

Примеры архитектур: Intel x86 и RISC-V

Луцив Дмитрий Вадимович

Кафедра системного программирования СПбГУ



- 1 Архитектура и система команд x86
 - Регистры и адресация
 - Система команд
- 2 Архитектура и система команд RISC-V
 - Регистры
 - Соглашение о вызовах
 - Команды и формат машинного кода
 - Кросс-компиляция

Архитектура и система команд x86

- Регистры и адресация
- Система команд

Регистры (для 32-битной ЭВМ)

- EAX (общий, аккумулятор), 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

Регистры (для 32-битной ЭВМ)

- EAX (общий, аккумулятор), 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

Фрагменты регистров

- _H, _L — 8-разрядные
- _X, _S — 16-разрядные
- E_ — 32-разрядные
- R_ — 64-разрядные

Например, для аккумулятора

(AH (8), AL (8)) → AX (16) → EAX (32) → RAX (64)

Регистр флагов 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

- Непосредственная (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,
- CWD (EAX → EDX:EAX)

Сдвига

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

ASCII и BCD — для быстрого преобразования двоично-десятичных чисел

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

Переходы Безусловные

- JMP FAR, NEAR, JMP M[xx], JMP REG

Команды Сравнения

- CMP — как SUB
- TEST — как AND
- CMPS — CMPSB, CMPSW, CMPSD

Переходы Безусловные

- JMP FAR, NEAR, JMP M[xx], JMP REG

Команды Сравнения

- CMP — как SUB
- TEST — как AND
- CMPS — CMPSB, CMPSW, CMPSD

Compare-exchange

- CMPXCHG dest, src — Сравнивает аккумулятор (8-64 bits) с dest. Если равны, то в dest грузят src, иначе в аккумулятор загружают dest

Команды сравнения и передачи управления

Переходы Безусловные

- JMP FAR, NEAR, JMP M[xx], JMP REG

Команды Сравнения

- CMP — как SUB
- TEST — как AND
- CMPS — CMPSB, CMPSW, CMPSD

Compare-exchange

- CMPXCHG dest, src — Сравнивает аккумулятор (8-64 bits) с dest. Если равны, то в dest грузят src, иначе в аккумулятор загружают dest

Ужас. Кошмар. Для чего она?.. [↗](#)

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

Беззнаковые

- $JA/JNBE$ — если $A > B$;
- $JAЕ/JNB/JNC$ — 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 $R < 0$.

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

IN (mem/DX), OUT (mem/DX) — с AL

- 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)

Команды обработки строк (микроциклы)

- 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)

Команды учитывают DF — флаг направления. Выставив его «неправильно» можно быстро размножить участок памяти

Стековые

- FLD, FSTP — загрузить из памяти / выгрузить в память, формат
- FILD, FILD, ... — загрузить из регистра целое / выгрузить в регистр целое
- FMUL, ... — операции и функции
- FWAIT — синхронизация для старых процессоров

Регистровые

MULSD, MULSF — работают с векторными регистрами (появились в Pentium MMX, позволяют производить по несколько операций с числами разной длины)

Загрузка таблиц страниц и дескрипторов, изменение режимов работы процессора

Архитектура и система команд RISC-V

- Регистры
- Соглашение о вызовах
- Команды и формат машинного кода
- Кросс-компиляция

- При помощи **BuildRoot** [↗](#)
- С отладкой — при помощи **Ripes** [↗](#)

Вопросы

- 1 Приведите примеры арифметико-логических команд x86
- 2 Что такое микроциклы?
- 3 Приведите примеры и опишите работу нескольких команд условного перехода
- 4 Что такое лексема?
- 5 Что такое синтаксическое дерево?
- 6 Назовите обязательные стадии трансляции
- 7 Назовите опциональные стадии трансляции

Упражнения

- 1 Попробуйте воспользоваться претрансляцией для любого языка (Scheme, Julia, Nemerle, ...)
- 2 Скомпилируйте программу из примера для любой незнакомой архитектуры; пользуясь справочниками, объясните действия всех машинных команд

Вопросы



[EDU.DLUCIV.NAME](#) ↗