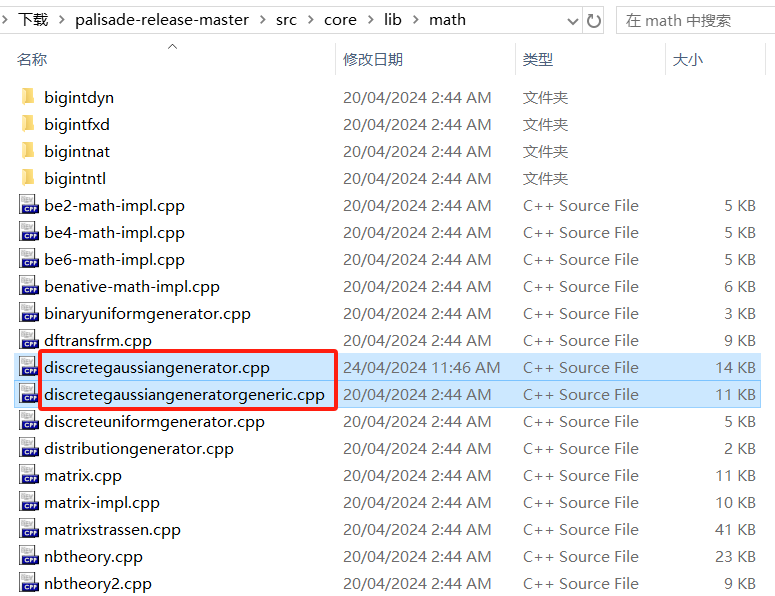
从PALISADE(一个格密码库)中下载了采样器的源码，其采样方法有：

拒绝采样法、Karney、Knuth-Yao、Peikert’s Inversion Method、**Generic Constant Time Sampling**

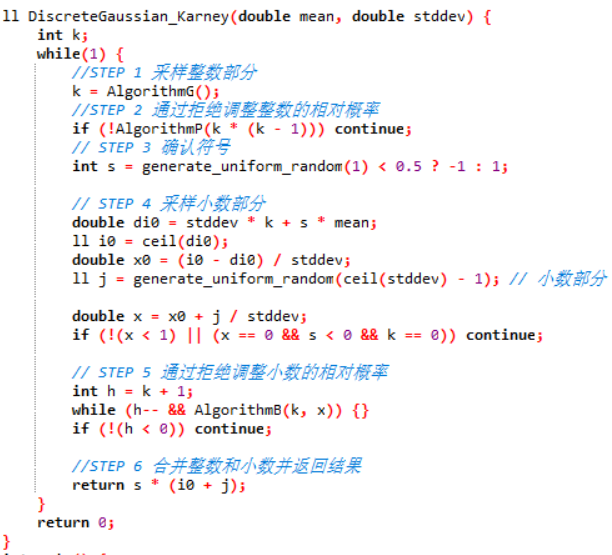
**PALISADE项目地址：**<https://gitlab.com/palisade/palisade-release>

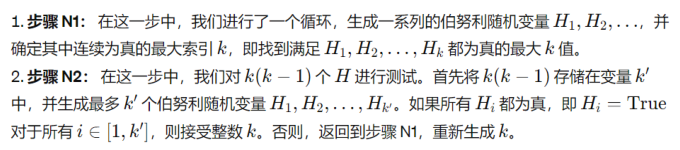
**其采样代码主要在下图中两个cpp文件中：**



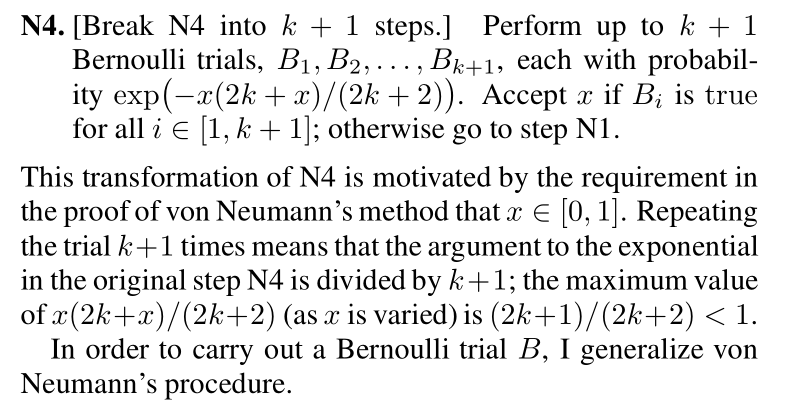
**我对它的Karney部分进行了修改**

**代码实现步骤与上节讨论中发的文档基本一致**









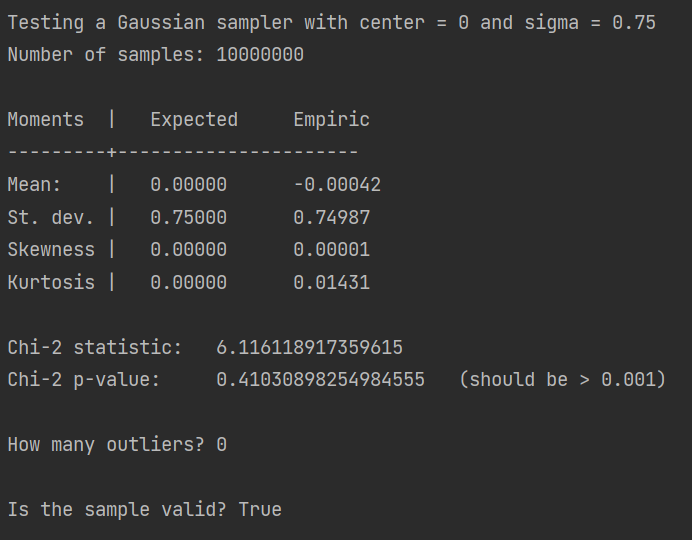
测试：

使用saga进行了测试

① 准确性：

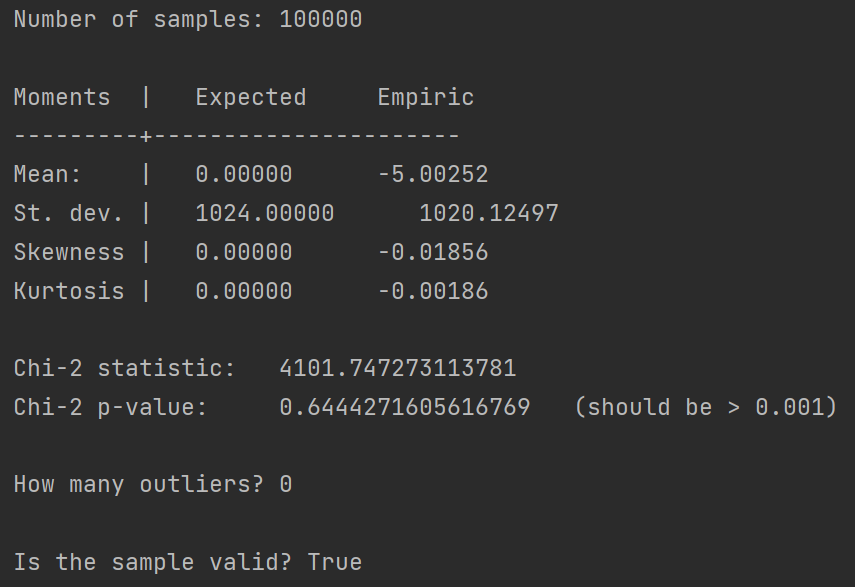
(1)

可以稳定通过数据规模为1e7的检验，生成1e7的数据大概需要7s。

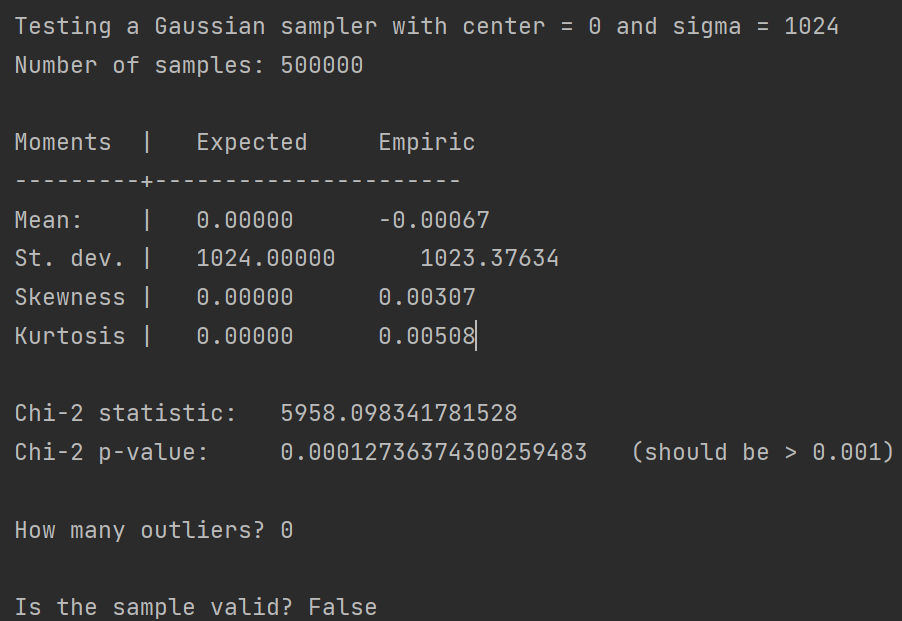


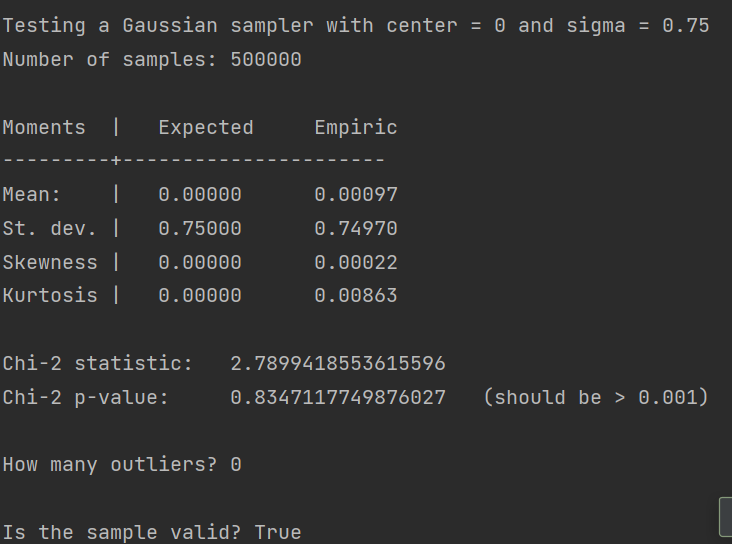
(2)

数据规模1e5可以稳定通过



5e5可能失败(寻找原因ing





② 时间：

|  |  |  |
| --- | --- | --- |
| 数据规模 | = 0.75 | = 1024 |
| 1e6 | 633ms | 500ms |

尚未完成：

生成均匀分布的随机数，我使用了c库里的rand()。之后还要完善一下这部分的代码。