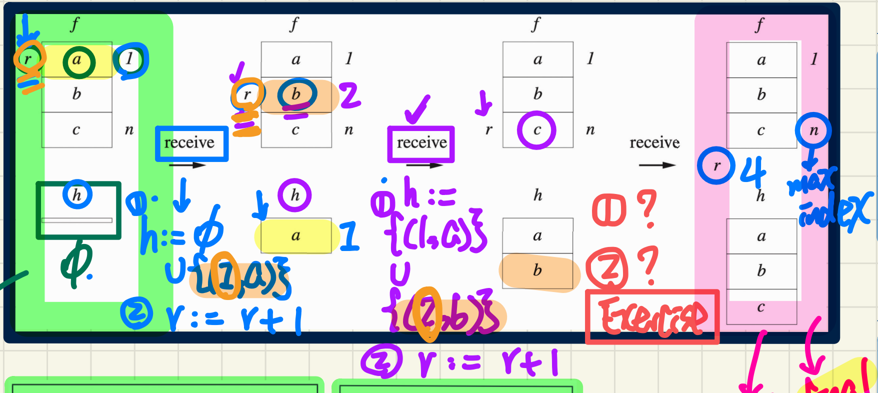
Exercises

inv1_2: elements up to index **r - 1** have been transmitted

inv1_3: transmission completed means no more elements to be transmitted

thm1_1: transmission completed means receiver has a copy of sender's file

FTP: Concrete Events in 2nd Refinement



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: b, h, r

invariants:
- inv1_1 : $r \in 1 \,..\, n+1$
- inv1_2 : $h = (1 \,..\, r-1) \lhd f$
- inv1_3 : $b = TRUE \Rightarrow r = n+1$
- thm1_1 : $b = TRUE \Rightarrow h = f$

as soon as "receive" becomes disabled → "final" should be ready to occur.

init: getting the transmission ready

```
init
  begin
    ??
  end
```

$b := FALSE$
$h := \emptyset$
$r := 1$

receive: transmitting element by element

```
receive
  when
    ??
  then
    ??
  end
```

$r \leq n$

$h := h \cup \{(r, f(r))\}$

occurrence of final is returned to 1

final: finalizing the transmission

sender's private info should be hidden

```
final
  when
    ??
  then
    ??
  end
```

$\boxed{b = FALSE}$
$r = n+1$

$b := TRUE$