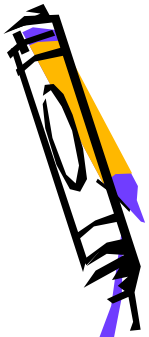
2013年度（平成25年度）版

Ver. 2013-10-07

情報工学科 情報実験第四 組み込みシステム
アセンブリコードのデバッグ方法

情報工学科　荒堀喜貴
arahori_at_cs.titech.ac.jp

アセンブリコードのデバッグ



- 目的
  - MIPSアセンブリコードの効果的なデバッグ
- 手法
  - MIPSアーキテクチャの計算機システムシミュレータSimMipsを用いた命令実行トレース
- 参考
  - SimMips: http://www.arch.cs.titech.ac.jp/SimMips/index.html

SimMipsを用いた命令実行トレース

- 例題: 001_dotプログラムの命令実行トレース
- 準備: サーバ計算機で001_dotプログラムの実行可能コードinitを生成:
  - $ cd ~/Emb/asm/001_dot/
  - $ make
- SimMipsコマンドでinitの命令実行をトレース:
  - $ SimMips -d3 -k36 -e40 init

*1. SimMipsコマンドでのデバッグではELF形式のデバッギinitを使用(init.binではないことに注意)
*2. -d3オプションで(レジスタ値表示付き)命令実行 トレースを指示
*3. -k[num]オプションで[num]サイクルまでの命令実行トレースをスキップ
*4. -e[num]オプションで[num]サイクルまでの命令実行トレースを表示

✓ デバッグ時には, 意図した命令が意図したレジスタ値で実行されているかを観測

```
main:
        .set    noreorder

        li      $3,0x900000     # $3 = vram address
        li      $2,7            # $2 = 7 (white)
        sb      $2,4288($3)     # vram[4288] = 7;
                                # (33 * 128 + 64) = 4288
$L1:
        j       $L1             # while(1);
        nop                     #

        .end    main
```

001_dotプログラムのソースコード(main.S)

```
-EE-:%%-F1  main.S          (Assembler)--L16--Bot--------
[arahori@sc440 001_dot]$ SimMips -d3 -k36 -e40 init
## SimMips: Simple Computer Simulator of MIPS Version 0.6.7
## debug mode 3: detailed instruction.
## 00000200: <main>
[         37] 00000200: lui     $v1, 0x90
                $v1<00900000
[         38] 00000204: addiu   $v0, $zr, 7
                $v0<00000007
[         39] 00000208: sb      $v0, 4288($v1)
                $v1>00900000 $v0>00000007
[         40] 0000020c: j       0000020c

## cycle count reaches the limit
```

第39サイクルでのsb 命令実行時のレジスタ$v0, $v1の値は0x7, 0x900000

001_dotプログラム(init)の命令実行トレース

SimMipsを用いた命令実行トレース(2)

- 例題: 001_dotプログラムの命令実行トレース

- SimMipsコマンドでデバッギの命令列実行後の全レジスタの内容をダンプ:
  - $ SimMips -d1 -e38 init

*1. -d1オプションで命令列実行後の全レジスタの内容をダンプ
*2. -e[num]オプションで[num]サイクルまでの命令列実行を指示

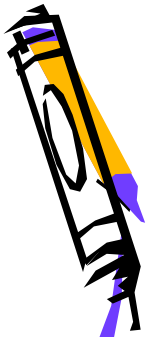
✓ デバッグ時には，意図した命令列実行後のレジスタ内容が意図したものになっているかを確認

```
[arahori@sc440 001_dot]$ SimMips -d1 -e38 init
## SimMips: Simple Computer Simulator of MIPS Version 0.6.7 2010-07-31
## debug mode 1: state.

## cycle count reaches the limit
## cycle count: 38
## inst count: 38
## simulation time:    0.000
## mips: 2.375
```

initの命令列を38サイクルまで実行した後の全レジスタの内容

```
$zr       $at       $v0       $v1       $a0       $a1       $a2       $a3

00000000  00000000  00000007  00900000  00000000  00000000  00000000  00000000

$t0       $t1       $t2       $t3       $t4       $t5       $t6       $t7

00000000  00000000  00000000  00000000  00000000  00000000  00000000  00000000

$s0       $s1       $s2       $s3       $s4       $s5       $s6       $s7

00000000  00000000  00000000  00000000  00000000  00000000  00000000  00000000

$t8       $t9       $k0       $k1       $gp       $sp       $fp       $ra

00000000  00000000  00000000  00000000  00000000  0007ff00  00000000  00000000

pc        hi        lo
00000208  00000000  00000000
```

SimMipsのその他の機能



- 実行した命令列のみを表示（レジスタ値の表示なし）
  - SimMipsを-d2オプションで実行
- 命令列実行後に命令ミックスを表示
  - SimMipsを-iオプションで実行
- より詳しい情報は以下を参照
  - http://www.arch.cs.titech.ac.jp/SimMips/index.html