Prof. Bernd Finkbeiner, Ph.D.
Peter Faymonville, M.Sc.
Michael Gerke, B.Sc.

Winter term 2011/2012
Problem Set 13

Verification

Please write the names of all group members on the solutions you hand in.

Problem 1: Invariance Diagrams

Consider the transition system DEQUE in Figure 1, representing a ring buffer for a double-ended queue. The buffer consists of five cells (represented by integer variables), which can be either free (0) or occupied (1). Starting with a single occupied cell x_1, we can toggle a cell's state if the states of its neighbors differ.

Θ	$x_1 = 1 \land x_2 = 0 \land x_3 = 0 \land x_4 = 0 \land x_5 = 0$
ρ_1	$x_5 + x_2 = 1 \land x_1' = 1 - x_1 \land pres(x_2, x_3, x_4, x_5)$
ρ_2	$x_1 + x_3 = 1 \land x_2' = 1 - x_2 \land pres(x_1, x_3, x_4, x_5)$
ρ_3	$x_2 + x_4 = 1 \land x_3' = 1 - x_3 \land pres(x_1, x_2, x_4, x_5)$
ρ_4	$x_3 + x_5 = 1 \land x_4' = 1 - x_4 \land pres(x_1, x_2, x_3, x_5)$
ρ_5	$x_4 + x_1 = 1 \land x_5' = 1 - x_5 \land pres(x_1, x_2, x_3, x_4)$

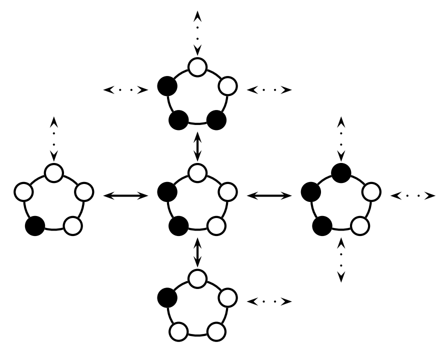

Figure 1: DEQUE transition system.

Create an INVARIANCE diagram which proves for the DEQUE system that the state with all cells occupied is not reachable.

Hints:

- Keep it simple - the verification diagram in the sample solution only has five nodes.
- State any auxiliary invariants needed to prove P-validity.
- You do not need to give proofs for individual verification conditions.