Example Application: Coriolis Mass Flow Meter

CPU Module & Network Interface
Vibrating The Tube Permits Flow Measurement

- Used to precisely measure viscous fluids and slurries

[http://en.wikipedia.org/wiki/Mass_flow_meter]

Where Are We Now?

- REMINDER: Do Pre-Labs COMPLETELY ON YOUR OWN!
  - Do not work with your lab partner (or anyone else)
  - Do not talk about it with your lab partner until AFTER you BOTH hand in

- Where we’ve been:
  - Embedded hardware
  - Microcontroller Instruction Set – the basics

- Where we’re going today:
  - Microcontroller Instruction Set – advanced
  - Note: you saw assembly stuff in 18-240, so we’re covering it pretty quickly
  - If this stuff is confusing, go to office hours to get help

- Where we’re going next:
  - Engineering process & design
  - Embedded-specific C
  - Coding hacks & multiprecision math
  - ...
Preview

◆ Stack usage
  • Pushing & popping with stack
  • Subroutine linkage

◆ Other assembler operations
  • Position, memory, and other management
  • Labels
  • Macros

◆ More on timing
  • Cycle-accurate simulation

The Stack – Concept & Implementation

◆ Concept:

![Concept Diagram](image)

[Koopman]

◆ Implementation:
  • Uses a pointer to memory
  • The pointer moves up and down as top of stack, not the memory contents!
  • Points to top of stack

[Valvano]
Pushing To The Stack

- "PSH" instructions – pushes a register onto the stack
  - PSHA, PSHB, PSHD, PSHX, PSHY
  - PSHC – condition codes (will get to that in a moment)

Example:

LDAA #1
LDAB #2
PSHA
PSHB
LDAA #3
PSHA

At end, A=3, B=2
- PSH doesn’t change register values

(On 6812, SP always points to top-most element in use)

---

PSHA

Push A onto Stack

Operation:

(SP) = SP + 1
(A) = M_{SP}

Description:

Stacks the content of accumulator A. The stack pointer is decremented by one. The content of A is then stored at the address the SP points to.

Push instructions are commonly used to save the contents of one or more CPU registers at the start of a subroutine. Complementary pop instructions can be used to restore the saved CPU registers just before returning from the subroutine.

CCR Details:

<table>
<thead>
<tr>
<th>S</th>
<th>X</th>
<th>H</th>
<th>I</th>
<th>N</th>
<th>Z</th>
<th>V</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Form</th>
<th>Address Mode</th>
<th>Object Code</th>
<th>Access Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSHA</td>
<td>INH</td>
<td>36</td>
<td>Os</td>
</tr>
</tbody>
</table>

[Freescale]
Pulling ("Popping") From The Stack

- "PUL" instructions – pulls a register value from the stack
  - PULA, PULB, PULD, PULX, PULY
  - PULC – condition codes (will get to that in a moment)

Example:

PULA
PULB
PULB

At end, A=3, B=1

- PUL doesn’t erase memory values BUT unsafe to access them after PUL due to interrupts!!!

(On HC12, SP always points to top-most element in use)

---

PULC

Pull Condition Code Register from Stack

Operation:

\[(M_{SP}) = CCR\]
\[(SP) + \$0001 \Rightarrow SP\]

Description:

The condition code register is loaded from the address indicated by the stack pointer. The SP is then incremented by one.

Pull instructions are commonly used at the end of a subroutine to restore the contents of CPU registers that were pushed onto the stack before subroutine execution.

CCR Details:

<table>
<thead>
<tr>
<th>S</th>
<th>X</th>
<th>H</th>
<th>I</th>
<th>N</th>
<th>Z</th>
<th>V</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\Delta)</td>
<td>(\uparrow)</td>
<td>(\Delta)</td>
<td>(\Delta)</td>
<td>(\Delta)</td>
<td>(\Delta)</td>
<td>(\Delta)</td>
<td></td>
</tr>
</tbody>
</table>

Condition codes take on the value pulled from the stack, except that the X mask bit cannot change from 0 to 1. Software can leave the X bit set, leave it cleared, or change it from 1 to 0, but it can be set only by a reset or by recognition of an XIRQ interrupt.

<table>
<thead>
<tr>
<th>Source Form</th>
<th>Address Mode</th>
<th>Object Code</th>
<th>Access Detail HCS12</th>
<th>Access Detail M68HC12</th>
</tr>
</thead>
<tbody>
<tr>
<td>PULC</td>
<td>INH</td>
<td>38</td>
<td>uro</td>
<td>uro</td>
</tr>
</tbody>
</table>

[Valvano]
Stack Implementation

- Implementation of stack grows from top of memory down

$500 \ldots$ unused; start stack position …
$4FF$ “bottom” of stack (deepest byte)
$4FE \ldots$
$4B0$ “top” of stack if there are $50$ elements on it
$4AF$ … next unused element for stack …
… expansion space for stack
… expansion space for stack
… RAM data
$0000$ start of RAM

Hardware Support For Subroutines

- Allows use of a procedure (or method in Object Oriented terminology)

```
... 
  x = a + b;
  c = dosomething(x,a);
  y = c + d;
  ... 
  z = dosomething(w,k);
```

- What has to happen to make this work?
  - Prepare parameters for use
    - It isn’t always the same variables passed to the subroutine
  - Unconditional branch to subroutine
  - Execute subroutine
  - Prepare return value
    - The result doesn’t always go in the same output variable
  - Return to calling point to resume caller execution
    - How do we know where that is?
Subroutine Calls

◆ **Hardware support:** JSR, BSR
  
  - JSR – full, 16-bit address mode subroutine call
  - BSR – REL mode branch (8-bit PC-relative address), otherwise same as JSR
  - They pretty much do the same thing
    - BSR saves a byte of memory for instruction…
      … but still uses **2 bytes of stack space for return address**

◆ **JSR (and BSR) operations:**
  
  - PUSH current program counter onto stack  (2-byte value)
  - Put address of subroutine into the PC
  - Start executing code at new PC value (the subroutine)
  
  - This takes care of saving return address and the actual jump
  - But, doesn’t help with parameter values

---

**JSR**  
Jump to Subroutine

**Operation:**

(\(SP\) – 6002 \(\Rightarrow\) \(SP\))

\(RTN_8 : RTN_8 = M_{(SP)} : M_{(SP) + 1}\)

Subroutine Address \(\Rightarrow\) PC

**Description:**

Sets up conditions to return to normal program flow, then transfers control to a subroutine. Uses the address of the instruction following the JSR as a return address.

- Decrements the SP by two to allow the two bytes of the return address to be stacked.
- Stacks the return address. The SP points to the high order byte of the return address.
- Calculates an effective address according to the rules for extended, direct, or indexed addressing.
- Jumps to the location determined by the effective address.

Subroutines are normally terminated with an RTS instruction, which restores the return address from the stack.

**CCR Details:**

<table>
<thead>
<tr>
<th>S</th>
<th>X</th>
<th>H</th>
<th>I</th>
<th>N</th>
<th>Z</th>
<th>V</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Form</th>
<th>Address Mode</th>
<th>Object Code</th>
<th>Access Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>HC512</td>
</tr>
<tr>
<td>JSR spdr</td>
<td>DIR</td>
<td>17 dd</td>
<td>BEEE</td>
</tr>
<tr>
<td>JSR spdir</td>
<td>EXT</td>
<td>16 lb 11</td>
<td>EEEE</td>
</tr>
<tr>
<td>JSR spdr</td>
<td>IDX</td>
<td>15 ab</td>
<td>EEEE</td>
</tr>
<tr>
<td>JSR spdx</td>
<td>IDX1</td>
<td>15 ab rr</td>
<td>EEEE</td>
</tr>
<tr>
<td>JSR spdr</td>
<td>IDX2</td>
<td>15 ab 44 ff</td>
<td>EEEE</td>
</tr>
<tr>
<td>JSR [D,x]</td>
<td>[D,DX]</td>
<td>15 ab</td>
<td>EEEE</td>
</tr>
<tr>
<td>JSR [spdr,16,spdx]</td>
<td>[IDX2]</td>
<td>15 ab 44 ff</td>
<td>EEEE</td>
</tr>
</tbody>
</table>

[Freescale]
Subroutine Returns

- **Hardware support:** RTS
  - RTS – INH address mode  *(how do you know the return address?)*

- **RTS operations:**
  - POP top of stack and put it into PC
  - Start executing program at that new PC value (back to calling program)

  - This takes care of jumping back to calling program
  - But, doesn’t help with parameter values

---

RTS Operations:

- **Operation:**
  \[(M_{(SP)}; M_{(SP+1)}) = PC_H; PC_L; (SP) + \$0002 \Rightarrow SP\]

- **Description:**
  Restores context at the end of a subroutine. Loads the program counter with a 16-bit value pulled from the stack and increments the stack pointer by two. Program execution continues at the address restored from the stack.

- **CCR Details:**
  
<table>
<thead>
<tr>
<th>S</th>
<th>X</th>
<th>H</th>
<th>I</th>
<th>N</th>
<th>Z</th>
<th>V</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

- **Source Form** | **Address Mode** | **Object Code** | **Access Detail**
  | HCS12 | M68HC12 |
  | RTS | INH | \$00D | U0D | [Freescale]
How Do You Pass Parameters?

Multiple methods, all of which can be useful

◆ **Put values in particular registers**
  - Example: sqrt(D) \(\Rightarrow\) D  
    D register used as both input and output
  - Fast, but very limited by number of registers!
  - In the C language, it is very common to put the single return value in a register

◆ **Hard-code addresses into subroutine**
  - Easy to do
  - But, makes subroutine less flexible – need a different version for each data structure
  - Can make sense when you are just saving space by avoiding duplicated code

◆ **Pass parameters on stack**
  - Pass pointers to data structures
  - Pass values of variables
  - Flexible, usual method of passing parameters

◆ (Note: we’ll do stack frames and C variables in a later lecture …)

Example: Passing By Registers

```
LDAA #47
LDAB #63
BSR COMPUTE_AVERAGE
STAA Average_result
...

; note – the below code only works on unsigned numbers!
COMPUTE_AVERAGE:
  ABA ; sum to A, assume both are non-negative
  ; top bit of A contains carry-out of add
  LSRA ; divide by two for unsigned number sum
  RTS ; result is in register A
```
Passing Parameters To A Subroutine (simple version)

1. PUSH parameters onto stack
2. CALL subroutine
3. Subroutine reads parameters from stack and does computations
4. RTS
5. Calling program deletes parameters from stack
   • Why done here? (look at next slide to understand reason)

Example: Passing Via Stack (simple version)

; Assume SP value is $4FA at this point
LDAA #47
PSHA
LDAA #63
PSHA
JSR COMPUTE_AVERAGE
PULB ; discard second parameter (could also use INS, but that is 2 bytes)
PULB ; discard first parameter (could also use INS, but that is 2 bytes)
STAA Average_result
; SP is back to $4FA at this point
; only works on unsigned numbers!
COMPUTE_AVERAGE:
LDAA +2,SP ; second parameter
ADDA +3,SP ; first parameter
LSRA ; divide by two for non-negative
RTS ; result is in register A

<table>
<thead>
<tr>
<th>Address</th>
<th>Stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>$4FA</td>
<td>SP</td>
</tr>
<tr>
<td>$4F9</td>
<td>47</td>
</tr>
<tr>
<td>$4F8</td>
<td>63</td>
</tr>
<tr>
<td>$4F7</td>
<td>RetLo</td>
</tr>
<tr>
<td>$4F6</td>
<td>RetHi</td>
</tr>
<tr>
<td>$4F5</td>
<td>invalid</td>
</tr>
<tr>
<td>$4F4</td>
<td>invalid</td>
</tr>
</tbody>
</table>
Passing Parameters To A Subroutine (complete)

1. PUSH parameters onto stack
2. CALL subroutine
3. Save registers that are going to be modified by subroutine
   • Avoids unexpected corruption of registers used by the calling program
4. Subroutine reads parameters from stack and does computations
5. Subroutine writes results back to parameters on stack
6. Restore registers modified by subroutine
7. RTS
8. Calling program PULLs parameters from stack

Passing Via Stack Example (complete version)

; Assume SP value is $4FA at this point
LDAA #47
PSHA
LDAA #63
PSHA
PSHA ; dummy push to make room for result; could also use DES
JSR COMPUTE_AVERAGE
PULA; result stored in third parameter
STAA Average_result
PULB ; discard second parameter
PULB ; discard first parameter
; SP is back to $4FA at this point
; only works on non-negative numbers!

COMPUTE_AVERAGE:
PSHA ; make sure A isn’t trashed
LDAA +4,SP ; second parameter
ADDA +5,SP ; first parameter
LSRA ; divide by two for non-negative number sum
STAA +3,SP ; store result in third parameter position
PULA ; restore register A
RTS; result is on stack

<table>
<thead>
<tr>
<th>Address</th>
<th>Stack</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>$4FA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$4F9</td>
<td></td>
<td>47</td>
</tr>
<tr>
<td>$4F8</td>
<td></td>
<td>63</td>
</tr>
<tr>
<td>$4F7</td>
<td>Result</td>
<td></td>
</tr>
<tr>
<td>$4F6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$4F5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$4F4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$4F3</td>
<td></td>
<td>invalid</td>
</tr>
</tbody>
</table>
Rules For Safe Stack Use

◆ **PULL as many times as you PUSH**
  - Stack overflow will trash RAM
  - Stack underflow will give invalid PULL values
    - Very often it will also trash RAM
  - Mismatched number results in invalid subroutine return address

◆ **Don’t access stack memory after that value has been PULLed**
  - Interrupts can change the memory values at random times
    - We’ll talk about interrupts later in course
  - The program will still work *most* of the time – very nasty bug to track down

◆ **Beware of “stack smashing” attacks**
  - Frequent security vulnerability is someone intentionally over-running data structure to modify return address

---

```c
char *getProductName(void)
{
    char productName[128];
    char *cp = productName;

    readNameFromEEPROM(cp, 127);
    return cp;
}
```

We’re returning a pointer to an object on the stack. This is unsafe, yet may appear to work until an ISR runs on the same stack.
**Assembler Pseudo-Ops**

- **Not everything in a program is “executable code”**
  - By end of this lecture, you should know what everything below is doing…

  ```
  ROMStart EQU $C000  ; absolute address to place my code/constant data
  RAMStart EQU $0     ; absolute address to place my variable data
  RAMEnd EQU $03FF    ; absolute address of last usable RAM byte
  // variable/data section
  ORG RAMStart
  ; Insert here your data definition.
  Average_result DS.B 1
  // code section
  ORG ROMStart
  Entry:
  LDS #RAMEnd+1       ; initialize the stack pointer
  CLI                   ; enable interrupts
  LDAA #$47
  PSHA
  LDAA #$63
  PSHA
  JSR COMPUTE_AVERAGE
  ORG $FFFE
  DC.W Entry ; Reset Vector
  ```

---

**Labels**

- **Labels are a convenient way to refer to a particular address**
  - Can be used for program addresses as well as data addresses
  - You know it is a label because it starts in column 1 (“;” is optional)

- **Assume you are currently assembling to address $4712**
  - (how you do that comes in a moment)

**Mylabela:**

```
ABA       ; this is at address $4712
```

**Mylabelb:**

**Mylabelc**

```
PSHA      ; this is at address $4713
```

- The following all do EXACTLY the same thing:
  - JMP $4713
  - JMP Mylabelb
  - JMP Mylabelc
  - JMP Mylabela+1
- And it is valid to say: LDDA Mylabelb *(what does this do?)*
**ORG ; DS ; DC**

- **DS** – define storage space, but don’t initialize (RAM usually)
  - (“Define Space”)
    - `DS.B 1 ; allocate 1 byte of storage`
    - `DS.W 1 ; allocate one word (2 bytes)`
    - `DS.B 370 ; 370 more bytes`
    - `DS.W 100 ; 200 more bytes`

- **DC** – define storage space, and initialize with a value (ROM only)
  - (“Define Constant”)
    - `DC.B 13 ; one byte, with value $0D`
    - `DC.W 13 ; two bytes, with value $000D`
    - `DC.B 370 ; illegal – 8-bit value > 255`

- **ORG** – start laying down bytes at this address (ROM or RAM)
  - (“Origin”)
    - `ORG $3000`
      ; next instruction, DS, DC,... is at address $3000`

---

**EQU**

- **EQU** is “equate” – means give this label a certain value
  - This is a “compiler directive” – done at compile time, not at run time!
  - No bytes are deposited in memory!
  - Format: Label EQU Value

```
Foo  EQU  $C000
Bar  EQU  Foo
     LDAA  Foo  ; same as  LDAA  $C000
     LDAA  Bar  ; same as  LDAA  $C000
```
### Labels vs. ORG vs .EQU

<table>
<thead>
<tr>
<th></th>
<th>ORG</th>
<th>EQU</th>
<th>DS.W</th>
<th>DC.W</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foo</td>
<td>$5000</td>
<td>$C000</td>
<td>$17</td>
<td>$19</td>
</tr>
<tr>
<td>Baz</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Questions:
- What is the address of Baz?
- What address does the DS.W $53 start at? What value is stored there?
- What value is at address $D001 (high byte stored first)

- Note: don’t intermingle DS and DC in real programs – this is just an illustration
  - DS is for RAM; DC is for ROM/Flash memory in our hardware

### Does It Create Bytes?

- **These DO NOT create bytes of data in memory**
  - Label – creates a value for use by the assembler, no run-time effect
  - EQU – creates a value for use by the assembler, no run-time effect
    - (Really, it’s just a more general way to create a “label” value)
  - ORG – directs where the next byte goes
  - DS.B; DS.W – allocates storage space, but doesn’t put in any values

- **These DO create bytes of data in memory**
  - Instructions – these put opcode etc. for instructions in ROM
  - DC.B, DC.W – these store a “constant” value (pre-initialized variable, etc.) in ROM
Now Do We Know What All This Means?

ROMStart EQU $C000 ; absolute address to place my code/constant data
RAMStart EQU $0 ; absolute address to place my variable data
RAMEnd EQU $03FF ; absolute address of last usable RAM byte

; variable/data section

ORG RAMStart
; Insert here your data definition.
Average_result DS.B 1

; code section

ORG ROMStart

Entry:
LDS #RAMEnd+1 ; initialize the stack pointer
CLI ; enable interrupts

LDAA #$47
PSHA
LDAA #$63
PSHA
JSR COMPUTE_AVERAGE

ORG $FFFE
DC.W Entry ; Reset Vector

Other Info

◆ http://www.ece.utep.edu/courses/web3376/Directives.html
  • ("essential code warrior syntax" for assembly)

◆ Codewarrior documentation is available on the course web site
  • http://www.ece.cmu.edu/~ece348/reading/index.html
    • Assembler manual
    • C compiler manual
    • Build tools manual
    • Debugger manual
Some instructions have variable execution times – especially branches

Branch timing cases:
- Branch not taken
  - Just continues along as if it were a no-op
- Branch taken
  - Must refill instruction prefetch queue to get back to normal operation
  - (Remember, small microcontrollers don’t have cache memory, don’t speculate, etc.)
Lab Cycle-Accurate Simulator

- The IDE simulator provides several useful capabilities
  - Run code without a module
  - Easy single-step debugging
  - Count CPU cycles

- Generally a simulator is the only way to get exact CPU cycle counts
  - But only if the simulator is actually accurate (a problem on complex CPUs)
  - And only if the actual run-time environment matches the simulation
Simulator vs. Real Hardware vs. Hand Counting

- Motivation: need to know execution time for real time scheduling

- Hand counting
  - Doesn’t require fancy tools
  - Is tedious
  - Is OK for “best case” but often humanly impossible for worst case
    - in critical systems worst case is the important case!

- Simulator
  - If you have a simulator (luckily we do!) counting isn’t so bad
    - Single-step through program and subtract start count from end count
    - Can use “break points” (covered in debugging lecture)

- Real hardware
  - Can use hardware timers to assist (covered in counter/timer lecture)
  - Can use a stopwatch if timing is repeatable
  - Other approaches (covered in debugging lecture)
  - Issue: hard to get really precise and accurate times

NOP Timing Loops

What if your CPU doesn’t even have a timer?
What if you need just a few microseconds of delay?

- Sometimes (and frequently in old systems) => NOP Timing Loops

LDA A, #FF

Start_loop:
  NOP
  NOP
  NOP
  DBNE A, Start_loop  ; Cool loop instruction

- Number of NOP instructions and index values used to tune time
  - Very commonly used in 1980s era embedded systems
    - BUT – really a problem if you have cache memory, interrupts, etc. etc.
    - What happens if you start using a new chip that is faster/different timing?
  - We still use it in this class until you know more advanced techniques
    - BUT – dangerous to use in production systems unless you are really sure it is OK!
Advance Processors & Timing Prediction

✦ Fancy CPUs and systems have practically unpredictable timing
  • Speculative execution
  • Cache memory
  • Virtual memory
  • Variable timing on multiplication and division
  • DRAM refresh delays
  • System-level interrupts
  • Operating system latencies
  • …

✦ Timing analysis for complex systems is a tough problem
  • Something to NOT do – “run loop 1 million times and divide by 1 million”
  • Why?
**Intel 80386 Timing For Simple Loop**

- **Interrupt Service Routine** that puts bytes into a queue
  - “Memory sweeper” task running in foreground, including Virtual Memory

[Graph showing timing for different routines]

**Review**

- **Stack usage**
  - Pushing & popping with stack
  - Subroutine calls
  - Parameter passing to/from subroutines
  - SP-relative loads and stores

- **Other assembler operations**
  - Position, memory, and other management
  - Labels
  - Differences among label, EQU, DS, DC, ORG

- **More on timing**
  - Cycle-accurate simulation
  - Nop timing loop
# Lab Skills

- **Register-based subroutine interface**
  - Write a program that uses registers to pass values

- **Stack-based subroutine interface**
  - Write a program that uses the stack to pass values

- **Timing**
  - Hand compute timing
  - Simulation-based timing
  - Stop-watch based timing