Master's Thesis Exam
Verification of the Blocking and Non-Blocking Michael-Scott Queue Algorithms

Mathias Pedersen, 201808137
Advisor: Amin Timany

Aarhus University

June 2024

AARHUS UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

Overview of the Project and Contributions

- Initial goal was to prove soundness of the two M&S Queues
- The project later generalised the results to apply to queues in general
- In particular, three different specifications for queues were given
  - Sequential specification
    - Useful for sequential clients
  - Concurrent specification
    - Proves soundness of concurrent queues
    - Useful for some concurrent clients
  - HOCAP-style specification
    - Stronger specification, useful for more complex clients
    - Demonstrated with a specific queue client (queueAdd)
- It was demonstrated that the HOCAP-style specification derives the other two specifications
- Implementations of the M&S Queues in HeapLang were proven to meet the three specifications
  - In particular, both version are sound
- All proofs have been mechanised in the Coq proof assistant

Outline

Queue Specifications

Specifications for Queues

Assumptions on Queues

- Queues consists of initialize, enqueue, and dequeue
- initialize creates an empty queue: []
- enqueue adds a value, v, to the beginning of the queue xs_v: $v :: xs_v$
- dequeue depends on whether queue is empty:
  - If non-empty, $xs_v \mathbin{++} v$, remove v and return Some v
  - If empty, [], return None

Nature of Specifications

- Specifications written in Iris, a higher order CSL
- Expressed in terms of *Hoare triples*: $\{P\}\, e\, \{v.\Phi\ v\}$
- Hoare triples prove partial correctness of programs, e
- In particular: safety
- Idea: clients can use Hoare triples to prove results about their own code

Sequential Specification

Definition (Sequential Specification)

$$\exists\, \mathrm{isQueue}_S : \mathit{Val} \to \mathit{List\ Val} \to \mathit{SeqQgnames} \to \mathrm{Prop}.$$

$$\{\mathrm{True}\}\ \mathrm{initialize}\ ()\ \{v_q.\exists G.\ \mathrm{isQueue}_S(v_q, [], G)\}$$

$$\wedge \quad \forall v_q, v, xs_v, G.\ \{\mathrm{isQueue}_S(v_q, xs_v, G)\}\ \mathrm{enqueue}\ \ v_q\ \ v\ \{w.\ \mathrm{isQueue}_S(v_q, (v :: xs_v), G)\}$$

$$\wedge \quad \forall v_q, xs_v, G.\ \{\mathrm{isQueue}_S(v_q, xs_v, G)\}$$

$$\mathrm{dequeue}\ \ v_q$$

$$\left\{ w.\ \begin{array}{l} (xs_v = [] * w = \mathrm{None} * \mathrm{isQueue}_S(v_q, xs_v, G)) \vee \\ (\exists v, xs'_v.\ xs_v = xs'_v \mathbin{++} [v] * w = \mathrm{Some}\ v * \ \mathrm{isQueue}_S(v_q, xs'_v, G)) \end{array} \right\}$$

- The proposition $\mathrm{isQueue}_S(v_q, xs_v, G)$, states that value v_q represents the queue, which contains elements xs_v
- $G \in \mathit{SeqQgnames}$ is a collection of ghost names (depends on specific queue)
- Specification consists of three Hoare triples – one for each queue function
- Important: $\mathrm{isQueue}_S$ not required to be persistent!

Concurrent Specification

- To support concurrent clients, we shall require the queue predicate be persistent
- Tracking the contents of queue in the way that the sequential specification did doesn't work
- Threads will start disagreeing on contents of queue, as they have only local view of contents
- Give up on tracking contents for now
- Instead, promise that all elements satisfy client-defined predicate, Ψ

Definition (Concurrent Specification)

$$\exists\, \mathrm{isQueue_C} : (\mathit{Val} \to \mathrm{Prop}) \to \mathit{Val} \to \mathit{ConcQgnames} \to \mathrm{Prop}.$$

$$\forall \Psi : \mathit{Val} \to \mathrm{Prop}.$$

$$\begin{aligned} & \forall v_q, G.\ \mathrm{isQueue_C}(\Psi, v_q, G) \implies \Box\, \mathrm{isQueue_C}(\Psi, v_q, G) \\ \wedge \quad & \{\mathrm{True}\}\ \text{initialize}\ ()\ \{v_q.\exists G.\ \mathrm{isQueue_C}(\Psi, v_q, G)\} \\ \wedge \quad & \forall v_q, v, G.\ \{\mathrm{isQueue_C}(\Psi, v_q, G) * \Psi(v)\}\ \text{enqueue}\ \ v_q\ \ v\ \{w.\mathrm{True}\} \\ \wedge \quad & \forall v_q, G.\ \{\mathrm{isQueue_C}(\Psi, v_q, G)\}\ \text{dequeue}\ \ v_q\ \{w.w = \mathrm{None} \vee (\exists v.\ w = \mathrm{Some}\ v * \Psi(v))\} \end{aligned}$$

HOCAP-style Specification - Abstract State RA

- We will need a construction to allow clients to track contents of queue
- Idea: have two "views" of the abstract state of the queue

Authoritative view	**Fragmental view**
$\gamma \Mapsto_\bullet xs_v$	$\gamma \Mapsto_\circ xs_v$
Owned by queue	Owned by client

- Construction ensures:
  - authoritative and fragmental views always agree on abstract state of queue
  - views can only be updated in unison
- Implemented using the resource algebra: $\textsc{Auth}((\textsc{Frac} \times \textsc{Ag}(\mathit{List\ Val}))^?)$
- The desirables are captured by the following lemmas

Lemmas on the Abstract State RA

$$\vdash \Rrightarrow \exists \gamma.\, \gamma \Mapsto_\bullet xs_v * \gamma \Mapsto_\circ xs_v \qquad \text{(Abstract State Alloc)}$$

$$\gamma \Mapsto_\bullet xs_v' * \gamma \Mapsto_\circ xs_v \vdash xs_v = xs_v' \qquad \text{(Abstract State Agree)}$$

$$\gamma \Mapsto_\bullet xs_v' * \gamma \Mapsto_\circ xs_v \Rrightarrow \gamma \Mapsto_\bullet xs_v'' * \gamma \Mapsto_\circ xs_v'' \qquad \text{(Abstract State Update)}$$

HOCAP-style Specification

- Post-condition of initialize specification now gives fragmental view to clients
- Hoare triples for enqueue and dequeue are conditioned on view-shifts
- Clients must show that they can supply the fragmental view, so that the abstract (and concrete) state can be updated
- View-shifts and Hoare-triples parametrised by predicates P and Q
  - Client might have resources that need to be updated as a result of enqueue/dequeue
  - P is the clients resources before enqueue/dequeue and Q the resources after

Definition (HOCAP Specification)

$$
\begin{aligned}
&\exists\, \mathrm{isQueue} : \mathit{Val} \to \mathit{Qgnames} \to \mathrm{Prop}.\\
&\qquad \forall v_q, G.\ \mathrm{isQueue}(v_q, G) \implies \Box\, \mathrm{isQueue}(v_q, G)\\
&\wedge \quad \{\mathrm{True}\}\ \mathrm{initialize}\ ()\ \{v_q.\exists G.\ \mathrm{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_{\circ} []\}\\
&\wedge \quad \forall v_q, v, G, P, Q.\ \ (\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_{\bullet} xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright\, G.\gamma_{\mathrm{Abst}} \Mapsto_{\bullet} (v :: xs_v) * Q) \mathrel{-\!\!*}\\
&\qquad\qquad\qquad\qquad \{\mathrm{isQueue}(v_q, G) * P\}\ \mathrm{enqueue}\ \ v_q\ \ v\ \{w.Q\}\\
&\wedge \quad \forall v_q, G, P, Q.\\
&\qquad \left(\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_{\bullet} xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright \left(\begin{array}{l} (xs_v = [] * G.\gamma_{\mathrm{Abst}} \Mapsto_{\bullet} xs_v * Q(\mathrm{None}))\\ \vee \left(\begin{array}{l} \exists v, xs'_v.\ xs_v = xs'_v \mathbin{+\!\!+} [v] *\\ G.\gamma_{\mathrm{Abst}} \Mapsto_{\bullet} xs'_v * Q(\mathrm{Some}\ v) \end{array}\right) \end{array}\right)\right.\\
&\qquad \{\mathrm{isQueue}(v_q, G) * P\}\ \mathrm{dequeue}\ \ v_q\ \{w.Q(w)\}
\end{aligned}
$$

Queue Client - A PoC Client

- Idea: a minimal client complex enough to require HOCAP specification
- Uses parallel composition, so sequential specification insufficient
- Relies on dequeues not returning None, so concurrent specification insufficient
- HOCAP specification supports consistency and allows us to track queue contents, allowing us to exclude cases where dequeue returns None

$$\mathsf{unwrap}\ \ w \triangleq \mathsf{match}\ w\ \mathsf{with}\ \mathsf{None} \Rightarrow ()\ ()\ |\ \mathsf{Some}\ v \Rightarrow v\ \mathsf{end}$$

$$\mathsf{enqdeq}\ \ v_q\ \ c \triangleq \mathsf{enqueue}\ \ v_q\ \ c; \mathsf{unwrap}(\mathsf{dequeue}\ \ v_q)$$

$$\begin{aligned}
&\mathsf{queueAdd}\ \ a\ b \triangleq \\
&\quad \mathsf{let}\ v_q = \mathsf{initialize}\ ()\ \mathsf{in} \\
&\quad \mathsf{let}\ p = (\mathsf{enqdeq}\ \ v_q\ \ a) \,||\, (\mathsf{enqdeq}\ \ v_q\ \ b)\ \mathsf{in} \\
&\quad \mathsf{fst}\ p + \mathsf{snd}\ p
\end{aligned}$$

Queue Client - A PoC Client (continued)

Lemma (QueueAdd Specification)

$$\forall a, b \in \mathbb{Z}.\ \{True\}\ \text{queueAdd}\ \ a\ b\,\{v.v = a + b\}$$

- Proof idea: Create invariant capturing possible states of queue contents
- Tokens are used to reason about which state we are in

Definition (Invariant for QueueAdd)

$$\begin{aligned} I_{QA}(G, Ga, a, b) \triangleq\ & G.\gamma_{\text{Abst}} \Mapsto_\circ [\,] \ast \text{TokD1}\ \ Ga \ast \text{TokD2}\ \ Ga \lor \\ & G.\gamma_{\text{Abst}} \Mapsto_\circ [a] \ast \text{TokA}\ \ Ga \ast (\text{TokD1}\ \ Ga \lor \text{TokD2}\ \ Ga) \lor \\ & G.\gamma_{\text{Abst}} \Mapsto_\circ [b] \ast \text{TokB}\ \ Ga \ast (\text{TokD1}\ \ Ga \lor \text{TokD2}\ \ Ga) \lor \\ & G.\gamma_{\text{Abst}} \Mapsto_\circ [a; b] \ast \text{TokA}\ \ Ga \ast \text{TokB}\ \ Ga \lor \\ & G.\gamma_{\text{Abst}} \Mapsto_\circ [b; a] \ast \text{TokB}\ \ Ga \ast \text{TokA}\ \ Ga \lor \end{aligned}$$

The Two-Lock Michael-Scott Queue

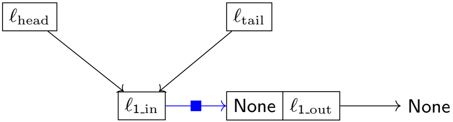
Implementation: initialize

- The queue data structure is a linked list
- A node x in the linked list is a triple, $x = (\ell_{\text{in}}, w, \ell_{\text{out}})$ with $\ell_{\text{in}} \mapsto (w, \ell_{\text{out}})$
- We use the following notation for nodes

$$\mathsf{in}(x) = \ell_{\text{in}} \qquad \mathsf{val}(x) = w \qquad \mathsf{out}(x) = \ell_{\text{out}}$$

- The initialize function first creates an initial head node, x_{head}
- Then, a lock protecting the head pointer, and a lock protecting the tail pointer
- Finally, it creates the head and tail pointers, ℓ_{head} and ℓ_{tail}, both pointing to x_{head}

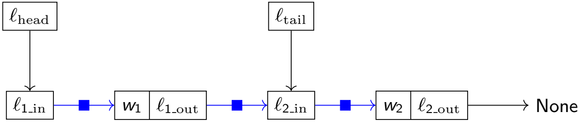
```
initialize ≜
  let node = ref (None, ref (None)) in
  let H_lock = newLock() in
  let T_lock = newLock() in
  ref ((ref (node), ref (node)), (H_lock, T_lock))
```



Implementation: enqueue

- The enqueue function consists of the following steps
  1. Create a new node, x_{new}, containing value to be enqueued
  2. Acquire the tail lock
  3. Add x_{new} to linked list
  4. Swing tail pointer to x_{new}
  5. Release the tail lock
- Once a node is enqueued, its position in the linked list is fixed
- Adding and swinging not atomic $\rightarrow$ Tail node is either last or second last
- dequeue ignores tail pointer $\rightarrow$ Tail node can lag behind head node

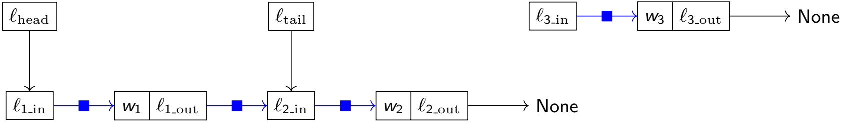
```
enqueue Q value ≜
  let node = ref (Some value, ref (None)) in
  acquire(snd(snd(! Q)));
  snd(!(!(snd(fst(! Q))))) ← node;
  snd(fst(! Q)) ← node;
  release(snd(snd(! Q)))
```



Implementation: enqueue

- The enqueue function consists of the following steps
  1. Create a new node, x_{new}, containing value to be enqueued
  2. Acquire the tail lock
  3. Add x_{new} to linked list
  4. Swing tail pointer to x_{new}
  5. Release the tail lock
- Once a node is enqueued, its position in the linked list is fixed
- Adding and swinging not atomic $\rightarrow$ Tail node is either last or second last
- dequeue ignores tail pointer $\rightarrow$ Tail node can lag behind head node

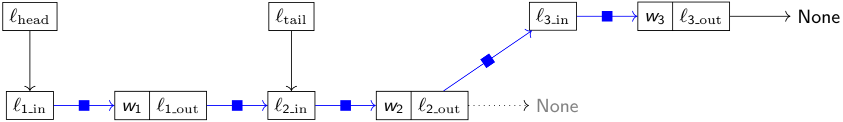
```
enqueue  Q value ≜
  let node = ref (Some value, ref (None)) in
  acquire(snd(snd(! Q)));
  snd(!(!(snd(fst(! Q))))) ← node;
  snd(fst(! Q)) ← node;
  release(snd(snd(! Q)))
```



Implementation: enqueue

- The enqueue function consists of the following steps
  1. Create a new node, x_{new}, containing value to be enqueued
  2. Acquire the tail lock
  3. Add x_{new} to linked list
  4. Swing tail pointer to x_{new}
  5. Release the tail lock
- Once a node is enqueued, its position in the linked list is fixed
- Adding and swinging not atomic $\rightarrow$ Tail node is either last or second last
- dequeue ignores tail pointer $\rightarrow$ Tail node can lag behind head node

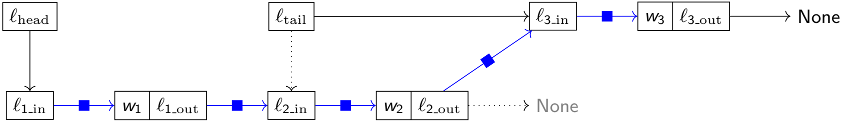
```
enqueue  Q value ≜
  let node = ref (Some value, ref (None)) in
  acquire(snd(snd(! Q)));
  snd(!(!(snd(fst(! Q))))) ← node;
  snd(fst(! Q)) ← node;
  release(snd(snd(! Q)))
```



Implementation: enqueue

- The enqueue function consists of the following steps
  1. Create a new node, x_{new}, containing value to be enqueued
  2. Acquire the tail lock
  3. Add x_{new} to linked list
  4. Swing tail pointer to x_{new}
  5. Release the tail lock
- Once a node is enqueued, its position in the linked list is fixed
- Adding and swinging not atomic $\rightarrow$ Tail node is either last or second last
- dequeue ignores tail pointer $\rightarrow$ Tail node can lag behind head node

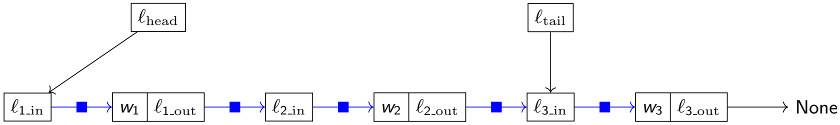
```
enqueue  Q value ≜
  let node = ref (Some value, ref (None)) in
  acquire(snd(snd(! Q)));
  snd(!(!(snd(fst(! Q))))) ← node;
  snd(fst(! Q)) ← node;
  release(snd(snd(! Q)))
```



Implementation: dequeue

- The dequeue function checks if queue is empty
  - If empty, return *None*
  - Else, swing head pointer to new head, and return dequeued value
- Dequeued node not freed $\rightarrow$ linked list only grows

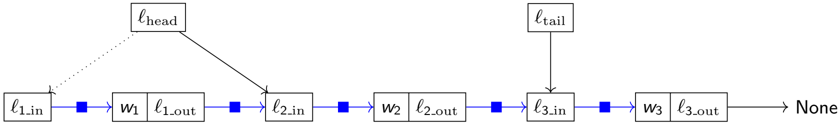
```
dequeue  Q ≜
   acquire(fst(snd(! Q)));
   let node = !(fst(fst(! Q))) in
   let new_head = !(snd(! node)) in
   if new_head = None then
      release(fst(snd(! Q)));
      None
   else
      let value = fst(! new_head) in
      fst(fst(! Q)) ← new_head;
      release(fst(snd(! Q)));
      value
```



Implementation: dequeue

- The dequeue function checks if queue is empty
  - If empty, return *None*
  - Else, swing head pointer to new head, and return dequeued value
- Dequeued node not freed → linked list only grows

```
dequeue  Q ≜
  acquire(fst(snd(! Q)));
  let node = !(fst(fst(! Q))) in
  let new_head = !(snd(! node)) in
  if new_head = None then
    release(fst(snd(! Q)));
    None
  else
    let value = fst(! new_head) in
    fst(fst(! Q)) ← new_head;
    release(fst(snd(! Q)));
    value
```



Proving that the Two-Lock Michael-Scott Queue Satisfies the HOCAP-style Specification

The isLL Predicate

▶format slide◀

- Idea: express the structure of the linked list in terms of points-to predicates
- Also captures persistent and non-persistent parts of the linked list

Definition (Linked List Chain Predicate)

$$\begin{aligned}
\mathrm{isLL_chain}([]) &\triangleq \mathrm{True} \\
\mathrm{isLL_chain}([x]) &\triangleq \mathrm{in}(x) \mapsto^{\square} (\mathrm{val}(x), \mathrm{out}(x)) \\
\mathrm{isLL_chain}(x :: x' :: xs) &\triangleq \mathrm{in}(x) \mapsto^{\square} (\mathrm{val}(x), \mathrm{out}(x)) * \mathrm{out}(x') \mapsto^{\square} \mathrm{in}(x) * \mathrm{isLL_chain}(x' :: x
\end{aligned}$$

Definition (Linked List Predicate)

$$\begin{aligned}
\mathrm{isLL}([]) &\triangleq \mathrm{True} \\
\mathrm{isLL}(x :: xs) &\triangleq \mathrm{out}(x) \mapsto \mathrm{None} * \mathrm{isLL_chain}(x :: xs)
\end{aligned}$$

Example

Invariant

- Queue predicate must be persistent (according to specification)
- The queue relies on non-persistent resources (e.g. $\ell_{\text{head}} \mapsto \ell_{\text{in}}$)
- Solution: identify an *invariant* (persistent), describing the resources
  - Contains abstract state of queue – existentially quantified as it can change
  - Defines structure of the concrete linked list, *xsc*
  - Asserts relation between abstract state and concrete state
  - Identifies four possible queue states – see next slide

Definition (Two-Lock M&S Queue HOCAP Invariant)

$$
\begin{aligned}
\mathsf{I}_{\mathsf{TLH}}(\ell_{\text{head}}, \ell_{\text{tail}}, G) \triangleq\ & \exists xs_v.\ G.\gamma_{\text{Abst}} \Mapsto_\bullet xs_v * \\
& \exists xs, xs_{\text{queue}}, xs_{\text{old}}, x_{\text{head}}, x_{\text{tail}}. \\
& xs = xs_{\text{queue}} +\!\!+ [x_{\text{head}}] +\!\!+ xs_{\text{old}} * \\
& \mathsf{isLL}(xs) * \\
& \mathsf{projVal}(xs_{\text{queue}}) = \mathsf{wrapSome}(xs_v) * \\
& \ldots
\end{aligned}
$$

Invariant (Queue States)

- Two locks $\rightarrow$ four queue states: **Static**, **Enqueue**, **Dequeue**, and **Both**
- Idea: the enqueueing thread keeps half of tail pointer between invariant openings
- Guarantees that the pointer is not updated (full pointer needed for update)
- Similarly for the dequeueing thread
- **Enqueue** and **Both** also captures "gap" between adding x_{new} and swinging ℓ_{tail}
- Tokens used to reason about which state queue is in

Definition (Two-Lock M&S Queue HOCAP Invariant – continued)

$$
\begin{aligned}
&\dots \\
&\quad \ell_{\mathrm{head}} \mapsto \mathsf{in}(x_{\mathrm{head}}) * \ell_{\mathrm{tail}} \mapsto \mathsf{in}(x_{\mathrm{tail}}) * \mathsf{isLast}(x_{\mathrm{tail}}, xs) * && \textbf{(Static)} \\
&\quad \mathsf{TokNE}\ G * \mathsf{TokND}\ G * \mathsf{TokUpdated}\ G \\
&\vee\ \ell_{\mathrm{head}} \mapsto \mathsf{in}(x_{\mathrm{head}}) * \ell_{\mathrm{tail}} \mapsto^{\frac{1}{2}} \mathsf{in}(x_{\mathrm{tail}}) * && \textbf{(Enqueue)} \\
&\quad (\mathsf{isLast}(x_{\mathrm{tail}}, xs) * \mathsf{TokBefore}\ G \vee \mathsf{isSndLast}(x_{\mathrm{tail}}, xs) * \mathsf{TokAfter}\ G) * \\
&\quad \mathsf{TokE}\ G * \mathsf{TokND}\ G \\
&\vee\ \ell_{\mathrm{head}} \mapsto^{\frac{1}{2}} \mathsf{in}(x_{\mathrm{head}}) * \ell_{\mathrm{tail}} \mapsto \mathsf{in}(x_{\mathrm{tail}}) * \mathsf{isLast}(x_{\mathrm{tail}}, xs) * && \textbf{(Dequeue)} \\
&\quad \mathsf{TokNE}\ G * \mathsf{TokD}\ G * \mathsf{TokUpdated}\ G \\
&\vee\ \ell_{\mathrm{head}} \mapsto^{\frac{1}{2}} \mathsf{in}(x_{\mathrm{head}}) * \ell_{\mathrm{tail}} \mapsto^{\frac{1}{2}} \mathsf{in}(x_{\mathrm{tail}}) * && \textbf{(Both)} \\
&\quad (\mathsf{isLast}(x_{\mathrm{tail}}, xs) * \mathsf{TokBefore}\ G \vee \mathsf{isSndLast}(x_{\mathrm{tail}}, xs) * \mathsf{TokAfter}\ G) * \\
&\quad \mathsf{TokE}\ G * \mathsf{TokD}\ G
\end{aligned}
$$

Queue Predicate

- HOCAP-style specification requires the existence of a persistent queue predicate
- We define it in terms of our invariant

Definition (Two-Lock M&S Queue - isQueue Predicate)

$$\begin{aligned}\mathsf{isQueue}(v_q, G) \triangleq\; & \exists \ell_{\mathrm{queue}}, \ell_{\mathrm{head}}, \ell_{\mathrm{tail}} \in \mathit{Loc}.\ \exists h_{\mathrm{lock}}, t_{\mathrm{lock}} \in \mathit{Val}. \\ & v_q = \ell_{\mathrm{queue}} * \ell_{\mathrm{queue}} \mapsto^{\square} ((\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}), (h_{\mathrm{lock}}, t_{\mathrm{lock}})) * \\ & \boxed{\mathrm{I}_{\mathsf{TLH}}(\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}, G)}^{\mathcal{N}.\mathit{queue}} * \\ & \mathsf{isLock}(G.\gamma_{\mathrm{Hlock}}, h_{\mathrm{lock}}, \mathsf{TokD}\ \ G) * \\ & \mathsf{isLock}(G.\gamma_{\mathrm{Tlock}}, t_{\mathrm{lock}}, \mathsf{TokE}\ \ G)\end{aligned}$$

- The queue predicate is persistent, as all its constituents are
- Proving that TLMSQ satisfies the HOCAP-style specification then consists of proving the Hoare triples for initialize, enqueue, and dequeue
- We here focus on enqueue

Proof Sketch of the Hoare Triple for enqueue

$$\forall v_q, v, G, P, Q. \quad \big(\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet (v :: xs_v) * Q\big) -\!\!* \\ \{\mathsf{isQueue}(v_q, G) * P\}\ \mathsf{enqueue}\ \ v_q\ \ v\ \{w.Q\}$$

Proof Sketch of the Hoare Triple for enqueue

$$\forall v_q, v, G, P, Q.\quad \left(\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Rrightarrow_\bullet xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i^\uparrow} \triangleright G.\gamma_{\mathrm{Abst}} \Rrightarrow_\bullet (v :: xs_v) * Q\right) \twoheadrightarrow \{\mathsf{isQueue}(v_q, G) * P\}\ \mathsf{enqueue}\ \ v_q\ \ v\ \{w.Q\}$$

(Proof)

Assume the view-shift, and the persistent information in $\mathsf{isQueue}(v_q, Qgnames)$:

- $v_q = \ell_{\mathrm{queue}} * \ell_{\mathrm{queue}} \mapsto^{\square} ((\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}), (h_{\mathrm{lock}}, t_{\mathrm{lock}}))$
- $\boxed{I_{\mathsf{TLH}}(\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}, G)}^{\mathcal{N}.queue}$
- $\mathsf{isLock}(G.\gamma_{\mathrm{Tlock}}, t_{\mathrm{lock}}, \mathsf{TokE}\ \ G)$

Proof Sketch of the Hoare Triple for enqueue

$$\forall v_q, v, G, P, Q. \quad \begin{array}{l}(\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Rrightarrow_{\bullet} xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright G.\gamma_{\mathrm{Abst}} \Rrightarrow_{\bullet} (v :: xs_v) * Q) \twoheadrightarrow \\ \{\mathsf{isQueue}(v_q, G) * P\}\ \mathsf{enqueue}\ \ v_q\ \ v\, \{w.Q\}\end{array}$$

(Proof)

Assume the view-shift, and the persistent information in $\mathsf{isQueue}(v_q, Qgnames)$:

- $v_q = \ell_{\mathrm{queue}} * \ell_{\mathrm{queue}} \mapsto^{\square} ((\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}), (h_{\mathrm{lock}}, t_{\mathrm{lock}}))$
- $\boxed{\mathsf{I}_{\mathsf{TLH}}(\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}, G)}^{\mathcal{N}.queue}$
- $\mathsf{isLock}(G.\gamma_{\mathrm{Tlock}}, t_{\mathrm{lock}}, \mathsf{TokE}\ \ G)$

$\{P\}$

$\quad$ **let** $node = $ **ref** (Some v, **ref** (None)) **in** $\quad$ (create node x_{new})

$\{P * \mathsf{out}(x_{\mathrm{new}}) \mapsto \mathsf{None}\}$

Proof Sketch of the Hoare Triple for enqueue

$\forall v_q, v, G, P, Q.\quad (\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_{\bullet} xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright G.\gamma_{\mathrm{Abst}} \Mapsto_{\bullet} (v :: xs_v) * Q) \twoheadrightarrow$
$\{\mathrm{isQueue}(v_q, G) * P\}$ enqueue v_q v $\{w.Q\}$

(Proof)

Assume the view-shift, and the persistent information in $\mathrm{isQueue}(v_q, Qgnames)$:

- $v_q = \ell_{\mathrm{queue}} * \ell_{\mathrm{queue}} \mapsto^{\square} ((\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}), (h_{\mathrm{lock}}, t_{\mathrm{lock}}))$
- $\boxed{\mathrm{I_{TLH}}(\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}, G)}^{\mathcal{N}.queue}$
- $\mathrm{isLock}(G.\gamma_{\mathrm{Tlock}}, t_{\mathrm{lock}}, \mathrm{TokE}\ \ G)$

$\{P\}$

let $node$ = ref (Some v, ref (None)) in (create node x_{new})

$\{P * \mathrm{out}(x_{\mathrm{new}}) \mapsto \mathrm{None}\}$

acquire(snd(snd(! v_q))); (acquire tail lock)

$\{P * \mathrm{out}(x_{\mathrm{new}}) \mapsto \mathrm{None} * \mathrm{TokE}\ \ G\}$

Proof Sketch of the Hoare Triple for enqueue

$\forall v_q, v, G, P, Q.\quad (\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet (v :: xs_v) * Q) \mathrel{-\!\!*}$
$\{\text{isQueue}(v_q, G) * P\}$ enqueue $v_q\ v\ \{w.Q\}$

(Proof)

Assume the view-shift, and the persistent information in isQueue(v_q, *Qgnames*):

- $v_q = \ell_{\mathrm{queue}} * \ell_{\mathrm{queue}} \mapsto^{\Box} ((\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}), (h_{\mathrm{lock}}, t_{\mathrm{lock}}))$
- $\boxed{\mathrm{I_{TLH}}(\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}, G)}^{\mathcal{N}.queue}$
- isLock($G.\gamma_{\mathrm{Tlock}}, t_{\mathrm{lock}}$, TokE G)

$\{P\}$

let *node* = ref (Some v, ref (None)) in (create node x_{new})

$\{P * \text{out}(x_{\mathrm{new}}) \mapsto \text{None}\}$

acquire(snd(snd(! v_q))); (acquire tail lock)

$\{P * \text{out}(x_{\mathrm{new}}) \mapsto \text{None} * \text{TokE}\ \ G\}$

e_t = !(snd(fst(! v_q))) (find current tail, x_{tail}. $\mathrm{I_{TLH}}$: **Static**/**Dequeue** $\to$ **Enqueue**/**Both** (before))

$\{P * \text{out}(x_{\mathrm{new}}) \mapsto \text{None} * \ell_{\mathrm{tail}} \mapsto^{\frac{1}{2}} \text{in}(x_{\mathrm{tail}}) * \text{TokNE}\ \ G * \text{TokAfter}\ \ G\}$

Proof Sketch of the Hoare Triple for enqueue

$$\forall v_q, v, G, P, Q.\quad (\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet (v :: xs_v) * Q) \mathrel{-\!\!*} \{\mathrm{isQueue}(v_q, G) * P\}\ \mathrm{enqueue}\ \ v_q\ \ v\ \{w.Q\}$$

(Proof)

Assume the view-shift, and the persistent information in $\mathrm{isQueue}(v_q, Qgnames)$:

- $v_q = \ell_{\mathrm{queue}} * \ell_{\mathrm{queue}} \mapsto^{\square} ((\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}), (h_{\mathrm{lock}}, t_{\mathrm{lock}}))$
- $\boxed{\mathrm{I_{TLH}}(\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}, G)}^{\mathcal{N}.queue}$
- $\mathrm{isLock}(G.\gamma_{\mathrm{Tlock}}, t_{\mathrm{lock}}, \mathrm{TokE}\ \ G)$

$\{P\}$

let $node$ = ref (Some v, ref (None)) in (create node x_{new})

$\{P * \mathrm{out}(x_{\mathrm{new}}) \mapsto \mathrm{None}\}$

acquire(snd(snd(! v_q))); (acquire tail lock)

$\{P * \mathrm{out}(x_{\mathrm{new}}) \mapsto \mathrm{None} * \mathrm{TokE}\ \ G\}$

e_t = !(snd(fst(! v_q))) (find current tail, x_{tail}. $\mathrm{I_{TLH}}$: **Static**/**Dequeue** $\rightarrow$ **Enqueue**/**Both** (before))

$\{P * \mathrm{out}(x_{\mathrm{new}}) \mapsto \mathrm{None} * \ell_{\mathrm{tail}} \mapsto^{\frac{1}{2}} \mathrm{in}(x_{\mathrm{tail}}) * \mathrm{TokNE}\ \ G * \mathrm{TokAfter}\ \ G\}$

snd(!(e_t)) $\leftarrow$ $node$; (make x_{tail} point to x_{new}. $\mathrm{I_{TLH}}$: **Enqueue**/**Both** (before) $\rightarrow$ **Enqueue**/**Both** (after))

$\{Q * \ell_{\mathrm{tail}} \mapsto^{\frac{1}{2}} \mathrm{in}(x_{\mathrm{tail}}) * \mathrm{TokNE}\ \ G * \mathrm{TokBefore}\ \ G\}$

Proof Sketch of the Hoare Triple for enqueue

$$\forall v_q, v, G, P, Q.\quad (\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet (v :: xs_v) * Q) \twoheadrightarrow$$
$$\{\mathsf{isQueue}(v_q, G) * P\}\ \mathsf{enqueue}\ \ v_q\ \ v\ \{w.Q\}$$

(Proof)

Assume the view-shift, and the persistent information in isQueue(v_q, *Qgnames*):

- $v_q = \ell_{\mathrm{queue}} * \ell_{\mathrm{queue}} \mapsto^{\square} ((\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}), (h_{\mathrm{lock}}, t_{\mathrm{lock}}))$
- $\boxed{\mathsf{I}_{\mathsf{TLH}}(\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}, G)}^{\mathcal{N}.queue}$
- $\mathsf{isLock}(G.\gamma_{\mathrm{Tlock}}, t_{\mathrm{lock}}, \mathsf{TokE}\ \ G)$

$\{P\}$

let *node* = ref (Some v, ref (None)) in (create node x_{new})

$\{P * \mathsf{out}(x_{\mathrm{new}}) \mapsto \mathsf{None}\}$

acquire(snd(snd(! v_q))); (acquire tail lock)

$\{P * \mathsf{out}(x_{\mathrm{new}}) \mapsto \mathsf{None} * \mathsf{TokE}\ \ G\}$

e_t = !(snd(fst(! v_q))) (find current tail, x_{tail}. $\mathsf{I}_{\mathsf{TLH}}$: **Static**/**Dequeue** $\to$ **Enqueue**/**Both** (before))

$\{P * \mathsf{out}(x_{\mathrm{new}}) \mapsto \mathsf{None} * \ell_{\mathrm{tail}} \mapsto^{\frac{1}{2}} \mathsf{in}(x_{\mathrm{tail}}) * \mathsf{TokNE}\ \ G * \mathsf{TokAfter}\ \ G\}$

snd(!(e_t)) $\leftarrow$ *node*; (make x_{tail} point to x_{new}. $\mathsf{I}_{\mathsf{TLH}}$: **Enqueue**/**Both** (before) $\to$ **Enqueue**/**Both** (after))

$\{Q * \ell_{\mathrm{tail}} \mapsto^{\frac{1}{2}} \mathsf{in}(x_{\mathrm{tail}}) * \mathsf{TokNE}\ \ G * \mathsf{TokBefore}\ \ G\}$

snd(fst(! v_q)) $\leftarrow$ *node*; (swing tail pointer to x_{new}. $\mathsf{I}_{\mathsf{TLH}}$: **Enqueue**/**Both** (after) $\to$ **Static**/**Dequeue**)

$\{Q * \mathsf{TokE}\ \ G\}$

Proof Sketch of the Hoare Triple for enqueue

$$\forall v_q, v, G, P, Q. \quad (\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet (v :: xs_v) * Q) \twoheadrightarrow$$
$$\{\mathrm{isQueue}(v_q, G) * P\}\ \mathrm{enqueue}\ \ v_q\ \ v\ \{w.Q\}$$

(Proof)

Assume the view-shift, and the persistent information in $\mathrm{isQueue}(v_q, \mathit{Qgnames})$:

- $v_q = \ell_{\mathrm{queue}} * \ell_{\mathrm{queue}} \mapsto^{\square} ((\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}), (h_{\mathrm{lock}}, t_{\mathrm{lock}}))$
- $\boxed{\mathrm{I}_{\mathrm{TLH}}(\ell_{\mathrm{head}}, \ell_{\mathrm{tail}}, G)}^{\mathcal{N}.queue}$
- $\mathrm{isLock}(G.\gamma_{\mathrm{Tlock}}, t_{\mathrm{lock}}, \mathrm{TokE}\ \ G)$

$\{P\}$

  let *node* = ref (Some v, ref (None)) in (create node x_{new})

$\{P * \mathrm{out}(x_{\mathrm{new}}) \mapsto \mathrm{None}\}$

  acquire(snd(snd(! v_q))); (acquire tail lock)

$\{P * \mathrm{out}(x_{\mathrm{new}}) \mapsto \mathrm{None} * \mathrm{TokE}\ \ G\}$

  e_t = !(snd(fst(! v_q))) (find current tail, x_{tail}. $\mathrm{I}_{\mathrm{TLH}}$: **Static**/**Dequeue** → **Enqueue**/**Both** (before))

$\{P * \mathrm{out}(x_{\mathrm{new}}) \mapsto \mathrm{None} * \ell_{\mathrm{tail}} \mapsto^{\frac{1}{2}} \mathrm{in}(x_{\mathrm{tail}}) * \mathrm{TokNE}\ \ G * \mathrm{TokAfter}\ \ G\}$

  snd(!(e_t)) ← *node*; (make x_{tail} point to x_{new}. $\mathrm{I}_{\mathrm{TLH}}$: **Enqueue**/**Both** (before) → **Enqueue**/**Both** (after))

$\{Q * \ell_{\mathrm{tail}} \mapsto^{\frac{1}{2}} \mathrm{in}(x_{\mathrm{tail}}) * \mathrm{TokNE}\ \ G * \mathrm{TokBefore}\ \ G\}$

  snd(fst(! v_q)) ← *node*; (swing tail pointer to x_{new}. $\mathrm{I}_{\mathrm{TLH}}$: **Enqueue**/**Both** (after) → **Static**/**Dequeue**)

$\{Q * \mathrm{TokE}\ \ G\}$

  release(snd(snd(! v_q))) (release tail lock)

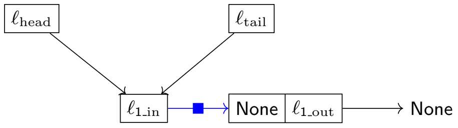
$\{Q\}$

The Lock-Free Michael-Scott Queue

Implementation: initialize

- Queue data structure is still a linked list
- The lock-free versions of initialize, enqueue, and dequeue perform the same manipulations of the linked list as two-lock versions
- Difference is how the manipulations take place – now with CAS instructions
- No longer need locks

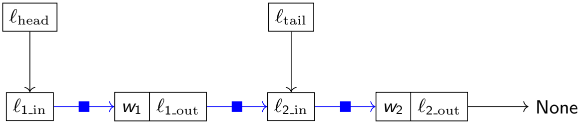
initialize $\triangleq$
  let *node* = **ref** (None, **ref** (None)) **in**
  ref (**ref** (*node*), **ref** (*node*))



Implementation: enqueue

- Appending x_{new} to linked list is now done with CAS
- Ensures that no other thread has performed an enqueue while we have been working
- Swinging tail to x_{new} might fail: another thread has helped us

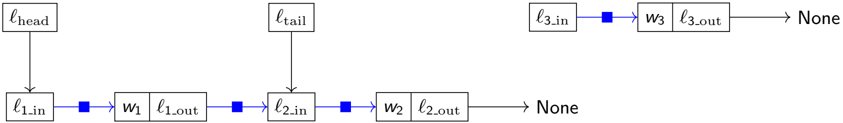
```
enqueue  Q value ≜
  let node = ref (Some value, ref (None)) in
  (rec  loop_ =
    let tail = !(snd(! Q)) in
    let next = !(snd(! tail)) in
    if tail = !(snd(! Q)) then
      if next = None then
        if CAS (snd(! tail)) next node then
          CAS (snd(! Q)) tail node
        else loop ()
      else CAS (snd(! Q)) tail next; loop ()
    else loop ()
  ) ()
```



Implementation: enqueue

- Appending x_{new} to linked list is now done with CAS
- Ensures that no other thread has performed an enqueue while we have been working
- Swinging tail to x_{new} might fail: another thread has helped us

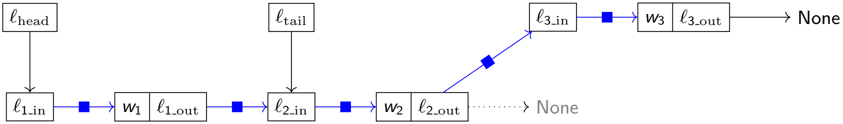
```
enqueue  Q value ≜
   let node = ref (Some value, ref (None)) in
   (rec  loop_ =
      let tail = !(snd(! Q)) in
      let next = !(snd(! tail)) in
      if tail = !(snd(! Q)) then
         if next = None then
            if CAS (snd(! tail)) next node then
               CAS (snd(! Q)) tail node
            else loop ()
         else CAS (snd(! Q)) tail next; loop ()
      else loop ()
   ) ()
```



Implementation: enqueue

- Appending x_{new} to linked list is now done with CAS
- Ensures that no other thread has performed an enqueue while we have been working
- Swinging tail to x_{new} might fail: another thread has helped us

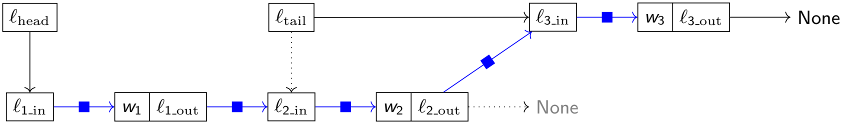
```
enqueue  Q value ≜
  let node = ref (Some value, ref (None)) in
  (rec  loop_ =
    let tail = !(snd(! Q)) in
    let next = !(snd(! tail)) in
    if tail = !(snd(! Q)) then
      if next = None then
        if CAS (snd(! tail)) next node then
          CAS (snd(! Q)) tail node
        else loop ()
      else CAS (snd(! Q)) tail next; loop ()
    else loop ()
  ) ()
```



Implementation: enqueue

- Appending x_{new} to linked list is now done with CAS
- Ensures that no other thread has performed an enqueue while we have been working
- Swinging tail to x_{new} might fail: another thread has helped us

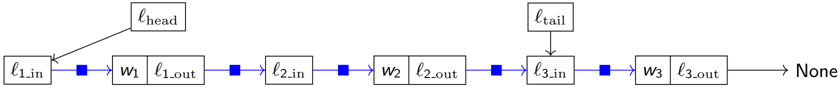
```
enqueue  Q value ≜
  let node = ref (Some value, ref (None)) in
  (rec  loop_ =
    let tail = !(snd(! Q)) in
    let next = !(snd(! tail)) in
    if tail = !(snd(! Q)) then
      if next = None then
        if CAS (snd(! tail)) next node then
          CAS (snd(! Q)) tail node
        else loop ()
      else CAS (snd(! Q)) tail next; loop ()
    else loop ()
  ) ()
```



Implementation: dequeue

- Head now swung with CAS instruction
- Ensures that another thread hasn't dequeued the element we are trying to dequeue

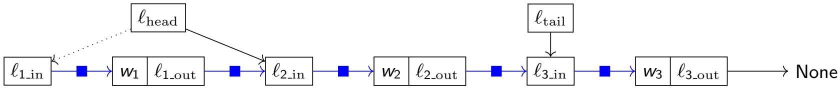
```
dequeue  Q ≜
  (rec  loop_ =
    let head = !(fst(! Q)) in
    let tail = !(snd(! Q)) in
    let p = newproph in
    let next = !(snd(! head)) in
    if head = Resolve(!(fst(! Q)), p, ()) then
      if head = tail then
        if next = None then
          None
        else
          CAS(snd(! Q)) tail next; loop ()
      else
        let value = fst(! next) in
        if CAS (fst(! Q)) head next then
          value
        else loop ()
    else loop ()
  )()
```



Implementation: dequeue

- Head now swung with CAS instruction
- Ensures that another thread hasn't dequeued the element we are trying to dequeue

```
dequeue  Q ≜
  (rec  loop_ =
    let head = !(fst(! Q)) in
    let tail = !(snd(! Q)) in
    let p = newproph in
    let next = !(snd(! head)) in
    if head = Resolve(!(fst(! Q)), p, ()) then
      if head = tail then
        if next = None then
          None
        else
          CAS(snd(! Q)) tail next; loop ()
      else
        let value = fst(! next) in
        if CAS (fst(! Q)) head next then
          value
        else loop ()
    else loop ()
  )()
```



Prophecies

- Proving adherence to HOCAP-style specification requires applying the view-shift at some point (must update P to Q)
- View-shift is applied at *Linearisation Points* – points where the effect of the function takes place
- When the queue is empty, the linearisation point is when reading *next* (specifically, the dereference instruction)
- We deduce that at exactly that read, the queue was empty
- But we only conclude the queue is empty if consistency check on next line succeeds
- The dereference is only the linearisation point if consistency check succeeds
- Prophecies: reason about future computations (e.g. the consistency check)
  - $!(\mathsf{fst}(!\,Q))$ will evaluate to some v_p (later proof obligation)
  - Before reading *next*, reason about whether $head = v_p$

```
...
let p = newproph in
let next = !(snd(! head)) in
if head = Resolve(!(fst(! Q)), p, ()) then
   if head = tail then
      if next = None then
         None
...
 else loop ()
...
```

The Lock-and-CC-Free Michael-Scott Queue

- Reason for consistency checks: ABA problem in original implementation
- HeapLang is garbage collected language, so we can remove consistency checks
- Can also remove prophecy in dequeue
  - When we read *next*, we know immediately whether dequeue will conclude empty queue
  - both *head* and *tail* are already fixed

```
initialize ≜
  let node = ref (None, ref (None)) in
  ref (ref (node), ref (node))

enqueue  Q value ≜
  let node = ref (Some value, ref (None)) in
  (rec  loop_ =
    let tail = !(snd(! Q)) in
    let next = !(snd(! tail)) in
    if next = None then
      if CAS (snd(! tail)) next node then
        CAS (snd(! Q)) tail node
       else loop ()
     else CAS (snd(! Q)) tail next; loop ()
  ) ()
```

```
dequeue  Q ≜
  (rec  loop_ =
    let head = !(fst(! Q)) in
    let tail = !(snd(! Q)) in
    let next = !(snd(! head)) in
    if head = tail then
      if next = None then
        None
       else
        CAS(snd(! Q)) tail next; loop ()
     else
      let value = fst(! next) in
      if CAS (fst(! Q)) head next then
        value
       else loop ()
    )()
```

Proving that the Lock-and-CC-Free Michael-Scott Queue Satisfies the HOCAP-style Specification

Reachability

- The queue relies on some important properties to function correctly:
  - The set of nodes reachable from a particular node only grows
  - The head and tail are only moved forward in the linked list
  - The tail cannot lag behind the head (unlike in the two-lock version)
- We capture all these properties with a notion of *reachability*
- Consists of a concrete and abstract version of reachability

Concrete Reachability

- Concrete reachability essentially captures a section of the linked list (á la isLL)
- The proposition $x_n \rightsquigarrow x_m$ asserts that x_n can reach x_m through the linked list
- Defined inductively as follows

$$x_n \rightsquigarrow x_m \triangleq \mathrm{in}(x_n) \mapsto^{\square} (\mathrm{val}(x_n), \mathrm{out}(x_n)) * (x_n = x_m \vee \exists x_p.\ \mathrm{out}(x_n) \mapsto^{\square} \mathrm{in}(x_p) * x_p \rightsquigarrow x_m)$$

- Concrete reachability is reflexive and transitive

Reachability (continued)

Abstract Reachability

- Abstract reachability is concerned with tracking specific *types* of nodes, such as the head node, the tail node, and the last node
- Tracked using ghost names, e.g. γ_{Head}, γ_{Tail}, and γ_{Last}
  - Implemented using the resource algebra $\mathrm{AUTH}(\mathcal{P}(\mathit{Node}))$
- Defined in two parts: Abstract Points-to ($\gamma \rightarrowtail x$) and Abstract Reach ($x \dashrightarrow \gamma$)
- For instance, $\gamma_{\mathrm{Tail}} \rightarrowtail x_n$ means that the current tail node is x_n
- And $x_m \dashrightarrow \gamma_{\mathrm{Tail}}$ means that node x_m can always reach the tail node

Lemmas for Reachability (simplified)

$$x \rightsquigarrow x \Rrightarrow \exists \gamma.\, \gamma \rightarrowtail x \qquad \text{(Abs Reach Alloc)}$$

$$x_n \dashrightarrow \gamma_m * \gamma_m \rightarrowtail x_m \twoheadrightarrow\!\!* \; x_n \rightsquigarrow x_m \qquad \text{(Abs Reach Concr)}$$

$$x_n \rightsquigarrow x_m * \gamma_m \rightarrowtail x_m \Rrightarrow x_n \dashrightarrow \gamma_m \qquad \text{(Abs Reach Abs)}$$

$$\gamma_m \rightarrowtail x_m * x_m \rightsquigarrow x_o \Rrightarrow \gamma_m \rightarrowtail x_o \qquad \text{(Abs Reach Advance)}$$

In Coq!