13. The Leader Election Protocol (IEEE 1394)

Jean-Raymond Abrial

2009

Outline of Lecture

- Background :-)

- An informal presentation of the protocol :-)

- Step by step formal design :-|

- Short Conclusion. :-)

IEEE 1394 High Performance Serial Bus (FireWire)

- 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 Problem (1)

- 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

The Problem (2)

- 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

Informal Abstract Properties of the Protocol

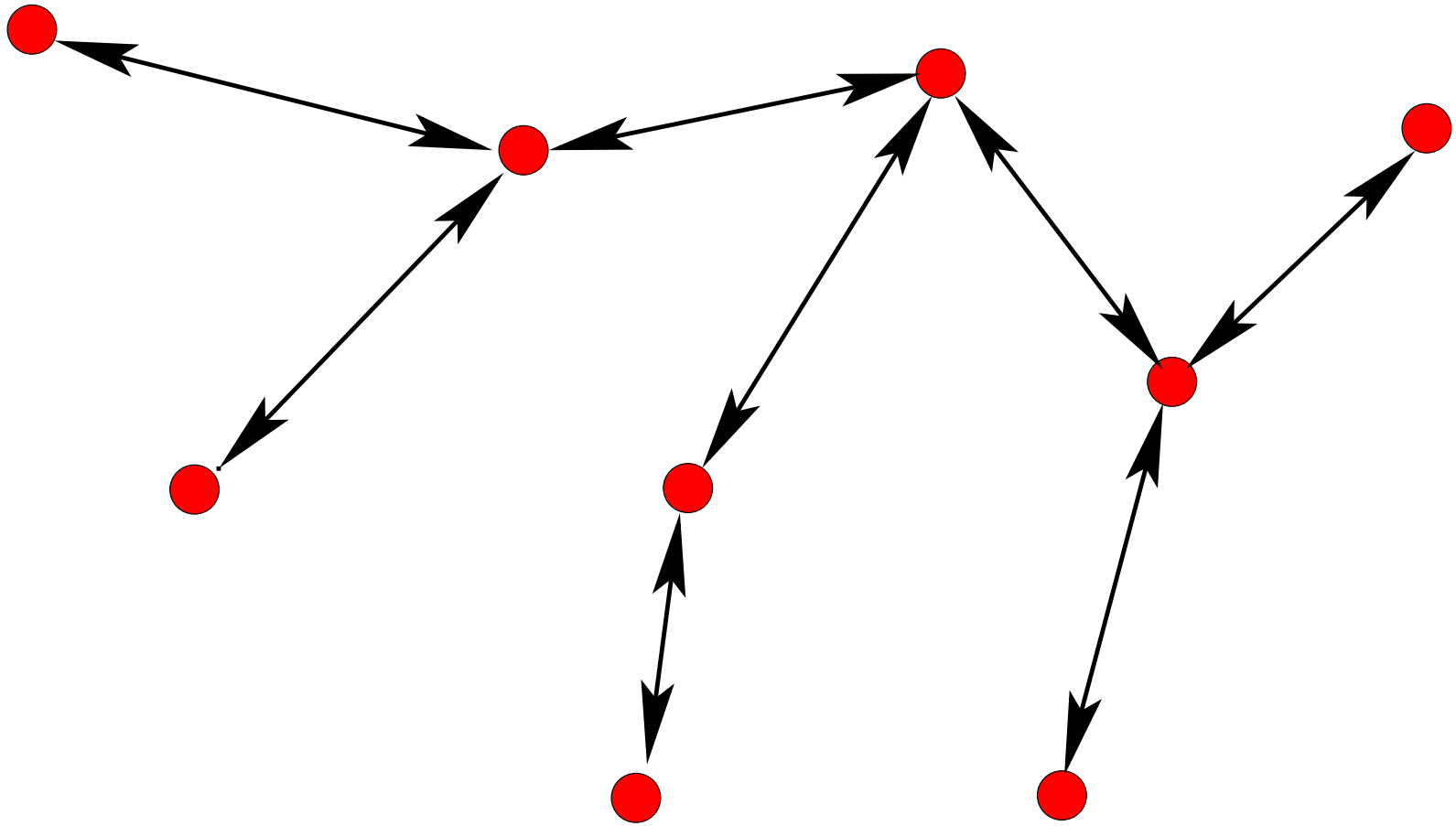
- We are given a connected and acyclic network of nodes

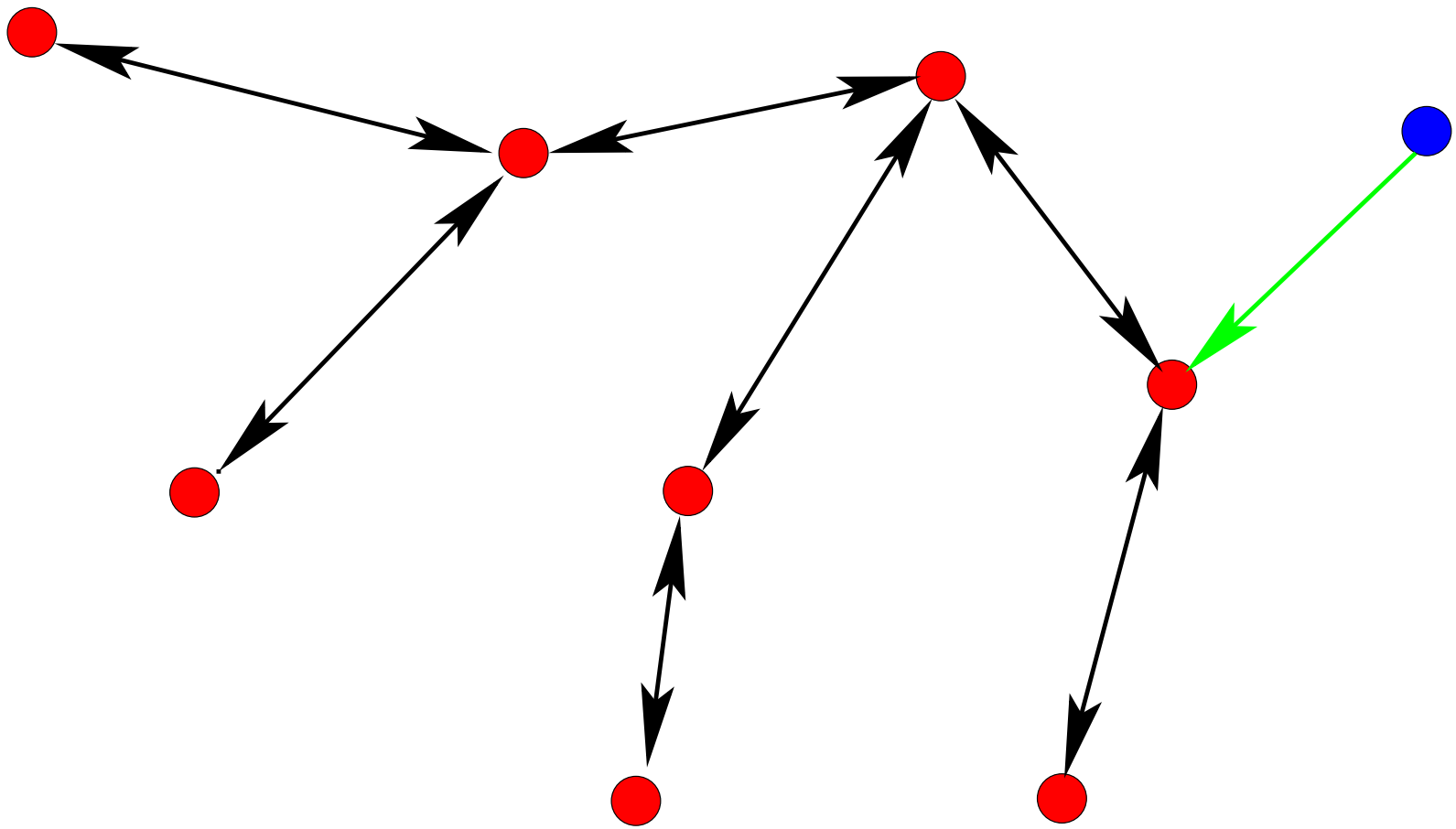
- Nodes are linked by bidirectional channels

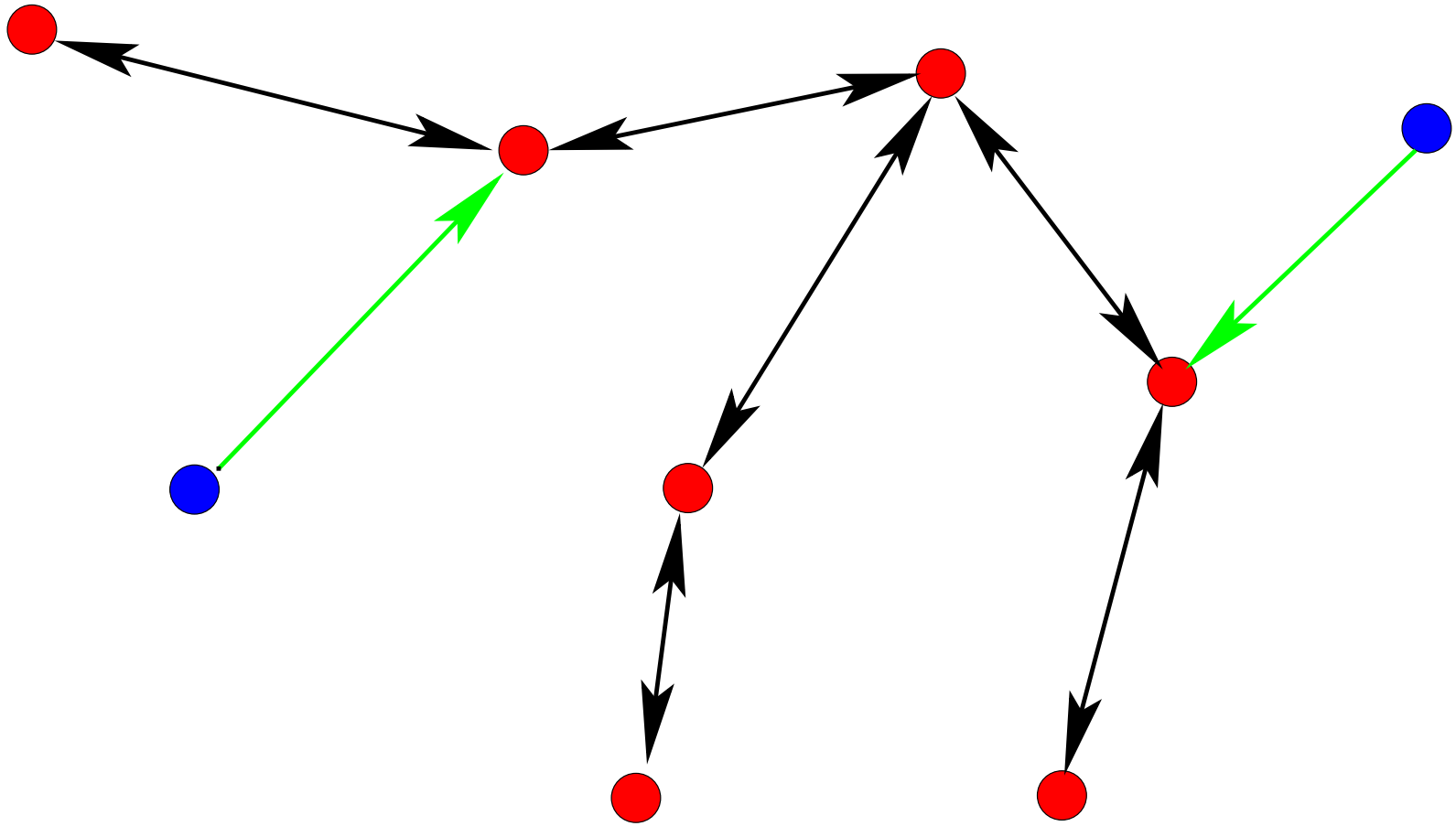
- We want to have one node being elected the leader in a finite time

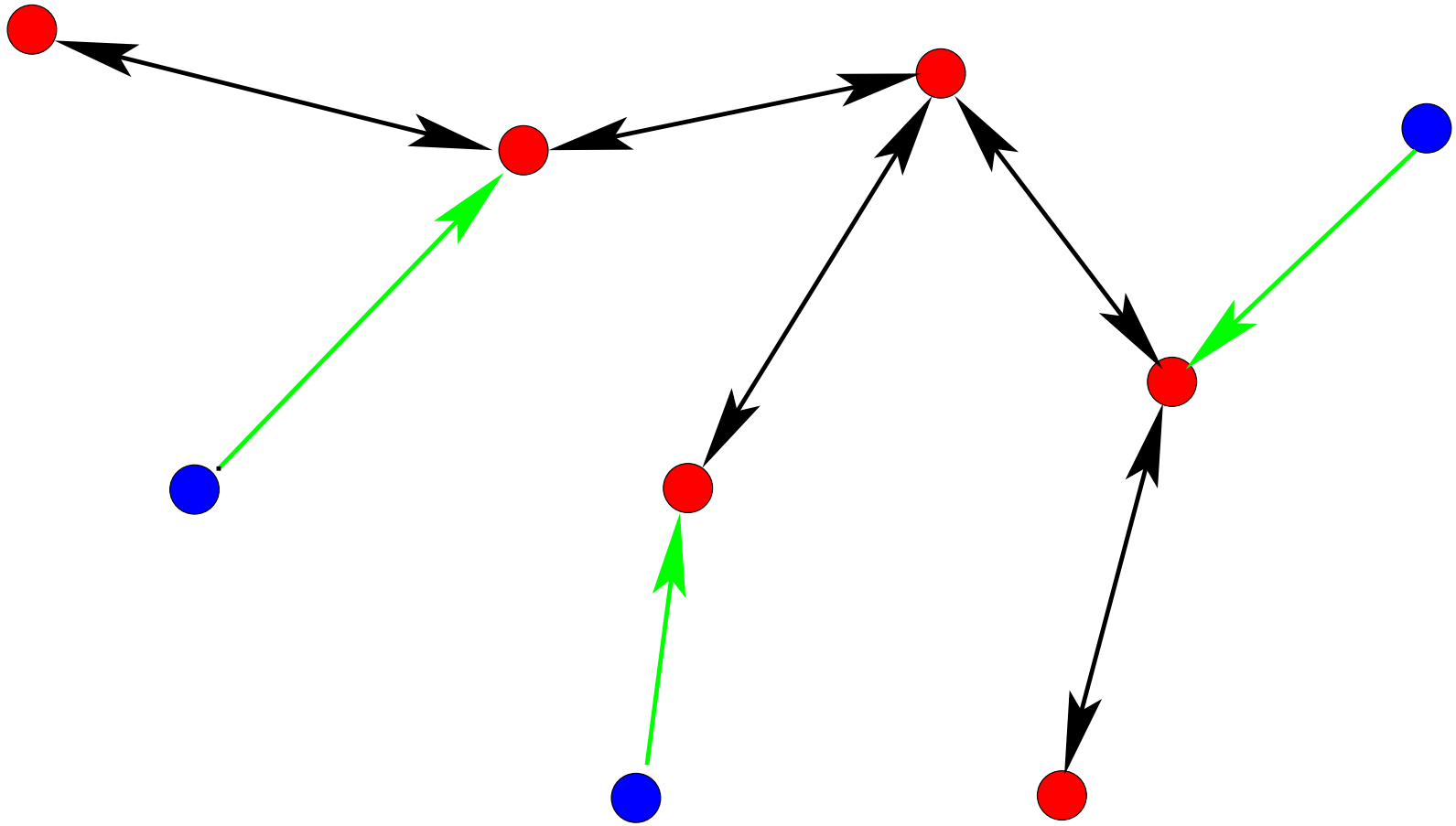
- This is to be done in a distributed and non-deterministic way

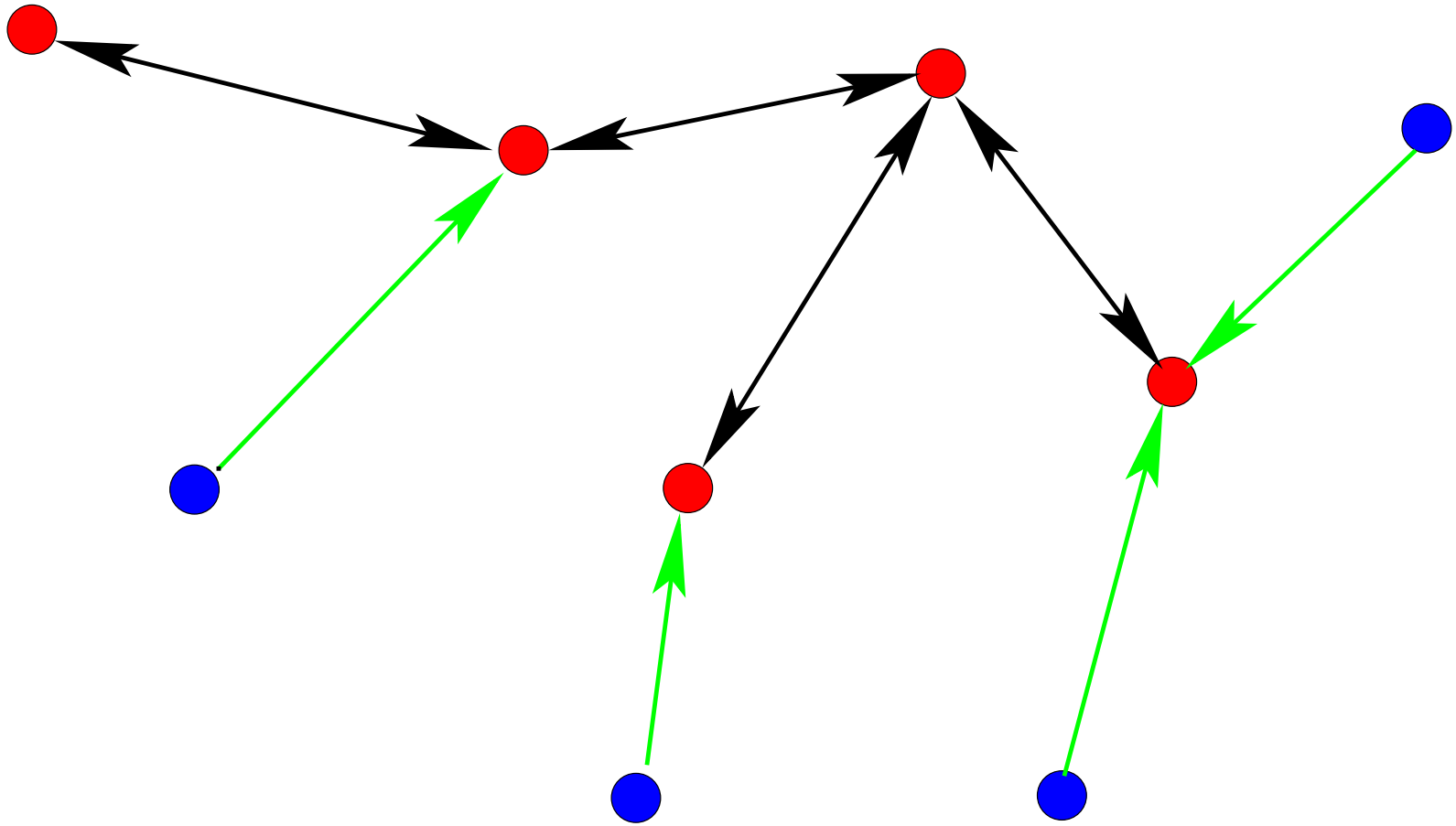
- Next are two distinct abstract animations of the protocol

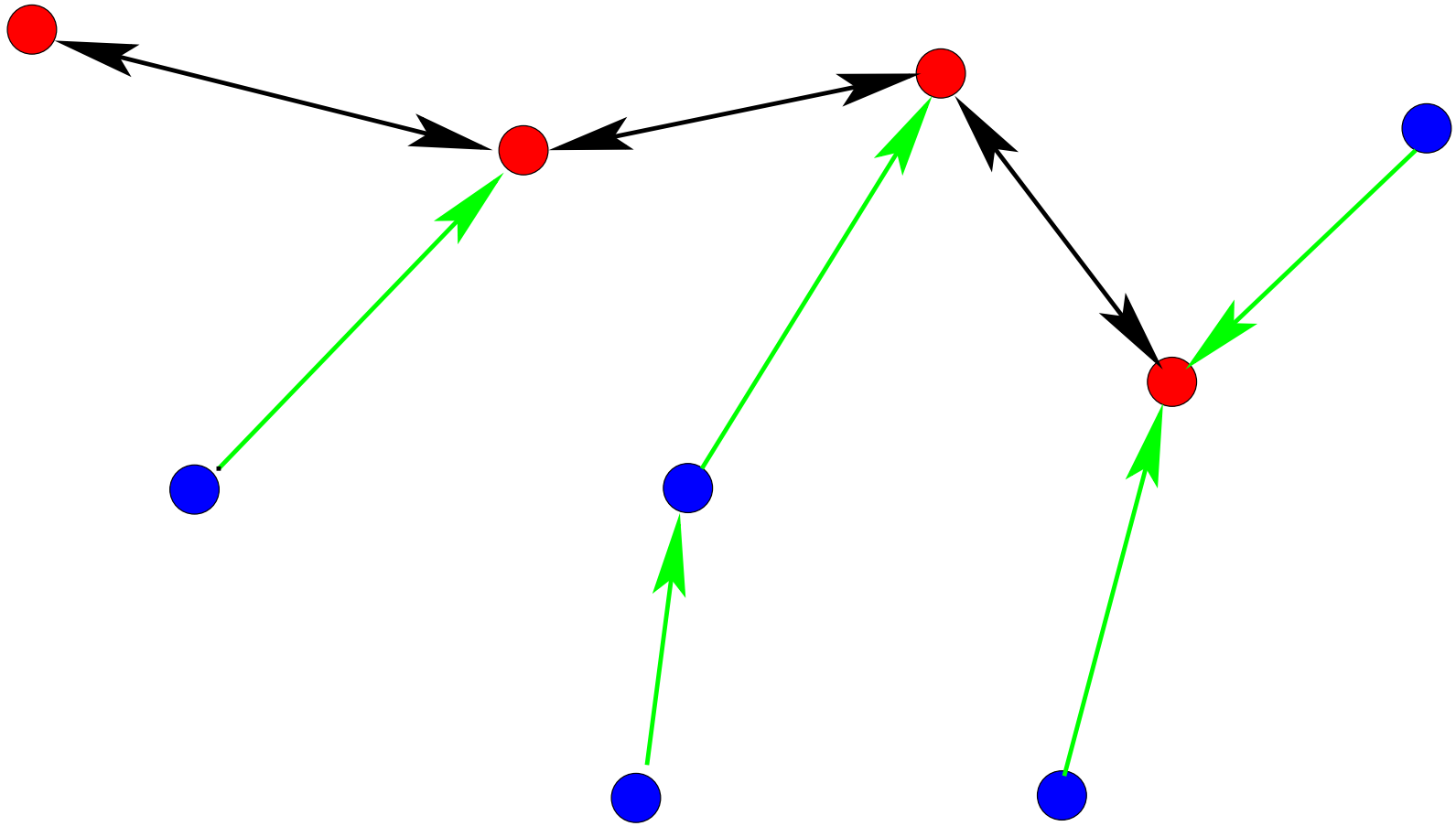


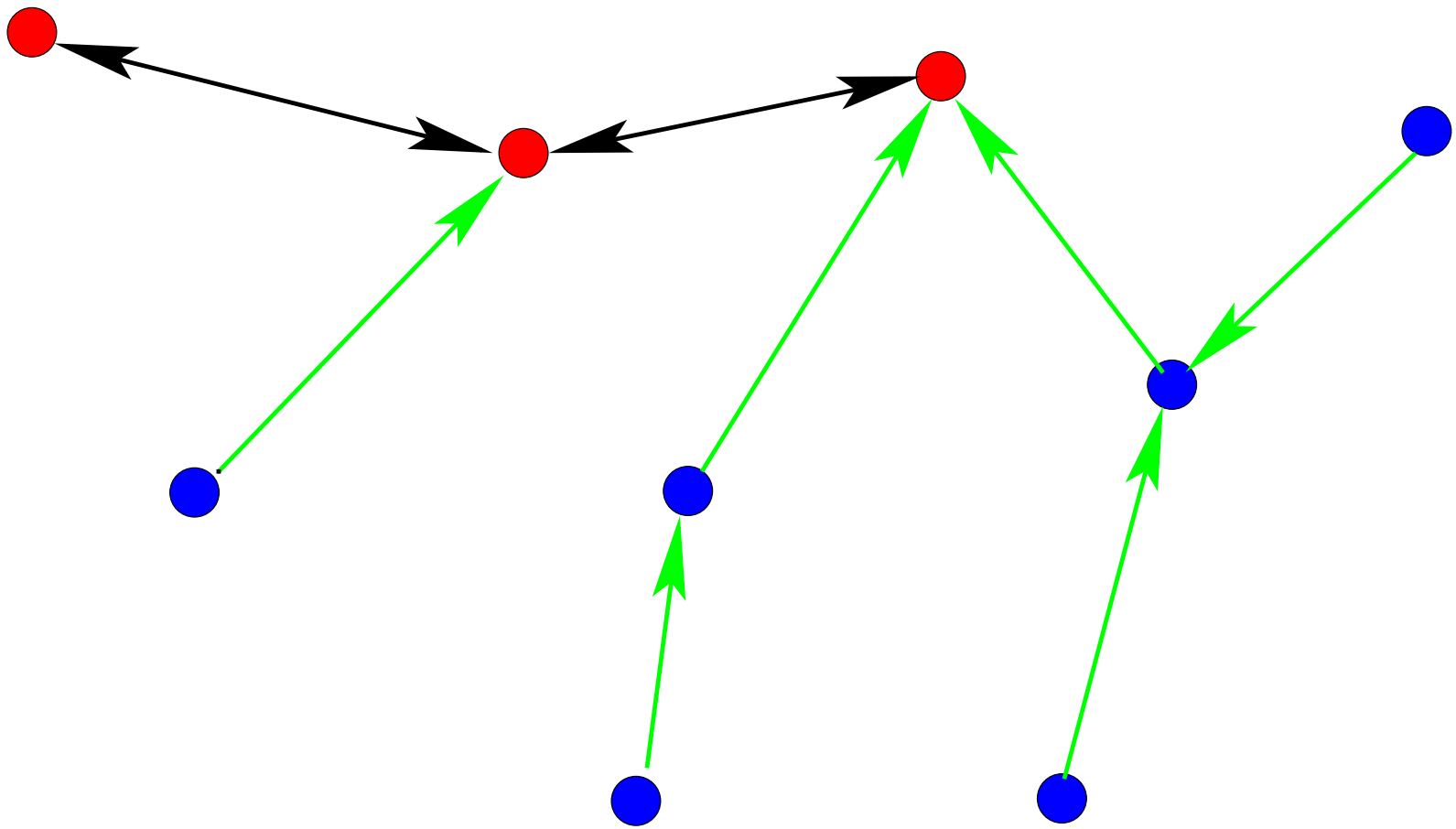


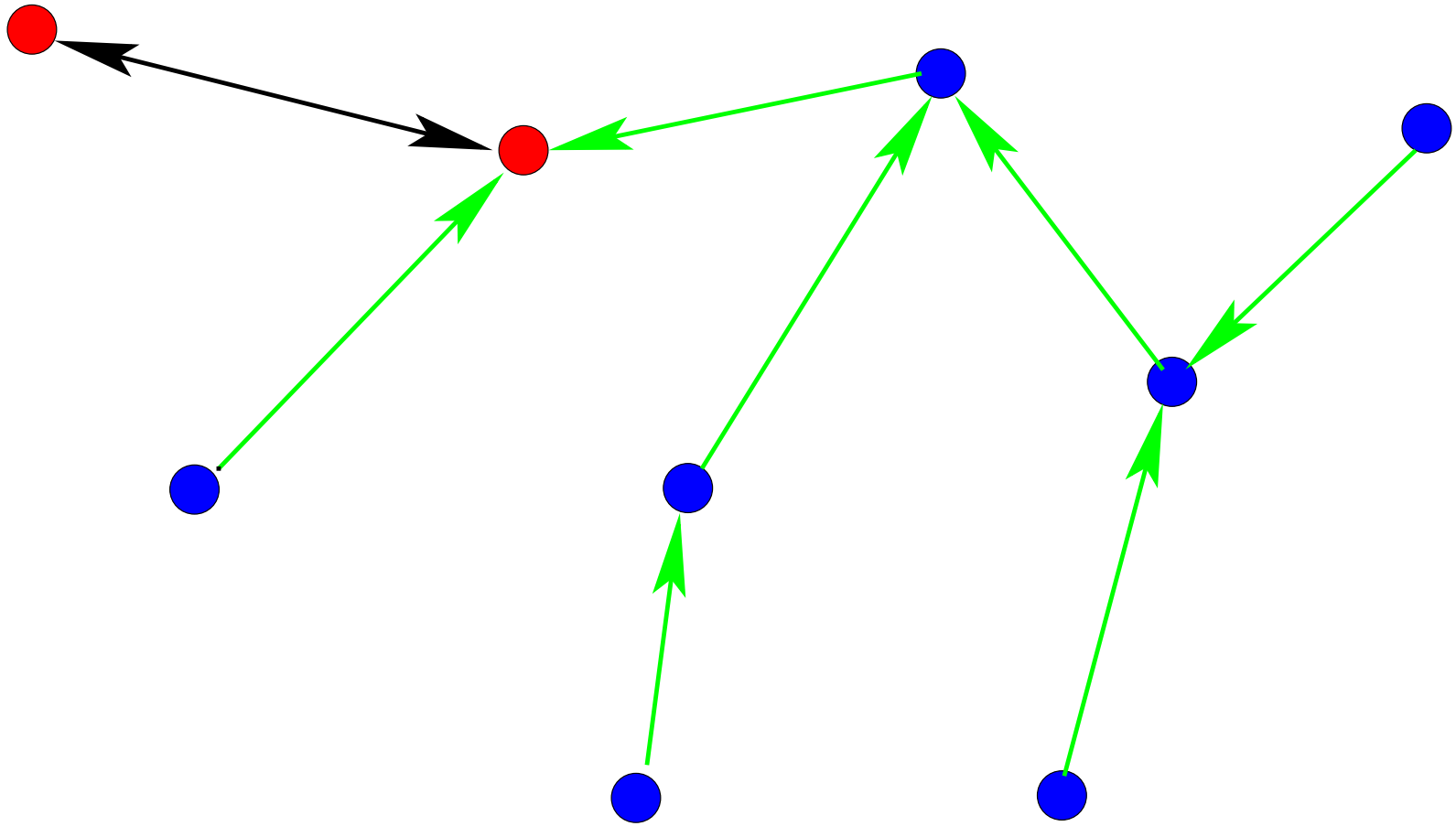


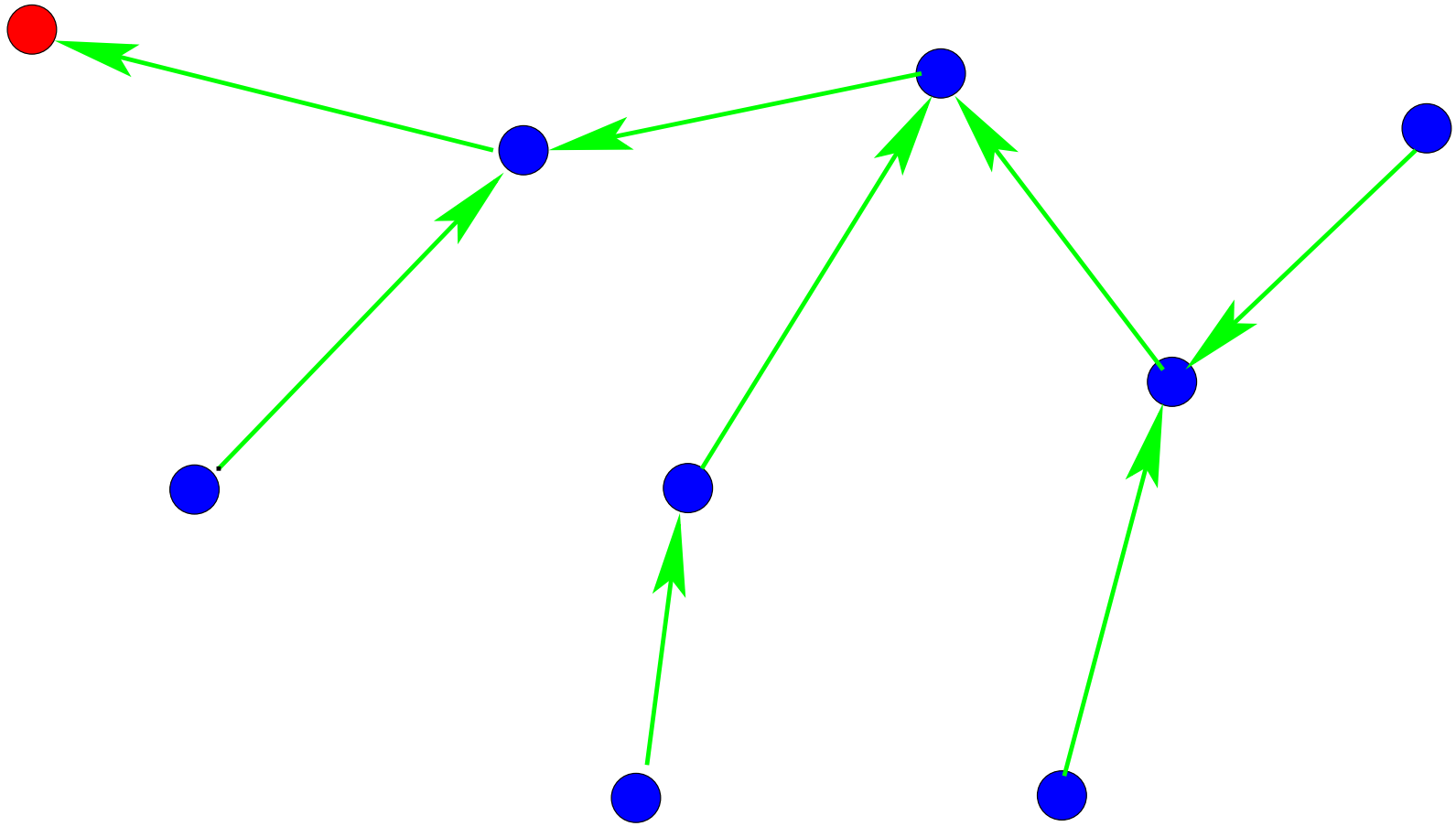












Development Strategy

- 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

Initial Model

sets: N

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

variables: l

inv0_1: $l \in N$

init

$l :\in N$

elect

any x **where**

$x \in N$

then

$l := x$

end

First Refinement: Defining the Free Tree

constant: g

axm_5: $\forall h, S \cdot \; h \cup h^{-1} = g \;\; h \cap h^{-1} = \varnothing \;\; S \subseteq h[S] \;\; \Rightarrow \;\; S = \varnothing$

axm1_1: $g \in N \leftrightarrow N$

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

axm1_3: $g \cap \mathrm{id}(N) = \varnothing$

axm1_4: $\forall s \cdot \; S \subseteq N \;\; S \neq \varnothing \;\; g[S] \subseteq S \;\; \Rightarrow \;\; N \subseteq S$

- **axm1_4** expresses that g is a strongly connected graph

- **axm1_5** expresses that any partition of g has no cycle

First Refinement: Extending the State

variable: l
n

inv1_1: $n \subseteq N$

inv1_2: $\forall s \cdot$ $S \subseteq n$
$S \neq \varnothing$
$(n \lhd g \rhd n)[S] \subseteq S$
$\Rightarrow$
$n \subseteq S$

- Variable n is a subset of N

- The graph reduced to n is still connected

First Refinement: the Events

init
$l :\in N$
$n := N$

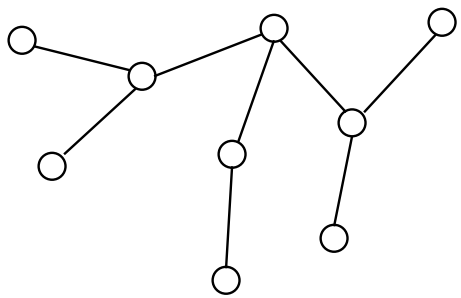
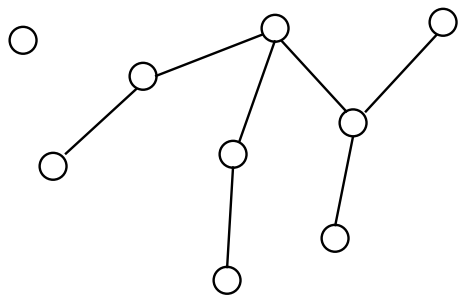
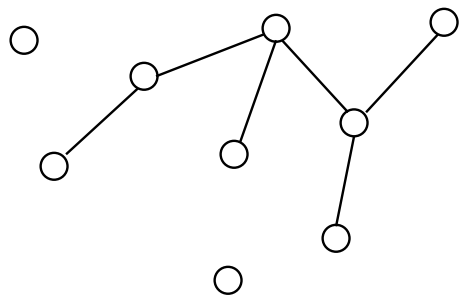
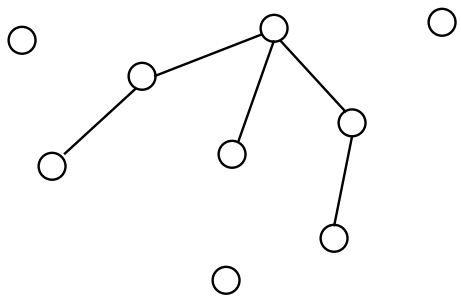
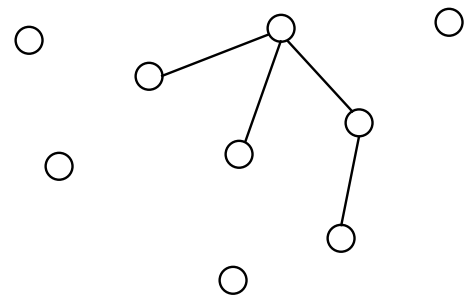
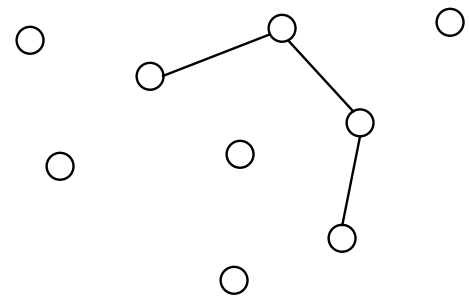
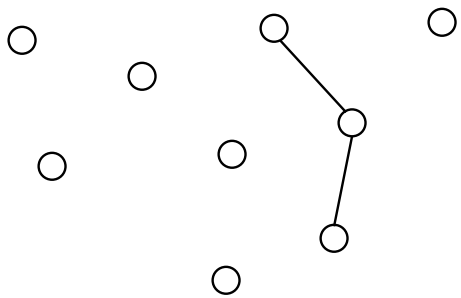
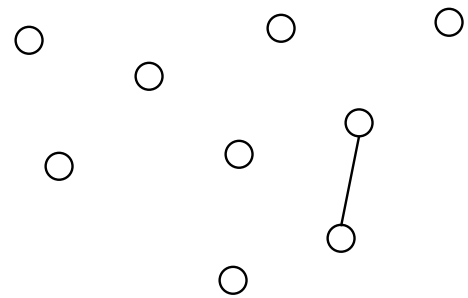
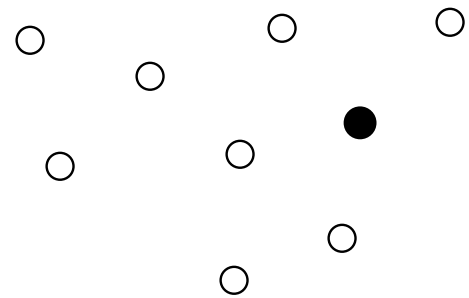
elect
any x **where**
$n = \{x\}$
then
$l := x$
end

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

Second Refinement: Extending the State with Messages

variables: l, n, m

inv2_1: $m \subseteq g$

inv2_2: $m \in n \pfun n$

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

Second Refinement: the Events

send_msg

any x, y **where**

$x \in n$

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

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

then

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

end

progress

any x, y **where**

$x \mapsto y \in m$

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

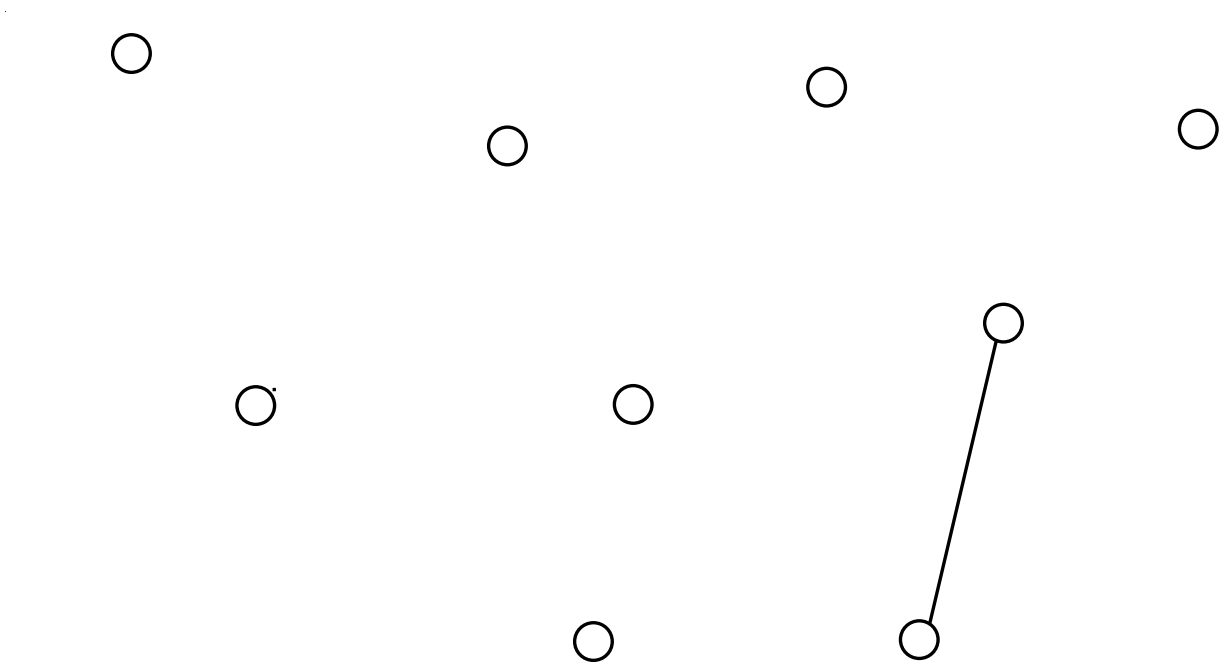
then

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

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

end

Third Refinement: the Problem of Contention



Third Refinement: the State

variables: l, n, m, c, bm

inv3_1: $c \subseteq g$

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

inv3_3: $m \cap c = \varnothing$

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

Third Refinement: the Events (1)

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

Third Refinement: the Events (2)

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
$c := \varnothing$
$bm := bm \setminus \{x, y\}$
end

Fourth Refinement: Simplification

variables: l, d, m, c, bm

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

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

Fourth Refinement: the Events (1)

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

elect
any x where
$x \in \mathrm{dom}(d)$
$d(x) = \varnothing$
then
$l := x$
end

send_msg
any x, y where
$x \in \mathrm{dom}(d)$
$d(x) = \{y\}$
$x \notin bm$
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
$d := (\{x\} \lhd d) \lhd\!\!+ \{y \mapsto d(y) \setminus \{x\}\}$
$m := m \setminus \{x \mapsto y\}$
$bm := bm \setminus \{x\}$
end

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

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

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

Fifth Refinement: the Events(1)

init

$$l :\in N$$

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

$$m := \varnothing$$

$$c := \varnothing$$

$$bm := \varnothing$$

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

Fifth Refinement: the Events(2)

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

Fifth Refinement: the Events(4)

progress

any x, y **where**

$x \mapsto y \in m$

$y \notin bm$

then

$d := (\{x\} \lhd d) \lhd\!\!+ \{y \mapsto d(y) \setminus \{x\}\}$

$r := (\{x\} \lhd r) \lhd\!\!+ \{y \mapsto r(y) - 1\}$

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

end