Boring Stuff

- Shell Lab due THIS Thursday, 28 March 2013
  - We will have more TAs at office hours this week to speed up the queue
- Malloc Lab comes out this Thursday
  - My favorite lab!
  - Design and implement a memory allocator
- Pressing concerns?
MENU FOR TODAY

- Teensy Bit of Shell Lab
- I/O (with Pictures!)
- Virtual Memory
- Address Translation
- Extra: C Primer
Rubber Duck Debugging

“To use this process, a programmer explains code to an inanimate object, such as a rubber duck, with the expectation that upon reaching a piece of incorrect code and trying to explain it, the programmer will notice the error.”
ABOUT SIGSUSPEND()

- For those of you who still need help with it...
  - This site is pretty good
    - “Figure 10.22. Protecting a critical region from a signal” is a really good example of how sigsuspend() works
I/O

- Four basic operations
  - open()
  - close()
  - read()
  - write()

- What's a file descriptor?
  - Returned by open()
  - Some positive value, or -1 to denote error
  - `int fd = open("/path/to/file", O_RDONLY);`
FILE DESCRIPTORS

- Every process starts with these 3 by default
  - 0 – STDIN
  - 1 – STDOUT
  - 2 – STDERR

- Every process gets its own **file descriptor table**
- Forked processes share open file tables
- All processes share v-node tables
  - Contains the stat structure with info about a file
Parent and Child After fork()

- Shamelessly stolen from lecture:

**Descriptor table**
[one table per process]

**Open file table**
[shared by all processes]

**v-node table**
[shared by all processes]

```
Parent

fd 0
fd 1
fd 2
fd 3
fd 4

File A (terminal)

File pos
refcnt=2
...

File B (disk)

File pos
refcnt=2
...

Child

fd 0
fd 1
fd 2
fd 3
fd 4

File access
File size
File type
...
```
**DUP2() SUPER RELEVANT EXAMPLE**

- Use `open()` to open a file to redirect `stdout`
  - `shelllab`: Done before `exec` in the child process

- Call `dup2(4,1)`
  - Copies `fd` entries
  - Cause `fd=1` to refer to disk file pointed at by `fd=4`

- Diagram:
  - Before `exec`: `stdin`, `stdout`, `stderr` mapped to `fd 0`, `fd 1`, `fd 2`
  - After `exec`: `stdin` mapped to `fd 0`, `stdout` mapped to `fd 1`, `stderr` mapped to `fd 2`
VM: Problems with Direct Mapping

- Questions to ponder:
  - How can we grow processes safely?
  - What to do about fragmentation?
  - How can we make large contiguous chunks fit easier?

Direct Mapping Fragmentation

- Process 1
- Process 2
- Process 3
- Process 4
- Process 5
- Process 6
HOW DO WE SOLVE THESE PROBLEMS?

- We are scientists (and engineers)...
  - Insert a level of indirection
VIRTUAL MEMORY

- ..Is the Best Thing Ever™
  - Demand paging
  - Memory Management
  - Protection

- Allows the illusion of infinite memory
  - Kernel manages page faults

- Each process gets its own virtual address space
  - Mapping is the heart of virtual memory
VM OF A LINUX PROCESS

- **Process-specific data structs** (ptables, task and mm structs, kernel stack)
- **Physical memory**
- **Kernel code and data**
- **User stack**
- **Memory mapped region for shared libraries**
- **Runtime heap (malloc)**
- **Uninitialized data (.bss)**
- **Initialized data (.data)**
- **Program text (.text)**

**Different for each process**

**Identical for each process**

**Kernel virtual memory**

**Process virtual memory**
VM: ADDRESS TRANSLATIONS

Virtual address

Page table base register (PTBR)

Page table address for process

Valid bit = 0: page not in memory (page fault)

Physical address

Virtual page number (VPN)  Virtual page offset (VPO)

Physical page number (PPN)  Physical page offset (PPO)
OVERVIEW OF A HIT

CPU Chip

CPU

MMU

Cache/ Memory

Data

1 VA

2 PTEA

3 PTE

4 PA

5
TWO-LEVEL PAGE TABLE

32 bit addresses, 4KB pages, 4-byte PTEs
TRANSLATING W/ A K-LEVEL PAGE TABLE

VIRTUAL ADDRESS

PHYSICAL ADDRESS
But Memory accesses are slow

- At least 2 memory accesses
  - Fetch page-table entry (PTE) from memory
  - Then fetch data from memory
- In x86, 3 memory accesses
  - Page directory, page table, physical memory
- In x86_64, 4 level page-mapping system
- What should we do?
  - Please don’t say insert a level of “indirection”
TRANSLATION LOOKASIDE BUFFER (TLB)

- Super fast hardware cache of PTEs
- Idea: Locality exists between memory accesses
  - Typically access nearby memory
  - Usually on the same page as current data
    - Arrays with loops
    - Program instructions
VM: TRANSLATIONS w/ TLB AND TABLES

Virtual address

Virtual page number (VPN)        Virtual page offset (VPO)

Physical address

Physical page number (PPN)        Physical page offset (PPO)

Translation Lookaside Buffer (TLB)

Page table base register (PTBR)

Page table address for process

TLB Hit: Fetch straight from TLB

TLB Miss: Do a page walk to fetch the entry

Valid     Physical page number (PPN)

m-1         p         p-1         0

n-1
Overview of a TLB Hit

1. CPU Chip
2. TLB
3. MMU
4. Cache/Memory
5. Data

**CPU Chip**

**CPU**

**MMU**

**Cache/Memory**

**TLB**

**PTE**

**VPN**

**VA**

**PA**

**Data**
Overview of a TLB Miss
TUTORIAL: VIRTUAL ADDRESS TRANSLATION

- **Addressing**
  - 32 bit virtual address
  - 32 bit physical address
  - Page size = 4 kb

- **Paging**
  - 10 bit page directory index
  - 10 bit page table index
  - 12 bit offset

- **TLB**
  - Direct Mapped
  - 4 entries
TUTORIAL: ADDRESS TRANSLATION HIT

Always access TLB first

<table>
<thead>
<tr>
<th>Set</th>
<th>Tag</th>
<th>PPN</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3A7AE</td>
<td>5F7F7</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Tutorial: Address Translation Hit**

VPO and PPO are always the same!
**Tutorial: Address Translation Miss**

1. **TLBT**
2. **TLBI**
3. **VPO**

<table>
<thead>
<tr>
<th>Set</th>
<th>Tag</th>
<th>PPN</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3B8AC</td>
<td>DEAD</td>
<td>0</td>
</tr>
</tbody>
</table>

- **TLB Miss! Do page walk**
**Tutorial: Address Translation Miss**

<table>
<thead>
<tr>
<th>Page Directory Index</th>
<th>Page Table Address</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x3B8</td>
<td>0xFAFF8034</td>
<td>1</td>
</tr>
<tr>
<td>0x3B9</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>...</td>
<td>..</td>
<td>..</td>
</tr>
</tbody>
</table>
# Tutorial: Address Translation Miss

<table>
<thead>
<tr>
<th>PDI</th>
<th>PTA</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>0x3B8</td>
<td>0xFAFF8034</td>
<td>1</td>
</tr>
<tr>
<td>0x3B9</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PTI</th>
<th>PPN</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PTI</th>
<th>PPN</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PTI</th>
<th>PPN</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
</tr>
</tbody>
</table>

Diagram:
- 3B8: PDI
- 2B3: PTI
- BEE: VPO
- 0xFAFF8034
- 0xFAFF9034
TUTORIAL: ADDRESS TRANSLATION MISS

<table>
<thead>
<tr>
<th>Page Table Index</th>
<th>PPN</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2B2</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>0x2B3</td>
<td>0x2D00D</td>
<td>1</td>
</tr>
</tbody>
</table>

Page Table Index: 0x2B3

The PPN column shows the physical page number, and the Valid column indicates whether the page is valid (1) or not (0).
**Tutorial: Address Translation Miss**

- **PDI**: 3B8
- **PTI**: 2B3
- **VPO**: BEE

<table>
<thead>
<tr>
<th>PTI</th>
<th>PPN</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2B3</td>
<td>0x2D00D</td>
<td>1</td>
</tr>
</tbody>
</table>

- **PPN**: 2D00D
- **PPO**: BEE

**Physical Page Number**

**Physical Page Offset**
TRANSLATION MACRO EXERCISE

- 32 bit address: 10 bit VPN1, 10 bit VPN2, 12 bit VPO
- 4KB pages
- Define the following function like macros:
  - Page align
    #define PAGE_ALIGN(v_addr) _________________________________
  - Gets VPN1/VPN2 as unsigned int from virtual address
    #define VPN1(v_addr) _______________________________________
    #define VPN2(v_addr) _______________________________________
  - Gets VPO as unsigned int from virtual address
    #define VPO(v_addr) ________________________________________
  - Calculates the address of the page directory index
    #define PDEA(pd_addr, v_addr) ________________________________
  - Calculate address of page table entry
    #define PTEA(pd_addr, v_addr)_______________________________
  - Calculate physical address
    #define PA(pd_addr, v_addr) ________________________________
TRANSLATION MACRO SOLUTION

- 32 bit address: 10 bit VPN1, 10 bit VPN2, 12 bit VPO
- 4KB pages
- Define the following function like macros:
  - Page align
    ```c
    #define PAGE_ALIGN(v_addr) ((unsigned int) v_addr & ~0xfff)
    ```
  - Gets VPN1/VPN2 as unsigned int from virtual address
    ```c
    #define VPN1(v_addr) ((unsigned int) (((v_addr)>>22)&0x3ff))
    #define VPN2(v_addr) ((unsigned int) (((v_addr)>>12)&0x3ff))
    ```
  - Gets VPO as unsigned int from virtual address
    ```c
    #define VPO(v_addr) ((unsigned int) ((v_addr)&0xffff))
    ```
  - Calculates the address of the page directory index
    ```c
    #define PDEA(pd_addr, v_addr) (((void **)pd_addr)+VPN1(v_addr))
    ```
  - Calculate address of page table entry
    ```c
    #define PTEA(pd_addr, v_addr)
    (((void **)PAGE_ALIGN(*PDEA(pd_addr,v_addr)))+VPN2(v_addr))
    ```
  - Calculate physical address
    ```c
    #define PA(pd_addr, v_addr)
    (((PAGE_ALIGN(*PTEA(pd_addr,v_addr)))) | VPO(v_addr))
    ```
EXTRA STUFF

- For next week, or for your enjoyment
All the C!

- “Saving you from malloc misery...”
- Basics
- Useful C Stuff
- Debugging

C and Pointer Basics

- Statically allocated arrays:
  - `int prices[100];`
  - Getting rid of magic numbers:
    - `int prices[NUMITEMS];`

- Dynamically allocated arrays:
  - `int *prices2 = (int *) malloc(sizeof(int) * var);`

- Which is valid:
  - `prices2 = prices;`
  - `prices = prices2;`

- The & operator:
  - `&prices[1] is the same as prices+1`

- Function Pointer:
  - `int (*fun)();`
  - Pointer to function returning int
Peeling the Onion (K&R p. 101)

- char **argv
  - argv: pointer to a pointer to a char
- int (*daytab)[13]
  - daytab: pointer to array[13] of int
- int *daytab[13]
  - daytab: array[13] of pointer to int
- char (*(*x()));()
  - x: function returning pointer to array[] of pointer to function returning char
- char (*(*x[3])());[5]

Takeaway
- There is an algorithm to decode this (see K&R p. 101)
- Always use parenthesis!!
- Typedef
WHY TYPEDEFS?

- For convenience and readable code

  **Example:**
  ```c
  typedef struct {
    int x;
    int y;
  } point;
  
  Function Pointer example:
  ```
  ```c
  typedef int (*pt2Func)(int, int);
  
  pt2Func is a pointer to a function that takes 2 int arguments and returns an int
  ```
MACROS ARE COOL

- C Preprocessor looks at macros in the preprocessing step of compilation
- Use `#define` to avoid magic numbers:
  - `#define TRIALS 100`
- Function like macros – short and heavily used code snippets
  - `#define GET_BYTE_ONE(x) ((x) & 0xff)`
  - `#define GET_BYTE_TWO(x) ((x) >> 8) & 0xff`
- Also look at inline functions (example prototype):
  - `inline int fun(int a, int b)`
  - Requests compiler to insert assembly of `max` wherever a call to `max` is made
- Both useful for malloc lab
DEBUGGING – FAVORITE METHODS

- Using the DEBUG flag:
  - #define DEBUG
    
    . . .
    #ifdef DEBUG
    . . . // debugging print statements, etc.
    #endif

- Compiling (if you want to debug):
  - gcc -DDEBUG foo.c -o foo

- Using assert
  - assert(posvar > 0);
  - man 3 assert

- Compiling (if you want to turn off asserts):
  - gcc -DNDEBUG foo.c -o foo
**Little Things**

- **Usage messages**
  - Putting this in is a good habit – allows you to add features while keeping the user up to date
  - `man -h`

- **fopen/fclose**
  - Always error check!

- **malloc()**
  - Error check
  - Free everything you allocate

- **Global variables**
  - Namespace pollution
  - If you must, make them private:
    - `static int foo;`
QUESTIONS AND REFERENCES SLIDE

- Rubber Duck 1
- Rubber Duck Debugging on Wiki
- Good sgsuspend() reference
- Indirection on Wiki
- Pictures stolen from lecture slides
- Stole from 15-410 Virtual Memory Slides
  - Lectures reside here
  - BTW, Prof. Eckhardt is super cool