The Best Queue Specifications You Will Ever See today probably

Mathias Pedersen

Aarhus University

November 2025

AARHUS UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

Context

- Based on my Master's Thesis
- Goal of project was to prove safety of two concurrent queues
- Success! – but not too interesting

Context

- Based on my Master's Thesis
- Goal of project was to prove safety of two concurrent queues
- Success! – but not too interesting
- Today: Queue Specifications

Context

- Based on my Master's Thesis
- Goal of project was to prove safety of two concurrent queues
- Success! – but not too interesting
- Today: Queue Specifications
- In particular, three different specifications
  - Sequential specification
  - Concurrent specification
  - HOCAP-style specification

Context

- Based on my Master's Thesis
- Goal of project was to prove safety of two concurrent queues
- Success! – but not too interesting
- Today: Queue Specifications
- In particular, three different specifications
  - Sequential specification
  - Concurrent specification
  - HOCAP-style specification
- Uses HeapLang, but should be mostly language-agnostic

Context

- Based on my Master's Thesis
- Goal of project was to prove safety of two concurrent queues
- Success! – but not too interesting
- Today: Queue Specifications
- In particular, three different specifications
  - Sequential specification
  - Concurrent specification
  - HOCAP-style specification
- Uses HeapLang, but should be mostly language-agnostic
- Project was advised by Amin

Specifications for Queues

Informal Queue Specification

- 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, $xs_v ++ [v]$, remove value v at end of queue and return Some v
  - If empty, [], return None

Specifications for Queues

Informal Queue Specification

- 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, $xs_v ++ [v]$, remove value v at end of queue 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

Sequential Specification

Definition (Sequential Specification)

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

- The proposition $\mathsf{isQueue}_S(v_q, xs_v, G)$, 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: $\mathsf{isQueue}_S$ *not* required to be persistent!

Sequential Specification

Definition (Sequential Specification)

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

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

- The proposition $\text{isQueue}_S(v_q, xs_v, G)$, 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: isQueue_S *not* required to be persistent!

Sequential Specification

Definition (Sequential Specification)

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

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

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

- 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!

Sequential Specification

Definition (Sequential Specification)

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

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

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

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

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

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

- 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)

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

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

$$\forall v_q, G.\ \mathsf{isQueue}_C(\Psi, v_q, G) \implies \Box\, \mathsf{isQueue}_C(\Psi, v_q, G)$$

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)

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

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

$$\forall v_q, G.\ \mathrm{isQueue}_C(\Psi, v_q, G) \implies \Box\, \mathrm{isQueue}_C(\Psi, v_q, G)$$

$$\land \quad \{\mathrm{True}\}\ \mathrm{initialize}\ ()\ \{v_q.\exists G.\ \mathrm{isQueue}_C(\Psi, v_q, G)\}$$

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)

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

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

$$\forall v_q, G.\ \mathrm{isQueue}_C(\Psi, v_q, G) \implies \Box\, \mathrm{isQueue}_C(\Psi, v_q, G)$$

$$\wedge \quad \{\mathrm{True}\}\ \mathrm{initialize}\ ()\ \{v_q.\exists G.\ \mathrm{isQueue}_C(\Psi, v_q, G)\}$$

$$\wedge \quad \forall v_q, v, G.\ \{\mathrm{isQueue}_C(\Psi, v_q, G) * \Psi(v)\}\ \mathrm{enqueue}\ \ v_q\ \ v\ \{w.\mathrm{True}\}$$

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)

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

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

$$\forall v_q, G.\ \mathrm{isQueue}_C(\Psi, v_q, G) \implies \Box\, \mathrm{isQueue}_C(\Psi, v_q, G)$$

$$\land \quad \{\mathrm{True}\}\ \mathrm{initialize}\ ()\ \{v_q.\exists G.\ \mathrm{isQueue}_C(\Psi, v_q, G)\}$$

$$\land \quad \forall v_q, v, G.\ \{\mathrm{isQueue}_C(\Psi, v_q, G) * \Psi(v)\}\ \mathrm{enqueue}\ \ v_q\ \ v\ \{w.\mathrm{True}\}$$

$$\land \quad \forall v_q, G.\ \{\mathrm{isQueue}_C(\Psi, v_q, G)\}\ \mathrm{dequeue}\ \ v_q\ \{w.w = \mathrm{None} \lor (\exists v.\ w = \mathrm{Some}\ v * \Psi(v))\}$$

HOCAP-style Specification - Abstract State RA

- We will need a construction to allow clients to track contents of queue

- 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

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 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)

$\exists\, \text{isQueue} : \mathit{Val} \to \mathit{Qgnames} \to \text{Prop}.$

$$\forall v_q, G.\ \text{isQueue}(v_q, G) \implies \square\, \text{isQueue}(v_q, G)$$

HOCAP-style Specification

- Post-condition of initialize specification 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)

$\exists\, \mathrm{isQueue} : \mathit{Val} \to \mathit{Qgnames} \to \mathrm{Prop}.$

$$\forall v_q, G.\ \mathrm{isQueue}(v_q, G) \implies \Box\, \mathrm{isQueue}(v_q, G)$$

$$\land \quad \{\mathrm{True}\}\ \mathrm{initialize}\ ()\ \{v_q.\exists G.\ \mathrm{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_{\circ} []\}$$

HOCAP-style Specification

- Post-condition of initialize specification 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)

$\exists\, \mathrm{isQueue} : \mathit{Val} \to \mathit{Qgnames} \to \mathrm{Prop}.$

$$\forall v_q, G.\ \mathrm{isQueue}(v_q, G) \implies \Box\, \mathrm{isQueue}(v_q, G)$$

$$\wedge\quad \{\mathrm{True}\}\ \mathrm{initialize}\ ()\ \{v_q.\exists G.\ \mathrm{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_{\circ} []\}$$

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

HOCAP-style Specification

- Post-condition of initialize specification 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)

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

Queue Client - A PoC Client

- Add two numbers after having two threads enqueue and subsequently dequeue them

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

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

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

Queue Client - A PoC Client

- Add two numbers after having two threads enqueue and subsequently dequeue them
- Idea: a minimal client complex enough to require HOCAP-style specification

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

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

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

Queue Client - A PoC Client

- Add two numbers after having two threads enqueue and subsequently dequeue them
- Idea: a minimal client complex enough to require HOCAP-style specification
- Uses parallel composition, so sequential specification insufficient

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

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

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

Queue Client - A PoC Client

- Add two numbers after having two threads enqueue and subsequently dequeue them
- Idea: a minimal client complex enough to require HOCAP-style specification
- Uses parallel composition, so sequential specification insufficient
- Relies on dequeues not returning None, so concurrent specification insufficient

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

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

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

Queue Client - A PoC Client

- Add two numbers after having two threads enqueue and subsequently dequeue them
- Idea: a minimal client complex enough to require HOCAP-style specification
- Uses parallel composition, so sequential specification insufficient
- Relies on dequeues not returning None, so concurrent specification insufficient
- HOCAP-style specification supports consistency and tracks 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)

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

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)

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

- When using the HOCAP-style Queue specification to prove the above, we will make P and Q talk about the tokens.
- E.g for enqueue:
  - $P = \text{TokA}\ \ Ga \ \vee \ \text{TokB}\ \ Ga$
  - $Q = \text{TokD1}\ \ Ga \ \vee \ \text{TokD2}\ \ Ga$

Queue Specifications Overview

Spec\Feature	Supports Tracking	Supports Concurrency	
Sequential	✓	✗	
Concurrent	✗	✓	
HOCAP	✓	✓	

Queue Specifications Overview

Spec\Feature	Supports Tracking	Supports Concurrency	Price
Sequential	✓	✗	\$199
Concurrent	✗	✓	\$249
HOCAP	✓	✓	\$399

Queue Specifications Overview

Spec\Feature	Supports Tracking	Supports Concurrency	Price
Sequential	✓	✗	$199
Concurrent	✗	✓	$249
HOCAP	✓	✓	$399

- HOCAP generalises Sequential and Concurrent specs
- In fact, they are provably derivable from HOCAP

HOCAP Derives Sequential

Definition (Sequential Specification (reminder))

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

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

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

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

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

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

HOCAP Derives Sequential

Definition (HOCAP Specification)

$\exists\,\mathsf{isQueue} : \mathit{Val} \to \mathit{Qgnames} \to \mathsf{Prop}.$

$$\forall v_q, G.\ \mathsf{isQueue}(v_q, G) \implies \Box\,\mathsf{isQueue}(v_q, G)$$

$$\wedge\quad \{\mathsf{True}\}\ \mathsf{initialize}\ ()\ \{v_q.\exists G.\ \mathsf{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_\circ []\}$$

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

$$\wedge\quad \forall v_q, G, P, Q. \\ \left(\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright \left(\begin{array}{l} (xs_v = [] * G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * Q(\mathsf{None})) \\ \vee \left(\begin{array}{l} \exists v, xs_v'.\ xs_v = xs_v' +\!\!+ [v] * \\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v' * Q(\mathsf{Some}\ v) \end{array}\right) \end{array}\right)\right) -\!\!* \\ \{\mathsf{isQueue}(v_q, G) * P\}\ \mathsf{dequeue}\ \ v_q\ \{w.Q(w)\}$$

- Chose $\mathsf{isQueue}_S(v_q, xs_v, G) = \mathsf{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_\circ xs_v$

HOCAP Derives Sequential

Definition (HOCAP Specification)

$\exists\, \mathsf{isQueue} : Val \to Qgnames \to \mathsf{Prop}.$

$$\forall v_q, G.\ \mathsf{isQueue}(v_q, G) \implies \Box\, \mathsf{isQueue}(v_q, G)$$

$$\land\quad \{\mathsf{True}\}\ \mathsf{initialize}\ ()\ \{v_q.\exists G.\ \mathsf{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_\circ []\}$$

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

$$\land\quad \forall v_q, G, P, Q.\ \left(\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright \left(\begin{array}{l} (xs_v = [] * G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * Q(\mathsf{None})) \\ \lor \left(\begin{array}{l} \exists v, xs_v'.\ xs_v = xs_v' \mathbin{++} [v] * \\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v' * Q(\mathsf{Some}\ v) \end{array}\right) \end{array}\right)\right) \twoheadrightarrow \{\mathsf{isQueue}(v_q, G) * P\}\ \mathsf{dequeue}\ \ v_q\ \{w.Q(w)\}$$

- Chose $\mathsf{isQueue}_S(v_q, xs_v, G) = \mathsf{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_\circ xs_v$
- Initialise then follows directly

HOCAP Derives Sequential

Definition (HOCAP Specification)

$\exists\, \mathsf{isQueue} : \mathit{Val} \to \mathit{Qgnames} \to \mathsf{Prop}.$

$$\forall v_q, G.\ \mathsf{isQueue}(v_q, G) \implies \Box\, \mathsf{isQueue}(v_q, G)$$

$$\land \quad \{\mathsf{True}\}\ \mathsf{initialize}\ ()\ \{v_q.\exists G.\ \mathsf{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_\circ []\}$$

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

$$\land \quad \forall v_q, G, P, Q.\ \left(\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright \left(\begin{array}{l} (xs_v = [] * G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * Q(\mathsf{None})) \\ \lor \left(\begin{array}{l} \exists v, xs_v'.\ xs_v = xs_v' \mathbin{+\!\!+} [v] * \\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v' * Q(\mathsf{Some}\ v) \end{array}\right) \end{array}\right)\right) \twoheadrightarrow \{\mathsf{isQueue}(v_q, G) * P\}\ \mathsf{dequeue}\ \ v_q\ \{w.Q(w)\}$$

- Chose $\mathsf{isQueue}_S(v_q, xs_v, G) = \mathsf{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_\circ xs_v$
- Initialise then follows directly
- For enqueue, pick
  - $P = G.\gamma_{\mathrm{Abst}} \Mapsto_\circ xs_v$
  - $Q = G.\gamma_{\mathrm{Abst}} \Mapsto_\circ v :: xs_v$

HOCAP Derives Sequential

Definition (HOCAP Specification)

$\exists\, \mathrm{isQueue} : Val \to Qgnames \to \mathrm{Prop}.$

$$\forall v_q, G.\ \mathrm{isQueue}(v_q, G) \implies \Box\, \mathrm{isQueue}(v_q, G)$$

$$\land\quad \{\mathrm{True}\}\ \mathrm{initialize}\ ()\ \{v_q.\exists G.\ \mathrm{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_\circ []\}$$

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

$$\land\quad \forall v_q, G, P, Q. \\ \left(\forall xs_v.\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * P \Rrightarrow_{\mathcal{E}\setminus\mathcal{N}.i\uparrow} \triangleright \left(\begin{array}{l} (xs_v = [] * G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs_v * Q(\mathrm{None})) \\ \lor \left(\begin{array}{l} \exists v, xs'_v.\ xs_v = xs'_v +\!\!+ [v] * \\ G.\gamma_{\mathrm{Abst}} \Mapsto_\bullet xs'_v * Q(\mathrm{Some}\ v) \end{array}\right) \end{array}\right)\right) -\!\!* \\ \{\mathrm{isQueue}(v_q, G) * P\}\ \mathrm{dequeue}\ \ v_q\ \{w.Q(w)\}$$

- Chose $\mathrm{isQueue}_S(v_q, xs_v, G) = \mathrm{isQueue}(v_q, G) * G.\gamma_{\mathrm{Abst}} \Mapsto_\circ xs_v$
- Initialise then follows directly
- For enqueue, pick
  - $P = G.\gamma_{\mathrm{Abst}} \Mapsto_\circ xs_v$
  - $Q = G.\gamma_{\mathrm{Abst}} \Mapsto_\circ v :: xs_v$
- For dequeue, pick
  - $P = G.\gamma_{\mathrm{Abst}} \Mapsto_\circ xs_v$
  - $Q(w) = (G.\gamma_{\mathrm{Abst}} \Mapsto_\circ [] * w = \mathrm{None}) \lor (\exists v, xs'_v.xs_v = xs'_v +\!\!+ [v] * w = \mathrm{Some}\ v * G.\gamma_{\mathrm{Abst}} \Mapsto_\circ xs'_v)$

HOCAP Derives Concurrent

Left as an exercise :)

Thanks for your time

Questions?