## 动带参数列表实验报告

**Mysum函数的实现：**

若caller function调用mysum时，传递的参数符合要求，即第一个参数n为加数的个数，接下来n个参数为加数，则当程序执行至mysum时，依据C语言的calling convention可知，栈中$ebp+0x8的值为n，$ebp+0xC、$bep+0x10…$ebp+(0x8+n\*4)分别为第一个加数、第二个加数、…、第n个加数。将它们依次相加即得到和，将之返回。

**问题：**

1. float版本的mysum如何实现？
2. 如何进行mysum函数的非法调用判断？

**思考与搁浅：**

1. 本人试图实现float版本的思路是简单粗暴地把适当的位置的int变量类型改为float变量类型，思考和试验后发现这种实现是错误的。因为在逐个提取加数的过程中，提取的方式为以第一个参数（加数个数n）的地址为基准，用语句\*(++&n)提取n个加数。由于n为int型，所以++的过程会4字节的提取，然而当加数为float型时，其大小为8个字节，因此提取发生错误。

因而，可能试图在float版本的mysum中8字节的提取，但出现了bug。还未处理完毕。

1. 当nr\_num为4，后续加数的个数不等于4时，如何返回调用错误的信息？思路应该是在栈中找到调用参数的个数，将之与nr\_num进行比对，然而有办法获取参数个数的信息吗？似乎是没有。Stack overflow中相关问题有人明确回答不可以。实现方式应该是caller和callee约定一套规则，比如调用参数的最后一个参数必为0，以此计算参数的个数。