CS370 Operating Systems

Colorado State University
Yashwant K Malaiya
Spring 1018 L10
Synchronization

Slides based on
• Text by Silberschatz, Galvin, Gagne
• Various sources
Process Synchronization: Objectives

- Concept of process synchronization.
- The critical-section problem, whose solutions can be used to ensure the consistency of shared data
- Software and hardware solutions of the critical-section problem
- Classical process-synchronization problems
- Tools that are used to solve process synchronization problems
Process Synchronization

EW Dijkstra *Go To Statement Considered Harmful*
<table>
<thead>
<tr>
<th>Time</th>
<th>Person A</th>
<th>Person B</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:30</td>
<td><strong>Look in fridge. Out of milk.</strong></td>
<td></td>
</tr>
<tr>
<td>12:35</td>
<td>Leave for store.</td>
<td></td>
</tr>
<tr>
<td>12:40</td>
<td>Arrive at store.</td>
<td><strong>Look in fridge. Out of milk.</strong></td>
</tr>
<tr>
<td>12:45</td>
<td>Buy milk.</td>
<td>Leave for store.</td>
</tr>
<tr>
<td>12:50</td>
<td>Arrive home, <strong>put milk away.</strong></td>
<td>Arrive at store.</td>
</tr>
<tr>
<td>12:55</td>
<td></td>
<td>Buy milk.</td>
</tr>
<tr>
<td>1:00</td>
<td></td>
<td>Arrive home, <strong>put milk away.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Oh no!</td>
</tr>
</tbody>
</table>
• Processes can execute concurrently
  – May be interrupted at any time, partially completing execution
• Concurrent access to shared data may result in data inconsistency
• Maintaining data consistency requires mechanisms to ensure the orderly execution of cooperating processes
• **Illustration:** we wanted to provide a solution to the consumer-producer problem that fills *all* the buffers.
  – have an integer `counter` that keeps track of the number of full buffers.
  – Initially, `counter` is set to 0.
  – It is incremented by the producer after it produces a new buffer
  – decremented by the consumer after it consumes a buffer.

Will it work without any problems?
Consumer-producer problem

Producer

```java
while (true) {
    /* produce an item*/
    while (counter == BUFFER_SIZE) ;
    /* do nothing */
    buffer[in] = next_produced;
    in = (in + 1) % BUFFER_SIZE;
    counter++;
}
```

Consumer

```java
while (true) {
    while (counter == 0);
    /* do nothing */
    next_consumed = buffer[out];
    out = (out + 1) % BUFFER_SIZ
    counter--;
    /* consume the item in
    next consumed */
}
```

They run “concurrently” (or in parallel), and are subject to context switches at unpredictable times.

_In, out: indices of empty and filled items in the buffer._
Race Condition

Consider this execution interleaving with “count = 5” initially:

S0: producer execute \textit{register1} = \textit{counter} \quad \{\text{register1} = 5\}
S1: producer execute \textit{register1} = \textit{register1} + 1 \quad \{\text{register1} = 6\}
S2: consumer execute \textit{register2} = \textit{counter} \quad \{\text{register2} = 5\}
S3: consumer execute \textit{register2} = \textit{register2} - 1 \quad \{\text{register2} = 4\}
S4: producer execute \textit{counter} = \textit{register1} \quad \{\text{counter} = 6\}
S5: consumer execute \textit{counter} = \textit{register2} \quad \{\text{counter} = 4\}

\texttt{counter++} could be compiled as
\texttt{counter--} could be compiled as

\begin{align*}
\textit{register1} &= \textit{counter} \\
\textit{register1} &= \textit{register1} + 1 \\
\textit{counter} &= \textit{register1} \\
\textit{register2} &= \textit{counter} \\
\textit{register2} &= \textit{register2} - 1 \\
\textit{counter} &= \textit{register2}
\end{align*}

They run concurrently, and are subject to context switches at unpredictable times.

Overwrites!
Critical Section Problem

We saw race condition between counter ++ and counter –

Solution to the “race condition” problem: critical section

- Consider system of $n$ processes $\{p_0, p_1, \ldots, p_{n-1}\}$
- Each process has critical section segment of code
  - Process may be changing common variables, updating table, writing file, etc
  - When one process in critical section, no other may be in its critical section
- Critical section problem is to design protocol to solve this
- Each process must ask permission to enter critical section in entry section, may follow critical section with exit section, then remainder section

Race condition: when outcome depends on timing/order that is not predictable
Process Synchronization: Outline

- Process synchronization: critical-section problem to ensure the consistency of shared data
- Software and hardware solutions of the critical-section problem
  - Peterson’s solution
  - Atomic instructions
  - Mutex locks and semaphores
- Classical process-synchronization problems
  - Bounded buffer, Readers Writers, Dining Philosophers
- Another approach: Monitors
do { 
  entry section
  critical section
  exit section
  remainder section
} while (true);

Request permission to enter
Housekeeping to let processes to enter other
Algorithm for Process $P_i$

do {
    while (turn == j);
    turn = j;
} while (true);

$P_i$ Waits to enter
$P_i$ Executes critical section
$P_i$ lets $j$ enter critical section
1. **Mutual Exclusion** - If process $P_i$ is executing in its critical section, then no other processes can be executing in their critical sections

2. **Progress** - If no process is executing in its critical section and there exist some processes that wish to enter their critical section, then the selection of the processes that will enter the critical section next cannot be postponed indefinitely

3. **Bounded Waiting** - A bound must exist on the number of times that other processes are allowed to enter their critical sections after a process has made a request to enter its critical section and before that request is granted
   - Assume that each process executes at a nonzero speed
   - No assumption concerning relative speed of the $n$ processes
Two approaches depending on if kernel is preemptive or non-preemptive

- **Preemptive** – allows preemption of process when running in kernel mode
- **Non-preemptive** – runs until exits kernel mode, blocks, or voluntarily yields CPU
  - Essentially free of race conditions in kernel mode
Peterson’s Solution

- Good algorithmic description of solving the problem
- Two process solution only
- Assume that the load and store machine-language instructions are atomic; that is, cannot be interrupted
- The two processes share two variables:
  - int turn;
  - Boolean flag[2]
- The variable turn indicates whose turn it is to enter the critical section
- The flag array is used to indicate if a process is ready to enter the critical section. flag[i] = true implies that process \( P_i \) is ready!
Algorithm for Process $P_i$

For process $P_i$ do

{
    flag[$i$] = true;
    turn = $j$;
    while (flag[$j$] && turn == $j$);  /*Wait*/

    critical section

    flag[$i$] = false;

    remainder section

} while (true);

• The variable turn indicates whose turn it is to enter the critical section
• The flag array is used to indicate if a process is ready to enter the critical section. flag[$i$] = true implies that process $P_i$ is ready!
Provable that the three CS requirement are met:

1. Mutual exclusion is preserved
   \( P_i \) enters CS only if:
   
   either \( \text{flag}[j] = \text{false} \) or \( \text{turn} = i \)

2. Progress requirement is satisfied

3. Bounded-waiting requirement is met

Detailed proof in the text.

Note: there exists a generalization of Peterson’s solution for more than 2 processes, but bounded waiting is not assured.
Synchronization: Hardware Support

• Many systems provide hardware support for implementing the critical section code.
• All solutions below based on idea of locking
  – Protecting critical regions via locks
• Modern machines provide special atomic hardware instructions
  • **Atomic** = non-interruptible
    – test memory word and set value
    – swap contents of two memory words
Solution using `test_and_set()`

- Shared Boolean variable `lock`, initialized to FALSE
- Solution:
  ```c
  do {
    while (test_and_set(&lock)); /* do nothing */

    /* critical section */
    ....
    lock = false;
    /* remainder section */
    ...
  } while (true);
  ```

To break out:
Return value of `TestAndSet` should be FALSE

Lock FALSE: not locked.
If two `TestAndSet()` are executed simultaneously, they will be executed sequentially in some arbitrary order.

test_and_set(&lock) returns the lock value and sets it to True.
void Swap(boolean *a, boolean *b) {
    boolean temp = *a;
    *a = *b;
    *b = temp;
}
do {
    key = TRUE;
    while (key == TRUE) {
        Swap(&lock, &key)
    }
}
critical section
lock = FALSE;
remainder section
} while (TRUE);

Cannot enter critical section UNLESS lock == FALSE

lock is a SHARED variable key is a LOCAL variable

If two Swap() are executed simultaneously, they will be executed sequentially in some arbitrary order
Bounded-waiting Mutual Exclusion with test_and_set

For process $i$:
do
  \begin{align*}
    \text{waiting}[i] &= \text{true}; \\
    \text{key} &= \text{true}; \\
    \text{while} \ (\text{waiting}[i] \ \&\& \ \text{key}) \\
    &\quad \text{key} = \text{test_and_set}(&\text{lock}); \\
    \text{waiting}[i] &= \text{false}; \\
    /* \text{critical section} */ \\
    j &= (i + 1) \mod n; \\
    \text{while} \ ((j \neq i) \ \&\& \ \text{!waiting}[j]) \\
    &\quad j &= (j + 1) \mod n; \\
    \text{if} \ (j == i) \\
    &\quad \text{lock} &= \text{false}; \\
    \text{else} \\
    &\quad \text{waiting}[j] &= \text{false}; \\
    /* \text{remainder section} */
  \end{align*}
} while (true);

**Shared** Data structures initialized to FALSE
  - boolean waiting[n];
  - boolean lock;

The entry section for process $i$:
  - First process to execute TestAndSet will find key == false ; ENTER critical section,
  - EVERYONE else must wait

The exit section for process $i$:
Part I: Finding a suitable waiting process $j$ and enable it to get through the while loop, or if there is no suitable process, make lock FALSE.
The previous algorithm satisfies the three requirements

- **Mutual Exclusion**: The first process to execute TestAndSet(lock) when lock is false, will set lock to true so no other process can enter the CS.

- **Progress**: When a process exits the CS, it either sets lock to false, or waiting[j] to false (allowing j to get in), allowing the next process to proceed.

- **Bounded Waiting**: When a process exits the CS, it examines all the other processes in the waiting array in a circular order. Any process waiting for CS will have to wait at most n-1 turns.
Mutex Locks

- Previous solutions are complicated and generally inaccessible to application programmers
- OS designers build software tools to solve critical section problem
- Simplest is mutex lock
- Protect a critical section by first acquire() a lock then release() the lock
  - Boolean variable indicating if lock is available or not
- Calls to acquire() and release() must be atomic
  - Usually implemented via hardware atomic instructions
- But this solution requires busy waiting
  - This lock therefore called a spinlock
acquire() and release()

<table>
<thead>
<tr>
<th>acquire()</th>
<th>release()</th>
</tr>
</thead>
<tbody>
<tr>
<td>{</td>
<td>{</td>
</tr>
<tr>
<td>\begin{verbatim}</td>
<td>available = true;</td>
</tr>
<tr>
<td>while (!available)</td>
<td>}</td>
</tr>
<tr>
<td>; /* busy wait */</td>
<td>}</td>
</tr>
<tr>
<td>\end{verbatim}</td>
<td>}</td>
</tr>
</tbody>
</table>

*Usage*

do {  
\begin{verbatim}  
acquire lock
\end{verbatim}  
critical section
\begin{verbatim}  
release lock
\end{verbatim}  
remainder section
} while (true);
acquire() and release()

Process 0
- Start acquire, get lock
- Critical section
- Release lock

Lock
- Locked by Process 0
- Locked by Process 1

Process 1
- Start acquire
- Busy waiting
- Gets lock
- Critical section
- Release lock
### acquire() and release()

<table>
<thead>
<tr>
<th>Process 0</th>
<th>Lock</th>
<th>Process 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>..</td>
<td>open</td>
<td>Attempt to acquire lock</td>
</tr>
<tr>
<td>..</td>
<td>closed</td>
<td>Acquires lock</td>
</tr>
<tr>
<td>Attempt to acquire lock</td>
<td>closed</td>
<td>Critical section</td>
</tr>
<tr>
<td>Attempt to acquire lock</td>
<td>closed</td>
<td>Critical section</td>
</tr>
<tr>
<td>Attempt to acquire lock</td>
<td>open</td>
<td>Release lock</td>
</tr>
<tr>
<td>Acquires lock</td>
<td>closed</td>
<td>..</td>
</tr>
<tr>
<td><strong>Critical section</strong></td>
<td>closed</td>
<td>..</td>
</tr>
</tbody>
</table>
• Synchronization tool that provides more sophisticated ways (than Mutex locks) for process to synchronize their activities.
• Semaphore $S$ – integer variable
• Can only be accessed via two indivisible (atomic) operations
  – wait() and signal()
    • Originally called $P()$ and $V()$ based on Dutch words
• Definition of the wait() operation
  
  \[
  \text{wait}(S) \{
  \text{while } (S \leq 0) \;
  \text{; // busy wait} \\
  S--; \\
  \}
  \]
• Definition of the signal() operation
  
  \[
  \text{signal}(S) \{ \\
  S++; \\
  \}
  \]

Waits until another process makes $S=1$

Binary semaphore: When $s$ is 0 or 1, it is a mutex lock
Wait(S) and Signal (S)

Process 0
- Wait(S)
- Critical section
- Signal (S)

Semaphore S
- S = 1
- S = 0
- S = 1
- Locked by Process 1

Process 1
- Wait (S)
- Busy waiting
- Gets lock, S -
- Critical section
- Signal (S)

State University
### acquire() and release()

<table>
<thead>
<tr>
<th>Process 0</th>
<th>Semaphore S</th>
<th>Process 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical section</strong></td>
<td>0</td>
<td>wait ( ), busy waiting</td>
</tr>
<tr>
<td><strong>Signal ( ) S++</strong></td>
<td>1</td>
<td>Waiting, finished</td>
</tr>
<tr>
<td>..</td>
<td>0</td>
<td>S- -</td>
</tr>
<tr>
<td><strong>Wait( )</strong></td>
<td>0</td>
<td>Critical section</td>
</tr>
<tr>
<td><strong>Wait( )</strong></td>
<td>0</td>
<td>Critical section</td>
</tr>
<tr>
<td><strong>Waiting finished</strong></td>
<td>1</td>
<td>Signal ( ) S++</td>
</tr>
<tr>
<td><strong>S--</strong></td>
<td>0</td>
<td>..</td>
</tr>
<tr>
<td><strong>Critical section</strong></td>
<td>0</td>
<td>..</td>
</tr>
</tbody>
</table>
Semaphore Usage

- **Counting semaphore** – integer value can range over an unrestricted domain
- **Binary semaphore** – integer value can range only between 0 and 1
  - Same as a mutex lock
- Can solve various synchronization problems
- Consider $P_1$ and $P_2$ that require $S_1$ to happen before $S_2$
  Create a semaphore “synch” initialized to 0
  
  $P_1:$
  
  $S_1;$
  
  signal(synch);
  
  $P_2:$
  
  wait(synch);
  
  $S_2;$

- Can implement a counting semaphore $S$ as a binary semaphore
The counting semaphore

- Controls access to a finite set of resources
- Initialized to the number of resources
- Usage:
  - Wait (S): to use a resource
  - Signal (S): to release a resource
- When all resources are being used: $S == 0$
  - Block until $S > 0$ to use the resource
Semaphore Implementation

- Must guarantee that no two processes can execute the `wait()` and `signal()` on the same semaphore at the same time
- Thus, the implementation becomes the critical section problem where the `wait` and `signal` code are placed in the critical section
  - Could now have **busy waiting** in critical section implementation
    - But implementation code is short
    - Little busy waiting if critical section rarely occupied
- Note that applications may spend lots of time in critical sections and therefore this is not a good solution
- Alternative: block and wakeup (next slide)
wait(semaphore *S) {
    S->value--;
    if (S->value < 0) {
        add this process to S->list;
        block();
    }
}

signal(semaphore *S) {
    S->value++;
    if (S->value <= 0) {
        remove a process P from S->list;
        wakeup(P);
    }
}

typedef struct{
    int value;
    struct process *list;
} semaphore;

If value < 0
abs(value) is the number of waiting processes
Classical Problems of Synchronization

- Classical problems used to test newly-proposed synchronization schemes
  - Bounded-Buffer Problem
  - Readers and Writers Problem
  - Dining-Philosophers Problem
- Monitors
Bounded-Buffer Problem

- \( n \) buffers, each can hold one item
- Binary semaphore (mutex)
  - Provides mutual exclusion for accesses to buffer pool
  - Initialized to 1
- Counting semaphores
  - empty: Number of empty slots available
    - Initialized to \( n \)
  - full: Number of filled slots available \( n \)
    - Initialized to 0
Problems with Semaphores

- Incorrect use of semaphore operations:
  - Omitting of wait (mutex)
    - Violation of mutual exclusion
  - or signal (mutex)
    - Deadlock!
Monitors
Monitors

• Monitor: A high-level abstraction that provides a convenient and effective mechanism for process synchronization
• Abstract data type, internal variables only accessible by code within the procedure
• Only one process may be active within the monitor at a time
  – Automatically provide mutual exclusion
• Originally proposed for Concurrent Pascal 1975
• Directly supported by Java but not C