An approximate deep hole algorithm based on dual HKZ-bases of lattices

Wen-Wen Wang and Ke-Wei Lv†

State Key Laboratory of Information Security,
Institute of Information Engineering,
Data Assurance Communication Security Research Center ,
Chinese Academy of Sciences,Beijing 100093,
China .University of Chinese Academy Sciences,
Beijing 100049, China. E-mail: wangwenwen@iie.ac.cn

We present a deterministic algorithm in time on input a dual HKZ-basis of a latticeof rank n to find a point whose distance from at least , where is an integer, , is the input size, and is covering radius of . This provides a method to approximately find a deep hole. Furthermore, we study the relation between the covering radius and successive minima in any norms which extends Haviv's result to .

Keywords: lattice; Covering Radius; dual HKZ-bases; successive minima.

1. Introduction

The Covering Radius Problem (CRP) is an important lattice problem. Computing the covering radius of a lattice is a classic problem in the geometry of numbers. In 2004, Micciancio [1] showed that finding collision of some hash function can be reduced to approximate Covering Radius Problem of lattice. Guruswami, Micciancio, and Regev [2] initiated the study for computation complexity of the CRP, and showed that lies in AM, lies in . Peikert[3] showed that lies in coNP in the norm for . The first hardness result of CRP was presented by Haviv and Regev, they obtained there exists some constant such that the problem is -hard in the norm for any suffintly large value of p [4]. In 2013, Micciancio and Voulgaris[5] gave a deterministic time algorithm to solve all the important lattice problems in NP including the Shortest Vector Problem (SVP) [6]and the Closest Vector Problem (CVP). Then, using a randomized polynomial time reduction from CVP to CRP in [2], can be approximately solved in single exponential time. Using the algorithm for Voronoi cell in [5], we can compute the exact value of the covering radius by enumerating all the vertices of the Voronoi cell and selecting the longest. In 2015, Haviv[7] proposed the Remote Set Problem (RSP) on lattices and proved that the relations between the covering radius and the nth successive minimum in norms for .

Kannan[8] computed a shortest vector in lattice within the time basing on HKZ-bases. Blömer[9] solved CVP in time basing on dual HKZ-bases.

A point in the span of a lattice at distance the covering radius from the lattice is called deep hole. How to find an approximate deep hole is an interesting problem. In this paper, we will use the algorithm closest vector based on dual HKZ-bases of lattice to solve the problem. From[2], we have a construction to find a point quite far from a lattice which is the linear combinations of basis vectors with coefficient in . By this construction, we knew that there exits at least one point quite far from a lattice. We will give a new algorithm to find the point. The algorithm that we give is to find a point in time whose distance from is at least, where n is the rank of the lattice. Indeed, basing on the construction of [2], we can have target vectors. Using the algorithm for CVP based on a dual HKZ-basis, for each target vector, we can find a lattice vector closest to it. Then, we can obtain a maximum distance that must be at least . The relation of CRP and other lattice problem have known is very little. We use the triangle inequality of norms and Hölder's Inequality to get the connection between the covering radius and the successive minima in any l_p norm.

2. Preliminaries

A lattice of rank n is the set of all linear combinations generated by n linearly independent vectorin .The ith minimum of is the smallest value such that contains linearly independent lattice vectors.

Definition 2.1.(Covering Radius). For every , the covering radius is defined as the maximum distance : . A deep hole of is a point at distance from . For p=2, we set = .

Lemma2.2.([2]). For every , any basis and an integer , there exists a point such that {0, 1/M,⋯,(M-1)/M} for all , and (1-1/M).

For a lattice with basis, its dual lattice.If is satisfying

(1)

then is a basis of called a dual basis of . For a basis of lattice , we define their Gram-Schmidt orthogonalized vector byfor, wherefor .For a lattice , we define projection operations from onto by.In particular,.is a lattice of rank .

Definition2.3.A basis of a lattice is called a HKZ-basis if for , and is a shortest non-zero vector in , for , i.e., .

If the dual basis is an HKZ-basis of the dual lattice , then a basis of a lattice is also a dual HKZ-basis. By [9], we know that, if is a dual HKZ-basis for, then is a dual HKZ-basis for ,.By this, we can use induction in Theorem 3.2 of section3 .

It is well-known that for two different norms and on vector space, we have the follwing inequalities.

Theorem 2.5.(Hölder's Inequality).For any vector, the following inequalities hold:

- *for any , ,*
- *for any ,,*
- *for ,.*

3. An Approximate Deep Hole Algorithm Based on dual HKZ-Bases

We give a new algorithm to find a deterministic point far from the lattice. Our technique uses the algorithm for CVP based on dual HKZ-bases to find a lattice vector closest to a target vector, and then, we can find the point.

Lemma 3.1.([9])Let be a lattice of rankwith dual HKZ-basis and letbe a vector in ,, . If, , is a vector in closest to , then n/2.

Theorem 3.2.For an integer , there is a deterministic -time algorithm that on input a dual HKZ-basis , outputs a exact point has distance from a lattice at least, where b is the input size, is the rank of the lattice.

Proof. Basing on Lemma 2.2, we construct a set where, , runs over , . So there exists a for some a such that 1/M.Now we prove that the Algorithm 1in Table 1 can find the vector.

We construct vectors corresponding to respectively. Then, a vector is fixed and let for some . We need to prove the Algorithm 1 which on input a dual HKZ-basis of the lattice and a target vector where , outputs a vector in closest to . We prove the algorithm by induction on the rank n of lattice. For , the Algorithm1 correctly computer closest to , . We know that is a dual HKZ-basis for, by induction assumption, the recursions compute a vector in closest to the target vector ,where is the orthogonal projection of into span . By Lemma 3.1,, we have . For a fixed , there exists such that For any vector of form , ,the distance from to is. Since is independent of , there exists a vector such that. Hence, in closest to that is closest to. Then, we can choose a fix such that a vector in is closest to , that is,, where .

For a fixed , we can compute a vector in closest to vector Then, for all , we exactly compute the distance from to lattice . So, for some and , we have . Let ,for some , if ,we set and . By Lemma 2.2, we find the vector such that (1-1/M).

By Lemma 3.1, we haven/2. In recursions, finding a closest vector to the target vector costs time . We construct vectors , this costs running time of in total.□

By [9], given a lattice of rank *n* and its representation size *b*, computing HKZ-bases costs time . So we get the following result.

Theorem3.3.For an integer M>0, there is a deterministic -time algorithm that on input lattice of rank n, outputs a exact point, which has distance from at least (1-1/M), where is the input size.

4. The Covering Radius and the nth Successive Minimum

We prove the relations between covering radius and the n-th successive minimum. This extends Haviv's result for to . Theorem4.1.For any and a lattice of rank n, .

Proof. Let be a basis of lattice . We have for .By Lemma 2.2, there exists a point such that for all , {0,1/M,⋯,(M-1)/M} and (1-1/M).So .

Using the Hölder's Inequality, we can obtain the following relations between the covering radius and the nth successive minimum in norms for

Corollary 4.2.*For any and lattice of rank n and dimension m, . Specially, for any full-rank lattice, . And for any, .*

5. Conclusion

In our paper, basing on a dual HKZ-basis of a lattice, we give a deterministic algorithm in time that can find a point quite far from a lattice, we can exactly find the deep hold when . Using the norm triangle inequality and Hölder's Inequality, we prove the relations between the covering radius and the nth successive minimum in norms for and this extends Haviv's result. By the relations between the HKZ-bases and the successive minimum, we get the relations in norm. Here, we use dual HKZ-bases, whose computation costs at least as far as we know. So it is an interesting whether there exists more efficient deterministic algorithm to solve approximately deep hole problem.

Appendix

Table 1. Algorithm 1- Deep-Hole Algorithm based on dual HKZ-bases.

Input: A dual HKZ-basis of a lattice.
Output: A point which is at least l/M far from .
1.
2.Let , where , , take over all the value of .
3.if then
4.Compute . /* is a vector in closest to */
5.Compute .
6.else
7.for
8.fork/2k/2.
9.compute the orthogonal projection of onto
10.compute a vector in closest to the target vector .
11.
12.
13. if then .
14. return .

Acknowledgement

This work is supported by National Natural Science Foundation of China (Grant No.61272039).

References

1. D. Micciancio, *Almost Perfect Lattices, the Covering Radius Problem, and Applications to Ajtai's Connection Factor*,(SIAM J. Comput.,2004), pp. 118-169.
2. V. Guruswami, D. Micciancio, and O. Regev, *The complexity of the covering radius problem*,Vol.14 (Computational Complexity, 2005), pp.90-121.
3. C. Peikert, *Limits on the Hardness of Lattice Problems in l_p Norms*, Vol.17 (Computational Complexity, 2008), pp. 300-351.
4. I. Haviv and O. Regev, *Hardness of the Covering Radius Problem on Lattices*, Vol.4(Chicago J. Theoretical Computer Science, 2012), pp. 1-12.
5. D. Micciancio, P. Voulgaris, *A Deterministic Single Exponential Time Algorithm for Most Lattice Problems Based on Voronoi Cell Computation*, Vol.42 (SIAM J.COMPUT, 2013), pp. 1364-1391.

6. W. Wang, K. Lv, On promise problem of the Generalized Shortest Vector Problem, in Proc.*Information and Communications Security (ICICS'15)*,(Beijing, China, 2015).
7. I. Haviv, *The Remote Set Problem on Lattice*, Vol. 24 (Computational Complexity, 2015), pp.103-131.
8. R.Kanna, *Minkowski's Convex Body Theorem and Integer Programming*,Vol. 12 (Mathematics of Operations Research, 1987), pp.415-440.
9. J. Blömer, Closest vector, Successive Minima, and Dual HKZ-Bases of Lattices,in proc. *International colloq. on AutomataLanguages and Programming,(IACLP'00)*,(Geneva, Switzerland ,2000).