实验报告

焦一帆 524031910224

1.如何测试的

0）阅读代码，看看代码的整体思路

1）打断点，用gdb看内存

2）编译的时候启用asan，看asan的报错信息

2. 发现的bug类别

1. segement fault : s->x 未初始化
2. heap buffer overflow： 分配的空间在进行matmul的时候不够用
3. use after free： 多余的delete s
4. memory leak： 析构函数未完成

3.如何发现的

1. 第一遍运行到`forward`里的embedding的时候报错segement fault，设置断点看到s->x的值很小，像是野指针，检查构造函数发现没有初始化
2. 后续运行在`transformer`中`matmul`遇到问题，asan输出的信息是 *WRITE of size 4 at 0x50200010ecf0 thread T0*；检查key_cache和value_cache，发现分配的空间应该是`cache-elements`
3. 继续运行到`ffn`时，asan报错use after free，检查代码发现`attention`中有多余的delete s
4. 运行完整个模型发现没有释放内存，析构函数没有完成

4. 如何修复的

1. 在构造函数中初始化s->x
2. 修改key_cache和value_cache的分配空间为`cache-elements`
3. 删除多余的delete s
4. 完成析构函数，释放内存