Concurrent Objects and Linearizability

EECS 395 “Rust”

Feb. 2, 2016
What is a concurrent object?

- How do we describe one?
- How do we implement one?
- How do we tell if we’re right?
What is a concurrent object?

- How do we describe one?
- How do we tell if we’re right?
Case study: FIFO queue

\[ q = \begin{array}{c}
2 \\
4 \\
\end{array} \]
Case study: FIFO queue

q =  

q.enq(6)
Case study: FIFO queue

$q = \begin{array}{c}
| 2 | 4 | 6 |
\end{array}$

$q.\text{enq}(6)$
Case study: FIFO queue

\[ q = \begin{array}{c}
2 \\
4 \\
6 \\
\end{array} \]

\[ q\text{.enq}(6) \]

\[ q\text{.deq}() \]
Case study: FIFO queue

\[ q = \begin{array}{c}
4 \\
6 \\
\end{array} \]

q.enq(6)
q.deq() ⇒ 2
Implementation: lock-based ring buffer

template<typename Element, int capacity>
class Lock_based_FIFO
{
public:
    void enq(Element);
    Element deq();

private:
    array<Element, capacity> data;
    unsigned head = 0, tail = 0;
    Lock lock;
};
Implementation: lock-based enqueue

template \langle \text{typename } \text{Element, int capacity} \rangle
void \text{Lock\_based\_FIFO::enq}(\text{Element } x)
{
    \text{auto guard} = \text{lock.acquire}();
    \text{if (tail} - \text{head} == \text{capacity})\ \text{throw fifo\_full}();
    \text{data[\text{tail}++ \ % \ \text{capacity}] = x;}
}
Implementation: lock-based dequeue

```cpp
template<typename Element, int capacity>
Element Lock_based_FIFO::deq()
{
    auto guard = lock.acquire();
    if (tail == head) throw fifo_empty{};
    return data[head++ % capacity];
}
```
Now consider this

Same thing, but:

- no mutual exclusion
- only two threads:
  - one only enqueues
  - one only dequeues
Wait-free SRSW FIFO

template <typename Element, int capacity>
class Wf_SRSW_FIFO
{
    array<Element, capacity> data;
    unsigned head = 0, tail = 0;

public:
    void enq(Element) {
        if (tail - head == capacity) throw fifo_full{};
        data[tail++ % capacity] = x;
    }

    Element deq() {
        if (tail == head) throw fifo_empty{};
        return data[head++ % capacity];
    }
};
What *is* a concurrent queue?

- Need a way to **specify** a concurrent queue object
- Need a way to **prove** that an algorithm implements the spec
What is a concurrent queue?

- Need a way to specify a concurrent queue object
- Need a way to prove that an algorithm implements the spec

How do we specify objects?
Object specification

In a concurrent setting:

- it gets the right answer (correctness, a safety property)
- it doesn’t get stuck (progress, a liveness property)

Let’s start with correctness.
Sequential objects

Each object has

- a state:
  - fields, usually
  - FIFO example: the sequence of elements

- a set of methods:
  - only way to manipulate the state
  - FIFO example: `enq` and `deq` methods
Sequential specification

- If (precondition)
  - the object is in such-and-such a state
  - before you call the method,
Sequential specification

- If (precondition)
  - the object is in such-and-such a state
  - before you call the method,

- then (postcondition)
  - the method will return a particular value
  - or throw a particular exception,
Sequential specification

- If (precondition)
  - the object is in such-and-such a state
  - before you call the method,
- then (postcondition)
  - the method will return a particular value
  - or throw a particular exception,
- and (postcondition)
  - the object will be in some specified state
  - when the method returns.
Example sequential specification: dequeue

- **Precondition:**
  - queue is non-empty

- **Postcondition:**
  - returns first item in queue

- **Postcondition:**
  - removes first item in queue
Example sequential specification: dequeue

- **Precondition:**
  - queue is non-empty

- **Postcondition:**
  - returns first item in queue

- **Postcondition:**
  - removes first item in queue

Easy!
Example sequential specification: dequeue

- **Precondition:**
  - queue is empty

- **Postcondition:**
  - throws fifo_empty exception

- **Postcondition:**
  - state is unchanged

Easy!
Sequential specifications are awesome

- All method interactions captured by side-effects on state
- Each method described in isolation
- Can add new methods easily
Sequential specifications are awesome

- All method interactions captured by side-effects on state
- Each method described in isolation
- Can add new methods easily

What about concurrent specifications?
Complication: methods take time

- Sequential: what is time? who cares?
- Concurrent: method call is interval, not event
Complication: methods take overlapping time

- Sequential: what is time? who cares?
- Concurrent: method call is interval, not event

- Sequential: invariants must hold between calls
- Concurrent: overlapping means might never even be between calls
What does it mean for a *concurrent* object to be correct?
The Big Question

What does it mean for a concurrent object to be correct? Or, what is a concurrent FIFO queue?
The Big Question

What does it mean for a concurrent object to be correct? Or, what is a concurrent FIFO queue?

- FIFO means stuff happens in order
- concurrent means time/order is kinda ambiguous
template<typename Element, int capacity>
Element Lock_based_FIFO::deq() {
    auto guard = lock.acquire();
    if (tail == head) throw fifo_empty();
    return data[head++ % capacity];
}

template<typename Element, int capacity>
void Lock_based_FIFO::enq(Element x) {
    auto guard = lock.acquire();
    if (tail - head == capacity) throw fifo_full();
    data[tail++ % capacity] = x;
}
Intuitively…

template <typename Element, int capacity>
Element Lock_based_FIFO::deq() {
    auto guard = lock.acquire();
    if (tail == head) throw fifo_empty{};
    return data[head++ % capacity];
}

template <typename Element, int capacity>
void Lock_based_FIFO::enq(Element x) {
    auto guard = lock.acquire();
    if (tail - head == capacity) throw fifo_full{};
    data[tail++ % capacity] = x;
}

Mutual exclusion means we can describe the behavior sequentially
Linearizability

- Each method “takes effect” “instantaneously” between invocation and response events
- Object is correct if this “sequential” behavior is correct
Linearizability

- Each method “takes effect” “instantaneously” between invocation and response events
- Object is correct if this “sequential” behavior is correct

Such a concurrent object is *linearizable*
Is linearizability really about the object?

A linearizable object: all of its possible executions are linearizable

(Linearizable execution examples on board)
Formal model of executions

Split method call into two events:

<table>
<thead>
<tr>
<th>Invocation</th>
<th>A q.enq(x)</th>
<th>Thread A calls q.enq(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response</td>
<td>A q:void</td>
<td>Result is void</td>
</tr>
</tbody>
</table>
$H =$

A q.enq(3)
A q:void
B p.enq(4)
B p:void
B q.deq()
B q:3
Object projection:

\[ H | q = \]

\[ A \ q.\text{enq}(3) \]
\[ A \ q:\text{void} \]

\[ B \ q.\text{deq}() \]
\[ B \ q:3 \]
Thread projection:

\[
H|B = \begin{array}{l}
B \text{ p.enq}(4) \\
B \text{ p:void} \\
B \text{ q.deq()} \\
B \text{ q:3}
\end{array}
\]
History

\[ H = \]

A q.enq(3)
A q: void
B p.enq(4)
B p: void
B q.deq()
B q: 3
Complete subhistories

Remove pending invocations:

\[ H = \]

A q.enq(3)
A q:void
A q.deq()

B p.enq(4)
B p:void
B q.deq()
B q:3
Complete subhistories

Remove pending invocations:

\[
\text{Complete}(H) = \begin{align*}
A & \ q.\text{enq}(3) \\
A & \ q:\text{void} \\
B & \ p.\text{enq}(4) \\
B & \ p:\text{void} \\
B & \ q.\text{deq}() \\
B & \ q:3
\end{align*}
\]
Sequential subhistories

Responses immediately follow invocations (except possibly a final invocation):

\[ H = \]

\[
\begin{array}{l}
A \ q.\text{enq}(3) \\
A \ q:\text{void} \\
\hline
B \ p.\text{enq}(4) \\
B \ p:\text{void} \\
\hline
B \ q.\text{deq}() \\
B \ q:3 \\
\hline
A \ q.\text{enq}(5)
\end{array}
\]
History well-formedness

\[ H = \]

- A q.enq(3)
- B p.enq(4)
- B p:void
- B q:deq()
- B q:3
- A q:void
History well-formedness

\[ H = \]

A q.enq(3)
B p.enq(4)
B p:void
B q:deq()
B q:3
A q:void

\( H \) is well formed if its thread projections are sequential:
History well-formedness

\[ H = \]

- A q.enq(3)
- B p.enq(4)
- B p:void
- B q:deq()
- B q:3

\( H \) is well formed if its thread projections are sequential:

\[ H \mid A = \]

- A q.enq(3)
- A q:void

\[ H \mid B = \]

- B p.enq(4)
- B p:void
- B q:deq()
- B q:3
History equivalence

\[ H = \begin{align*}
A & \text{ q.enq}(3) \\
B & \text{ p.enq}(4) \\
B & \text{ p:void} \\
B & \text{ q:deq()} \\
A & \text{ q:void} \\
B & \text{ q:3}
\end{align*} \]

\[ G = \begin{align*}
A & \text{ q.enq}(3) \\
A & \text{ q:void} \\
B & \text{ p.enq}(4) \\
B & \text{ p:void} \\
B & \text{ q:deq()} \\
B & \text{ q:3}
\end{align*} \]
History equivalence

\[ H = \]
\[
A \text{ q.enq(3)} \\
B \text{ p.enq(4)} \\
B \text{ p:void} \\
B \text{ q:deq()} \\
A \text{ q:void} \\
B \text{ q:3}
\]

\[ G = \]
\[
A \text{ q.enq(3)} \\
A \text{ q:void} \\
B \text{ p.enq(4)} \\
B \text{ p:void} \\
B \text{ q:deq()} \\
B \text{ q:3}
\]

\(G \sim H\) iff threads see the same things:

\[ H|A = G|A\]
\[ H|B = G|B\]
Sequential specification

A *sequential specification* describes a legal single-thread, single-object history.
Sequential specification

A *sequential specification* describes a legal single-thread, single-object history

Example: CFG for sequential histories of *unbounded* FIFO:

\[
\begin{align*}
BH & ::= \epsilon \\
BH & ::= BH; BH \\
BH & ::= q\text{.enq}(x); q\text{.void}; BH; q\text{.deq}(); q\text{:}x \\
H & ::= BH \\
H & ::= q\text{.deq}(); q\text{:}Empty \\
H & ::= H; H
\end{align*}
\]
Legal histories

A sequential (multi-object, multi-thread) history $H$ is legal if:
For every object $x$, $H|x$ is in the sequential spec for $x$
Precedence

A method call \textit{c precedes} a method call \textit{d} if c’s response comes before d’s invocation.
Precedence

A method call $c$ precedes a method call $d$ if $c$’s response comes before $d$’s invocation.

Example:

```
A q.enq(3)
B p.enq(4)
B p:void
A q:void
B q.deq()
B q:3
```

- Method call $A$ `q.enq(3)` precedes method call $B$ `q.deq()`
- Method call $B$ `q.enq(4)` precedes method call $B$ `q.deq()`
- Method call $A$ `q.enq(3)` does not precede method call $B$ `q.enq(4)`
Properties of precedence

- In general, it’s a partial order
- For a sequential history, it’s a total order

Have we seen this before?
Properties of precedence

- In general, it’s a partial order
- For a sequential history, it’s a total order

Have we seen this before?

Yes: Precedence is happens-before (→) for method call intervals
Linearizability, formally

History $H$ is linearizable if it can be extended to complete history $G$ by

- appending responses to some pending invocations, and/or
- discarding the remaining pending invocations

such that there exists some legal sequential history $S$ where

$\rightarrow_G \subseteq \rightarrow_S$
Example

\[ H = \]
- A q.enq(3)
- B q.enq(4)
- B q:void
- B q.deq()
- B q:4
- B q.enq(6)

\[ S \text{ is legal and } \sim G \]
Example

\[ H = \begin{align*}
\text{A q.enq(3)} \\
\text{B q.enq(4)} \\
\text{B q:void} \\
\text{B q.deq()} \\
\text{B q:4} \\
\text{B q.enq(6)}
\end{align*} \]

\[ G = \begin{align*}
\text{A q.enq(3)} \\
\text{B q.enq(4)} \\
\text{B q:void} \\
\text{B q.deq()} \\
\text{B q:4} \\
\text{A q:void}
\end{align*} \]

\( S \) is legal and \( \sim G \)
Example

\[ H = \]
\begin{align*}
A & \text{ q.enq(3)} \\
B & \text{ q.enq(4)} \\
B & \text{ q:void} \\
B & \text{ q.deq()} \\
B & \text{ q:4} \\
B & \text{ q.enq(6)}
\end{align*}

\[ G = \]
\begin{align*}
A & \text{ q.enq(3)} \\
B & \text{ q.enq(4)} \\
B & \text{ q:void} \\
B & \text{ q.deq()} \\
B & \text{ q:4}
\end{align*}

\[ S = \]
\begin{align*}
B & \text{ q.enq(4)} \\
B & \text{ q:void} \\
A & \text{ q.enq(3)} \\
A & \text{ q:void} \\
B & \text{ q.deq()} \\
B & \text{ q:4}
\end{align*}

S is legal and \( \sim G \)
Composability theorem

History $H$ is linearizable iff for every object $x$, $H|x$ is linearizable
Composability theorem

History $H$ is linearizable iff for every object $x$, $H|x$ is linearizable

This means we can reason about objects independently
This work is licensed under a Creative Commons “Attribution-ShareAlike 3.0 Unported” license. These slides are derived from the companion slides for *The Art of Multiprocessor Programming*, by Maurice Herlihy and Nir Shavit. Its original license reads:

*This work is licensed under a Creative Commons Attribution-ShareAlike 2.5 License.*

- **You are free:**
  - to **Share** — to copy, distribute and transmit the work
  - to **Remix** — to adapt the work
- **Under the following conditions:**
  - **Attribution.** You must attribute the work to “The Art of Multiprocessor Programming” (but not in any way that suggests that the authors of that work or this endorse you or your use of the work).
  - **Share Alike.** If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.
- For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to
  - [http://creativecommons.org/licenses/by-sa/3.0/](http://creativecommons.org/licenses/by-sa/3.0/).
- Any of the above conditions can be waived if you get permission from the copyright holder.
- Nothing in this license impairs or restricts the author's moral rights.