网络空间安全数学基础（7）

网络空间安全学院

高莹

2020年 11 月 11日

本次课程内容目录

格

定义

设$v_1, v_2, .., v_n \in \mathbb{R}^m$是一组线性无关的向量。则由它们生成的格L是指系数为整数的$v_1, v_2, .., v_n$的线性组合

$$L = \{a_1 v_1 + a_2 v_2 + ...a_n v_n : a_1, a_2, ..., a_n \in \mathbb{Z}\}$$

L的基是能生成L的任意线性无关的向量集。任意两个这样的集合有相同数量的元素。L的维数是指L的基的向量个数。

格的张量空间

格的张量空间

设L是一个维数为n的格，$v_1, v_2, .., v_n$是L的一组基，称

$$\text{span}(L) = \{a_1v_1 + a_2v_2 + \cdots a_nv_n : a_1, a_2, \cdots, a_n \in \mathbb{R}\}$$

为格的张量空间。

显然，格L是其张量空间span(L)的子集合，span(L)是$\mathbb{R}^m$的n维子空间。

格的性质（1）

性质

格L的任意两组基可以被一个矩阵所关联，这个矩阵系数为整数且行列式为± 1

为了计算需求，通常来说向量分量都为整数的格很方便进行讨论，例如

$$\mathbb{Z}^n = \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in \mathbb{Z}\}$$

这个格中所有的向量都具有整数分量

定义.

一个整格(integral lattice)是指其中所有向量分量都为整数的格。等价地，一个整格实际上是$\mathbb{Z}^m$的加法子群对某个$m \geq 1$，

格的例子

示例

考虑一个维数为3的格$L \subset \mathbb{R}^3$由如下三个向量生成

$$v_1 = (2, 1, 3),\ v_2 = (1, 2, 0),\ v_3 = (2, -3, -5)$$

然后将它们作为行向量构造矩阵

$$A = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & -3 & 5 \end{bmatrix}$$

我们给出3个新的L中的向量

$$w_1 = v_1 + v_3,\ w_2 = v_1 - v_2 + 2v_3,\ w_3 = v_1 + 2v_2$$

格的例子

这实际等价于对矩阵A左乘一个矩阵

$$U = \begin{bmatrix} 1 & 0 & 1 \\ 1 & -1 & 2 \\ 1 & 2 & 0 \end{bmatrix}$$

同样按行向量构造矩阵

$$B = UA = \begin{bmatrix} 4 & -2 & -2 \\ 5 & -7 & -7 \\ 4 & 5 & 3 \end{bmatrix}$$

矩阵U的行列式为-1。所以w_1, w_2, w_3是L的基。U的逆为

$$U^{-1} = \begin{bmatrix} 4 & -2 & -1 \\ -2 & 1 & 1 \\ -3 & 2 & 1 \end{bmatrix}$$

格的例子

$$U^{-1} = \begin{bmatrix} 4 & -2 & -1 \\ -2 & 1 & 1 \\ -3 & 2 & 1 \end{bmatrix}$$

U^{-1}的行说明了我们如何用w_j的线性组合表示出v_i

$$v_1 = 4w_1 - 2w_2 - w_3,\ v_2 = -2w_1 + w_2 + w_3,\ v_3 = -3w_1 + 2w_2 + w_3$$

格的注记

注释

设$L \subset \mathbb{R}^m$是维数为n的格，然后L的一个基可以写成$n \times m$的矩阵A。要获得一个新的L的基可以对A左乘一个$n \times n$的矩阵U，U满足其中项为整数且行列式为± 1。满足这种条件的U的集合我们称为一般线性群（$\mathbb{Z}$上的）并且记为$GL_n(\mathbb{Z})$。这一类矩阵项都为整数，而且矩阵的逆的项也为整数。

格的基础区域

一个格和向量空间很类似，只不过格是通过基的整数系数的线性组合生成。通常将一个格看成先在$\mathbb{R}^m$中有序安排一些点，每个向量的尾端指向这些点的看法很有帮助。

定义.

设L是一个维数为n的格，$v_1, v_2, .., v_n$是L的一组基，L的关于这组基的基础区域（fundamental domain (or fundamental parallelepiped)）是指集合

$$\mathcal{F}(L) = \mathcal{F}(v_1, v_2, .., v_n) = \{t_1 v_1 + t_2 v_2 + ... + t_n v_n : 0 \leq t_i < 1\}$$

格的基本域

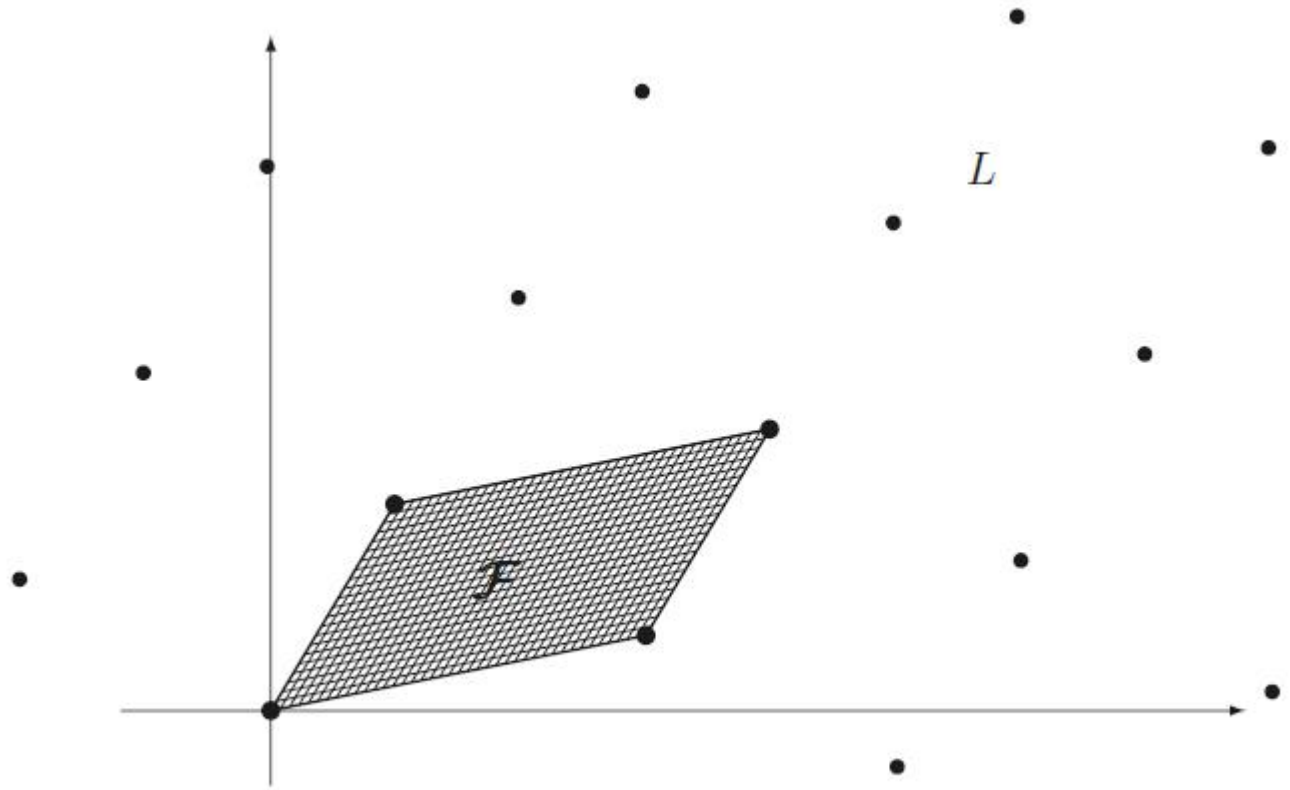

Figure 7.1: A lattice L and a fundamental domain $\mathcal{F}$

格的性质（2）

性质

设$L \subset \mathbb{R}^m$是维数为n的格。$\mathcal{F}$是L的基础区域。那么每一个向量$w \in \mathbb{R}^m$可以写为如下形式

$$w = t + v$$

其中$t \in \mathcal{F}(L), v \in L$是唯一的
等价地，随着v遍历格L内的向量，集合

$$\mathcal{F}(L) + v = \{t + v : t \in \mathcal{F}\}$$

将会遍历整个$\mathbb{R}^n$。

格的性质（2）

Proof. Let $v_1, \ldots, v_n$ be a basis of L that gives the fundamental domain $\mathcal{F}$. Then $v_1, \ldots, v_n$ are linearly independent in $\mathbb{R}^n$, so they are a basis of $\mathbb{R}^n$. This means that any $w \in \mathbb{R}^n$ can be written in the form

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \qquad \text{for some } \alpha_1, \ldots, \alpha_n \in \mathbb{R}.$$

We now write each α_i as

$$\alpha_i = t_i + a_i \qquad \text{with } 0 \le t_i < 1 \text{ and } a_i \in \mathbb{Z}.$$

Then

$$w = \overbrace{t_1 v_1 + t_2 v_2 + \cdots + t_n v_n}^{\text{this is a vector } \boldsymbol{t} \in \mathcal{F}} + \overbrace{a_1 v_1 + a_2 v_2 + \cdots + a_n v_n}^{\text{this is a vector } \boldsymbol{v} \in L}.$$

This shows that w can be written in the desired form.

格的性质（2）

Next suppose that $\boldsymbol{w} = \boldsymbol{t} + \boldsymbol{v} = \boldsymbol{t}' + \boldsymbol{v}'$ has two representations as a sum of a vector in $\mathcal{F}$ and a vector in L. Then

$$\begin{aligned}(t_1 + a_1)\boldsymbol{v}_1 + (t_2 + a_2)\boldsymbol{v}_2 + \cdots + (t_n + a_n)\boldsymbol{v}_n \\ = (t_1' + a_1')\boldsymbol{v}_1 + (t_2' + a_2')\boldsymbol{v}_2 + \cdots + (t_n' + a_n')\boldsymbol{v}_n.\end{aligned}$$

Since $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ are independent, it follows that

$$t_i + a_i = t_i' + a_i' \qquad \text{for all } i = 1, 2, \ldots, n.$$

Hence

$$t_i - t_i' = a_i' - a_i \in \mathbb{Z}$$

is an integer. But we also know that t_i and t_i' are greater than or equal to 0 and strictly smaller than 1, so the only way for $t_i - t_i'$ to be an integer is if $t_i = t_i'$. Therefore $\boldsymbol{t} = \boldsymbol{t}'$, and then also

$$\boldsymbol{v} = \boldsymbol{w} - \boldsymbol{t} = \boldsymbol{w} - \boldsymbol{t}' = \boldsymbol{v}'.$$

This completes the proof that $\boldsymbol{t} \in \mathcal{F}$ and $\boldsymbol{v} \in L$ are uniquely determined by $\boldsymbol{w}$. □

格的基

定理

设L是一个维数为n的格，$v_1, v_2, .., v_n$是L的一组线性无关的向量，则$v_1, v_2, .., v_n$是L的一组基的充分必要条件是$\mathcal{F}(L) \cap L = \{0\}$.

格的行列式

定义.

设L是一个维数为n的格，$v_1, v_2, .., v_n$是L的一组基。称$\sqrt{\det(VV^T)}$为格L的行列式，记为det(L)，其中V是由基为列向量组成的$n \times m$矩阵。
当L的阶数等于维数时，矩阵V为方阵，$\det(L) = |\det(V)|$。
若$\mathcal{F}$是L的基础区域，L的行列式也称为$\mathcal{F}$的n维体积$Vol(\mathcal{F})$。

性质

格L的行列式是常数，不随基的选取而改变。

证明

设矩阵V和W是格L的两组基，则存在矩阵U使得$V = UW$,且$detU = \pm 1$. 故有

$$detL = \sqrt{det(VV^T)} = \sqrt{det(UWW^TU^T)} = \sqrt{det(WW^T)}$$

向量的长度（欧式范数）

向量的长度

设向量$a = (a_1, a_2, \cdots, a_n) \in \mathbb{R}^m$, 则$a$的长度$||a||$定义为$\sqrt{\sum_{i=1}^{m} a_i^2}$.

Hadamard不等式

性质(Hadamard不等式).

设L是维数为n的格，取L的任意一组基$v_1, v_2, \cdots, v_n$, $\mathcal{F}(L)$是L的基础区域。则

$$del(L) = Vol(\mathcal{F}) \leq ||v_1||\ ||v_2||...||v_n||$$

若把L的$v_1, v_2, \cdots, v_n$看成是固定长度的向量,则显然当任意两个基向量都正交时，行列式的值最大。从而说明：基越接近正交，则Hadamard不等式就越接近等式。

本次课程内容目录

格中的困难问题

格中的两个困难问题：

- 最短向量问题(The Shortest Vector Problem, SVP)：在格中找到一个最短向量，即找到一个非零向量$v \in L$拥有最小的欧式范数$||v||$
- 最近向量问题(The Closest Vector Problem, CVP)：给定一个向量$w \in \mathbb{R}^m$不在L中，找到一个向量$v \in L$最接近w，即找到$v \in L$使得欧式范数$||w - v||$最小

注意可能存在多于1个的最短向量。举例来说，在$\mathbb{Z}^2$中，$(0, \pm 1), (\pm 1, 0)$这四个向量全部是SVP的解。

格中的困难问题

在现实情景下，基于NP难问题或NP完全问题的密码系统往往依赖于一类问题的子集，以此获得效率或者创造陷门。在此操作后，所选问题子类的某些特殊属性总是有可能使它们比一般情况更容易解决。我们之前已经在背包问题中见识到了这点。一般的背包问题是NP完全问题但掩盖后的超递增背包问题却因为非常容易解决而曾经被建议作为密码系统的设计基础。

格中的困难问题

SVP和CVP在理论中和实际中有许多重要的变种被提出：
最短基问题(Shortest Basis Problem, SBP)
近似最短向量问题(Approximate Shortest Vector Problem, apprSVP)
近似最近向量问题(Approximate Closest Vector Problem, apprCVP)

Shortest Basis Problem (SBP) Find a basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ for a lattice that is shortest in some sense. For example, we might require that

$$\max_{1 \le i \le n} \|\boldsymbol{v}_i\| \qquad \text{or} \qquad \sum_{i=1}^{n} \|\boldsymbol{v}_i\|^2$$

be minimized. There are thus many different versions of SBP, depending on how one decides to measure the "size" of a basis.

Approximate Shortest Vector Problem (apprSVP) Let $\psi(n)$ be a function of n. In a lattice L of dimension n, find a nonzero vector that is no more than $\psi(n)$ times longer than a shortest nonzero vector. In other words, if $\boldsymbol{v}_{\text{shortest}}$ is a shortest nonzero vector in L, find a nonzero vector $\boldsymbol{v} \in L$ satisfying

$$\|\boldsymbol{v}\| \leq \psi(n)\|\boldsymbol{v}_{\text{shortest}}\|.$$

Each choice of function $\psi(n)$ gives a different apprSVP. As specific examples, one might ask for an algorithm that finds a nonzero $\boldsymbol{v} \in L$ satisfying

$$\|\boldsymbol{v}\| \leq 3\sqrt{n}\|\boldsymbol{v}_{\text{shortest}}\| \qquad \text{or} \qquad \|\boldsymbol{v}\| \leq 2^{n/2}\|\boldsymbol{v}_{\text{shortest}}\|.$$

Clearly an algorithm that solves the former is much stronger than one that solves the latter, but even the latter may be useful if the dimension is not too large.

Approximate Closest Vector Problem (apprCVP) This is the same as apprSVP, but now we are looking for a vector that is an approximate solution to CVP, instead of an approximate solution to SVP.

最短向量的上限

注释

普遍的情况下，求解SVP问题和CVP问题都被认为是极其困难的问题，随着格的维数的增加，求解变得更加困难。在实际应用中，认为最近向量问题可能比最短向量问题难一点，这是因为最近向量问题可以规约到稍高维度的最短向量问题。

一个格的最短向量到底有多长？这个问题的答案依赖于格的维数和行列式。

Hermite定理

一个n维格L中一定包含一个非零向量$v \in L$, 满足

$$||v|| \leq \sqrt{n} det(L)^{\frac{1}{n}}$$

由正交基生成的格中的SVP问题

由正交基生成的格中的SVP问题

设$L \subset \mathbb{R}^m$有一组基$v_1, v_2, \ldots v_n$且两两正交，那么解决SVP和CVP都将变得简单。为了解决SVP问题，我们注意到

$$||a_1 v_1 + a_2 v_2 + \ldots + a_n v_n||^2 = a_1^2||v_1||^2 + a_2^2||v_2||^2 + \ldots + a_n^2||v_n||^2$$

由于a_i都为整数，于是L中的最短向量实际上就在集合$\{\pm v_1, \ldots, \pm v_n\}$中。

由正交基生成的格中的CVP问题

由正交基生成的格中的CVP问题

类似地，如果要找到L中最接近给定向量$w \in \mathbb{R}^m$的向量，我们首先将w写为

$$w = t_1 v_1 + t_2 v_2 + \ldots + t_n v_n,\ t_1, t_2, \ldots, t_n \in \mathbb{R}$$

则对于$v = a_1 v_1 + a_2 v_2 + \ldots + a_n v_n \in L$，我们有

$$||v - w||^2 = (a_1 - t_1)^2 ||v_1||^2 + (a_2 - t_2)^2 ||v_2||^2 + \ldots + (a_n - t_n)^2 ||v_n||^2$$

由于a_i都为整数，所以要使得其最小只需要取每个a_i为最靠近t_i的整数即可

由正交基生成的格中的SVP问题和CVP问题

注记

对L的任意一组基来说，如果基中的向量两两正交那么我们很容易就可以解决SVP问题和CVP问题。但事实是经常面对的是格中不存在一组正交基，所以求解这两个问题变得很困难。因此在研究给理论的过程中，应该尽量找到一组两两正交或者接近两两正交的基，在这个前提下可以有很大可能性解决SVP问题和CVP问题。

Hadamard比率

定义

定义格L中的任意基$\mathcal{B} = \{v_1, v_2, \cdots, v_n\}$的Hadamard比率为:

$$\mathcal{H}(\mathcal{B}) = (\frac{det\ L}{||v_1||...||v_n||})^{1/n}$$

显然有 $0 < \mathcal{H}(\mathcal{B}) \leq 1$，并且随着基中向量越正交，Hadamard比率就越接近1。当$v_1, v_2, \cdots, v_n$两两正交时，$det(L) = ||v_1||||v_2|| \cdots ||v_n||$, 此时Hadamard比率等于1. 因此，Hadamard比率能反映出格中基的正交情况。

CVP问题的假设解

格L的一组基$\{v_1, v_2, ...v_n\}$确定了一个基本区域$\mathcal{F}(v_1, v_2, ...v_n)$，前面的性质说明$\mathcal{F}(v_1, v_2, ...v_n)$的平移可以遍历整个空间，所以任意一个$w \in \mathbb{R}^m$都在一个特定的$\mathcal{F} + v$中，我们取$\mathcal{F} + v$中接近w的顶点作为CVP问题的假设解。很容易找到最接近的顶点，因为

$$w = v + \epsilon_1 v_1 + \epsilon_2 v_2 + ... + \epsilon_n v_n, \quad , for\ 0 \leq \epsilon_1, \epsilon_2, ..., \epsilon_n < 1$$

如果ϵ_i小于1/2就替换为0，如果大于等于1/2就将它替换为1

CVP问题的假设解

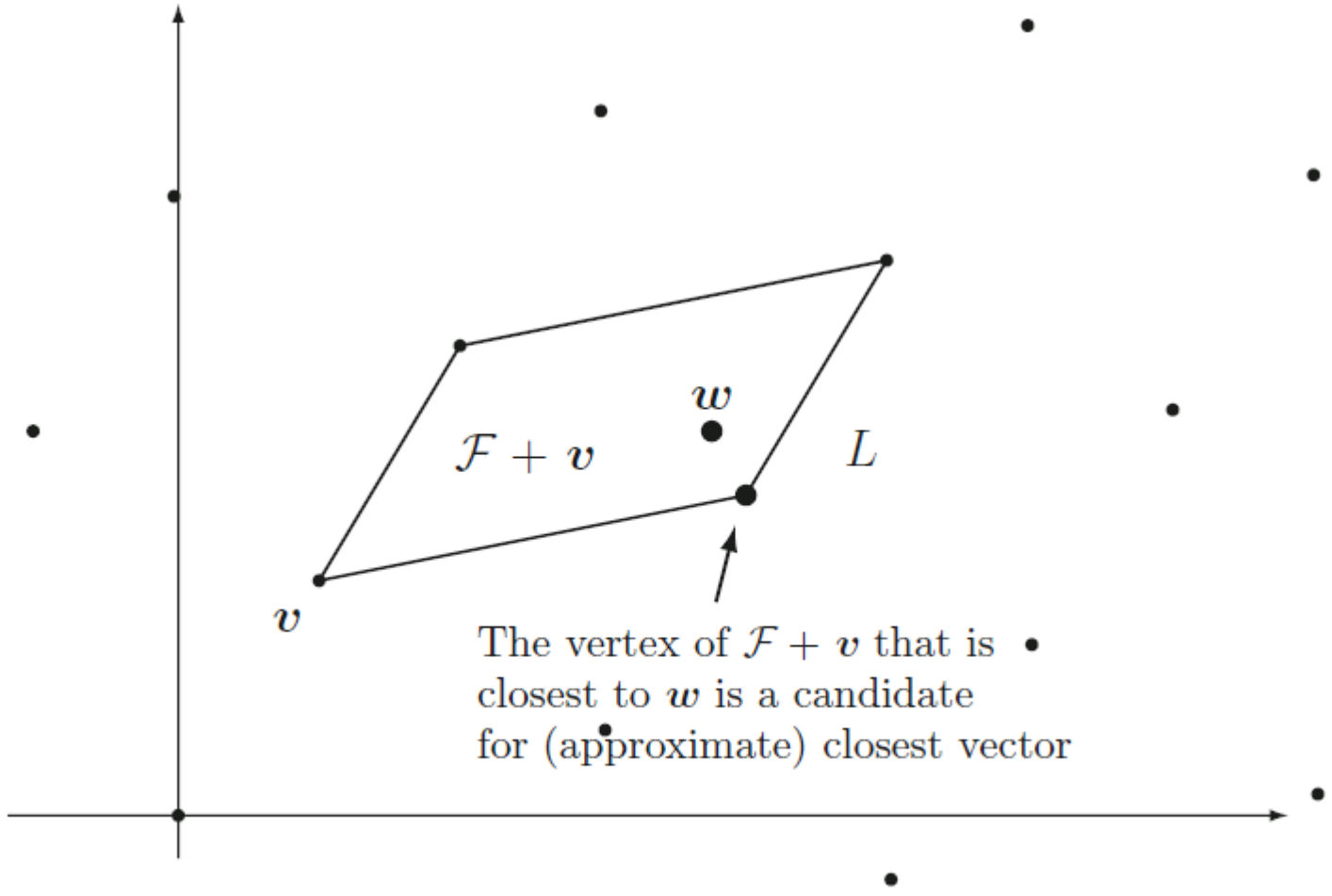

Figure 7.3: Using a given fundamental domain to try to solve CVP

CVP问题的假设解

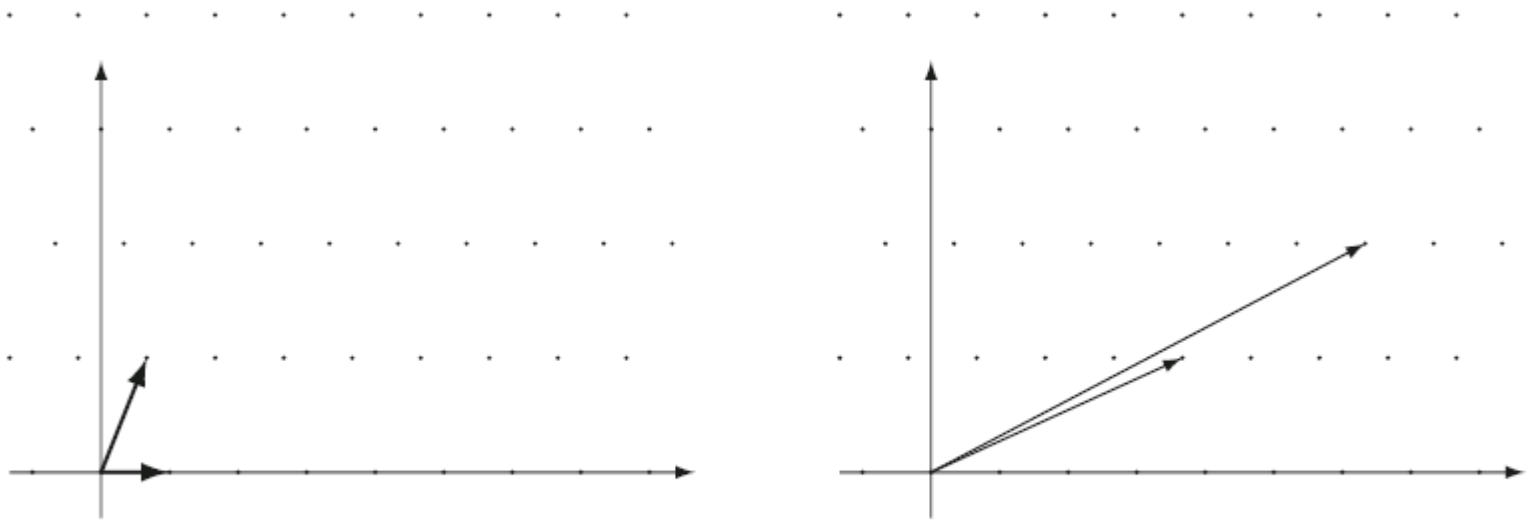

Figure 7.4: Two different bases for the same lattice

CVP问题的假设解

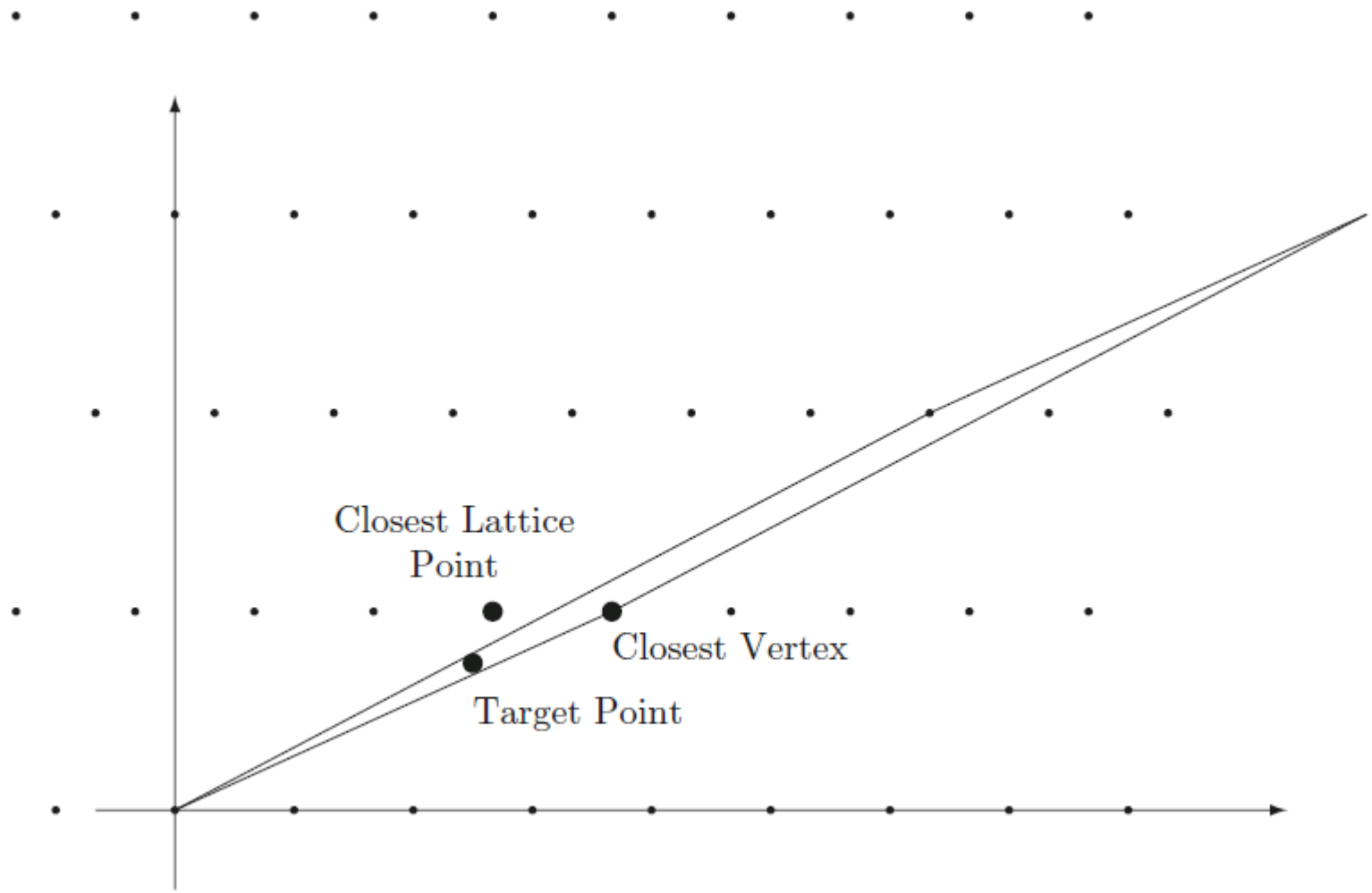

Figure 7.5: Babai's algorithm works poorly if the basis is "bad"

Babai算法

定理(Babai最近顶点算法).

设L是一个维数为n的格，$v_1, v_2, .., v_n$是L的基，$w \in \mathbb{R}^m$是任意一个向量。如果基中的向量互相之间足够正交，那么如下的算法就能解决CVP.

Write $\boldsymbol{w} = t_1\boldsymbol{v}_1 + t_2\boldsymbol{v}_2 + \cdots + t_n\boldsymbol{v}_n$ with $t_1, \ldots, t_n \in \mathbb{R}$.
Set $a_i = \lfloor t_i \rceil$ for $i = 1, 2, \ldots, n$.
Return the vector $\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n$.

通常来说，如果基中的向量互相合理的正交，那么这个算法也能解决apprCVP中的部分版本，但如果高度的不正交，那么这个算法返回的向量将与真正的结果相差甚远

Babai算法举例

示例

设$L \subset \mathbb{R}^2$是一个格，并且给定基$v_1 = (137, 312), v_2 = (215, -187)$
我们通过Babai的算法来找L中的向量使得最接近w=(53172,81743)
第一步就是将w表示为v_1, v_2线性组合的形式$w = t_1 v_1 + t_2 v_2,\ t_1, t_2 \in \mathbb{R}$

我们求得$t_1 \approx 296.85, t_2 \approx 58.15$。Babai的算法告诉我们取离$t_1, t_2$最靠近的整数然后计算

$$v = 297v_1 + 58v_2 = (53159, 81818)$$

确实很小，并且这就是所要求的的，因为给定的基的向量是几乎正交的，这点也可从Hadamard比看出

$$\mathcal{H}(\mathcal{B}) = \left(\frac{det\ L}{||v_1||\ ||v_2||}\right)^{1/2} \approx 0.977$$

Babai算法举例

然后我们在同样的格中解决同样的最近向量问题，但使用一组新的基

$$v_1' = (1975, 438) = 5v_1 + 6v_2 \; v_2' = (7548, 1627) = 19v_1 + 23v_2$$

同样求得$t_1 \approx 5722.66, t_2 \approx -1490.34$，因此令

$$v' = 5723v_1 - 1490v_2 = (56405, 82444)$$

$v' \in L$但实际上一点也不接近w，而且新的基$\{v_1', v_2'\}$的不正交可以通过Hadamard比很小看出

$$\mathcal{H}(\mathcal{B}) = (\frac{det\ L}{||v_1||\ ||v_2||})^{1/2} \approx 0.077$$

本次课程内容目录

Gauss约减算法

在维数为2的格中找到一组最优的基的算法是Gauss提出的，基本思想是交替地从一个基向量减去另一个基向量的倍数直到不能进一步改进。
设$L \subset \mathbb{R}^2$是一个维数为2的格，并且给定基v_1, v_2，不妨假设$||v_1|| < ||v_2||$。现在我们尝试通过减去v_1的倍数使得v_2小于v_1。

$$v_2^* = v_2 - \frac{v_1 \cdot v_2}{||v_1||^2} v_1$$

这个向量与v_1正交。向量v_2^*是v_2在v_1正交补空间上的投影。

Gauss约减算法

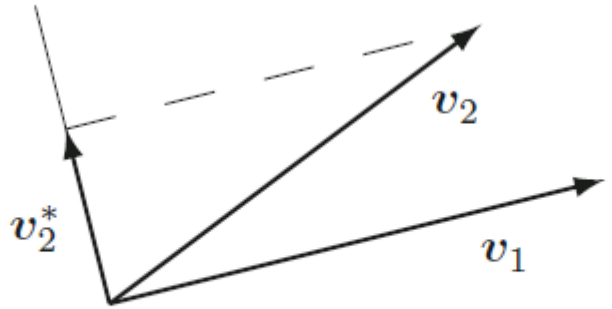

Figure 7.7: v_2^* is the projection of v_2 onto the orthogonal complement of v_1

Gauss约减算法

当然，这个是有问题的，因为v_2^*可能根本不在L中，实际上，我们应该只能减去v_1的整数倍数，因此我们尽力将v_2替换为

$$v_2 - mv_1,\ m = \lfloor \frac{v_1 \cdot v_2}{||v_1||^2} \rceil$$

如果v_2仍然比v_1长，则停止，否则交换v_1, v_2并重复这一过程，Gauss证明了这一过程将最终终止并且返回一个很好的L的基。接下来的性质将更清晰的说明。

Gauss约减算法

算法(Gaussian Lattice Reduction).

设$L \subset \mathbb{R}^2$是一个维数为2的格，基为v_1, v_2。下列算法将会终止并返回一个L中的良好性质的基。

Loop

If $\|\boldsymbol{v}_2\| < \|\boldsymbol{v}_1\|$, swap $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$.

Compute $m = \lfloor \boldsymbol{v}_1 \cdot \boldsymbol{v}_2 / \|\boldsymbol{v}_1\|^2 \rceil$.

If $m = 0$, return the basis vectors $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$.

Replace $\boldsymbol{v}_2$ with $\boldsymbol{v}_2 - m\boldsymbol{v}_1$.

Continue Loop

更准确的，当算法终止时，v_1是L中一个最短的非零向量，所以这一算法解决了SVP问题，进一步的，v_1, v_2间的夹角θ满足$|cos\theta| \leq ||v_1||/2||v_2||$。特别的，$\frac{\pi}{3} \leq \theta \leq \frac{2\pi}{3}$

Gauss约减算法正确性证明

Proof. We prove that $\boldsymbol{v}_1$ is a smallest nonzero lattice vector and leave the other parts of the proof to the reader. So we suppose that the algorithm has terminated and returned the vectors $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$. This means that $\|\boldsymbol{v}_2\| \geq \|\boldsymbol{v}_1\|$ and that

$$\frac{|\boldsymbol{v}_1 \cdot \boldsymbol{v}_2|}{\|\boldsymbol{v}_1\|^2} \leq \frac{1}{2}. \tag{7.51}$$

(Geometrically, condition (7.51) says that we cannot make $\boldsymbol{v}_2$ smaller by subtracting an integral multiple of $\boldsymbol{v}_1$ from $\boldsymbol{v}_2$.) Now suppose that $\boldsymbol{v} \in L$ is any nonzero vector in L. Writing

$$\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 \quad \text{with } a_1, a_2 \in \mathbb{Z},$$

Gauss约减算法正确性证明

we find that

$$\begin{aligned}
\|\boldsymbol{v}\|^2 &= \|a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2\|^2 \\
&= a_1^2\|\boldsymbol{v}_1\|^2 + 2a_1a_2(\boldsymbol{v}_1 \cdot \boldsymbol{v}_2) + a_2^2\|\boldsymbol{v}_2\|^2 \\
&\geq a_1^2\|\boldsymbol{v}_1\|^2 - 2|a_1a_2|\,|\boldsymbol{v}_1 \cdot \boldsymbol{v}_2| + a_2^2\|\boldsymbol{v}_2\|^2 \\
&\geq a_1^2\|\boldsymbol{v}_1\|^2 - |a_1a_2|\|\boldsymbol{v}_1\|^2 + a_2^2\|\boldsymbol{v}_2\|^2 \quad \text{from (7.51)}, \\
&\geq a_1^2\|\boldsymbol{v}_1\|^2 - |a_1a_2|\|\boldsymbol{v}_1\|^2 + a_2^2\|\boldsymbol{v}_1\|^2 \quad \text{since } \|\boldsymbol{v}_2\| \geq \|\boldsymbol{v}_1\|, \\
&= (a_1^2 - |a_1|\,|a_2| + a_2^2)\|\boldsymbol{v}_1\|^2.
\end{aligned}$$

For any real numbers t_1 and t_2, the quantity

$$t_1^2 - t_2t_2 + t_2^2 = \left(t_1 - \frac{1}{2}t_2\right)^2 + \frac{3}{4}t_2^2 = \frac{3}{4}t_1^2 + \left(\frac{1}{2}t_1 - t_2\right)^2$$

is not zero unless $t_1 = t_2 = 0$. So the fact that a_1 and a_2 are integers and not both 0 tells us that $\|\boldsymbol{v}\|^2 \geq \|\boldsymbol{v}_1\|^2$. This proves that $\boldsymbol{v}_1$ is a smallest nonzero vector in L. □

Gauss约减算法例子

示例

我们演示一下Gaussian Lattice Reduction算法。以格L为例，其基为

$$v_1 = (66586820, 65354729), v_2 = (6513996, 6393464)$$

我们首先计算$||v_1||^2 \approx 8.71 \cdot 10^{15}, ||v_2||^2 \approx 8.33 \cdot 10^{13}$，由于$v_2$更短，交换，

$$v_1 = (6513996, 6393464), v_2 = (66586820, 65354729)$$

Gauss约减算法例子

$$m = \lfloor \frac{v_1 \cdot v_2}{||v_1||^2} \rceil = 10$$

因此替换$v_2 = v_2 - mv_1 = (1446860, 1420089)$
新向量范数$||v_2||^2 \approx 4.11 \cdot 10^{12}$，比$||v_1||^2 \approx 8.33 \cdot 10^{13}$小，继续交换

$$v_1 = (1446860, 1420089), v_2 = (6513996, 6393464)$$

Gauss约减算法例子

重复这一过程$m = \lfloor \frac{v_1 \cdot v_2}{||v_1||^2} \rceil = 5$,给出新向量

$$v_2 = v_2 - mv_1 = (-720304, -706981)$$

有范数$||v_2||^2 \approx 1.01 \cdot 10^{12}$，因此继续交换。重复以上操作直到基越来越小，算法终止，结果如下

Step	v_1	v_2	m
1	$(6513996, 6393464)$	$(66586820, 65354729)$	10
2	$(1446860, 1420089)$	$(6513996, 6393464)$	5
3	$(-720304, -706981)$	$(1446860, 1420089)$	-2
4	$(6252, 6127)$	$(-720304, -706981)$	-115
5	$(-1324, -2376)$	$(6252, 6127)$	-3
6	$(2280, -1001)$	$(-1324, -2376)$	0

最终的基相当小，SVP问题的解为(2280,-1001)。

课后作业

7.13. Let L be the lattice given by the basis

$$\mathcal{B} = \{(3, 1, -2),\ (1, -3, 5),\ (4, 2, 1)\}.$$

Which of the following sets of vectors are also bases for L? For those that are, express the new basis in terms of the basis $\mathcal{B}$, i.e., find the change of basis matrix.

(a) $\mathcal{B}_1 = \{(5, 13, -13),\ (0, -4, 2),\ (-7, -13, 18)\}$.

(b) $\mathcal{B}_2 = \{(4, -2, 3),\ (6, 6, -6),\ (-2, -4, 7)\}$.

7.14. Let $L \subset \mathbb{R}^m$ be a lattice of dimension n and let $v_1, \dots, v_n$ be a basis for L. Note that we are allowing n to be smaller than m. The *Gram matrix of* $v_1, \dots, v_n$ is the matrix

$$\mathrm{Gram}(v_1, \dots, v_n) = \big(v_i \cdot v_j\big)_{1 \le i,j \le n}.$$

(a) Let $F(v_1, \dots, v_n)$ be the matrix (7.11) described in Proposition (7.20), except that now $F(v_1, \dots, v_n)$ is an n-by-m matrix, so it need not be square. Prove that

$$\mathrm{Gram}(v_1, \dots, v_n) = F(v_1, \dots, v_n) F(v_1, \dots, v_n)^t,$$

where $F(v_1, \dots, v_n)^t$ is the transpose matrix, i.e., the matrix with rows and columns interchanged.

(b) Prove that

$$\det\big(\mathrm{Gram}(v_1, \dots, v_n)\big) = \det(L)^2, \tag{7.62}$$

where note that $\det(L)$ is the volume of the parallelepiped spanned by any basis for L. (You may find it easier to first do the case $n = m$.)

(c) Let $L \subset \mathbb{R}^4$ be the 3-dimensional lattice with basis

$$v_1 = (1, 0, 1, -1), \quad v_2 = (1, 2, 0, 4), \quad v_3 = (1, -1, 2, 1).$$

Compute the Gram matrix of this basis and use it to compute $\det(L)$.

(d) Let $v_1^*, \dots, v_n^*$ be the Gram–Schmidt orthogonalized vectors (Theorem 7.13) associated to $v_1, \dots, v_n$. Prove that

$$\det\big(\mathrm{Gram}(v_1, \dots, v_n)\big) = \|v_1^*\|^2 \|v_2^*\|^2 \cdots \|v_n^*\|^2.$$