Operating System Concepts

Lecture 19: Synchronization Primitives — Part 2

Omid Ardakanian
oardakan@ualberta.ca
University of Alberta

MWF 12:00-12:50 VVC 2 215

Today's class

- Synchronization primitives
  - Semaphore
  - Monitor

Why should we really care?

```
class Account {
public:
  void deposit(int amount) {
    balance += amount;
  }
  void withdraw(int amount) {
    balance -= amount;
  }
private:
  int balance;
}
```

Why should we really care?

```
class Account {
public:
  void deposit(int amount) {
    balance += amount;
  }
  void withdraw(int amount) {
    balance -= amount;
  }
private:
  int balance;
}
```

atbfinancial @atbfinancial · Oct 8

ATB has corrected a technical issue that caused duplicate payments for some customers.

Our highest priority is making sure any impact to you is fixed as quickly as possible.

This article will stay up-to-date with the latest information.

Issues with duplicate payments | ATB Financial
www.atb.com

CBC | MENU

news | Top Stories | Local | The National | Opinion | World | Canada | Politics | Indigenous

British Columbia

'You're at their mercy': customer says RBC charged him twice for Visa cheque transactions

Semaphores

- semaphores are generalized locks invented by Dijkstra in 1965
  - they are a (non-negative) integer variable that supports two **atomic** operations: `wait` and `signal` (or `down` and `up`)

Semaphores

- semaphores are generalized locks invented by Dijkstra in 1965
  - they are a (non-negative) integer variable that supports two **atomic** operations: `wait` and `signal` (or `down` and `up`)
- **binary semaphore**: used for mutual exclusion (just like mutex locks)
  - guarantees mutually exclusive access to a resource (i.e., only one thread/process in the critical section at a time)
  - can vary from 0 to 1; it is initialized to free (value = 1)

Semaphores

- semaphores are generalized locks invented by Dijkstra in 1965
  - they are a (non-negative) integer variable that supports two **atomic** operations: `wait` and `signal` (or `down` and `up`)
- **binary semaphore**: used for mutual exclusion (just like mutex locks)
  - guarantees mutually exclusive access to a resource (i.e., only one thread/process in the critical section at a time)
  - can vary from 0 to 1; it is initialized to free (value = 1)
- **counting semaphore**: used for conditional synchronization
  - useful when multiple units or instances of a specific resource are available
  - the semaphore is usually initialized to the number of resources
  - a process can acquire access so long as at least one unit of the resource is available

Atomic operations with semaphores

- each semaphore supports a queue of processes that are waiting to access the critical section (e.g., to check and buy milk)
- if a thread executes `Wait( )` and the semaphore is free (non-zero), it continues executing after decrementing the semaphore's variable. But if it is not free, the OS puts the thread on the wait queue for that semaphore
- `Signal( )` unblocks one thread on the semaphore's wait queue

Using semaphores to implement mutual exclusion

```
Semaphore milksemaphore; // suppose value is set to 1

milksemaphore.Wait()
<critical section>
milksemaphore.Signal()
```

acquired before accessing shared data

released after accessing shared data

Implementing signal and wait by disabling interrupts

```
class Semaphore {
public:
  void Wait(Thread T);
  void Signal();
private:
  int value;
  Queue Q;
}

Semaphore::Semaphore(int val) {
  value = val; // initialized to the number of available resources
}

Semaphore::Wait(Thread T) {
  intr_disable();
  value = value - 1;
  if(value < 0) {     // |value| is the number of waiting threads
    queue_add(Q, T);
    thread_block(T);
  }
  intr_enable();
}

Semaphore::Signal() {
  intr_disable();
  value = value + 1;
  if(value <= 0)      // if there is a waiting thread
    thread_unblock(queue_remove(Q));
  intr_enable();
}
```

Implementing signal and wait by disabling interrupts

```
class Semaphore {
public:
  void Wait(Thread T);
  void Signal();
private:
  int value;
  Queue Q;
}

Semaphore::Semaphore(int val) {
  value = val; // initialized to the number of available resources
}

Semaphore::Wait(Thread T) {
  intr_disable();
  value = value - 1;
  if(value < 0) {    // |value| is the number of waiting threads
    queue_add(Q, T);
    thread_block(T);
  }
  intr_enable();
}

Semaphore::Signal() {
  intr_disable();
  value = value + 1;
  if(value <= 0)     // if there is a waiting thread
    thread_unblock(queue_remove(Q));
  intr_enable();
}
```

can you implement these atomic operations using test_and_set?

Example: counting semaphore

	Semaphore value	Semaphore queue	Thread 1's state	Thread 2's state
	2	empty		
`Thread 1: SM.wait()`	1	empty		
`Thread 2: SM.wait()`	0	empty		
`Thread 1: SM.wait()`	0	T1	waiting	
`Thread 2: SM.signal()`	0	empty		
`Thread 1: SM.signal()`	1	empty		
`Thread 1: SM.signal()`	2	empty		

Example: counting semaphore

Suppose each thread needs two units of the available resource

	Semaphore value	Semaphore queue	Thread 1's state	Thread 2's state
	2	empty		
`Thread 1: SM.wait()`	1	empty		
`Thread 2: SM.wait()`	0	empty		
`Thread 1: SM.wait()`	0	T1	waiting	
`Thread 2: SM.wait()`	0	T1, T2	waiting	waiting

Example: counting semaphore

Suppose each thread needs two units of the available resource

	Semaphore value	Semaphore queue	Thread 1's state	Thread 2's state
	2	empty		
`Thread 1: SM.wait()`	1	empty		
`Thread 2: SM.wait()`	0	empty		
`Thread 1: SM.wait()`	0	T1	waiting	
`Thread 2: SM.wait()`	0	T1, T2	waiting	waiting

Deadlock

Example: counting semaphore

	Semaphore value	Semaphore queue	Thread 1's state	Thread 2's state	Thread 3's state
	2	empty			
`Thread 1: SM.wait()`	1	empty			
`Thread 1: SM.wait()`	0	empty			
`Thread 2: SM.wait()`	0	T2		waiting	
`Thread 3: SM.wait()`	0	T2, T3		waiting	waiting
`Thread 1: SM.signal()`	0	T3			waiting
`Thread 1: SM.signal()`	0	empty			
`Thread 3: SM.signal()`	1	empty			
`Thread 2: SM.signal()`	2	empty			

Semaphores versus condition variables

- semaphore can be implemented using a count variable, a condition variable, and a mutex lock

Semaphores versus condition variables

- semaphore can be implemented using a count variable, a condition variable, and a mutex lock
- condition variables do not have any history, but semaphores do
  - on a condition variable signal if no one is waiting, the signal is a no operation
    - if a thread then does a condition.Wait, it waits
  - on a semaphore.Signal if no one is waiting, the value of the semaphore is incremented
    - if a thread then does a semaphore.Wait, then value is decremented and the thread continues

Semaphores versus condition variables

- semaphore can be implemented using a count variable, a condition variable, and a mutex lock
- condition variables do not have any history, but semaphores do
  - on a condition variable signal if no one is waiting, the signal is a no operation
    - if a thread then does a condition.Wait, it waits
  - on a semaphore.Signal if no one is waiting, the value of the semaphore is incremented
    - if a thread then does a semaphore.Wait, then value is decremented and the thread continues
- semaphore Wait and Signal are commutative, i.e., the result is the same regardless of the order of execution

Semaphores versus condition variables

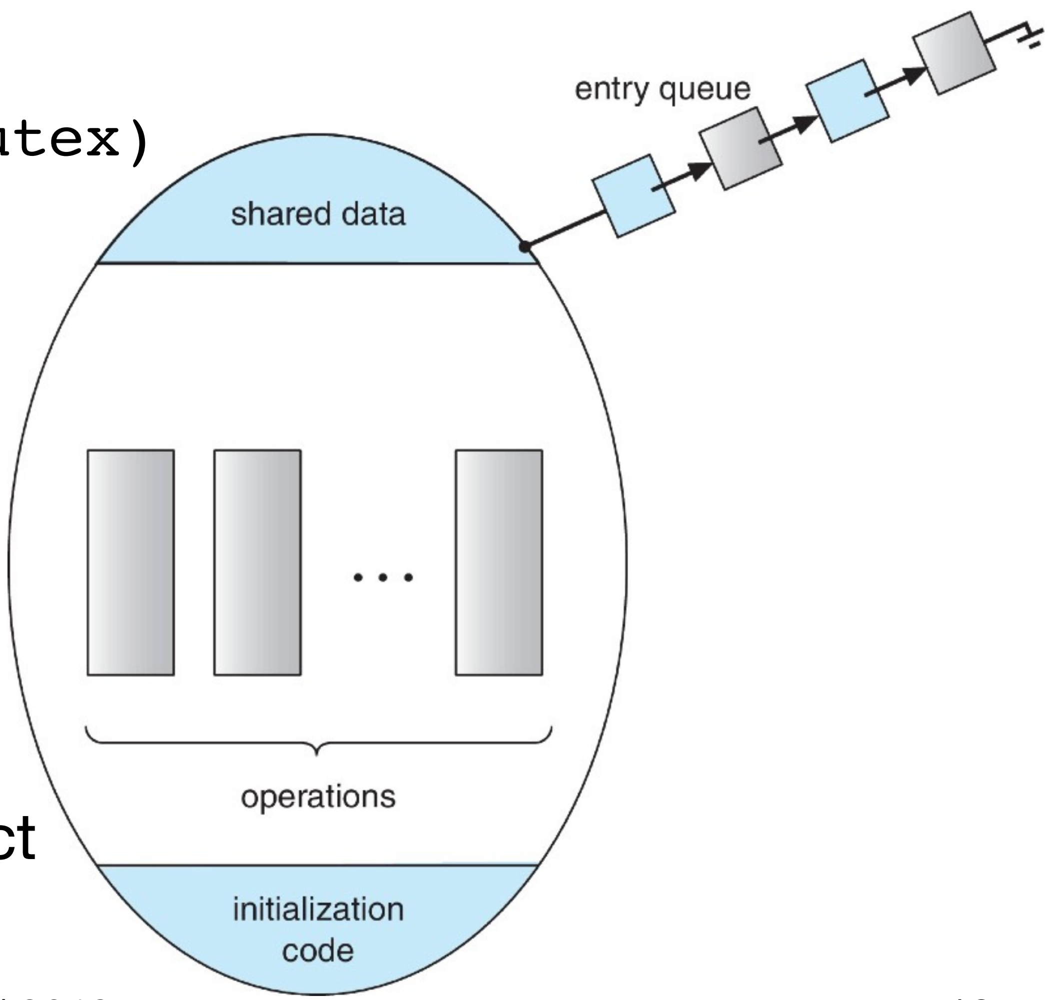
- semaphore can be implemented using a count variable, a condition variable, and a mutex lock
- condition variables do not have any history, but semaphores do
  - on a condition variable signal if no one is waiting, the signal is a no operation
    - if a thread then does a condition.Wait, it waits
  - on a semaphore.Signal if no one is waiting, the value of the semaphore is incremented
    - if a thread then does a semaphore.Wait, then value is decremented and the thread continues
- semaphore Wait and Signal are commutative, i.e., the result is the same regardless of the order of execution
- condition variables are not, and as a result they must be in a critical section to access state variables and do their job

What's wrong with semaphores?

- semaphore operations can be used incorrectly by programmers $\rightarrow$ two processes/threads may be in their critical sections simultaneously or may permanently block!
  - `signal(mutex)` … `wait(mutex)`
  - `wait(mutex)` … `wait(mutex)`
  - omitting `wait(mutex)` and/or `signal(mutex)`

What’s wrong with semaphores?

- semaphore operations can be used incorrectly by programmers → two processes/threads may be in their critical sections simultaneously or may permanently block!
  - `signal(mutex) … wait(mutex)`
  - `wait(mutex) … wait(mutex)`
  - omitting `wait(mutex)` and/or `signal(mutex)`



solution? a higher-level synchronization construct

Monitors

- Definition: a thread-safe class that ties (private) data and methods (including the synchronization operations) together, introduced by Per Brinch Hansen in 1970s
  - guarantees mutual exclusion, i.e., only one thread may execute a given monitor method at a time
  - provides a mechanism for threads to temporarily give up exclusive access to wait for a certain condition

Monitors

- Definition: a thread-safe class that ties (private) data and methods (including the synchronization operations) together, introduced by Per Brinch Hansen in 1970s
  - guarantees mutual exclusion, i.e., only one thread may execute a given monitor method at a time
  - provides a mechanism for threads to temporarily give up exclusive access to wait for a certain condition
- it defines a lock and zero, one, or more condition variables for managing concurrent access to shared data
  - the lock provides mutual exclusion for shared data
    - used to ensure that only a single thread is active in the monitor at a time
  - condition variables enable threads to go to sleep inside critical sections, by releasing their lock at the same time they are put to sleep
    - used when an operation cannot complete (because the condition is not true)

Monitors

- Definition: a thread-safe class that ties (private) data and methods (including the synchronization operations) together, introduced by Per Brinch Hansen in 1970s
  - guarantees mutual exclusion, i.e., only one thread may execute a given monitor method at a time
  - provides a mechanism for threads to temporarily give up exclusive access to wait for a certain condition
- it defines a lock and zero, one, or more condition variables for managing concurrent access to shared data
  - the lock provides mutual exclusion for shared data
    - used to ensure that only a single thread is active in the monitor at a time
  - condition variables enable threads to go to sleep inside critical sections, by releasing their lock at the same time they are put to sleep
    - used when an operation cannot complete (because the condition is not true)
- many programming languages, such as C# and Java, incorporated the idea of Monitor

Recall the CokeMachine class

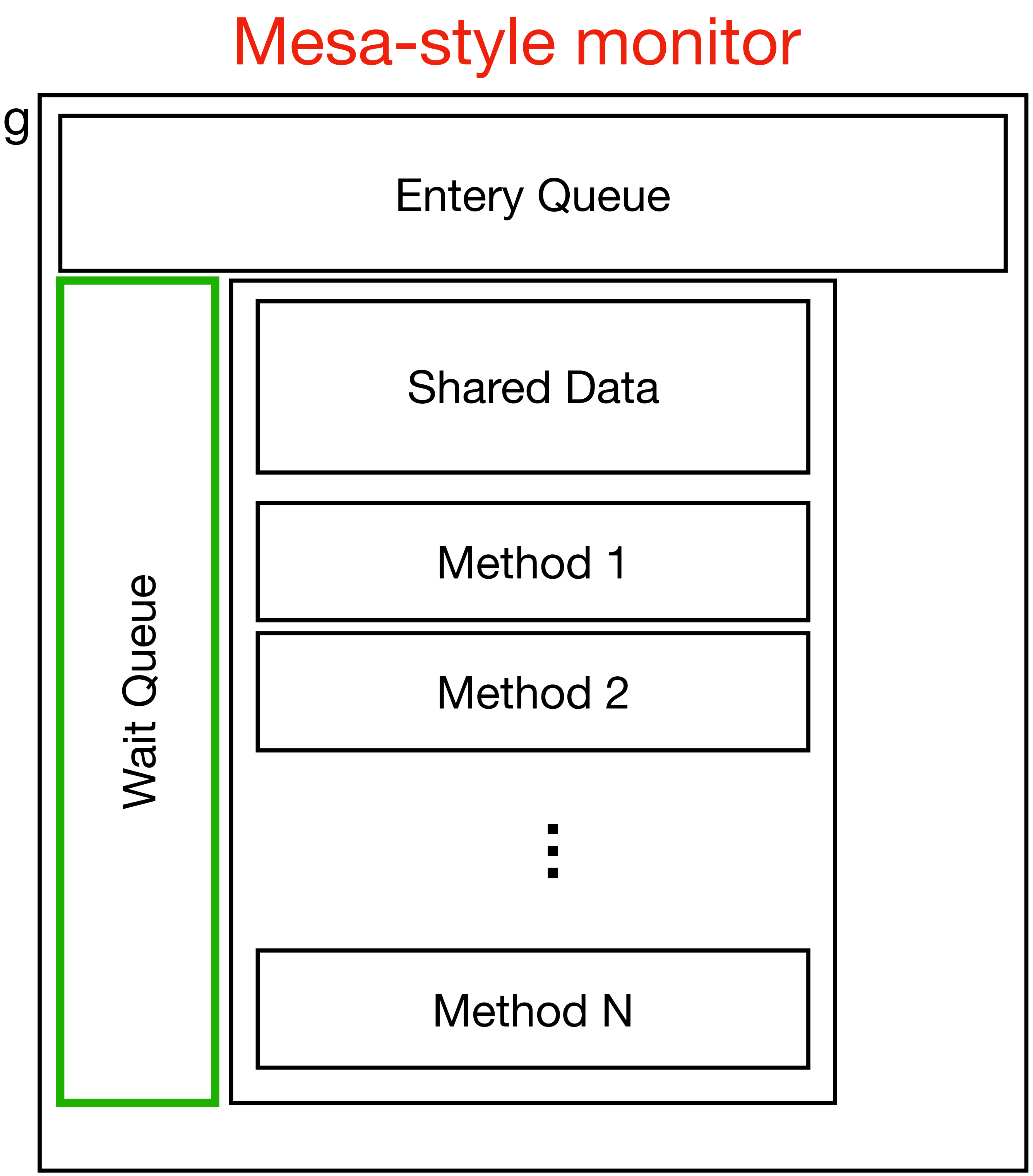
```
Class CokeMachine{
     …
     storage for cokes (buffer)
     Lock lock;                          // a shared lock
     int count = 0;
     Condition notFull, notEmpty;
}

CokeMachine::Deposit(){
     lock->acquire( );
     while(count == n)
        notFull.wait(&lock);
     add coke to the machine;
     count++;
     notEmpty.notify();
     lock->release();
}

CokeMachine::Remove(){
     lock->acquire();
     while(count == 0)
        notEmpty.wait(&lock);
     remove coke from the machine;
     count--;
     notFull.notify();
     lock->release();
}
```

Monitor implementation with semaphores

- there is an entry queue (binary semaphore) for the entire class
- there is a wait queue for every counting semaphore defined inside the class



What if a thread frees a resource needed by a waiting thread?

- should the waiting thread be immediately awakened or should the signalling thread finish first?
  - this gives rises to different versions of monitor semantics

```
CokeMachine::Deposit(){
    lock->acquire( );
    while(count == n)
       notFull.wait(&lock);
    add coke to the machine;
    count++;
    notEmpty.notify();
    lock->release();
}

CokeMachine::Remove(){
    lock->acquire();
    while(count == 0)
       notEmpty.wait(&lock);
    remove coke from the machine;
    count--;
    notFull.notify();
    lock->release();
}
```

thread A is put to sleep after releasing the lock

What if a thread frees a resource needed by a waiting thread?

- should the waiting thread be immediately awakened or should the signalling thread finish first?
  - this gives rises to different versions of monitor semantics

```
CokeMachine::Deposit(){
    lock->acquire( );
    while(count == n)
       notFull.wait(&lock);
    add coke to the machine;
    count++;
    notEmpty.notify();
    lock->release();
}
```

thread A is put to sleep after releasing the lock

```
CokeMachine::Remove(){
    lock->acquire();
    while(count == 0)
       notEmpty.wait(&lock);
    remove coke from the machine;
    count--;
    notFull.notify();
    lock->release();
}
```

thread B removes a coke so thread A can resume execution now

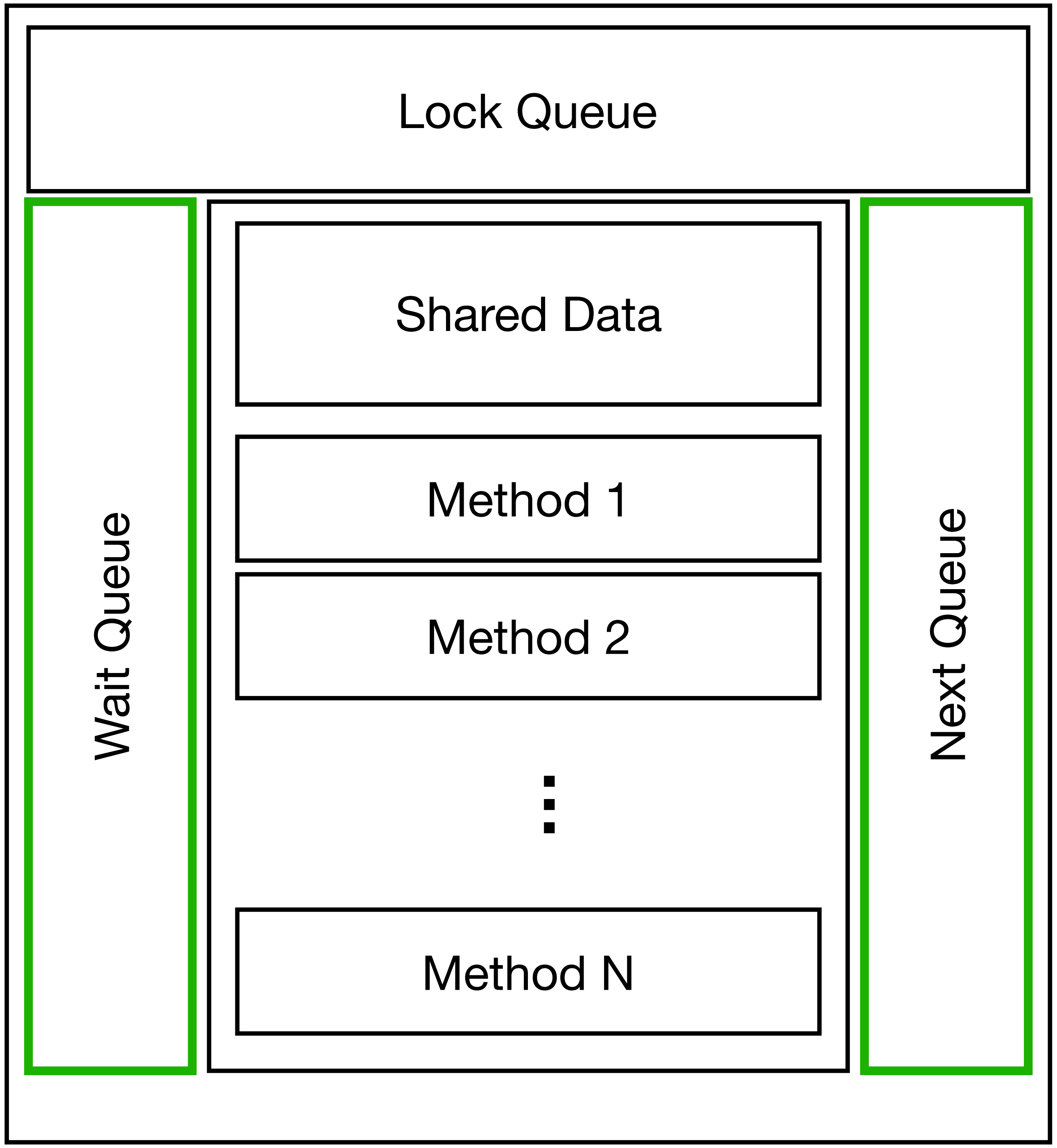
Two types of monitors

- Mesa-style monitors (used in most real operating systems)
  - signal puts a waiting thread on ready queue (with no special priority) but the signalling thread keeps the lock and thus the processor
    - some other thread could grab the lock before the waiting thread gets to run
    - hence, the waiting thread may have to wait again after it is woken up (the condition may not be met at that time)!
- Hoare-style monitors (not commonly used but presented in textbooks)
  - signalling thread gives the processor and the lock to the waiting thread which should immediately execute
  - when the waiting finishes or waits again, processor and lock are given back to the signalling thread
    - so the signalling thread should be kept in another queue known as the signal queue

Monitor implementation with semaphores

- there is an lock queue (binary semaphore) for the entire class
- there is a wait queue for every counting semaphore defined inside the class
- there is a next queue for every counting semaphore defined inside the class

Hoare-style monitor



Implications

- with Mesa semantics, you always have to check the condition after waking up (done in a while loop)
  - efficient implementation but can lead to concurrency bugs if the condition is not checked again

Implications

- with Mesa semantics, you always have to check the condition after waking up (done in a while loop)
    - efficient implementation but can lead to concurrency bugs if the condition is not checked again

```
CokeMachine::Deposit(){
    lock->acquire( );
    while(count == n)
       notFull.wait(&lock);
    add coke to the machine;
    count++;
    notEmpty.notify();
    lock->release();
}
```

Implications

- with Mesa semantics, you always have to check the condition after waking up (done in a while loop)
  - efficient implementation but can lead to concurrency bugs if the condition is not checked again
- with Hoare semantics, you can assume that the condition holds after wait (‘while’ can be replaced with ‘if’)
  - inefficient and much more complicated, but leads to a nicer proof of correctness

```
CokeMachine::Deposit(){
    lock->acquire( );
    while(count == n)
       notFull.wait(&lock);
    add coke to the machine;
    count++;
    notEmpty.notify();
    lock->release();
}
```

```
CokeMachine::Deposit(){
    lock->acquire( );
    if(count == n)
       notFull.wait(&lock);
    add coke to the machine;
    count++;
    notEmpty.notify();
    lock->release();
}
```

EXAMPLES OF MESA-STYLE MONITOR

Monitor in the Producer-Consumer problem

- use a binary semaphore for mutual exclusion
- use counting semaphores **for each constraint**
- putting them together:

```
Semaphore mutex;
Semaphore full_buffer;
Semaphore empty_buffer;
```

Monitor implementation with semaphores

```
class BoundedBuffer {
  public:
    void Producer();
    void Consumer();
  private:
    /* shared data */
    Items buffer;
    int last, count;
    /* shared data */

    Semaphore mutex; // control access to buffers
    Semaphore empty; // number of free slots
    Semaphore full;  // number of used slots
}

BoundedBuffer::BoundedBuffer(int N){
  mutex.value = 1;   // initially free
  empty.value = N;   // initially all slots are empty
  full.value  = 0;   // initially all slots are empty

  buffer = new Items[N];
  last = 0;
  count = 0;
}
```

Monitor implementation with semaphores

```
BoundedBuffer::Producer(){
  <produce item>
  empty.Wait();   // one fewer full slot, or wait
  mutex.Wait();   // entering critical section to access buffer
  <add item to buffer>
  mutex.Signal(); // leaving critical section
  full.Signal();  // one more used slot
}

BoundedBuffer::Consumer(){
  full.Wait();    // one fewer full slot, or wait
  mutex.Wait();   // entering critical section to access buffer
  <remove item from buffer>
  mutex.Signal(); // leaving critical section
  empty.Signal(); // one more free slot
}
```

Monitor implementation with semaphores

```
BoundedBuffer::Producer(){
  <produce item>
  empty.Wait();   // one fewer full slot, or wait
  mutex.Wait();   // entering critical section to access buffer
  <add item to buffer>
  mutex.Signal(); // leaving critical section
  full.Signal();  // one more used slot
}

BoundedBuffer::Consumer(){
  full.Wait();    // one fewer full slot, or wait
  mutex.Wait();   // entering critical section to access buffer
  <remove item from buffer>
  mutex.Signal(); // leaving critical section
  empty.Signal(); // one more free slot
}
```

what if there are multiple producers and/or consumers?

Monitor implementation with semaphores

```
BoundedBuffer::Producer(){
  <produce item>
  empty.Wait();   // one fewer full slot, or wait
  mutex.Wait();   // entering critical section to access buffer
  <add item to buffer>
  mutex.Signal(); // leaving critical section
  full.Signal();  // one more used slot
}

BoundedBuffer::Consumer(){
  full.Wait();    // one fewer full slot, or wait
  mutex.Wait();   // entering critical section to access buffer
  <remove item from buffer>
  mutex.Signal(); // leaving critical section
  empty.Signal(); // one more free slot
}
```

what if there are multiple producers and/or consumers?

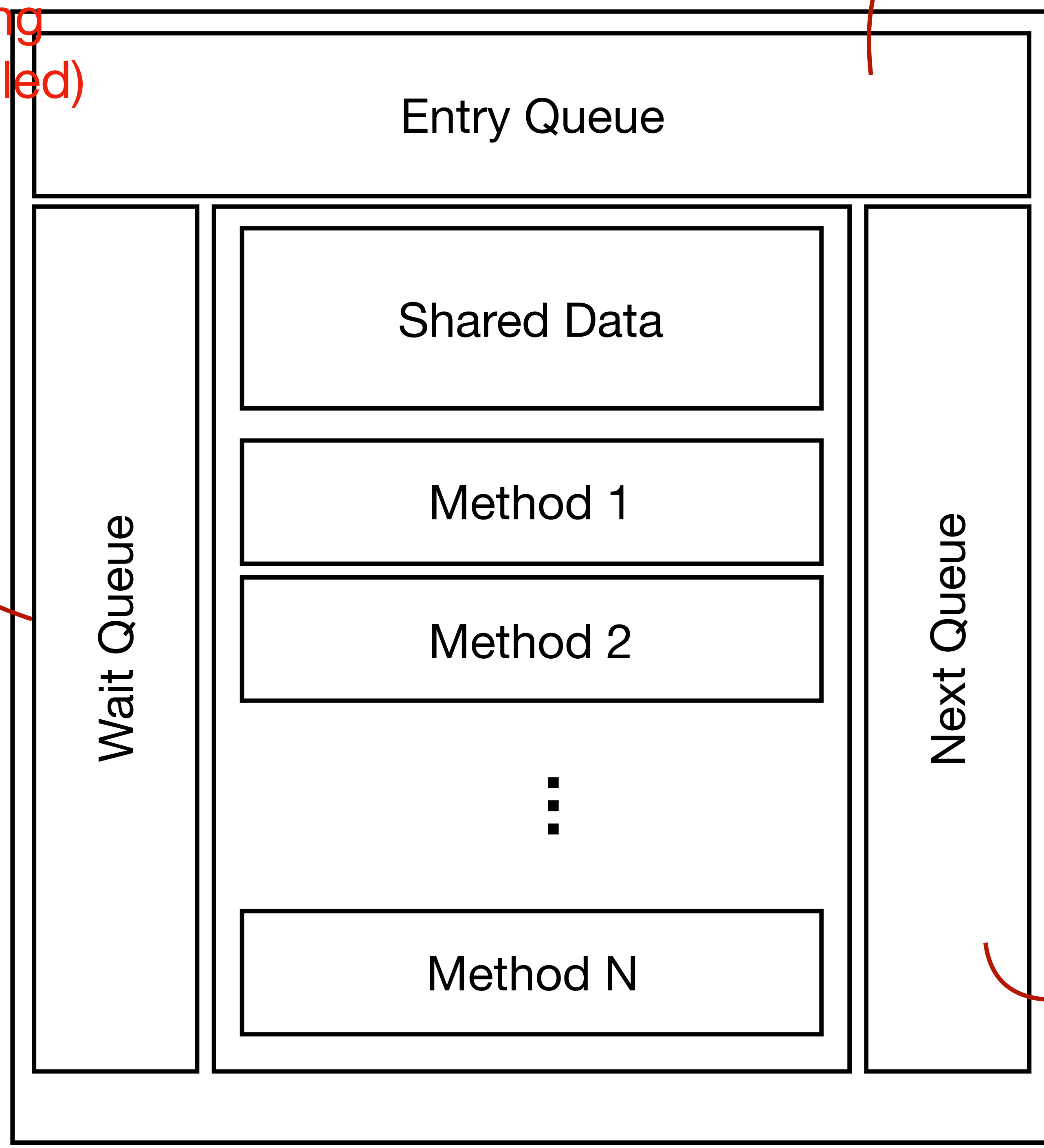
it still works!

EXAMPLES OF HOARE-STYLE MONITOR

How does it work?

queue of threads waiting for a condition inside a monitor method (i.e., counting semaphore is signalled)

queue of a binary semaphore ensuing that one thread may execute a given monitor method at a time



queue of threads signalled counting semaphore (they have to wait now if there was a thread waiting for th condition)

Hoare Monitor implementation with semaphores

```
class Monitor {
  public:
    void ConditionWait();   // calls cvar.wait() and implements Hoare semantics
    void ConditionSignal(); // calls cvar.singal() and implements Hoare semantics
    void someMethod();      // user-defined methods working on shared data

  private:
    <shared data>;      // data being protected by monitor
    semaphore lock;     // controls entry to monitor

    semaphore cvar;     // suspends a thread on a wait
    int waiters_cvar;   // number of threads waiting on a cvar

    semaphore next;     // suspends this thread when signalling another
    int waiters_next;   // number of threads suspended on next
}

Monitor::Monitor(int N) {
  cvar = N; // initialized to N
  lock = 1; // initialized to 1 as nobody is in the monitor
  next = 0; // initialized to 0 as nobody is suspended because of signalling
  waiters_next = 0;
  waiters_cvar = 0;
}
```

Monitor implementation with semaphores

```
void Monitor::ConditionWait() {
  waiters_cvar += 1;// increment the number of waiters
  if(waiters_next > 0)
    next.Signal();  // resume a suspended thread
  else
    lock.Signal();  // allow a new thread in the monitor
  cvar.wait();      // wait on the condition
  waiters_cvar -= 1;// on waking up decrement the number of waiters
}

void Monitor::ConditionSignal() {
  if (waiters_cvar > 0) { // don't signal cvar if nobody is waiting
    waiters_next += 1; // increment the number of suspended threads
    cvar.Signal();     // awaken a waiting thread
    next.Wait();       // wait for it to finish or wait again
    waiters_next -= 1; // decrement the number of suspended threads
  }
}
```

Using the monitor class

```
void Monitor::someMethod() {
  lock.Wait();     // lock the monitor
  <ops on data and calls to ConditionWait() and ConditionSignal()>
  if (waiters_next > 0)
    next.Signal(); // resume a suspended thread
  else
    lock.Signal(); // allow a new thread into the monitor
}
```