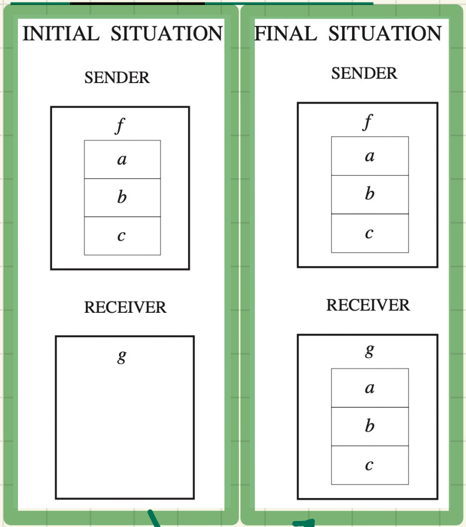
Lecture 3

Part B

Case Study on Distributed Programs - File Transfer Protocol 1st Refinement: State, Events, Proofs

FTP: Abstraction in the 1st Refinement

m0: most abstract

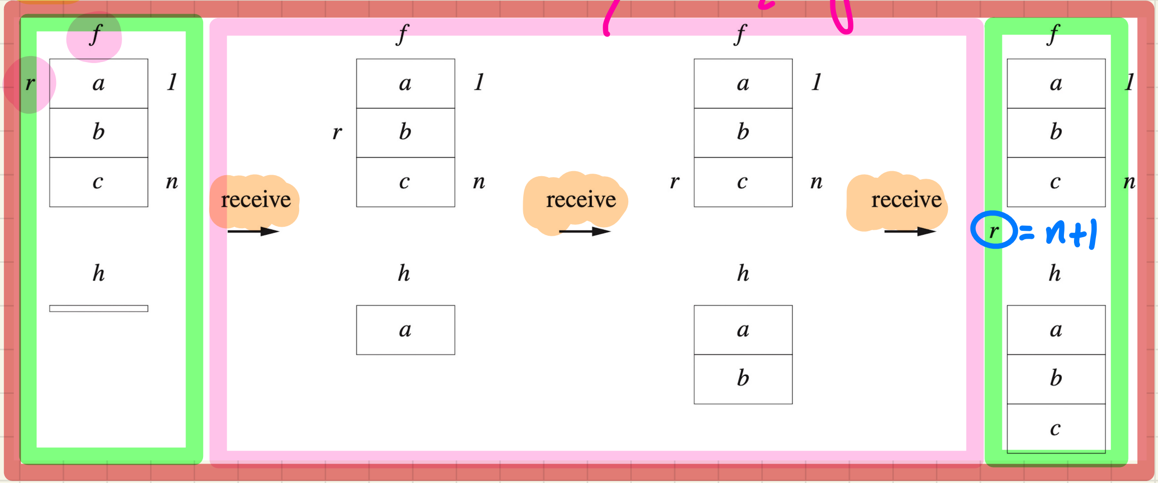


synchronous & instantaneous

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.

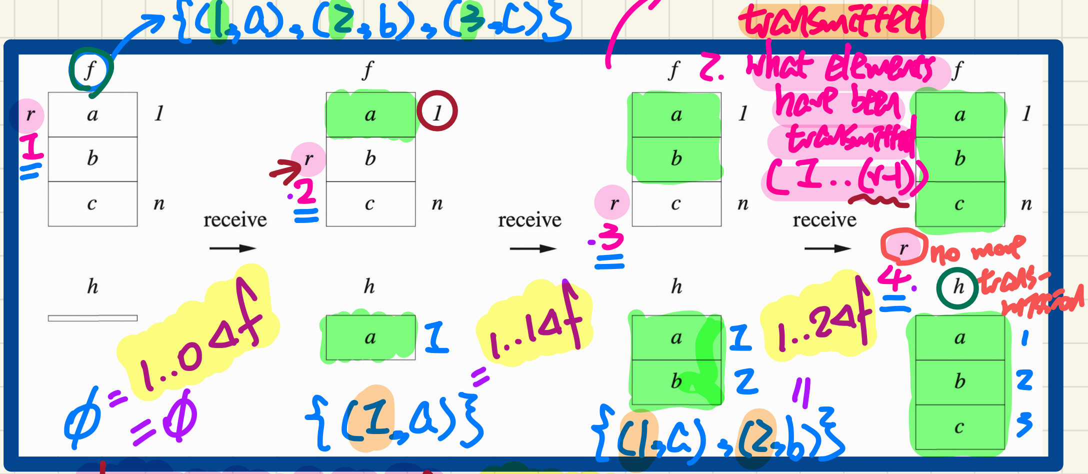
refinement:
1. asynchronous
2. gradual

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 $(1..(r-1))$



Static Part of Model

sets: $D, BOOLEAN$

constants: n, f

axioms:
- axm0_1 : $n > 0$
- axm0_2 : $f \in 1..n \rightarrow D$
- 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

* $h = (\underbrace{1..(r-1)}_{\{1, 2, \ldots, r-1\}}) \lhd f$

$1..0 = \emptyset$

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

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

$\{(1,a),(2,b),(3,c)\} = \underbrace{1..4}_{dom(f)} \lhd f$

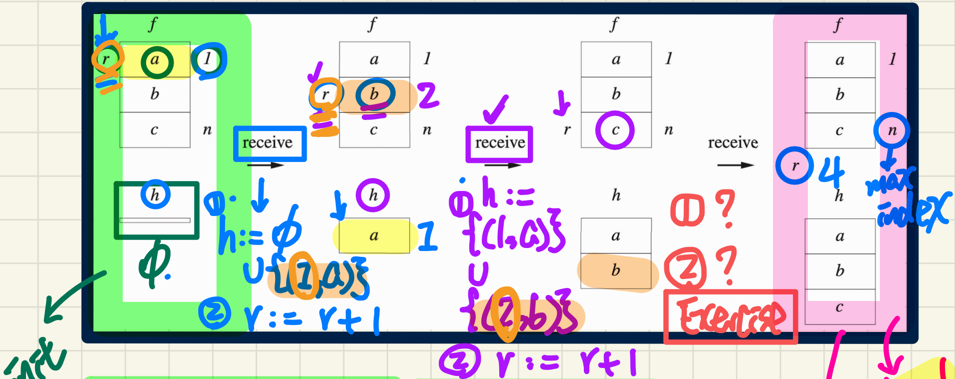
Exercises

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 : $f \in 1 \,..\, n \to D$
- 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 final

"receive" becomes disabled, "final" should be ready to occur.

init: getting the transmission ready

```
init
  begin
    ??
  end
```

$b := FALSE$

$h := \varnothing$

$r := 1$

receive: transmitting element by element

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

$r \leq n$

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

sender's private info should be hidden

occurrence of final is restricted to 1

final: finalizing the transmission

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

$\boxed{b = FALSE}$

$r = n + 1$

$b := TRUE$