

13. The Leader Election Protocol (IEEE 1394)

Jean-Raymond Abrial

2009

- Background :-)
- An informal presentation of the protocol :-)
- Step by step formal design :-|
- Short Conclusion. :-)

- It is an **international standard**
- There exists a **widespread commercial interest** in its correctness
- Sun, Apple, Philips, Microsoft, Sony, etc **involved in its development**
- Made of **three layers** (physical, link, transaction)
- The protocol under study is the **Tree Identify Protocol**
- Situated in the **Bus Reset phase** of the physical layer

- The bus is used to transport digitized **video and audio signals**
- It is **“hot-pluggable”**
- Devices and peripherals can be **added and removed at any time**
- Such changes are followed by a **bus reset**
- The **leader election** takes place after a bus reset in the network
- A leader needs to be chosen to act as the **manager of the bus**

- After a bus reset: all nodes in the network have **equal status**
- A node **only knows** to which nodes it is **directly connected**
- The network is **connected**
- The network is **acyclic**

BASIC

- IEEE. *IEEE Standard for a High Performance Serial Bus. Std 1394-1995*. 1995
- IEEE. *IEEE Standard for a High Performance Serial Bus (supplement). Std 1394a-2000*. 2000

GENERAL

- N. Lynch. *Distributed Algorithms*. Morgan Kaufmann. 1996
- R. G. Gallager et al. *A Distributed Algorithm for Minimum Weight Spanning Trees*. IEEE Trans. on Prog. Lang. and Systems. 1983.

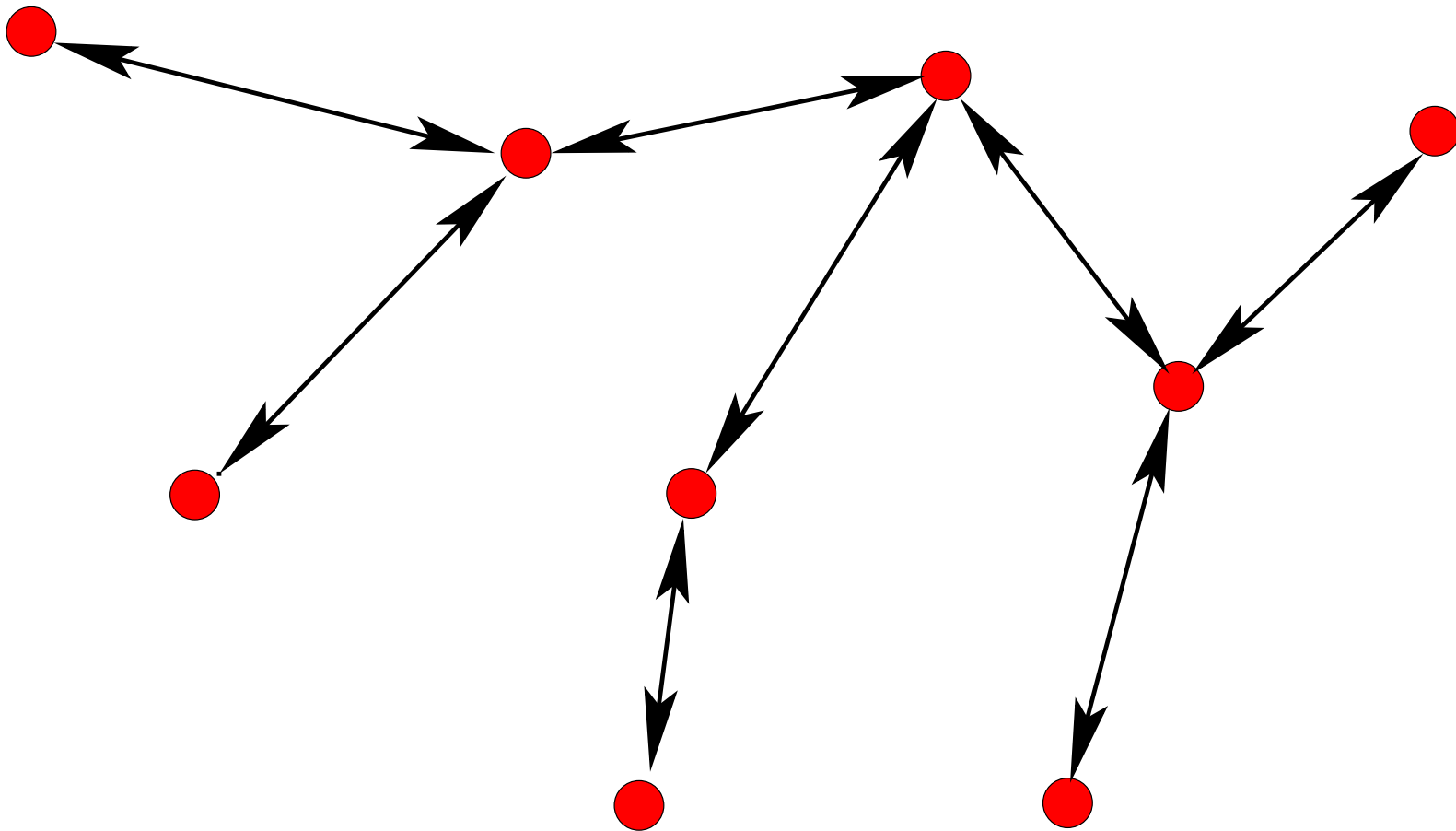
MODEL CHECKING

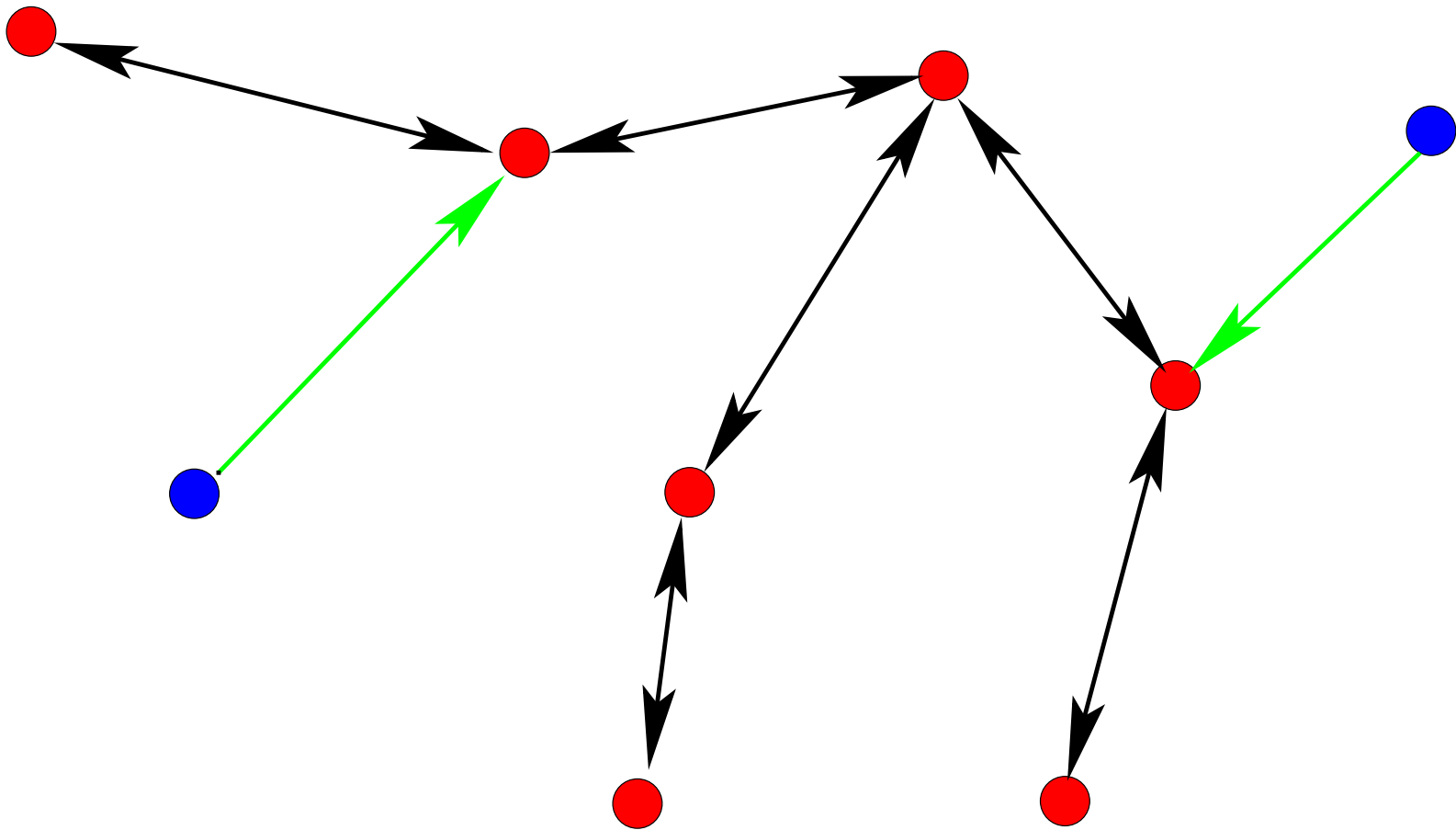
- D.P.L. Simons et al. *Mechanical Verification of the IEE 1394a Root Contention Protocol using Uppaal2* Springer International Journal of Software Tools for Technology Transfer. 2001
- H. Toetenel et al. *Parametric verification of the IEEE 1394a Root Contention Protocol using LPMC* Proceedings of the 7th International Conference on Real-time Computing Systems and Applications. IEEE Computer Society Press. 2000

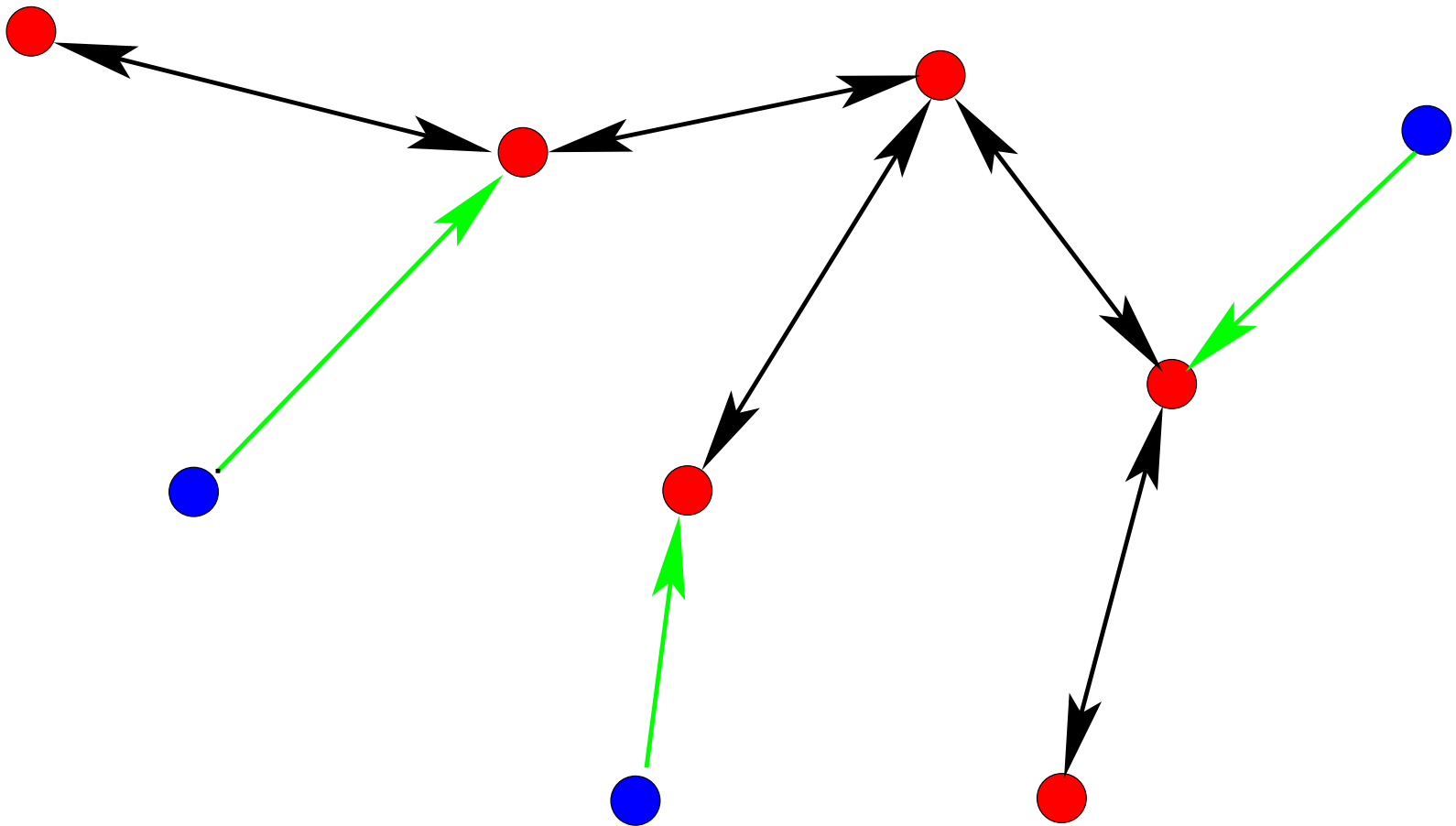
THEOREM PROVING

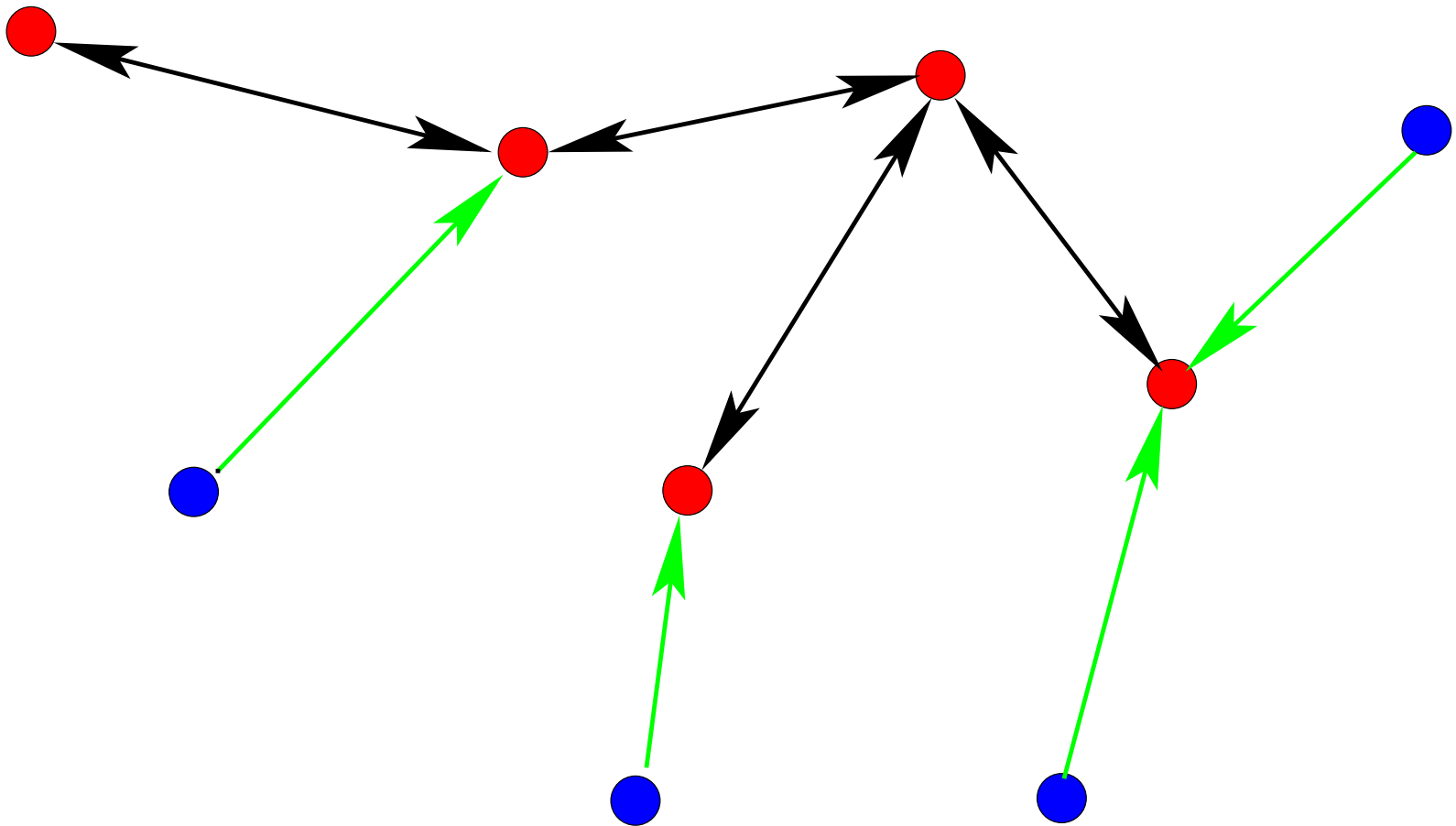
- M. Devillers et al. *Verification of the Leader Election: Formal Method Applied to IEEE 1394*. Formal Methods in System Design. 2000
- J.R. Abrial et al. *A Mechanically Proved and Incremental Development of IEEE 1394*. Formal Aspects of Computing. 2003

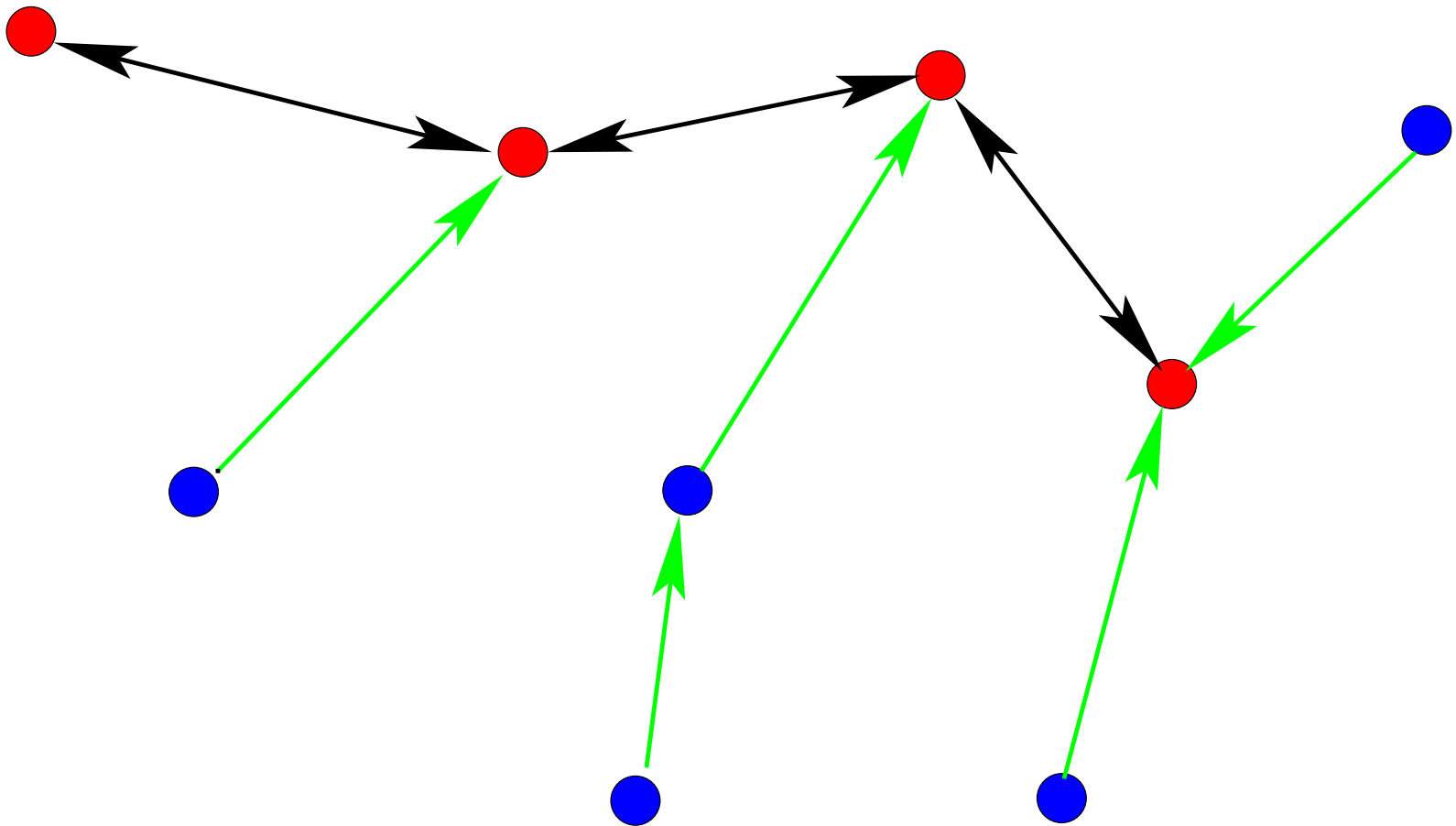
- We are given a **connected** and **acyclic** network of nodes
- Nodes are linked by **bidirectional channels**
- We want to have one node being elected **the leader** in a finite time
- This is to be done in a **distributed** and **non-deterministic** way
- Next are two distinct **abstract animations** of the protocol

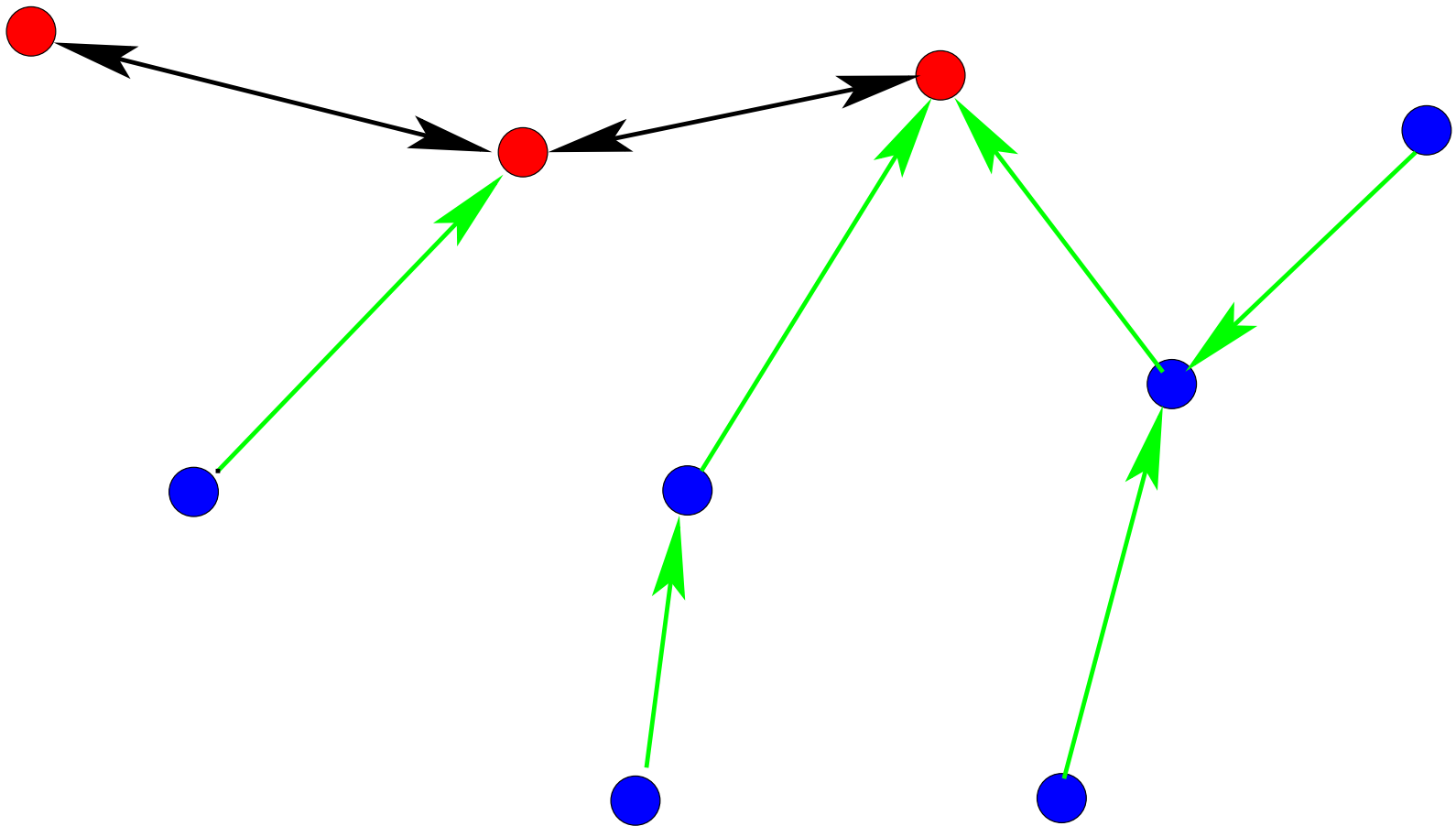


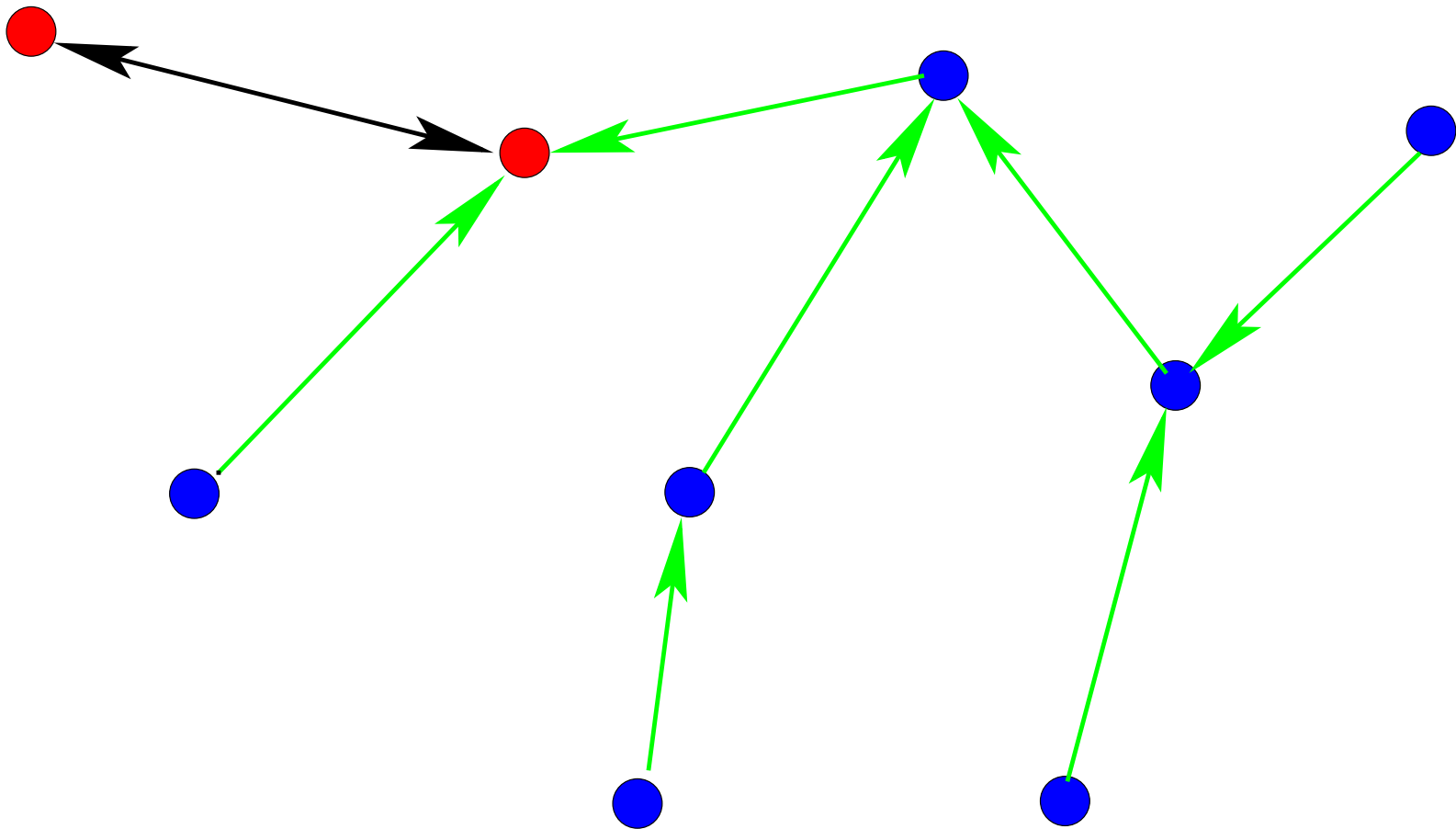


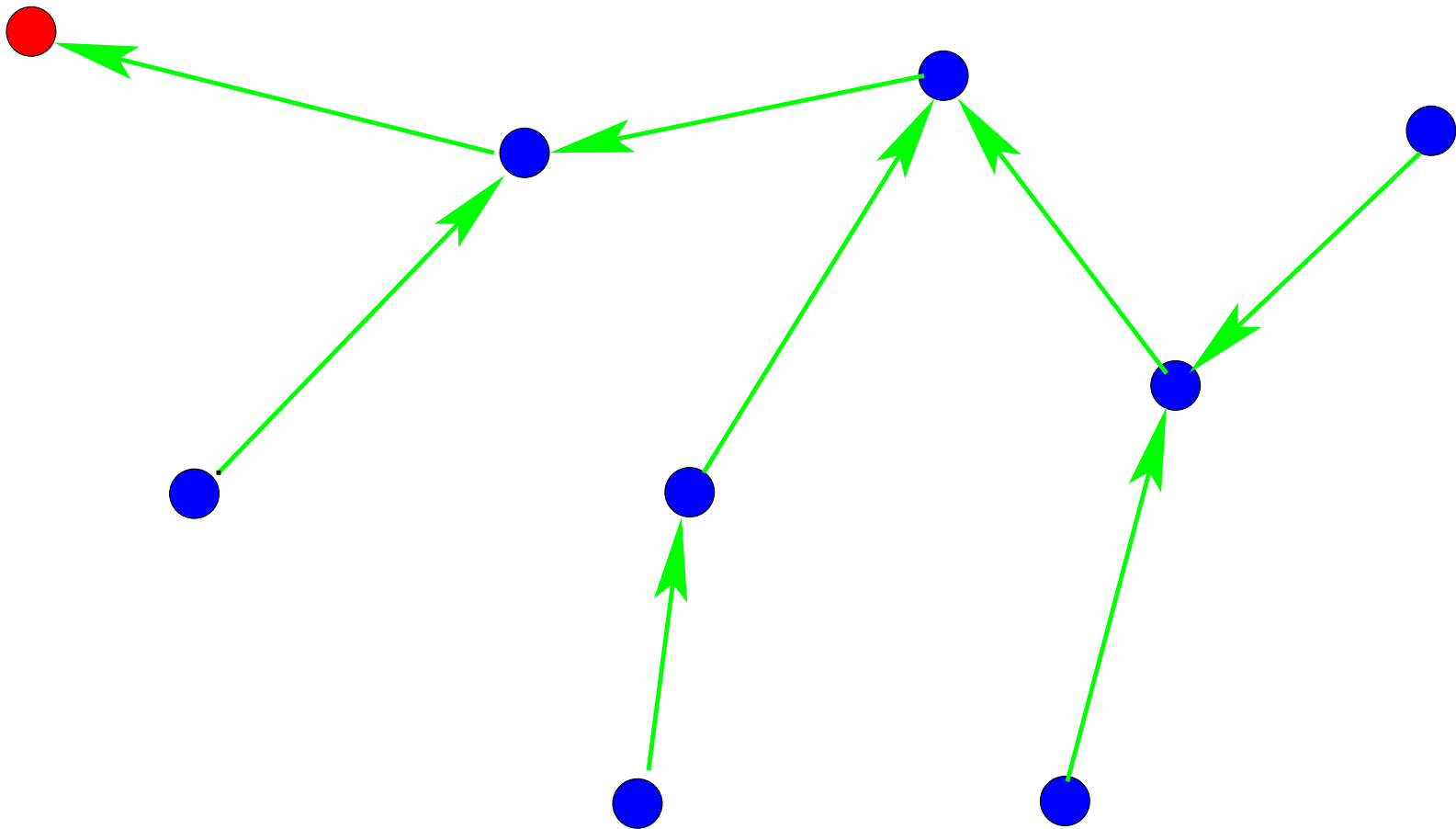












- Formal **definition** and **properties** of the network
- A **one-shot** abstract model of the protocol
- Presenting a (still abstract) loop-like **centralized solution**
- Introducing **message passing** between the nodes (**delays**)
- Modifying the data structure in order to **distribute the protocol**

sets: N

axm0_1: $\text{finite}(N)$

variables: l

inv0_1: $l \in N$

init
 $l := N$

elect
any x **where**
 $x \in N$
then
 $l := x$
end

constant: g

$$\begin{aligned} \text{axm_5: } \forall h, S \cdot & h \cup h^{-1} = g \\ & h \cap h^{-1} = \emptyset \\ & S \subseteq h[S] \\ \Rightarrow & \\ & S = \emptyset \end{aligned}$$

$$\text{axm1_1: } g \in N \leftrightarrow N$$

$$\text{axm1_2: } g = g^{-1}$$

$$\text{axm1_3: } g \cap \text{id}(N) = \emptyset$$

$$\begin{aligned} \text{axm1_4: } \forall s \cdot & S \subseteq N \\ & S \neq \emptyset \\ & g[S] \subseteq S \\ \Rightarrow & \\ & N \subseteq S \end{aligned}$$

- **axm1_4** expresses that g is a **strongly connected graph**
- **axm1_5** expresses that any partition of g has **no cycle**

variable: l
 n

inv1_1: $n \subseteq N$

inv1_2: $\forall s \cdot$
 $S \subseteq n$
 $S \neq \emptyset$
 $(n \triangleleft g \triangleright n)[S] \subseteq S$
 \Rightarrow
 $n \subseteq S$

- Variable n is a subset of N
- The graph reduced to n is **still connected**

```
init
```

```
   $l \in N$ 
```

```
   $n := N$ 
```

```
elect
```

```
  any  $x$  where
```

```
     $n = \{x\}$ 
```

```
  then
```

```
     $l := x$ 
```

```
  end
```

```
progress
```

```
  status
```

```
    convergent
```

```
  any  $x, y$  where
```

```
     $x \in n$ 
```

```
     $g[\{x\}] \cap n = \{y\}$ 
```

```
  then
```

```
     $n := n \setminus \{x\}$ 
```

```
  end
```

- A **leaf** x of the reduced graph is **removed from** n
- The remaining **unique element** of n is elected

```
variant1:  $n$ 
```


variables: l, n, m

inv2_1: $m \subseteq g$

inv2_2: $m \in n \leftrightarrow n$

inv2_3: $\forall x, y \cdot x \mapsto y \in m \Rightarrow g[\{x\}] \cap n = \{y\}$

send_msg

any x, y **where**

$x \in n$

$g[\{x\}] \cap n = \{y\}$

$x \notin \text{dom}(m)$

then

$m := m \cup \{x \mapsto y\}$

end

progress

any x, y **where**

$x \mapsto y \in m$

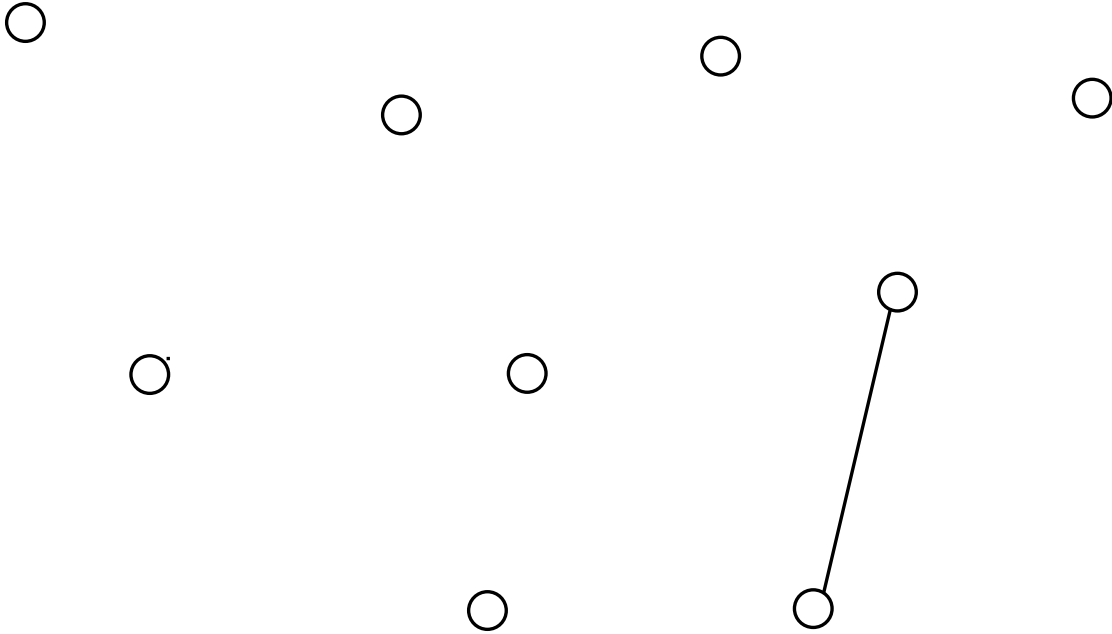
$y \notin \text{dom}(m)$

then

$n := n \setminus \{x\}$

$m := m \setminus \{x \mapsto y\}$

end



variables: l, n, m, c, bm

inv3_1: $c \subseteq g$

inv3_2: $m \cup c \in n \leftrightarrow n$

inv3_3: $m \cap c = \emptyset$

inv3_4: $bm = \text{dom}(m \cup c)$

```
send_msg
  any  $x, y$  where
     $x \in n$ 
     $g[\{x\}] \cap n = \{y\}$ 
     $x \notin bm$ 
  then
     $m := m \cup \{x \mapsto y\}$ 
     $bm := bm \cup \{x\}$ 
  end
```

```
progress
  any  $x, y$  where
     $x \mapsto y \in m$ 
     $y \notin bm$ 
  then
     $n := n \setminus \{x\}$ 
     $m := m \setminus \{x \mapsto y\}$ 
  end
```

discover_contention

any x, y **where**

$x \mapsto y \in m$

$y \in bm$

then

$c := c \cup \{x \mapsto y\}$

$m := m \setminus \{x \mapsto y\}$

end

solve_contention

any x, y **where**

$c = \{x \mapsto y, y \mapsto x\}$

then

$c := \emptyset$

$bm := bm \setminus \{x, y\}$

end

variables: l, d, m, c, bm

inv4_1: $d \in n \rightarrow \mathbb{P}(n)$

inv4_2: $\forall x \cdot x \in n \Rightarrow d(x) = g[\{x\}] \cap n$

```

init
   $l \in N$ 
   $d :| \left( \begin{array}{l} d' \in N \rightarrow \mathbb{P}(N) \\ \forall x \cdot (x \in N \Rightarrow d'(x) = g[\{x\}]) \end{array} \right)$ 
   $m := \emptyset$ 
   $c := \emptyset$ 
   $bm := \emptyset$ 
    
```

```

elect
  any  $x$  where
     $x \in \text{dom}(d)$ 
     $d(x) = \emptyset$ 
  then
     $l := x$ 
  end
    
```

```

send_msg
  any  $x, y$  where
     $x \in \text{dom}(d)$ 
     $d(x) = \{y\}$ 
     $x \notin bm$ 
  then
     $m := m \cup \{x \mapsto y\}$ 
     $bm := bm \cup \{x\}$ 
  end
    
```

```

progress
  any  $x, y$  where
     $x \mapsto y \in m$ 
     $y \notin bm$ 
  then
     $d := (\{x\} \triangleleft d) \triangleleft \{y \mapsto d(y) \setminus \{x\}\}$ 
     $m := m \setminus \{x \mapsto y\}$ 
     $bm := bm \setminus \{x\}$ 
  end
    
```

variables: l, d, m, c, bm, r

inv5_1: $r \in N \rightarrow \mathbb{N}$

inv5_2: $\forall x \cdot (x \in N \Rightarrow r(x) = \text{card}(d(x)))$

init

$$l := N$$

$$d := \left(\begin{array}{l} d' \in N \rightarrow \mathbb{P}(N) \\ \forall x \cdot (x \in N \Rightarrow d'(x) = g[\{x\}]) \end{array} \right)$$

$$m := \emptyset$$

$$c := \emptyset$$

$$bm := \emptyset$$

$$r := \left(\begin{array}{l} r' \in N \rightarrow \mathbb{N} \\ \forall x \cdot (x \in N \Rightarrow r'(x) = \text{card}(g[\{x\}])) \end{array} \right)$$

elect

any x **where**

$$x \in N$$

$$r(x) = 0$$

then

$$l := x$$

end

send_msg

any x, y **where**

$$x \in N$$

$$r(x) = 1$$

$$y \in d(x)$$

$$x \notin bm$$

then

$$m := m \cup \{x \mapsto y\}$$

$$bm := bm \cup \{x\}$$

end

progress

any x, y **where**

$$x \mapsto y \in m$$

$$y \notin bm$$

then

$$d := (\{x\} \triangleleft d) \triangleleft \{y \mapsto d(y) \setminus \{x\}\}$$

$$r := (\{x\} \triangleleft r) \triangleleft \{y \mapsto r(y) - 1\}$$

$$m := m \setminus \{x \mapsto y\}$$

end