UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
Facultad de Ingeniería, Arquitectura y Diseño

Ingeniero en Software y Tecnologías Emergentes

Manual de Talleres de la materia Organización de Computadoras

AUTOR(ES)
Jonatan Crespo Ragland

Taller No. 8

Objetivo: Desarrollar los códigos de operación y proceso de ensamblaje

Fundamentos teóricos del taller

- Lenguaje Ensamblador x86

Instrucciones para el desarrollo del taller

1. Desarrolla los siguientes puntos

Recursos

1. Apuntes de clase.
2. Fuentes bibliográficas.
3. Lápiz.
4. Equipo de cómputo.

Tiempo e instrucciones de entrega

Duración: 2 horas.

Documenta y desarrolla los siguientes conceptos de lenguaje ensamblador x86, identificando sus conceptos y sus usos:

Stack Pointer:

Un puntero de pila es un pequeño registro que almacena la dirección de memoria del último elemento de datos añadido a la pila o, en algunos casos, la primera dirección disponible en ella. Una pila es un búfer especializado que las funciones de un programa utilizan para almacenar datos como parámetros, variables locales y otra información relacionada con la

función. El puntero de pila, también conocido como puntero de pila extendido (ESP), garantiza que el programa siempre añade datos a la ubicación correcta en la pila.

Base Pointer:

Este registro se denomina puntero base, ya que su uso más común es apuntar a la base de un marco de pila durante las llamadas a funciones. Sin embargo, a diferencia de los registros mencionados anteriormente, puede usar cualquier otro registro para este propósito si es necesario.

Instruction Pointer:

El registro de puntero de instrucción, llamado registro EIP, es simplemente el registro más importante con el que se trabajará en cualquier ingeniería inversa. El EIP registra la siguiente instrucción a ejecutar. El EIP apunta a la siguiente instrucción a ejecutar. Si se modifica este puntero para saltar a otra área del código, se tiene control total sobre el programa.

Carry Flag:

En ensamblaje, la bandera de acarreo (carry flag) es un indicador de estado del procesador que indica si se ha producido un acarreo o préstamo aritmético. Se utiliza para realizar operaciones aritméticas precisas de varias palabras.

Auxiliary Carry Flag

El indicador de acarreo auxiliar (AC) del microprocesador 8085 es un indicador de estado específico que se utiliza principalmente en operaciones aritméticas con código decimal binario (BCD). Es uno de los cinco indicadores del registro de indicadores del 8085, que también incluye los indicadores de signo, cero, paridad y acarreo.

Parity Flag:

El indicador de paridad indica si el byte de orden más bajo del resultado de una operación aritmética o bit a bit tiene un número par o impar de unos . Indicador = 1 si la paridad es par; Indicador = 0 si la paridad es impar.

Overflow Flag:

La bandera de acarreo auxiliar (AF) es un indicador de ajuste que se utiliza en ensamblaje para ampliar la capacidad de realizar operaciones aritméticas con números más grandes.

Sign Flag:

En ensamblador, la bandera de signo (S) es un bit lógico que indica si el resultado de una operación es positivo o negativo. Se activa cuando se activa el indicador de desbordamiento de complemento a dos o el indicador negativo, pero no ambos.

Zero Flag:

En ensamblador, la bandera cero (ZF) y la bandera de signo (SF) son indicadores que se usan para comprobar el resultado de operaciones aritméticas y lógicas.

Direction Flag:

En ensamblador, la bandera de dirección (DF) controla la dirección de las operaciones de cadenas. Se aplica a todas las instrucciones de ensamblaje que usan el prefijo REP, como MOVS, MOVSD, y MOVSW.

Interrupt Flag:

La función de interrupción (INT). Puede utilizarse para acceder a funciones del DOS o del BIOS. Las funciones del BIOS se utilizan normalmente para acceder al hardware, mientras que las del DOS se utilizan para salir de programas, leer un carácter del teclado y escribirlo en la pantalla.

Code Segment

Un segmento de código, también conocido como segmento de texto, es una porción de un archivo objeto o la sección correspondiente del espacio de direcciones virtuales del programa que contiene instrucciones ejecutables .

Data Segment:

El segmento de datos es el lugar en la RAM donde un programa almacena sus datos globales y estáticos. Estos datos se definen en tiempo de compilación. El segmento de datos no contiene variables asignadas en tiempo de ejecución (el montículo se utiliza para este propósito) ni variables locales de subprocedimientos (la pila se utiliza para almacenarlas).

Extra Segment:

En ensamblador, el segmento extra (ES) es una ubicación de memoria adicional para variables, que se utiliza cuando el segmento de datos no es suficiente. Se usa para acceder a otro segmento que contiene más datos.

Stack Segment:

En ensamblador, el segmento de pila (SS) es un área de memoria que contiene la pila de llamadas de un programa. Se utiliza para gestionar variables locales, argumentos de funciones, y direcciones de retorno.

Anexos

Instrucción de Salto	Condición
JE	Salta si los operandos son iguales
JNE	Salta si los operandos no son iguales
JG	Salta si el primer operando es mayor que el segundo
JGE	Salta si el primer operando es mayor o igual al segundo
JL	Salta si el primer operando es menor que el segundo
JLE	Salta si el primer operando es menor o igual al segundo
JA	Salta si el primer operando es mayor sin acarreo
JAE	Salta si el primer operando es mayor o igual sin acarreo
JB	Salta si el primer operando es menor con acarreo
JBE	Salta si el primer operando es menor o igual con acarreo
JC	Salta si hubo acarreo (Carry Flag = 1)
JNC	Salta si no hubo acarreo (Carry Flag = 0)
JO	Salta si hubo desbordamiento (Overflow Flag = 1)
JNO	Salta si no hubo desbordamiento (Overflow Flag = 0)

JS	Salta si el resultado es negativo (Sign Flag = 1)
JNS	Salta si el resultado no es negativo (Sign Flag = 0)
JP / JPE	Salta si el resultado tiene paridad par (Parity Flag = 1)
JNP / JPO	Salta si el resultado tiene paridad impar (Parity Flag = 0)
JZ	Salta si el resultado es cero (Zero Flag = 1)
JNZ	Salta si el resultado no es cero (Zero Flag = 0)

Instrucción	Descripción
AND	Realiza una operación lógica AND entre dos operandos
OR	Realiza una operación lógica OR entre dos operandos
XOR	Realiza una operación lógica XOR entre dos operandos
NOT	Realiza una operación lógica NOT (negación) sobre un operando
TEST	Realiza una operación AND entre dos operandos y ajusta las banderas sin almacenar el resultado
SHL / SAL	Desplazamiento lógico a la izquierda (Shift Left)
SHR	Desplazamiento lógico a la derecha (Shift Right)
ROL	Rotación a la izquierda (Rotate Left)
ROR	Rotación a la derecha (Rotate Right)

Bandera	Descripción
CF	Carry Flag: Indica si hubo un acarreo en una operación de suma o si ocurrió un "préstamo" en una resta.
PF	Parity Flag: Indica si el número de bits 1 en el resultado es par (1) o impar (0).
AF	Auxiliary Carry Flag: Se activa si hay un acarreo entre los 3 y 4 bits más bajos en una operación.
ZF	Zero Flag: Se activa si el resultado de la operación es 0.
SF	Sign Flag: Indica si el resultado de la operación es negativo (el bit más significativo es 1).
TF	Trap Flag: Se activa para permitir la ejecución de una instrucción de "trampa" (utilizado en depuración).
IF	Interrupt Enable Flag: Indica si las interrupciones están habilitadas (1) o deshabilitadas (0).

DF	Direction Flag: Determina si el procesamiento de cadenas de caracteres ocurre hacia arriba o hacia abajo en memoria.
OF	Overflow Flag: Se activa si ocurrió un desbordamiento aritmético.
SF	Sign Flag: Indica el signo del resultado de una operación.
ZF	Zero Flag: Se activa si el resultado de la operación es cero.

Instrucción	Descripción
DB	Define un byte o un conjunto de bytes.
DW	Define una palabra (2 bytes).
DD	Define una doble palabra (4 bytes).
DQ	Define una cuádruple palabra (8 bytes).
DT	Define un tipo de 10 bytes (utilizado para valores de punto flotante de precisión extendida).
RESB	Reserva espacio en bytes. No inicializa los valores.
RESW	Reserva espacio en palabras (2 bytes).
RESD	Reserva espacio en doble palabra (4 bytes).
RESQ	Reserva espacio en cuádruple palabra (8 bytes).
RESY	Reserva espacio en 80 bytes (usado generalmente en operaciones de precisión extendida de punto flotante).