ARM Cortex-A9: Initialization + Bootstrapping

Caio Pereira Oliveira (15100724)
Ricardo do Nascimento Boing (14200760)
Thomas Fernandes Feijoo (12200662)

Introdução

- Como ocorre o boot no ARM Cortex-A9?
- Como criar uma imagem bootavel para o QEMU?
- Como programar em C++ para o ARM Cortex-A9?

Requisitos

- Linux
- GCC ARM Cross-Compiler Toolchain
- QEMU - máquina realview-pbx-a9
- Build System - pacote build-essential

```
.section .vector_table
.global _reset
_reset:
b _start // 0x0 Reset
b .      // 0x4 Undefined Instruction
b .      // 0x8 Software Interrupt
b .      // 0xC Prefetch Abort
b .      // 0x10 Data Abort
b .      // 0x14 Reserved
b .      // 0x18 IRQ
b .      // 0x1C FIQ
```

startup.s

```
.section .entry
_start:
// init stack
ldr sp, =_stack_end
```

```
// clear bss
mov r0, #0
ldr r1, =_bss_start
ldr r2, =_bss_end

bss_loop:
cmp   r1, r2
strlt r0, [r1], #4
blt   bss_loop
```

```
// init static objects
ldr r0, =_init_array_start
ldr r1, =_init_array_end

globals_init_loop:
cmp   r0, r1
ldrlt r2, [r0], #4
blxlt r2
blt   globals_init_loop
```

startup.s

```
// jump to main
bl main
```

```
// destroy static objects in reverse order
ldr r0, =_fini_array_start
ldr r1, =_fini_array_end

globals_fini_loop:
cmp   r0, r1
ldrlt r2, [r0], #4
blxlt r2
blt   globals_fini_loop
```

startup.s

```
volatile unsigned int* const UART0DR = (unsigned int*) 0x10009000;

void print_uart0(const char *s) {
    while (*s != '\0') { /* Loop until end of string */
        *UART0DR = (unsigned int)(*s); /* Transmit char */
        s++; /* Next char */
    }
}
```

main.cpp

```
class SideEffect {
public:
    SideEffect(const char* s): _s(s) {
        print_uart0("SideEffect created ");
        print_uart0(_s);
        print_uart0("\n");
    }

    ~SideEffect() {
        print_uart0("SideEffect destroyed ");
        print_uart0(_s);
        print_uart0("\n");
    }
private:
    const char* _s;
};

SideEffect se_global1("global 1");
SideEffect se_global2("global 2");
SideEffect se_global3("global 3");
SideEffect se_global4("global 4");
SideEffect se_global5("global 5");
```

main.cpp

```cpp
int zero_array[] = {0, 0, 0, 0, 0, 0};

void test_bss_is_zero() {
    bool is_zero = true;

    for (int i = 0; i < sizeof(zero_array) / sizeof(zero_array[0]); ++i) {
        if (zero_array[i] != 0) {
            is_zero = false;
        }
    }

    if (is_zero) {
        print_uart0("zero_array was initialized\n");
    } else {
        print_uart0("zero_array was NOT initialized!!!\n");
    }
}
```

main.cpp

```cpp
int main() {
    SideEffect se_local("local");

    test_bss_is_zero();

    print_uart0("Hello world!\n");

    return 0;
}
```

main.cpp

```
SECTIONS {
    . = 0x0;

    .startup : {
        src/startup.o(.vector_table)
    }
```

main.ld

```
. = 0x10000;

.text : {
    *(.entry)
    *(.text)
    *(.rodata)
}
```

main.ld

```
.bss : {
    _bss_start = .;
    *(.bss)
    . = ALIGN(8);
    _bss_end = .;
}

.data : {
    _data_start = .;
    *(.data)
    . = ALIGN(8);
    _data_end = .;
}

.init_array : {
    _init_array_start = .;
    *(.init_array)
    *(.init_array.*)
    _init_array_end = .;
}

.fini_array : {
    _fini_array_start = .;
    *(.fini_array)
    *(.fini_array.*)
    _fini_array_end = .;
}
```

main.ld

```
    . = ALIGN(8);
    _stack_start = .;
    . = . + 0x1000; /* 4kB of stack memory */
    _stack_end = .;
}
```

main.ld

Compilação

```
arm-gcc -c -mcpu=cortex-a9 -g -fno-exceptions
-fno-threadsafe-statics -fno-use-cxa-atexit -nostdlib
-lgcc src/main.cpp -o src/main.o
```

Compilação

```
arm-as src/startup.s -o src/startup.o
```

Compilação

```
arm-ld -T main.ld src/*.o -o main.elf
```

Compilação

```
arm-objcopy -O binary main.elf main.bin
```

Execução

```
qemu-system-arm -M realview-pbx-a9 -m 128M -nographic
-no-reboot -serial stdio -monitor
telnet:0.0.0.0:1234,server,nowait -kernel main.bin
```

Execução

```
SideEffect created global 1
SideEffect created global 2
SideEffect created global 3
SideEffect created global 4
SideEffect created global 5
SideEffect created local
zero_array was initialized
Hello world!
SideEffect destroyed local
SideEffect destroyed global 5
SideEffect destroyed global 4
SideEffect destroyed global 3
SideEffect destroyed global 2
SideEffect destroyed global 1
```

Referências

http://bravegnu.org/gnu-eprog/lds.html
https://sourceware.org/binutils/docs/ld/Scripts.html
http://newtoncbraga.com.br/index.php/telecom-artigos/1709-
http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dui0447j/Bbabegge.html
http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dui0440b/Bbabegge.html
http://umanovskis.se/files/arm-baremetal-ebook.pdf
https://arobenko.gitbooks.io/bare_metal_cpp/content/
https://wiki.qemu.org/Documentation/Platforms/ARM
https://balau82.wordpress.com/2010/02/28/hello-world-for-bare-metal-arm-using-qemu/