(d) Compare the state spaces of the verification runs of (b) and (c) and explain the difference in the size of the state space.

EXERCISE 15. We assume N processes in a ring topology, connected by unbounded queues. A process can only send messages in a clockwise manner. Initially, each process has a unique identifier *ident* (which is assumed to be a natural number). A process can be either active or relaying. Initially a process is active. In Peterson's leader election algorithm (1982) each process in the ring carries out the following task:

<u>*active:*</u>
$d := ident$;
do forever
begin
  /* start phase */
  $send(d)$;
  $receive(e)$;
  if $e = ident$ **then** announce elected;
  if $d > e$ **then** $send(d)$ **else** $send(e)$;
  $receive(f)$;
  if $f = ident$ **then** announce elected;
  if $e \geqslant max(d, f)$ **then** $d := e$ **else goto** *relay*;
end

<u>*relay:*</u>
do forever
begin
  $receive(d)$;
  if $d = ident$ **then** announce elected;
  $send(d)$
end

Model this leader election protocol in PROMELA (avoid invalid end-states!), and verify the following properties:

1. There is always at most one leader.
2. Always a leader will be elected eventually.

3. The elected leader will be the process with the highest number.

4. The maximum total amount of messages sent in order to elect a leader is at most $2N\lfloor \log_2 N \rfloor + N$. (*Hint:* choose an appropriate N such that $\log_2 N$ is easily computable.)

Check the above properties for two different assignments of process identities to processes.

2.12 Selected references

Linear temporal logic:

- A. Pnueli. The temporal logic of programs. *Proceedings 18th IEEE Symposium on Foundations of Computer Science*, pages 46–57, 1977.
- R. Gotzhein. Temporal logic and applications–a tutorial. *Computer Networks & ISDN Systems*, **24**: 203–218, 1992.
- Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems: Specification.* Springer-Verlag, 1992.

Past operators in temporal logic:

- O. Lichtenstein, A. Pnueli, and L. Zuck. The glory of the past. *Logics of Programs*, LNCS 193, pages 196–218, 1985.

Büchi automata and the connection between PLTL and LBAs:

- M. Vardi. An automata-theoretic approach to linear temporal logic. *Logics for Concurrency – Structure versus Automata*, LNCS 1043, pages 238–265, 1995.