Covering Radius of Two-dimensional Lattices*

Yupeng Jiang, Yingpu Deng, Yanbin Pan
Key Laboratory of Mathematics Mechanization,
Academy of Mathematics and Systems Science,
Chinese Academy of Sciences, Beijing 100190, P.R. China

Abstract

The covering radius problem in any dimension is not known to be solvable in nondeterministic polynomial time, but when in dimension two, we give a deterministic polynomial time algorithm by computing a reduced basis using Gauss' algorithm in this paper.

Keywords: Lattice-based cryptography, Deep hole, Covering radius, Gauss' algorithm

1 Introduction

The covering radius of a lattice Λ in Euclidean space, denoted by $\rho(\Lambda)$, is defined as the smallest radius ρ such that the closed spheres of radius ρ centered at all lattice points cover the entire space, i.e., any point in $\mathrm{span}(\Lambda)$ is within distance ρ from the lattice. The covering radius problem is to find $\rho(\Lambda)$ for a given lattice Λ. To solve this problem we need to find a point in $\mathrm{span}(\Lambda)$ at distance $\rho(\Lambda)$ from the lattice, a so called deep hole. However, given a point $\boldsymbol{t} \in \mathrm{span}(\Lambda)$, computing the distance of $\boldsymbol{t}$ from Λ is not easy than CVP (Closest Vector Problem), which is NP-complete [8], and then we should compare all the distance when $\boldsymbol{t}$ ranges over $\mathrm{span}(\Lambda)$. So the (exact) covering radius problem is in Π_2 at the second level of the polynomial hierarchy, a presumably strictly bigger class than NP.

Lattices have been widely used in cryptology, both in cryptanalysis [2] and cryptography [1][5]. Micciancio [7] reduced finding collisions of some hash function to GapCRP (approximate Covering Radius Problem) of lattices. Fukshansky and Robins [3] and Kannan [6] related Frobenius problem with the covering radius of a lattice with respect to a given input norm (different from the Euclidean one) defined by a convex polytope specified as a system of linear inequalities. Guruswami, Micciancio and Regev [4] showed that, for an n-dimensional lattice, $\mathrm{GapCRP}_{\gamma(n)}$ lie in AM for $\gamma(n) = 2$, in coAM for $\gamma(n) = \sqrt{n/\log n}$, and in $\mathsf{NP} \cap \mathsf{coNP}$ for $\gamma(n) = \sqrt{n}$.

So it is interesting to find a polynomial time algorithm for the covering radius of a lattice with low dimension under the Euclidean norm. In this paper, for a two-dimensional lattice with given basis, we first use the polynomial time Gauss' algorithm [8] to obtain a reduced basis, then we prove a theorem concerning the deep holes of the lattice for which it can be easily found. Further the covering radius of the lattice is obtained.

*Supported by the NNSF of China (No. 60821002)

2 Closest Lattice Points

Let m be a positive integer, $\mathbb{R}^m$ the m-dimensional Euclidean space consisting of m-tuples $(x_1, \ldots, x_m)$ where each $x_i \in \mathbb{R}$ for $1 \leqslant i \leqslant m$. For $\boldsymbol{x} = (x_1, \ldots, x_m)$, $\| \boldsymbol{x} \| = \sqrt{x_1^2 + \ldots + x_m^2}$ is the Euclidean norm. Vectors considered in this paper are all in $\mathbb{R}^m$.

Let $\boldsymbol{a}, \boldsymbol{b}$ be two linearly independent vectors in $\mathbb{R}^m$. The two-dimensional lattice Λ generated by $\boldsymbol{a}$ and $\boldsymbol{b}$ is the set $\Lambda = \{i\boldsymbol{a} + j\boldsymbol{b} \mid i, j \in \mathbb{Z}\}$ and $[\boldsymbol{a}, \boldsymbol{b}]$ is called a basis of the lattice. According to [8], a lattice basis $[\boldsymbol{a}, \boldsymbol{b}]$ is reduced if

$$\| \boldsymbol{a} \|, \| \boldsymbol{b} \| \leqslant \| \boldsymbol{a} + \boldsymbol{b} \|, \| \boldsymbol{a} - \boldsymbol{b} \| .$$

Geometrically, this definition means that the diagonals of the fundamental parallelogram associated to the basis of the lattice are at least as long as the edges. It is well known that there is a polynomial time algorithm known as Gauss' algorithm, from any basis of a two-dimensional lattice, we can obtain a reduced basis of the same lattice(see [8]). We first introduce two lemmas which can be used on this kind of basis.

Lemma 2.1. *[8] Consider three vectors on a line, $\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{y}$, and $\boldsymbol{x}+\alpha\boldsymbol{y}$, where $\alpha \in [1, \infty)$. If $\| \boldsymbol{x} \| \leqslant \| \boldsymbol{x} + \boldsymbol{y} \|$, then $\| \boldsymbol{x} + \boldsymbol{y} \| \leqslant \| \boldsymbol{x} + \alpha\boldsymbol{y} \|$.*

Lemma 2.2. *The conditions are as above Lemma 2.1. If $1 \leqslant \alpha < \beta$, then $\| \boldsymbol{x} + \alpha\boldsymbol{y} \| \leqslant \| \boldsymbol{x} + \beta\boldsymbol{y} \|$.*

Proof. For $\alpha = 1$, this is just Lemma 2.1. Now suppose $\alpha > 1$. By Lemma 2.1, we have $\| \boldsymbol{x} + \boldsymbol{y} \| \leqslant \| \boldsymbol{x} + \alpha\boldsymbol{y} \|$. We set $\boldsymbol{X} = \boldsymbol{x} + \boldsymbol{y}$ and $\boldsymbol{Y} = (\alpha - 1)\boldsymbol{y}$. Hence $\| \boldsymbol{X} \| \leqslant \| \boldsymbol{X} + \boldsymbol{Y} \|$. Since $\frac{\beta-1}{\alpha-1} > 1$, by Lemma 2.1, we have

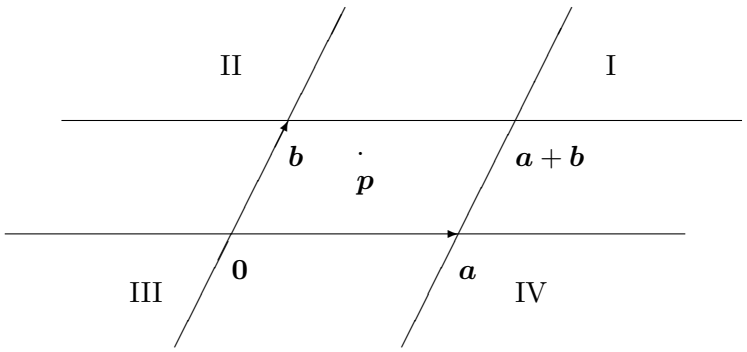
$$\| \boldsymbol{X} + \boldsymbol{Y} \| \leqslant \| \boldsymbol{X} + \frac{\beta - 1}{\alpha - 1}\boldsymbol{Y} \| .$$

This is just $\| \boldsymbol{x} + \alpha\boldsymbol{y} \| \leqslant \| \boldsymbol{x} + \beta\boldsymbol{y} \|$. □

Then we can get the main theorem by using the above lemmas.

Theorem 2.3. *Let $[\boldsymbol{a}, \boldsymbol{b}]$ be a reduced basis of Λ, then for every point in the area $\{s\boldsymbol{a}+t\boldsymbol{b} \mid 0 \leqslant s,t < 1\}$, the closest lattice point from it must be one of $\boldsymbol{0}$, $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{a} + \boldsymbol{b}$.*

Proof. Divide the lattice points into four parts I, II, III, IV each with one of the four points as a vertex respectively(see the figure below).



Then for each $\boldsymbol{p} \in \{s\boldsymbol{a} + t\boldsymbol{b} \mid 0 \leqslant s, t < 1\}$,

$$dist(\boldsymbol{p}, \Lambda) = min\{dist(\boldsymbol{p}, I), dist(\boldsymbol{p}, II), dist(\boldsymbol{p}, III), dist(\boldsymbol{p}, IV)\}.$$

When $\boldsymbol{p} \in \{s\boldsymbol{a} + t\boldsymbol{b} \mid 0 \leqslant s, t < 1\}$, if we have $dist(\boldsymbol{p}, I) = dist(\boldsymbol{p}, \boldsymbol{a} + \boldsymbol{b}), dist(\boldsymbol{p}, II) = dist(\boldsymbol{p}, \boldsymbol{b}), dist(\boldsymbol{p}, III) = dist(\boldsymbol{p}, \boldsymbol{0}), dist(\boldsymbol{p}, IV) = dist(\boldsymbol{p}, \boldsymbol{a})$, then we get the theorem. Let $\boldsymbol{p} = s\boldsymbol{a} + t\boldsymbol{b}, 0 \leqslant s, t < 1$. First we prove all these reduce the following fact

$$\| (1-u)\boldsymbol{a} + (1-v)\boldsymbol{b} \| \leqslant \| (m-u)\boldsymbol{a} + (n-v)\boldsymbol{b} \|, m, n \in \mathbb{Z}_{\geqslant 1}, 0 \leqslant u, v \leqslant 1. \tag{2.1}$$

Since I=$\{m\boldsymbol{a} + n\boldsymbol{b} \mid m, n \in \mathbb{Z}, m, n \geqslant 1\}$, $dist(\boldsymbol{p}, I) = dist(\boldsymbol{p}, \boldsymbol{a} + \boldsymbol{b})$ means that $\| (1-s)\boldsymbol{a} + (1-t)\boldsymbol{b} \| \leqslant \| (m-s)\boldsymbol{a} + (n-t)\boldsymbol{b} \|$. Since II=$\{m\boldsymbol{a} + n\boldsymbol{b} \mid m, n \in \mathbb{Z}, m \leqslant 0, n \geqslant 1\}$, $dist(\boldsymbol{p}, II) = dist(\boldsymbol{p}, \boldsymbol{b})$ means that $\| (1-(1-s))(-\boldsymbol{a}) + (1-t)\boldsymbol{b} \| \leqslant \| ((1-m)-(1-s))(-\boldsymbol{a}) + (n-t)\boldsymbol{b} \|$. Since III=$\{m\boldsymbol{a} + n\boldsymbol{b} \mid m, n \in \mathbb{Z}, m, n \leqslant 0\}$, $dist(\boldsymbol{p}, III) = dist(\boldsymbol{p}, \boldsymbol{0})$ means that $\| (1-(1-s))\boldsymbol{a} + (1-(1-t))\boldsymbol{b} \| \leqslant \| ((1-m)-(1-s))\boldsymbol{a} + ((1-n)-(1-t))\boldsymbol{b} \|$. Since IV=$\{m\boldsymbol{a} + n\boldsymbol{b} \mid m, n \in \mathbb{Z}, m \geqslant 1, n \leqslant 0\}$, $dist(\boldsymbol{p}, IV) = dist(\boldsymbol{p}, \boldsymbol{a})$ means that $\| (1-s)\boldsymbol{a} + (1-(1-t))(-\boldsymbol{b}) \| \leqslant \| (m-s)\boldsymbol{a} + ((1-n)-(1-t))(-\boldsymbol{b}) \|$. Because $[\boldsymbol{a}, \boldsymbol{b}]$ is reduced, then $[-\boldsymbol{a}, \boldsymbol{b}]$ and $[\boldsymbol{a}, -\boldsymbol{b}]$ are also reduced. Therefore, to obtain the theorem, we only need to prove (2.1).

When $m = n = 1$, it's trivial. When $m = 1, n \geqslant 2$, if $u = 1$, it is trivial. Suppose $u < 1$. As $\frac{n-v}{1-u} > \frac{1-v}{1-u}$, if $\frac{1-v}{1-u} \geqslant 1$, then by Lemma 2.2, we have

$$\| \boldsymbol{a} + \frac{1-v}{1-u}\boldsymbol{b} \| \leqslant \| \boldsymbol{a} + \frac{n-v}{1-u}\boldsymbol{b} \| .$$

Multipling by $1-u$ on both sides then we obtain

$$\| (1-u)\boldsymbol{a} + (1-v)\boldsymbol{b} \| \leqslant \| (1-u)\boldsymbol{a} + (n-v)\boldsymbol{b} \| .$$

If $0 \leqslant \frac{1-v}{1-u} < 1$, sine $\| \boldsymbol{a} \| \leqslant \| \boldsymbol{a} + \boldsymbol{b} \|$, we have $\| \boldsymbol{a} + \frac{1-v}{1-u}\boldsymbol{b} \| = \| (1 - \frac{1-v}{1-u})\boldsymbol{a} + \frac{1-v}{1-u}(\boldsymbol{a} + \boldsymbol{b}) \| \leqslant (1 - \frac{1-v}{1-u}) \| \boldsymbol{a} \| + \frac{1-v}{1-u} \| \boldsymbol{a} + \boldsymbol{b} \| \leqslant \| \boldsymbol{a} + \boldsymbol{b} \| \leqslant \| \boldsymbol{a} + \frac{n-v}{1-u}\boldsymbol{b} \|$. The last inequality follows from Lemma 2.1, as $\frac{n-v}{1-u} \geqslant 1$. This completes the proof for the case $m = 1$ and $n \geqslant 2$.

When $m \geqslant 2, n = 1$, the proof is the same. We only left when $m \geqslant 2, n \geqslant 2$. If $\frac{n-v}{m-u} \geqslant 1$, since $\frac{n-v}{m-u} > \frac{n-1-v}{m-u}$, then similar to the above proof we have $\| (m-u)\boldsymbol{a} + (n-v)\boldsymbol{b} \| \geqslant \| (m-u)\boldsymbol{a} + (n-1-v)\boldsymbol{b} \|$. If $0 < \frac{n-v}{m-u} < 1$, then $\frac{m-u}{n-v} > 1$. Similarly, we have $\| (m-u)\boldsymbol{a} + (n-v)\boldsymbol{b} \| \geqslant \| (m-1-u)\boldsymbol{a} + (n-v)\boldsymbol{b} \|$. Therefore we always have $\| (m-u)\boldsymbol{a} + (n-v)\boldsymbol{b} \| \geqslant \min(\| (m-u)\boldsymbol{a} + (n-1-v)\boldsymbol{b} \|, \| (m-1-u)\boldsymbol{a} + (n-v)\boldsymbol{b} \|)$. So we can reduce the case (m, n) to $(m-1, n)$ or to $(m, n-1)$. Continuing this process, we can reduce to $m = 1$ or $n = 1$ ultimately. This completes the proof of the theorem. □

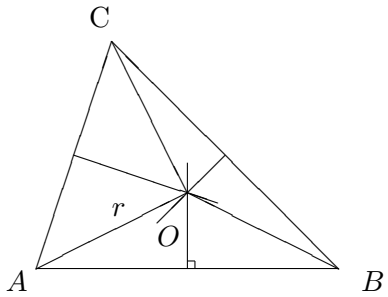
Using the result of the above theorem, for a given point of span(Λ), the closest lattice point from it must be a vertex of the parallelogram it locates. What left to do is to find the smallest radius such that the closed circles centered at vertices of the parallelogram cover the parallelogram.

3 Covering the Parallelogram

Let's define covering radius and deep hole for a polygon. The covering radius is the smallest radius such that the closed circles centered at vertices cover the polygon and the deep hole is the points as far as possible from the vertices. We have the following lemma.

Lemma 3.1. *For an acute (right) triangle, the deep hole is its circumcenter and the covering radius is the radius of its circumcircle.*

Proof. First consider acute triangle. As the following figure shows, denoted O to be the circumcenter of $\triangle ABC$ and r the radius of its circumcircle.

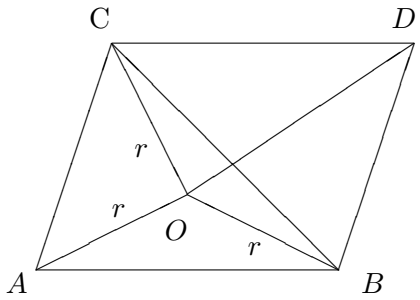


Because $\triangle ABC$ is an acute triangle, O is in $\triangle ABC$. Since $\mid OA \mid = \mid OB \mid = \mid OC \mid = r$, the covering radius is at least r. In the figure the triangle is divided into six small right triangles with hypotenuse length r, and each point in a small triangle has distance at most r from the corresponding vertex of the big triangle. So the covering radius is r and the circumcenter is the deep hole. When the triangle is right, the proof is similar and more simple, and the deep hole is the middle point of the hypotenuse. □

Let $[\boldsymbol{a}, \boldsymbol{b}]$ be a reduced basis. We can set the angle of $\boldsymbol{a}$ and $\boldsymbol{b}$ to be acute(right), for else let $-\boldsymbol{b}$ instead of $\boldsymbol{b}$, then the fundamental parallelogram generated by it can be divided into two congruent acute(right) triangle, and we have the following theorem.

Theorem 3.2. *Suppose we have a parallelogram generated by a reduced basis as the above. Then its deep holes are the deep holes of the two acute (right) triangles and its covering radius is the covering radius of the triangles.*

Proof. As the following figure shows that, in parallelogram $ABDC$, $\angle BAC$ is acute(or right), because of $\mid BC \mid \geqslant \mid AB \mid, \mid BC \mid \geqslant \mid AC \mid$, so $\angle BAC$ is the biggest angle of $\triangle ABC$ and $\triangle ABC$ is an acute(or a right) triangle. Again let O, r denote its deep hole and covering radius.



By Lemma 3.1, the covering radius of the parallelogram is at most r. For closed circles centered at A, B, C with radius r can cover $\triangle ABC$, and closed circles centered at B, C, D with radius r can also cover $\triangle BCD$. We have $\mid OA \mid = \mid OB \mid = \mid OC \mid = r$. If $\mid OD \mid \geqslant r$, then by Theorem 2.3 the covering radius is r. Let's assume $\mid OD \mid < r$, then $\angle ODC > \angle OCD, \angle ODB > \angle OBD$, so

$$\angle BDC = \angle ODC + \angle ODB > \angle OCD + \angle OBD \geqslant \angle BCD + \angle CBD = \angle ABD.$$

But we have $\angle BDC + \angle ABD = \pi$, so $\angle BDC > \pi/2$, contradicting with $\angle BAC$ is acute(right). Moreover, when $\angle BAC$ is right, then the two deep holes coincide, and the deep hole is the center of the parallelogram. The proof is completed. □

4 Algorithm

By the above Theorem 3.2, we can devise an algorithm to compute the covering radius and deep holes of a two-dimensional lattice.

Algorithm

Input: A two-dimensional lattice Λ given by a basis $[\boldsymbol{x}, \boldsymbol{y}]$.

Output: The covering radius and a deep hole of the lattice Λ.

1. Compute a reduced basis $[\boldsymbol{a}, \boldsymbol{b}]$ of the lattice Λ by Gauss' algorithm;
2. If it is necessary, we let the angle between $\boldsymbol{a}$ and $\boldsymbol{b}$ be acute or right;
3. Let O be the origin, and let A, B be two points such that $\boldsymbol{a} = \overrightarrow{OA}$ and $\boldsymbol{b} = \overrightarrow{OB}$. Compute a point D such that $\mid OD \mid = \mid AD \mid = \mid BD \mid$. Output point D as a deep hole and positive real $\mid OD \mid$ as the covering radius of the lattice Λ.

By Theorem 3.2, the above algorithm correctly compute a deep hole and the covering radius of the lattice. The main algorithmic problem is Gauss' algorithm, for if we get the reduced basis, finding a deep hole is only to solve two linear equations and then we can get the covering radius by direct computation. As we mentioned before, the Gauss' algorithm is polynomial time, so we have a polynomial time algorithm to solve the covering radius problem in two-dimensional lattice.

5 Conclusion

The covering radius problem of lattices in Euclidean spaces in any dimension is not known to be solvable in nondeterministic polynomial time. In fact, the (exact) covering radius problem is in Π_2 at the second level of the polynomial hierarchy, a presumably strictly bigger class than NP. But when in dimension two, we give a deterministic polynomial time algorithm by computing a reduced basis using Gauss' algorithm.

References

[1] M. Ajtai, C. Dwork, A public-key cryptosystem with worst-case/average-case equivalence, in Proc. of 29th STOC, New York, USA: ACM, 1997, pp. 284–293.

[2] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, Journal of Cryptology, **10**(1997), 233–260.

[3] L. Fukshansky, S. Robins, Frobenius problem and the covering radius of a lattice, Discrete and Computational Geometry, **37**(2007), 471–483.

[4] V. Guruswami, D. Micciancio, O. Regev, The complexity of the covering radius problem, computational complexity, **14**(2005), 90–121.

[5] J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: a ring-based public key cryptosystem, in Proc. of Algorithmic Number Theory (Lecture Notes in Computer Science), J.P. Buhler, Ed. Berlin, Germany: Springer-Verlag, 1998, vol. 1423, pp. 267–288.

[6] R. Kannan, Lattice translates of a polytope and the Frobenius problem, Combinatorica, **12**(1992), 161–177.

[7] D. Micciancio, Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor, SIAM J. Comput., **34**(2004), 118–169.

[8] D. Micciancio, S. Goldwasser, Complexity of lattice problems: a cryptographic perspective, Kluwer Academic Publishers, Boston, 2002.