CS370 Operating Systems
Colorado State University
Yashwant K Malaiya
Spring 1019 L10
Synchronization

Slides based on
• Text by Silberschatz, Galvin, Gagne
• Various sources
• Development project: You need to get your own board/hardware and locate the software needed.
• What if processes have the same priority?
• Time quantum - How?
  – Rule of thumb: 80% of CPU bursts should be shorter than q
• Thread scheduling similar to process scheduling
  – process-contention scope (PCS) vs system-contention scope (SCS)
• Multiple processor vs multicore
• Non-uniform memory access: Multiple processor system with some memory closer to each processor
Example of Multilevel Feedback Queue

• Three queues:
  – $Q_0$ – RR with time quantum 8 milliseconds
  – $Q_1$ – RR time quantum 16 milliseconds
  – $Q_2$ – FCFS (no time quantum limit)

• Scheduling
  – A new job enters queue $Q_0$ which is served FCFS
    • When it gains CPU, job receives 8 milliseconds
    • If it does not finish in 8 milliseconds, job is moved to queue $Q_1$
  – At $Q_1$ job is again served FCFS and receives 16 additional milliseconds
    • If it still does not complete, it is preempted and moved to queue $Q_2$

Details at ARPACI-DUSSEAU
Operating System Examples

- Solaris scheduling: 6 classes, Inverse relationship between priorities and time quantum
- Windows XP scheduling: 32 priority levels (real-time, not real-time levels)
- Linux scheduling schemes have continued to evolve.
- Linux Completely fair scheduler (CFS, 2007):
  - Variable time-slice based on number and priority of the tasks in the queue.
  - Maximum execution time based on waiting processes (Q/n).
  - Processes kept in a red-black binary tree with scheduling complexity of $O(\log N)$
  - Process with lowest weighted spent execution (virtual run time) time is picked next. Weighted by priority (“niceness”).
Algorithm Evaluation

• How to select CPU-scheduling algorithm for an OS?
• Determine criteria, then evaluate algorithms
• **Deterministic modeling**
  – Type of **analytic evaluation**
  – Takes a particular predetermined workload and defines the performance of each algorithm for that workload
• Consider 5 processes arriving at time 0:

<table>
<thead>
<tr>
<th>Process</th>
<th>Burst Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1$</td>
<td>10</td>
</tr>
<tr>
<td>$P_2$</td>
<td>29</td>
</tr>
<tr>
<td>$P_3$</td>
<td>3</td>
</tr>
<tr>
<td>$P_4$</td>
<td>7</td>
</tr>
<tr>
<td>$P_5$</td>
<td>12</td>
</tr>
</tbody>
</table>
Deterministic Evaluation

- For each algorithm, calculate minimum average waiting time
- Simple and fast, but requires exact numbers for input, applies only to those inputs
  - FCS is 28ms:
  - Non-preemptive SFJ is 13ms:
  - RR is 23ms:

<table>
<thead>
<tr>
<th>Process</th>
<th>Burst Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>P₁</td>
<td>10</td>
</tr>
<tr>
<td>P₂</td>
<td>29</td>
</tr>
<tr>
<td>P₃</td>
<td>3</td>
</tr>
<tr>
<td>P₄</td>
<td>7</td>
</tr>
<tr>
<td>P₅</td>
<td>12</td>
</tr>
</tbody>
</table>
Probabilistic Models

- Assume that the arrival of processes, and CPU and I/O bursts are random
  - Repeat deterministic evaluation for many random cases and then average

- Approaches:
  - Analytical: Queuing models
  - Simulation: simulate using realistic assumptions
Queueing Models

• Describes the arrival of processes, and CPU and I/O bursts probabilistically
  – Commonly exponential, and described by mean
  – Computes average throughput, utilization, waiting time, etc

• Computer system described as network of servers, each with queue of waiting processes
  – Knowing arrival rates and service rates
  – Computes utilization, average queue length, average wait time, etc
Little’s Formula for avg Queue Length

- \( n \) = average queue length
- \( W \) = average waiting time in queue
- \( \lambda \) = average arrival rate into queue
- Little’s law – in steady state, processes leaving queue must equal processes arriving, thus:
  \[ n = \lambda x W \]
  – Valid for any scheduling algorithm and arrival distribution
- For example, if on average 7 processes arrive per second, and normally 14 processes in queue, then average wait time per process = 2 seconds
Simulations

• Queueing models limited

• **Simulations** more accurate
  – Programmed model of computer system
  – Clock is a variable
  – Gather statistics indicating algorithm performance
  – Data to drive simulation gathered via
    • Random number generator according to probabilities
    • Distributions defined mathematically or empirically
    • Trace tapes record sequences of real events in real systems
Evaluation of CPU Schedulers by Simulation

- Actual process execution
  - CPU 10
  - I/O 213
  - CPU 12
  - I/O 112
  - CPU 2
  - I/O 147
  - CPU 173

- Trace tape

- Simulation
  - FCFS
  - SJF
  - RR (q = 14)

Performance statistics for FCFS
Performance statistics for SJF
Performance statistics for RR (q = 14)
Implementation

- Even simulations have limited accuracy
- Just implement new scheduler and test in real systems
  - High cost, high risk
  - Environments vary
- Most flexible schedulers can be modified per-site or per-system
- Or APIs to modify priorities
- But again environments vary
CS370 Operating Systems
Colorado State University
Yashwant K Malaiya
Spring 1019
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*
### Too Much Milk Example

<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><strong>Leave for store.</strong></td>
<td><strong>Look in fridge. Out of milk.</strong></td>
</tr>
<tr>
<td>12:40</td>
<td><strong>Arrive at store.</strong></td>
<td><strong>Leave for store</strong></td>
</tr>
<tr>
<td>12:45</td>
<td><strong>Buy milk.</strong></td>
<td><strong>Arrive at store.</strong></td>
</tr>
<tr>
<td>12:50</td>
<td><strong>Arrive home, put milk away.</strong></td>
<td><strong>Buy milk</strong></td>
</tr>
<tr>
<td>12:55</td>
<td><strong>Arrive home, put milk away.</strong> Oh no!</td>
<td></td>
</tr>
</tbody>
</table>
Background

• 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

`counter++` could be compiled as

\[
\begin{align*}
&\text{register1} = \text{counter} \\
&\text{register1} = \text{register1} + 1 \\
&\text{counter} = \text{register1}
\end{align*}
\]

`counter--` could be compiled as

\[
\begin{align*}
&\text{register2} = \text{counter} \\
&\text{register2} = \text{register2} - 1 \\
&\text{counter} = \text{register2}
\end{align*}
\]

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

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

\begin{align*}
S0: \text{producer execute } &\text{register1} = \text{counter} & \{\text{register1} = 5\} \\
S1: \text{producer execute } &\text{register1} = \text{register1} + 1 & \{\text{register1} = 6\} \\
S2: \text{consumer execute } &\text{register2} = \text{counter} & \{\text{register2} = 5\} \\
S3: \text{consumer execute } &\text{register2} = \text{register2} - 1 & \{\text{register2} = 4\} \\
S4: \text{producer execute } &\text{counter} = \text{register1} & \{\text{counter} = 6\} \\
S5: \text{consumer execute } &\text{counter} = \text{register2} & \{\text{counter} = 4\}
\end{align*}

Overwrites!
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

- 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
General structure: Critical section

```c
do {
    entry section
    critical section
    exit section
    remainder section
} while (true);
```

- Request permission to enter
- Housekeeping to let other processes to enter
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.
Critical-Section Handling in OS

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 $P_i$

```plaintext
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.

For process $P_i$, $P_j$ runs the same code concurrently.
Peterson’s Solution (Cont.)

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

\[\text{test\_and\_set}(&\text{lock}) \text{ returns the lock value and sets it to True}.\]
Solution using test_and_set()

- Shared Boolean variable lock, initialized to FALSE
- Solution:
  
  ```
  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 attempted simultaneously, they will be executed sequentially in some arbitrary order.
void Swap(boolean *a, boolean *b) {
    boolean temp = *a;
    *a = *b;
    *b = temp;
}

Using Swap (concurrently executed by both)

do {
    key = TRUE;
    while (key == TRUE) {
        Swap(&lock, &key)
    }

    critical section

    lock = FALSE;

    remainder section
} while (TRUE);

Lock == false when no process is in critical section.

Cannot enter critical section UNLESS lock == FALSE by other process

Lock is a SHARED variable.
Key is a variable local to the process.

If two Swap() are executed simultaneously, they will be executed sequentially in some arbitrary order.
Swap()

Process 0

Key = TRUE
Swap( )
Key ==FALSE, enter

Critical section

Lock = FALSE

Locked by Process 0

Lock = TRUE

Locked by Process 1

Process 1

Key = TRUE
Swap( )
Key == TRUE, wait

Busy waiting

Swap( ), Key ==False

Critical section

Lock = FALSE

Colorado State University
For process i:
    do {
        waiting[i] = true;
        key = true;
        while (waiting[i] && key)
            key = test_and_set(&lock);
        waiting[i] = false;
        /* critical section */
        j = (i + 1) % n;
        while ((j != i) && !waiting[j])
            j = (j + 1) % n;
        if (j == i)
            lock = false;
        else
            waiting[j] = false;
        /* remainder section */
    } while (true);

Shared Data structures initialized to FALSE
• boolean waiting[n]; Pr n wants to enter
• 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:
Attempts to finding a suitable waiting process j (while loop) and enable it,
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 $i$ exits the CS, it either sets lock to false, or `waiting[i]` 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>
</table>
| ```
acquire() {
    while (!available)
    ; /* busy wait */
}
``` | ```
release() {
    available = true;
}
``` |

**Usage**

```
do {
    acquire lock
    critical section
    release lock
    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>Critical section</td>
<td>closed</td>
<td>..</td>
</tr>
</tbody>
</table>
How are locks supported by hardware?

- Atomic read-modify-write
- Atomic instruction in x86
  - LOCK instruction prefix, which applies to an instruction does a read-modify-write on memory (INC, XCHG, CMPXCHG etc)
  - Ex: lock cmpxchg <dest>, <source>
- In RISK processors? Instruction-pairs
  - LL (Load Linked Word), SC (Store Conditional Word) instructions in MIPS
  - LDREX, STREX in ARM
  - Creates an atomic sequence
Semaphores by Dijkstra

• 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
  ```c
  wait(S) {
    while (S <= 0) ; // busy wait
    S--;
  }
```
• Definition of the signal() operation
  ```c
  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
- S = 0

Locked by Process 1

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

Locked by Process 1
**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><strong>wait ( ), busy waiting</strong></td>
</tr>
<tr>
<td><strong>Signal ( ) S++</strong></td>
<td><strong>1</strong></td>
<td>Waiting, finished</td>
</tr>
<tr>
<td>..</td>
<td>0</td>
<td><strong>S- -</strong></td>
</tr>
<tr>
<td><strong>Wait( )</strong></td>
<td>0</td>
<td><strong>Critical section</strong></td>
</tr>
<tr>
<td><strong>Wait( )</strong></td>
<td>0</td>
<td><strong>Critical section</strong></td>
</tr>
<tr>
<td><strong>Waiting finished</strong></td>
<td><strong>1</strong></td>
<td><strong>Signal ( ) S++</strong></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

<table>
<thead>
<tr>
<th>P1:</th>
<th>P2:</th>
</tr>
</thead>
</table>
| $S_1$;  
signal(synch); | 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).
Semaphore Implementation with no Busy waiting

• With each semaphore there is an associated waiting queue
• Each entry in a waiting queue has two data items:
  – value (of type integer)
  – pointer to next record in the list
• Two operations:
  – block – place the process invoking the operation on the appropriate waiting queue
  – wakeup – remove one of processes in the waiting queue and place it in the ready queue

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