


Article

# Faster Provable Sieving Algorithms for the Shortest Vector Problem and the Closest Vector Problem on Lattices in $\ell_p$ Norm

Priyanka Mukhopadhyay <sup>†</sup> 

Department of Combinatorics and Optimization, University of Waterloo, Waterloo, ON N2L 3G1, Canada; p3mukhop@uwaterloo.ca or mukhopadhyay.priyanka@gmail.com

<sup>†</sup> Current address: Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada.

**Abstract:** In this work, we give provable sieving algorithms for the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP) on lattices in  $\ell_p$  norm ( $1 \leq p \leq \infty$ ). The running time we obtain is better than existing provable sieving algorithms. We give a new linear sieving procedure that works for all  $\ell_p$  norm ( $1 \leq p \leq \infty$ ). The main idea is to divide the space into hypercubes such that each vector can be mapped efficiently to a sub-region. We achieve a time complexity of  $2^{2.751n+o(n)}$ , which is much less than the  $2^{3.849n+o(n)}$  complexity of the previous best algorithm. We also introduce a mixed sieving procedure, where a point is mapped to a hypercube within a ball and then a quadratic sieve is performed within each hypercube. This improves the running time, especially in the  $\ell_2$  norm, where we achieve a time complexity of  $2^{2.25n+o(n)}$ , while the List Sieve Birthday algorithm has a running time of  $2^{2.465n+o(n)}$ . We adopt our sieving techniques to approximation algorithms for SVP and CVP in  $\ell_p$  norm ( $1 \leq p \leq \infty$ ) and show that our algorithm has a running time of  $2^{2.001n+o(n)}$ , while previous algorithms have a time complexity of  $2^{3.169n+o(n)}$ .

**Keywords:** lattice; shortest vector problem; closest vector problem; provable sieving algorithm



**Citation:** Mukhopadhyay, P. Faster Provable Sieving Algorithms for the Shortest Vector Problem and the Closest Vector Problem on Lattices in  $\ell_p$  Norm. *Algorithms* **2021**, *14*, 362. <https://doi.org/10.3390/a14120362>

Academic Editor: Frank Werner

Received: 26 October 2021  
Accepted: 9 December 2021  
Published: 13 December 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

A lattice  $\mathcal{L}$  is the set of all integer combinations of linearly independent vectors  $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^d$ ,

$$\mathcal{L} = \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n) := \left\{ \sum_{i=1}^n z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}.$$

We call  $n$  the rank of the lattice and  $d$  the dimension of the lattice. The matrix  $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$  is called a basis of  $\mathcal{L}$ . A lattice is said to be full-rank if  $n = d$ . In this work, we only consider full-rank lattices unless otherwise stated.

The two most important computational problems on lattices are the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). Given a basis for a lattice  $\mathcal{L} \subseteq \mathbb{R}^d$ , the goal of SVP is to compute the shortest non-zero vector in  $\mathcal{L}$ , while the goal of CVP is to compute a lattice vector at a minimum distance to a given target vector  $\mathbf{t}$ . Typically, the length/distance is defined in terms of the  $\ell_p$  norm, which is given by

$$\begin{aligned} \|\mathbf{x}\|_p &= (|x_1|^p + |x_2|^p + \dots + |x_d|^p)^{1/p} \quad \text{for } 1 \leq p < \infty \\ \text{and } \|\mathbf{x}\|_\infty &= \max_{1 \leq i \leq d} |x_i| \end{aligned}$$

These lattice problems have been mostly studied in the Euclidean norm ( $p = 2$ ). Starting with the seminal work of [1], algorithms for solving these problems either exactly or approximately have been studied intensely. These algorithms have found applications in various fields, such as factoring polynomials over rationals [1], integer programming [2–5], cryptanalysis [6–8], checking the solvability by radicals [9], and solving low-density subset-sum problems [10]. More recently, many powerful cryptographic primitives have been

constructed whose security is based on the worst-case hardness of these or related lattice problems [11–19].

### 1.1. Prior Work

The lattice algorithms that have been developed to solve SVP and CVP are either based on sieving techniques [20,21], enumeration methods [3,22], basis reduction [1,23], or Voronoi cell-based deterministic computation [4,24,25]. The fastest of these run in a time of  $2^{cn}$ , where  $n$  is the rank of the lattice and  $c$  is some constant. Since the aim of this paper is to improve time complexity of sieving algorithms, we mainly focus on these. For an overview of the other types of algorithms, interested readers can refer to the survey by Hanrot et al. [26].

#### 1.1.1. Sieving Algorithms in the Euclidean Norm

The first algorithm to solve SVP in the time exponential in the dimension of the lattice was given by Ajtai, Kumar, and Sivakumar [21] who devised a method based on “randomized sieving”, whereby exponentially many randomly generated lattice vectors are iteratively combined to create increasingly short vectors, eventually resulting in the shortest vector in the lattice. The time complexity of this algorithm was shown to be  $2^{3.4n+o(n)}$  by Micciancio and Voulgaris [27]. This was later improved by Pujol and Stehle [28], who analyzed it with the birthday paradox and gave a time complexity of  $2^{2.571n+o(n)}$ . In [27] the authors introduced List Sieve, which was modified in [28] (List Sieve Birthday) to give a time complexity of  $2^{2.465n+o(n)}$ . The current fastest provable algorithm for exact SVP runs in a time of  $2^{n+o(n)}$  [20,29], and the fastest algorithm that gives a large constant approximation runs in a time of  $2^{0.802n+o(n)}$  [30].

To make lattice sieving algorithms more practical for implementation, heuristic variants were introduced in [27,31]. Efforts have been made to decrease the asymptotic time complexity at the cost of using more space [32–35] and to study the trade-offs in reducing the space complexity [35–38]. Attempts have been made to make these algorithms competitive in high-performance computing environments [39–43]. The theoretically fastest heuristic algorithm that is conjectured to solve SVP runs in a time of  $2^{0.29n+o(n)}$  [33] (LD-Sieve).

The CVP is considered to be a harder problem than SVP since there is a simple dimension and approximation-factor preserving reduction from SVP to CVP [44]. Based on a technique due to Kannan [3], Ajtai, Kumar, and Sivakumar [45] gave a provable sieving based algorithm that gives a  $1 + \alpha$  approximation of CVP in time  $(2 + 1/\alpha)^{O(n)}$ . Later, exact exponential time algorithms for CVP were discovered [24,46]. The current fastest algorithm for CVP runs in a time of  $2^{n+o(n)}$  and is due to [46].

#### 1.1.2. Algorithms in Other $\ell_p$ Norms

Blomer and Naewe [47] and then Arvind and Joglekar [48] generalized the AKS algorithm [21] to give exact provable algorithms for SVP that run in a time of  $2^{O(n)}$ . Additionally, ref. [47] gave a  $1 + \varepsilon$  approximation algorithm for CVP for all  $\ell_p$  norms that runs in a time of  $(2 + 1/\varepsilon)^{O(n)}$ . For the special case when  $p = \infty$ , Eisenbrand et al. [5] gave a  $2^{O(n)} \cdot (\log(1/\varepsilon))^n$  algorithm for  $(1 + \varepsilon)$ -approx CVP. Aggarwal and Mukhopadhyay [49] gave an algorithm for SVP and approximate CVP in the  $\ell_\infty$  norm using a linear sieving technique that significantly improves the overall running time. In fact, for a large constant approximation factor, they achieved a running time of  $3^n$  for SVP. The authors have argued that it is not possible for any of the above-mentioned algorithms to achieve this running time in the  $\ell_\infty$  norm.

#### 1.1.3. Hardness Results

The first NP hardness result for CVP in all  $\ell_p$  norms and SVP in the  $\ell_\infty$  norm was given by Van Emde Boas [50]. Ajtai [51] proved that SVP is NP-hard under randomized reductions. Micciancio [52] showed that SVP is NP-hard to approximate within some

constant approximation factor. Subsequently, it was shown that approximating CVP in any  $\ell_p$  norm and SVP in  $\ell_\infty$  norm up to a factor of  $n^{c/\log \log n}$  is NP-hard [53,54]. This difficulty of the approximation factor has been improved to  $n^c$  in [55], assuming the Projection Games Conjecture [56]. Furthermore, the difficulty of SVP up to factor  $2^{\log^{1-\epsilon} n}$  has been obtained assuming  $\text{NP} \not\subseteq \text{RTIME}(n^{\text{poly}(\log n)})$  [57,58]. Recently, ref. [59] showed that for almost all  $p \geq 1$ , CVP in the  $\ell_p$  norm cannot be solved in  $2^{n(1-\epsilon)}$  of time under the strong exponential time hypothesis. A similar difficulty result has also been obtained for SVP in the  $\ell_p$  norm [60].

## 1.2. Our Results and Techniques

In this paper, we adopt the framework of [21,45] and give sieving algorithms for SVP and CVP in  $\ell_p$  norm for  $1 \leq p \leq \infty$ . The primary difference between our sieving algorithm and the previous AKS-style algorithms such as those in [21,45,47,48] is in the sieving procedure—ours is a linear sieve, while theirs is a quadratic sieve. This results in an improvement in the overall running time.

Before describing our idea, we give an informal description of the sieving procedure of [21,45,47,48]. The algorithm starts by randomly generating a set  $S$  of  $N = 2^{O(n)}$  lattice vectors with a length of at most  $R = 2^{O(n)}$ . It then runs a sieving procedure a polynomial number of times. In the  $i$ th iteration, the algorithm starts with a list  $S$  of lattice vectors of a length of at most  $R_{i-1} \approx \gamma^{i-1}R$ , for some parameter  $\gamma \in (0, 1)$ . The algorithm maintains and updates a list of “centers”  $C$ , which is initialized to be the empty set. Then, for each lattice vector  $\mathbf{y}$  in the list, the algorithm checks whether there is a center  $\mathbf{c}$  at a distance of at most  $\gamma \cdot R_{i-1}$  from this vector. If there exists such a center, then the vector  $\mathbf{y}$  is replaced in the list by  $\mathbf{y} - \mathbf{c}$ , and otherwise it is deleted from  $S$  and added to  $C$ . This results in  $N_{i-1} - |C|$  lattice vectors which have a length of at most  $R_i \approx \gamma R_{i-1}$ , where  $N_{i-1}$  is the number of lattice vectors at the end of  $i - 1$  sieving iterations. We would like to mention here that this description hides many details and in particular, in order to show that this algorithm succeeds eventually in obtaining the shortest vector, we need to add a small perturbation to the lattice vectors to start with. The details of this can be found in Section 3.

A crucial step in this algorithm is to find a vector  $\mathbf{c}$  from the list of centers that is close to  $\mathbf{y}$ . This problem is called the nearest neighbor search (NNS) problem and has been well studied, especially in the context of heuristic algorithms for SVP (see [33] and the references therein). A trivial bound on the running time for this is  $|S| \cdot |C|$ , but much effort has been dedicated to improving this bound under heuristic assumptions (see Section 1.1.1 for some references). Since they require heuristic assumptions, such improved algorithms for the NNS have not been used to improve the provable algorithms for SVP.

One can also view such sieving procedures as a division of the “ambient” geometric space (consisting of all the vectors in the current list). In the  $i$ th iteration, the space of all vectors with a length of at most  $R_{i-1}$  is divided into a number of sub-regions such that in each sub-region the vectors are within a distance of at most  $\gamma R_{i-1}$  from a center. In the previous provable sieving algorithms such as those in [21,27,47,48] or even the heuristic ones, these sub-regions have been an  $\ell_p$  ball of certain radius (if the algorithm is in  $\ell_p$  norm) or some sections of it (spherical cap, etc.). Given a vector, one has to compare it with all the centers (and hence sub-regions formed so far) to determine in which of these sub-regions it belongs. If none is found, we make it a center and associate a new sub-region with it. Note that such a division of space depends on the order in which the vectors are processed.

The basic idea behind our sieving procedure (let us call it Linear Sieve) is similar to that used in [49] in the special case of the  $\ell_\infty$  norm. In fact, our procedure is a generalization of this method for all  $\ell_p$  norm ( $1 \leq p \leq \infty$ ). We select these sub-regions as hypercubes and divide the ambient geometric space a priori (before we start processing the vectors in the current list) considering only the maximum length of a vector in the list. A diagrammatic representation of such a division of space in two dimensions has been given in Figure 1. It must be noted that in this figure (for ease of illustration), the radius of the small hypercube (square) is the same for  $\ell_1, \ell_2$ , and  $\ell_\infty$  balls (circles). However, in our algorithm, this radius

depends on the norm. The advantage we obtain is that we can map a vector to a sub-region efficiently -in  $O(n)$  time; i.e., in a sense we obtain better “decodability” property. If the vector’s hypercube (sub-region) does not contain a center, we select this point as the center; otherwise, we subtract this vector from the center to obtain a shorter lattice vector. Thus, the time complexity of each sieving procedure is linear in the number of sampled vectors. Overall, we obtain an improved time complexity at the cost of increased space complexity compared to previous algorithms [26,47,48]. A more detailed explanation can be found in Section 3.1.

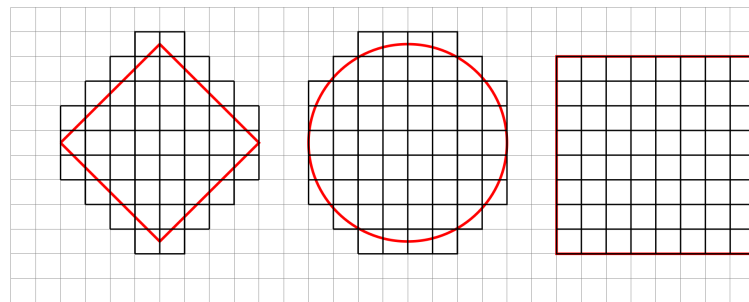


Figure 1. Division of the area of a circle in  $\ell_1, \ell_2,$  and  $\ell_\infty$  norm (respectively) into smaller squares.

Specifically, we obtain the following result.

Theorem 3 in Section 3.3

Let  $\gamma \in (0, 1)$ , and let  $\xi > 1/2$ . Given a full-rank lattice  $\mathcal{L} \subset \mathbb{Q}^n$ , there is a randomized algorithm for  $SVP^{(p)}$  with a success probability of at least  $1/2$ , space complexity of at most  $2^{c_{space}n+o(n)}$ , and running time of at most  $2^{c_{time}n+o(n)}$ , where  $c_{space} = c_s + \max(c_c, c_b/2)$  and  $c_{time} = \max(c_{space}, c_b)$ , where  $c_c = \log\left(2 + \frac{2}{\gamma}\right)$ ,  $c_s = -\log\left(0.5 - \frac{1}{4\xi}\right)$  and  $c_b = \log\left(1 + \frac{2\xi(2-\gamma)}{1-\gamma}\right)$ .

A mixed sieving algorithm

In an attempt to gain as many advantages as possible, we introduce a mixed sieving procedure (let us call it Mixed Sieve). Here, we divide a hyperball into larger hypercubes so that we can map each point efficiently to a hypercube. Within a hypercube, we perform a quadratic sieving procedure such as AKS with the vectors in that region. This improves both time and space complexity, especially in the Euclidean norm.

Approximation algorithms for  $SVP^{(p)}$  and  $CVP^{(p)}$

We have adopted our sieving techniques to approximation algorithms for  $SVP^{(p)}$  and  $CVP^{(p)}$ . The idea is quite similar to that described in [49] (where it was shown to work for only the  $\ell_\infty$  norm). In Section 5.1, we have shown that our approximation algorithms are faster than those of [47,48], but again they require more space.

**Remark 1.** It is quite straightforward to extend our algorithm to the Subspace Avoiding Problem (SAP) (or Generalized Shortest Vector Problem GSVP) [47,48]: replace the quadratic sieve by any one of the faster sieves described in this paper. We thus obtain a similar improvement in running time. By Theorem 3.4 in [47], there are polynomial time reductions from other lattice problems such as the Successive Minima Problem (SMP) (given a lattice  $\mathcal{L}$  with rank  $n$ , the Successive Minima Problem (SMP) requires to find  $n$  linearly independent vectors  $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathcal{L}$  such that  $\|\mathbf{v}_i\|_p \leq c\lambda_i^{(p)}(\mathcal{L})$ .) and Shortest Independent Vector Problem (SIVP) (given a rank  $n$  lattice  $\mathcal{L}$  the Shortest Independent Vector Problem (SIVP) requires to find  $n$  linearly independent vectors  $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathcal{L}$  such that  $\|\mathbf{v}_i\|_p \leq c\lambda_n^{(p)}(\mathcal{L})$ ). The definition of  $\lambda_i^{(p)}$  (and hence  $\lambda_n^{(p)}$ ) has been given in Section 2 (Definition 5);  $c$  is the approximation factor) with approximation factor  $1 + \epsilon$  to GSVP with approximation factor  $1 + \epsilon$ . Thus, we can obtain a similar improvement in running time for

both these problems. Since in this paper, we focus mainly on SVP and CVP, we do not delve into further details for these other problems.

**Remark 2.** Our algorithm (and in that case any sieving algorithm) is quite different from deterministic algorithms such as those in [4,61]. They reduce the problem in any norm to a  $\ell_2$  norm and compute an approximation of the shortest vector length (or distance of the closest lattice point to a target in case of CVP) using the Voronoi cell-based deterministic algorithm in [27]. Then, they enumerate all lattice points within a convex region to find the shortest one. Constructing ellipsoidal coverings, it has been shown that the lattice points within a convex body can be computed in a time proportional to the maximum number of lattice points that the body can contain in any translation of an ellipsoid. Note for  $\ell_p$  norm that any smaller  $\ell_q$  ball (where  $p = q$  or  $p \neq q$ ) can serve this purpose, and the bound on the number of translates comes from standard packing arguments. For these deterministic algorithms, the target would be to choose a shape so that the upper bound (packing bound) on the number of translates can be reduced. Thus, the authors chose small  $\ell_p$  balls to cover a larger  $\ell_p$  ball.

In contrast, in our sieving algorithm, we aimed to map each lattice point efficiently within a sub-region. Thus, we divided any arbitrary  $\ell_p$  ball into smaller hypercubes. The result was an increase in space complexity, but due to the efficient mapping, we reduced the running time. To the best of our knowledge, this kind of sub-divisions has not been used before in any sieving algorithm. The focus of our paper is to develop randomized sieving algorithms. Thus, we will not delve further into the details of the above-mentioned deterministic algorithms. Clearly, these are different procedures.

### 1.3. Organization of the Paper

In Section 2, we give some preliminary definitions and results that are useful for this paper. In Section 3, we introduce the linear sieving technique, while in Section 4, we describe the mixed sieving technique. In Section 5, we discuss how to extend our sieving methods to approximation algorithms.

## 2. Preliminaries

### 2.1. Notations

We write  $\log_q$  to represent the logarithm to the base  $q$ , and simply  $\log$  when the base is  $q = 2$ . We denote the natural logarithm by  $\ln$ .

We use bold lowercase letters (e.g.,  $\mathbf{v}^n$ ) for vectors and bold uppercase letters for matrices (e.g.,  $\mathbf{M}^{m \times n}$ ). We may drop the dimension in the superscript whenever it is clear from the context. Sometimes, we represent a matrix as a vector of column (vectors) (e.g.,  $\mathbf{M}^{m \times n} = [\mathbf{m}_1 \mathbf{m}_2 \dots \mathbf{m}_n]$  where each  $\mathbf{m}_i$  is an  $m$ -length vector). The  $i$ th co-ordinate of  $\mathbf{v}$  is denoted by  $v_i$ .

Given a vector  $\mathbf{x} = \sum_{i=1}^n x_i \mathbf{m}_i$  with  $x_i \in \mathbb{Q}$ , the representation size of  $\mathbf{x}$  with respect to  $\mathbf{M}$  is the maximum of  $n$  and the binary lengths of the numerators and denominators of the coefficients  $x_i$ .

We denote the volume of a geometric body  $A$  by  $\text{vol}(A)$ .

### 2.2. $\ell_p$ Norm and Ball

**Definition 1.** The  $\ell_p$  norm of a vector  $\mathbf{v} \in \mathbb{R}^n$  is defined by

$$\|\mathbf{v}\|_p = \left( \sum_{i=1}^n |v_i|^p \right)^{1/p} \text{ for } 1 \leq p < \infty \text{ and } \|\mathbf{v}\|_\infty = \max\{|v_i| : i = 1, \dots, n\} \text{ for } p = \infty.$$

**Fact 1.** For  $\mathbf{x} \in \mathbb{R}^n$   $\|\mathbf{x}\|_p \leq \|\mathbf{x}\|_2 \leq \sqrt{n} \|\mathbf{x}\|_p$  for  $p \geq 2$  and  $\frac{1}{\sqrt{n}} \|\mathbf{x}\|_p \leq \|\mathbf{x}\|_2 \leq \|\mathbf{x}\|_p$  for  $1 \leq p < 2$ .

**Definition 2.** A **ball** is the set of all points within a fixed distance or radius (defined by a metric) from a fixed point or center. More precisely, we define the (closed) ball centered at  $\mathbf{x} \in \mathbb{R}^n$  with radius  $r$  as

$$B_n^{(p)}(\mathbf{x}, r) = \{\mathbf{y} \in \mathbb{R}^n : \|\mathbf{y} - \mathbf{x}\|_p \leq r\}.$$

The boundary of  $B_n^{(p)}(\mathbf{x}, r)$  is the set

$$\text{bd}(B_n^{(p)}(\mathbf{x}, r)) = \{\mathbf{y} \in \mathbb{R}^n : \|\mathbf{y} - \mathbf{x}\|_p = r\}.$$

We may drop the first argument when the ball is centered at the origin  $\mathbf{0}$  and drop both arguments for a unit ball centered at the origin. Let

$B_n^{(p)}(\mathbf{x}, r_1, r_2) = B_n^{(p)}(\mathbf{x}, r_2) \setminus B_n^{(p)}(\mathbf{x}, r_1) = \{\mathbf{y} \in \mathbb{R}^n : r_1 < \|\mathbf{y} - \mathbf{x}\|_p \leq r_2\}$ . We drop the first argument if the spherical shell or corona is centered at the origin.

**Fact 2.**  $|B_n^{(p)}(\mathbf{x}, c \cdot r)| = c^n \cdot |B_n^{(p)}(\mathbf{x}, r)|$  for all  $c > 0$ .

**Fact 3.**  $\text{vol}(B_n^{(p)}(R)) = \frac{(2\Gamma(\frac{1}{p}+1)R)^n}{\Gamma(\frac{n}{p}+1)}$ . Specifically  $\text{vol}(B_n^{(\infty)}(R)) = (2R)^n$ .

The algorithm of Dyer, Frieze, and Kannan [62] almost uniformly selects a point in any convex body in polynomial time if a membership oracle is given [63]. For the sake of simplicity, we ignore the implementation detail and assume that we are able to uniformly select a point in  $B_n^{(p)}(\mathbf{x}, r)$  in polynomial time.

### 2.3. Lattice

**Definition 3.** A **lattice**  $\mathcal{L}$  is a discrete additive subgroup of  $\mathbb{R}^d$ . Each lattice has a basis  $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n]$ , where  $\mathbf{b}_i \in \mathbb{R}^d$  and

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^n x_i \mathbf{b}_i : x_i \in \mathbb{Z} \text{ for } 1 \leq i \leq n \right\}$$

For algorithmic purposes, we can assume that  $\mathcal{L} \subseteq \mathbb{Q}^d$ . We call  $n$  the *rank* of  $\mathcal{L}$  and  $d$  the *dimension*. If  $d = n$ , the lattice is said to be full-rank. Though our results can be generalized to arbitrary lattices, in the rest of the paper, we only consider full-rank lattices.

**Definition 4.** For any lattice basis  $\mathbf{B}$ , we define the **fundamental parallelepiped** as

$$\mathcal{P}(\mathbf{B}) = \{\mathbf{B}\mathbf{x} : \mathbf{x} \in [0, 1]^n\}$$

If  $\mathbf{y} \in \mathcal{P}(\mathbf{B})$ , then  $\|\mathbf{y}\|_p \leq n\|\mathbf{B}\|_p$ , as can be easily seen by triangle inequality. For any  $\mathbf{z} \in \mathbb{R}^n$ , there exists a unique  $\mathbf{y} \in \mathcal{P}(\mathbf{B})$  such that  $\mathbf{z} - \mathbf{y} \in \mathcal{L}(\mathbf{B})$ . This vector is denoted by  $\mathbf{y} \equiv \mathbf{z} \pmod{\mathbf{B}}$  and it can be computed in polynomial time given  $\mathbf{B}$  and  $\mathbf{z}$ .

**Definition 5.** For  $i \in [n]$ , the  *$i$ th successive minimum* is defined as the smallest real number  $r$  such that  $\mathcal{L}$  contains  $i$  linearly independent vectors with a length of at most  $r$ :

$$\lambda_i^{(p)}(\mathcal{L}) = \inf\{r : \dim(\text{span}(\mathcal{L} \cap B_n^{(p)}(r))) \geq i\}$$

Thus, the *first successive minimum* of a lattice is the length of the shortest non-zero vector in the lattice:

$$\lambda_1^{(p)}(\mathcal{L}) = \min\{\|\mathbf{v}\|_p : \mathbf{v} \in \mathcal{L} \setminus \{\mathbf{0}\}\}$$

We consider the following lattice problems. In all the problems defined below,  $c \geq 1$  is some arbitrary approximation factor (usually specified as subscript), which can be a constant or a function of any parameter of the lattice (usually rank). For exact versions of the problems (i.e.,  $c = 1$ ), we drop the subscript.

**Definition 6 (Shortest Vector Problem (SVP<sub>c</sub><sup>(p)</sup>)).** Given a lattice  $\mathcal{L}$ , find a vector  $\mathbf{v} \in \mathcal{L} \setminus \{\mathbf{0}\}$  such that  $\|\mathbf{v}\|_p \leq c\|\mathbf{u}\|_p$  for any other  $\mathbf{u} \in \mathcal{L} \setminus \{\mathbf{0}\}$ .

**Definition 7 (Closest Vector Problem (CVP<sub>c</sub><sup>(p)</sup>)).** Given a lattice  $\mathcal{L}$  with rank  $n$  and a target vector  $\mathbf{t} \in \mathbb{R}^n$ , find  $\mathbf{v} \in \mathcal{L}$  such that  $\|\mathbf{v} - \mathbf{t}\|_p \leq c\|\mathbf{w} - \mathbf{t}\|_p$  for all other  $\mathbf{w} \in \mathcal{L}$ .

**Lemma 1 ([49]).** The LLL algorithm [1] can be used to solve SVP<sub>2<sup>n</sup></sub><sup>(p)</sup> in polynomial time.

The following result shows that in order to solve SVP<sub>1+ε</sub><sup>(p)</sup>, it is sufficient to consider the case when  $2 \leq \lambda_1^{(p)}(\mathcal{L}) < 3$ . This is done by appropriately scaling the lattice.

**Lemma 2 (Lemma 4.1 in [47]).** For all  $\ell_p$  norms, if there is an algorithm  $A$  that for all lattices  $\mathcal{L}$  with  $2 \leq \lambda_1^{(p)}(\mathcal{L}) < 3$  solves SVP<sub>1+ε</sub><sup>(p)</sup> in time  $T = T(n, b, \epsilon)$ , then there is an algorithm  $A'$  that solves SVP<sub>1+ε</sub><sup>(p)</sup> for all lattices in time  $O(nT + n^4b)$ .

Thus, henceforth, we assume  $2 \leq \lambda_1^{(p)}(\mathcal{L}) < 3$ .

#### 2.4. Some Useful Definitions and Results

In this section, we give some results and definitions which are useful for our analysis later.

**Definition 8.** Let  $P$  and  $Q$  are two point sets in  $\mathbb{R}^n$ . The *Minkowski sum* of  $P$  and  $Q$ , denoted as  $P \oplus Q$ , is the point set  $\{p + q : p \in P, q \in Q\}$ .

**Lemma 3.** Let  $B_1 = B_n^{(p)}(\mathbf{0}, a)$  and  $B_2 = B_n^{(p)}(\mathbf{v}, a)$  such that  $\|\mathbf{v}\|_p = \lambda_1^{(p)}$  and  $\lambda_1^{(p)} < 2a$ . Let  $D = B_1 \cap B_2$ .

If  $|D|$  and  $|B_1|$  are the volumes of  $D$  and  $B_1$ , respectively, then

1. [64]  $\frac{|D|}{|B_1|} \geq 2^{-n} \left(1 - \frac{\lambda_1^{(p)}}{2a}\right)^n$  if  $1 \leq p < \infty$ .
2. [26] When  $p = 2$ , further optimization can be done such that we get  $\frac{|D|}{|B_1|} \geq \left[1 - \left(\frac{\lambda_1^{(2)}}{2a}\right)^2\right]^{n/2}$ .
3. [49] When  $p = \infty$  then  $\frac{|D|}{|B_1|} \geq \left(1 - \frac{\lambda_1^{(\infty)}}{2a}\right)^n$ .

**Theorem 1 (Kabatiansky and Levenshtein [65]).** Let  $E \subseteq \mathbb{R}^n \setminus \{\mathbf{0}\}$ . If there exists  $\phi_0 > 0$  such that for any  $\mathbf{u}, \mathbf{v} \in E$ , we have  $\phi_{\mathbf{u}, \mathbf{v}} \geq \phi_0$ , then  $|E| \leq 2^{c_n + o(n)}$  with  $c = -\frac{1}{2} \log[1 - \cos(\min(\phi_0, 62.99^\circ))]$  – 0.099.

Here,  $\phi_{\mathbf{u}, \mathbf{v}}$  is the angle between the vectors  $\mathbf{u}$  and  $\mathbf{v}$ .

Below, we give some bounds which work for all  $\ell_p$  norms. We especially mention the bounds obtained for the  $\ell_2$  norm where some optimization has been performed using Theorem 1.

**Lemma 4. 1.** [47] Let  $c_c = \log(1 + \frac{2}{\gamma})$ . If  $\mathcal{C}$  is a set of points in  $B_n^{(p)}(R)$  such that the distance between two points is at least  $\gamma R$ , then  $|\mathcal{C}| \leq 2^{c_c n + o(n)}$ .

2. [26,27] When  $p = 2$ , we can have  $|\mathcal{C}^{(2)}| \leq 2^{c_c^{(2)} n + o(n)}$  where  $c_c^{(2)} = -\log \gamma + 0.401$ .

Since the distance between two lattice vectors is at most  $\lambda_1^{(p)}(\mathcal{L})$ , we obtain the following corollary.

**Corollary 1.** *Let  $\mathcal{L}$  be a lattice and  $R$  be a real number greater than the length of the shortest vector in the lattice.*

1. [64]  $|B_n^{(p)}(R) \cap \mathcal{L}| \leq 2^{c_b n}$  where  $c_b = \log\left(1 + \frac{2R}{\lambda_1^{(p)}}\right)$ .
2. [26,28]  $|B_n^{(2)}(R) \cap \mathcal{L}| \leq 2^{c_b^{(2)} n + o(n)}$  where  $c_b^{(2)} = \log \frac{R}{\lambda_1^{(2)}} + 0.401$ .

### 3. A Faster Provable Sieving Algorithm in $\ell_p$ Norm

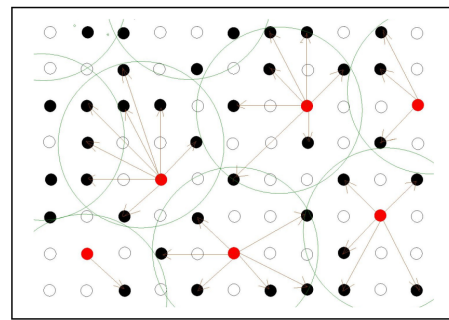
In this section, we present an algorithm for  $\text{SVP}^{(p)}$  that uses the framework of the AKS algorithm [21] but uses a different sieving procedure that yields a faster running time. Using Lemma 1, we can obtain an estimate  $\lambda^*$  of  $\lambda_1^{(p)}(\mathcal{L})$  such that  $\lambda_1^{(p)}(\mathcal{L}) \leq \lambda^* \leq 2^n \cdot \lambda_1^{(p)}(\mathcal{L})$ . Thus, if we try polynomially many different values of  $\lambda = (1 + 1/n)^{-i} \lambda^*$ , for  $i \geq 0$ , then for one of them, we have  $\lambda_1^{(p)}(\mathcal{L}) \leq \lambda \leq (1 + 1/n) \cdot \lambda_1^{(p)}(\mathcal{L})$ . For the rest of this section, we assume that we know an estimated  $\lambda$  of the length of the shortest vector in  $\mathcal{L}$ , which is correct up to a factor  $1 + 1/n$ .

The AKS algorithm (or its  $\ell_p$  norm generalization in [47,48]) initially uniformly samples a large number of perturbation vectors,  $\mathbf{e} \in B_n^{(p)}(d)$ , where  $d \in \mathbb{R}_{>0}$ , and for each such perturbation vector, it maintains a vector  $\mathbf{y}$  close to the lattice ( $\mathbf{y}$  is such that  $\mathbf{y} - \mathbf{e} \in \mathcal{L}$ ). Thus, initially, we have a set  $S$  of many such pairs  $(\mathbf{e}, \mathbf{y}) \in B_n^{(p)}(d) \times B_n^{(p)}(R)$  for some  $R \in 2^{O(n)}$ . The desired situation is that after a polynomial number of such sieving iterations, we are left with a set of vector pairs  $(\mathbf{e}'', \mathbf{y}'')$  such that  $\mathbf{y}'' - \mathbf{e}'' \in \mathcal{L} \cap B_n^{(p)}(O(\lambda_1^{(p)}(\mathcal{L})))$ . Finally, we take the pair-wise differences of the lattice vectors corresponding to these vector pairs and output the one with the smallest non-zero norm. It was shown in [21,47,48] that, with overwhelming probability, this is the shortest vector in the lattice.

One of the main and usually the most expensive steps in this algorithm is the sieving procedure, where given a list of vector pairs  $(\mathbf{e}, \mathbf{y}) \in B_n^{(p)}(d) \times B_n^{(p)}(R)$  in each iteration, it outputs a list of vector pairs  $(\mathbf{e}', \mathbf{y}') \in B_n^{(p)}(d) \times B_n^{(p)}(\gamma R)$  where  $\gamma \in \mathbb{R}_{(0,1)}$ . In each sieving iteration, a number of vector pairs (usually exponential in  $n$ ) are identified as “center pairs”. The second element of each such center pair is referred to as the “center”. By a well-defined map, each of the remaining vector pairs is associated to a “center pair” such that after certain operations (such as subtraction) on the vectors, we obtain a pair with a vector difference yielding a lattice vector with a norm less than  $R'$ . If we start an iteration with say  $N'$  vector pairs and identify  $|\mathcal{C}|$  number of center pairs, then the output consists of  $N' - |\mathcal{C}|$  vector pairs. An illustration is given in Figure 2. In [21] and most other provable variants or generalizations such as [47,48], the running time of this sieving procedure, which is the dominant part of the total running time of the algorithm, is roughly quadratic in the number of sampled vectors.

Here, we propose a different sieving approach to reduce the overall time complexity of the algorithm. This can be thought of as a generalization of the sieving method introduced in [49] for the  $\ell_\infty$  norm. We divide the space such that each lattice vector can be mapped efficiently into some desired division. In the following subsection, we explain this sieving procedure, whose running time is linear in the number of sampled vectors.



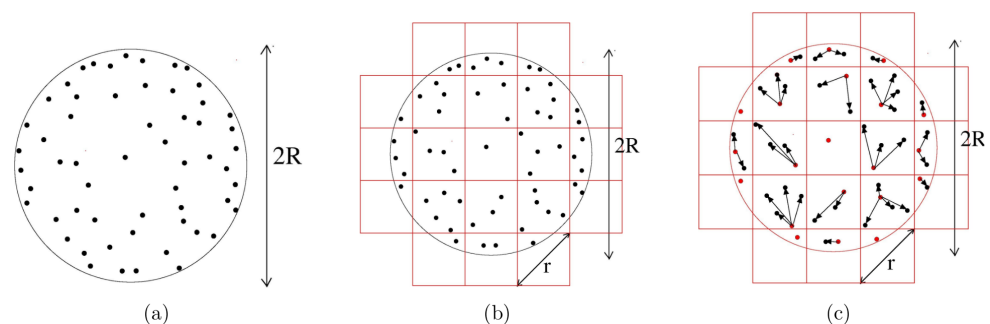


**Figure 2.** One iteration of the quadratic AKS sieve in the  $\ell_2$  norm. Each point represents a vector pair. The solid dots are the sampled ones, while the hollow dots are the unsampled ones. Among the sampled vector pairs, some are identified as centers (red dots) and the space is divided into a number of balls, centered around these red dots. Vector subtraction (denoted by arrow) is performed with the center pair in each ball, such that we obtain shorter lattice vectors in the next iteration.

### 3.1. Linear Sieve

In the initial AKS algorithm [21,45] as well as in all its variants thereafter [27,47,48], in the sieving sub-routine, a space  $B_n^{(p)}(R)$  has been divided into sub-regions such that each sub-region is associated with a center. Then, given a vector, we map it to a sub-region and subtract it from the center so that we get a vector of length at most  $\gamma R$ . We must aim to select these sub-regions such that we can (i) map a vector efficiently to a sub-region (ii) without increasing the number of centers “too much”. The latter factor is determined by the number of divisions of  $B_n^{(p)}(R)$  into these sub-regions and directly contributes to the space (and hence time) complexity.

In all the previous provable sieving algorithms, the sub-regions were small hyperballs (or parts of them) in  $\ell_p$  norm. In this paper, our sub-regions are hypercubes. The choice of this particular sub-region makes the mapping very efficient. First, let us note that, in contrast with the previous algorithms (except [49]), we divide the space a priori. This can be done by dividing each co-ordinate axis into intervals of length  $\frac{\gamma R}{n^{1/p}}$  so that the distance between any two vectors in the resulting hypercube is at most  $\gamma R$ . In an ordered list, we store an appropriate index (say, co-ordinates of one corner) of only those hypercubes which have a non-zero intersection with  $B_n^{(p)}(R)$ . We can map a vector to a hypercube in  $O(n)$  time simply by looking at the intervals in which each of its co-ordinates belong. If the hypercube contains a center, then we subtract the vectors and store the difference; otherwise, we assign this vector as the center. An illustration is given in Figure 3.



**Figure 3.** One iteration of the linear sieve in the  $\ell_2$  norm. (a) A number of vector pairs (solid black dots) with (Euclidean) length at most  $R$  are sampled. (b) The space is divided into a number of hypercubes with diagonal length  $r$ , and each vector pair is mapped into a hypercube. (c) Within each hypercube, a subtraction operation (denoted by arrow) is performed between a center (red dot) and the remaining vector pairs, such that we obtain shorter lattice vectors in the next iteration.

The following lemma gives a bound on the number of hypercubes or centers we obtain by this process. Such a volumetric argument can be found in [66].

**Lemma 5.** Let  $\gamma \in (0, 1), R \in \mathbb{R}_{\geq 1}, 1 \leq p \leq \infty$  and  $r = \frac{\gamma R}{2n^{1/p}}$ . The number of translates of  $B_n^{(\infty)}(r)$  required to cover  $B_n^{(p)}(R)$  is at most  $O\left(\left(2 + \frac{2}{\gamma}\right)^n\right)$ .

**Proof.** Let  $N_h$  be the number of translates of  $L = B_n^{(\infty)}(r)$  required to cover  $K = B_n^{(p)}(R)$ . These translates are all within  $K \oplus 2L$ . In addition, noting that  $L \subseteq \frac{rn^{1/p}}{R}K$ , we have

$$N_h * \text{vol}(L) \leq \text{vol}(K + 2L) \leq \left(1 + \frac{2rn^{1/p}}{R}\right)^n \text{vol}(K)$$

Plugging in the value of  $r$ , we have  $N_h \leq (1 + \gamma)^n \frac{\text{vol}(K)}{\text{vol}(L)}$ .

Using Fact 3, we have  $N_h \in O\left(\left(2 + \frac{2}{\gamma}\right)^n\right)$ .  $\square$

Note that the above lemma implies a sub-division where one hypercube is centered at the origin. Thus, along each axis, we can have the following  $2r$ -length intervals:

$$\dots [-5r, -3r), [-3r, -r), [-r, r), [r, 3r), [3r, 5r), \dots$$

We do not know whether this is the most optimal way of sub-dividing  $B_n^{(p)}(R)$  into smaller hypercubes. In [49], it has been shown that if we divide  $[-R, R]$  from one corner—i.e., place one small hypercube at one corner of the larger hypercube  $B_n^{(\infty)}(R)$ —then  $O\left(\left(\left\lceil \frac{2}{\gamma} \right\rceil\right)^n\right)$  copies of hypercubes of radius  $r$  suffices.

Suppose in one sieving iteration, we have a set  $S$  of lattice vectors of length at most  $R$ ; i.e., they all lie in  $B_n^{(p)}(R)$  (Figure 3a). We would like to combine points so that we are left with vectors in  $B_n^{(p)}(\gamma R)$ . We divide each axis into intervals of length  $y = \frac{\gamma R}{n^{1/p}}$  and store in an ordered set  $\mathcal{I}$  co-ordinates of one corner of the resulting hypercubes that have a non-zero intersection with  $B_n^{(p)}(R)$  (Figure 3b). Note that this can be done in a time of  $O(nN_h)$ , where  $N_h$  is the maximum number of hypercube translates as described in Lemma 5.

We maintain a list  $\mathcal{C}$  of pairs, where the first entry of each pair is an  $n$ -tuple in  $\mathcal{I}$  (let us call it “index-tuple”) and the second one, initialized as empty set, is for storing a center pair. Given  $\mathbf{y}$ , we map it to its index-tuple  $I_{\mathbf{y}}$  as follows: we calculate the interval in which each of its co-ordinates belong (steps 10–13 in Algorithm 2). This can be done in  $O(n)$  time. This is equivalent to storing information about the hypercube (in Figure 3b) in which it belongs or is mapped to. We can access  $\mathcal{C}[I_{\mathbf{y}}]$  in constant time. For each  $(\mathbf{e}, \mathbf{y}) \in S$ , if there exists a  $(\mathbf{e}_c, \mathbf{c}) \in \mathcal{C}[I_{\mathbf{y}}]$ —i.e.,  $I_{\mathbf{y}} = I_{\mathbf{c}}$  (implying  $\|\mathbf{y} - \mathbf{c}\|_p \leq \gamma R$ )—then we add  $(\mathbf{e}, \mathbf{y} - \mathbf{c} + \mathbf{e}_c)$  to the output set  $S'$  (Figure 3c). Otherwise, we add vector pair  $(\mathbf{e}, \mathbf{y})$  to  $\mathcal{C}[I_{\mathbf{y}}]$  as a center pair. This implies that if there exists a center in the hypercube, then we perform subtraction operations to obtain a shorter vector. Otherwise, we make  $(\mathbf{e}, \mathbf{y})$  the center for its hypercube. Finally, we return  $S'$ .

More details of this sieving procedure (Linear Sieve) can be found in Algorithm 2.

### 3.2. AKS Algorithm with a Linear Sieve

Algorithm 1 describes an exact algorithm for  $\text{SVP}^{(p)}$  with a linear sieving procedure (Linear Sieve) (Algorithm 2).

---

**Algorithm 1:** An exact algorithm for  $SVP^{(p)}$

---

**Input:** (i) A basis  $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$  of a lattice  $\mathcal{L}$ , (ii)  $0 < \gamma < 1$ , (iii)  $\xi > 1/2$ , (iv)  $\lambda \approx \lambda_1^{(p)}(\mathcal{L})$ , (v)  $N \in \mathbb{N}$   
**Output:** A shortest vector of  $\mathcal{L}$

```

1  $S \leftarrow \emptyset$ ;
2 for  $i = 1$  to  $N$  do
3    $\mathbf{e}_i \leftarrow_{\text{uniform}} B_n^{(p)}(\mathbf{0}, \xi\lambda)$ ;
4    $\mathbf{y}_i \leftarrow \mathbf{e}_i \bmod \mathcal{P}(\mathbf{B})$ ;
5    $S \leftarrow S \cup \{(\mathbf{e}_i, \mathbf{y}_i)\}$ ;
6 end
7  $R \leftarrow n \max_i \|\mathbf{b}_i\|_p$ ;
8 for  $j = 1$  to  $k = \lceil \log_\gamma \left( \frac{\xi}{nR(1-\gamma)} \right) \rceil$  do
9    $S \leftarrow \text{sieve}(S, \gamma, R, \xi)$  using Linear Sieve (Algorithm 2);
10   $R \leftarrow \gamma R + \xi\lambda$ ;
11 end
12 Compute the non-zero vector  $\mathbf{v}_0$  in  $\{(\mathbf{y}_i - \mathbf{e}_i) - (\mathbf{y}_j - \mathbf{e}_j) : (\mathbf{e}_i, \mathbf{y}_i), (\mathbf{e}_j, \mathbf{y}_j) \in S\}$ 
    with the smallest  $\ell_p$  norm;
13 return  $\mathbf{v}_0$ ;

```

---

**Algorithm 2:** Linear Sieve for  $\ell_p$  norm

---

**Input:** (i) Set  $S = \{(\mathbf{e}_i, \mathbf{y}_i) : i \in I\} \subseteq B_n^{(p)}(\xi\lambda) \times B_n^{(p)}(R)$  such that  $\forall i \in I, \mathbf{y}_i - \mathbf{e}_i \in \mathcal{L}$ , (ii)  $(\gamma, R, \xi)$   
**Output:** A set  $S' = \{(\mathbf{e}'_i, \mathbf{y}'_i) : i \in I'\} \subseteq B_n^{(p)}(\xi\lambda) \times B_n^{(p)}(\gamma R + \xi\lambda)$  such that  $\forall i \in I', \mathbf{y}'_i - \mathbf{e}'_i \in \mathcal{L}$

```

1  $R \leftarrow \max_{(\mathbf{e}, \mathbf{y}) \in S} \|\mathbf{y}\|_p$ ;
2  $S' \leftarrow \emptyset$ ;
3 Divide each axis into intervals of length  $\frac{\gamma R}{n^{1/p}}$  and store a corner of those resulting
    hypercubes with a non zero intersection with  $B_n^{(p)}(R)$  in ordered set  $\mathcal{I}$ ;
4  $\mathcal{C} \leftarrow \{((i_1, i_2, \dots, i_n), \emptyset) : (i_1, i_2, \dots, i_n) \in \mathcal{I}\}$ ;
5 for  $(\mathbf{e}, \mathbf{y}) \in S$  do
6   if  $\|\mathbf{y}\|_p \leq \gamma R$  then
7      $S' \leftarrow S' \cup \{(\mathbf{e}, \mathbf{y})\}$ ;
8   else
9      $I \leftarrow \emptyset$ ;
10    for  $i = 1, \dots, n$  do
11      Find the integer  $j$  such that  $(j - 1) \leq \frac{y_i + R}{\gamma R / n^{1/p}} < j$ ;
12       $I[i] = j$ ;
13    end
14    if  $\exists (\mathbf{c}_c, \mathbf{c}) \in \mathcal{C}[I]$  then
15       $S' \leftarrow S' \cup \{(\mathbf{e}, \mathbf{y} - \mathbf{c} + \mathbf{e}_c)\}$ ;
16    else
17       $\mathcal{C}[I] \leftarrow \mathcal{C}[I] \cup \{(\mathbf{e}, \mathbf{y})\}$ ;
18    end
19  end
20 end
21 return  $S'$ ;

```

---

**Lemma 6.** Let  $\gamma \in \mathbb{R}_{(0,1)}$ . The number of center pairs in Algorithm 2 always satisfies  $|\mathcal{C}| \leq 2^{c_c n + o(n)}$  where  $c_c = \log\left(2 + \frac{2}{\gamma}\right)$ .

**Proof.** This follows from Lemma 5 in Section 3.1.

□

**Claim 1.** The following two invariants are maintained in Algorithm 1:

1.  $\forall(\mathbf{e}, \mathbf{y}) \in S, \mathbf{y} - \mathbf{e} \in \mathcal{L}$
2.  $\forall(\mathbf{e}, \mathbf{y}) \in S, \|\mathbf{y}\|_p \leq R.$

**Proof.** 1. The first invariant is maintained at the beginning of the sieving iterations in Algorithm 1 due to the choice of  $\mathbf{y}$  at step 4 of Algorithm 1.

Since each center pair  $(\mathbf{e}_c, \mathbf{c})$  once belonged to  $S, \mathbf{c} - \mathbf{e}_c \in \mathcal{L}$ . Thus, at step 15 of the sieving procedure (Algorithm 2), we have  $(\mathbf{e} - \mathbf{y}) + (\mathbf{c} - \mathbf{e}_c) \in \mathcal{L}$ .

2. The second invariant is maintained in steps 2–6 of Algorithm 1 because  $\mathbf{y} \in \mathcal{P}(\mathbf{B})$  and hence  $\|\mathbf{y}\|_p \leq \sum_{i=1}^n \|\mathbf{b}_i\|_p \leq n \max_i \|\mathbf{b}_i\|_p = R.$

We claim that this invariant is also maintained in each iteration of the sieving procedure.

Consider a pair  $(\mathbf{e}, \mathbf{y}) \in S$  and let  $I_y$  be its index-tuple. Let  $(\mathbf{e}_c, \mathbf{c})$  be its associated center pair. By Algorithm 2, we have  $I_y = I_c$ ; i.e.,  $\|\mathbf{y} - \mathbf{c}\|_p^p = \sum_{i=1}^n |y_i - c_i|^p \leq \sum_{i=1}^n \frac{\gamma^p R^p}{n} \leq \gamma^p R^p$ . Thus,  $\|\mathbf{y} - \mathbf{c}\|_p \leq \gamma R$  and hence  $\|\mathbf{y} - \mathbf{c} + \mathbf{e}_c\|_p \leq \|\mathbf{y} - \mathbf{c}\|_p + \|\mathbf{e}_c\|_p \leq \gamma R + \xi \lambda.$

The claim follows by the re-assignment of variable  $R$  at step 10 in Algorithm 1.

□

In the following lemma, we bound the length of the remaining lattice vectors after all the sieving iterations are over. The proof is similar to that given in [49], so we write it briefly.

**Lemma 7.** At the end of  $k$  iterations in Algorithm 1, the length of lattice vectors  $\|\mathbf{y} - \mathbf{e}\|_p \leq \frac{\xi(2-\gamma)\lambda}{1-\gamma} + \frac{\gamma\xi}{n(1-\gamma)} =: R'.$

**Proof.** Let  $R_k$  be the value of  $R$  after  $k$  iterations, where

$$\log_\gamma \left( \frac{\xi}{nR(1-\gamma)} \right) \leq k \leq \log_\gamma \left( \frac{\xi}{nR(1-\gamma)} \right) + 1.$$

Then,

$$R_k = \gamma^k R + \sum_{i=1}^k \gamma^{k-i} \xi \lambda \leq \frac{\xi \gamma}{n(1-\gamma)} + \frac{\xi \lambda}{1-\gamma} \left[ 1 - \frac{\xi}{nR(1-\gamma)} \right]$$

Thus, after  $k$  iterations,  $\|\mathbf{y}\|_p \leq R_k$ , and hence after  $k$  iterations,

$$\begin{aligned} \|\mathbf{y} - \mathbf{e}\|_p &\leq \|\mathbf{y}\|_p + (\|\mathbf{e}\|_p) \leq R_k + \xi \lambda \\ &= \frac{(2-\gamma)\xi \lambda}{1-\gamma} + \frac{\gamma \xi}{n(1-\gamma)} \end{aligned}$$

□

Using Corollary 1 and assuming  $\lambda \approx \lambda_1^{(p)}$ , we obtain an upper bound on the number of lattice vectors of a length of at most  $R'$ ; i.e.,

$$|B_n^{(p)}(R') \cap \mathcal{L}| \leq 2^{c_b n + o(n)}, \text{ where } c_b = \log \left( 1 + \frac{2\xi(2-\gamma)}{1-\gamma} \right).$$

The above lemma along with the invariants implies that at the beginning of step 12 in Algorithm 1, we have “short” lattice vectors; i.e., vectors with a norm bounded by  $R'$ . We want to start with a “sufficient number” of vector pairs so that we do not end up with all zero vectors at the end of the sieving iterations. For this, we work with the following conceptual modification proposed by Regev [67].

Let  $\mathbf{u} \in \mathcal{L}$  such that  $\|\mathbf{u}\|_p = \lambda_1^{(p)}(\mathcal{L}) \approx \lambda$  (where  $2 < \lambda_1^{(p)}(\mathcal{L}) \leq 3$ ),  $D_1 = B_n^{(p)}(\xi\lambda) \cap B_n^{(p)}(-\mathbf{u}, \xi\lambda)$  and  $D_2 = B_n^{(p)}(\xi\lambda) \cap B_n^{(p)}(\mathbf{u}, \xi\lambda)$ . Define a bijection  $\sigma$  on  $B_n^{(p)}(\xi\lambda)$  that maps  $D_1$  to  $D_2$ ,  $D_2$  to  $D_1$  and  $B_n^{(p)}(\xi\lambda) \setminus (D_1 \cup D_2)$  to itself :

$$\sigma(\mathbf{e}) = \begin{cases} \mathbf{e} + \mathbf{u} & \text{if } \mathbf{e} \in D_1 \\ \mathbf{e} - \mathbf{u} & \text{if } \mathbf{e} \in D_2 \\ \mathbf{e} & \text{else} \end{cases}$$

For the analysis of the algorithm, we assume that for each perturbation vector  $\mathbf{e}$  chosen by our algorithm, we replace  $\mathbf{e}$  by  $\sigma(\mathbf{e})$  with probability  $1/2$  and that it remains unchanged with probability  $1/2$ . We call this procedure *tossing* the vector  $\mathbf{e}$ . This does not change the distribution of the perturbation vectors  $\{\mathbf{e}\}$ . Further, we assume that this replacement of the perturbation vectors happens at the step where this has any effect on the algorithm for the first time. In particular, at step 17 in Algorithm 2, after we have identified a center pair  $(\mathbf{e}_c, \mathbf{c})$ , we apply  $\sigma$  on  $\mathbf{e}_c$  with probability  $1/2$ . Then, at the beginning of step 12 in Algorithm 1, we apply  $\sigma$  to  $\mathbf{e}$  for all pairs  $(\mathbf{e}, \mathbf{y}) \in S$ . The distribution of  $\mathbf{y}$  remains unchanged by this procedure because  $\mathbf{y} \equiv \mathbf{e} \equiv \sigma(\mathbf{e}) \pmod{\mathcal{P}(\mathbf{B})}$  and  $\mathbf{y} - \mathbf{e} \in \mathcal{L}$ . A somewhat more detailed explanation of this can be found in the following result of [47].

**Lemma 8 (Theorem 4.5 in [47] (re-stated)).** *The modification outlined above does not change the output distribution of the actual procedure.*

Note that since this is just a conceptual modification intended for ease in analysis, we should not be concerned with the actual running time of this modified procedure. Even the fact that we need a shortest vector to begin the mapping  $\sigma$  does not matter.

The following lemma will help us to estimate the number of vector pairs to sample at the beginning of the algorithm.

**Lemma 9 (Lemma 4.7 in [47]).** *Let  $N \in \mathbb{N}$  and  $q$  denote the probability that a random point in  $B_n^{(p)}(\xi\lambda)$  is contained in  $D_1 \cup D_2$ . If  $N$  points  $\mathbf{x}_1, \dots, \mathbf{x}_N$  are chosen uniformly at random in  $B_n^{(p)}(\xi\lambda)$ , then with a probability larger than  $1 - \frac{4}{q^N}$ , there are at least  $\frac{qN}{2}$  points  $\mathbf{x}_i \in \{\mathbf{x}_1, \dots, \mathbf{x}_N\}$  with the property  $\mathbf{x}_i \in D_1 \cup D_2$ .*

From Lemma 3, we have

$$q \geq 2^{-c_s n} \quad \text{where } c_s = -\log\left(0.5 - \frac{1}{4\xi}\right)$$

Thus, with a probability of at least  $1 - \frac{4}{q^N}$ , we have at least  $2^{-c_s n} N$  pairs  $(\mathbf{e}_i, \mathbf{y}_i)$  before the sieving iterations such that  $\mathbf{e}_i \in D_1 \cup D_2$ .

**Lemma 10.** *If  $N \geq \frac{2}{q}(k|\mathcal{C}| + 2^{c_b n} + 1)$ , then with a probability of at least  $1/2$ , Algorithm 1 outputs a shortest non-zero vector in  $\mathcal{L}$  with respect to  $\ell_p$  norm for  $1 \leq p \leq \infty$ .*

**Proof.** Of the  $N$  vector pairs  $(\mathbf{e}, \mathbf{y})$  sampled in steps 2–6 of Algorithm 1, we consider those such that  $\mathbf{e} \in (D_1 \cup D_2)$ . We have already seen there are at least  $\frac{qN}{2}$  such pairs with a probability of at least  $1 - \frac{4}{q^N}$ . We remove  $|\mathcal{C}|$  vector pairs in each of the  $k$  sieve iterations. Thus, at step 12 of Algorithm 1, we have  $N' \geq 2^{c_b n} + 1$  pairs  $(\mathbf{e}, \mathbf{y})$  to process.

By Lemma 7, each of them is contained within a ball of radius  $R'$  which can have at most  $2^{c_b n}$  lattice vectors. Thus, there exists at least one lattice vector  $\mathbf{w}$  for which the perturbation is in  $D_1 \cup D_2$ , and it appears twice in  $S$  at the beginning of step 12. With a probability of  $1/2$ , it remains  $\mathbf{w}$ , or with the same probability, it becomes either  $\mathbf{w} + \mathbf{u}$  or

$\mathbf{w} - \mathbf{u}$ . Thus, after taking pair-wise difference at step 12 with a probability of at least  $1/2$ , we find the shortest vector.  $\square$

**Theorem 2.** Let  $\gamma \in (0, 1)$ , and let  $\xi > 1/2$ . Given a full rank lattice  $\mathcal{L} \subset \mathbb{Q}^n$ , there is a randomized algorithm for  $SVP^{(p)}$  with a success probability of at least  $1/2$ , a space complexity of at most  $2^{c_{space}n+o(n)}$ , and running time of at most  $2^{c_{time}n+o(n)}$ , where  $c_{space} = c_s + \max(c_c, c_b)$  and  $c_{time} = \max(c_{space}, 2c_b)$ , where  $c_c = \log\left(2 + \frac{2}{\gamma}\right)$ ,  $c_s = -\log\left(0.5 - \frac{1}{4\xi}\right)$  and  $c_b = \log\left(1 + \frac{2\xi(2-\gamma)}{1-\gamma}\right)$ .

**Proof.** If we start with  $N$  pairs (as stated in Lemma 10), then the space complexity is at most  $2^{c_{space}n+o(n)}$  with  $c_{space} = c_s + \max(c_c, c_b)$ .

In each iteration of the sieving Algorithm 2, it takes at most  $O(nN_h)$  time to initialize and index  $\mathcal{C}$  (Lemmas 5 and 6). For each vector pair  $(\mathbf{e}, \mathbf{y}) \in S$ , it takes a time of at most  $n$  to calculate its index-tuple  $I_y$ . Thus, the time taken to process each vector pair is at most  $(n + 1)$ , and the total time taken per iteration of Algorithm 2 is at most  $O(n(N_h + N))$ , which is at most  $2^{c_{space}n+o(n)}$ , and there are at most  $\text{poly}(n)$  such iterations.

If  $N' \geq 2^{c_b n} + 1$ , then the time complexity for the computation of the pairwise differences is at most  $(N')^2 \in 2^{2c_b n+o(n)}$ .

Thus, the overall time complexity is at most  $2^{c_{time}n+o(n)}$  where  $c_{time} = \max(c_{space}, 2c_b)$ .  $\square$

### 3.3. Improvement Using the Birthday Paradox

We can obtain a better running time and space complexity if we use the birthday paradox to decrease the number of sampled vectors but obtain at least two vector pairs corresponding to the same lattice vector after the sieving iterations [26,28]. For this, we have to ensure that the vectors are independent and identically distributed before step 12 of Algorithm 1. Thus, we incorporate the following modification, as discussed in [26]. Very briefly, the trick is to set aside many uniformly distributed vector pairs as centers for each sieving step, even before the sieving iterations begin. In each sieving iteration, the probability that a vector pair is not within the required distance of any center pair decreases. Now, if we sample enough vectors, then with a good probability at step 12, we have at least two vectors whose perturbation is in  $D_1 \cup D_2$ , implying that with a probability of at least  $1/2$ , we obtain the shortest vector.

In the analysis of [26], the authors simply stated that the required center pairs can be sampled uniformly at the beginning. In our linear sieving algorithm, we have an advantage. Unlike the AKS-style algorithms, in which the center pairs are selected and then the space is divided, in our case, we can divide the space a priori. We take advantage of this and conduct a number of random divisions of the space. Since in each iteration, the length of the vectors decreases, the size of the hypercubes also decreases, and this can be calculated. Thus, for each iteration we have a number of divisions of the space into hypercubes of a certain size. For this, we need to divide the axes into intervals of a fixed size. Simply by shifting the intervals in each axis, we can make this division random. Then, among the uniformly sampled vectors, we select a center for each hypercube.

Assume we start with  $N \geq \frac{2}{q}(n^3 k |\mathcal{C}| + n 2^{\frac{c_b}{2} n})$  sampled pairs. After the initial sampling, for each of the  $k$  sieving iterations, we fix  $\Omega\left(\frac{2n^3}{q} |\mathcal{C}|\right)$  pairs to be used as center pairs in the following way.

1. Let  $R = \max_{i \in [N]} \|\mathbf{y}_i\|_p$ . We maintain  $k$  lists of pairs,  $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k$ , where each list is similar to  $(\mathcal{C})$ , as described in Algorithm 2. In the  $i$ th list, we store the indices (co-ordinates of a corner) of translates of  $B_n^{(\infty)}(r_i)$  that have a non-zero intersection with  $B_n^{(p)}(R_i)$  where  $R_i = \gamma^{i-1} R + \xi \lambda \frac{1-\gamma^{i-1}}{1-\gamma}$  and  $r_i = \frac{\gamma R_i}{2n^{1/p}}$ . For such a division, we can obtain  $O(|\mathcal{C}|)$  center pairs in each list. To meet our requirement, we maintain  $O(n^3)$  such lists for each  $i$ . We call these  $O(n^3)$  lists the ‘‘sibling lists’’ of  $\mathcal{C}_i$ .

2. For each  $(\mathbf{e}, \mathbf{y}) \in S$  (where  $S$  is the set of sampled pairs), we first calculate  $\|\mathbf{y}\|_p$  to check in which list group it can potentially belong, say  $\mathcal{C}_j$ . That is,  $\mathcal{C}_j$  corresponds to the smallest hyperball containing  $\mathbf{y}$ . Then, we map it to its index-tuple  $I_y$ , as has already been described before. We add  $(\mathbf{e}, \mathbf{y})$  to a list in  $\mathcal{C}_j$  or any of its sibling lists if it was empty before. Since we sampled uniformly, this ensures we obtain the required number of (initially) fixed centers, and no other vector can be used as a center throughout the algorithm.

Having set aside the centers, now we repeat the following sieving operations  $k$  times. For each vector pair  $(\mathbf{e}_1, \mathbf{y}_1) \in S$ , we can check which list (or its sibling lists) it can belong to from  $\|\mathbf{y}_1\|_p$ . Then, if a center pair is found, we subtract as in step 15 of Algorithm 2. Otherwise, we discard it and consider it “lost”.

Let us call this modified sieving procedure **LinearSieveBirthday**. We obtain the following improvement in the running time.

**Theorem 3.** *Let  $\gamma \in (0, 1)$ , and let  $\xi > 1/2$ . Given a full rank lattice  $\mathcal{L} \subset \mathbb{Q}^n$ , there is a randomized algorithm for  $SVP^{(p)}$  with a success probability of at least  $1/2$ , a space complexity of at most  $2^{c_{space}n+o(n)}$ , and running time of at most  $2^{c_{time}n+o(n)}$ , where  $c_{space} = c_s + \max(c_c, \frac{c_b}{2})$  and  $c_{time} = \max(c_{space}, c_b)$ , where*

$$c_c = \log\left(2 + \frac{2}{\gamma}\right), \quad c_s = -\log\left(0.5 - \frac{1}{4\xi}\right) \text{ and } c_b = \log\left(1 + \frac{2\xi(2-\gamma)}{1-\gamma}\right).$$

**Proof.** This analysis has been taken from [26]. At the beginning of the algorithm, among the pairs set aside as centers for the first step, there are  $\Omega(n^3|\mathcal{C}|)$  pairs such that the perturbation is in  $D_1 \cup D_2$  with high probability (Lemma 9). We call them good pairs. After fixing these pairs as centers, the probability that the distance between the next perturbed vector and the closest center is more than  $\gamma R$  decreases. The sum of these probabilities is bounded from above by  $|\mathcal{C}|$ . As a consequence, once all centers have been processed, the probability for any of the subsequent pairs to be lost is  $O\left(\frac{1}{n^3}\right)$ . By induction, it can be proved that the same proportion of pairs is lost at each step of the sieve with high probability. As a consequence, no more than  $1 - \left(1 - \frac{1}{n^3}\right)^{O(n^2)} = O\left(\frac{1}{n}\right)$  pairs are lost during the whole algorithm. This means that in the final ball, there are  $\Omega\left(n2^{\frac{c_b}{2}n}\right)$  probabilistically independent lattice points corresponding to good pairs with high probability. As in the proof of Lemma 10 this implies that the algorithm returns a shortest vector with a probability of at least  $1/2$ .  $\square$

*Comparison of Linear Sieve with provable sieving algorithms [21,45,47,48]*

For  $1 \leq p \leq \infty$ , the number of centers obtained by [47] is  $|\mathcal{C}(BN)| \leq 2^{c_c(BN)n}$ , where  $c_c(BN) = \log\left(1 + \frac{2}{\gamma}\right)$  (Lemma 4). If we conducted a similar analysis for their algorithm, we would obtain space and time complexities of  $2^{c_{space}(BN)n+o(n)}$  and  $2^{c_{time}(BN)n+o(n)}$ , respectively, where

$$\begin{aligned} c_{space}(BN) &= c_s + \max(c_c(BN), c_b) \\ \text{and } c_{time}(BN) &= \max(c_{space}(BN) + c_c(BN), 2c_b). \end{aligned}$$

We can incorporate modifications to apply the birthday paradox, as has been done in [26] (for  $\ell_2$  norm). This would improve the exponents to

$$\begin{aligned} c_{space}(BN') &= c_s + \max(c_c(BN), c_b/2) \\ \text{and } c_{time}(BN') &= \max(c_{space}(BN) + c_c(BN), c_b). \end{aligned}$$

Clearly, the running time of our algorithm is less since  $\left(1 + \frac{2}{\gamma}\right)^2 > \left(2 + \frac{2}{\gamma}\right)$  for all  $\gamma < 1$ . In [47], the authors did not specify the constant in the exponent of running time. However, using the above formulae, we found out that their algorithm can achieve a time complexity

of  $2^{3.849n+o(n)}$  and space complexity of  $2^{2.023n+o(n)}$  at parameters  $\gamma = 0.78, \zeta = 1.27$  (without the birthday paradox, the algorithm in [47] can achieve time and space complexities of  $2^{5.179n+o(n)}$  and  $2^{3.01n+o(n)}$ , respectively, at parameters  $\gamma = 0.572, \zeta = 0.742$ ). In comparison, our algorithm can achieve a time and space complexity of  $2^{2.751n+o(n)}$  at parameters  $\gamma = 0.598, \zeta = 0.82$ .

For  $p = 2$ , we can use Theorem 1 to obtain a better bound on the number of lattice vectors that remain after all sieving iterations. This is reflected in the quantity  $c_b$ , which is then given by  $c_b^{(2)} = 0.401 + \log\left(\frac{2\zeta(2-\gamma)}{1-\gamma}\right)$  (Corollary 1). Furthermore,  $c_s^{(2)} = -0.5 \log\left(1 - \frac{1}{4\zeta^2}\right)$  (Lemma 3). At parameters  $\gamma = 0.693$  and  $\zeta = 0.99$ , we obtain  $c_{time}^{(2)} = c_{space}^{(2)} = 2.49$ . The AKS algorithm with the birthday paradox manages to achieve a time complexity of  $2^{2.571n+o(n)}$  and space complexity of  $2^{1.407n+o(n)}$  when  $\gamma = 0.589$  and  $\zeta = 0.9365$  [26]. Thus, our algorithm achieves a better time complexity at the cost of more space.

For  $p = \infty$ , we can reduce the space complexity by using the sub-division mentioned in Section 3.1 and achieve a space and time complexity of  $2^{2.443n+o(n)}$  at parameters  $\gamma = 0.501, \zeta = 0.738$  (in [49], the authors mentioned a time and space complexity of  $2^{2.82n+o(n)}$  in  $\ell_\infty$  norm. We obtain a slightly better running time by using  $c_b$ , as mentioned in this paper). Again, this is better than the time complexity of [47] (which is for all  $\ell_p$  norms).

#### 4. A Mixed Sieving Algorithm

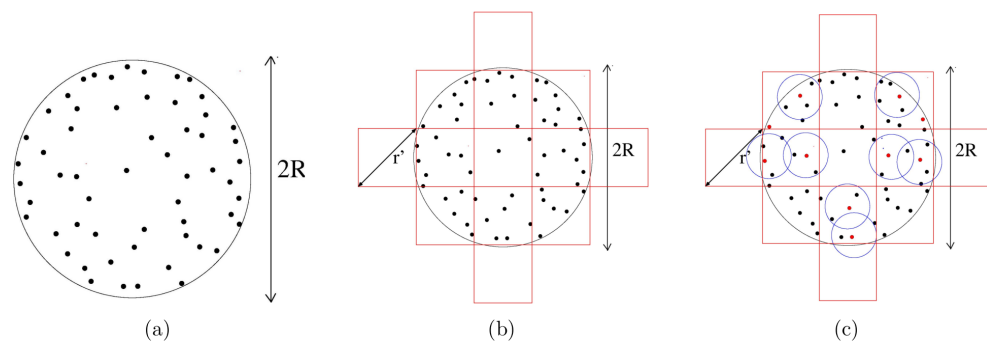
The main advantage in dividing the space (hyperball) into hypercubes (as we did in Linear Sieve) is the efficient “decodability” in the sense that a vector can be mapped to a sub-region (and thus be associated with a center) in  $O(n)$  time. However, the price we pay is in space complexity, because the number of hypercubes required to cover a hyperball is greater than the number of centers required if we used smaller hyperballs like in [21,47,48]. To reduce the space complexity, we perform a mixed sieving procedure. Double sieving techniques have been used for heuristic algorithms as in [32], where the rough idea is the following. There are two sets of centers: the first set consists of centers of larger radius balls, and for each such center, there is another set of centers of smaller radius balls within the respective large ball. In each sieving iteration, each non-center vector is mapped to the larger balls by comparing with the centers in the first set. Then, they are mapped to a smaller ball by comparing with the second set of centers. Thus, in both levels, a quadratic sieve is applied.

In our mixed sieving, the primary difference is the fact that in the two levels, we use two types of sieving methods: a linear sieve in the first level and then a quadratic sieve such as AKS in the next level. The overall outline of the algorithm is the same as in Algorithm 1, except at step 9, where we apply the following sieving procedure, which we call Mixed Sieve. An illustration is given in Figure 4.

The input to Mixed Sieve is a set of vectors of length  $R$ , and the output is a set of smaller vectors of length  $\gamma R$ .

1. We divide the whole space into large hypercubes of length  $\frac{A\gamma R}{n^{1/p}}$ , where  $A$  is some constant. In  $O(n)$  time, we map a vector to a large hypercube by comparing its co-ordinates. This has been explained in Section 3.1. We do not assign centers yet and do not perform any vector operation at this step. The distance between any two vectors mapped to the same hypercube is at most  $A\gamma R$  (Figure 4b).
2. Next, we perform the AKS sieving procedure within each hypercube. For each hypercube, we have a set (initially null) of centers. When a vector is mapped to a hypercube, we check if it is within distance  $\gamma R$  of any center (within that hypercube). If yes, then we subtract it from the center and add the resultant shorter vector to output set. If no, then we add this vector to the set of centers (Figure 4c).





**Figure 4.** One iteration of the mixed sieve in the  $\ell_2$  norm. (a) A number of vector pairs (solid black dots) with a (Euclidean) length of at most  $R$  are sampled. (b) The space is divided into hypercubes with diagonal length  $r'$ , and the vector pairs are mapped into each hypercube. (c) Within each hypercube, some vector pairs are selected as centers (red dots) and a hypercube is further sub-divided into a number of  $\ell_2$  balls, centered around these red dots. Then, vector subtraction is performed between the center and the vector pairs in each  $\ell_2$  ball (like AKS).

Using the same kind of counting method as in Section 3.1, we can say we need  $2^{c'n}$  large hypercubes, where  $c' = \log\left(2 + \frac{2}{A\gamma}\right)$ . The maximum distance between any two vectors in each hypercube is  $A\gamma R$ , and we want to get vectors of length at most  $\gamma R$  by applying the AKS sieve. Thus, the number of centers (let us call these “AKS sieve-centers”) within each hypercube is  $2^{c_p n + o(n)}$  where  $c_p = \log(1 + A)$  (in the special case of Euclidean norm, we have  $c_2 = 0.401 - \log\left(\frac{2}{A}\right)$ ).  $c_p$  (and  $c_2$ ) are obtained by applying Lemma 4. Note that the value of  $A$  must ensure the non-negativity of  $c_2$ . Thus, the total number of centers is  $2^{c^{(p)}n + o(n)}$  where  $c^{(p)} = c' + c_p$ .

To use the birthday paradox, we apply similar methods as given in Section 3.3 and [26]. Assume that we initially sample  $N \geq \frac{2}{q}(n^3 k 2^{c^{(p)}n + o(n)} + n 2^{\frac{c_b}{2}n})$  vectors. Then, using similar arguments as in Section 3, we can conclude that, with high probability, we end up with the shortest vector in the lattice. We are not re-writing the proof since it is similar to that in Theorem 3. The only thing that is slightly different is the number of center pairs set aside at the beginning of the sieving iterations. As in Section 3, we randomly divide the space  $n^3$  times into  $2^{c'n}$  hypercubes. Then, among the uniformly sampled vectors, we set aside  $2^{c_p n}$  vector pairs as centers for each hypercube. Thus, in Theorem 3, we replace  $|\mathcal{C}|$  by  $2^{c^{(p)}n + o(n)}$ .

Thus, space complexity is  $2^{c_{space}n + o(n)}$  where  $c_{space} = c_s + \max(c^{(p)}, c_b/2)$ . It takes  $O(n)$  time to map each vector to a large hypercube, and then at most  $2^{c_p n + o(n)}$  time to compare it with the “AKS sieve-centers” within each hypercube. Thus, the time complexity is  $2^{c_{time}n + o(n)}$  where  $c_{time} = \max(c_{space} + c_p, c_b)$ .

**Theorem 4.** Let  $\gamma \in (0, 1)$ ,  $\xi > 1/2$  and  $A$  be some constant. Given a full-rank lattice  $\mathcal{L} \subset \mathbb{Q}^n$ , there is a randomized algorithm for  $SVP^{(p)}$  with a success probability of at least  $1/2$ , a space complexity of at most  $2^{c_{space}n + o(n)}$ , and a running time of at most  $2^{c_{time}n + o(n)}$ . Here,  $c_{space} = c_s + \max(c^{(p)}, \frac{c_b}{2})$  and  $c_{time} = \max(c_{space} + c_p, c_b)$ .  $c_s = -\log\left(0.5 - \frac{1}{4\xi}\right)$ ,  $c_b = \log\left(1 + \frac{2\xi(2-\gamma)}{1-\gamma}\right)$ ,  $c_p = \log(1 + A)$  and  $c^{(p)} = \log\left(2 + \frac{2}{A\gamma}\right) + c_p$ .

In the Euclidean norm, we have  $c_2 = 0.401 - \log\left(\frac{2}{A}\right)$ ,  $c^{(2)} = \log\left(2 + \frac{2}{A\gamma}\right) + c_2$ ,  $c_s^{(2)} = -0.5 \log\left(1 - \frac{1}{4\xi^2}\right)$  and  $c_b^{(2)} = 0.401 + \log\left(\frac{2\xi(2-\gamma)}{1-\gamma}\right)$ .

*Comparison with previous provable sieving algorithms [20,27,28]*

In the Euclidean norm with parameters  $\gamma = 0.645$ ,  $\xi = 0.946$  and  $A = 2^{0.599}$ , we obtain a space and time complexity of  $2^{2.25n + o(n)}$ , while the List Sieve Birthday [26,28] has space and time complexities of  $2^{1.233n + o(n)}$  and  $2^{2.465n + o(n)}$ , respectively. We can also use a

different sieve in the second level, such as List Sieve [27], etc., which works in  $\ell_2$  norm and is faster than the AKS sieve. We can therefore expect to achieve a better running time.

The Discrete Gaussian-based sieving algorithm of Aggarwal et al. [20] with a time complexity of  $2^{n+o(n)}$  performs better than both our sieving techniques. However, their algorithm works for the Euclidean norm and, to the best of our knowledge, it has not been generalized to any other norm.

### 5. Approximation Algorithms for $SVP^{(p)}$ and $CVP^{(p)}$

In this section, we show how to adopt our sieving techniques to approximation algorithms for  $SVP^{(p)}$  and  $CVP^{(p)}$ . The analysis and explanations are similar to that given in [49]. For completeness, we give a brief outline.

#### 5.1. Algorithm for Approximate $SVP^{(p)}$

We note that at the end of the sieving procedure in Algorithm 1, we obtain lattice vectors of length at most  $R' = \frac{\xi(2-\gamma)\lambda}{1-\gamma} + O(\lambda/n)$ . Thus, if we can ensure that one of the vectors obtained at the end of the sieving procedure is non-zero, we obtain a  $\tau = \frac{\xi(2-\gamma)}{1-\gamma} + o(1)$ -approximation of the shortest vector. Consider a new algorithm  $\mathcal{A}$  (let us call it Approx-SVP) that is identical to Algorithm 1, except that Step 12 is replaced by the following:

- Find a non-zero vector  $\mathbf{v}_0$  in  $\{(\mathbf{y}_i - \mathbf{e}_i) : (\mathbf{e}_i, \mathbf{y}_i) \in S\}$ .

We now show that if we start with sufficiently many vectors, we must obtain a non-zero vector.

**Lemma 11.** *If  $N \geq \frac{2}{q}(k|C| + 1)$ , then with a probability of at least  $1/2$ , Algorithm  $\mathcal{A}$  outputs a non-zero vector in  $\mathcal{L}$  of a length of at most  $\frac{\xi(2-\gamma)\lambda}{1-\gamma} + O(\lambda/n)$  with respect to  $\ell_p$  norm.*

**Proof.** Of the  $N$  vector pairs  $(\mathbf{e}, \mathbf{y})$  sampled in steps 2–6 of Algorithm  $\mathcal{A}$ , we consider those such that  $\mathbf{e} \in (D_1 \cup D_2)$ . We have already seen there are at least  $\frac{qN}{2}$  such pairs. We remove  $|C|$  vector pairs in each of the  $k$  sieve iterations. Thus, at step 12 of Algorithm 1, we have  $N' \geq 1$  pairs  $(\mathbf{e}, \mathbf{y})$  to process.

With a probability of  $1/2$ ,  $\mathbf{e}$ , and hence  $\mathbf{w} = \mathbf{y} - \mathbf{e}$  is replaced by either  $\mathbf{w} + \mathbf{u}$  or  $\mathbf{w} - \mathbf{u}$ . Thus, the probability that this vector is the zero vector is at most  $1/2$ .  $\square$

We thus obtain the following result.

**Theorem 5.** *Let  $\gamma \in (0, 1)$ ,  $\xi > 1/2$  and  $\tau = \frac{\xi(2-\gamma)}{1-\gamma} + o(1)$ . Assume we are given a full-rank lattice  $\mathcal{L} \subset \mathbb{Q}^n$ . There is a randomized algorithm that  $\tau$  approximates  $SVP^{(p)}$  with a success probability of at least  $1/2$  and a space and time complexity  $2^{(c_s+c_c)n+o(n)}$ , where  $c_c = \log\left(2 + \frac{2}{\gamma}\right)$ , and  $c_s = -\log\left(0.5 - \frac{1}{4\xi}\right)$ .*

Note that while presenting the above theorem, we assumed that we are using the Linear Sieve in Algorithm 1. We can also use the Mixed Sieve procedure as described in Section 4. Then, we will obtain space and time complexities of  $2^{(c_s+c^{(p)})n+o(n)}$  and  $2^{(c_s+c^{(p)}+c_p)n+o(n)}$ , respectively, where  $c^{(p)} = \log\left(2 + \frac{2}{A\gamma}\right) + c_p$  and  $c_p = \log(1 + A)$ , respectively (in the Euclidean norm, the parameters are as described in Theorem 4).

*Comparison with provable approximation algorithms [30,47,48]*

We have mentioned in Section 1 that [47,48] gave approximation algorithms for lattice problems that work for all  $\ell_p$  norms and use the quadratic sieving procedure (as has

been described before). Using our notations, the space and time complexities of their approximate algorithms are  $2^{c_{space}(BN)n+o(n)}$  and  $2^{c_{time}(BN)n+o(n)}$ , respectively, where

$$\begin{aligned} c_{space}(BN) &= c_s + c_c(BN) \\ \text{and } c_{time}(BN) &= c_{space}(BN) + c_c(BN) = c_s + 2c_c(BN). \end{aligned}$$

The authors did not mention any explicit value of the constant in the exponent. Using the above formulae, we conclude that [47,48] can achieve time and space complexities of  $2^{3.169n+o(n)}$  and  $2^{1.586n+o(n)}$ , respectively, at parameters  $\gamma = 0.99, \xi = 10.001$  with a large constant approximation factor. In comparison, we can achieve a space and time complexity of  $2^{2.001n+o(n)}$  with a large constant approximation factor at the same parameters.

In  $\ell_2$  norm, using the mixed sieving procedure, we obtain a time and space complexity of  $2^{1.73n+o(n)}$  and a large constant approximation factor at parameters  $\gamma = 0.999, \xi = 1$ . In [30], the best running time reported is  $2^{0.802n}$  for a large approximation factor.

Using a similar linear sieve, a time and space complexity of  $3^n$  i.e.,  $2^{1.585n+o(n)}$  can be achieved for the  $\ell_\infty$  norm for a large constant approximation factor [49].

### 5.2. Algorithm for Approximate CVP<sup>(p)</sup>

Given a lattice  $\mathcal{L}$  and a target vector  $\mathbf{t}$ , let  $d$  denote the distance of the closest vector in  $\mathcal{L}$  to  $\mathbf{t}$ . Just as in Section 3.2, we assume that we know the value of  $d$  within a factor of  $1 + 1/n$ . We can get rid of this assumption by using Babai’s [68] algorithm to guess the value of  $d$  within a factor of  $2^n$  and then run our algorithm for polynomially many values of  $d$ .

For  $\tau > 0$ , define the following  $(n + 1)$ -dimensional lattice  $\mathcal{L}'$

$$\mathcal{L}' = \mathcal{L} \left( \{(\mathbf{v}, 0) : \mathbf{v} \in \mathcal{L}\} \cup \{(\mathbf{t}, \tau d/2)\} \right).$$

Let  $\mathbf{z}^* \in \mathcal{L}$  be the lattice vector closest to  $\mathbf{t}$ .

Then  $\mathbf{u} = (\mathbf{z}^* - \mathbf{t}, -\tau d/2) \in \mathcal{L}' \setminus (\mathcal{L} - k'\mathbf{t}, 0)$  for some  $k' \in \mathbb{Z}$ .

We sample  $N$  vector pairs  $(\mathbf{e}, \mathbf{y}) \in B_n^{(p)}(\xi d) \times \mathcal{P}(\mathbf{B}')$  (8–12 of Algorithm 3), where  $\mathbf{B}' = [(\mathbf{b}_1, 0), \dots, (\mathbf{b}_n, 0), (\mathbf{t}, \tau d/2)]$  is a basis for  $\mathcal{L}'$ . Next, we run a number of iterations of the sieving Algorithm 2 to obtain a number of vector pairs such that  $\|\mathbf{y}\|_p \leq R = \frac{\xi d}{1-\gamma} + o(1)$ . Further details can be found in Algorithm 3. Note that in the algorithm,  $\mathbf{v}|_{[n]}$  is the  $n$ -dimensional vector  $\mathbf{v}'$  obtained by restricting  $\mathbf{v}$  to the first  $n$  co-ordinates (with respect to the computational basis).

From Lemma 7, we have seen that after  $\lceil \log_\gamma \left( \frac{\xi}{nR_0(1-\gamma)} \right) \rceil$  iterations (where  $R_0 = n \cdot \max_i \|\mathbf{b}_i\|_p$ ),  $R \leq \frac{\xi\gamma}{n(1-\gamma)} + \frac{\xi d}{1-\gamma} \left[ 1 - \frac{\xi}{nR_0(1-\gamma)} \right]$ . Thus, after the sieving iterations, the set  $S'$  consists of vector pairs such that the corresponding lattice vector  $\mathbf{v}$  has  $\|\mathbf{v}\|_p \leq \frac{\xi d}{1-\gamma} + \xi d + c = \frac{\xi(2-\gamma)d}{1-\gamma} + o(1)$ .

Selecting  $\xi < \frac{(1-\gamma)\tau}{2-\gamma} - o(1)$  ensures that our sieving algorithm does not return vectors from  $(\mathcal{L}, 0) - (k'\mathbf{t}, k'\tau d/2)$  for some  $k'$  such that  $|k'| \geq 2$ . Then, every vector has  $\|\mathbf{v}\|_p < \tau d$ , and so either  $\mathbf{v} = \pm(\mathbf{z}' - \mathbf{t}, 0)$  or  $\mathbf{v} = \pm(\mathbf{z} - \mathbf{t}, -\tau d/2)$  for some lattice vector  $\mathbf{z}, \mathbf{z}' \in \mathcal{L}$ .

With similar arguments as in [49] (using the tossing argument outlined in Section 3.2), we can conclude that with some non-zero probability we have at least one vector in  $\mathcal{L}' \setminus (\mathcal{L} \pm \mathbf{t}, 0)$  after the sieving iterations.

Thus, we obtain the following result.

---

**Algorithm 3:** Approximate algorithm for  $CVP^{(p)}$

---

**Input:** (i) A basis  $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$  of a lattice  $L$ , (ii) Target vector  $\mathbf{t}$ , (iii) Approximation factor  $\tau$ , (iv)  $0 < \gamma < 1$ , (v)  $\xi$  such that  $\frac{1}{2} \max(1, \tau/2) < \xi < \frac{(1-\gamma)\tau}{2-\gamma} - c'$  where  $c'$  is a small constant, (vi)  $\alpha > 0$ , (vii)  $N \in \mathbb{N}$

**Output:** A  $2\tau$ -approximate closest vector to  $\mathbf{t}$  in  $L$

```

1  $d \leftarrow (1 + \alpha)$ ;
2  $T \leftarrow \emptyset$ ;  $S'' \leftarrow \emptyset$ ;
3 while  $d \leq n \cdot \max_i \|\mathbf{b}_i\|_p$  do
4    $S, S' \leftarrow \emptyset$ ;
5    $\mathbf{B}' \rightarrow [(\mathbf{b}_1, 0), \dots, (\mathbf{b}_n, 0), (\mathbf{t}, \tau d/2)]$ ;
6    $L' \rightarrow \mathcal{L}(\mathbf{B}')$ ;
7    $M \rightarrow \text{span}(\{(\mathbf{v}, 0) : \mathbf{v} \in L\})$ ;
8   for  $i = 1$  to  $N$  do
9      $\mathbf{e}_i \leftarrow_{\text{uniform}} B_n^{(p)}(0, \xi\lambda)$ ;
10     $\mathbf{y}_i \leftarrow \mathbf{e}_i \bmod \mathcal{P}(\mathbf{B})$ ;
11     $S \leftarrow S \cup \{(\mathbf{e}_i, \mathbf{y}_i)\}$ ;
12  end
13   $R \leftarrow n \max_i \|\mathbf{b}_i\|_p$ ;
14  while  $R > \frac{\xi d}{1-\gamma}$  do
15     $S \leftarrow \text{sieve}(S, \gamma, R, \xi)$  using Algorithm 2;
16     $R \leftarrow \gamma R + \xi d$ ;
17  end
18   $S' \leftarrow \{\mathbf{y} - \mathbf{e} : (\mathbf{e}, \mathbf{y}) \in S\}$ ;
19  Compute  $\mathbf{w} \in S'$  such that
     $\|\mathbf{w}\|_{[n]} = \min\{\|\mathbf{v}'\|_{[n]} : \mathbf{v}' \in S' \text{ and } (\mathbf{v}')_{n+1} \neq 0\}$ ;
20   $T \rightarrow T \cup \{\mathbf{w}\}$ ;
21   $d \rightarrow d(1 + \alpha)$ ;
22 end
23 Let  $\mathbf{v}_0$  be any vector in  $T$  such that  $\|\mathbf{v}_0\|_{[n]} = \min\{\|\mathbf{w}\|_{[n]} : \mathbf{w} \in T\}$ ;
24  $\mathbf{v}'_0 \leftarrow \mathbf{v}_0|_{[n]}$ ;
25 if  $(\mathbf{v}_0)_{n+1} = -\tau d/2$  then
26 | return  $\mathbf{v}'_0 + \mathbf{t}$ ;
27 else
28 | return  $\mathbf{v}'_0 - \mathbf{t}$ ;
29 end

```

---

**Theorem 6.** Let  $\gamma \in (0, 1)$ , and for any  $\tau > 1$  let  $\xi > \max(1/2, \tau/4)$ . Given a full-rank lattice  $\mathcal{L} \subset \mathbb{Q}^n$ , there is a randomized algorithm that, for  $\tau = \frac{\xi(2-\gamma)}{1-\gamma} + o(1)$ , approximates  $CVP^{(p)}$  with a success probability of at least  $1/2$  and a space and time complexity of  $2^{(c_s+c_c)n+o(n)}$ , where  $c_c = \log\left(2 + \frac{2}{\gamma}\right)$  and  $c_s = -\log\left(0.5 - \frac{1}{4\xi}\right)$ .

Again, using Mixed Sieve in Algorithm 1, we obtain space and time complexities of  $2^{(c_s+c^{(p)})n+o(n)}$  and  $2^{(c_s+c^{(p)}+c_p)n+o(n)}$ , respectively, where  $c^{(p)} = \log\left(2 + \frac{2}{A\gamma}\right) + c_p$  and  $c_p = \log(1 + A)$ , respectively (in the Euclidean norm, the parameters are as described in Theorem 4).

### 6. Discussions

In this paper, we have designed new sieving algorithms that work for any  $\ell_p$  norm. A comparative performance evaluation has been given in Table 1. We achieve a better time complexity at the cost of space complexity for every  $1 \leq p \leq \infty$ , except for the algorithm

in [20] that employs a Discrete Gaussian-based sieving algorithm and has better space and time complexity in the Euclidean norm. To the best of our knowledge, this algorithm does not work for any other norm.

**Table 1.** Comparison of the performance of various sieving algorithms in different  $\ell_p$  norms. In the last row, DGS stands for Discrete Gaussian Sampling-based sieve.

$p$	Ref.	Type of Sieve	Time Complexity	Space Complexity
$1 \leq p \leq \infty$	[47]	Quadratic	$2^{3.849n+o(n)}$	$2^{2.023n+o(n)}$
	This work	Linear	$2^{2.751n+o(n)}$	$2^{2.751n+o(n)}$
$p = \infty$	[49]	Linear	$2^{2.443n+o(n)}$	$2^{2.443n+o(n)}$
	[26]	Quadratic	$2^{2.571n+o(n)}$	$2^{1.407n+o(n)}$
	This work	Linear	$2^{2.49n+o(n)}$	$2^{2.49n+o(n)}$
$p = 2$	[26,27]	Quadratic	$2^{2.465n+o(n)}$	$2^{1.233n+o(n)}$
	This work	Mixed	$2^{2.25n+o(n)}$	$2^{2.25n+o(n)}$
	[20]	DGS	$2^{n+o(n)}$	$2^{n+o(n)}$

#### Future Work

An obvious direction for further research would be to design heuristic algorithms on these kind of sieving techniques and to study if these can be adapted to other computing environments like parallel computing.

The major difference between our algorithm and the others like [21,47] is in the choice of the shape of the sub-regions in which we divide the ambient space (as has already been explained before). Due to this we get superior “decodability” in the sense that a vector can be efficiently mapped to a sub-region, at the cost of inferior space complexity, as described before. It might be interesting to study what other shapes of these sub-regions might be considered and what are the trade-offs we get.

It might be possible to improve the bound on the number of hypercubes required to cover the hyperball. At least in the  $\ell_\infty$  norm we have seen that the number of hypercubes may depend on the initial position of the smaller hypercube, whose translates cover the bigger hyperball. In fact it might be possible to get some lower bound on the complexity of this kind of approach.

**Funding:** Research at IQC was supported in part by the Government of Canada through Innovation, Science and Economic Development Canada, Public Works and Government Services Canada, and Canada First Research Excellence Fund.

**Acknowledgments:** The author would like to acknowledge the anonymous reviewers for their helpful comments that have helped to improve the manuscript significantly.

**Conflicts of Interest:** The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

#### References

1. Lenstra, A.K.; Lenstra, H.W., Jr.; Lovász, L. Factoring polynomials with rational coefficients. *Math. Ann.* **1982**, *261*, 515–534. [[CrossRef](#)]
2. Lenstra, H.W., Jr. Integer programming with a fixed number of variables. *Math. Oper. Res.* **1983**, *8*, 538–548. [[CrossRef](#)]
3. Kannan, R. Minkowski’s convex body theorem and integer programming. *Math. Oper. Res.* **1987**, *12*, 415–440. [[CrossRef](#)]
4. Dadush, D.; Peikert, C.; Vempala, S. Enumerative lattice algorithms in any norm via  $m$ -ellipsoid coverings. In Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, Palm Springs, CA, USA, 22–25 October 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 580–589.
5. Eisenbrand, F.; Hähnle, N.; Niemeier, M. Covering cubes and the closest vector problem. In Proceedings of the Twenty-Seventh Annual Symposium on Computational Geometry, Paris, France, 13–15 June 2011; ACM: New York, NY, USA, 2011; pp. 417–423.

6. Odlyzko, A.M. The rise and fall of knapsack cryptosystems. *Cryptol. Comput. Number Theory* **1990**, *42*, 75–88.
7. Joux, A.; Stern, J. Lattice reduction: A toolbox for the cryptanalyst. *J. Cryptol.* **1998**, *11*, 161–185. [[CrossRef](#)]
8. Nguyen, P.Q.; Stern, J. The two faces of lattices in cryptology. In *Cryptography and Lattices*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 146–180.
9. Landau, S.; Miller, G.L. Solvability by radicals is in polynomial time. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*; ACM: New York, NY, USA, 1983; pp. 140–151.
10. Coster, M.J.; Joux, A.; LaMacchia, B.A.; Odlyzko, A.M.; Schnorr, C.; Stern, J. Improved low-density subset sum algorithms. *Comput. Complex* **1992**, *2*, 111–128. [[CrossRef](#)]
11. Ajtai, M. Generating hard instances of lattice problems. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, Philadelphia, PA, USA, 22–24 May 1996; ACM: New York, NY, USA, 1996; pp. 99–108.
12. Micciancio, D.; Regev, O. Worst-case to average-case reductions based on Gaussian measures. *SIAM J. Comput.* **2007**, *37*, 267–302. [[CrossRef](#)]
13. Gentry, C. Fully homomorphic encryption using ideal lattices. In *Proceedings of the STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing*, Bethesda, MD, USA, 31 May–2 June 2009; ACM: New York, NY, USA, 2009; pp. 169–178.
14. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* **2009**, *56*, 34. [[CrossRef](#)]
15. Brakerski, Z.; Vaikuntanathan, V. Efficient fully homomorphic encryption from (standard) LWE. In *Proceedings of the FOCS*, Palm Springs, CA, USA, 23–25 October 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 97–106.
16. Brakerski, Z.; Langlois, A.; Peikert, C.; Regev, O.; Stehlé, D. Classical hardness of learning with errors. In *Proceedings of the STOC*, Palo Alto, CA, USA, 1–4 June, 2013; pp. 575–584.
17. Brakerski, Z.; Vaikuntanathan, V. Lattice-based FHE as secure as PKE. In *Proceedings of the ITCS*, Princeton, NJ, USA, 12–14 January 2014; pp. 1–12.
18. Peikert, C. A decade of lattice cryptography. *Found. Trends Theor. Comput. Sci.* **2016**, *10*, 283–424. [[CrossRef](#)]
19. Ducas, L.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehlé, D. Crystals–Dilithium: Digital Signatures from Module Lattices. *IACR Transactions on Symmetric Cryptology*. 2018. pp. 238–268. Available online: <https://repository.ubn.ru.nl/bitstream/handle/2066/191703/191703.pdf> (accessed on 8 December 2021).
20. Aggarwal, D.; Dadush, D.; Regev, O.; Stephens-Davidowitz, N. Solving the Shortest Vector Problem in  $2^n$  time via Discrete Gaussian sampling. In *Proceedings of the STOC*, Portland, OR, USA, 14–17 June 2015.
21. Ajtai, M.; Kumar, R.; Sivakumar, D. A sieve algorithm for the shortest lattice vector problem. In *Proceedings of the STOC*, Heraklion, Greece, 6–8 July 2001; pp. 601–610.
22. Fincke, U.; Pohst, M. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comput.* **1985**, *44*, 463–471. [[CrossRef](#)]
23. Schnorr, C.-P. A hierarchy of polynomial time lattice basis reduction algorithms. *Theor. Comput. Sci.* **1987**, *53*, 201–224. [[CrossRef](#)]
24. Micciancio, D.; Voulgaris, P. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. *SIAM J. Comput.* **2013**, *42*, 1364–1391. [[CrossRef](#)]
25. Dadush, D.; Vempala, S.S. Near-optimal deterministic algorithms for volume computation via m-ellipsoids. *Proc. Natl. Acad. Sci. USA* **2013**, *110*, 19237–19245. [[CrossRef](#)]
26. Hanrot, G.; Pujol, X.; Stehlé, D. Algorithms for the shortest and closest lattice vector problems. In *International Conference on Coding and Cryptology*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 159–190.
27. Micciancio, D.; Voulgaris, P. Faster exponential time algorithms for the shortest vector problem. In *Proceedings of the SODA*, Austin, TX, USA, 17–19 January 2010; pp. 1468–1480.
28. Pujol, X.; Stehlé, D. Solving the shortest lattice vector problem in time  $2^{2 \cdot 465n}$ . *IACR Cryptol. ePrint Arch.* **2009**, *2009*, 605.
29. Aggarwal, D.; Stephens-Davidowitz, N. Just take the average! an embarrassingly simple  $2^n$ -time algorithm for SVP (and CVP). *arXiv* **2017**, arXiv:1709.01535.
30. Liu, M.; Wang, X.; Xu, G.; Zheng, X. Shortest lattice vectors in the presence of gaps. *IACR Cryptol. ePrint Arch.* **2011**, *2011*, 139.
31. Nguyen, P.Q.; Vidick, T. Sieve algorithms for the shortest vector problem are practical. *J. Math. Cryptol.* **2008**, *2*, 181–207. [[CrossRef](#)]
32. Wang, X.; Liu, M.; Tian, C.; Bi, J. Improved Nguyen-Vidick heuristic sieve algorithm for shortest vector problem. In *Proceedings of the AsiaCCS*, Hong Kong, China, 22–24 March 2011; pp. 1–9.
33. Becker, A.; Ducas, L.; Gama, N.; Laarhoven, T. New directions in nearest neighbor searching with applications to lattice sieving. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, Arlington, VA, USA, 10–12 January 2016; Society for Industrial and Applied Mathematics: Philadelphia, PA, USA, 2016; pp. 10–24.
34. Laarhoven, T.; de Weger, B. Faster sieving for shortest lattice vectors using spherical locality-sensitive hashing. In *International Conference on Cryptology and Information Security in Latin America*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 101–118.
35. Becker, A.; Laarhoven, T. Efficient (ideal) lattice sieving using cross-polytope LSH. In *International Conference on Cryptology in Africa*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 3–23.
36. Herold, G.; Kirshanova, E. Improved algorithms for the approximate k-list problem in Euclidean norm. In *IACR International Workshop on Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 16–40.
37. Herold, G.; Kirshanova, E.; Laarhoven, T. Speed-ups and time–memory trade-offs for tuple lattice sieving. In *IACR International Workshop on Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 407–436.

38. Laarhoven, T.; Mariano, A. Progressive lattice sieving. In *International Conference on Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 292–311.
39. Mariano, A.; Bischof, C. Enhancing the scalability and memory usage of hash sieve on multi-core CPUs. In Proceedings of the 2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), Heraklion, Greece, 17–19 February 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 545–552.
40. Mariano, A.; Laarhoven, T.; Bischof, C. A parallel variant of LD sieve for the SVP on lattices. In Proceedings of the 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), St. Petersburg, Russia, 6–8 March 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 23–30.
41. Yang, S.-Y.; Kuo, P.-C.; Yang, B.-Y.; Cheng, C.-M. Gauss sieve algorithm on GPUs. In *Cryptographers' Track at the RSA Conference*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 39–57.
42. Ducas, L. Shortest vector from lattice sieving: A few dimensions for free. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 125–145.
43. Albrecht, M.R.; Ducas, L.; Herold, G.; Kirshanova, E.; Postlethwaite, E.W.; Stevens, M. The general sieve kernel and new records in lattice reduction. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 717–746.
44. Goldreich, O.; Micciancio, D.; Safra, S.; Seifert, J.-P. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Inf. Process. Lett.* **1999**, *71*, 55–61. [[CrossRef](#)]
45. Ajtai, M.; Kumar, R.; Sivakumar, D. Sampling short lattice vectors and the closest lattice vector problem. In Proceedings of the CCC, Beijing, China, 15–20 April 2002; pp. 41–45.
46. Aggarwal, D.; Dadush, D.; Stephens-Davidowitz, N. Solving the closest vector problem in  $2^n$  time—the Discrete Gaussian strikes again! In Proceedings of the Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium, Berkeley, CA, USA, 18–20 October 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 563–582.
47. Blömer, J.; Naewe, S. Sampling methods for shortest vectors, closest vectors and successive minima. *Theor. Comput. Sci.* **2009**, *410*, 1648–1665. [[CrossRef](#)]
48. Arvind, V.; Joglekar, P.S. Some sieving algorithms for lattice problems. In *LIPICs-Leibniz International Proceedings in Informatics*; Schloss Dagstuhl-Leibniz-Zentrum für Informatik: Wadern, Germany, 2008; Volume 2.
49. Aggarwal, D.; Mukhopadhyay, P. Improved algorithms for the shortest vector problem and the closest vector problem in the infinity norm. *arXiv* **2018**, arXiv:1801.02358.
50. van Emde Boas, P. *Another NP-Complete Partition Problem and the Complexity of Computing Short Vectors in a Lattice*; Technical Report; Department of Mathematics, University of Amsterdam: Amsterdam, The Netherlands, 1981.
51. Ajtai, M. The shortest vector problem in  $\ell_2$  is NP-hard for randomized reductions. In Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, Dallas, TX, USA, 24–26 May 1998; ACM: New York, NY, USA, 1998; pp. 10–19.
52. Micciancio, D. The shortest vector problem is NP-hard to approximate to within some constant. *SIAM J. Comput.* **2001**, *30*, 2008–2035. [[CrossRef](#)]
53. Dinur, I.; Kindler, G.; Raz, R.; Safra, S. Approximating CVP to within almost-polynomial factors is NP-hard. *Combinatorica* **2003**, *23*, 205–243. [[CrossRef](#)]
54. Dinur, I. Approximating  $SVP_\infty$  to within almost-polynomial factors is NP-hard. In *Italian Conference on Algorithms and Complexity*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 263–276.
55. Mukhopadhyay, P. The projection games conjecture and the hardness of approximation of SSAT and related problems. *J. Comput. Syst. Sci.* **2021**, *123*, 186–201. [[CrossRef](#)]
56. Moshkovitz, D. The projection games conjecture and the NP-hardness of  $\ln n$ -approximating Set-Cover. *Theory Comput.* **2015**, *11*, 221–235. [[CrossRef](#)]
57. Khot, S. Hardness of approximating the shortest vector problem in lattices. *J. ACM* **2005**, *52*, 789–808. [[CrossRef](#)]
58. Haviv, I.; Regev, O. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. *Theory Comput.* **2012**, *8*, 513–531. [[CrossRef](#)]
59. Bennett, H.; Golovnev, A.; Stephens-Davidowitz, N. On the quantitative hardness of CVP. *arXiv* **2017**, arXiv:1704.03928.
60. Aggarwal, D.; Stephens-Davidowitz, N. (gap/S)ETH hardness of SVP. In Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, Los Angeles, CA, USA, 25–29 June 2018; ACM: New York, NY, USA, 2018; pp. 228–238.
61. Dadush, D.; Kun, G. Lattice sparsification and the approximate closest vector problem. In Proceedings of the Twenty-Fourth annual ACM-SIAM Symposium on Discrete Algorithms, New Orleans LA, USA, 6–8 January 2013; Society for Industrial and Applied Mathematics: Philadelphia, PA, USA, 2013; pp. 1088–1102.
62. Dyer, M.; Frieze, A.; Kannan, R. A random polynomial-time algorithm for approximating the volume of convex bodies. *J. ACM* **1991**, *38*, 1–17. [[CrossRef](#)]
63. Goldreich, O.; Goldwasser, S. On the limits of nonapproximability of lattice problems. *J. Comput. Syst. Sci.* **2000**, *60*, 540–563. [[CrossRef](#)]
64. Blömer, J.; Naewe, S. Sampling methods for shortest vectors, closest vectors and successive minima. In *International Colloquium on Automata, Languages, and Programming*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 65–77.
65. Kabatiansky, G.A.; Levenshtein, V.I. On bounds for packings on a sphere and in space. *Probl. Peredachi Informatsii* **1978**, *14*, 3–25.
66. Pisier, G. *The Volume of Convex Bodies and Banach Space Geometry*; Cambridge University Press: Cambridge, UK, 1999; Volume 94.

- 
67. Regev, O. *Lecture Notes on Lattices in Computer Science*, New York University: New York, NY, USA, 2009.
  68. Babai, L. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica* **1986**, *6*, 1–13. [[CrossRef](#)]