4 格

4.1 格的定义

设**R**是实数集，R^m是**m**维欧式空间，在R^m上定义了内积$<x,y>=x^Ty$，以及向量长度$\|x\|=\sqrt{x^Tx}$.

格：设$b_1,b_2,\cdots b_n$是R^m中的n个线性无关的向量$(m\leq n)$，**Z**为整数集，称$L(b_1,b_2,\cdots b_n)=\{\sum\limits_{i=1}^{n}x_ib_i:x_i\in Z\}$称为$R^m$中的一个格***(lattice)***，简记为**L**，并称$b_1,b_2,\cdots b_n$为格**L**的一组基，m为格**L**的维数，n为格**L**的秩.当$m=n$时，称格**L**是满秩的.

格的矩阵形式：格**L**的基也常写为矩阵的形式，即以$b_1,b_2,\cdots b_n$为列向量构成的矩阵$B=[b_1,b_2,\cdots b_n]\in Z^{m\times n}$，此时格**L**可以写作$L(B)=\{Bx:x\in Z^n\}$，定义格的行列式$det(L)=\sqrt{B^TB}$，与格基的选择无关，当格式满秩的时候格的行列式为矩阵**B**的行列式的绝对值即$det(L)=|det(B)|$.

Gram-Schmidt正交化：与线性代数类似，可以对R^m中的格**L**的一组基(一组线性无关的向量)$b_1,b_2,\cdots b_n$进行**Gram-Schmidt**正交化，规定$b_1^*=b_1,b_i^*=b_i-\sum\limits_{i=1}^{i-1}\mu_{i,j}b_j^*,i>1$,其中$\mu_{i,j}=\frac{<b_i,b_j^*>}{<b_j^*,b_j^*>},1\leq j<i\leq n$，得到$R^m$中的一组正交向量$b_1^*,b_2^*,\cdots b_n^*$，注意这里$b_1^*,b_2^*,\cdots b_n^*$通常不是格**L**的基.格**L**的行列式满足$det(L)=\prod\limits_{i=1}^{n}b_i^*,det(L)\leq\prod\limits_{i=1}^{n}b_i$.

格上的最短向量问题：格上的最短向量问题是指格中一个最短的非零向量的问题(**shortest vector problem,SVP**)，这一问题已被证明在随机约化下是**NP-**困难问题，我们首先考虑在一个给定的特殊区域里是否存在某个事先给定的格的非零向量问题.

Minkowski定理：设**L**是R^m中的格，**S**是R^m中的一个可测的关于原点对称的凸集$(\alpha\beta\in S\Rightarrow\alpha+\beta/2)\in S$，若**S**的体积$\mu(S)\geq 2^nfdet(L)$，则$S\cap L$中有非零向量.（这个结论来自代数数论，在此处证明略去）

格的最短向量长度的上界：设**L**是R^m中秩为n的格,设格**L**中的最短向量的长度为λ_1，那么$\lambda_1\leq\sqrt{n}det(L)^{\frac{1}{n}}$(在$span(b_1,b_2$取区域**S**为以原点为中心$\sqrt{n}det(L)^{\frac{1}{n}}$为半径的开球中，其中包含一个$n$维的边长为$2det(L)^{\frac{1}{n}}$的超立方体，体积满足**Minkowski**定理的条件，故在内部存在向量$v\in S\cap L$使得$\rfloor v\rfloor\leq\sqrt{n}det(L)^{\frac{1}{n}}$)

4.2 格基约化算法(LLL算法)

上一节中介绍了格中最短向量长度的一个上界，但没有构造出具体的短向量，本节我们介绍约化基的概念和用格基约化算法找出格中的短向量，为了叙述方便，本节中格**L**均指维数为n的满秩格.