Course Report: Advanced topics in cryptography

On Approximating the Covering Radius and Finding Dense Lattice Subspaces

Shucheng Chi, Benyu Wang, Tianle Xie

December 26, 2022

1 Covering Radius and Kannan-Lovasz Conjecture

1.1 Integer Programming

As a motivation of this section, integer programming is a classical algorithmic problem, which has the form

$$\max cx,$$
$$\text{subject to } Ax \leq b, \quad x \geq 0, \quad x \in \mathbb{Z}^n.$$

In practice, what we always do is to relax the integer program to a linear program, and round its solution to get an approximation result. However, to give an exact solution to IP is NP-hard, and the best known algorithm [Kan87] works in time $n^{O(n)}$. In this report we will introduce [Dad19] algorithm that works in time $2^{O(n)}$.

A natrual way to solve IP is to enumerate all the feasible integer points.

1.2 Covering Radius and Kannan-Lovasz Conjecture

Definition 1.1. $\mu(K, \mathbb{Z}^n) :=$ the smallest s s.t. for any $t \in \mathbb{R}^n$, $sK + t$ contains an integer point.

This is equivalent to say that if we put a copy of sK on each integer point, the whole space is covered, where the name "covering radius" comes from.

When the covering radius is small, meaning the region is fat, it is easy to find a lattice point via approximate CVP from the center. When the covering radius is large, however, we should try to decrease it via projection to lower dimension.

Theorem 1.2. *[KL86] If $\mu(K, \mathbb{Z}^n) \geq 1$, there exists a projection $P \in \mathbb{Z}^{k \times n}$ s.t.*

$$vol_k(PK) \leq n^k.$$

This implies $2^{O(n)}n^n$ time algorithm for IP, and their conjecture is $vol_k(PK) \leq (\log n)^k$, i.e.

Conjecture 1.3 (Kannan-Lovasz)**.**

$$1 \leq \mu(K, \mathbb{Z}^n) \min_{P \in \mathbb{Z}^{k \times n}} vol_k(PK)^{1/k} \leq O(\log n),$$

which implies $2^{O(n)}(\log n)^n$ time algorithm for IP.

1.3 Covering Radius in Lattice

We can generalize definition 1.1 from integer points to lattice points, with the form $\mu(K, \mathcal{L})$. We define the covering radius of $\mathcal{L}$ to be

$$\mu(\mathcal{L}) := \mu(B_2^n, \mathcal{L}).$$

There is another way to define it which is more tracktable. Let the Voronoi cell of $\mathcal{L}$ consists of all the points that are closer to the origin than any other lattice point, i.e.

$$V(\mathcal{L}) := \{x \in \mathbb{R}^n \mid \|x\| < \|x - y\|, \forall y \in \mathcal{L}\},$$

and $\mu(\mathcal{L})$ is the radius of the smallest ball that covers the Voronoi cell.

Claim 1.4.

$$vol(\mu(\mathcal{L})B_2^n) \geq vol(V) = det(\mathcal{L}).$$

Then we get $\mu(\mathcal{L}) \geq vol(B_2^n)^{-1/n} det(\mathcal{L})^{1/n}$, or roughly $\mu(\mathcal{L}) \geq \sqrt{n}\ det(\mathcal{L})^{1/n}$.

A linear subspace $W \subset \mathbb{R}^n$ is a **lattice subspace** of $\mathcal{L}$ if W admits a basis in $\mathcal{L}$, i.e. $W = span(\mathcal{L} \cap W)$. Let $\mathcal{L}/W := \pi_{W^\perp}(\mathcal{L})$ denote the lattice projected orthogonal to W.

When projected to lower dimension, the covering radius decreases, so

$$\mu(\mathcal{L}) \geq \max_W \mu(\mathcal{L}/W) \geq \max_{dim(w)=k} \sqrt{k}\ det(\mathcal{L}/W)^{1/k}.$$

1.4 l_2- Kannan-Lovasz Conjecture

Let $C_{KL,2}(n)$ be the smallest number s.t.

$$\mu(\mathcal{L}) \leq C_{KL,2}(n) \max_{dim(w)=k} \sqrt{k}\ det(\mathcal{L}/W)^{1/k},$$

for all lattices $\mathcal{L}$ with dimension no larger than n.

- $C_{KL,2}(n) = \Omega(\sqrt{\log n})$. Choose lattice generated by $e_1, \frac{1}{\sqrt{2}}e_2, \cdots, \frac{1}{\sqrt{n}}e_n$.
- $\sqrt{n}$. [KL86]
- $\log^{3/2}(n)$. By Reverse Minkovski Theorem. [RSD17]

Can find W s.t. $\mu(\mathcal{L}) \leq O(\log^{5/2}(n))\sqrt{k}\ det(\mathcal{L}/W)^{1/k}$, in $2^{O(n)}$ time w.h.p. [Dad19]

2 Finding Dense Lattice Subspace

2.1 Canonical Polytype and Canonical Filtration

Let $\mathcal{L}$ be a lattice. For any of its lattice subspace M, draw a point $(dim(M), \log det(M))$ on the $x-y$ plane. Now the **cannonical polytype** of $\mathcal{L}$ is defined as the lower convex hull of these points, starting from $(0, 0)$. Denote this chain by L_0 (the trivial lattice), $L_1, L_2, \cdots, L_m$. Surprisingly, these lattices form a chain $L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_m$. This is called the **cannonical filtration**.

If the cannonical filtration is trivial, i.e the chain is $0 \subset \mathcal{L}$, we call this a stable lattice. Obeserve that in a general cannonical filtration, each slope L_{i+1}/L_i is stable, and the slope is increasing, i.e. $nd(L_i/L_{i-1}) < nd(L_{i+1}/L_i)$. Here $nd(\mathcal{L}) := det(\mathcal{L})^{1/dim(\mathcal{L})}$ means the normalized determinant.

2.2 Covering Radius based on Canonical Filtration

- For an n-dimensional stable lattice $\mathcal{L}$, [RSD17]

  $$\mu(\mathcal{L}) \leq L_n \sqrt{n}\; nd(\mathcal{L}).$$

  L_n is some constant related with the slicing of Voronoi cell. They show that $L_n = O(\log n)$.

- For a canonnical filtration $L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_m$,

  $$\mu(\mathcal{L}) \leq \sum_{i=1}^{m} \mu(L_i/L_{i-1})^2 \leq \log n \; {L_n}^2 \max_k dim(\mathcal{L}/L_k) nd(\mathcal{L}/L_k)^2.$$

2.3 Algorithm for Finding a Dense Lattice Subspace

Problem: Find a lattice subspace $M \subset \mathcal{L}$ with the smallest nd.

This means finding the point with the smallest slope in the $dim - logdet$ diagram, or in other words, the L_1 in the canonical filtration.

We give an approximate algorithm, which is straight forward but its analysis requires reverse Minkovski theorem.

Theorem 2.1. *[Dad19] Algorithm 1 can compute a dense lattice subspace with $O(\log n)$ approximate rate, in $2^{O(n)}$ time with high probability.*

Algorithm 1 Algorithm for Finding a Dense Lattice Subspace

```
procedure DenseSubLat(($\mathcal{L}, \varepsilon$))
    Input: Lattice $\mathcal{L}$, dimension $n$, error parameter $\varepsilon > 0$.
    if $n \geq 2$ then
        Sample $X$ within statistical distance $\frac{\varepsilon}{2^n}$ from discrete Guassian distribution $D_{nd(\mathcal{L})\mathcal{L}^*/2}$.
        if $X \neq 0$ then
            $M :=$ DenseSubLat($\mathcal{L} \cap X^{\perp}, \varepsilon$)
            if $nd(M) < nd(\mathcal{L})$ then
                return $M$
            end if
        end if
    end if
    return $\mathcal{L}$
end procedure
```

References

[Dad19] D. Dadush. On approximating the covering radius and finding dense lattice subspaces. In *Symposium on the Theory of Computing*, 2019. 1, 2, 3

[Kan87] R. Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research*, 12(3):415–440, 1987. 1

[KL86] R. Kannan and L Lovász. Covering minima and lattice-point-free convex bodies. In *Foundations of Software Technology and Theoretical Computer Science, Sixth Conference, New Delhi, India, December 18-20, 1986, Proceedings*, 1986. 1, 2

[RSD17] O. Regev and N. Stephens-Davidowitz. A reverse minkowski theorem. *ACM*, 2017. 2, 3