Arquitecturas Intel 64 e IA-32

Organización del Computador II

Segundo Cuatrimestre 2021

Enunciado nro. 2

En esta actividad, vamos a trabajar con el primer y segundo volumen de los manuales Intel® 64 and IA-32 Architectures Software Developer's Manual. Nuestro objetivo de aprendizaje es familiarizarnos con los manuales, buscar características fundamentales de las arquitecturas Intel® 64 e IA-32 y entender las explicaciones de algunas de las instrucciones básicas de la programación en el lenguaje ensamblador de Intel.

Pueden descargar los manuales con los que vamos a trabajar desde los links:

- Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 1: Basic Architecture
- Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 2: Instruction Set Reference, A-Z

1. Arquitectura básica IA-32 e Intel 64

En esta sección, vamos a trabajar con el primer volumen de los manuales de Intel para entender la arquitectura básica de los procesadores Intel.

Ejercicio 1 Intel 64 Entorno de ejecución
Busquen en el manual la sección ***3.2.1 64-Bit Mode Execution Environment*** en *Vol. 1 3-2*. En base a lo que dice la sección ***Address Space*** y la figura *3-2 64-Bit Mode Basic Execution Environment*. Indiquen:

a) ¿Cuál es el tamaño en bits de una dirección de memoria en la arquitectura Intel 64?

b) ¿Cuál es el tamaño de memoria direccionable?

c) ¿Cuántos registros de propósito general hay en Intel 64 y que tamaño tienen?

d) Busque en el manual que guarda el registro RFLAGS, indique su tamaño en bits y su formato.

e) Busque en el manual que guarda el registro RIP, indique su tamaño en bits y su formato.

f) ¿Por qué el RIP tiene ese tamaño?

Ejercicio 2 Flags
Busquen en el manual la sección ***3.2.1 64-Bit Mode Execution Environment*** en *Vol. 1 3-5*. En base a lo que dice la sección ***Address Space*** y la figura *3-2 64-Bit Mode Basic Execution Environment*. Indiquen:

a) Busque en el manual que guarda el registro EFLAGS e indique su tamaño en bits.

b) En el formato del registro, busque los siguiente bits e indique para que son y en que posición del registro estan almacenados:

   - Flag de Cero
   - Flag de Carry
   - Flag de Interrupciones

c) Indique si en la arquitectura Intel 64 se usa el mismo registro. En caso que sea otro, indiquen su tamaño y la relación tendría con el de IA-32.

Ejercicio 3 Stack y llamadas a función
Busquen en el manual la sección ***Overview of the basic execution environment*** en *3-2 Vol. 1*. Indiquen:

a) ¿Para qué es necesaria la pila?

b) ¿Donde está ubicada?

Investiguemos un poco más como maneja la pila Intel y que debemos hacer nosotros como programadores. Para eso, vayan a la sección ***6.2 Stacks*** en *Vol. 1 6-1.* Observen el dibujo de la pila *Figure 6-1. Stack Structure.*
Luego, en las secciones ***6.2.4.1 Stack-Frame Base Pointer*** y ***6.2.4.2 Return Instruction Pointer*** van a encontrar información sobre los registros ESP y EBP. Expliquen con sus palabras:

a) ¿Para qué sirve el registro ESP?

b) ¿Para qué sirve el registro EBP?

c) En el primer parrafo, ¿Qué registro se pushea en la pila al hacer un CALL? Discutan con sus compañeros por qué creen que hace eso

d) En el primer parrafo, ¿Qué ocurre al hacer un RET? Discutan con sus compañeros por qué creen que hace eso

e) En el segundo parrafo, ¿Qué debe asegurarse el programador antes de llamar a un RET cuando esta escribiendo una subrutina? ¿Cómo lo asegura?

f) ¿Cuál es el ancho de la pila en modo 32 bits y en 64 bits? (tamaño del dato de PUSH y POP)

g) Luego de responder las preguntan anteriores, discutan en grupo si el EBP podría ser usado para guardar datos que no sean la base de la pila. ¿Qué opinan?

Checkpoint 1

2. Set de Instrucciones IA-32 e Intel 64

Ya hemos explorado la arquitectura básica de Intel. En esta sección vamos a conocer algunas de las instrucciones más básicas.

Ejercicio 4 Set de instrucciones En el segundo volumen del manual Intel® 64 and IA-32 Architectures Software Developerś Manual Volume 2: Instruction Set Reference, A-Z busquen las siguientes instrucciones:

a) SUB

b) XOR

c) INC

d) JE

Expliquen con sus palabras

a) Observen el formato de la instrucción y respondan, ¿cuántos operandos recibe, de qué tipo son y qué tamaño tienen?. Por ejemplo, 2 operandos de los tipo registro-registro de 8 a 64 bits, memoria-registro, memoria-memoria

b) ¿Qué hace la instrucción?

c) Den uno o más ejemplos de su uso (traten que varien los operandos y tamaño de dato leido). Por ejemplo, SUB EAX, 0x00000001 o ADD RAX, 1.

Los jumps figuran en la sección ***Jcc—Jump if Condition Is Meet*** del segundo volumen.

Adicionalmente pueden apoyarse en sitios de Internet que sumarizen la información para ayudarse a responder las preguntas sobre las instrucciones.

Checkpoint 2