Junhao Zhang "Freddie"
[redacted]

Assignment 1
Cpts 360 – MWF 2:10 to 3:00 pm

1. Problem 2.2 in Chapter 2 of TEXT

(A).

	text	data	bss	dec	hex	filename
(1)	1136	280	8	1424	590	a.out
(2)	1136	284	4	1424	590	a.out
(3)	1136	280	40032	41448	a1e8	a.out
(4)	1136	40304	4	41444	a1e4	a.out
(5)	1136	280	8	1424	590	a.out
(6)	1152	280	40068	41500	a21c	a.out

1. Variables in DATA: INITIALIZED globals (i.e: g = 3, g[10000] = {4}), STATIC locals
   Variables in BSS: UNINITIALIZED globals (i.e: g, g[10000]), STATIC locals

2. The "Text" and "Data" are in a.out but not "BSS" and I got it from the textbook. The "BSS" and stack and heap are initialized only during the run-time.

(B).

	text	data	bss	dec	hex	filename
(1)	654791	4096	5052	663939	a2183	a.out
(2)	654791	4096	5020	663907	a2163	a.out
(3)	654791	4096	45020	703907	abda3	a.out
(4)	654791	44128	5020	703939	abdc3	a.out
(5)	654791	4096	5052	663939	a2183	a.out
(6)	654791	4096	45084	703971	abde3	a.out

I saw that the sizes of Data section, Text and BSS section increased significantly.
The reason is the STATIC locals were saved in both the Data section and BSS section, and the reason why the size of Text increased is because those STATIC variables had been allocated statically already.

2. Problem 2.3 in Chapter 2 of TEXT

enter main
&argc=ffc8fee0 argv=ffc8ff74 env=ffc8ff88
&a=ffc8fec4 &b=ffc8fec8 &c=ffc8fecc
enter A
enter B
enter C
FP -> FFC8FE48 ->
FP -> FFC8FE78 ->
FP -> FFC8FEA8 ->
FP -> FFC8FED8 ->
FP -> 0

-6(FP) -> FFC8FE30
-6(FP) = 10

-5(FP) -> FFC8FE34
-5(FP) = 11

-4(FP) -> FFC8FE38
-4(FP) = 12

-3(FP) -> FFC8FE3C
-3(FP) = -3604920

-2(FP) -> FFC8FE40
-2(FP) = 0

-1(FP) -> FFC8FE44
-1(FP) = 0

0(FP) -> FFC8FE48
0(FP) = -3604872

1(FP) -> FFC8FE4C
1(FP) = 134514017

2(FP) -> FFC8FE50
2(FP) = 7

3(FP) -> FFC8FE54
3(FP) = 8

4(FP) -> FFC8FE58
4(FP) = 7

5(FP) -> FFC8FE5C
5(FP) = -145041664

6(FP) -> FFC8FE60
6(FP) = 134513196

7(FP) -> FFC8FE64
7(FP) = 7

8(FP) -> FFC8FE68
8(FP) = 8

9(FP) -> FFC8FE6C
9(FP) = 9

10(FP) -> FFC8FE70
10(FP) = 0

11(FP) -> FFC8FE74
11(FP) = 0

12(FP) -> FFC8FE78
12(FP) = -3604824

13(FP) -> FFC8FE7C
13(FP) = 134513946

14(FP) -> FFC8FE80
14(FP) = 4

15(FP) -> FFC8FE84
15(FP) = 5

16(FP) -> FFC8FE88
16(FP) = -3604776

17(FP) -> FFC8FE8C
17(FP) = -144724881

18(FP) -> FFC8FE90
18(FP) = -143304000

19(FP) -> FFC8FE94
19(FP) = 4

20(FP) -> FFC8FE98
20(FP) = 5

21(FP) -> FFC8FE9C

21(FP) = 6

22(FP) -> FFC8FEA0
22(FP) = -3604768

23(FP) -> FFC8FEA4
23(FP) = -143034056

24(FP) -> FFC8FEA8
24(FP) = -3604776

25(FP) -> FFC8FEAC
25(FP) = 134513875

26(FP) -> FFC8FEB0
26(FP) = 1

27(FP) -> FFC8FEB4
27(FP) = 2

28(FP) -> FFC8FEB8
28(FP) = -3604792

29(FP) -> FFC8FEBC
29(FP) = -3604788

30(FP) -> FFC8FEC0
30(FP) = -143305788

31(FP) -> FFC8FEC4
31(FP) = 1

32(FP) -> FFC8FEC8
32(FP) = 2

33(FP) -> FFC8FECC
33(FP) = 3

34(FP) -> FFC8FED0
34(FP) = 134514256

35(FP) -> FFC8FED4
35(FP) = 0

36(FP) -> FFC8FED8
36(FP) = 0

37(FP) -> FFC8FEDC
37(FP) = -144934301

38(FP) -> FFC8FEE0
38(FP) = 4

39(FP) -> FFC8FEE4
39(FP) = -3604620

40(FP) -> FFC8FEE8
40(FP) = -3604600

41(FP) -> FFC8FEEC
41(FP) = -143110934

42(FP) -> FFC8FEF0
42(FP) = 4

43(FP) -> FFC8FEF4
43(FP) = -3604620

44(FP) -> FFC8FEF8
44(FP) = -3604716

45(FP) -> FFC8FEFC
45(FP) = 134520856

46(FP) -> FFC8FF00
46(FP) = 134513196

47(FP) -> FFC8FF04
47(FP) = -143306752

48(FP) -> FFC8FF08
48(FP) = 0

49(FP) -> FFC8FF0C
49(FP) = 0

50(FP) -> FFC8FF10
50(FP) = 0

51(FP) -> FFC8FF14
51(FP) = 1749750549

52(FP) -> FFC8FF18
52(FP) = 1094883076

53(FP) -> FFC8FF1C
53(FP) = 0

54(FP) -> FFC8FF20
54(FP) = 0

55(FP) -> FFC8FF24
55(FP) = 0

56(FP) -> FFC8FF28
56(FP) = 4

57(FP) -> FFC8FF2C
57(FP) = 134513488

58(FP) -> FFC8FF30
58(FP) = 0

59(FP) -> FFC8FF34
59(FP) = -143088384

60(FP) -> FFC8FF38
60(FP) = -144934535

61(FP) -> FFC8FF3C
61(FP) = -143036416

62(FP) -> FFC8FF40
62(FP) = 4

63(FP) -> FFC8FF44
63(FP) = 134513488

64(FP) -> FFC8FF48
64(FP) = 0

65(FP) -> FFC8FF4C
65(FP) = 134513521

66(FP) -> FFC8FF50
66(FP) = 134513741

67(FP) -> FFC8FF54
67(FP) = 4

68(FP) -> FFC8FF58
68(FP) = -3604620

69(FP) -> FFC8FF5C
69(FP) = 134514256

70(FP) -> FFC8FF60

70(FP) = 134514368

71(FP) -> FFC8FF64
71(FP) = -143109760

72(FP) -> FFC8FF68
72(FP) = -3604628

73(FP) -> FFC8FF6C
73(FP) = 28

74(FP) -> FFC8FF70
74(FP) = 4

75(FP) -> FFC8FF74
75(FP) = -3602278

76(FP) -> FFC8FF78
76(FP) = -3602270

77(FP) -> FFC8FF7C
77(FP) = -3602266

78(FP) -> FFC8FF80
78(FP) = -3602262

79(FP) -> FFC8FF84
79(FP) = 0

80(FP) -> FFC8FF88
80(FP) = -3602256

81(FP) -> FFC8FF8C
81(FP) = -3602245

82(FP) -> FFC8FF90
82(FP) = -3602227

83(FP) -> FFC8FF94
83(FP) = -3602211

84(FP) -> FFC8FF98
84(FP) = -3602200

85(FP) -> FFC8FF9C
85(FP) = -3602169

86(FP) -> FFC8FFA0
86(FP) = -3602159

87(FP) -> FFC8FFA4
87(FP) = -3600846

88(FP) -> FFC8FFA8
88(FP) = -3600829

89(FP) -> FFC8FFAC
89(FP) = -3600815

90(FP) -> FFC8FFB0
90(FP) = -3600801

91(FP) -> FFC8FFB4
91(FP) = -3600781

92(FP) -> FFC8FFB8
92(FP) = -3600687

93(FP) -> FFC8FFBC
93(FP) = -3600662

94(FP) -> FFC8FFC0
94(FP) = -3600645

95(FP) -> FFC8FFC4
95(FP) = -3600637

96(FP) -> FFC8FFC8
96(FP) = -3600622

97(FP) -> FFC8FFCC
97(FP) = -3600601

98(FP) -> FFC8FFD0
98(FP) = -3600590

99(FP) -> FFC8FFD4
99(FP) = -3600575

100(FP) -> FFC8FFD8
100(FP) = -3600562

101(FP) -> FFC8FFDC
101(FP) = -3600530

102(FP) -> FFC8FFE0
102(FP) = -3600516

103(FP) -> FFC8FFE4
103(FP) = -3600505

104(FP) -> FFC8FFE8
104(FP) = -3600471

105(FP) -> FFC8FFEC
105(FP) = -3600446

106(FP) -> FFC8FFF0
106(FP) = -3600410

107(FP) -> FFC8FFF4
107(FP) = 0

108(FP) -> FFC8FFF8
108(FP) = 32

109(FP) -> FFC8FFFC
109(FP) = -143174624

110(FP) -> FFC90000
110(FP) = 33

111(FP) -> FFC90004
111(FP) = -143175680

112(FP) -> FFC90008
112(FP) = 16

113(FP) -> FFC9000C
113(FP) = -1075053569

114(FP) -> FFC90010
114(FP) = 6

115(FP) -> FFC90014
115(FP) = 4096

116(FP) -> FFC90018
116(FP) = 17

117(FP) -> FFC9001C
117(FP) = 100

118(FP) -> FFC90020
118(FP) = 3

119(FP) -> FFC90024

119(FP) = 134512692

120(FP) -> FFC90028
120(FP) = 4

121(FP) -> FFC9002C
121(FP) = 32

122(FP) -> FFC90030
122(FP) = 5

123(FP) -> FFC90034
123(FP) = 9

124(FP) -> FFC90038
124(FP) = 7

125(FP) -> FFC9003C
125(FP) = -143171584

126(FP) -> FFC90040
126(FP) = 8

127(FP) -> FFC90044
127(FP) = 0

exit B
exit A
exit main

argc at **38(FP)**
argv at **75(FP)**
env at **80(FP)**

Code:

```
#include <stdio.h>
#include <stdlib.h>

int *FP;

main(int argc, char *argv[ ], char *env[ ])
{
  int a,b,c;
  printf("enter main\n");

  printf("&argc=%x argv=%x env=%x\n", &argc, argv, env);
  printf("&a=%8x &b=%8x &c=%8x\n", &a, &b, &c);

  a=1; b=2; c=3;
  A(a,b);

  printf("exit main\n");
}

int A(int x, int y)
{
  int d,e,f;
  printf("enter A\n");
  // printf("&d=%8x &e=%8x &f=%8x\n", &d, &e, &f);
  d=4; e=5; f=6;
  B(d,e);
  printf("exit A\n");
}

int B(int x, int y)
{
  int g,h,i;
  printf("enter B\n");
  // printf("&g=%8x &h=%8x &i=%8x\n", &g, &h, &i);
  g=7; h=8; i=9;
  C(g,h);
  printf("exit B\n");
}

int C(int x, int y)
{
  int u, v, w, i, *p;

  printf("enter C\n");
  // printf("&u=%8x &v=%8x &w=%8x\n", &u, &v, &w);
  u=10; v=11; w=12;
```

```
  asm("movl %ebp, FP");

  int *tmp = FP;

  while(FP != 0)
  {
    printf("FP -> %8X ->\n", FP);
    FP = *FP;
  }
  printf("FP -> %8X\n\n\n", FP);

  i = -6;
  p = tmp + i;
  while(i < 128)
  {
      printf("%d(FP) -> %8X\n%d(FP) = %d        ", i, p, i, *p);

/*aslkkdmlkasmdkasmdlkmasdlkmakslmd

*/

      printf("\n\n");
      i++;
      p++;
  }
}
```