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**, $out \neq (in + 1)\ mod\ N$, so $p4$ cannot increment such that $out = in$

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 $out \neq (in + 1)$
  - Only statement which can change in or out is $q3$ ($out = out + 1$)
  - Since **lemma 1**, out cannot be incremented such that $out = in+1$, as this implies that $out = in$
- Thus can increment to $out + 1$, so $(out + 1) \neq (in + 1)\ mod\ N$
- $out \neq (in + 1)\ mod\ N$ cannot become false between $p2..p4$
- Thus cannot increment in such that $in = out$

1 Proof of Mutual Exclusion

Theorem 1: $\sim (p3 \wedge q2)$

- Assume $p3 \wedge q2$
- Using **lemma 1**: $q2 \implies in \neq out \longrightarrow \sim q2 \vee in \neq out$ (Negation of implication)
- Using **lemma 2**: $p3 \implies out \neq (in + 1)\ mod\ N \longrightarrow \sim p3 \vee out \neq (in + 1)\ mod\ N$ (Negation of implication)
- $(\sim q2 \vee in \neq out) \wedge (\sim p3 \vee out \neq (in + 1)\ mod\ N$
- If we assume $p3 \wedge q2$, then $\sim q2 = false$ and $\sim p3 = false$

- $(in \neq out) \wedge (out \neq (in + 1)\ mod\ N)$
- $in \neq (in + 1)\ mod\ N$
- Proof by contradiction
- Therefore theorem holds

2 Proof of Freedom from Starvation

Theorem 2: $\Box(p1 \implies \Diamond p3) \wedge \Box(q1 \implies \Diamond q2)$

$\Box(p1 \implies \Diamond p3)$

- From $p1$, progresses to $p2$
- To progress to $p3$, $out \neq (in + 1)\ mod\ N$ must be true, using **Lemma 2**
  - Since $p4$ is the only line that can change in, therefore the only variable that can update and break the await condition is out
  - The only line which can update out is $q3$
- Initially $in = out = 0$, so $0 \neq (0 + 1)\ mod\ N$ is true, thus progresses to $p3$
- For every subsequent run, the q process must run at least once (such that there is something in the buffer to read)

$\Box(q1 \implies \Diamond q2)$

- To progress to $q2$, $in \neq out$ must be true, using **Lemma 1**
- Initially $in = out = 0$, thus the process will block until p has been run at least once
- Once p has been run at least once, it will increment in, making $in \neq out$ true and allowing $q1$ to progress
  - Since $q3$ is the only line which can change out, therefore the only variable that can update and break the await condition is in
  - The only line that changes in is $p4$, thus p must enter it's critical section before q can run

- When an item is added, $in \neq out$ will be true and will progress to $q2$
- If $in = out$, the process will block until an item is added, which will increment in