**作业F** 等级：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

学号：\_\_1929409021\_\_\_\_\_ 姓名:\_\_\_\_\_胡志彬\_\_\_\_\_

[F1]基于VC2010环境，在目标代码中，主程序常常利用\_寄存器\_\_\_和\_\_\_堆栈3\_\_向子程序传递入口参数；子程序利用\_\_寄存器\_\_\_\_传递出口参数。

[F2]基于VC2010环境，在目标代码中，把动态局部变量安排在\_堆栈\_\_\_和\_\_\_\_寄存器\_中。

[F3]目前为止，涉及到堆栈操作的指令有\_\_PUSH\_\_、\_\_POP\_\_、\_CALL\_\_\_、\_\_RET\_、\_\_\_ENTER\_\_、\_\_LEAVE、MOV\_\_和\_ADD\_等。

**[S1]以下关于堆栈用途的叙述，正确的是（多选）？ ABCDF**

（A）堆栈可以用于保存返回地址。

（B）堆栈可以用于传递调用参数。

（C）堆栈可以用于安排局部变量。

（D）堆栈可以用于保护重要现场。

（E）堆栈可以用于安排全局变量。

（F）堆栈可以用于传递返回参数。

**[S2]以下关于调整堆栈指针的叙述，错误的是？ B**

（A）必要时，可以利用MOV指令调整堆栈指针。

（B）必要时，可以利用CALL指令或RET指令调整堆栈指针。

（C）必要时，可以利用ADD指令或SUB指令调整堆栈指针。

（D）必要时，可以利用PUSH指令或POP指令调整堆栈指针。

**[S3]以下关于堆栈的叙述，错误的是？ C**

（A）堆栈必须保持平衡。

（B）堆栈有多种用途。

（C）堆栈的使用和其他内存区域的使用并没有本质区别。

（D）在通过涉及堆栈操作的指令存取堆栈时，遵循先进后出的规则。

**[S4]以下关于调用和调用指令的叙述，正确的是（多选）？ ABC**

（A）调用指令是调用子程序的指令。

（B）可以利用条件转移指令调用子程序。

（C）可以利用无条件转移指令调用子程序。

（D）可以利用返回指令调用子程序。

**[S5]以下关于返回和返回指令的叙述，正确的是（多选）？ ABC**

（A）返回指令是从子程序返回的指令。

（B）可以利用条件转移指令返回主程序。

（C）可以利用无条件转移指令返回主程序。

（D）可以利用传送指令返回主程序。

**[S6]以下关于参数传递的叙述，错误的是（多选）？ BC**

（A）可以利用通用寄存器传递入口参数和出口参数。

（B）不可以利用状态标志传递入口参数和出口参数。

（C）利用堆栈，只可以传递入口参数，不可以传递出口参数。

（D）利用约定内存单元，也可以传递参数。

**[S7]以下关于调用和返回的叙述，错误的是（多选）？**

（A）通常情况下，调用指令和返回指令应当配对使用。

（B）特殊情况下，调用指令和返回指令可不配对使用。

（C）调用和返回必须遵循约定。

（D）调用和返回无需遵循约定。

[R1]设有如下C函数，其功能是计算等差数列之和：

unsigned sum(unsigned a1, unsigned n, unsigned d)

{ unsigned sum;

sum = a1\*n;

sum += n\*(n-1)/2\*d;

return sum;

}

在VC2010环境中，禁止编译优化情形下，可得到如下的目标代码。请说明指定汇编格式指令的作用（可以利用高级语言语句或表达式来描述）。

push ebp

mov ebp, esp ; 保存调用者的栈帧基址，建立当前函数的栈帧(1)

push ecx ; 为局部变量sum预留栈空间(2)

mov eax, DWORD PTR [ebp+8]

imul eax, DWORD PTR [ebp+12] ;\_ 计算a1\*n的结果\_\_\_\_\_\_(3)

mov DWORD PTR [ebp-4], eax

mov ecx, DWORD PTR [ebp+12]

sub ecx, 1 ;\_\_ 计算n-1\_\_\_\_\_\_\_\_\_(4)

imul ecx, DWORD PTR [ebp+12]

shr ecx, 1 ;\_\_ 计算n\*(n-1)/2\_\_\_(5)

imul ecx, DWORD PTR [ebp+16]

add ecx, DWORD PTR [ebp-4]

mov DWORD PTR [ebp-4], ecx

mov eax, DWORD PTR [ebp-4]

mov esp, ebp

pop ebp

ret ;\_ 从子程序返回\_\_\_(6)

[Q1]请简要说明C语言中未初始化动态局部变量的初值是随机值的原因。

动态局部变量存储在堆栈中，其初值是之前堆栈位置残留的数据，未被显式初始化时保留原内存内容，因此表现为随机值。

[Q2]如何利用段内无条件转移指令JMP调用子程序？请举例说明。

1. main:
2. push return\_address  ; 手动保存返回地址
3. jmp subroutine      ; 跳转到子程序
4. return\_address:
5. ...
6. subroutine:
7. ...                 ; 子程序代码
8. pop eax             ; 弹出返回地址
9. jmp eax             ; 跳转回主程序