CS 537: Introduction to Operating Systems (Summer 2017)
University of Wisconsin-Madison
Department of Computer Sciences

Midterm Exam 2

July 21st, 2017

3 pm - 5 pm

There are sixteen (16) total numbered pages with ten (10) questions.

PLEASE READ ALL QUESTIONS CAREFULLY!

There are many easy questions and a few hard questions in this exam. You may want to use a easiest-question-first scheduling policy. This will help you to answer most questions on this exam without getting stuck on a single hard question. The last 2 questions are worth 20 points each. All other questions are worth 10 points each.

Good luck with your exam!

Please write your FULL NAME and UW ID below.

NAME: ____________________

GÉRALD

UW ID: ____________________
<table>
<thead>
<tr>
<th>Question</th>
<th>Points Scored</th>
<th>Maximum Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>20</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>120</strong></td>
</tr>
</tbody>
</table>
1. Page Replacement Policies

a. Consider the following request sequence of virtual pages

\[ 3, 2, 1, 0, 3, 2, 4, 3, 2, 1, 0, 4 \]

For each replacement policy below, give the number of hits and the virtual page numbers remaining in physical memory at the end of this request sequence.

The number of physical frames = 4

<table>
<thead>
<tr>
<th>Policy</th>
<th># of Hits</th>
<th>VPNs remaining at end</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPT</td>
<td>6</td>
<td>0, 4, any two of (1, 2, 3)</td>
</tr>
<tr>
<td>FIFO</td>
<td>2</td>
<td>0, 1, 2, 4</td>
</tr>
<tr>
<td>LRU</td>
<td>4</td>
<td>0, 1, 2, 4</td>
</tr>
</tbody>
</table>

b. Write a sequence of 10 virtual page requests that has a hit rate of zero with LRU page replacement policy.

Virtual Pages available: 0, 1, 2, 3, 4
The number of physical frames = 4

0, 1, 2, 3, 4, 0, 1, 2, 3, 4 OR any looping sequential pattern.

c. What are the disadvantages of using the following page replacement policies in real-world systems?

i. OPT: Impossible to implement. Cannot predict the future.

ii. FIFO: Exhibits behavior's anomaly & doesn't use any info from past to understand the importance of VP.

iii. LRU: HW cannot fault to the OS for each & every memory access. Also, too much overhead in terms of data structures modification. Access to find the "least" recently used page.
2. Hardware Locks

Suppose we have a new instruction called \texttt{CompareAndRestore (CAR)}, and it does the following \textit{atomically} (here is the C pseudo-code):

```c
int CompareAndRestore(int *ptr, int expected, int new) {
    int original = *ptr;
    if (original != expected)
        *ptr = new;
    return original;
}
```

a. Implement a working \textbf{spin-lock} using the \texttt{CompareAndRestore (CAR)} instruction.

```c
typedef struct __lock_t {
    int isFree;
} lock_t;

void init(lock_t *lock) {
    lock->isFree = 1;
}

void acquire(lock_t *lock) {
    while (CAR(lock->isFree, 0, 0) == 0) // spin
}

void release(lock_t *lock) {
    lock->isFree = 1
}
```

b. How would you \textbf{evaluate} your lock based on the following 2 criteria?

i. \textbf{Fairness}: \textit{Not fair since a thread can starve while trying to acquire the lock.}

ii. \textbf{Performance}: \textit{Not good since spinning unnecessarily wastes CPU cycles.}
3. Segmentation + Paging

In this question, we consider address translation in a system which uses a hybrid of segmentation and paging for memory management. There are three segments namely, code, heap, and stack. The two higher-order bits (MSBs) in the virtual address are used to identify the segment. 00 for code, 01 for heap, and 11 for stack.

Parameters and Assumptions:

- Size of virtual address space = 1 KB
- Page size = 16 bytes
- Size of physical memory = 4 KB
- Size of one Page Table Entry (PTE) = 2 bytes
- The virtual pages with VPNs 0, 1, 16, 17, 18, and 63 are the ONLY valid pages.

Answer the following questions based on the parameters and assumptions described above.

1. Number of bits needed for the Virtual Page Number (VPN):

2. Number of valid virtual pages in the code segment:

3. Value of the bounds register for the heap segment:

4. Number of PTEs in the stack segment’s page table:

5. Total size of ALL the page tables used in this system:
4. Locked Data Structures

Assume you have the following code for removing the head of a shared linked list. Assume each line is performed atomically. Assume a list L originally contains nodes with keys 1, 2, 3 and 4. Now there are two threads T and S that are popping the list concurrently.

```c
typedef struct __node_t {
    int key;
    struct __node_t *next;
} node_t;

typedef struct __list_t {
    node_t *head;
} list_t;

int pop(list_t *L) {
    if (!L->head) return -1;   // line 1
    int rkey = L->head->key;  // line 2
    L->head = L->head->next;  // line 3
    return rkey;              // line 4
}
```

a. Given the following sequences, fill in the results. The sequence contains T and S, designating that one line of C-code was scheduled for the corresponding thread. For example, a sequence of TTSSS indicates that 3 lines were run from thread T followed by 2 lines from thread S. You should assume that each sequence is executed independently. In other words, the state of the linked list is the same (with 4 nodes) at the start of each sequence. The rightmost column in the table below represents the value of L->head->key at the end of the sequence.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>rkey from T</th>
<th>rkey from S</th>
<th>L-&gt;head-&gt;key</th>
</tr>
</thead>
<tbody>
<tr>
<td>2TTSSTTS</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2TTSSTTS</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2TSSSTSS</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2TSSSTTS</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

b. In the pop() method given above, which line(s) of code form the critical section? Our goal here is to maximize the concurrency among threads that are trying to pop from this shared linked list.

```
# points/line of sequence
8x4
```

Lesson: Correctness is more important than performance.
5. TLB, Memory, and Page Faults!

In this question you will examine virtual memory reference traces. An access can be a TLB Hit or a TLB Miss; if it is a TLB miss, the reference can be a page hit (page present in physical memory) or a page fault (page not present in physical memory).

Assume a TLB with 2 entries and a memory that can hold 4 pages. Assume the TLB and memory are initially empty. Finally, assume LRU replacement is used for both TLB and memory.

Below each virtual memory reference, mark if the reference is a:

- TLB Hit (H), or
- TLB Miss followed by a page hit (M), or
- TLB Miss followed by a page fault (F)

Also, write the contents of the TLB and the Memory at the end of each virtual memory trace.

<table>
<thead>
<tr>
<th>Virtual Memory Reference</th>
<th>TLB</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 1, 2, 3, 4, 5, 6, 7</td>
<td>6, 7</td>
<td>4, 5, 6, 7</td>
</tr>
<tr>
<td>FFFFFFFF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0, 1, 2, 3, 0, 1, 2, 3</td>
<td>2, 3</td>
<td>0, 1, 2, 3</td>
</tr>
<tr>
<td>FFFFFMMM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0, 1, 2, 3, 4, 0, 1, 2</td>
<td>1, 2</td>
<td>4, 0, 1, 2</td>
</tr>
<tr>
<td>FFFFFF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3, 7, 3, 7, 1, 3, 1, 7</td>
<td>1, 7</td>
<td>3, 1, 7</td>
</tr>
<tr>
<td>FFHHFMHM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

order doesn't matter.
6. Inverted Page Tables

Assume a system that uses an Inverted Page Table (IPT) for memory management. Remember, that ALL processes in the system will share the same page table in this case.

**Parameters:**
- Size of virtual address space = 32 KB
- Page size = 4 KB
- Size of physical memory = 64 KB

Given below (on the left) are the contents of the physical memory (starting from physical frame 0 down to the max size). The entry in the physical frame 0 (i.e., P3 (VPN:1)) means that this physical frame contains the virtual page of process P3 with VPN = 1.

Draw a diagram of the Inverted Page Table (IPT) and write the contents of the Page Table that reflects the state of the physical memory shown below. Label the fields of the IPT properly. It is enough to show only the essential fields in your IPT that are needed for this scheme to work.

### Physical Memory Contents

<table>
<thead>
<tr>
<th>VPN</th>
<th>Page Frame Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>P3 (VPN:1)</td>
</tr>
<tr>
<td>2</td>
<td>P1 (VPN:2)</td>
</tr>
<tr>
<td></td>
<td>FREE</td>
</tr>
<tr>
<td>0</td>
<td>P3 (VPN:0)</td>
</tr>
<tr>
<td>5</td>
<td>P1 (VPN:5)</td>
</tr>
<tr>
<td></td>
<td>FREE</td>
</tr>
<tr>
<td>2</td>
<td>P0 (VPN:2)</td>
</tr>
<tr>
<td>6</td>
<td>P2 (VPN:6)</td>
</tr>
<tr>
<td>7</td>
<td>P1 (VPN:3)</td>
</tr>
<tr>
<td></td>
<td>FREE</td>
</tr>
<tr>
<td>7</td>
<td>P3 (VPN:7)</td>
</tr>
<tr>
<td></td>
<td>FREE</td>
</tr>
<tr>
<td>4</td>
<td>P1 (VPN:4)</td>
</tr>
<tr>
<td></td>
<td>FREE</td>
</tr>
<tr>
<td></td>
<td>FREE</td>
</tr>
<tr>
<td>1</td>
<td>P0 (VPN:1)</td>
</tr>
</tbody>
</table>

### Inverted Page Table

<table>
<thead>
<tr>
<th>VPN</th>
<th>PID</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
7. Condition Variables

Assume the following implementation for the famous **producer/consumer** problem. You may assume that the code compiles and executes successfully.

```c
void put(int value) {
    buffer[fillptr] = value;
    fillptr = (fillptr + 1) % max;
    count++;
}

void get() {
    int tmp = buffer[useptr];
    useptr = (useptr + 1) % max;
    count--;
    return tmp;
}

void *producer(void *arg) {
    int i;
    for (i = 0; i < loops; i++) {
        P_mutex_lock(&mutex);   // p1
        if (count == max)       // p2
            P_cond_wait(&empty,&mutex); // p3
        put(i);                // p4
        P_cond_signal(&fill);   // p5
        P_mutex_unlock(&mutex);  // p6
    }
}

void *consumer(void *arg) {
    int i;
    for (i = 0; i < loops; i++) {
        P_mutex_lock(&mutex);   // c1
        if (count == 0)         // c2
            P_cond_wait(&fill,&mutex); // c3
        int tmp = get();        // c4
        P_cond_signal(&empty);  // c5
        P_mutex_unlock(&mutex);  // c6
        printf("\n", tmp);
    }
}
```

Assume further that the only way a thread stops running is when it explicitly blocks in either a condition variable or lock (in other words, no untimely interrupts switch from one thread to the other). Also assume there are NO SPURIOUS WAKEUPS from wait().

a. In the following, show which lines of code (from p1 - p6 and c1 - c6) run given a particular scenario. Scenario 0 is completed for you as an example.

**Scenario 0:** 1 producer (P), 1 consumer (C), max = 1. Producer P runs first. Stop when consumer C has consumed one entry.

P: p1, p2, p4, p5, p6, p1, p2, p3
C: c1, c2, c4

**Scenario 1:** 1 producer (P), 1 consumer (C), max = 1. Consumer C runs first. Stop when consumer C has consumed one entry.

P: c1, c2, c3, c4
C: c1, c2, c3

**Scenario 2:** 1 producer (P), 2 consumers (Ca, Cb), max = 1. Consumer Ca runs first, then P, then Cb. Stop when each consumer has consumed one entry.

P: c1, c2, c3, c4
Ca: c1, c2, c3
Cb: c1, c2, c3

b. Are there any bugs in this implementation? If so, how do you fix them?
8. Advanced Locks!

Consider the following implementation for a lock in Solaris using Queues, Test-And-Set, Yield, and Wakeup.

```c
typedef struct __lock_t {
    int     flag;
    int     guard;
    queue_t *q;
} lock_t;

void lock_init(lock_t *lock) {
    lock->flag = lock->guard = 0;
    lock->q    = queue_init();
}

void lock(lock_t *lock) {
    while (xchg(&lock->guard, 1) == 1) // spin
        if (lock->flag == 0) { // \( x \)
            lock->flag = 1;
            lock->guard = 0;
        } else {
            queue_push(lock->q, gettid());
            setpark();
            lock->guard = 0;
            park();
        }
}

void unlock(lock_t *lock) {
    while (xchg(&lock->guard, 1) == 1) // spin
        if (queue_empty(lock->q))
            lock->flag = 0;
    else
        unpark(queue_pop(lock->q));
    lock->guard = 0;
}
```

The following are the definitions of the key routines:

- `park()`: Puts the calling thread to sleep.
- `unpark(threadID)`: Wake up the thread with the given threadID.
- `setpark()`: A thread indicates that it's about to park.
a. What is the **purpose** of the **guard lock**? What may happen if we don’t have the **guard lock**? **Explain** with a simple **example**.

Guard lock is used to protect the flag lock & the queue.

If we don’t have the guard lock, then 2 threads may enter the critical section(s) by acquiring the flag lock, e.g., \( l_1 \) is executed in \( t_1 \) & context switch to \( t_2 \).

\( t_2 \) enters CS.

\( t_1 \) enters CS.

\( t_2 \) is executed in \( t_2 \).

\( l_2 \) is executed in \( l_2 \).

\[ \text{RACE CONDITION} \]

b. Assume thread 1 is currently holding the **flag lock** and is inside the **critical section**. During this time, there are **9 more threads** that are currently waiting in the queue for the lock to be released. You may assume that there are no more threads waiting for this lock. You may also assume that all these threads will acquire the flag lock only once. Under this scenario, how many times will the flag lock be **released** by these 10 threads? **Explain** the reasoning behind your answer.

Only **once** by the last thread acquiring the lock.

Flag lock is **just transferred from one thread to the next**.

c. What will happen if **park()** is called **before releasing the guard lock**?

The thread(s) with the guard locks sleeps forever since no other thread can call **unlock** (and wake up \( t_1 \)).

**DEADLOCK**

d. This lock still **spins** while trying to acquire the **guard lock**. So, is this better in any way than simple spin locks with respect to **performance**? **Explain** your answer.

Yes, it is definitely better than simple spin locks because the critical section there is relatively too small (just a few lines of code in the lock( ) routine) when compared to user-defined critical sections in simple spin locks.
9. Threads vs Processes!

Assume that the code snippet below compiles successfully, all the APIs like `pthread_create()` do not fail, and the values in the `malloc`'ed memory are all initialized to 0.

```c
void worker(int *balance) {
    int *counter = malloc(sizeof(int));
    for (int i = 0; i < 1000000; i++) {
        (*balance)++;
        (*counter)++;
    }
    printf("balance : val %d, addr %p\n", *balance, balance);
    printf("counter : val %d, addr %p\n", *counter, counter);
}

int main() {
    int *balance;
    balance = malloc(sizeof(int));
    pthread_t t[2];
    for (int i = 0; i < 2; i++) // Creating new threads
        pthread_create(&t[i], NULL, worker, balance);
    for (int i = 0; i < 2; i++)
        pthread_join(t[i], NULL);
}
```

a. What are the values of the 2 variables (balance and counter) after the 2 threads (t1 and t2) finish execution? Value here means the contents printed using the following statements. If the value of a variable may be different in different runs of the program, you should write N/A.

```c
printf("%d\n", *balance); printf("%d\n", *counter);
```

<table>
<thead>
<tr>
<th>Value</th>
<th>t1</th>
<th>t2</th>
</tr>
</thead>
<tbody>
<tr>
<td>balance</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>counter</td>
<td>1M</td>
<td>1M</td>
</tr>
</tbody>
</table>

b. Consider the Virtual Addresses (VA) printed using the following statements in the 2 threads (t1 and t2). PA stands for Physical Address.

```c
printf("%p\n", balance); printf("%p\n", counter);
```

i. VA of balance in t1 == VA of balance in t2? (TRUE / FALSE)

ii. VA of counter in t1 == VA of counter in t2? (TRUE / FALSE)

iii. PA of balance in t1 == PA of balance in t2? (TRUE / FALSE)

iv. PA of counter in t1 == PA of counter in t2? (TRUE / FALSE)
void worker(int *balance) {
    int *counter = malloc(sizeof(int));
    for (int i = 0; i < 1000000; i++) {
        (*balance)++;
        (*counter)++;
    }
    printf("balance : val %d, addr %p\n", *balance, balance);
    printf("counter : val %d, addr %p\n", *counter, counter);
}

int main() {
    int *balance;
    balance = malloc(sizeof(int));
    for (int i = 0; i < 2; i++) { // Creating new processes
        if (fork() == 0) {
            worker(balance);
            exit(0);
        }
    }
    for (int i = 0; i < 2; i++)
        wait(NULL);
}

c. What are the values of the 2 variables (balance and counter) after the 2 processes (p1 and p2) created using fork(), finish execution? Value here means the contents printed using the following statements. If the value of a variable may be different in different runs of the program, you should write N/A.

    printf("%d\n", *balance);    printf("%d\n", *counter);

<table>
<thead>
<tr>
<th>Value</th>
<th>p1</th>
<th>p2</th>
</tr>
</thead>
<tbody>
<tr>
<td>balance</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>counter</td>
<td>m</td>
<td>m</td>
</tr>
</tbody>
</table>

    1.5 x 4

    d. Consider the Virtual Addresses (VA) printed using the following statements in the 2 processes (p1 and p2). PA stands for Physical Address.

    printf("%p\n", balance);    printf("%p\n", counter);

    i. VA of balance in p1 == VA of balance in p2? (TRUE / FALSE)
    ii. VA of counter in p1 == VA of counter in p2? (TRUE / FALSE)
    iii. PA of balance in p1 == PA of balance in p2? (TRUE / FALSE)
    iv. PA of counter in p1 == PA of counter in p2? (TRUE / FALSE)

    1 x 4
10. Multi-level Page Tables!

Assume a system with a 2-level page table.

Parameters:
- page size = 32 bytes
- virtual address space size = 32 KB
- physical memory size = 4 KB
- Size of one Page Directory Entry (PDE) = 1 byte
- Size of one Page Table Entry (PTE) = 1 byte
- Value of Page Directory Base Register (PDBR) = 30 (decimal) [This means the page directory is held in this page]

The format of the PDE and the PTE is simple. The high-order (left-most) bit is the VALID bit. If the bit is 1, the rest of the entry is the PFN. If the bit is 0, the page is not valid.

You are given two pieces of information to begin with. First, you are given the value of the page directory base register (PDBR), which tells you which page the page directory is located upon. Second, you are given a complete dump of each page of physical memory in the next 2 pages. A page dump looks like this:

```
page  0:  0d 0f 0e 12 1d 0c 10 03 08 14 03 ...
page  1:  0e 0d 1b 19 0a 0c 12 1b 06 0c 02 ...
page  2:  00 00 00 00 00 00 00 00 00 00 00 ...
```

which shows the 32 bytes found on pages 0, 1, 2, and so forth. The first byte (0th byte) on page 0 has the value 0x0d, the second is 0x0f, the third 0x0e, and so forth.

For each virtual address:
- write down the physical address it translates to AND the data value at this physical address, OR
- if it is a segmentation fault (an out-of-bounds address) write the reason for this segmentation fault (Invalid PDE OR Invalid PTE).

Write all answers in hexadecimal.

<table>
<thead>
<tr>
<th>Virtual Address</th>
<th>Physical Address OR Seg Fault</th>
<th>Data Value</th>
<th>Reason for Seg fault</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1ebe</td>
<td>Seg Fault 5</td>
<td></td>
<td>5 Invalid PTE</td>
</tr>
<tr>
<td>0x45b0</td>
<td>0x5FD 5 0x14 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x7bb9</td>
<td>Seg Fault 2</td>
<td></td>
<td>2 Invalid PDE</td>
</tr>
</tbody>
</table>