author：Amuro Toru
data：2025-06-23

SIS解空间的构造

在Yingfei老师的讲义中，我对SIS lattice的构造产生了疑问，我查询了一些资料，理解了SIS lattice构造原理：

定义SIS：

令n，m，q为正整数，

$\geq n, A \in \mathbb{Z}_q{}^{m\times n}$为$\mathbb{Z}_q$上的一个服从均匀分布的随机均匀矩阵，$\beta \in \mathbb{R}, 0 < \beta < q$

SIS 问题是寻找满足如下条件的最短整数解 $z \in \mathbb{Z}^m$：

$$Az = 0 mod q 且 z \neq 0, |z| \leq \beta$$

SIS lattice 构造

SIS lattice是所有解向量z组成的空间：

$$B = \begin{pmatrix} q \cdot I_n & -A_1^{-1}A_2 \\ \vec{0} & I_{m-n} \end{pmatrix} \in \mathbb{Z}^{m\times m}$$

其中$A = [A_1 \quad A_2]$，A_1是一个$n \times n$的在$mod q$下可逆的矩阵,

$$AB = [A_1 \quad A_2] \begin{pmatrix} q \cdot I_n & -A_1^{-1}A_2 \\ \vec{0} & I_{m-n} \end{pmatrix}$$
$$= \begin{pmatrix} q \cdot A_1 & A_1(-A_1^{-1}A_2) + A_2 \end{pmatrix} = \mathbf{0} mod q$$

BKZ算法

LLL算法

LLL算法本质上是基于施密特正交基的求解方法，求得一组近似正交基 $(\beta_1, beta_2, \ldots, \beta_n)$ 满足以下条件:

1.对于每个 $i < j$, 我们有$|\mu_{i,j}| < \frac{1}{2}$

2.对于每个$\leq i \leq n$, 我们有$\sigma|\beta_i{}^*|^2 \leq |\mu_{i,i+1}\beta_i{}^* + \beta_{i+1}{}^*|^2$,其中$\beta_i{}^*$是每个向量对应的施密特正交化的向量

第一个条件说的是基中的向量要近似正交，第二个条件是说两个向量长度不能相差太大

Enumeration

我们通过枚举寻找最短向量，具体过程如下：
1.找到LLL减约后的最短向量β_1, β_2,使用施密特正交化得到$\beta_1{}^*, \beta_2{}^*$
2.取一个以$\beta_1{}^*$为半径的在由$\beta_1{}^*, \beta_2{}^*$构成的平面的球，将n维格投影到这个平面，利用$\beta_1{}^*, \beta_2{}^*$找到球内所有的投影的格点，枚举这些格点找到对应的三维子空间（由$\beta_1{}^*, \beta_2{}^*\beta_3^*$构成的）最短向量

3.以此类推，从i维空间到i+1维。
4.在此过程中，使用剪枝算法排除一些不可能是最短向量的分支

BKZ算法

bkz算法将格分为较小的block，在每个较小的block中求解SVP问题，然后利用求解结果跟新整个格基：
1.分块
将格基B分为大小为β的连续分块，如$B_{[i,i+\beta-1]}$，共分为$n-\beta+1$个block
2.局部枚举
在每个block内。使用enumeration算法寻找最短非零向量，如果最短向量不是该块的第一个向量，将其增加到该块的第一行
3.LLL
将找到的最短非零向量插入格基中，使用LLL算法重新减约，用以消除添加的心得向量带来的线性相关
4.迭代上述过程，直至基不再显著变化