Lower Bounds of Shortest Vector Lengths in Random NTRU Lattices ⋆ ⋆⋆

Jingguo Bi[1,2⋆] and Qi Cheng[2⋆⋆]

[1] School of Mathematics
Shandong University
Jinan, 250100, P.R. China.
Email: jguobi@mail.sdu.edu.cn
[2] School of Computer Science
University of Oklahoma
Norman, OK 73019, USA
Email: qcheng@cs.ou.edu

Abstract. Finding the shortest vector of a lattice is one of the most important problems in computational lattice theory. For a random lattice, one can estimate the length of the shortest vector using the Gaussian heuristic. However, no rigorous proof can be provided for some classes of lattices, as the Gaussian heuristic may not hold for them. In this paper, we propose a general method to estimate lower bounds of the shortest vector lengths for random integral lattices in certain classes, which is based on the incompressibility method from the theory of Kolmogorov complexity. As an application, we can prove that for a random NTRU lattice, with an overwhelming probability, the ratio between the length of the shortest vector and the length of the target vector, which corresponds to the secret key, is at least a constant, independent of the rank of the lattice.
Key words: Shortest vector problem, Kolmogorov complexity, NTRU lattices, random lattices, Gaussian heuristic.

1 Introduction

A lattice is a set of points in a Euclidean space with periodic structure. Given n linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^m (n \leq m)$, the lattice generated by them is the set of vectors

$$L(\mathbf{b_1}, \ldots, \mathbf{b_n}) = \{\sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z}\}$$

The vectors $\mathbf{b_1}, \ldots, \mathbf{b_n}$ form a basis of the lattice.

⋆ Partially supported by NSF of China Projects (No.61133013 and No.60931160442), GIIFSDU Project (No. 11140070613184) and Tsinghua University Initiative Scientific Research Program (No.2009THZ01002).
⋆⋆ Partially supported by NSF under grants CCF-0830522 and CCF-0830524.

The most famous computational problem on lattices is the shortest vector problem (SVP): Given a basis of a lattice L, find a non-zero vector $\mathbf{u} \in L$, such that $\| \mathbf{v} \| \geq \| \mathbf{u} \|$ for any vector $\mathbf{v} \in L \setminus \mathbf{0}$. For the hardness of SVP, Ajtai first proved that SVP is NP-hard under a randomized reduction [2] and his result was strengthened in [15][4][10][7]. An upper bound for the length of the shortest vector is given in the famous Minkowski Convex Body Theorem. Nevertheless, there is no known efficient algorithm which can always find a vector within the Minkowski bound.

The study of random lattices has a long history, dated back from [18]. It turns out that one can define a measure on the set of all n-dimensional lattices of a fixed determinant, and have a precise estimation of the expected length of the shortest vector [3], which can be summarized by the so-called Gaussian heuristic. Given an n-dimensional lattice L with determinant $det(L)$, the Gaussian heuristic predicts that there are about $vol(C)/det(L)$ many lattice points in a measurable subset C of $\mathbb{R}^n$ of volume $vol(C)$. It can be made precise, for example, when C is convex and symmetric around the original point O, and $vol(C)$ is much bigger than $det(L)$. If we take C to be an n-sphere centered at O, for C to contain a point other than O, $vol(C)$ should be about $det(L)$ according to the Gaussian heuristic. In other words, the length of the shortest vector can be approximated by the radius of a sphere whose volume is $det(L)$, which is about $\sqrt{n/2e\pi}det(L)^{1/n}$. As an interesting comparison, the Minkowski Convex Body Theorem asserts that if the volume of sphere C is greater than $2^n det(L)$, then it must contain a nonzero lattice point. This gives an upper bound of the shortest vector length at about $\sqrt{2n/e\pi}det(L)^{1/n}$, which is only twice as large as the prediction made from the Gaussian heuristic.

Most of lattices appearing in cryptanalysis are random in some sense, but many of them have integral bases and hence are not random according to the above measure. See [16] for further discussions. The length of the shortest vector may be much shorter than the prediction made from the Gaussian heuristic. In this paper, we investigate the idea of using the theory of Kolmogorov complexity to estimate the expected length of short vectors of a given random integral lattice. Kolmogorov complexity has many applications in computational complexity and combinatorics. It is an ideal tool to obtain lower bounds [12]. While all the methods based on Kolmogorov complexity can be replaced by elementary counting arguments, and our result is no exception, we believe that the Kolmogorov complexity method is conceptually simpler, more intuitive and more systematic than a direct counting argument.

As a crucial application, we consider random NTRU lattices which are used to analyze NTRU cryptosystems. The NTRU cryptosystem was first introduced at the rump section of Crypto 96 by [8]. It operates in the ring of truncated polynomials given by $\mathbb{Z}[X]/(X^N - 1)$. Let S_f and S_g be some sets of polynomials in $\mathbb{Z}[x]$ of degree at most $N-1$ and of very small coefficients. Let q be a positive integer. Select polynomials $f(x) \in S_f$ and $g(x) \in S_g$. Let $h(x) = \sum_{i=0}^{N-1} h_i x^i$ be the polynomial such that

$$h(x)f(x) = g(x) \pmod{q, x^N - 1}.$$

Define the cyclic matrix

$$H = \begin{pmatrix} h_0 & h_1 & \cdots & h_{N-1} \\ h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \cdots & h_0 \end{pmatrix}$$

The security of the NTRU cryptosystem is related to the difficulty of finding short vectors in an NTRU lattice [5, 8]:

$$L^{NTRU} = \begin{pmatrix} I & H \\ \mathbf{0} & qI \end{pmatrix}. \tag{1}$$

We call an NTRU lattice (S_f, S_g)-random if $f(x)$ is selected uniformly at random from the invertible elements (in the ring $(\mathbb{Z}/q\mathbb{Z})[x]/(x^N - 1)$) in S_f, and $g(x)$ is selected uniformly in random from S_g.

Remark 1. A random NTRU lattice can *not* be obtained by selecting $(h_0, h_1, h_2, \cdots, h_{N-1})$ uniformly at random from $(\mathbb{Z}/q\mathbb{Z})^N$. In fact, a lattice obtained in that manner is most likely not an NTRU lattice.

Interestingly Gaussian heuristic clearly does not hold for random NTRU lattices. According to the Gaussian heuristic, the shortest vector length is $\Omega(\sqrt{Nq})$. However, the vector of the coefficients of f and g, which will be called the target vector, is in the lattice and has length $O(\sqrt{N})$, since f and g have very small coefficients. Many researchers conjecture that the target vector is indeed the shortest vector in the lattice in most of cases. However, no formal proof has been provided.

Remark 2. It is important to bound the length of the shortest vector from below in an NTRU lattice, since if the shortest vector is significantly shorter than the target vector, say that it has length $o(\sqrt{N})$, then it can be recovered by an exhaustive search in time $2^{o(N)}$, and can be used in breaking NTRU cryptosystems [5].

In this paper, we prove that with an overwhelming probability, the ratio between the length of the shortest vector and length of the target vector is at least a constant. In other words, we prove that most likely, the target vector is as long as the shortest vector up to a constant factor. As far as we know, this is the first lower bound result on the lengths of the shortest vectors in random NTRU lattices.

Remark 3. Since it is known that approximating the shortest vector by any constant factor is NP-hard [10] for general lattices, this result provides a some evidence for the security of the NTRU cryptosystem against the lattice reduction attack. However, our results do not rule out other types of attacks that may not be based on lattice reductions.

The rest of the paper is organized as follows. In Section 2, we will review some backgrounds about lattices and Kolmogorov complexity. In section 3, we prove the main theorem that allows us to compute lower bounds of the shortest vector lengths in random lattices. In Section 4, we present and prove the lower bound of the shortest vector lengths of random NTRU lattices. We conclude this paper in Section 5. In this paper, we use log to denote the logarithm base 2 and use ln to denote the natural logarithm.

2 Preliminaries

2.1 Lattices

Let $\mathbb{R}^m$ be the m-dimensional Euclidean space. A lattice in $\mathbb{R}^m$ is the set

$$L(\mathbf{b_1}, \ldots, \mathbf{b_n}) = \{\sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z}\}$$

of all integral combinations of n linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^m$. The integers n and m are called the rank and dimension of the lattice. A lattice can be conveniently represented by a matrix $\mathbf{B}$, where $\mathbf{b_1}, \ldots, \mathbf{b_n}$ are the row vectors. The determinant of the lattice L is defined as

$$\det(L(\mathbf{B})) = \sqrt{\det(\mathbf{B}\mathbf{B}^T)} \tag{2}$$

The most famous computational problem on lattices is the shortest vector problem (SVP): Given a basis of a lattice L, find a non-zero vector $\mathbf{u} \in L$, such that $\| \mathbf{v} \| \geq \| \mathbf{u} \|$ for any vector $\mathbf{v} \in L \setminus \mathbf{0}$. The following is a well-known theorem on the upper bound of the shortest vector length in lattice L.

Theorem 1. *(Minkowski) Any lattice L of rank n contains a non-zero vector $\mathbf{v}$ with*

$$||\mathbf{v}|| \leq (1 + o(1))\sqrt{2n/e\pi}\det(L)^{\frac{1}{n}}$$

In many literatures, the theorem is presented with the upper bound $\sqrt{n}\det(L)^{\frac{1}{n}}$, which is a little weaker but free of an additive error term.

2.2 Number of integral points in a sphere

To obtain our results, it is important to have an accurate estimation of the number of integral points inside of the n-sphere centered at the origin of radius R. Denote the number by $W(n, R)$. In general, one can approximate $W(n, R)$ by the volume of the sphere, denoted by $V(n, R)$. This is an application of the Gaussian Heuristic. However, if the radius of the sphere is small, compared to the square root of the dimension, then the volume estimate is not very accurate. More precisely, if the radius of the sphere $R \geq n^{1/2+\epsilon}$, the number of integral points in the sphere is equal to the volume

$$V(n, R) = (\sqrt{\pi n} + O(1))^{-1}(\sqrt{\frac{2\pi e}{n}}R)^n$$

with a small additive error. If R is $\sqrt{\alpha n}$ for some small constant α, then the estimation using volume is not so precise. To see this, note that when $\alpha < \frac{1}{2\pi e}$, the volume of the sphere is less than 1, yet it still contains many integral points. We should use the result found in [14] to estimate $W(n, R)$ for $R = O(\sqrt{n})$:

Proposition 1. *Let α be a constant. Then there exists a constant δ, depending only on α, such that $W(n, \sqrt{\alpha n}) \geq e^{\delta n}$ for n large enough. Moreover, as α gets larger, δ is approaching $\ln(\sqrt{2\pi e \alpha})$.*

To find δ from α, one defines $\theta(z) = 1 + 2\sum_{i=1}^{\infty} z^{i^2}$. Set $\delta(\alpha, x) = \alpha x + \ln \theta(e^{-x})$. We can compute $\delta = \min_{x \geq 0} \delta(\alpha, x)$. As a comparison between the number of integral points in a ball and its volume, we have

$$W(n, \sqrt{0.1n}) \approx e^{0.394415n}, V(n, \sqrt{0.1n}) \approx e^{0.267645n}.$$

$$W(n, \sqrt{0.5n}) \approx e^{1.07246n}, V(n, \sqrt{0.5n}) \approx e^{1.07236n}.$$

For $\alpha > 0.5$, the difference between $\log V(n, \sqrt{\alpha n})/n$ and $\log W(n, \sqrt{\alpha n})/n$ is less than 0.0001. See Table 1 in [14]. We also have

Proposition 2. *Let δ be a constant. Then there exists a constant α such that if an n-sphere centered at the origin contains more than $e^{\delta n}$ many integral points, the radius of the sphere must be greater than $\sqrt{\alpha n}$ for n large enough. As δ gets larger, α is approaching $e^{2\delta}/2\pi e$.*

2.3 Kolmogorov complexity

The Kolmogorov complexity of a binary string x, conditional to y, is defined to be the length of the shortest program that given the input y, prints the string x, and is denoted by $K(x|y)$. We define $K(x)$ to be $K(x|\epsilon)$, where ϵ is the empty string. It turns out that if one switches from one programming language to another, the Kolmogorov complexity is invariant, up to an additive constant, as long as both of the programming languages are Turing Universal. The book [12] gave an excellent introduction to the theory of Kolmogorov complexity.

It can be shown that for any positive integer s, $K(s) \leq \log s + O(1)$. If $s = 1^n$, the binary string of length n consisting of only 1, then $K(s) \leq \log n + O(1)$. Similarly if s is the first n binary digits of the number π after the decimal point, then $K(s) \leq \log n + O(1)$. From the examples, one can see that the Kolmogorov complexity is a good measure of randomness in a string.

For each constant c, a positive integer x is c-incompressible if $K(x) \geq \log(x) - c$. By a counting argument, one can show

Proposition 3. *For any y, a finite set A of cardinality m has at least $m(1 - 2^{-c}) + 1$ elements x with $K(x|y) \geq \log m - c$.*

This observation yields a simple yet powerful proof technique — the incompressibility method.

3 The main theorem

Theorem 2. *Given a random integral lattice $\mathbf{L} \in \mathbb{R}^m$ represented by a matrix $\mathbf{B} \in \mathbb{Z}^{n \times m}$, let the vector $\mathbf{v}$ be the shortest vector of lattice $\mathbf{L}$. Let $\mathbf{S}$ denote some entries in $\mathbf{B}$ and $\mathbf{B} \setminus \mathbf{S}$ denote the rest of entries in the matrix. Assume that $K(\mathbf{S}|\mathbf{v}, \mathbf{B} \setminus \mathbf{S}) = O(\log m)$. Let R be a positive real number such that*

$$\log W(m, R) \leq K(\mathbf{S}|\mathbf{B} \setminus \mathbf{S}) - \log^2(m)$$

then the shortest vector is longer than R.

Proof. Suppose that the length of the short vectors is less than R. Then

$$K(\mathbf{v}|m) \leq \log W(m, R) + O(1).$$

On the other hand, to describe $\mathbf{S}$ from $\mathbf{B} \setminus \mathbf{S}$, we only need to describe $\mathbf{v}$ in addition to the program which computes $\mathbf{S}$ from $\mathbf{B} \setminus \mathbf{S}$ and $\mathbf{v}$, so we have

$$\begin{aligned} K(\mathbf{S}|\mathbf{B} \setminus \mathbf{S}) &\leq K(\mathbf{S}|\mathbf{v}, \mathbf{B} \setminus \mathbf{S}) + K(\mathbf{v}|m) + 2 \log K(\mathbf{S}|\mathbf{v}, \mathbf{B} \setminus \mathbf{S}) \\ &\leq K(\mathbf{v}|m) + O(\log m) \end{aligned}$$

so $K(\mathbf{v}|m) \geq K(\mathbf{S}|\mathbf{B} \setminus \mathbf{S}) - O(\log m)$, which is a contradiction.

To use the theorem, we select a part $\mathbf{S}$ of $\mathbf{B}$ such that $K(\mathbf{S}|\mathbf{B} \setminus \mathbf{S})$ is large but $K(\mathbf{S}|\mathbf{v}, \mathbf{B} \setminus \mathbf{S})$ is small, then according to the theorem, we have a good lower bound on the length of the shortest vectors. In other words, if some part of the matrix has high Kolmogorov complexity, yet it can be determined (almost) uniquely by a short vector and the rest of the matrix, then the lattice has long shortest vectors. The main technical part is to show that $K(\mathbf{S}|\mathbf{v}, \mathbf{B} \setminus \mathbf{S})$ is small. In some case, it is easy, as in the following remark, but in the case of NTRU lattices, it is highly non-trivial.

Remark 4. As a simple application of this theorem, we can compute the lower bound of the shortest vector lengths for the random knapsack lattice introduced by [11, 6]. A knapsack lattice is spanned by $\mathbf{b_1}, \ldots, \mathbf{b_n}$ below:

$$\begin{aligned} \mathbf{b_1} &= (a_1, 1, 0, \ldots, 0) \\ \mathbf{b_2} &= (a_2, 0, 1, \ldots, 0) \\ &\vdots \\ \mathbf{b_n} &= (a_n, 0, 0, \ldots, 1), \end{aligned}$$

where $a_1, a_2, \cdots, a_n$ are integers. We call the lattice *random*, if $a_1, a_2, \cdots, a_n$ are selected uniformly and independently from r-bit integers. Random knapsack lattices were used by Nguyen and Stehle [16] to assess the performance of LLL algorithm. Note that if $(v_0, v_1, \cdots, v_n)$ is the shortest vector, and assume w.l.o.g. that $v_1 \neq 0$. Then we use a_1 as $\mathbf{S}$ and apply the main theorem. Through a routine calculation, we obtain that with probability at least $1 - \frac{1}{nr}$, the length of the shortest vector in the knapsack lattice $L_{a_1, a_2, \cdots, a_n}$ is greater than $\sqrt{\frac{n+1}{2\pi e}} \cdot 2^{\frac{r}{n+1}}(1 + O(\frac{\log(nr)}{n}))$, which is not far away from the Gaussian heuristic.

4 The lower bounds of shortest vectors lengths of NTRU lattices

In this section, we first describe the NTRU cryptosystems in section 4.1. We prove a technical lemma in section 4.2 and prove the lower bounds of shortest vector lengths of NTRU lattices in section 4.3.

4.1 Description of the NTRU cryptosystem

The NTRU algorithm was first introduced by [8] at the rump section of Crypto 96. It operates in the ring of truncated polynomials given by $\mathbb{Z}[X]/(X^N-1)$. To describe the parameters of the NTRU cryptosystem, we begin by choosing a prime N and two moduli p, q such that $\gcd(N,p) = \gcd(p,q) = 1$. Let R, R_p, and R_q be the convolution polynomial rings

$$R = \mathbb{Z}[x]/(x^N-1), R_p = (\mathbb{Z}/p\mathbb{Z})[x]/(x^N-1), R_q = (\mathbb{Z}/q\mathbb{Z})[x]/(x^N-1)$$

For any positive integers d_1 and d_2, define the set

$$T(d_1,d_2) = \left\{ a(x) \in R : \begin{array}{r} a(x) \text{ has } \ d_1 \text{ coefficients equal to } 1; \\ d_2 \ \text{ coefficients equal to } \ -1; \\ \text{has all other coefficients equal to } 0 \end{array} \right\}$$

and the set

$$B(d) = \left\{ a(x) \in R : \begin{array}{l} a(x) \text{ has } \ d \text{ coefficients equal to } 1; \\ \text{has all other coefficients equal to } 0 \end{array} \right\}$$

Let S_f and S_g be some sets of polynomials of degree at most $N-1$ and of very small coefficients. Usually they are set to be $T(d_1,d_2)$ or $B(d_3)$ for d_1, d_2 and d_3 proportional to N. To prevent an exhaustive search attack, $|S_f|$ and $|S_g|$ have to be large. In fact, there exists a constant γ such that for all the NTRU implementations, $|S_g| > 2^{\gamma N}$. It implies that for a randomly chosen polynomial g, its Kolmogorov complexity is larger than γN. The public parameters are (N, p, q, S_f, S_g). The private key consists of two randomly chosen polynomials

$$f(x) = \sum_{i=0}^{N-1} f_i x^i \in S_f \text{ and } g(x) = \sum_{i=0}^{N-1} g_i x^i \in S_g$$

compute

$$F_q(x) = f(x)^{-1} \text{ in } R_q \text{ and } F_p(x) = f(x)^{-1} \text{ in } R_p$$

then compute

$$h(x) = F_q(x) * g(x) \text{ in } R_q \tag{3}$$

The public key is the polynomial $h(x) = \sum_{i=0}^{N-1} h_i x^i$. From Equation (3) we can obtain the relationship

$$f(x) * h(x) \equiv g(x) \text{ in } R_q. \tag{4}$$

Recall the definition of an NTRU lattice (1). The vector

$$(f_0, f_1, \cdots, f_{N-1}, g_0, g_1, \cdots, g_{N-1})$$

is a very short vector in the lattice. Since usually $g(1) = 0$ for any $g \in S_g$, so $h(1) = 0 \pmod q$, thus this lattice has a trivial short vector $(1^N, 0^N)$, which can be shorter than the private key. If we adopt Coppersmith and Shamir's approach [5], and use a slightly different lattice of rank $2N - 2$:

$$\begin{pmatrix}
1-1/N & -1/N & \cdots & -1/N & h_0 & h_1 & \cdots & h_{N-1} \\
-1/N & 1-1/N & \cdots & -1/N & h_{N-1} & h_0 & \cdots & h_{N-2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
-1/N & -1/N & \cdots & 1-1/N & h_1 & h_2 & \cdots & h_0 \\
0 & 0 & \cdots & 0 & q-q/N & -q/N & \cdots & -q/N \\
0 & 0 & \cdots & 0 & -q/N & q-q/N & \cdots & -q/N \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & -q/N & -q/N & \cdots & q-q/N
\end{pmatrix}$$

then the short vector $(1^N, 0^N)$ is eliminated from the lattice. Coppersmith and Shamir proved if one can find a sufficiently short vector in the NTRU lattice, then the short vector gives us an equivalent private key.

4.2 A technical lemma

Let N be a prime and let $q > N$ be a prime power r^l. Given a short vector

$$\mathbf{v} = (v_1, v_2, \ldots, v_{2N}) \in \mathbb{Z}^{2N},$$

in this section, we prove a lemma concerning the number of solutions in $(\mathbb{Z}/q\mathbb{Z})^N$ of the following linear system

$$\begin{aligned}
h_0 v_1 + h_{N-1} v_2 + \ldots + h_1 v_N &\equiv v_{N+1} \pmod q \\
h_1 v_1 + h_0 v_2 + \ldots + h_2 v_N &\equiv v_{N+2} \pmod q \\
&\vdots \\
h_{N-1} v_1 + h_{N-2} v_2 + \ldots + h_0 v_N &\equiv v_{2N} \pmod q
\end{aligned} \tag{5}$$

Note that if $l > 1$, $\mathbb{Z}/q\mathbb{Z}$ is not a field.

Lemma 1. *Let N be a prime and let $q > N$ be a prime power r^l. Suppose that r is a primitive root in $\mathbb{Z}/N\mathbb{Z}$, and*

$$(v_1, v_2, \cdots, v_N) \in \mathbb{Z}^N$$

is a non-zero vector whose ℓ_2 norm is less than $\sqrt{N}$. Assume that r does not divide $gcd(v_1, v_2, \cdots, v_N)$. Then there are at most q solutions in $(\mathbb{Z}/q\mathbb{Z})^N$ for the linear system (5).

The proof of lemma 1 is given in appendix because of the limit of space.

4.3 The lower bounds of lengths of shortest vectors of NTRU lattices

In most implementations of NTRU cryptosystems (See IEEE P1363.1/D12 Draft Standard for details), q is set to be a power of two, and N is a prime such that 2 has order $N-1$ or $(N-1)/2$ in $(\mathbb{Z}/N\mathbb{Z})^*$. In this case, the modulo q operation can be implemented as a bit-wise Boolean operation, thus it is more efficient than operations of mod primes. In the following theorem, we will assume that q is a prime power r^l and r has order $N-1$ in $\mathbb{Z}/N\mathbb{Z}$. It covers many NTRU implementations including that q is a prime and that q is a power of 2.

Theorem 3. *Let N be an odd prime. Let $q < N^2$ be a prime power r^l. Assume that r has order $N-1$ in $(\mathbb{Z}/N\mathbb{Z})^*$. Suppose*

$$K(h|N,q) \geq \gamma N$$

for some constant γ. The length of the shortest vector in L^{NTRU} is greater than $\sqrt{\alpha N}$ for some constant α depending only on γ.

Proof. Suppose the vector $\mathbf{v} = (v_1, v_2, \ldots, v_{2N}) \in \mathbb{Z}^{2N}$ is the shortest vector of L^{NTRU}. Hence it satisfies

$$gcd(v_1, v_2, \ldots, v_{2N}) = 1.$$

If it is $(1^N, 0^N)$, then its length is $\sqrt{N}$. Otherwise there exists integers $k_1, \ldots, k_N$ such that

$$\mathbf{v} = \sum_{i=1}^{N} v_i \mathbf{b_i} + \sum_{j=1}^{N} k_j \mathbf{b_{N+j}}. \tag{6}$$

From equation (6), we can obtain the linear system (5). We see that in fact r does not divide $gcd(v_1, v_2, \ldots, v_N)$. We may assume that $(v_1, v_2, \cdots, v_N)$ is a nonzero vector whose ℓ_2 norm is less than $\sqrt{N}$. We want to solve the linear system for $(h_0, h_1, \cdots, h_{N-1}) \in (\mathbb{Z}/q\mathbb{Z})^N$. It follows from Lemma 1 that there are at most q solutions, hence

$$K(H|\mathbf{v}, L^{NTRU} \setminus H) \leq \log q + O(1) = O(\log(2N)).$$

We also have

$$K(H|L^{NTRU} \setminus H) = K(h|N,q) + O(1) \geq \gamma N,$$

and for some constant α

$$W(2N, \sqrt{\alpha N}) = 2^{(\gamma-\epsilon)N},$$

by Proposition 2. So by our main theorem $R \geq \sqrt{\alpha N}$.

In many implementations of the NTRU cryptosystem, S_f is set to be $T(d+1, d)$, S_g is set to be $T(d, d)$, where d is an integer close to $\lfloor N/3 \rfloor$. In this case, we calculate α. We first compute a lower bound of the Kolmogorov complexity of h if g is selected randomly in $T(d, d)$.

Lemma 2. *Assume that $d = \lfloor \beta N \rfloor$ for some constant $1/10 < \beta \leq 1/2$. For an invertible polynomial f, if we randomly select a polynomial g in $T(d, d)$, then with probability at least $1 - 2^{-0.1N}$, we have*

$$K(h|N, q) \geq \gamma N$$

for some constant γ, when N is large enough.

Proof. First observe that since f is invertible, we have

$$|K(g|N, q, f) - K(h|N, q, f)| = O(1),$$

and

$$K(h|N, q) \geq K(h|N, q, f).$$

The cardinality of the set $T(d, d)$ is

$$\binom{N}{d}\binom{N-d}{d} \geq \frac{2^{(-2\beta \log \beta - (1-2\beta)\log(1-2\beta))N}}{N^{O(1)}}.$$

So the lemma follows from Proposition 3 if we take $\gamma = -2\beta \log \beta - (1 - 2\beta)\log(1 - 2\beta) - 0.1$.

Corollary 1. *If $S_g = T(\lfloor N/3 \rfloor, \lfloor N/3 \rfloor)$, then with probability greater than $1 - 2^{-0.1N}$, the shortest vector in a random NTRU lattice has length greater than $\sqrt{0.28N}$.*

Proof. By Lemma 2, we can take γ to be 1.48. Then

$$W(2N, \sqrt{0.14 * 2N}) \approx 2^{1.48N} = e^{0.51 * 2N}.$$

Hence $R \geq \sqrt{0.28N}$.

The above corollary shows that with an overwhelming probability, the shortest vector in a random NTRU lattice is as long as the target vector, up to a constant factor. Note that if the target vector is the shortest vector, then $R = \sqrt{4d + 1} \approx \sqrt{4N/3}$. It is an interesting open problem to close the gap.

For some instantiations of NTRU variants [1, 17], the polynomial g is chosen from binary polynomials, and f is in a special form. Note that one can get a lower bound of the Kolmogorov complexity of g for whatever f is chosen by counting S_g. Hence if the specific chosen values of q and N meet the conditions in Lemma 1, then we can also get the lower bounds of the shortest vector lengths of the corresponding NTRU lattices by the same method. We express the observation in the following corollary:

Corollary 2. *If there exists a positive constant γ such that $|S_g| > 2^{\gamma N}$, then for any constant $0 < \epsilon < \gamma$, with probability greater than $1 - 2^{-\epsilon N}$, the shortest vector in a random NTRU lattice has length greater than $\sqrt{\alpha N}$, for a positive constant α depending only on γ and ϵ.*

5 Conclusion

In this paper, we propose a general method to bound the lengths of the shortest vectors in random integral lattices. We obtain that with an overwhelming probability, the shortest vector length of a random NTRU lattice has length $\Omega(\sqrt{N})$, which is the same as the length of the target vector, up to a constant factor. The main problem left open by this work is to prove that with a high probability, the target vector is shortest in a random NTRU lattice.

References

1. Consortium for efficient embedded security. efficient embedded security standards ♯1: Implementation aspects of ntruencrypt and ntrusign version 2. Technical report, NTRU Corporation, June 2003.
2. Miklos Ajtai. The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract). In *Proc. 30th ACM Symp. on Theory of Computing*, pages 10–19, 1998.
3. Miklos Ajtai. Random lattices and a conjectured 0-1 law about their polynomial time computable properties. In *FOCS2002*, pages 13–39, 2002.
4. J.-Y. Cai and A. Nerurkar. Approximating the svp to within a factor $(1+1/dim^{\epsilon})$ is NP-hard under randomized reductions. *J. of Comput. Syst. Sci.*, 59(2):221–239, 1999.
5. D. Coppersmith and A. Shamir. Lattice attacks on ntru. In *Eurocrypt 1997*, pages 52–61. Springer, 1997.
6. Matthijs J. Coster, Antoine Joux, Brian A. LaMacchia, Andrew M. Odlyzko, Claus-Peter Schnorr, and Jacques Stern. Improved low-density subset sum algorithms. *Computational Complexity*, 2(2):111–128, 1992.
7. Ishay Haviv and Oded Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. In *Proc. 39th ACM Symp. on Theory of Computing*, pages 469–477, 2007.
8. J. Hoffstein, J. Pipher, and J. Silverman. Ntru: a ring based public key cryptosystem. In *ANTS III*, pages 267–288, 1998.
9. A. W. Ingleton. The rank of circulant matrices. *J. London Math Soc.*, s1-31:445–460, 1956.
10. Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of ACM*, 52(5):789–808, 2005.
11. J. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. *Jounal of the Association for Computing Machinery*, 1985.
12. M. Li and P.M.B. Vitányi. *An Introduction to Kolmogorov Complexity and its Applications*. Springer-Verlag, 1993.
13. Rudolf Lidl and Harald Niederreiter. *Finite Fields (2nd ed.)*. Cambridge University Press, 1997.
14. J. E. Mazo and A. M. Odlyzko. Lattice points in high-dimensional spheres. *Monatsh. Math*, 110:47–61, 1990.
15. D. Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. *SIAM J. on Computing*, 30(6):2008–2035, 2001.
16. Phong Q. Nguyen and Damien Stehle. LLL on the average. In *ANTS VII*, pages 238–256. Springer-Verlag, 2006.

17. N.Howgrave-Graham, J.H. Silverman, and W.Whyte. Choosing parameter sets for ntruencrypt with naep and sves-3. In *CT-RSA 2005*, pages 118–135. Springer, 2005.
18. C. L. Siegel. A mean value theorem in geometry of numbers. *Annals of Mathematics*, 46:340–347, 1945.

A Appendix

Proof of Lemma 1

Proof. Since r is a primitive root modulo N, we have that

$$(x^N - 1)/(x - 1) = x^{N-1} + x^{N-2} + \cdots + 1$$

is an irreducible polynomial over $\mathbb{F}_r$ [13]. To determine the size of the solutions of (5), We need to study the circulant matrix

$$V = \begin{pmatrix} v_1 & v_N & \cdots & v_2 \\ v_2 & v_1 & \cdots & v_3 \\ \vdots & \vdots & \ddots & \vdots \\ v_N & v_{N-1} & \cdots & v_1 \end{pmatrix} \tag{7}$$

Let ω be the N-th primitive root of unit in the algebraic closure of $\mathbb{F}_r$. One can verify that

$$V \begin{pmatrix} 1 \\ \omega^i \\ \omega^{2i} \\ \vdots \\ \omega^{(N-1)i} \end{pmatrix} = (v_1 + v_N\omega^i + \cdots + v_2\omega^{(N-1)i}) \begin{pmatrix} 1 \\ \omega^i \\ \omega^{2i} \\ \vdots \\ \omega^{(N-1)i} \end{pmatrix}$$

for $0 \le i \le N-1$. Thus for some i, if $v_1 + v_N\omega^i + \cdots + v_2\omega^{(N-1)i}$ is not zero, then it is an eigenvalue of V with the eigenvector $(1, \omega^i, \omega^{2i}, \cdots, \omega^{(N-1)i})$. Hence if d elements in $\{1, \omega, \omega^2, \cdots, \omega^{N-1}\}$ are zeros of the polynomial $v_N + v_{N-1}x + \cdots + v_1x^{N-1}$, then the rank of V is $N - d$ over $\mathbb{F}_r$ [9]. Since $v_1, \cdots, v_N$ can not be all 1, we have

$$\prod_{1 \le i \le N-1} (v_1 + v_N\omega^i + \cdots + v_2\omega^{(N-1)i})$$

is a nonzero element in $\mathbb{F}_r$. To solve (5), we first compute the Hermite Normal Form H of V through a sequence of elementary row transformations. Now we do a case analysis based on the value of $v_1 + v_2 + \cdots + v_N$.

Case 1: If

$$v_1 + v_2 + \cdots + v_N \neq 0 \pmod{r},$$

then V is non-singular over $\mathbb{F}_r$, thus there is no multiple of r in the diagonal line of H, we can recover $(h_0, h_1, \ldots, h_{N-1})$ from $\mathbf{v}$, and there is one unique solution.

Case 2: If

$$v_1 + v_2 + \cdots + v_N = 0 \pmod{r},$$

but

$$v_1 + v_2 + \cdots + v_N \neq 0,$$

then V is non-singular over $\mathbb{Q}$ but is singular over $\mathbb{F}_r$. Let r^t be the largest power of r which divides $v_1 + v_2 + \cdots + v_N$. We have $r^t \leq N < q$, and r^t is the largest power of r which divides the product of all the diagonal elements in H. The solution space of (5) has size at most $r^t < q$.

Case 3: In the last case,

$$v_1 + v_2 + \cdots + v_N = 0,$$

the rank of V over $\mathbb{F}_r$ is $N - 1$, and the first $N - 1$ rows of V are independent over $\mathbb{F}_r$. Thus the solution space of (5) has size at most q.