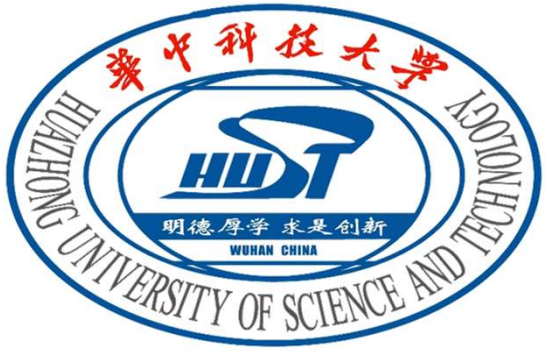
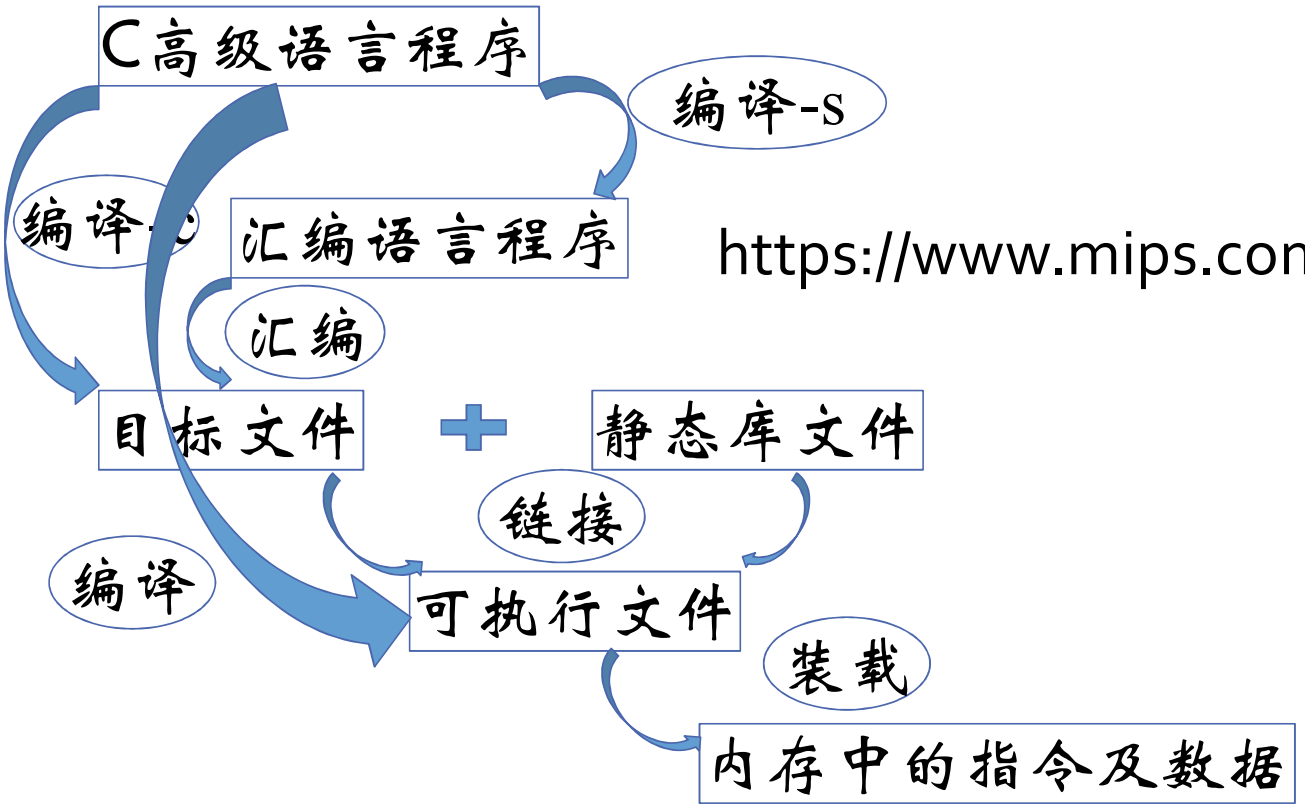
微机原理与接口技术

编译、汇编、链接、装载

华中科技大学　左冬红



高级语言由代码到执行需经历的过程



https://www.mips.com/develop/tools/compilers/

C语言源码

```
extern int expression2(int a,int b,int c,int d);
extern int expression1(int a,int b,int c,int d);
int main()
{
	int a,b,c,d,e,f;
	e=expression1(a,b,c,d);//(a+b)-(c+d)
	f=expression2(a,b,c,d);//(a-b)+(c-d)
}
```

mainproc.c

```
extern int factor1[15];
extern int sum(int a,int b);
int diff(int a,int b);
int factor2[15];
int expression2(int a,int b,int c,int d)
{	return diff(factor1[0]*sum(a,b),sum(c,d));
}
int diff(int a,int b)
{	return a-b;
}
```

expression2.c

```
extern int factor2[15];
extern int diff(int a,int b);
int sum(int a,int b);
int factor1[15];
int expression1(int a,int b,int c,int d)
{	return sum(factor2[0]*diff(a,b),diff(c,d));
}
int sum(int a,int b)
{	return a+b;
}
```

expression1.c

编译 -S -C

mips-img-elf-gcc -s -c mainproc.c

-c mainproc.c

mainproc.s

mainproc.o

mips-img-elf-gcc -s -c expression1.c

-c expression1.c

expression1.s

expression1.o

mips-img-elf-gcc -s -c expression2.c

-c expression2.c

expression2.s

expression2.o

查看obj文件

mips-img-elf-readelf -a mainproc.o

```
Relocation section '.rel.text' at offset 0x244 contains 2 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000020  00000c3d R_MIPS_PC26_S2    00000000   expression1
00000038  00000d3d R_MIPS_PC26_S2    00000000   expression2

Relocation section '.rel.pdr' at offset 0x254 contains 1 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000000  00000b02 R_MIPS_32         00000000   main
```

```
Section Headers:
  [Nr] Name              Type            Addr     Off    Size   ES Flg Lk Inf Al
  [ 0]                   NULL            00000000 000000 000000 00      0   0  0
  [ 1] .text             PROGBITS        00000000 000034 000058 00  AX  0   0  4
  [ 2] .rel.text         REL             00000000 000244 000010 08   I 12   1  4
  [ 3] .data             PROGBITS        00000000 00008c 000000 00  WA  0   0  1
  [ 4] .bss              NOBITS          00000000 00008c 000000 00  WA  0   0  1
  [ 5] .reginfo          MIPS_REGINFO    00000000 00008c 000018 18      0   0  4
  [ 6] .MIPS.abiflags    MIPS_ABIFLAGS   00000000 0000a8 000018 18   A  0   0  8
  [ 7] .pdr              PROGBITS        00000000 0000c0 000020 00      0   0  4
  [ 8] .rel.pdr          REL             00000000 000254 000008 08   I 12   7  4
  [ 9] .mdebug.abi32     PROGBITS        00000000 0000e0 000000 00      0   0  1
  [10] .comment          PROGBITS        00000000 0000e0 000045 01
  [11] .gnu.attributes   GNU_ATTRIBUTES  00000000 000125 000010 00
  [12] .symtab           SYMTAB          00000000 000138 0000e0 10
  [13] .strtab           STRTAB          00000000 000218 000029 00
  [14] .shstrtab         STRTAB          00000000 00025c 000078 00
```

```
Symbol table '.symtab' contains 14 entries:
   Num:    Value  Size Type    Bind   Vis      Ndx Name
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000     0 FILE    LOCAL  DEFAULT  ABS mainproc.c
     2: 00000000     0 SECTION LOCAL  DEFAULT    1
     3: 00000000     0 SECTION LOCAL  DEFAULT    3
     4: 00000000     0 SECTION LOCAL  DEFAULT    4
     5: 00000000     0 SECTION LOCAL  DEFAULT    9
     6: 00000000     0 SECTION LOCAL  DEFAULT    5
     7: 00000000     0 SECTION LOCAL  DEFAULT    6
     8: 00000000     0 SECTION LOCAL  DEFAULT    7
     9: 00000000     0 SECTION LOCAL  DEFAULT   10
    10: 00000000     0 SECTION LOCAL  DEFAULT   11
    11: 00000000    88 FUNC    GLOBAL DEFAULT    1 main
    12: 00000000     0 NOTYPE  GLOBAL DEFAULT  UND expression1
    13: 00000000     0 NOTYPE  GLOBAL DEFAULT  UND expression2
```

定义的大小明确、地址不明确

obj反汇编-mainproc.o

```
Disassembly of section .text:

00000000 <main>:
   0:   27bdffd0    addiu   sp,sp,-48
   4:   afbf002c    sw  ra,44(sp)
   8:   afbe0028    sw  s8,40(sp)
   c:   03a0f025    move    s8,sp
  10:   8fc7001c    lw  a3,28(s8)
  14:   8fc60018    lw  a2,24(s8)
  18:   8fc50014    lw  a1,20(s8)
  1c:   8fc40010    lw  a0,16(s8)
  20:   ebffffff    balc    20 <main+0x20>
  24:   afc20020    sw  v0,32(s8)
  28:   8fc7001c    lw  a3,28(s8)
  2c:   8fc60018    lw  a2,24(s8)
  30:   8fc50014    lw  a1,20(s8)
  34:   8fc40010    lw  a0,16(s8)
  38:   ebffffff    balc    38 <main+0x38>
  3c:   afc20024    sw  v0,36(s8)
  40:   00001025    move    v0,zero
  44:   03c0e825    move    sp,s8
  48:   8fbf002c    lw  ra,44(sp)
  4c:   8fbe0028    lw  s8,40(sp)
  50:   27bd0030    addiu   sp,sp,48
  54:   d81f0000    jrc ra
```

expression2.o

```
Relocation section '.rel.text' at offset 0x2cc contains 5 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000024  00000d05 R_MIPS_HI16       00000000   factor1
00000028  00000d06 R_MIPS_LO16       00000000   factor1
00000034  00000e3d R_MIPS_PC26_S2    00000000   sum
00000044  00000e3d R_MIPS_PC26_S2    00000000   sum
00000050  00000f3d R_MIPS_PC26_S2    0000006c   diff

Relocation section '.rel.pdr' at offset 0x2f4 contains 2 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000000  00000c02 R_MIPS_32         00000000   expression2
00000020  00000f02 R_MIPS_32         0000006c   diff
```

```
Symbol table '.symtab' contains 16 entries:
   Num:    Value  Size Type    Bind   Vis      Ndx Name
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000     0 FILE    LOCAL  DEFAULT  ABS expression2.c
     2: 00000000     0 SECTION LOCAL  DEFAULT    1
     3: 00000000     0 SECTION LOCAL  DEFAULT    3
     4: 00000000     0 SECTION LOCAL  DEFAULT    4
     5: 00000000     0 SECTION LOCAL  DEFAULT    9
     6: 00000000     0 SECTION LOCAL  DEFAULT    5
     7: 00000000     0 SECTION LOCAL  DEFAULT    6
     8: 00000000     0 SECTION LOCAL  DEFAULT    7
     9: 00000000     0 SECTION LOCAL  DEFAULT   10
    10: 00000000     0 SECTION LOCAL  DEFAULT   11
    11: 00000004    60 OBJECT  GLOBAL DEFAULT  COM factor2
    12: 00000000   108 FUNC    GLOBAL DEFAULT    1 expression2
    13: 00000000     0 NOTYPE  GLOBAL DEFAULT  UND factor1
    14: 00000000     0 NOTYPE  GLOBAL DEFAULT  UND sum
    15: 0000006c    48 FUNC    GLOBAL DEFAULT    1 diff
```

定义的大小明确、地址不明确

obj反汇编-expression2.o

```
Disassembly of section .text:

00000000 <expression2>:
   0:   27bdffe0    addiu   sp,sp,-32
   4:   afbf001c    sw  ra,28(sp)
   8:   afbe0014    sw  s8,20(sp)
   c:   afb00018    sw  s0,24(sp)
  10:   03a0f025    move    s8,sp
  14:   afc40020    sw  a0,32(s8)
  18:   afc50024    sw  a1,36(s8)
  1c:   afc60028    sw  a2,40(s8)
  20:   afc7002c    sw  a3,44(s8)
  24:   3c020000    lui v0,0x0
  28:   8c500000    lw  s0,0(v0)
  2c:   8fc50024    lw  a1,36(s8)
  30:   8fc40020    lw  a0,32(s8)
  34:   ebffffff    balc    34 <expression2+0x34>
  38:   02028098    mul s0,s0,v0
  3c:   8fc5002c    lw  a1,44(s8)
  40:   8fc40028    lw  a0,40(s8)
  44:   ebffffff    balc    44 <expression2+0x44>
  48:   00402825    move    a1,v0
  4c:   02002025    move    a0,s0
  50:   ebffffff    balc    50 <expression2+0x50>
  54:   03c0e825    move    sp,s8
  58:   8fbf001c    lw  ra,28(sp)
  5c:   8fbe0014    lw  s8,20(sp)
  60:   8fb00018    lw  s0,24(sp)
  64:   27bd0020    addiu   sp,sp,32
  68:   d81f0000    jrc ra
```

expression1.o

```
Relocation section '.rel.text' at offset 0x2cc contains 5 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000024  00000d05 R_MIPS_HI16       00000000   factor2
00000028  00000d06 R_MIPS_LO16       00000000   factor2
00000034  00000e3d R_MIPS_PC26_S2    00000000   diff
00000044  00000e3d R_MIPS_PC26_S2    00000000   diff
00000050  00000f3d R_MIPS_PC26_S2    0000006c   sum

Relocation section '.rel.pdr' at offset 0x2f4 contains 2 entries:
 Offset     Info    Type            Sym.Value  Sym. Name
00000000  00000c02 R_MIPS_32         00000000   expression1
00000020  00000f02 R_MIPS_32         0000006c   sum
```

定义的大小明确、地址不明确

```
Symbol table '.symtab' contains 16 entries:
   Num:    Value  Size Type    Bind   Vis      Ndx Name
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000     0 FILE    LOCAL  DEFAULT  ABS expression1.c
     2: 00000000     0 SECTION LOCAL  DEFAULT    1
     3: 00000000     0 SECTION LOCAL  DEFAULT    3
     4: 00000000     0 SECTION LOCAL  DEFAULT    4
     5: 00000000     0 SECTION LOCAL  DEFAULT    9
     6: 00000000     0 SECTION LOCAL  DEFAULT    5
     7: 00000000     0 SECTION LOCAL  DEFAULT    6
     8: 00000000     0 SECTION LOCAL  DEFAULT    7
     9: 00000000     0 SECTION LOCAL  DEFAULT   10
    10: 00000000     0 SECTION LOCAL  DEFAULT   11
    11: 00000004    60 OBJECT  GLOBAL DEFAULT  COM factor1
    12: 00000000   108 FUNC    GLOBAL DEFAULT    1 expression1
    13: 00000000     0 NOTYPE  GLOBAL DEFAULT  UND factor2
    14: 00000000     0 NOTYPE  GLOBAL DEFAULT  UND diff
    15: 0000006c    48 FUNC    GLOBAL DEFAULT    1 sum
```

obj反汇编-expression1.o

```
Disassembly of section .text:

00000000 <expression1>:
   0:   27bdffe0    addiu   sp,sp,-32
   4:   afbf001c    sw  ra,28(sp)
   8:   afbe0014    sw  s8,20(sp)
   c:   afb00018    sw  s0,24(sp)
  10:   03a0f025    move    s8,sp
  14:   afc40020    sw  a0,32(s8)
  18:   afc50024    sw  a1,36(s8)
  1c:   afc60028    sw  a2,40(s8)
  20:   afc7002c    sw  a3,44(s8)
  24:   3c020000    lui v0,0x0
  28:   8c500000    lw  s0,0(v0)
  2c:   8fc50024    lw  a1,36(s8)
  30:   8fc40020    lw  a0,32(s8)
  34:   ebffffff    balc    34 <expression1+0x34>
  38:   02028098    mul s0,s0,v0
  3c:   8fc5002c    lw  a1,44(s8)
  40:   8fc40028    lw  a0,40(s8)
  44:   ebffffff    balc    44 <expression1+0x44>
  48:   00402825    move    a1,v0
  4c:   02002025    move    a0,s0
  50:   ebffffff    balc    50 <expression1+0x50>
  54:   03c0e825    move    sp,s8
  58:   8fbf001c    lw  ra,28(sp)
  5c:   8fbe0014    lw  s8,20(sp)
  60:   8fb00018    lw  s0,24(sp)
  64:   27bd0020    addiu   sp,sp,32
  68:   d81f0000    jrc ra
```

链接

mips-img-elf-ld expression1.o expression2.o mainproc.o -o project_link

查看可执行文件project_link

不存在需重定义内容

```
Section Headers:
  [Nr] Name              Type            Addr     Off    Size   ES Flg Lk Inf Al
  [ 0]                   NULL            00000000 000000 000000 00      0   0  0
  [ 1] .MIPS.abiflags    MIPS_ABIFLAGS   00400098 000098 000018 18   A  0   0  8
  [ 2] .reginfo          MIPS_REGINFO    004000b0 000240 000018 18      0   0  4
  [ 3] .text             PROGBITS        004000b0 0000b0 000190 00  AX  0   0  4
  [ 4] .bss              NOBITS          00410240 000240 000078 00  WA  0   0  4
  [ 5] .comment          PROGBITS        00000000 000258 000044 01  MS  0   0  1
  [ 6] .pdr              PROGBITS        00000000 00029c 0000a0 00      0   0  4
  [ 7] .gnu.attributes   GNU_ATTRIBUTES  00000000 00033c 000010 00      0   0  1
  [ 8] .mdebug.abi32     PROGBITS        00000000 00034c 000000 00      0   0  1
  [ 9] .symtab           SYMTAB          00000000 00034c 0001b0 10     10  14  4
  [10] .strtab           STRTAB          00000000 0004fc 00008e 00      0   0  1
  [11] .shstrtab         STRTAB          00000000 00058a 00006a 00      0   0  1
```

查看可执行文件

不存在未定义

地址、大小都明确

```
Symbol table '.symtab' contains 27 entries:
   Num:    Value  Size Type    Bind   Vis      Ndx Name
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00400098     0 SECTION LOCAL  DEFAULT    1
     2: 004000b0     0 SECTION LOCAL  DEFAULT    2
     3: 004000b0     0 SECTION LOCAL  DEFAULT    3
     4: 00410240     0 SECTION LOCAL  DEFAULT    4
     5: 00000000     0 SECTION LOCAL  DEFAULT    5
     6: 00000000     0 SECTION LOCAL  DEFAULT    6
     7: 00000000     0 SECTION LOCAL  DEFAULT    7
     8: 00000000     0 SECTION LOCAL  DEFAULT    8
     9: 00000000     0 FILE    LOCAL  DEFAULT  ABS expression1.c
    10: 00000000     0 FILE    LOCAL  DEFAULT  ABS expression2.c
    11: 00000000     0 FILE    LOCAL  DEFAULT  ABS mainproc.c
    12: 00000000     0 FILE    LOCAL  DEFAULT  ABS
    13: 00418230     0 NOTYPE  LOCAL  DEFAULT    4 _gp
    14: 00410240     0 NOTYPE  GLOBAL DEFAULT    3 __fdata
    15: 0040014c   108 FUNC    GLOBAL DEFAULT    3 expression2
    16: 0041027c    60 OBJECT  GLOBAL DEFAULT    4 factor2
    17: 00410240    60 OBJECT  GLOBAL DEFAULT    4 factor1
    18: 0040011c    48 FUNC    GLOBAL DEFAULT    3 sum
    19: 004000b0   108 FUNC    GLOBAL DEFAULT    3 expression1
    20: 004000b0     0 NOTYPE  GLOBAL DEFAULT    3 __ftext
    21: 00410240     0 NOTYPE  GLOBAL DEFAULT    4 __bss_start
    22: 004001e8    88 FUNC    GLOBAL DEFAULT    3 main
    23: 004001b8    48 FUNC    GLOBAL DEFAULT    3 diff
    24: 00410240     0 NOTYPE  GLOBAL DEFAULT    4 _edata
    25: 004102b8     0 NOTYPE  GLOBAL DEFAULT    4 _end
    26: 00410240     0 NOTYPE  GLOBAL DEFAULT    4 _fbss
```

反汇编可执行文件

```
Disassembly of section .text:

004000b0 <expression1>:
  4000b0:   27bdffe0    addiu   sp,sp,-32
  4000b4:   afbf001c    sw  ra,28(sp)
  4000b8:   afbe0014    sw  s8,20(sp)
  4000bc:   afb00018    sw  s0,24(sp)
  4000c0:   03a0f025    move    s8,sp
  4000c4:   afc40020    sw  a0,32(s8)
  4000c8:   afc50024    sw  a1,36(s8)
  4000cc:   afc60028    sw  a2,40(s8)
  4000d0:   afc7002c    sw  a3,44(s8)
  4000d4:   3c020041    lui v0,0x41
  4000d8:   8c50027c    lw  s0,636(v0)
  4000dc:   8fc50024    lw  a1,36(s8)
  4000e0:   8fc40020    lw  a0,32(s8)
  4000e4:   e8000034    balc    4001b8 <diff>
  4000e8:   02028098    mul s0,s0,v0
  4000ec:   8fc5002c    lw  a1,44(s8)
  4000f0:   8fc40028    lw  a0,40(s8)
  4000f4:   e8000030    balc    4001b8 <diff>
  4000f8:   00402825    move    a1,v0
  4000fc:   02002025    move    a0,s0
  400100:   e8000006    balc    40011c <sum>
  400104:   03c0e825    move    sp,s8
  400108:   8fbf001c    lw  ra,28(sp)
  40010c:   8fbe0014    lw  s8,20(sp)
  400110:   8fb00018    lw  s0,24(sp)
  400114:   27bd0020    addiu   sp,sp,32
  400118:   d81f0000    jrc ra

0040011c <sum>:
  40011c:   27bdfff8    addiu   sp,sp,-8
  400120:   afbe0004    sw  s8,4(sp)
  400124:   03a0f025    move    s8,sp
  400128:   afc40008    sw  a0,8(s8)
  40012c:   afc5000c    sw  a1,12(s8)
  400130:   8fc30008    lw  v1,8(s8)
  400134:   8fc2000c    lw  v0,12(s8)
  400138:   00621021    addu    v0,v1,v0
  40013c:   03c0e825    move    sp,s8
  400140:   8fbe0004    lw  s8,4(sp)
  400144:   27bd0008    addiu   sp,sp,8
  400148:   d81f0000    jrc ra

0040014c <expression2>:
  40014c:   27bdffe0    addiu   sp,sp,-32
  400150:   afbf001c    sw  ra,28(sp)
  400154:   afbe0014    sw  s8,20(sp)
  400158:   afb00018    sw  s0,24(sp)
  40015c:   03a0f025    move    s8,sp
  400160:   afc40020    sw  a0,32(s8)
  400164:   afc50024    sw  a1,36(s8)
  400168:   afc60028    sw  a2,40(s8)
  40016c:   afc7002c    sw  a3,44(s8)
  400170:   3c020041    lui v0,0x41
  400174:   8c500240    lw  s0,576(v0)
  400178:   8fc50024    lw  a1,36(s8)
  40017c:   8fc40020    lw  a0,32(s8)
  400180:   ebffffe6    balc    40011c <sum>
  400184:   02028098    mul s0,s0,v0
  400188:   8fc5002c    lw  a1,44(s8)
  40018c:   8fc40028    lw  a0,40(s8)
  400190:   ebffffe2    balc    40011c <sum>
  400194:   00402825    move    a1,v0
  400198:   02002025    move    a0,s0
  40019c:   e8000006    balc    4001b8 <diff>
  4001a0:   03c0e825    move    sp,s8
  4001a4:   8fbf001c    lw  ra,28(sp)
  4001a8:   8fbe0014    lw  s8,20(sp)
  4001ac:   8fb00018    lw  s0,24(sp)
  4001b0:   27bd0020    addiu   sp,sp,32
  4001b4:   d81f0000    jrc ra
```

反汇编可执行文件

```
004001b8 <diff>:
  4001b8:   27bdfff8    addiu   sp,sp,-8
  4001bc:   afbe0004    sw  s8,4(sp)
  4001c0:   03a0f025    move    s8,sp
  4001c4:   afc40008    sw  a0,8(s8)
  4001c8:   afc5000c    sw  a1,12(s8)
  4001cc:   8fc30008    lw  v1,8(s8)
  4001d0:   8fc2000c    lw  v0,12(s8)
  4001d4:   00621023    subu    v0,v1,v0
  4001d8:   03c0e825    move    sp,s8
  4001dc:   8fbe0004    lw  s8,4(sp)
  4001e0:   27bd0008    addiu   sp,sp,8
  4001e4:   d81f0000    jrc ra
```

```
004001e8 <main>:
  4001e8:   27bdffd0    addiu   sp,sp,-48
  4001ec:   afbf002c    sw  ra,44(sp)
  4001f0:   afbe0028    sw  s8,40(sp)
  4001f4:   03a0f025    move    s8,sp
  4001f8:   8fc7001c    lw  a3,28(s8)
  4001fc:   8fc60018    lw  a2,24(s8)
  400200:   8fc50014    lw  a1,20(s8)
  400204:   8fc40010    lw  a0,16(s8)
  400208:   ebffffa9    balc    4000b0 <expression1>
  40020c:   afc20020    sw  v0,32(s8)
  400210:   8fc7001c    lw  a3,28(s8)
  400214:   8fc60018    lw  a2,24(s8)
  400218:   8fc50014    lw  a1,20(s8)
  40021c:   8fc40010    lw  a0,16(s8)
  400220:   ebffffca    balc    40014c <expression2>
  400224:   afc20024    sw  v0,36(s8)
  400228:   00001025    move    v0,zero
  40022c:   03c0e825    move    sp,s8
  400230:   8fbf002c    lw  ra,44(sp)
  400234:   8fbe0028    lw  s8,40(sp)
  400238:   27bd0030    addiu   sp,sp,48
  40023c:   d81f0000    jrc ra
```

装载

1）读取可执行文件头部，获取该程序的代码段以及数据段大小
2）在存储器中寻找可以匹配代码段和数据段大小的存储区域
3）将可执行文件中的代码段指令序列和数据写入存储器
4）将主程序的入口参数压入栈
5）初始化寄存器的值，并将$sp指向动态数据区顶端
6）运行启动过程将主程序的入口参数赋给参数寄存器，并调用该执行程序的主程序。

小结

- 了解程序由编写代码到执行需经历的过程
  - 编译程序功能
  - 汇编程序功能
  - 链接程序功能
  - 装载程序功能

下一讲： 汇编程序设计