1 Memory/Library Analogy
  1.1. Three Example Scenarios ........................................... 3
  1.2. Memory Technology .................................................... 7
  1.3. Cache Memories in Computer Architecture ......................... 11

2 Cache Concepts
  2.1. Single-Line Cache ..................................................... 14
  2.2. Multi-Line Cache ..................................................... 15
  2.3. Replacement Policies .................................................. 17
  2.4. Write Policies ....................................................... 19
  2.5. Categorizing Misses: The Three C’s ................................. 21

3 Memory Translation, Protection, and Virtualization ............... 24
  3.1. Memory Translation .................................................... 24
  3.2. Memory Protection .................................................... 32
  3.3. Memory Virtualization ................................................ 34

4 Analyzing Memory Performance ........................................ 37
  4.1. Estimating AMAL ..................................................... 38
1. Memory/Library Analogy

Our goal is to do some research on a new computer architecture, and so we wish to consult the literature to learn more about past computer systems. The library contains most of the literature we are interested in, although some of the literature is stored off-site in a large warehouse. There are too many distractions at the library, so we prefer to do our reading in our dorm room or office. Our dorm room or office has an empty bookshelf that can hold ten books or so, and our desk can hold a single book at a time.

1.1. Three Example Scenarios

- Use desk and library
- Use desk, book shelf, and library
- Use desk, book shelf, library, and warehouse
Books from library with no bookshelf “cache”

Some inherent “translation” since we need to use the online catalog to translate a book author and title into a physical location in the library (e.g., floor, row, shelf)

- Average latency to access a book: 40 minutes
- Average throughput including reading time: 1.2 books/hour
- Latency to access library limits our throughput
Books from library with bookshelf “cache”

- Average latency to access a book: <20 minutes
- Average throughput including reading time: \( \approx 2 \) books/hour
- Bookshelf acts as a small “cache” of the books in the library
  - **Cache Hit**: Book is on the bookshelf when we check, so there is no need to go to the library to get the book
  - **Cache Miss**: Book is not on the bookshelf when we check, so we need to go to the library to get the book
- Caches exploit structure in the access pattern to avoid the library access time which limits throughput
  - **Temporal Locality**: If we access a book once we are likely to access the same book again in the near future
  - **Spatial Locality**: If we access a book on a given topic we are likely to access other books on the same topic in the near future
Books from warehouse

- Keep very frequently used books on book shelf, but also keep books that have recently been checked out in the library before moving them back to long-term storage in the warehouse.
- We have created a “book storage hierarchy”

- **Book Shelf**: low latency, low capacity
- **Library**: high latency, high capacity
- **Warehouse**: very high latency, very high capacity
1.2. Memory Technology

Level-High Latch

Positive Edge-Triggered Register

CLK

D → Q

D → Q

CLK

D → Q

D → Q

CLK

D → Q

D → Q

CLK

D → Q

D → Q

CLK

D → Q

D → Q

CLK

D → Q

D → Q

CLK

D → Q

D → Q

CLK

D → Q

D → Q

CLK
Memory Arrays: Register Files

Memory Arrays: SRAM
Full-Word Write

Partial-Word Write

Combinational-Read

Synchronous-Read

No such thing as a “combinational write”!
1. Memory/Library Analogy

1.2. Memory Technology

**Memory Arrays: DRAM**

![Diagram of Memory Arrays: DRAM](image)

Adapted from [Foss, "Implementing Application-Specific Memory." ISSCC'96]
Flash and Disk

- Magnetic hard drives require rotating platters resulting in long random access times which have hardly improved over several decades.
- Solid-state drives using flash have $100 \times$ lower latencies but also lower density and higher cost.

Memory Technology Trade-Offs

- **Latches & Registers**
  - Low Capacity
  - Low Latency
  - High Bandwidth (more and wider ports)

- **Register Files**

- **SRAM**
  - High Capacity
  - High Latency
  - Low Bandwidth

- **DRAM**

- **Flash & Disk**
  - Low Capacity
  - Low Latency
  - Low Bandwidth
Latency numbers every programmer (architect) should know

<table>
<thead>
<tr>
<th>Operation</th>
<th>Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1 cache reference</td>
<td>1 ns</td>
</tr>
<tr>
<td>Branch mispredict</td>
<td>3 ns</td>
</tr>
<tr>
<td>L2 cache reference</td>
<td>4 ns</td>
</tr>
<tr>
<td>Mutex lock/unlock</td>
<td>17 ns</td>
</tr>
<tr>
<td>Main memory reference</td>
<td>100 ns</td>
</tr>
<tr>
<td>Send 2KB over commodity network</td>
<td>250 ns</td>
</tr>
<tr>
<td>Compress 1KB with zip</td>
<td>2 us</td>
</tr>
<tr>
<td>Read 1MB sequentially from main memory</td>
<td>9 us</td>
</tr>
<tr>
<td>SSD random read</td>
<td>16 us</td>
</tr>
<tr>
<td>Read 1MB sequentially from SSD</td>
<td>156 us</td>
</tr>
<tr>
<td>Round trip in datacenter</td>
<td>500 us</td>
</tr>
<tr>
<td>Read 1MB sequentially from disk</td>
<td>2 ms</td>
</tr>
<tr>
<td>Disk random read</td>
<td>4 ms</td>
</tr>
<tr>
<td>Packet roundtrip from CA to Netherlands</td>
<td>150 ms</td>
</tr>
</tbody>
</table>

http://www.eecs.berkeley.edu/~rcs/research/interactive_latency.html
1.3. Cache Memories in Computer Architecture

![Diagram of Memory/Library Analogy]

- **Desk**: Processor
- **Book Shelf**: Cache
- **Library**: Main Memory
- **Warehouse**: Disk/Flash

**Cache Accesses**: (10 or fewer cycles)

**Main Memory Access**: (100s of cycles)

**Disk Access**: (100,000s of cycles)

**Need Addr 0x100**
- Cache Req
- Cache Miss
- Refill Req
- Access Main Memory

**Need Addr 0x100**
- Cache Resp
- Cache Hit
- Refill Resp

**Need Addr 0x200**
- Cache Req
- Cache Miss
- Eviction Req
- Refill Req
- Access Main Memory

**Need Addr 0xF00**
- Cache Req
- Cache Miss
- Page Fault (SW Involved)
- Disk Req
- Access Disk

**Refill Req**
- Cache Resp
- Refill Resp
Cache memories exploit temporal and spatial locality
Understanding locality for assembly programs

Examine each of the following assembly programs and rank each program based on the level of temporal and spatial locality in both the instruction and data address stream on a scale from 0 to 5 with 0 being no locality and 5 being very significant locality.

<table>
<thead>
<tr>
<th></th>
<th>Inst Temp</th>
<th>Inst Spat</th>
<th>Data Temp</th>
<th>Data Spat</th>
</tr>
</thead>
<tbody>
<tr>
<td>loop:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lw x1, 0(x2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lw x3, 0(x4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>add x5, x1, x3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sw x5, 0(x6)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addi x2, x2, 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addi x4, x4, 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addi x6, x6, 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addi x7, x7, -1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bne x7, x0, loop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>loop:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lw x1, 0(x2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lw x3, 0(x1) # random ptrs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lw x4, 0(x3) # random ptrs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addi x4, x4, 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addi x2, x2, 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addi x7, x7, -1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bne x7, x0, loop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>loop:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lw x1, 0(x2) # many diff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>jalr x1 # func ptrs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addi x2, x2, 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>addi x7, x7, -1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bne x7, x0, loop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Cache Concepts

- Single-line cache
- Multi-line cache
- Replacement policies
- Write Policies
- Categorizing Misses

2.1. Single-Line Cache

Consider only 4B word accesses and only the read path for three single-line cache designs:
What about writes?

- Spatial Locality: Refill entire cache line at once
- Temporal Locality: Reuse word multiple times

## 2.2. Multi-Line Cache

Consider a four-line direct-mapped cache with 4B cache lines
### Example execution worksheet and table for direct-mapped cache

<table>
<thead>
<tr>
<th>Dynamic Transaction Stream</th>
<th>0x000</th>
<th>0x004</th>
<th>0x008</th>
<th>0x00c</th>
<th>0x010</th>
</tr>
</thead>
<tbody>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x004</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x004</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>V</th>
<th>Tag</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set 3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>rd 0x000</td>
</tr>
<tr>
<td>rd 0x004</td>
</tr>
<tr>
<td>rd 0x010</td>
</tr>
<tr>
<td>rd 0x000</td>
</tr>
<tr>
<td>rd 0x004</td>
</tr>
<tr>
<td>rd 0x020</td>
</tr>
</tbody>
</table>
Increasing cache associativity

Four-line direct-mapped cache with 4B cache lines

Four-line two-way set-associative cache with 4B cache lines

Four-line fully-associative cache with 4B cache lines
Combining associativity with longer cache lines

- Spatial Locality: Refill entire cache line + simple indexing to find set
- Temporal Locality: Reuse word multiple times + replacement policy

2.3. Replacement Policies

- No choice in a direct-mapped cache
- Random
  - Good average case performance, but difficult to implement
- Least Recently Used (LRU)
  - Replace cache line which has not been accessed recently
  - LRU cache state must be updated on every access which is expensive
  - True implementation only feasible for small sets
  - Two-way cache can use a single “last used bit”
  - Pseudo-LRU uses binary tree to approximate LRU for higher associativity
- First-In First-Out (FIFO, Round Robin)
  - Simpler implementation, but does not exploit temporal locality
  - Potentially useful in large fully associative caches
Example execution worksheet and table for 2-way set associative cache

<table>
<thead>
<tr>
<th>Dynamic Transaction Stream</th>
<th>Way 0</th>
<th>Way 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set 0</td>
<td>V</td>
<td>Tag</td>
</tr>
<tr>
<td>Set 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x004</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x010</td>
<td>0x000</td>
<td>13</td>
</tr>
<tr>
<td>rd 0x000</td>
<td>0x004</td>
<td>14</td>
</tr>
<tr>
<td>rd 0x004</td>
<td>0x008</td>
<td>15</td>
</tr>
<tr>
<td>rd 0x00c</td>
<td>0x010</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Set 0</th>
<th>Set 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>idx</td>
</tr>
<tr>
<td>rd 0x000</td>
<td></td>
</tr>
<tr>
<td>rd 0x004</td>
<td></td>
</tr>
<tr>
<td>rd 0x010</td>
<td></td>
</tr>
<tr>
<td>rd 0x000</td>
<td></td>
</tr>
<tr>
<td>rd 0x004</td>
<td></td>
</tr>
<tr>
<td>rd 0x020</td>
<td></td>
</tr>
</tbody>
</table>

20
2.4. Write Policies

Write-Through with No Write Allocate

- On write miss, write memory but do not bring line into cache
- On write hit, write both cache and memory
- Requires more memory bandwidth, but simpler to implement

<table>
<thead>
<tr>
<th></th>
<th>tag</th>
<th>idx</th>
<th>h/m</th>
<th>Set</th>
<th>write</th>
<th>mem?</th>
</tr>
</thead>
<tbody>
<tr>
<td>rd 0x010</td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wr 0x010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wr 0x024</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x024</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assume 4-line direct-mapped cache with 4B cache lines
Write-Back with Write Allocate

- On write miss, bring cache line into cache then write
- On write hit, only write cache, do not write memory
- Only update memory when a dirty cache line is evicted
- More efficient, but more complicated to implement

<table>
<thead>
<tr>
<th>tag</th>
<th>idx</th>
<th>h/m</th>
<th>Set</th>
<th>write mem?</th>
</tr>
</thead>
<tbody>
<tr>
<td>rd</td>
<td>0x010</td>
<td></td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>wr</td>
<td>0x010</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wr</td>
<td>0x024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd</td>
<td>0x024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd</td>
<td>0x020</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assume 4-line direct-mapped cache with 4B cache lines
2.5. Categorizing Misses: The Three C’s

- **Compulsory**: first-reference to a block
- **Capacity**: cache is too small to hold all of the data
- **Conflict**: collisions in a specific set

Classifying misses in a cache with a target capacity and associativity as a sequence of three questions:

- **Q1**) Would this miss occur in a cache with infinite capacity? If the answer is yes, then this is a compulsory miss and we are done. If the answer is no, then consider question 2.

- **Q2**) Would this miss occur in a fully associative cache with the desired capacity? If the answer is yes, then this is a capacity miss and we are done. If the answer is no, then consider question 3.

- **Q3**) Would this miss occur in a cache with the desired capacity and associativity? If the answer is yes, then this is a conflict miss and we are done. If the answer is no, then this is not a miss – it is a hit!
Example 1 illustrating categorizing misses

Assume we have a direct-mapped cache with two 16B lines, each with four 4B words for a total cache capacity of 32B. We will need four-bits for the offset, one bit for the index, and the remaining bits for the tag.

<table>
<thead>
<tr>
<th>tag</th>
<th>idx</th>
<th>h/m</th>
<th>type</th>
<th>Set 0</th>
<th>Set 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q1. Would the cache miss occur in an infinite capacity cache? For the first two misses, the answer is yes so they are compulsory misses. For the last two misses, the answer is no, so consider question 2.

Q2. Would the cache miss occur in a fully associative cache with the target capacity (two 16B lines)? Re-run address stream on such a fully associative cache. For the last two misses, the answer is no, so consider question 3.

<table>
<thead>
<tr>
<th>tag</th>
<th>h/m</th>
<th>Way 0</th>
<th>Way 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x020</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x020</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Would the cache miss occur in a cache with the desired capacity and associativity? For the last two misses, the answer is yes, so these are conflict misses. There is enough capacity in the cache; the limited associativity is what is causing the misses.
Example 2 illustrating categorizing misses

Assume we have a direct-mapped cache with two 16B lines, each with four 4B words for a total cache capacity of 32B. We will need four-bits for the offset, one bit for the index, and the remaining bits for the tag.

<table>
<thead>
<tr>
<th>tag</th>
<th>idx</th>
<th>h/m</th>
<th>type</th>
<th>Set 0</th>
<th>Set 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x030</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q1. Would the cache miss occur in an infinite capacity cache? For the first three misses, the answer is yes so they are compulsory misses. For the last miss, the answer is no, so consider question 2.

Q2. Would the cache miss occur in a fully associative cache with the target capacity (two 16B lines)? Re-run address stream on such a fully associative cache. For the last miss, the answer is yes, so this is a capacity miss.

<table>
<thead>
<tr>
<th>tag</th>
<th>h/m</th>
<th>Way 0</th>
<th>Way 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x020</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x030</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rd 0x000</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Categorizing misses helps us understand how to reduce miss rate. Should we increase associativity? Should we use a larger cache?
3. Memory Translation, Protection, and Virtualization

Memory Management Unit (MMU)

- **Translation**: mapping of virtual addresses to physical addresses
- **Protection**: permission to access address in memory
- **Virtualization**: transparent extension of memory space using disk

Most modern systems provide support for all three functions with a single paged-based MMU

3.1. Memory Translation

Mapping of virtual addresses to physical addresses
Why memory translation?

- Enables using full virtual address space with less physical memory
- Enables multiple programs to execute concurrently
- Can facilitate memory protection and virtualization

Simple base-register translation
Memory fragmentation

As users come and go, the storage is “fragmented”. Therefore, at some stage programs have to be moved around to compact the storage.
3. Memory Translation, Protection, and Virtualization

3.1. Memory Translation

Linear-page table translation

- Logical address can be interpreted as a page number and offset
- Page table contains the physical address of the base of each page
- Page tables make it possible to store the pages of a program non-contiguously
• Not all page table entries (PTEs) are valid

• Invalid PTE means the program has not allocated that page

• Each program has its own page table with entry for each logical page

• Where should page tables reside?
  – Space required by page table proportional to address space
  – Too large too keep in registers
  – Keep page tables in memory
  – Need one mem access for page bage address, and another for actual data
Size of linear page table?

- With 32-bit addresses, 4KB pages, and 4B PTEs
  - Potentially 4GB of physical memory needed per program
  - 4KB page means VPN is 20 bits and offset is 12 bits
  - $2^{20}$ PTEs, which means 4MB page table overhead per program

- With 64-bit addresses, 1MB pages, and 8B PTEs
  - 1MB pages means VPN is 44 bits and offset is 20 bits
  - $2^{44}$ PTEs, which means 140TB page table overhead per program

- How can this possible ever work? Exploit program structure, i.e., sparsity in logical address usage

Two-level table translation
• Again, we store page tables in physical memory
• Space requirements are now much more modest
• Now need three memory accesses to retrieve one piece of data
Translation lookaside buffers

- Address translation is very expensive
- Every reference requires multiple memory accesses
- Solution: Cache translations in a translation lookaside buffer
  - TLB Hit: Single-cycle translation
  - TLB Miss: Page table walk to refill TLB

- Typically 32-128 entries, usually fully associative
  - Each entry maps large number of consecutive addresses so most spatial locality within page as opposed to across pages -> More likely that two entries conflict
  - Sometimes larger TLBs (256-512 entries) are 4-8 way set-associative
  - Larger systems sometimes have multi-level (L1 and L2) TLBs

- Random or FIFO replacement policy

- Usually no program identifier in the TLB
  - Flush TLB on program context switch

- TLB Reach: Size of largest virtual address space that can be simultaneously mapped by TLB
  - Example: 64 TLB entries, 4KB pages, one page pery entry
  - TLB Reach: 64 entries * 4 KB = 256 KB (if contiguous)
• Handling a TLB miss in software (MIPS, Alpha)
  – TLB miss causes an exception and the operating system walks the page tables and reloads TLB. A privileged “untranslated” addressing mode used for walk

• Handling a TLB miss in hardware (SPARCv8, x86, PowerPC)
  – The memory management unit (MMU) walks the page tables and reloads the TLB, any additional complexities encountered during walk causes MMU to give up and signal an exception

3.2. Memory Protection

Base-and-bound protection

Base and bounds registers are visible/accessible only when processor is running in the supervisor mode
Separate areas for program and data

![Diagram showing memory protection](image)

Page-based protection

- We can store protection information in the page-tables to enable page-level protection
- Protection information prevents two programs from being able to read or write each other’s physical memory space
3.3. Memory Virtualization

- More than just translation and protection
- Use disk to extend apparent size of memory
- Treat DRAM as cache of disk contents
- Only need to hold active working set of processes in DRAM, rest of memory image can be swapped to disk
- Inactive processes can be completely swapped to disk (except usually the root of the page table)
- Hides machine configuration from software
- Implemented with combination of hardware/software

**Page Fault Handler**

- When the referenced page is not in DRAM:
  - The missing page is located (or created)
  - It is brought in from disk, and page table is updated
    *Another job may be run on the CPU while the first job waits for the requested page to be read from disk*
  - If no free pages are left, a page is swapped out
    *Pseudo-LRU replacement policy*
- Since it takes a long time to transfer a page (msecs), page faults are handled completely in software by the OS
  - Untranslated addressing mode is essential to allow kernel to access page tables
Caching vs. Demand Paging

Caching
- cache entry
- cache block (~32 bytes)
- cache miss rate (1% to 20%)
- cache hit (~1 cycle)
- cache miss (~100 cycles)
- a miss is handled in hardware

Demand paging
- page frame
- page (~4K bytes)
- page miss rate (<0.001%)
- page hit (~100 cycles)
- page miss (~5M cycles)
- a miss is handled mostly in software

Hierarchical Page Table with VM

Virtual Address

31 22 21 12 11 0
p1 p2 offset

10-bit 10-bit
L1 index L2 index

Root of the Current Page Table

(Processor Register)

Level 1 Page Table

Level 2 Page Tables

Data Pages

If on page table walk, reach page that is in secondary memory then must handle a page fault to bring page into primary memory.
Address Translation: putting it all together

Virtual Address

Restart instruction

TLB Lookup

Page Table Walk

Protection Check

Page Fault
(OS loads page)

Update TLB

Protection Fault

Physical Address (to cache)

SEGFAULT

Hardware

Hardware or software

Software

The page is

∉ Memory

∈ memory

denied

permitted
4. Analyzing Memory Performance

\[
\text{Time} \quad \frac{\text{Mem Access Sequence}}{\text{Mem Accesses Sequence}} = \frac{\text{Mem Accesses Sequence}}{\text{Mem Accesses}} \times \frac{\text{Avg Cycles Mem Access}}{\text{Time Cycle}}
\]

\[
\frac{\text{Avg Cycles Mem Access}}{\text{Hit}} = \frac{\text{Avg Cycles Hit}}{\text{Num Misses Num Accesses}} \times \frac{\text{Avg Extra Cycles Miss}}{\text{Avg Extra Cycles}}
\]

- Mem access / sequence depends on program and translation
- Time / cycle depends on microarchitecture and implementation
- Also called the average memory access latency (AMAL)
- Avg cycles / hit is called the hit latency
- Number of misses / number of accesses is called the miss rate
- Avg extra cycles / miss is called the miss penalty
- Avg cycles per hit depends on microarchitecture
- Miss rate depends on microarchitecture
- Miss penalty depends on microarchitecture, rest of memory system

<table>
<thead>
<tr>
<th>Microarchitecture</th>
<th>Hit Latency</th>
<th>Extra Accesses for Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSM Cache</td>
<td>&gt;1</td>
<td>1+</td>
</tr>
<tr>
<td>Pipelined Cache</td>
<td>≈1</td>
<td>1+</td>
</tr>
<tr>
<td>Pipelined Cache + TLB</td>
<td>≈1</td>
<td>≈0</td>
</tr>
</tbody>
</table>
4.1. Estimating AMAL

Consider the following sequence of memory accesses which might correspond to copying 4 B elements from a source array to a destination array. Each array contains 64 elements. Assume two-way set associative cache with 16 B cache lines, hit latency of 1 cycle and 10 cycle miss penalty. What is the AMAL in cycles?

\[
\begin{align*}
\text{rd} & \quad 0x1000 \\
\text{wr} & \quad 0x2000 \\
\text{rd} & \quad 0x1004 \\
\text{wr} & \quad 0x2004 \\
\text{rd} & \quad 0x1008 \\
\text{wr} & \quad 0x2008 \\
\ldots \\
\text{rd} & \quad 0x1040 \\
\text{wr} & \quad 0x2040
\end{align*}
\]

Consider the following sequence of memory accesses which might correspond to incrementing 4 B elements in an array. The array contains 64 elements. Assume two-way set associative cache with 16 B cache lines, hit latency of 1 cycle and 10 cycle miss penalty. What is the AMAL in cycles?

\[
\begin{align*}
\text{rd} & \quad 0x1000 \\
\text{wr} & \quad 0x1000 \\
\text{rd} & \quad 0x1004 \\
\text{wr} & \quad 0x1004 \\
\text{rd} & \quad 0x1008 \\
\text{wr} & \quad 0x1008 \\
\ldots \\
\text{rd} & \quad 0x1040 \\
\text{wr} & \quad 0x1040
\end{align*}
\]