hw1

T1

```
.file "foo.c"                // 源文件名
.text                        // 代码段开始
.globl fact                  // 声明 fact 是一个全局函数
.type fact, @function        // 标明 fact 是一个函数

fact:
    pushl %ebp               // 保存旧的栈底指针
    movl %esp, %ebp          // 设置新的栈底指针
    subl $4, %esp            // 分配 4 字节的局部栈空间

    cmpl $0, 8(%ebp)         // 比较参数 n 是否小于等于 0
    jg .L2                    // 如果大于 0，跳转到 .L2 标签，否则继续执行下一条指令

    movl $1, -4(%ebp)         // 如果 n <= 0，将 1 存储到局部变量中
    jmp .L1                   // 跳转到 .L1 标签

.L2:
    subl $12, %esp            // 分配 12 字节的局部栈空间
    movl 8(%ebp), %eax        // 将参数 n 复制到寄存器 %eax
    decl %eax                 // 将 %eax 中的值减一
    pushl %eax                // 将 %eax 中的值入栈
    call fact                 // 调用 fact 函数
    addl $16, %esp            // 释放栈空间，恢复栈指针
    imull 8(%ebp), %eax       // 将 %eax 中的值与参数 n 相乘，结果存储在 %eax 中
    movl %eax, -4(%ebp)       // 将 %eax 中的值存储到局部变量中

.L1:
    movl -4(%ebp), %eax       // 将局部变量的值复制到 %eax 中
    leave                     // 恢复栈帧并弹出栈底指针
    ret                       // 返回函数

.Lfe1:
    .size fact, .Lfe1-fact     // 函数 fact 的大小
.ident "GCC: (GNU) 3.2.2 20030222 (Red Hat Linux 3.2.2-5)" // 编译器信息
```

联系与解释：

1. 参数 `n` 在汇编中是通过 `%ebp` 偏移量来表示的，即 `8(%ebp)` 是参数 `n` 的位置。
2. `if (n <= 0)` 对应了汇编中的条件分支指令 `cmpl $0, 8(%ebp)` 和条件跳转指令 `jg .L2`。
3. 局部变量的值在汇编中是通过 `4(%ebp)` 来表示的，这个位置用于存储递归计算结果和临时变量。

4. 递归调用的部分在汇编中使用 `call` 指令来实现，递归参数的准备和结果的处理都是通过栈来完成的。
5. `leave` 指令用于清理当前函数的栈帧，然后 `ret` 指令用于返回函数。

homework1 20231915

[1] 见前页.

[2] (1) int(*(*(*p(int x))())[20])(int *y).

p是一个指向函数的指针，该函数接受一个整形参数x，返回一个指向函数指针的指针，函数指针指向的函数接收一个整型指针参数y，返回一个含有20个整型元素的数组的函数.

(2) 见附图.

CS 扫描全能王

```
PS C:\Users\Miner>  & 'c:\Users\Miner\.vscode\extensions\ms-vscode.cpptools-1.17.5
' '--stdin=Microsoft-MIEngine-In-4zmff4u4.plc' '--stdout=Microsoft-MIEngine-Out-uc
m2.jir' '--pid=Microsoft-MIEngine-Pid-x0z0ddlk.dbu' '--dbgExe=D:\settings\mingw64\
iii = 1000 @: 0x61fe0c
ii = 1000 @: 0x61fe0c
pii points to: 0x61fe0c with value = 1000 @: 0x61fe00
pr points to: 0x61fe0c with value = 1000 @: 0x61fe00
PS C:\Users\Miner>
```