

4. File Transfer Protocol

Jean-Raymond Abrial

2009

- To introduce another example: **the file transfer protocol**
- To present a number of **additional mathematical conventions**
- To slightly enlarge the usage of the **Proof Obligation Rules**
- Example studied in many places, in particular in the following book
- L. Lamport *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers* Addison-Wesley 1999

- A file is to be transferred from a **Sender** to a **Receiver**
- On the Sender's side the file is called f
- On the Receiver's side the file is called g
- At the beginning of the protocol, g is supposed to be empty
- At the end of the protocol, g should be equal to f

The protocol ensures the copy of a file from one site to another one

FUN-1

The file is supposed to be made of a sequence of items

FUN-2

The file is send piece by piece between the two sites

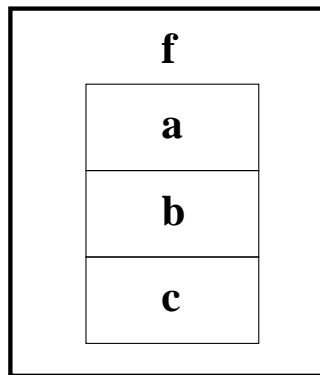
FUN-3

- Our approach at modeling is one of an **external observer**
- The observer “sees” the state space first **from very far away**
- He then approaches the future system and sees **more details**
- As he approaches he also sees **more things happening**

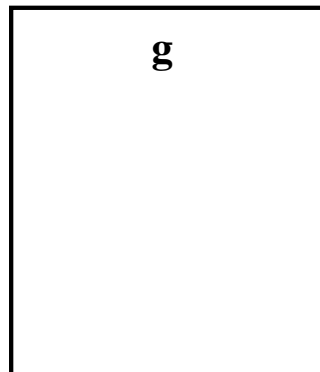
- **Initial model**: The file is transmitted in one shot (FUN1 and FUN2)
- **First refinement**: The file is transmitted gradually (FUN3)
- **Second refinement**: The two agents are separated
- **Third refinement**: Towards an implementation

INITIAL SITUATION

SENDER

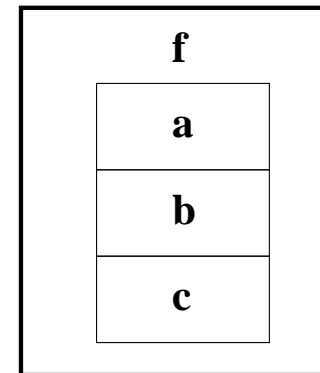


RECEIVER

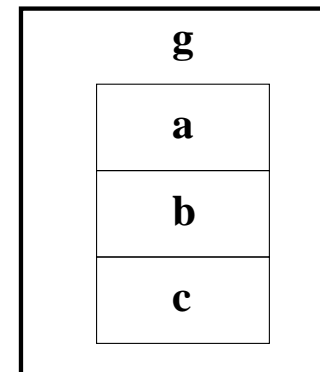


FINAL SITUATION

SENDER



RECEIVER



	f
1	a
	b
n	c

carrier sets: D

constants: n, f

axm0_1: $n \in \mathbb{N}$

axm0_2: $0 < n$

axm0_3: $f \in 1..n \rightarrow D$

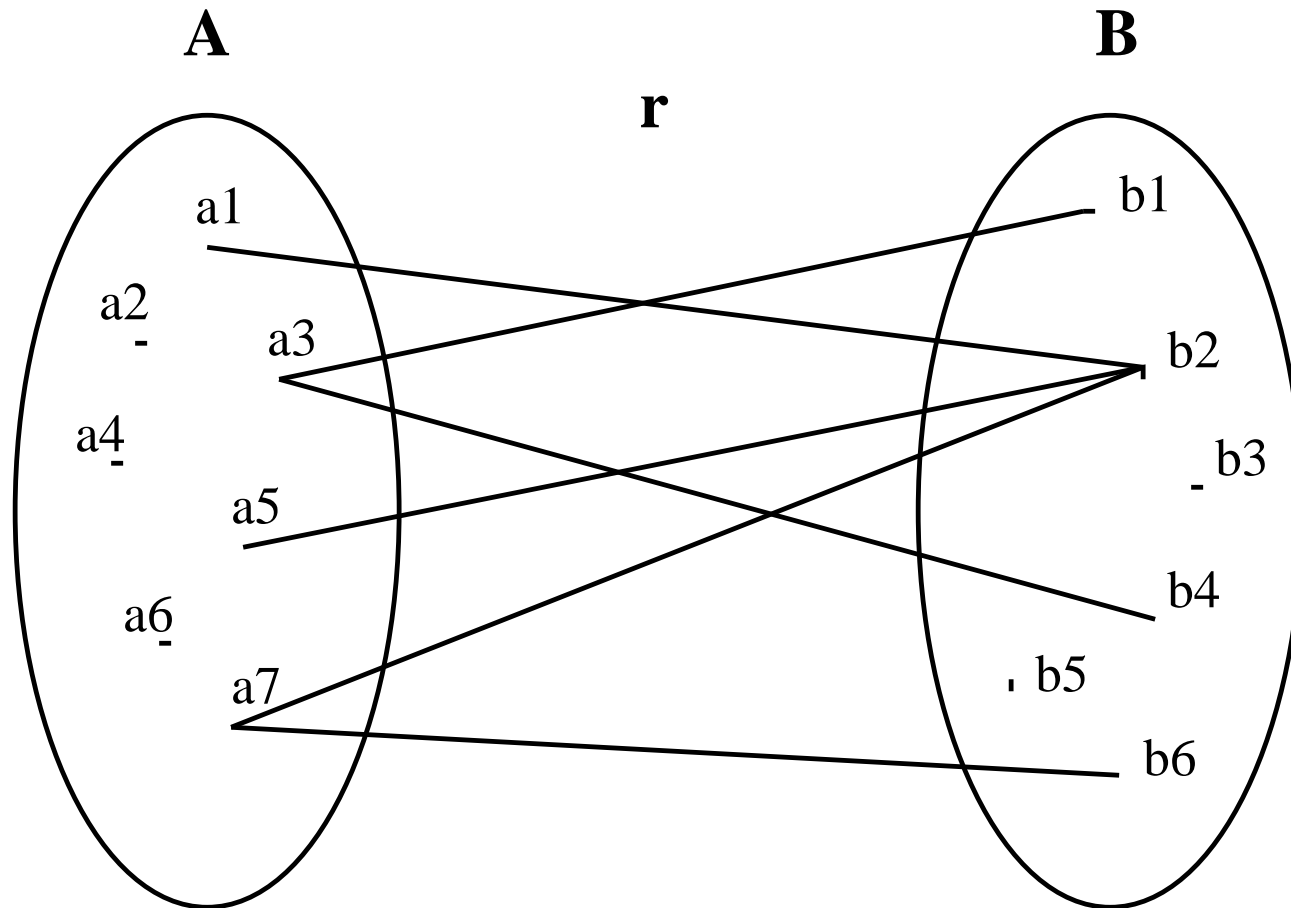
variables: g

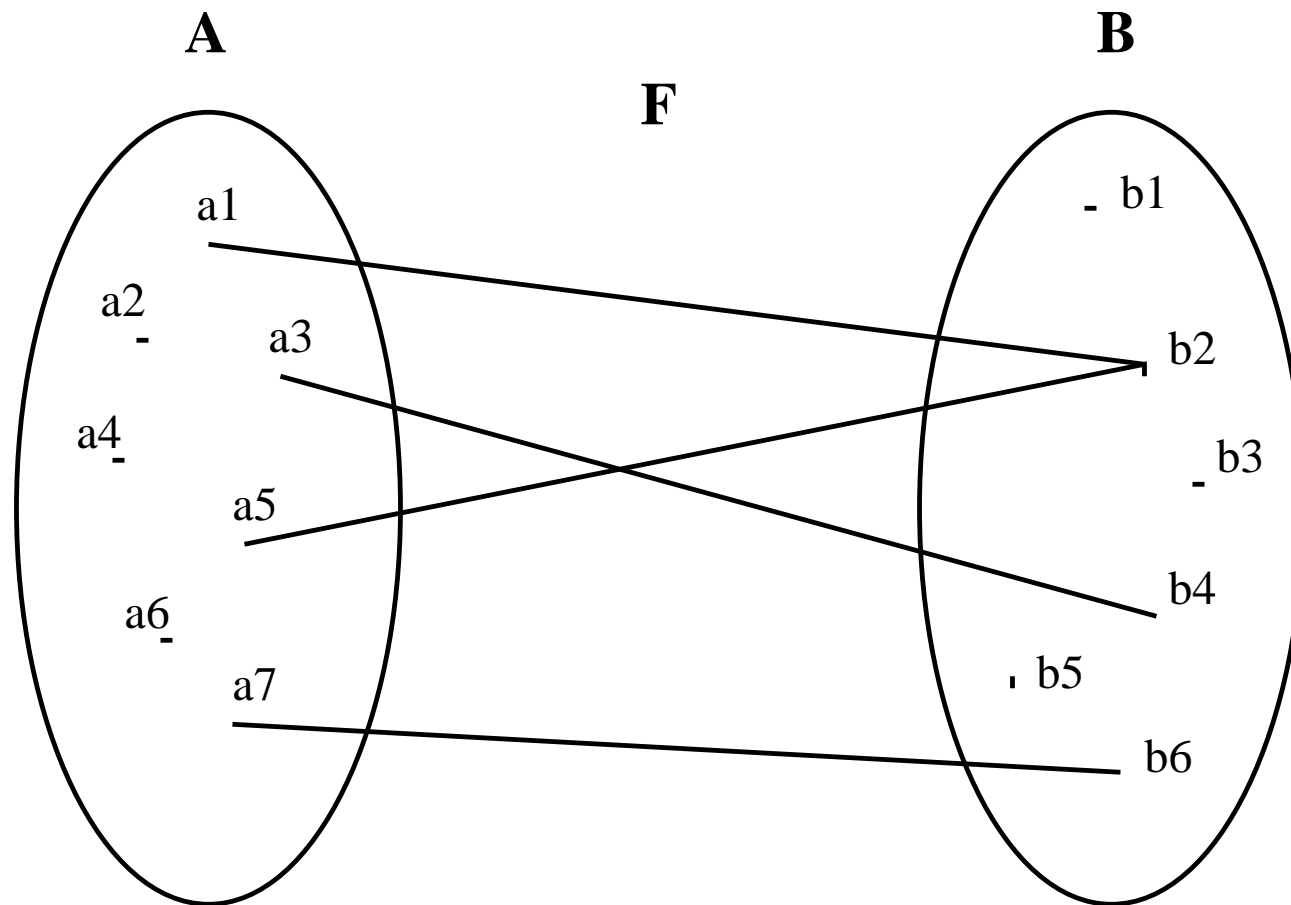
inv0_1: $g \in \mathbb{N} \leftrightarrow D$

- The **carrier set D** makes this development **generic**

$x \in S$	set membership operator
\mathbb{N}	set of natural numbers: $\{0, 1, 2, 3, \dots\}$
$a .. b$	interval from a to b : $\{a, a + 1, \dots, b\}$ (empty when $b < a$)
$a \mapsto b$	pair constructing operator
$S \times T$	Cartesian product operator
$S \subseteq T$	set inclusion operator
$\mathbb{P}(S)$	power set operator

$S \leftrightarrow T$	set of binary relations from S to T
$S \rightarrow T$	set of total functions from S to T
$S \twoheadrightarrow T$	set of partial functions from S to T
$\text{dom}(r)$	domain of a relation r
$\text{ran}(r)$	range of a relation r

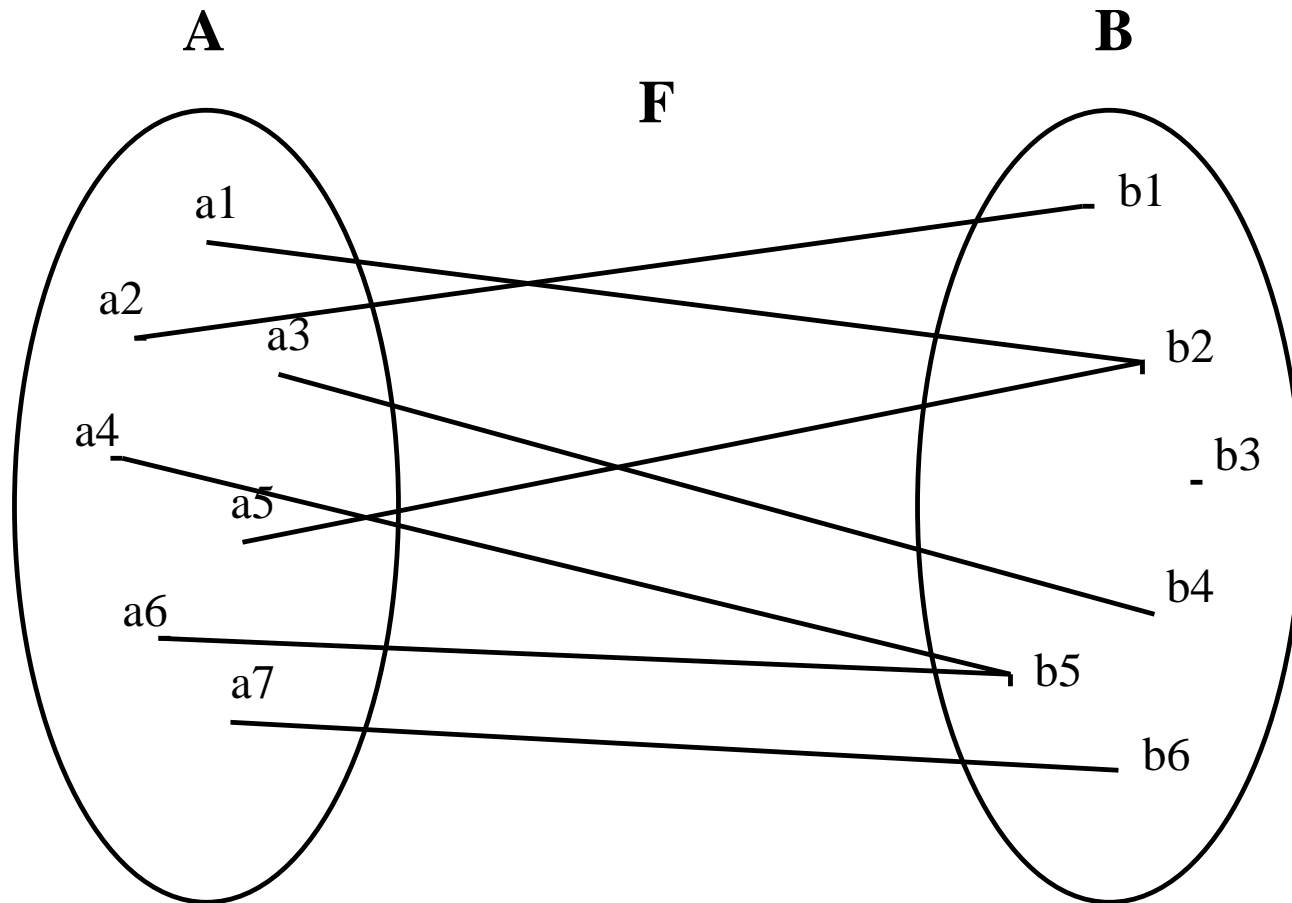




$$F = \{a1 \mapsto b2, a3 \mapsto b4, a5 \mapsto b2, a7 \mapsto b6\}$$

$$\text{dom}(F) = \{a1, a3, a5, a7\}$$

$$\text{ran}(F) = \{b2, b4, b6\}$$



$$\text{dom}(F) = A$$

init

$g : \in \mathbb{N} \leftrightarrow D$

final

when

$g = f$

then

skip

end

- An **anticipated** event will be updated later and **made convergent**

progress

status

anticipated

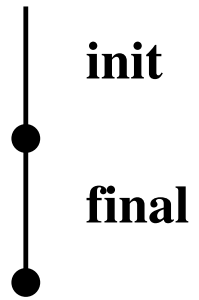
then

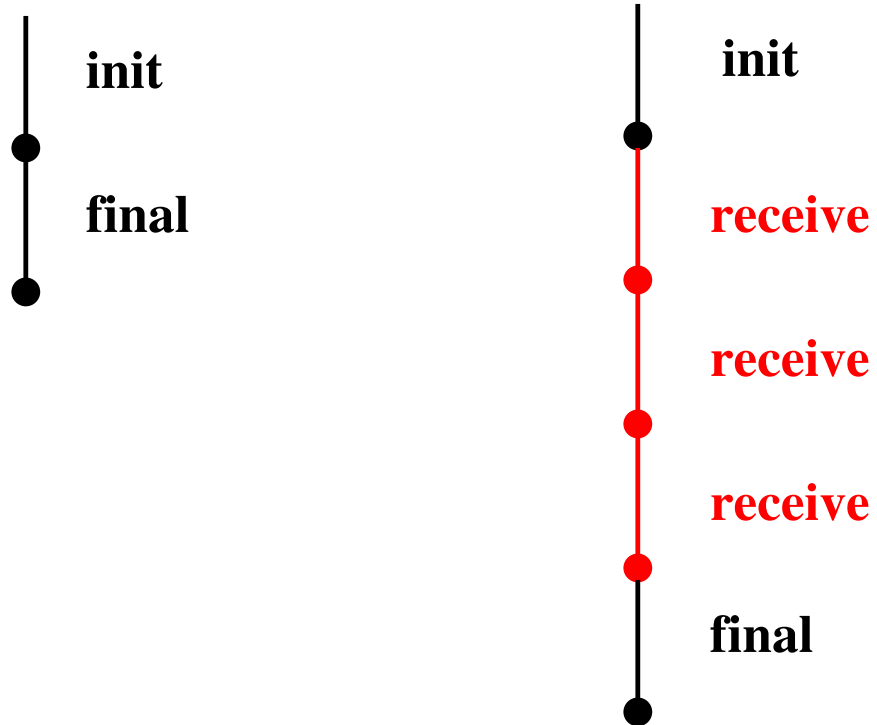
$g : \in \mathbb{N} \leftrightarrow D$

end

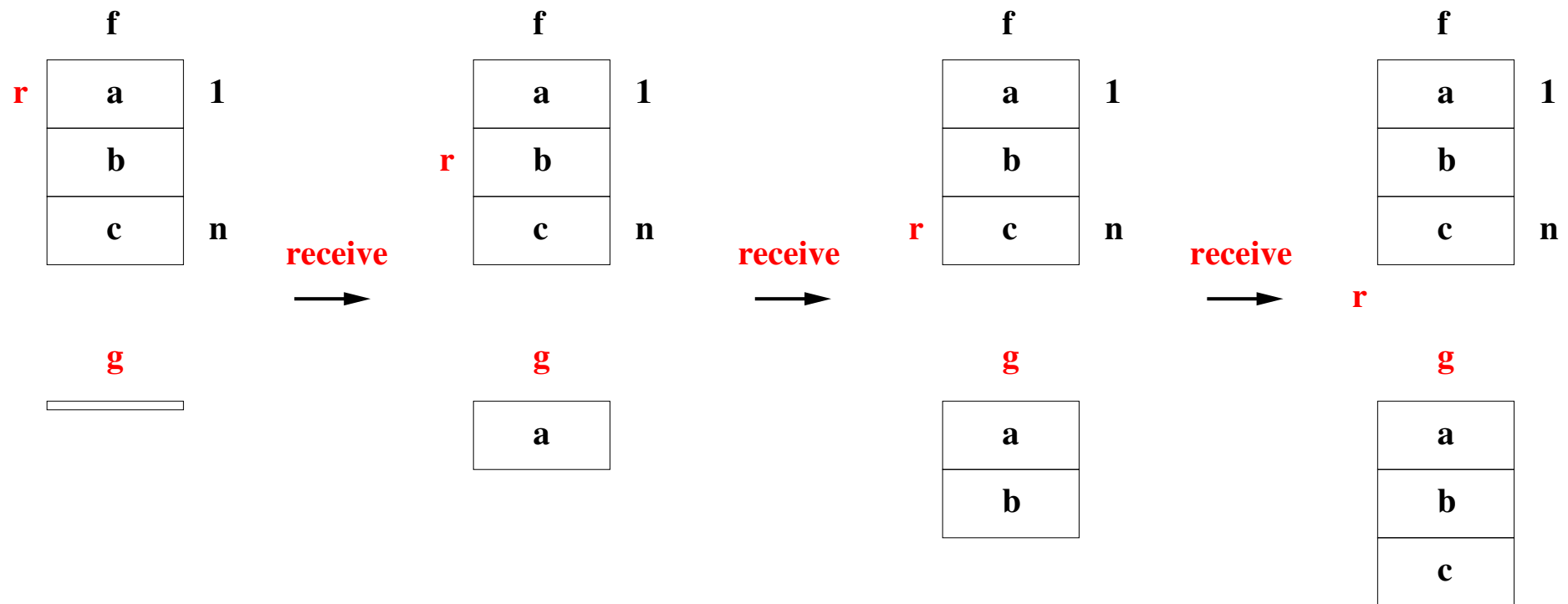
- **Initial model:** The file is transmitted in one shot (FUN1 and FUN2)
- **First refinement:** The file is transmitted gradually (FUN3)
- **Second refinement:** The two agents are separated
- **Third refinement:** Towards an implementation

- The observer **comes closer** to the future system
- So far he was just seeing **the beginning** and **the end**
- Now the observer will see **some intermediate moves**
- He sees the file being **gradually transfered** from Sender to Receiver
- But he still has a **partial view**





A new event is introduced: **receive**



- The new variable r lies within the interval $1 .. n + 1$
- The variable g is equal to f restricted to its $r - 1$ first values

- Introducing additional variable r

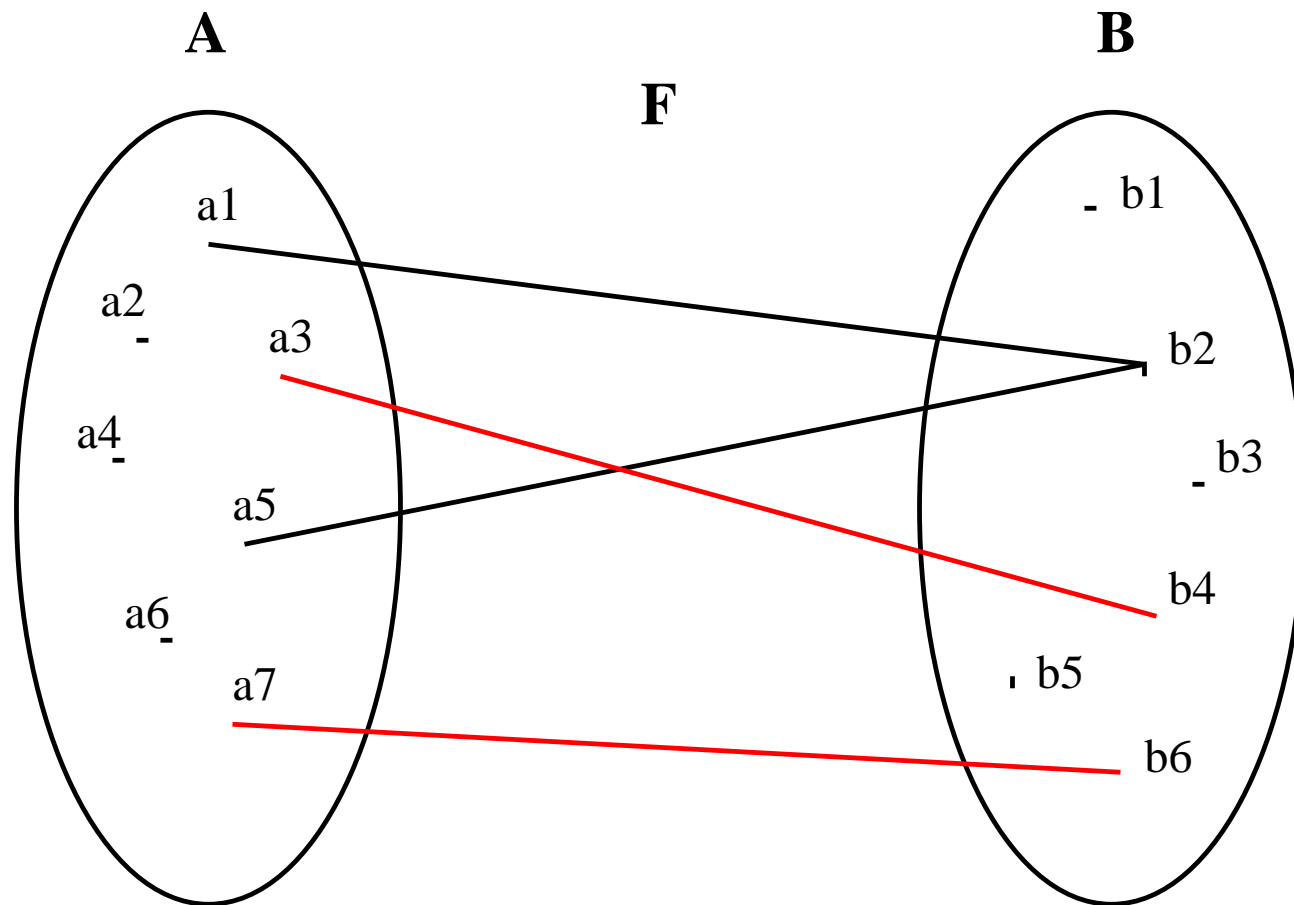
variables: g, r

inv1_1: $r \in 1 .. n + 1$

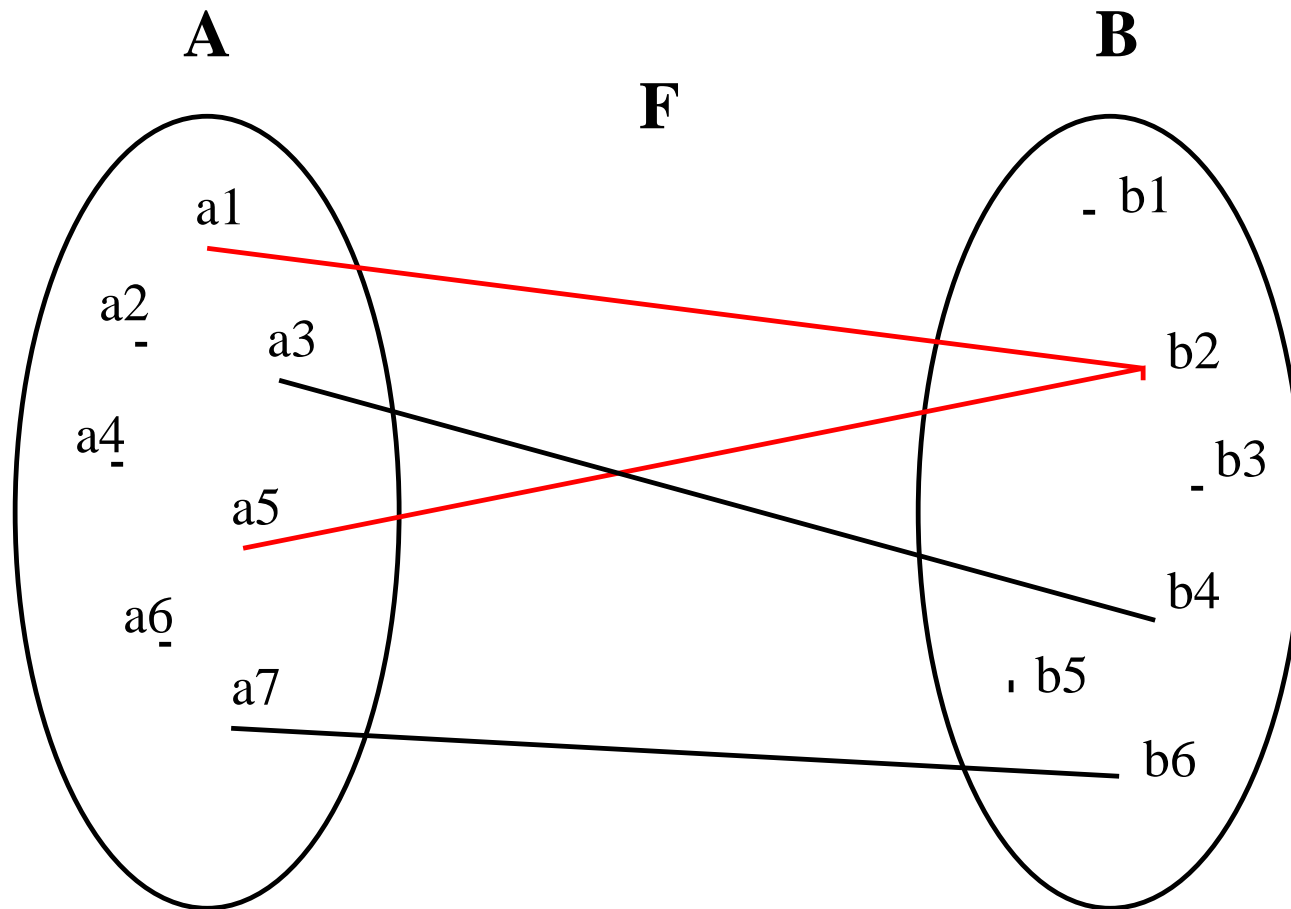
inv1_2: $g = (1 .. r - 1) \triangleleft f$

- g is defined to be the **domain restriction of f to $1 .. r - 1$**

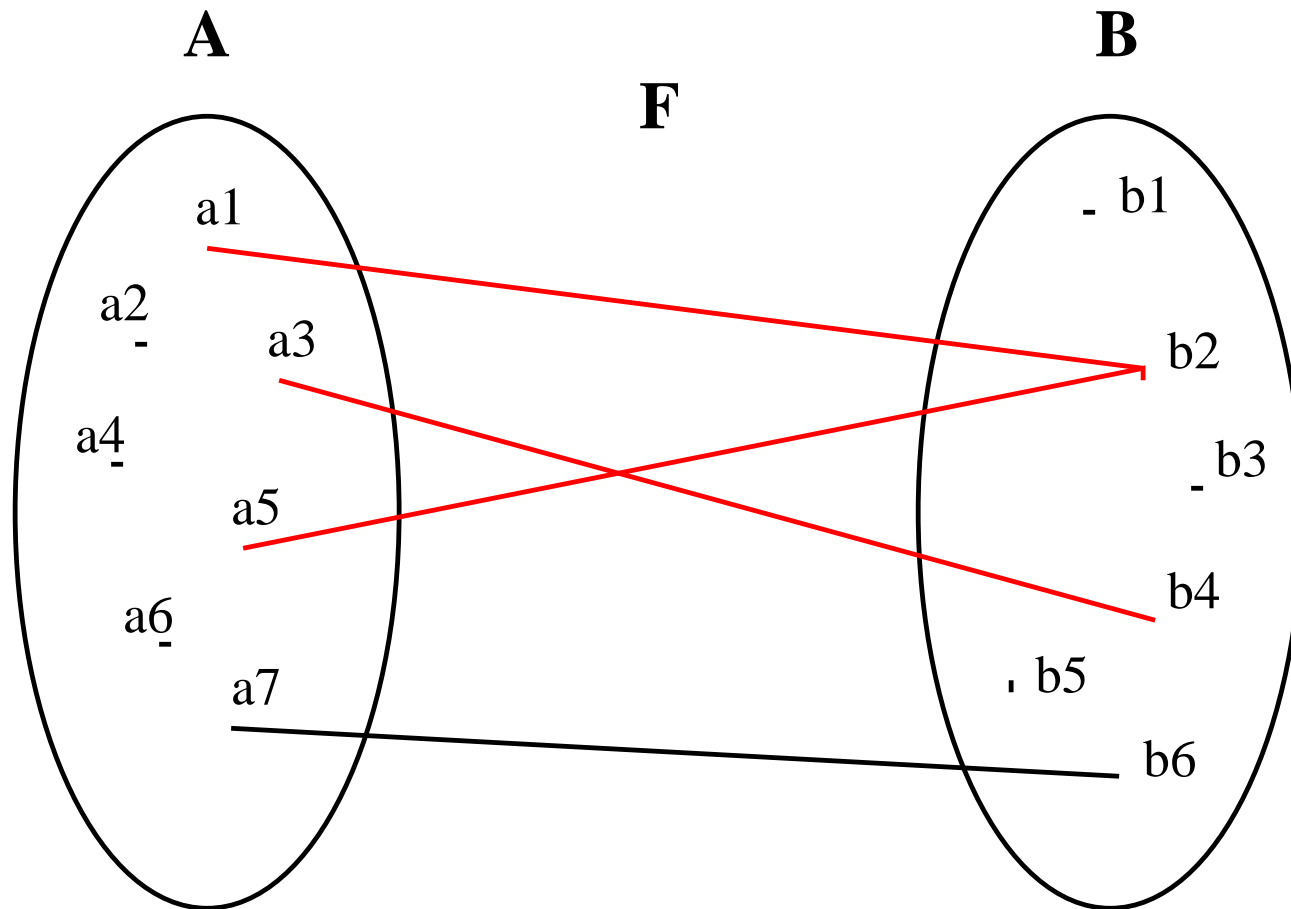
$s \triangleleft r$	domain restriction operator
$s \triangleleft r$	domain subtraction operator
$r \triangleright t$	range restriction operator
$r \triangleright t$	range subtraction operator



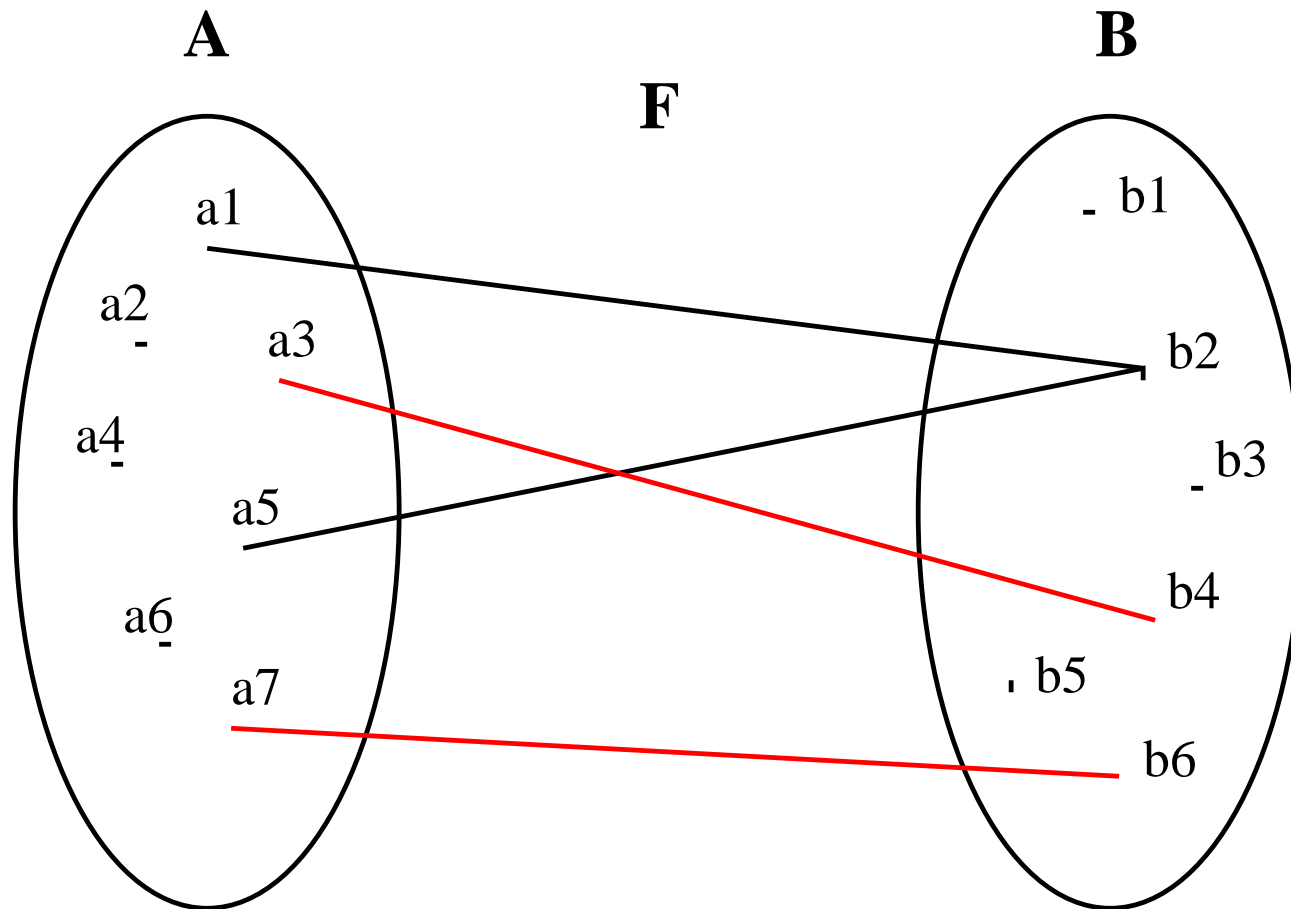
$$\{a_3, a_7\} \triangleleft F$$



$$\{a_3, a_7\} \triangleleft F$$



$$F \triangleright \{b2, b4\}$$



$$F \triangleright \{b_2\}$$

```

init
   $g := \emptyset$ 
   $r := 1$ 
  
```

```

receive
  refines
    progress
  refines
    convergent
  when
     $r \leq n$ 
  then
     $h := h \cup \{r \mapsto f(r)\}$ 
     $r := r + 1$ 
  end
  
```

```

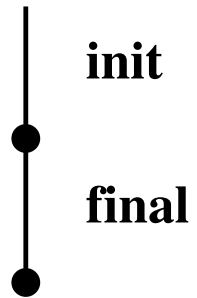
final
  when
     $r = n + 1$ 
  then
    skip
  end
  
```

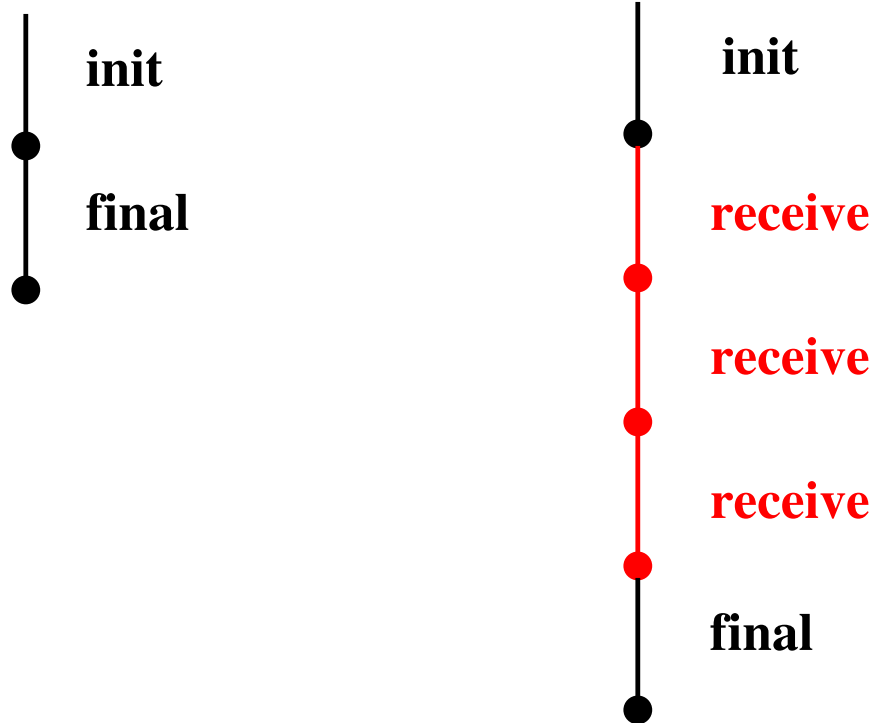
- The variant is **decreased** by the convergent event

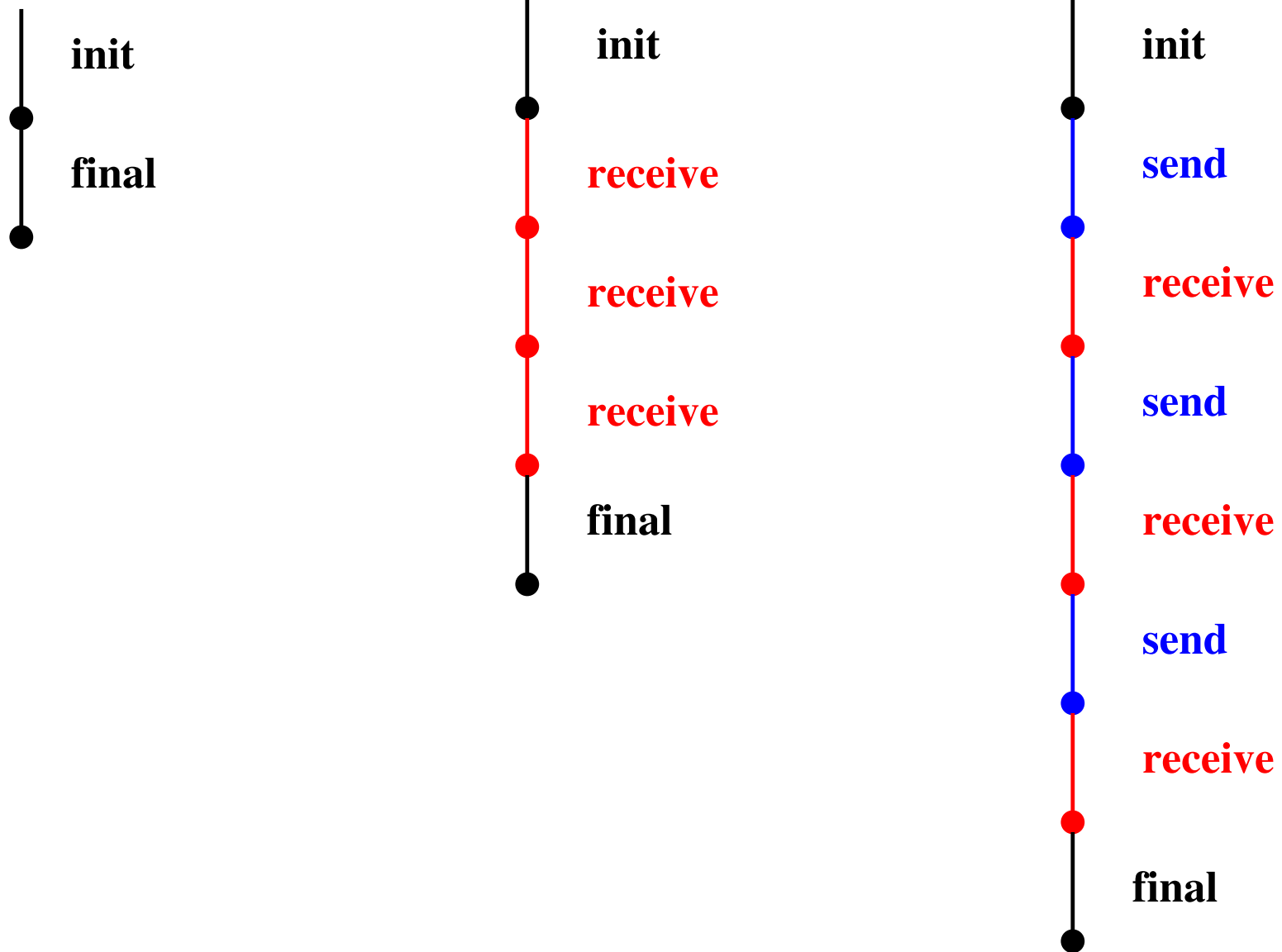
```

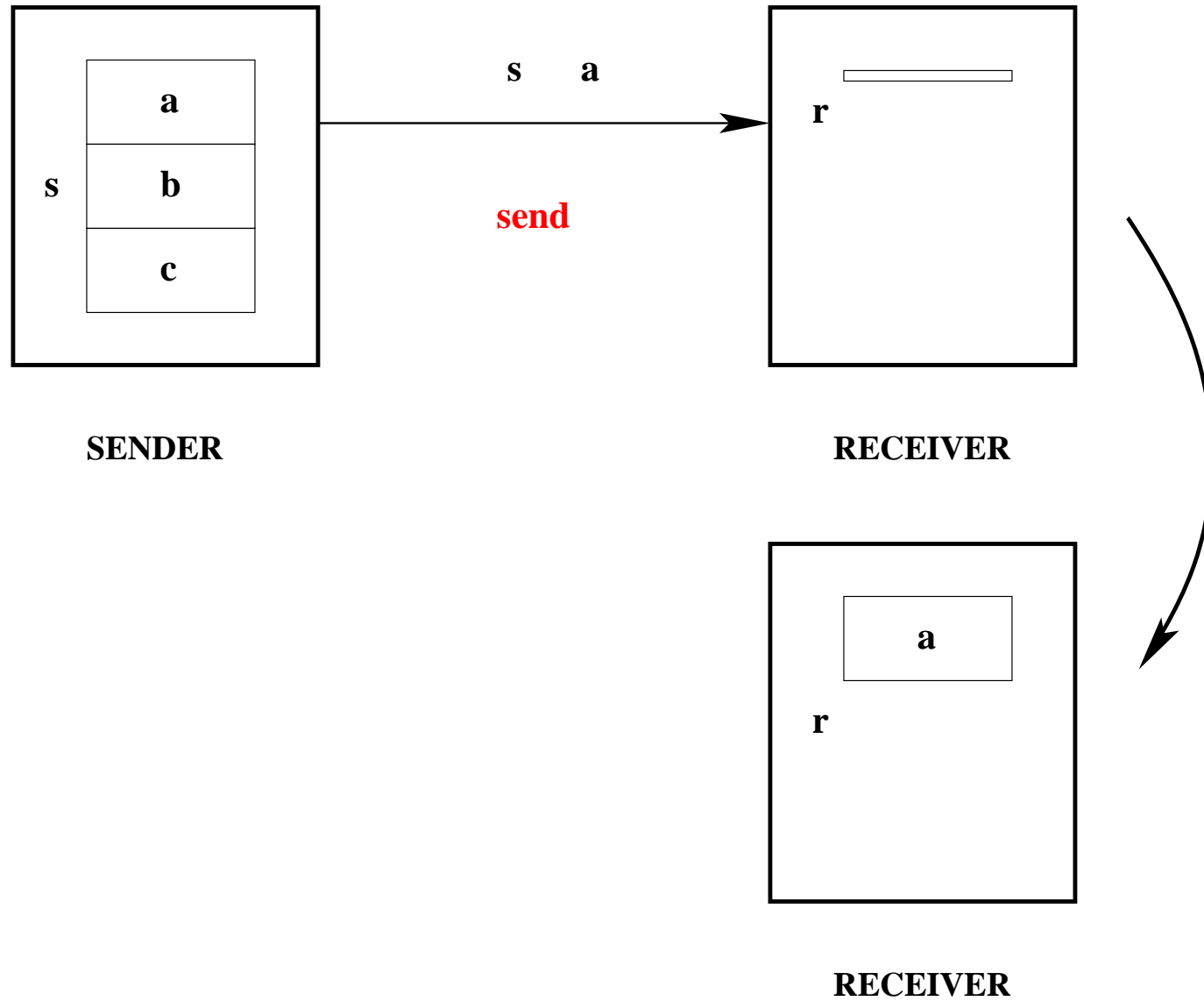
variant1:  $n + 1 - r$ 
  
```

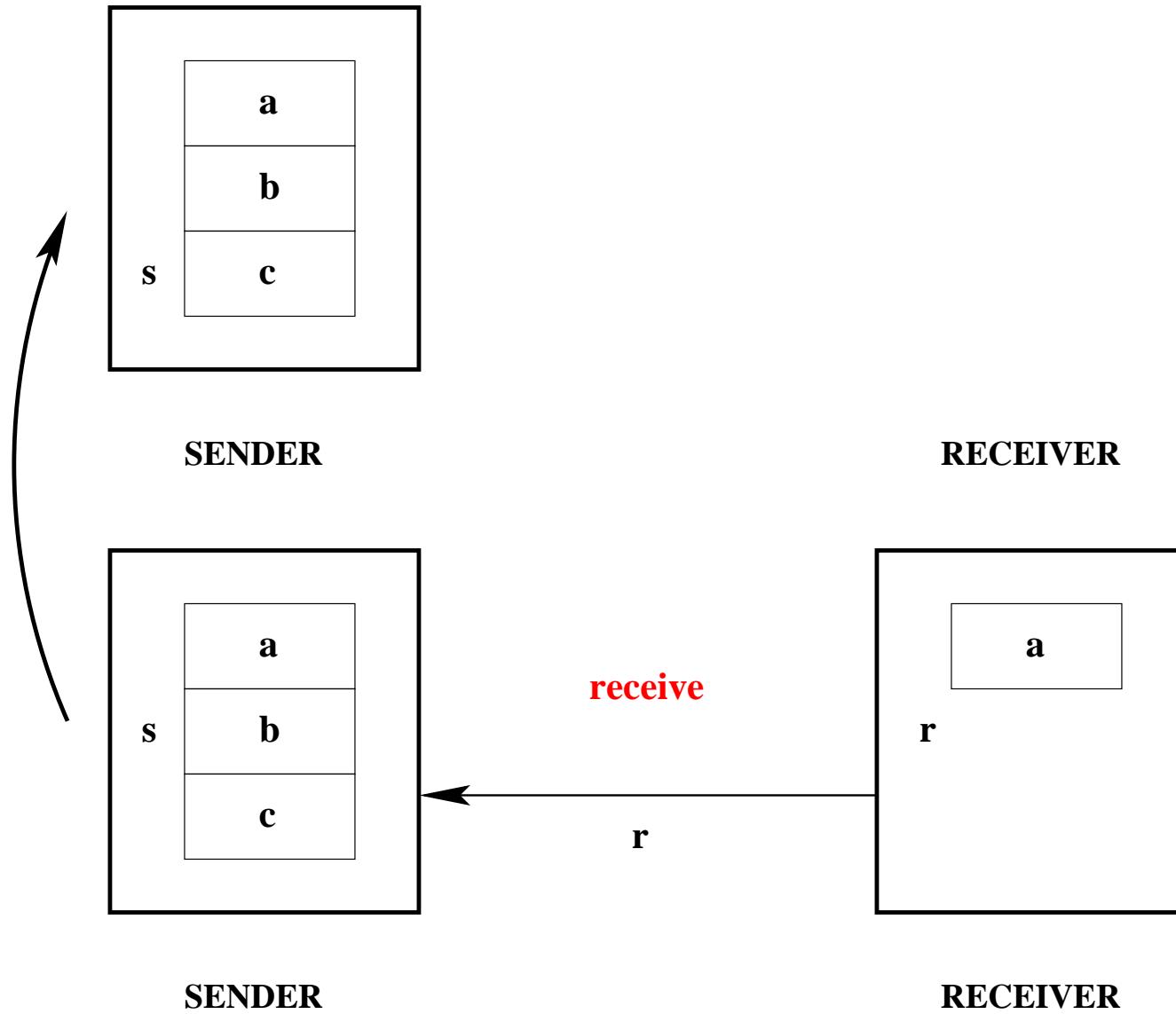
- **Initial model:** The file is transmitted in one shot (FUN1 and FUN2)
- **First refinement:** The file is transmitted gradually (FUN3)
- **Second refinement:** The two agents are separated
- **Third refinement:** Towards an implementation

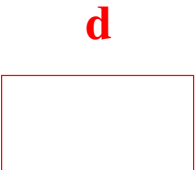
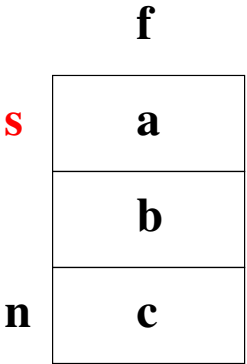


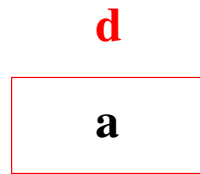
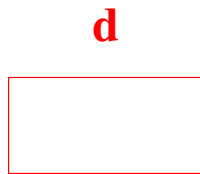
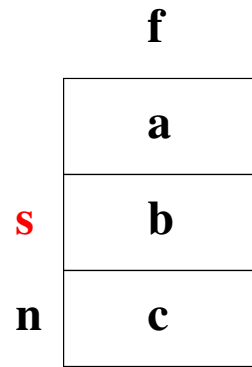
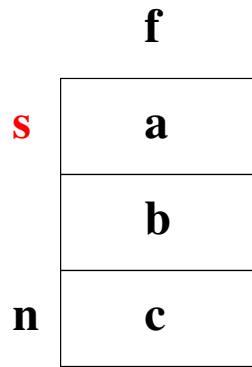


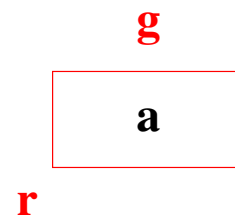
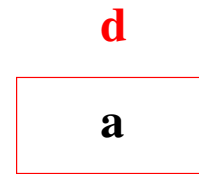
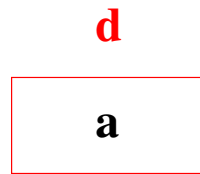
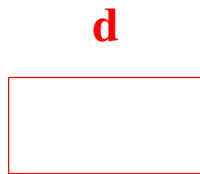
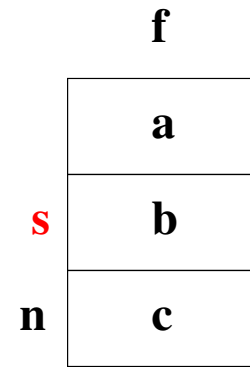
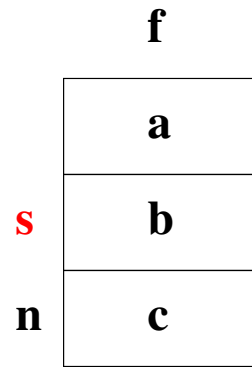
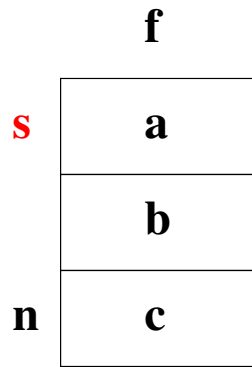


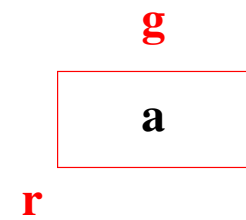
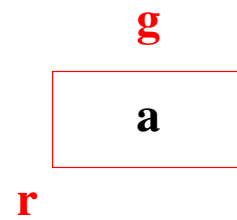
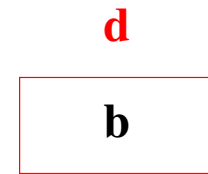
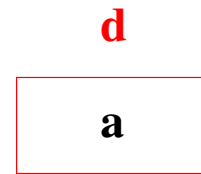
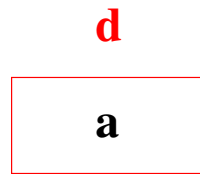
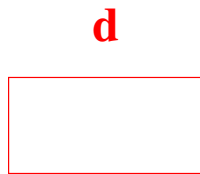
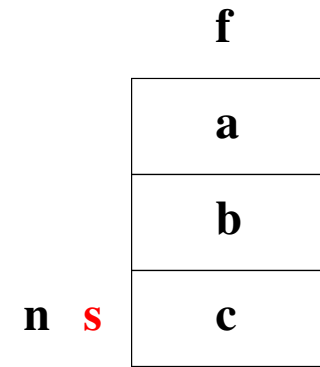
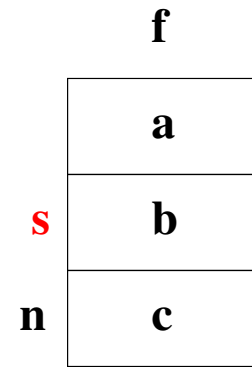
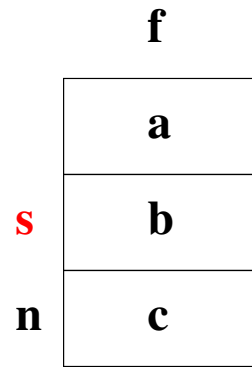
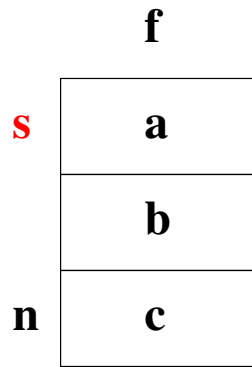


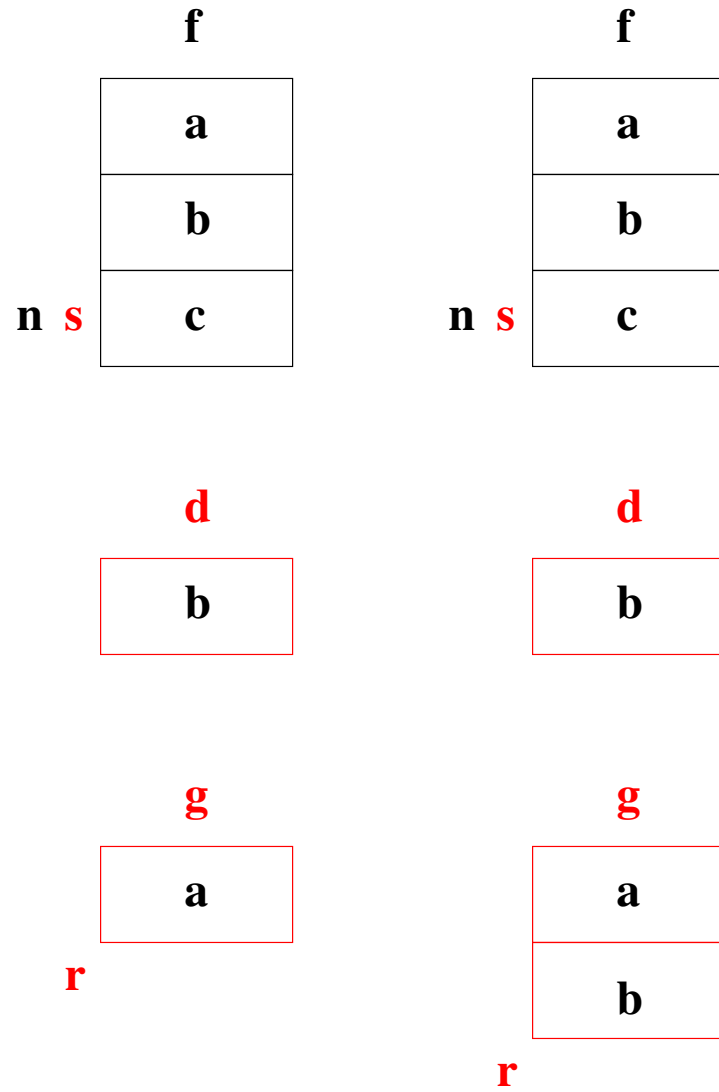


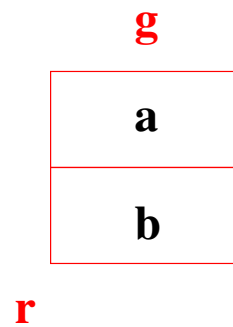
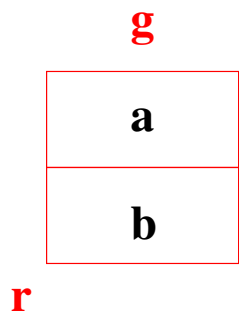
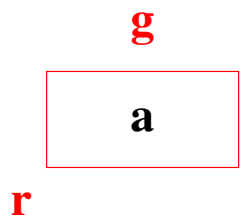
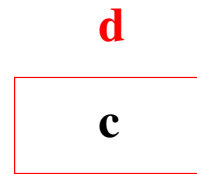
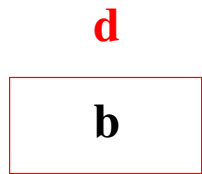
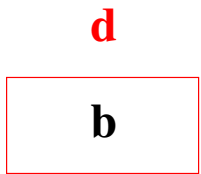
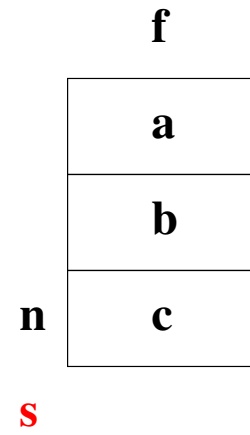
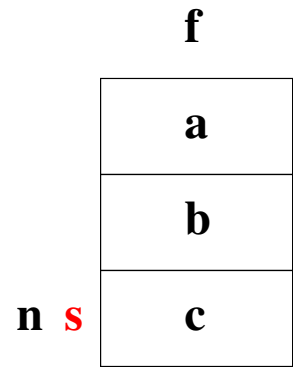
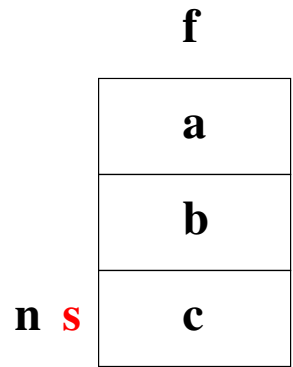


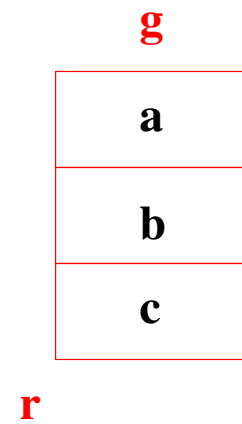
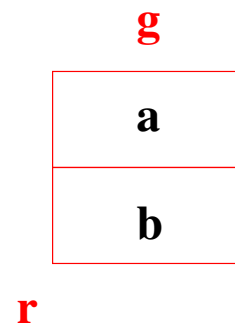
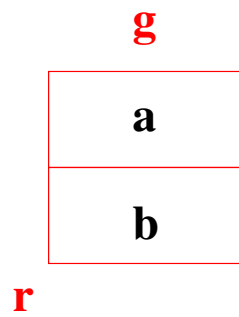
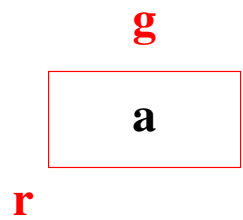
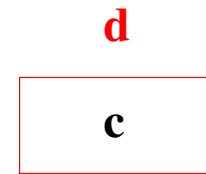
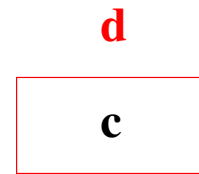
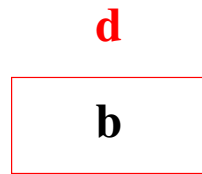
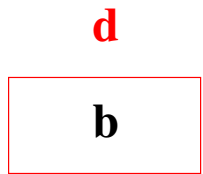
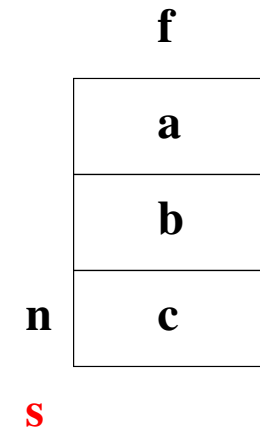
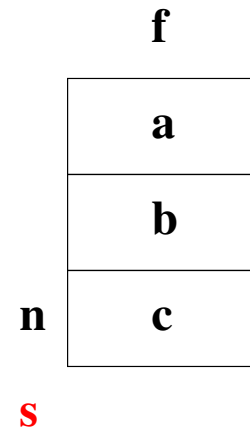
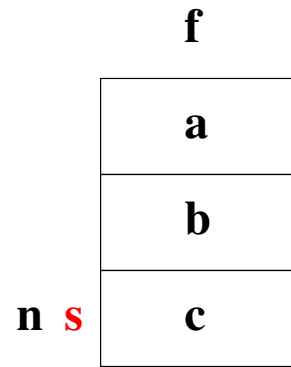
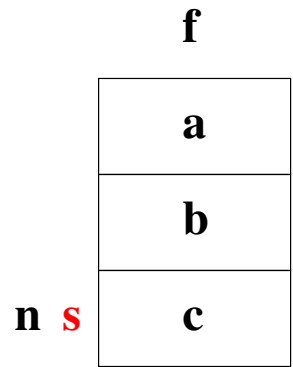


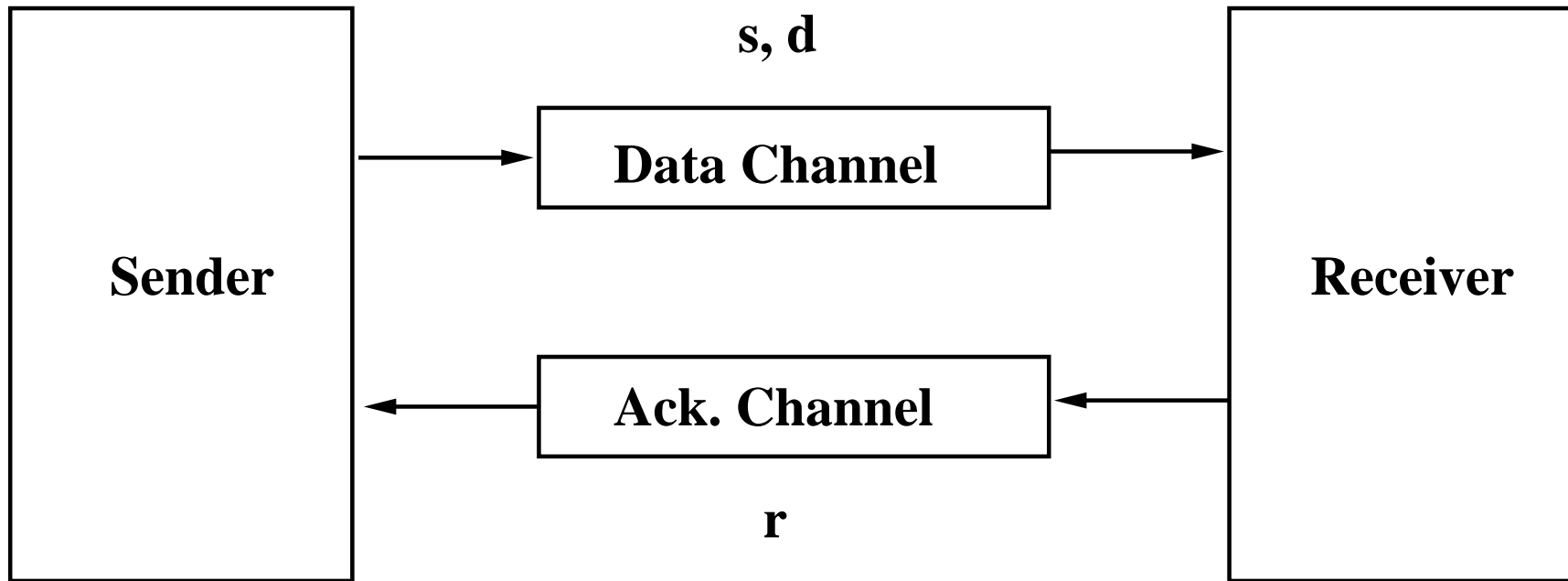












- We introduce an additional variable s , and a data item d

carrier sets: D

constants: $n, f, d0$

variables: g, r, s, d

inv2_1: $s \in 1 .. n + 1$

inv2_2: $s \in r .. r + 1$

inv2_3: $d \in D$

inv2_4: $s = r + 1 \Rightarrow d = f(r)$

axm2_1: $d0 \in D$

init

$g := \emptyset$

$s := 1$

$r := 1$

$d := d0$

send

when

$s = r$

$s \neq n + 1$

then

$d, s := f(s), s + 1$

end

receive

when

$s = r + 1$

then

$h := h \cup \{r \mapsto d\}$

$r := r + 1$

end

final

when

$r = n + 1$

then

skip

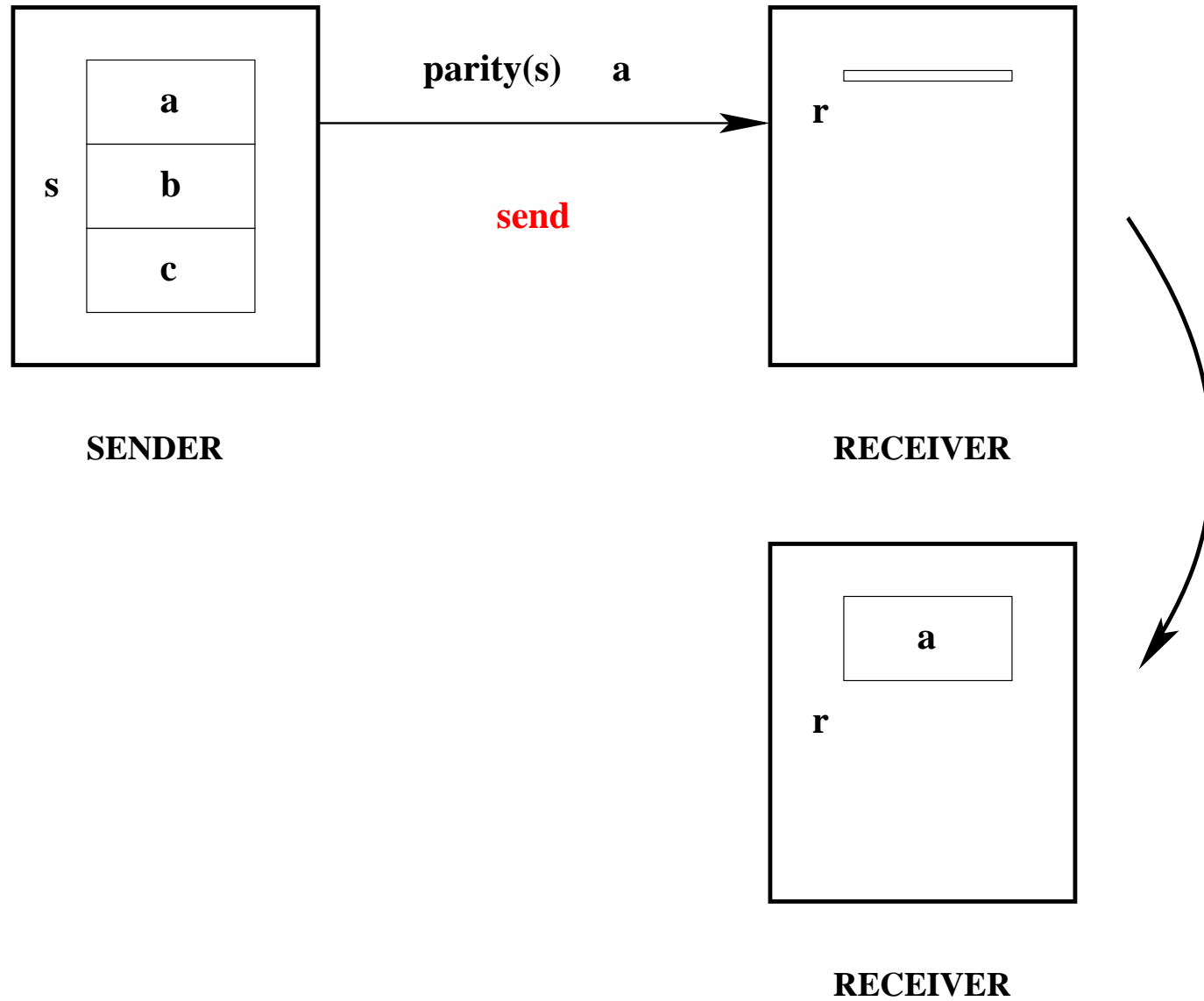
end

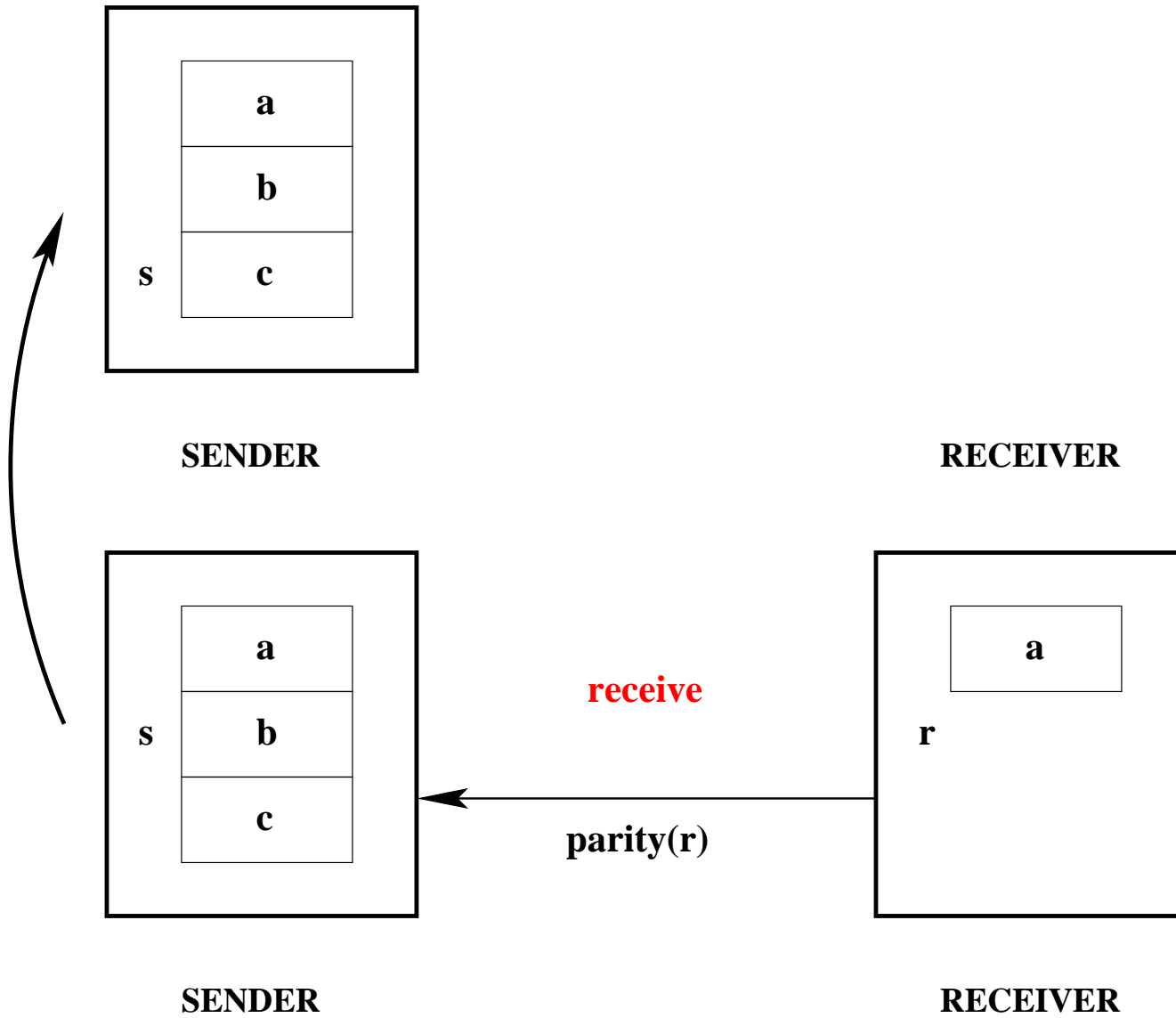
- **Initial model:** The file is transmitted in one shot (FUN1 and FUN2)
- **First refinement:** The file is transmitted gradually (FUN3)
- **Second refinement:** The two agents are separated
- **Third refinement:** Towards an implementation

```
send
  when
     $s = r$ 
     $s \neq n + 1$ 
  then
     $d := f(s)$ 
     $s := s + 1$ 
  end
```

```
receive
  when
     $s = r + 1$ 
  then
     $g := g \cup \{r \mapsto d\}$ 
     $r := r + 1$ 
  end
```

```
inv2_2:  $s \in r .. r + 1$ 
```





$$\mathbf{axm3_1:} \quad \mathit{parity} \in \mathbb{N} \rightarrow \{0, 1\}$$

$$\mathbf{axm3_2:} \quad \mathit{parity}(0) = 0$$

$$\mathbf{axm3_3:} \quad \forall x \cdot (x \in \mathbb{N} \Rightarrow \mathit{parity}(x + 1) = 1 - \mathit{parity}(x))$$

$$\mathbf{thm3_1:} \quad \forall x, y \cdot \left(\begin{array}{l} x \in \mathbb{N} \\ y \in \mathbb{N} \\ x \in y .. y + 1 \\ \mathit{parity}(x) = \mathit{parity}(y) \\ \Rightarrow \\ x = y \end{array} \right)$$

carrier sets: D

constants: $n, f, parity$

variables: g, s, r, d, p, q

inv3_1: $p = parity(s)$

inv3_2: $q = parity(r)$

axm3_1: $parity \in \mathbb{N} \rightarrow \{0, 1\}$

axm3_2: $parity(0) = 0$

axm3_3: $\forall x \cdot \left(\begin{array}{l} x \in \mathbb{N} \\ \Rightarrow \\ parity(x + 1) = 1 - parity(x) \end{array} \right)$

init

$g := \emptyset$
 $s := 1$
 $r := 1$
 $p := 1$
 $q := 1$
 $d := d_0$

final

when
 $r = n + 1$
then
 skip
end

send

when

$p = q$
 $s \neq n + 1$

then

$d := f(s)$
 $s := s + 1$
 $p := 1 - p$

end

receive

when

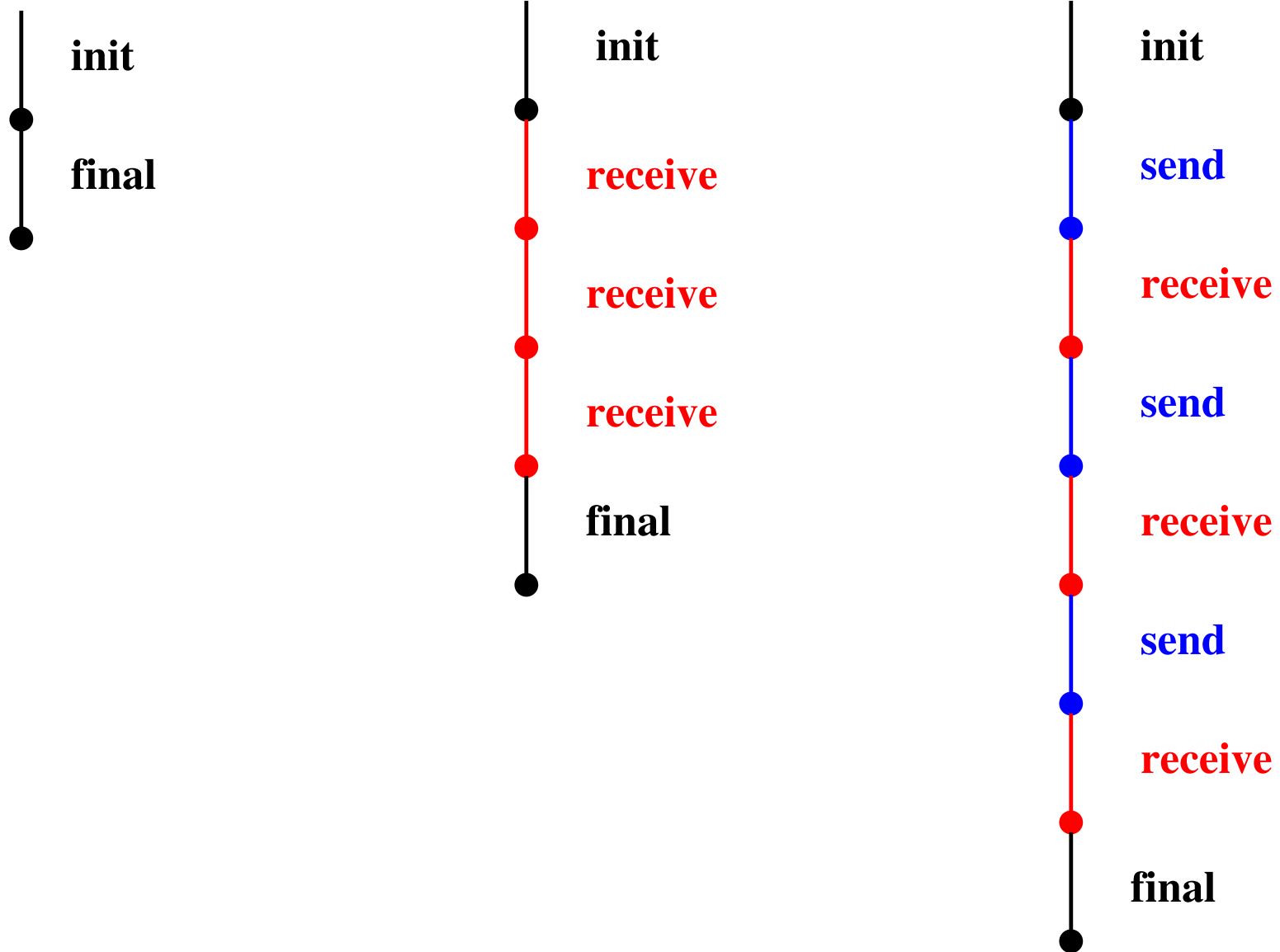
$p \neq q$

then

$g := g \cup \{r \mapsto d\}$
 $r := r + 1$
 $q := 1 - q$

end

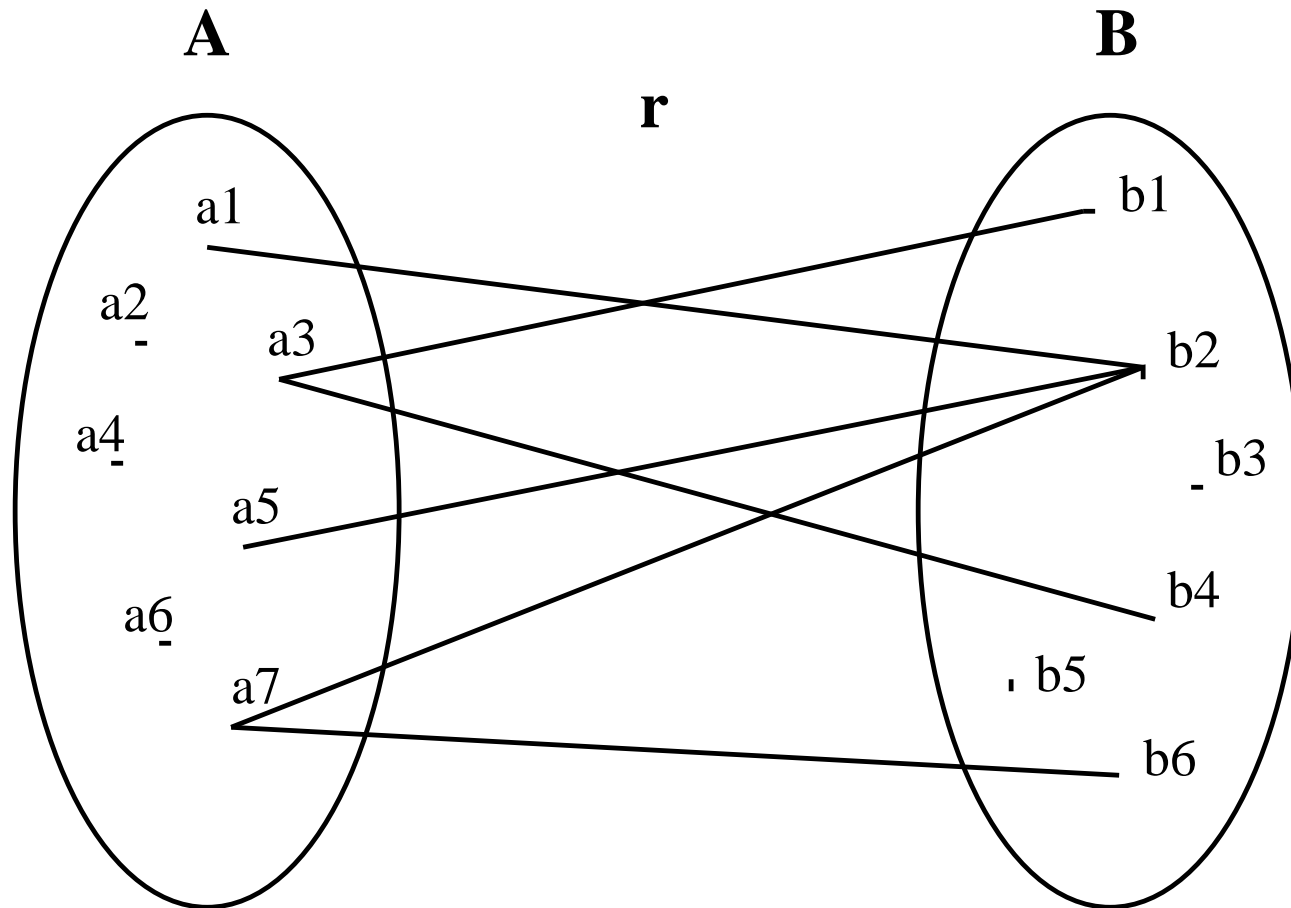
- More mathematical **conventions**
- **How to write a model**
- What kind of things we have **to prove**
- How the proof can **help finding invariants**
- Many things can be done by **tools**
- A small **theory of parities**

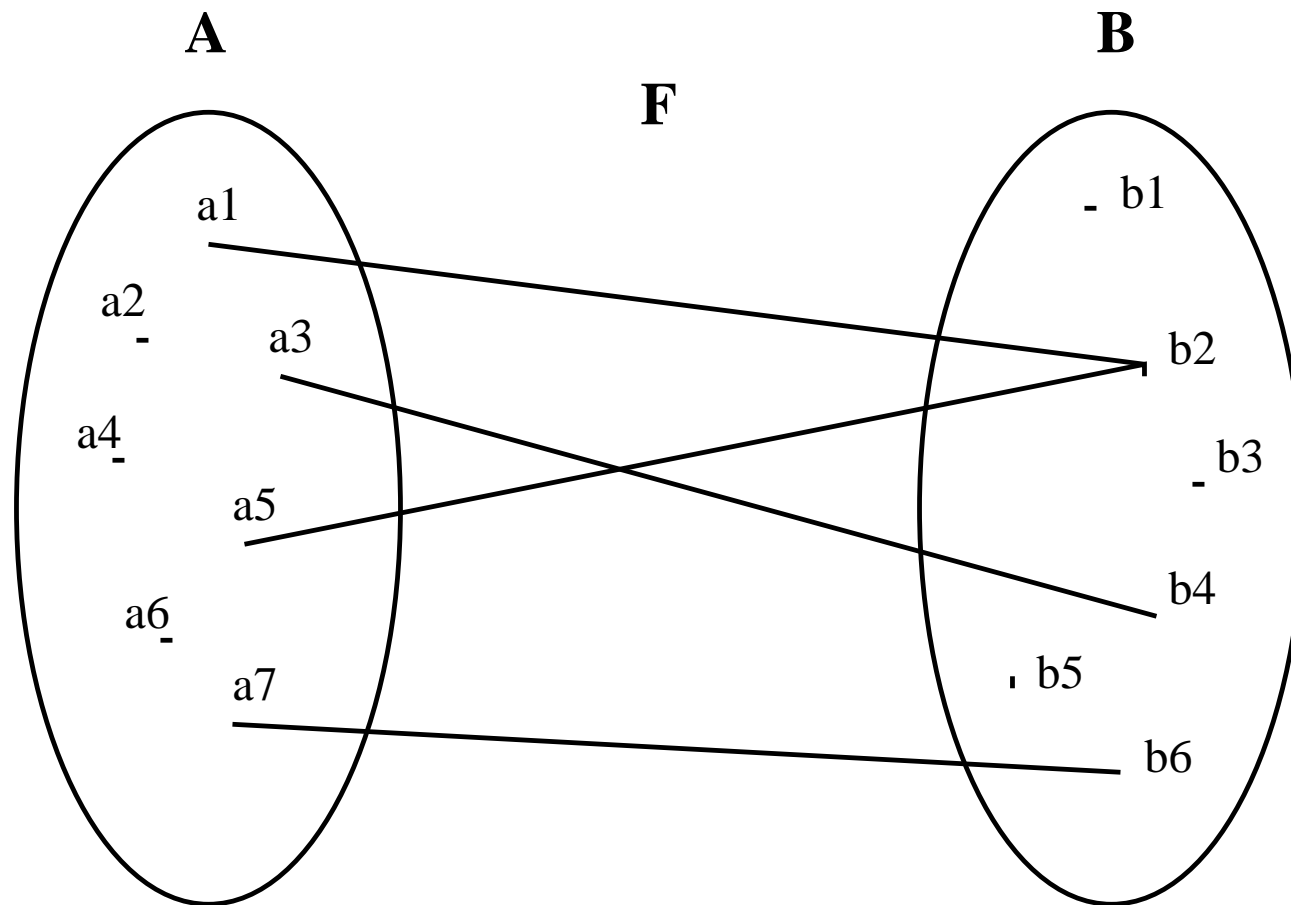


$x \in S$	Set membership operator
\mathbb{N}	set of Natural Numbers: $\{0, 1, 2, 3, \dots\}$
$a .. b$	Interval from a to b : $\{a, a + 1, \dots, b\}$ (empty when $b < a$)
$a \mapsto b$	pair constructing operator
$S \times T$	Cartesian product operator
$S \subseteq T$	set inclusion operator
$\mathbb{P}(S)$	power set operator

$S \leftrightarrow T$	Set of binary relations from S to T
$S \rightarrow T$	Set of total functions from S to T
$S \twoheadrightarrow T$	Set of partial functions from S to T
$\text{dom}(r)$	Domain of a relation r
$\text{ran}(r)$	Range of a relation r

$s \triangleleft r$	domain restriction operator
$s \triangleleft r$	domain subtraction operator
$r \triangleright t$	range restriction operator
$r \triangleright t$	range subtraction operator

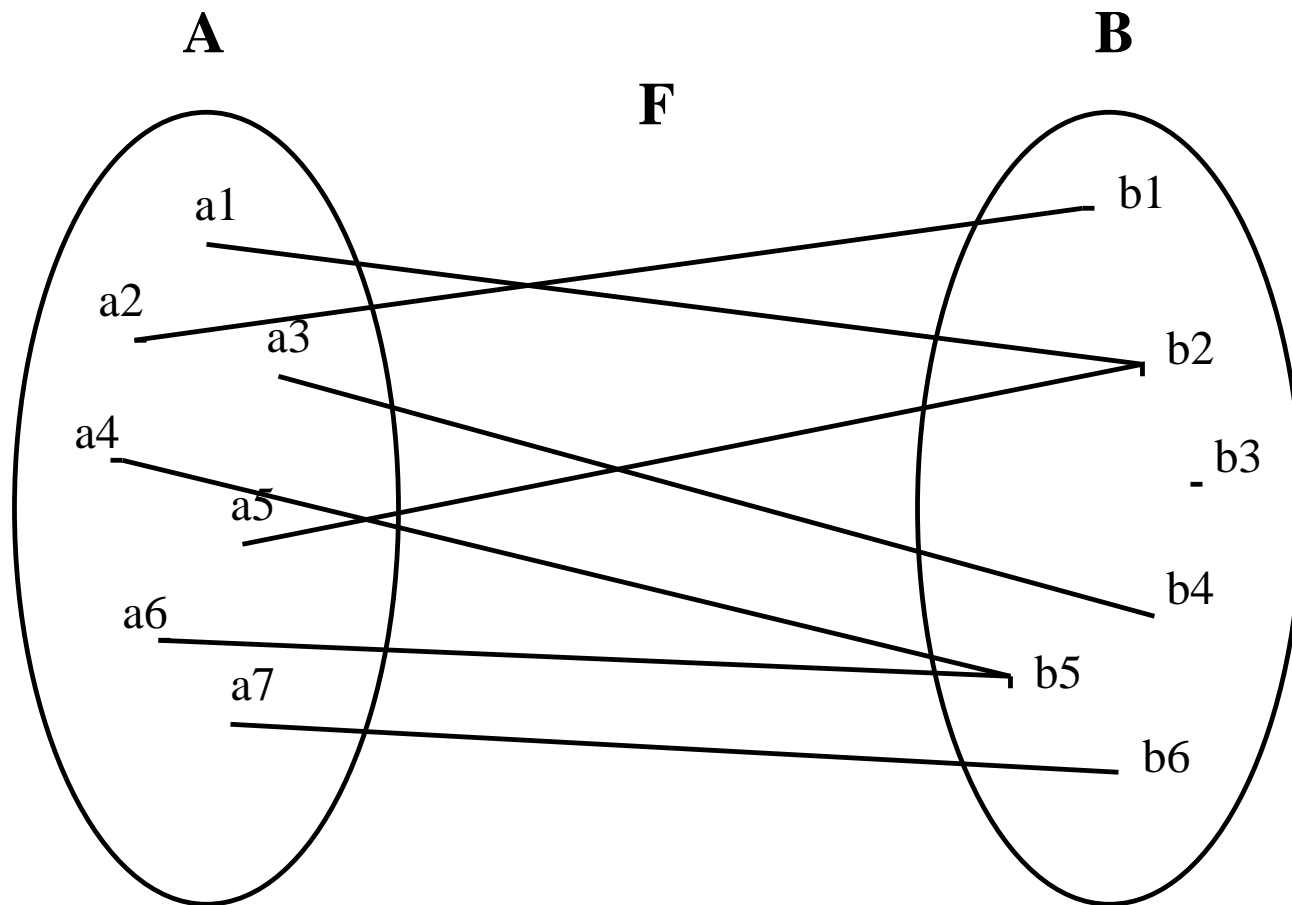




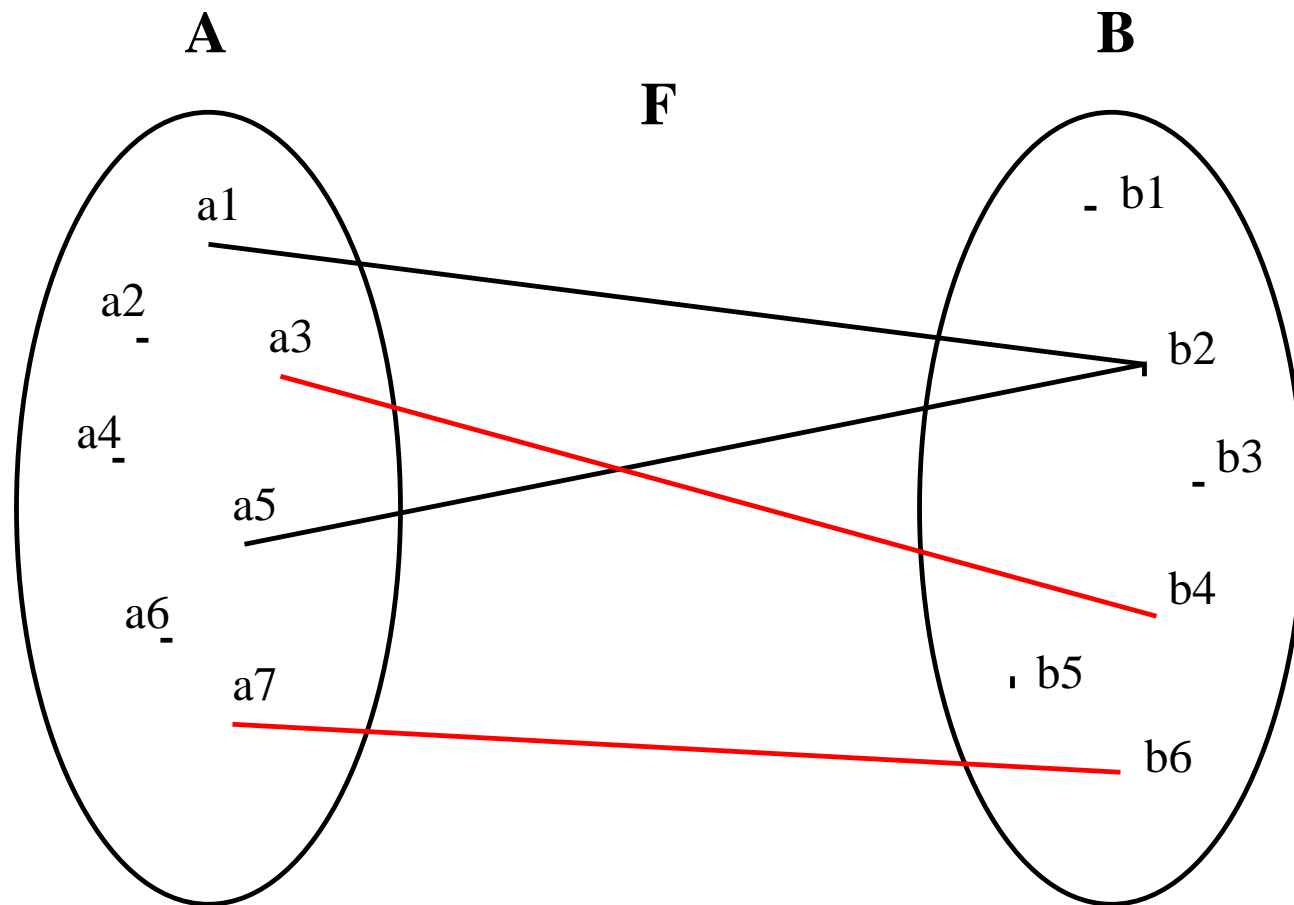
$$F = \{a1 \mapsto b2, a3 \mapsto b4, a5 \mapsto b2, a7 \mapsto b6\}$$

$$\text{dom}(F) = \{a1, a3, a5, a7\}$$

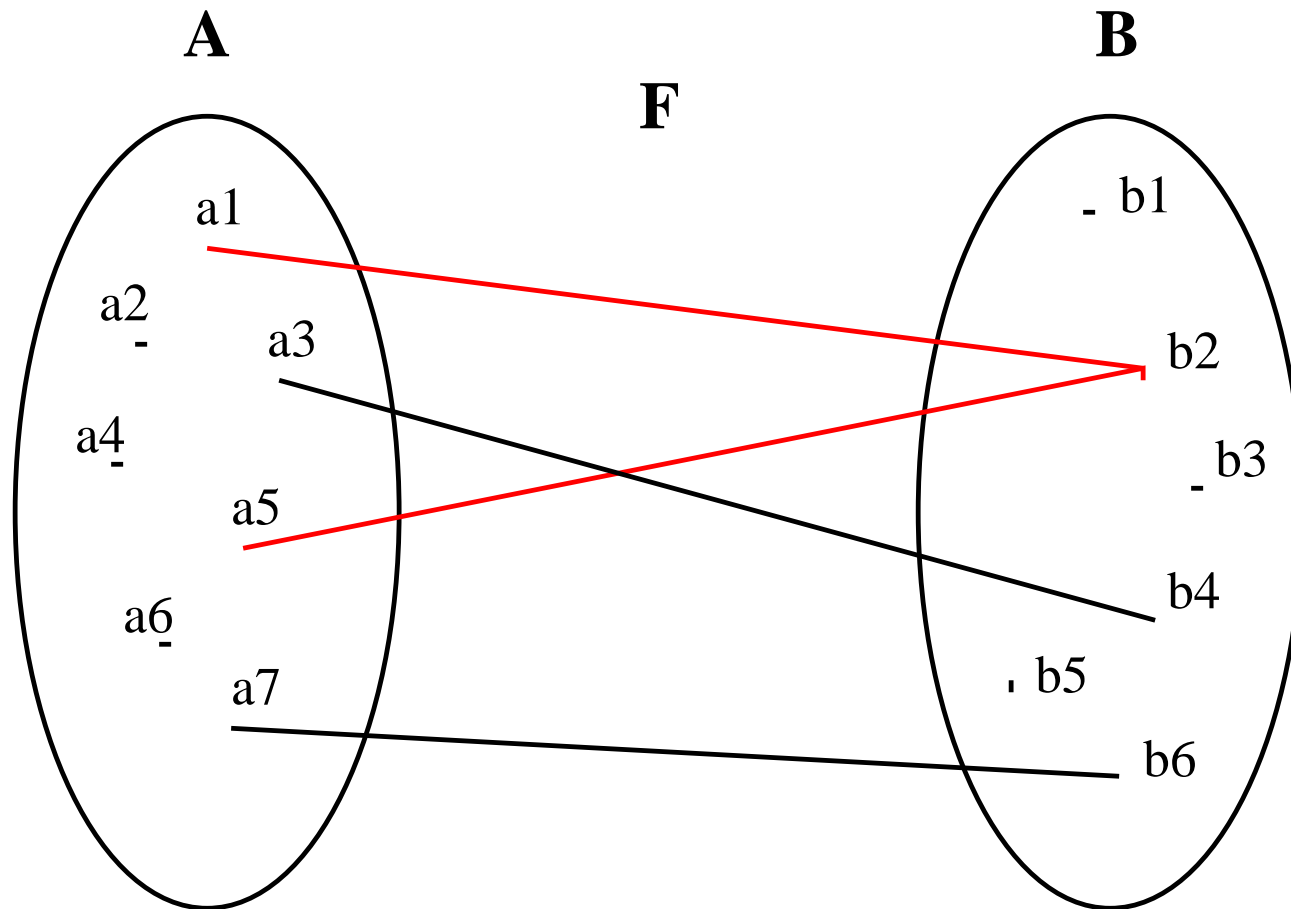
$$\text{ran}(F) = \{b2, b4, b6\}$$



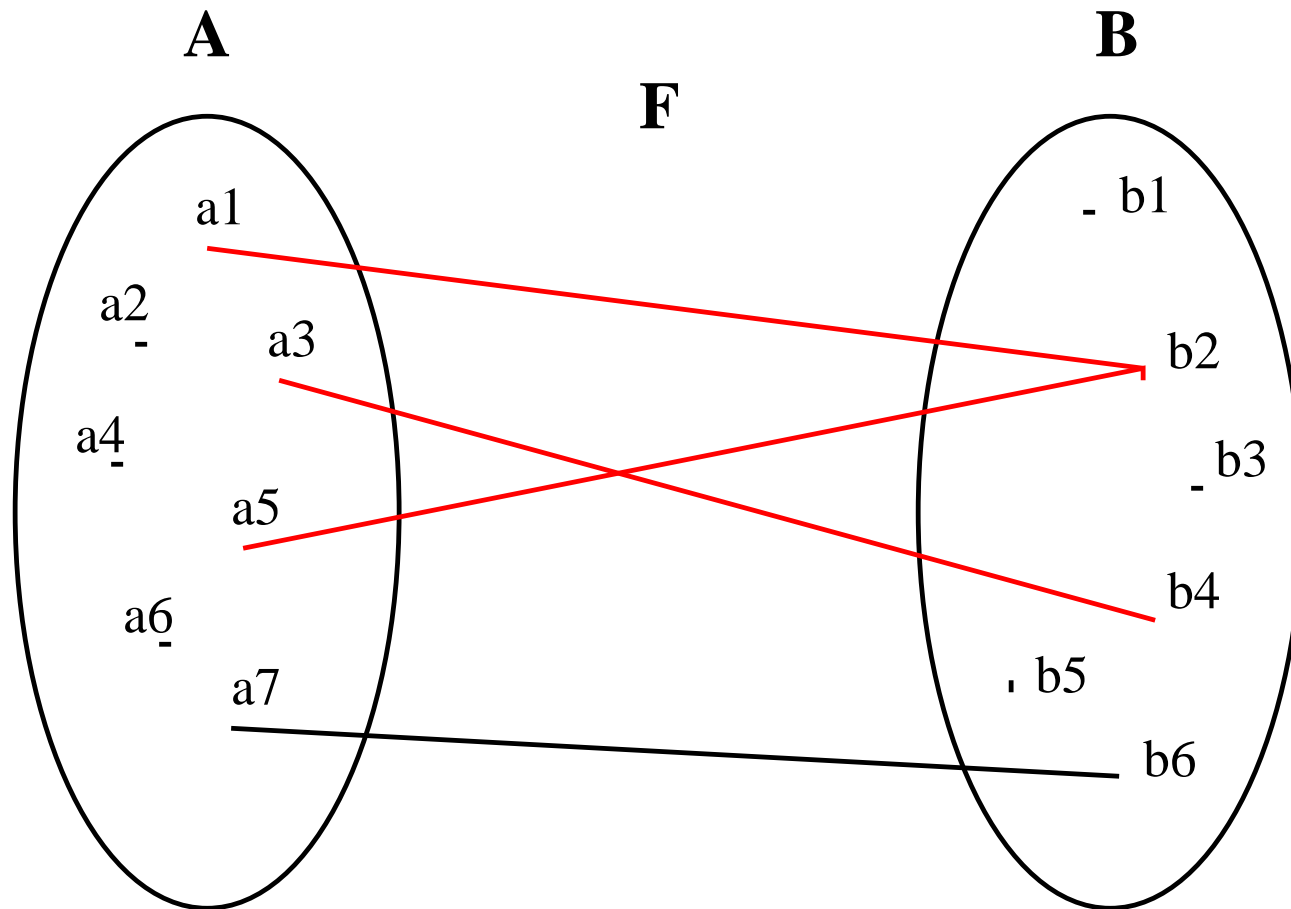
$$\text{dom}(F) = A$$



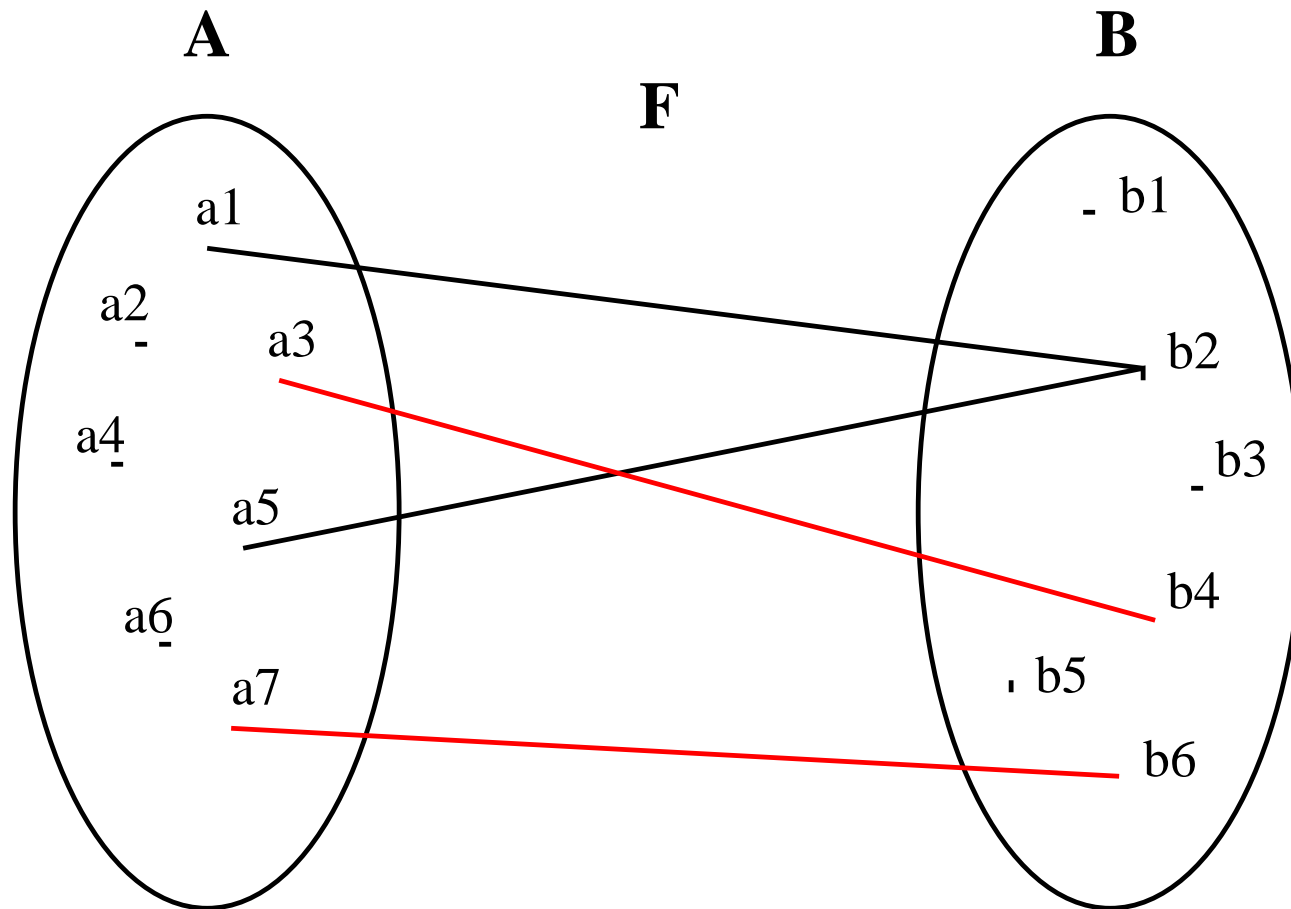
$$\{a_3, a_7\} \triangleleft F$$



$$\{a_3, a_7\} \triangleleft F$$



$$F \triangleright \{b2, b4\}$$



$$F \triangleright \{b_2\}$$

- List of **Carrier Sets** (identifiers)
- List of **Constants** (identifiers)
- List of **Axioms** (predicates built on sets and constants)
- List of **Variables** (identifiers)
- List of **Invariants** (predicates built on sets, constants, and variables)
- List of **Events**