Архитектура x86

Д. В. Луцив

Кафедра системого программирования СПбГУ

CS220 (231000)

CC BY NC SA

Содержание

Регистры

- $AH_8, AL_8, \ldots \rightarrow AX_{16}, \ldots \rightarrow EAX_{32}$
- EAX (общий), EDX (умножение и деление вместе с EAX), EBX (указатели), ECX (счетчик)
- EDI (dest index), ESI (source index)
- EBP, ESP, EIP
- CS, SS, DS, ES, FS, GS — сегментные
- EFLAGS

_H, _L — 8-разрядные,
_X, _S — 16-разрядные,
E_ — 32-разрядные.

EFLAGS

Весь регистр 32-битный (начиная с 80386).
Основные флаги (с 8086):

- OF — флаг переполнения;
- DF — флаг направления;
- IF — флаг прерывания;
- TF — флаг трассировки;
- SF — флаг знака;
- ZF — флаг нуля;
- AF — флаг дополнительного переноса (для упакованных двоично-десятичных операций);
- PF — флаг четности;
- CF — флаг переноса;

- Отсутствие (аргументы в коде)
- Регистровая (номер регистра в коде)
- Память[E_X + смещение], Память[EBP + смещение], + возможно префиксы сегментов

- MOV память обменивается только с арифметическими регистрами, ESI, EDI
- XCHG reg, mem/reg
- LAHF, SAHF — флаги $\leftrightarrow$ AH

Логические

AND, OR, XOR, NOT

Арифметические

- ADD, SUB, ADC, SBB, INC, DEC, NEG
- MUL (reg/mem), DIV (reg/mem), IMUL, IDIV,
- CWQ (EAX $\rightarrow$ EDX:EAX)

Сдвига

- ROR, ROL
- RCL, RCR — с переносом
- SHL, SHR — без переноса
- SAL, SAR — со знаковыми битами

BCD

ASCII и BCD — для быстрого преобразования двоично-десятичных чисел

- PUSH, POP
- PUSHA, POPA
- Косвенно — CALL, RET, INT, IRET

Переходы Безусловные

- JMP FAR, NEAR, JMP Mxx, JMP REG

Команды Сравнения

- CMP — как SUB
- TEST — как AND
- CMPS — CMPSB, CMPSW, CMPSD
- CMPXCHG dest, src — Сарвнивает аккумулятор (8-32 bits) с dest. Если равны, то в dest грузят src, иначе в аккумулятор загружают dest. Ужас.

Условные переходы I

По результату R или итогам сравнения $A?B$, в зависимости от получившихся значений флагов.

Беззнаковые

- JA/JNBE — если $A > B$;
- JAE/JNB/JNC — если $A \geq B$;
- JB/JNAE/JC — если $A < B$;
- JBE/JNA — если $A \leq B$.

Знаковые

- JG/JNLE — если $A > B$;
- JGE/JNL — если $A \geq B$;
- JL/JNGE — если $A < B$;
- JLE/JNG — если $A \leq B$;
- JNS — если $R \geq 0$;
- JS — если $R < 0$.

Условные переходы II

По результату R или итогам сравнения $A?B$, в зависимости от получившихся значений флагов.

- JE/JZ — если $A = B \vee R = 0$;
- JNE/JNZ — если $A \neq B \vee R \neq 0$;
- JNO — $\neg OF$;
- JO — OF;
- JCXZ — $CX = 0$ — для организации циклов `do ... while(--CX);`;
- JNP/JPO — $\neg PF$;
- JP/JPE — PF.

Вызовы

- Прерывания
  - Управление STI, CLI
  - Ожидание (HALT)

Команды ввода-вывода

IN (mem/DX), OUT (mem/DX) — с AL

Команды обработки строк

- REP, REPE, REPZ, REPNE, REPNZ
- LODS (загружает в аккумулятор),
  STOS (пишет из аккумулятора),
  MOVS (B-W-D — пересылка память-память),
  CMPS(сравнение память-память),
  SCAS (вычитает из аккумулятора)
- DF — флаг направления

Команды математического сопроцессора

- загрузить из памяти / выгрузить в память, формат
- загрузить из регистра целое / выгрузить в регистр целое
- операции и функции
- дублирование / стирание вершины
- FWAIT

Команды управления защитой и виртуальной памятью

Загрузка таблиц дескрипторов/страниц

Вопросы

EDU.DLUCIV.NAME