1 Proof

Lemma 1: $q2 \implies in \neq out$

- Initially $q2$ is false, lemma is true
- Only statement that progresses to $q2$ is $q1$ which requires $in \neq out$
- $in \neq out$ cannot become false between $q1$ and $q2$
  - Only other statement which can change in or out is $p4$
  - Since **lemma 2**, p cannot make $in \neq out$

Lemma 2: $p3..4 \implies out \neq (in + 1) \ mod \ N$

- Initially holds, as $p3..4$ is false
- Only statement that progresses to $p3..4$ is $p2$ which requires $out \neq (in + 1)$
- $out! = (in + 1) mod N$ cannot become false between $p2..p4$
- Thus cannot increment in such that $in = out$
  - Only statement which can change in or out is $q3$ $(out = out + 1)$
  - Thus can increment to $out + 1$, so $(out + 1) \neq (in + 1) \ mod \ N$