第九届（2024）全国高校密码数学挑战赛

赛题二

一、赛题名称：整数高斯采样算法

二、赛题描述

2.1 符号说明

记Z为整数集. 对于正实数σ, 记$\rho_\sigma(x) = exp(-\frac{x^2}{2\sigma^2})$表示一维高斯函数. 记$\rho_\sigma(Z-c) = \sum_{i\in Z}\rho_\sigma(i-c)$，其中$c$为实数.

2.2 基础知识

整数高斯分布是正态分布在整数集Z上的离散化，由标准差和中心两个参数确定。标准差为σ、中心为c的整数高斯分布，记作$D_{Z,\sigma,c}$，定义如下：$\forall i \in Z$，

$$D_{Z,\sigma,c}(i) = \frac{\rho_\sigma(i-c)}{\rho_\sigma(Z-c)}.$$

整数高斯分布在格密码中有重要应用，许多格密码算法需要生成服从高斯分布的整数（这一过程称为整数高斯采样），高斯采样的性能直接决定格密码整体性能，采样的准确性则会影响格密码安全性。对于不同的格密码算法，高斯采样的参数会有明显差异，因此需要使用最合适的算法完成采样。

2.3 问题描述

对于以下四种情形，设计并实现$D_{Z,\sigma,c}$的采样算法：

（1） 标准差$\sigma = 0.75$，中心$c = 0$；

（2） 标准差$\sigma = 1024$，中心$c = 0$；

（3） 标准差$\sigma = 1.5$，中心c在区间$[0,1)$均匀分布；

（4） 标准差σ在区间$(0.8, 1.6)$均匀分布，中心c在区间$[0,1)$均匀分布。

针对上述每一类情形分别提交高斯采样算法文档以及相应的 C 实现，测试将在普通 CPU 上完成。要求：

1. 算法实现不能调用现有 C 函数库，包括数学库 math。

2. 算法文档包含采样算法以及相关数值的完整描述，与提交代码一致。
3. 四类情形对应的采样算法的 API 已经在附件一文件夹中的文件/Integer_Gaussian_sampler/sampler.h 定义好，请在此基础上完成采样程序，请勿随意更改 API。

2.4 成绩评判标准

高斯采样算法评分考虑下列三方面因素。

（1） 准确度。要求提交的高斯采样算法能通过 p 值>0.001 的卡方正态性检验（chi-square normality test），否则视为无效提交。具体检测套件程序可参考 SAGA（https://github.com/PQShield/SAGA）。在附件一文件夹中的/Normality_test/已经提供了可用的 SAGA 程序，此项套件程序需要满足 python 版本至少 3.4+，需要安装的包可以通过”pip3 install requirements.txt”来进行安装。

（2） 时间。计算高斯采样算法 1 秒内成功采样的次数，次数越多，排名越高，

$$单项得分 = 1 - \frac{单项排名 - 1}{有效提交数}.$$

采样算法可以支持“在线/离线”模式，但离线计算时间也纳入总时间。

（3） 内存。计算高斯采样过程中所需的 RAM 大小，使用 RAM 越少，排名越高，

$$单项得分 = 1 - \frac{单项排名 - 1}{有效提交数}.$$

关于使用 RAM 的检测，在实现采样 C 程序过程中，有如下建议：

- 尽量避免使用递归函数
- 尽量避免使用动态分配（malloc 或者 alloca 等内存分配函数，或者变长数组）
- 尽量避免使用内联函数
- 尽量避免使用一些栈优化措施，例如尾调用优化等

对于每一类情形分别进行评分，四类情形对应的满分依次为：15/25/25/35，

$$每类情形得分 = 满分 \times (时间 \times 0.6 + 内存 \times 0.4),$$

四类情形得分相加即为总得分。

三、密码学背景及相关问题的研究进展

高斯采样是格密码的核心算法，广泛应用于基于格陷门的密码算法中，如：签名、身份基加密、属性基加密等。高维格高斯采样往往需要转化为整数高斯采样，因此整数高斯采样准确度和效率会直接影响格密码算法的安全性和性能。整数高斯采样的研究涉及概率统计、数值计算、级数理论等数学知识，同时采样算法的实现与优化需要扎实的编程能力，因此该问题可以考察学生的综合能力。目前，整数高斯采样已有较为丰富的研究成果，常见的采样算法包括：查表法、拒绝采样法、Karney 采样法、Knuth-Yao 方法等，各类算法适用于不同高斯分布参数。如何针对不同参数设计最合适的采样算法是一个有价值的研究课题，本问题列举了四类有代表性的高斯采样情形，希望学生通过解决问题对格密码核心算法有较好理解。

四、参考文献

[1] Daniele Micciancio and Michael Walter. "Gaussian sampling over the integers: Efficient, generic, constant-time." CRYPTO 2017.

[2] Thomas Prest. "Sharper bounds in lattice-based cryptography using the Rényi divergence." ASIACRYPT 2017.

[3] James Howe, Thomas Prest, Thomas Ricosset, and Mélissa Rossi. "Isochronous Gaussian Sampling: From Inception to Implementation. " PQCRYPTO 2020.