15-213
“The course that gives CMU its Zip!”

Virtual Memory
Oct. 21, 2003

Topics
- Motivations for VM
- Address translation
- Accelerating translation with TLBs

Classic Motivations for Virtual Memory

Use Physical DRAM as a Cache for the Disk
- Address space of a process can exceed physical memory size
- Sum of address spaces of multiple processes can exceed physical memory

Simplify Memory Management
- Multiple processes resident in main memory.
  - Each process has its own address space
  - Only “active” code and data is actually in memory
  - Allocate more memory to process as needed.

Provide Protection
- One process can’t interfere with another.
  - Because they operate in different address spaces.
  - User process cannot access privileged information
  - Different sections of address spaces have different permissions.

Modern Motivations for VM

- Memory sharing and control
  - Copy on write: share physical memory among multiple processes until a process tries to write to it. At that point make a copy. For example, this eliminates the need for vfork()
  - Shared libraries
  - Protection (debugging) via Segment-Drivers (Solaris)
- Sparse address space support (64bit systems)
- Memory as a fast communication device
  - Part of memory is shared by multiple processes
- Multiprocessing (beyond the scope of 15-213)

Why does VM Work?

It is not used!
Motivation #1: DRAM a “Cache” for Disk

Full address space is quite large:
- 32-bit addresses: ~4,000,000,000 (4 billion) bytes
- 64-bit addresses: ~16,000,000,000,000,000,000 (16 quintillion) bytes

Disk storage is ~500X cheaper than DRAM storage
- 80 GB of DRAM: ~ $25,000
- 80 GB of disk: ~ $50

To access large amounts of data in a cost-effective manner, the bulk of the data must be stored on disk

Levels in Memory Hierarchy

<table>
<thead>
<tr>
<th>Register</th>
<th>Cache</th>
<th>Memory</th>
<th>Disk Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size:</td>
<td>32 B</td>
<td>32 KB-4MB</td>
<td>1024 MB</td>
</tr>
<tr>
<td>Latency:</td>
<td>~1 ns</td>
<td>~2 ns</td>
<td>&gt; 50 ns</td>
</tr>
<tr>
<td>$/Mbyte:</td>
<td>$125/MB</td>
<td>$0.20/MB</td>
<td>$0.001/MB</td>
</tr>
<tr>
<td>Line size:</td>
<td>8(16) B</td>
<td>32(64) B</td>
<td>4(84+) KB</td>
</tr>
</tbody>
</table>

Impact of Properties on Design

If DRAM was to be organized similar to an SRAM cache, how would we set the following design parameters?

- Line size?
  Large, since disk better at transferring large blocks
- Associativity?
  High, to minimize miss rate
- Write through or write back?
  Write back, since can’t afford to perform small writes to disk

What would the impact of these choices be on:

- Miss rate
  Extremely low. << 1%
- Hit time
  Must match cache/DRAM performance
- Miss latency
  Very high. ~2ms
- Tag storage overhead
  Low, relative to block size

DRAM vs. SRAM as a “Cache”

DRAM vs. disk is more extreme than SRAM vs. DRAM

- Access latencies:
  - DRAM ~10X slower than SRAM
  - Disk ~160,000X slower than DRAM
- Importance of exploiting spatial locality:
  - First byte is ~160,000X slower than successive bytes on disk
  v.s. ~4X improvement for page-mode vs. regular accesses to DRAM
- Bottom line:
  - Design decisions made for DRAM caches driven by enormous cost of misses
Locating an Object in a “Cache”

**SRAM Cache**
- Tag stored with cache line
- Maps from cache block to memory blocks
  - From cached to uncached form
  - Save a few bits by only storing tag
- No tag for block not in cache
- Hardware retrieves information
  - Can quickly match against multiple tags

---

**Locating an Object in “Cache” (cont.)**

**DRAM Cache**
- Each allocated page of virtual memory has entry in page table
- Mapping from virtual pages to physical pages
  - From uncached form to cached form
  - Page table entry even if page not in memory
  - Specifies disk address
  - Only way to indicate where to find page
- OS retrieves information

---

A System with Physical Memory Only

**Examples:**
- Most Cray machines, early PCs, nearly all embedded systems, etc.
- Addresses generated by the CPU correspond directly to bytes in physical memory

---

A System with Virtual Memory

**Examples:**
- Workstations, servers, modern PCs, etc.
- Address Translation: Hardware converts virtual addresses to physical addresses via OS-managed lookup table (page table)
Page 4
**Contrast: Macintosh Memory Model**

MAC OS 1–9
- Does not use traditional virtual memory
  - P1 Pointer Table
  - Shared Address Space

Process P1

“Handles” Process P2

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>D</td>
</tr>
<tr>
<td>E</td>
<td></td>
</tr>
</tbody>
</table>

All program objects accessed through “handles”
- Indirect reference through pointer table
- Objects stored in shared global address space

**Macintosh Memory Management**

Allocation / Deallocation
- Similar to free-list management of malloc/free

Compaction
- Can move any object and just update the (unique) pointer in pointer table

Process P1

“Handles” Process P2

<table>
<thead>
<tr>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td></td>
</tr>
</tbody>
</table>

**Mac vs. VM-Based Memory Mgmt**

Allocating, deallocating, and moving memory:
- can be accomplished by both techniques

Block sizes:
- Mac: variable-sized
  - may be very small or very large
- VM: fixed-size
  - size is equal to one page (4KB on x86 Linux systems)

Allocating contiguous chunks of memory:
- Mac: contiguous allocation is required
- VM: can map contiguous range of virtual addresses to disjoint ranges of physical addresses

Protection
- Mac: “wild write” by one process can corrupt another’s data

**MAC OS X**

“Modern” Operating System
- Virtual memory with protection
- Preemptive multitasking
  - Other versions of MAC OS require processes to voluntarily relinquish control

Based on MACH OS
- Developed at CMU in late 1980’s
Motivation #3: Protection
Page table entry contains access rights information:
- hardware enforces this protection (trap into OS if violation occurs)

<table>
<thead>
<tr>
<th>Process:</th>
<th>Read?</th>
<th>Write?</th>
<th>Physical Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>VP 0</td>
<td>Yes</td>
<td>No</td>
<td>PP 9</td>
</tr>
<tr>
<td>VP 1</td>
<td>Yes</td>
<td>Yes</td>
<td>PP 4</td>
</tr>
<tr>
<td>VP 2</td>
<td>No</td>
<td>No</td>
<td>XXXXXXXX</td>
</tr>
</tbody>
</table>

VM Address Translation

Virtual Address Space
- \( V = \{ 0, 1, ..., N-1 \} \)

Physical Address Space
- \( P = \{ 0, 1, ..., M-1 \} \)
- \( M < N \) (usually, but >4 Gbyte on an IA32 possible)

Address Translation
- MAP: \( V \rightarrow P \cup \emptyset \)
- For virtual address \( a \):
  - MAP(a) = \( a' \) if data at virtual address \( a \) at physical address \( a' \) in \( P \)
  - MAP(a) = \( \emptyset \) if data at virtual address \( a \) not in physical memory
  - Either invalid or stored on disk

VM Address Translation: Hit

VM Address Translation: Miss
VM Address Translation

Parameters
- \( P = 2^r \) = page size (bytes).
- \( N = 2^s \) = Virtual address limit
- \( M = 2^u \) = Physical address limit

\[
\begin{array}{c|c|c|c}
\text{virtual page number} & \text{page offset} & \text{virtual address} \\
\hline
n-1 & p & 0 \\
\end{array}
\]

Address Translation:
- If valid, then page in memory
- If invalid, then page not in memory

Page offset bits don't change as a result of translation.

Page Tables

Virtual Page Number

Memory resident page table (physical page or disk address)

Disk Storage (swap file or regular file system file)

Physical Memory

Address Translation via Page Table

Page Table Operation

Translation
- Separate set of page table(s) per process
- VPN forms index into page table (points to a page table entry)

Physical page number (PPN)

Valid access physical page number (PPN)

Virtual address

Physical address

Page table base register
Page Table Operation

Computing Physical Address
- Page Table Entry (PTE) provides information about page
- If (valid bit = 1) then the page is in memory.
- Use physical page number (PPN) to construct address
- If (valid bit = 0) then the page is on disk

Page fault

```
  physical address
  ┌───────────────────┐
  │ m-1 │ p-1 │ p │ 0 │
  │ PPN │ data index │ virtual address │ p-1 │ page offset │
  └───────────────────┘
```

Valid access physical page number (PPN)
- If valid then page in memory
- Physical page number (PPN) + page offset

Checking Protection
- Access rights field indicate allowable access
  - e.g., read-only, read-write, execute-only
  - typically support multiple protection modes (e.g., kernel vs. user)
- Protection violation fault if user doesn’t have necessary permission

```
  physical address
  ┌───────────────────┐
  │ m-1 │ p-1 │ p │ 0 │
  │ PPN │ data index │ virtual address │ p-1 │ page offset │
  └───────────────────┘
```

Valid access physical page number (PPN)
- If valid then page not in memory
- Physical page number (PPN) + page offset

Integrating VM and Cache

Most Caches were “Physically Addressed”
- Accessed by physical addresses
- Allows multiple processes to have blocks in cache at same time
- Allows multiple processes to share pages
- Cache doesn’t need to be concerned with protection issues
- Access rights checked as part of address translation

Perform Address Translation Before Cache Lookup
- But this could involve a memory access itself (of the PTE)
- Of course, page table entries can also become cached

Speeding up Translation with a TLB

“Translation Lookaside Buffer” (TLB)
- Small hardware cache in MMU
- Maps virtual page numbers to physical page numbers
- Contains complete page table entries for small number of pages

```
  CPU
  ┌┐
  │Translation
  │data
  └┐
    Cache
    miss
    Main Memory

  CPU
  ┌┐
  │Translation
  │data
  └┐
    Cache
    miss
    Main Memory
```
Address Translation with a TLB

Simple Memory System Example

Addressing
- 14-bit virtual addresses
- 12-bit physical address
- Page size = 64 bytes

Simple Memory System Page Table
- Only show first 16 entries

Simple Memory System TLB
- 16 entries
- 4-way associative
Multi-Level Page Tables

Given:
- 4KB (2^12) page size
- 32-bit address space
- 4-byte PTE

Problem:
- Would need a 4 MB page table!
- 2^20/4 bytes

Common solution
- multi-level page tables
- e.g., 2-level table (P4)
  - Level 1 table: 1024 entries, each of which points to a Level 2 page table.
  - Level 2 table: 1024 entries, each of which points to a page

Main Themes

Programmer’s View
- Large “flat” address space
- Can allocate large blocks of contiguous addresses
- Processor “owns” machine
  - Has private address space
  - Unaffected by behavior of other processes

System View
- User virtual address space created by mapping to set of pages
  - Need not be contiguous
  - Allocated dynamically
  - Enforce protection during address translation
- OS manages many processes simultaneously
  - Continually switching among processes
  - Especially when one must wait for resource
    - E.g., disk I/O to handle page fault