

Homework 8

Problem I

Replace the following IA32 instructions with equivalent Y86 ones.

IA32 Instruction	Y86 Instruction
movl 8(%ebp),%ecx	rrmovl 8(%ebp),%ecx
testl %edx,%edx	andl %edx,%edx
movl %esp,%ebp	rrmovl %esp,%ebp
addl (%ecx),%eax	rrmovl (%ecx),%esi (not only %esi) addl %esi,%eax
decl %edx	irmovl \$-1,%ebx (not only %ebx) addl %ebx,%edx
cmpl %esi, %eax jg L1	subl %esi, %eax jg L1

Problem II

Read the following codes and answer the questions below.

Y86 Code	Assembly Code
0x000: 0x000: 30f400020000 0x006: 30f500020000 0x00c: 8024000000 0x011: 00	# Execution begins at address 0 .pos 0 init: irmovl Stack, %esp irmovl Stack, %ebp call Main halt
0x014: 0x014: 05000000 0x018: 0b000000 0x01c: 17000000 0x020: 12000000	# Array of 4 elements .align 4 array: .long 0x5 .long 0xb .long 0x17 .long 0x12
0x024: a05f 0x026: 2045 0x028: 30f004000000 0x02e: a00f 0x030: 30f214000000 0x036: a02f	Main: pushl %ebp rrmovl %esp, %ebp irmovl \$4, %eax pushl %eax irmovl array, %edx pushl %edx

0x038: 8042000000 0x03d: 2054 0x03f: b05f 0x041: 90	call Foo rrmovl %ebp, %esp popl %ebp ret
0x042: a05f 0x044: 2045 0x046: 501508000000 0x04c: 50250c000000 0x052: 500100000000 0x058: 30f304000000 0x05e: 6031 0x060: 30f3ffffff 0x066: 6032 0x068: 6222 0x06a: 739a000000 0x06f: 506100000000 0x075: 2003 0x077: 6163 0x079: 7283000000 0x07e: 7085000000 0x083: 2060 0x085: 30f304000000 0x08b: 6031 0x08d: 30f3ffffff 0x093: 6032 0x095: 746f000000 0x09a: 2054 0x09c: b05f 0x09e: 90	# int Foo(int *array, int count) Foo: pushl %ebp rrmovl %esp, %ebp rrmovl 8(%ebp), %ecx rrmovl 12(%ebp), %edx rrmovl (%ecx), %eax irmovl \$4, %ebx addl %ebx, %ecx irmovl \$-1, %ebx addl %ebx, %edx andl %edx, %edx je End Loop: rrmovl (%ecx), %esi rrmovl %eax, %ebx subl %esi, %ebx jl Then jmp After Then: rrmovl %esi, %eax After: irmovl \$4, %ebx addl %ebx, %ecx irmovl \$-1, %ebx addl %ebx, %edx jne Loop End: rrmovl %ebp, %esp popl %ebp ret

1. The starting address of the stack?
0x200
2. What's the value of %eax after running the program?
0x17.
3. Describe the behavior of function `Foo`.
Return the max value in the array.

Problem III

Read the following codes and fill the given table.

```
/* module a.c */
#include <stdio.h>
```

```

int c = 5;
int arr[10];

void print(int x)
{
    static int y = 7;
    int b = x + 1;
    printf("%d\n", b);
}

```

Indicate the location of the following symbols, which is .data, .bss, .text or stack.

Symbol	Location
c	.data
arr	.bss
y	.data
b	stack
print	.text

Problem IV

Read the following codes and fill the given table.

main.c	print.c
<pre> char *p = "hello"; void print(); int main() { print(); return 0; } </pre>	<pre> #include <stdio.h> extern char *p; char *p1 = "world\n"; static char *p2 = "hello moto!"; void print() { printf("%s %s", p, p1); } static void print2() { printf("%s", p2); } </pre>

Indicate the kind of the following symbols, which is defined global, referenced global or local

File	Symbol	Kind
main.c	p	defined global
	print	referenced global
print.c	p	referenced global
	p1	defined global
	p2	local
	print	defined global
	print2	local