CPU-ARM

罗胤

2018-03

目录

Chapter 1

ARM 指令集

1.1 指令类型

ARM 指令分类如下:

- 数据处理指令 (Data processing). 以 4 位 opcode 标识, 最多 16 条数据处理指令.
- 数据加载与存储指令 (Load/Store)
  - LDR cond 01IPU0W1 Rn Rd addr_mode
  - LDRB cond 01IPU1W1 Rn Rd addr_mode
  - LDRBT cond 01I0U111 Rn Rd addr_mode
  - LDRD cond 000PUIW0 Rn Rd addr_mode
  - LDREX cond 00011001 Rn Rd SBO(4) 1001 SBO(4)
  - LDRH cond 000PUIW1 Rn Rd addr_mode(4) 1011 addr_mode
  - LDRSB cond 000OUIW1 Rn Rd addr_mode(4) 1101 addr_mode
  - LDRSH cond 000PUIW1 Rn Rd addr_mode(4) 1111 addr_mode
  - LDRT cond 01I0U011 Rn Rd addr_mode
  - STR cond 01IPU0W0 Rn Rd addr_mode
  - STRB cond 01IPU1W0 Rn Rd addr_mode
  - STRBT cond 01I0U110 Rn Rd addr_mode
  - STRD cond 000PUIW0 Rn Rd addr_mode(4) 1111 addr_mode
  - STREX
  - STRH
  - STRT
  -
- 分支指令 (Branch)
  - B, BL: cond 101L simm24
  - BLX: 1111 101H simm24 / cond 00010010 SBO(12) 0011 Rm
  - BX: cond 00010010 SBO(12) 0001 Rm
  - BXJ: cond 00010010 SBO(12) 0010 Rm

1.1.1 Load/Store 指令

1.1.1.1 Addressing Mode

1.1.1.2 Load and Store word or unsigned byte

- 指令格式: LDR|STR|{<cond>}{B}{T} Rd, <addressing_mode>
- 指令编码: cond 01IPUBWL Rn Rd addr
  - I, P, U, W, Rn, adddr: addressing mode
  - L: Load (1) and Store (0)
  - B: unsigned byte (1) and word (0)

1.1.1.3 Load and Store halfword or doubleword, and load signed byte

- 指令格式: LDR|STR|{<cond>}D|H|SH|SB Rd, <addressing_mode>
- 指令编码: cond 000PUIWL Rn Rd addr(4) 1SH1 addr(4)
  - I, P, U, W, Rn, adddr: addressing mode
  - L, S, H

1.1.2 Data-processing 指令

1.1.2.1 opcode1

- 指令格式: <opcode1>{<cond>}{S} <Rd>, <shifter_operand>
- 指令编码: cond 00I opcode(4) S SBZ Rd shift(12)
- 指令: MOV (1101), MVN (1111)

1.1.2.2 opcode2

- 指令格式: <opcode1>{<cond>} <Rn>, <shifter_operand>
- 指令编码: cond 00I opcode(4) 1 Rn SBZ shift(12)
- 指令: CMP (1010), CMN (1011), TST (1000), TEQ (1001)

1.1.2.3 opcode3

- 指令格式: <opcode1>{<cond>}{S} <Rd>, <Rn>, <shifter_operand>
- 指令编码: cond 00I opcode(4) S Rn Rd shift(12)
- 指令: ADD (0100), SUB (0010), RSB (0011), ADC (0101), SBC (0110), RSC (0111), AND (0000), BIC (1110), EOR (0001), ORR (1100)

1.1.3 Branch 指令

1.1.3.1 B, BL

- 指令格式: B{L}{cond} <target_address>
- 指令编码: cond 101L simm24

1.1.3.2 BLX

- 指令格式: BLX <target_address>
- 指令编码: 1111 101H simm24
- 指令格式: BLX{<cond>} <Rm>
- 指令编码: cond 00010010 SBO(12) 0011 Rm
- 指令格式: BX{cond} <target_address>
- 指令编码: cond 00010010 SBO(12) 0001 Rm
- 指令格式: BXJ{cond} <target_address>
- 指令编码: cond 00010010 SBO(12) 0010 Rm

1.2 操作数类型

1.2.1 addressing_mode 1

1.2.1.1 指令编码

- 编码区间: op[27..25], op[11..0]
- 编码类型: op[27..25]=000 (imm shift & reg shift, by op[4])
  - op[4]=0 (imm shift): shift_imm(5) shift(2) 0 Rm
  - op[4]=1 (reg shift): Rs 0 shift(2) 1 Rm
- 编码类型: op[27..25]=001 (imm32)
  - rotate_imm imm8

1.2.1.2 具体指令

- #<immediate>: rotate_imm(4) imm8(8)
- <Rm>: SBZ(8) Rm
- <Rm>, LSL|LSR|ASR|ROR #<shift_imm>: shift_imm(5) 00|01|10|11 0 Rm
- <Rm>, LSL|LSR|ASR|ROR <Rs>: Rs 0 00|01|10|11 1 Rm
- <Rm>, RRX: 0000 0110 Rm

1.2.2 addressing_mode 2

- imm offset/index: 010 PUBWL Rn Rd offset_12
- reg offset/index: 011 PUBWL Rn Rd SBZ(8) Rm
- scaled reg offset/index: 011 PUBWL Rn Rd shift_imm(5) shift(2) 0 Rm
- 选项位
  - P (op[24]): post-indexed (P=0), offset or pre-indexed (P=1)
  - U (op[23]): offset added to the base (U=1), subtracted from the base (U=0)
  - B (op[22]): unsigned byte (B=1), word (B=0)
  - W (op[21])
    * P=0: LDR/LDRB/STR/STRB (W=0), LDRT/LDRBT/STRT/STRBT (W=1)
    * P=1: base reg not updated (offset, W=0), base reg updated (pre-index, W=1)
  - L (op[20]): Load (L=1), Store (L=0)

Chapter 2

ARM 汇编语言