CS 681: Computational Number Theory and Algebra	**Lecture 27**
Short Vectors in Lattices	
Lecturer: Manindra Agrawal	**Scribe: Chandan Saha**
	Novembor 25, 2005

1 Introduction

Definition 1.1 *A lattice* $\mathbf{L} \subseteq \mathbf{R}^n$ *is a set of points defined as:*

$$\mathbf{L} = \{\sum_{i=1}^{m} \alpha_i u_i \mid \alpha_i \in \mathbf{Z} \text{ and } u_i \in \mathbf{R}^n\}$$

We will assume that $m = n$ and $u_i's$ are linearly independent. The problem of computing a shortest vector in a given lattice is **NP**-hard. We define the volume of a lattice **L** as:

$$Vol(\mathbf{L}) = \mid det[u_1\, u_2\, \ldots\, u_n] \mid$$

If the $u_i's$ are linearly dependent then $Vol(\mathbf{L}) = 0$. The vectors $u_1, u_2, \ldots, u_n$ are called a *basis* for **L**.

Lemma 1.1 $Vol(\mathbf{L})$ *is independent of the choice of the basis.*

Proof: Let $v_1, v_2, \ldots, v_n$ be another basis for **L**. We have, $v_j = \sum_{i=1}^{n} \beta_{ij} u_i$, where $\beta_{ij} \in \mathbf{Z}$.

$$\begin{aligned} [v_1\, v_2\, \ldots\, v_n] &= [u_1\, u_2\, \ldots\, u_n] \cdot [\beta_{ij}] \\ \Rightarrow \mid det[v_1\, v_2\, \ldots\, v_n] \mid &= \mid det[u_1\, u_2\, \ldots\, u_n] \mid \cdot \mid det[\beta_{ij}] \mid \\ \Rightarrow \mid det[u_1\, u_2\, \ldots\, u_n] \mid & \text{ divides } \mid det[v_1\, v_2\, \ldots\, v_n] \mid \end{aligned}$$

Similarly, $\mid det[v_1\, v_2\, \ldots\, v_n] \mid$ *divides* $\mid det[u_1\, u_2\, \ldots\, u_n] \mid$.
Therefore, $\mid det[v_1\, v_2\, \ldots\, v_n] \mid = \mid det[u_1\, u_2\, \ldots\, u_n] \mid$. ∎

2 Application of finding Short Vector in a Lattice

Consider the scenario where the RSA cryptosystem is used. Let p and q be two large primes and $n = pq$. Let $(n, 3)$ be the public key. Suppose we encrypt message m such that the initial part of m is a fixed header h that is known, whereas the unknown content of the message be x that is l bits long. Without loss in generality assume that $0 \leq m < n$.

Let $m = h \cdot 2^l + x$ and $c = m^3 (mod n)$. Assume that the adversary knows c, h, l and $(n, 3)$. Since,

$$\begin{aligned} c &= (h \cdot 2^l + x)^3 \, (mod\, n) \\ \Rightarrow p(x) &= x^3 + a_2 x^2 + a_1 x + (a_0 - c) = 0 \, (mod\, n) \end{aligned}$$

The adversary computes $p(x)$ and tries to solve for x. Let a lattice $\mathbf{L} \in \mathbf{R^6}$ be defined by the following basis vectors:

$$\begin{pmatrix} a_0 - c \\ a_1 \\ a_2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ a_0 - c \\ a_1 \\ a_2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ a_0 - c \\ a_1 \\ a_2 \\ 1 \end{pmatrix}, \begin{pmatrix} n \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ n \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ n \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Therefore, $Vol(\mathbf{L}) = n^3$.

Theorem 2.1 *(Minkowski) Let $\mathbf{L} \in \mathbf{R}^d$ be a lattice. Then, the length of the shortest vector in $\mathbf{L} \leq d^{\frac{1}{2}} \cdot Vol(\mathbf{L})^{\frac{1}{d}}$.*

From the above theorem we conclude that the shortest vector in our lattice $\mathbf{L}$ has length $\leq \sqrt{6} n^{\frac{1}{2}}$.

Let $v = (v_0, v_1, \ldots, v_5)$ be the shortest vector in $\mathbf{L}$. Let the polynomial

$$\begin{aligned} v(x) &= \sum_{i=0}^{5} v_i x^i \\ &= \gamma_1 p(x) + \gamma_2 x p(x) + \gamma_3 x^2 p(x) + \gamma_4 n + \gamma_5 n x + \gamma_6 n x^2 \\ &= (\gamma_1 + \gamma_2 x + \gamma_3 x^2) p(x) \, (mod\, n) \end{aligned}$$

Suppose $x = m_0$ be the unknown message. Then

$$\begin{aligned} p(m_0) &= 0 (mod\, n) \\ \Rightarrow v(m_0) &= 0 (mod\, n) \\ \Rightarrow m_0 & \text{ is a root of } v(x) \text{ modulo } n \end{aligned}$$

$$\begin{aligned} \mid v(m_0) \mid &= \mid \sum_{i=0}^{5} v_i m_0^i \mid \\ &\leq 6\, max\{\mid v_i \mid\} m_0^5 \\ &\leq 6\, max\{\mid v_i \mid\} 2^{5l} \\ &\leq 6\sqrt{6} \cdot \sqrt{n} \cdot 2^{5l} \\ &< n \text{ if } l < \frac{1}{10} log \frac{n}{216} \end{aligned}$$

Therefore, $v(m_0) = 0$ over $\mathbf{Z}$. Thus if the actual message x is only about $\frac{1}{10}$-th of the total message then the adversary can solve for x by computing a shortest vector v in $\mathbf{L}$ and then solving for $v(x) = 0$ over $\mathbf{Z}$.