Faster Deterministic Volume Estimation in the Oracle model via Thin Lattice Coverings

Daniel Dadush[1]

1 **Centrum Wiskunde & Informatica, Netherlands**
`dadush@cwi.nl`

Abstract

We give a $2^{O(n)}(1+1/\varepsilon)^n$ time and poly(n)-space deterministic algorithm for computing a $(1+\varepsilon)^n$ approximation to the volume of a general convex body K, which comes close to matching the $(1+c/\varepsilon)^{n/2}$ lower bound for volume estimation in the oracle model by Bárány and Füredi [11, 12]. This improves on the previous results of [8], which gave the above result only for *symmetric bodies* and achieved a dependence of $2^{O(n)}(1+\log^{5/2}(1/\varepsilon)/\varepsilon^3)^n$.

For our methods, we reduce the problem of volume estimation in K to counting lattice points (via enumeration) in $K \subseteq \mathbb{R}^n$ for a specially constructed lattice $\mathcal{L}$: a so-called *thin covering of space* with respect to K (more precisely, for which $\mathcal{L} + K = \mathbb{R}^n$ and $\det(\mathcal{L})/\mathrm{vol}(K) = 2^{O(n)}$). The tradeoff between time and approximation ratio is achieved by scaling down the lattice.

As our main technical contribution, we give the first deterministic $2^{O(n)}$ time and poly(n)-space construction for thin covering lattices with respect to general convex bodies. This improves on a recent construction of [1] which requires exponential space, and only worked for symmetric bodies. For our construction, we combine the use of the M-ellipsoid from convex geometry [21] together with lattice sparsification and densification techniques [23, 6].

1998 ACM Subject Classification F.2.2

Keywords and phrases Deterministic Volume Estimation, Convex Geometry, Lattice Coverings of Space, Lattice Point Enumeration

Digital Object Identifier 10.4230/LIPIcs.xxx.yyy.p

1 Introduction

The problem of estimating the volume of a convex body is one of the most fundamental and well studied problems in high dimensional geometry. It is also one of the most striking examples of the *power of randomization*. In [11, 12], Bárány and Füredi showed that any deterministic volume algorithm for n dimensional convex bodies having access only to a membership oracle (which returns whether a point is in the convex body or not), requires at least $(1+c/\varepsilon)^{n/2}$ membership queries to estimate volume to within a $(1+\varepsilon)^n$ factor, for $c > 0$ an absolute constant any ε small enough. In particular, an $O(1)$-approximation requires $n^{\Omega(n)}$ queries. In a breakthrough result however, Dyer,Frieze and Kannan [9] showed that if the algorithm is allowed to err with small probability, then even a $(1+\varepsilon)$ approximation can be obtained in $\mathrm{poly}(n, 1/\varepsilon)$ time. Their algorithm relied on novel Monte Carlo Markov Chain techniques that spurred much further research. These works left a major open question: can the volume algorithm be made deterministic when the description of the convex body is given explicitly (e.g. a polytope given by its inequalities)?

A related (and more modest) question, which has only recently received attention, is whether one can come close to matching the lower bounds of Bárány and Füredi for deterministic volume computation in oracle model. We note it was open to achieve such bounds deterministically even for explicitly presented polytopes. This was recently answered in the affirmative by Vempala and the author in [8], which gave a deterministic $2^{O(n)}(1+\log^{5/2}(1/\varepsilon)/\varepsilon^3)^n$ time and polynomial space algorithm for estimating the volume of a *symmetric* convex body K (K is symmetric if $K = -K$) to within $(1+\varepsilon)^n$. The main tool developed there was an algorithmic version of (variants of) Milman's construction for the *M-ellipsoid* in convex geometry. An M-ellipsoid of an n-dimensional convex body K is an ellipsoid E (a linear transformation of the Euclidean unit ball) satisfying that $2^{O(n)}$ translates of E suffice to cover K and vice versa. Note that an M-ellipsoid immediately provides a $2^{O(n)}$ factor approximation to volume.

From the above, two natural avenues of improvement were to reduce the dependence on ε and to generalize the result to asymmetric convex bodies.

2 Results

We make improvements on both the above fronts. Our main result is stated below.

▶ **Theorem 1** (Volume Estimation). *For a convex body $K \subseteq \mathbb{R}^n$ given by a membership oracle, and any $\varepsilon > 0$, one can compute $V \geq 0$ satisfying $\mathrm{vol}_n(K) \leq V \leq (1+\varepsilon)^n \mathrm{vol}_n(K)$ in deterministic $2^{O(n)}(1+1/\varepsilon)^n$ time and $\mathrm{poly}(n)$ space.*

Both the algorithm and that of [8] share the same high level approach, namely, reducing volume estimation to counting lattice points within a carefully chosen convex body and lattice.

For large constant ε, we note that the volume of an M-ellipsoid already a good enough volume approximation for K, and hence lattice point counting is not needed. This holds for general convex bodies as well, by replacing K with $K - K$ (an oracle for which can be efficiently computed) and using standard volume inequalities relating these two. Hence the above result is truly interesting for the case of small constant ε.

The lattices we shall use for the counting reduction will be so-called *thin coverings of space* with respect to K (or a related body). The technical heart of our volume algorithm, and our main technical contribution, is an algorithmic construction of such lattices with *good* *enumeration properties.* In section 3.1, we will explain their role in our volume estimation algorithm in detail.

We now formally define the many relevant lattice concepts.

▶ **Definition 2** (Lattice). An n-dimensional lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is defined as all integer combinations of some basis $B = (\mathbf{b}_1, \dots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$.

The determinant of the lattice is defined as $\det(\mathcal{L}) = |\det(B)|$, and is invariant to the choice of lattice basis.

The determinant above can also be interpreted as the volume of the (symmetric) parallelepiped $\mathcal{P}(B) = B[-1/2, 1/2)^n$. More generally, any (measurable) set S which tiles $\mathbb{R}^n$ with respect to $\mathcal{L}$, i.e. $\mathcal{L} + S = \mathbb{R}^n$ and distinct lattice shifts of S are pairwise disjoint, satisfies $\mathrm{vol}_n(S) = \det(\mathcal{L})$ (note that $\mathcal{P}(B)$ tiles).

For a symmetric convex body K, we define $\|\mathbf{x}\|_K = \inf\{s \geq 0 : \mathbf{x} \in sK\}$ as the norm induced by K, which satisfies all norm properties.

▶ **Definition 3** (Lattice Packing). Let $\mathcal{L}$ be an n-dimensional lattice. For an n-dimensional symmetric convex body $K \subseteq \mathbb{R}^n$, we let

$$\lambda_1(K, \mathcal{L}) = \min_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{y}\|_K ,$$

denote the length of the shortest non-zero vector (or minimum distance) of $\mathcal{L}$ under $\|\cdot\|_K$.

$\mathcal{L}$ is packing with respect to K (or vice versa) if all distinct lattice shifts of K are pairwise interior disjoint, or equivalently, if $\lambda_1(K, \mathcal{L}) \geq 2$. The *packing density* of $\mathcal{L}$ with respect to K is $\mathrm{vol}_n(\lambda/2K)/\det(\mathcal{L})$, for $\lambda = \lambda_1(K, \mathcal{L})$.

▶ **Definition 4** (Lattice Covering). Let $\mathcal{L}$ be an n-dimensional lattice. For a set $C \subseteq \mathbb{R}^n$, we let $\mu(C, \mathcal{L}) = \inf\{s \geq 0 : \mathcal{L} + sC = \mathbb{R}^n\}$.

$\mathcal{L}$ is covering with respect to C (or vice versa) if $\mathcal{L} + C = \mathbb{R}^n$, or equivalently, if $\mu(C, \mathcal{L}) \leq 1$. The covering is α-thin if $\mathrm{vol}_n(C)/\det(\mathcal{L}) \leq \alpha$, where $\alpha \geq 1$.

For a symmetric convex body $K \subseteq \mathbb{R}^n$, we define its covering to packing ratio with respect to $\mathcal{L}$ (or vice versa) as $2\mu(K, \mathcal{L})/\lambda_1(K, \mathcal{L}) \geq 1$.

Much work has been dedicated to proving the existence of extremely thin-lattice coverings [23, 24, 26, 4, 10] – much of instigated by C.A. Rogers – for their important applications in convex geometry as well as lattice coding schemes (discovered later). For the strongest (and rather surprising) existential bound [26], Rogers shows that for n-dimensional convex body K there exists a covering lattice of thinness $n^{\log n + O(1)}$. Butler [4] further extended this result by showing that one can attain the same thinness with a covering to packing ratio of $2 + o(1)$.

All of these constructions rely on sampling from a probabilistic ensembles of lattices, occassionally with some additional postprocessing, and are intrinsically difficult to derandomize. More problematically however, these ensembles produce lattices that are as "hard as possible" to enumerate from with known polynomial space methods, severely complicating their use in our context (and in many others in fact). For the purpose of volume estimation, it will in fact be sufficient to construct $2^{O(n)}$-thin lattices which are "sufficiently easy" to enumerate from.

The currently most powerful polynomial space lattice point enumeration strategy is *Schnorr-Euchner* enumeration. We note that it is the primary enumeration method for all polynomial space solvers for the Closest Vector Problem (CVP) under the Euclidean norm (given a target $\mathbf{t}$ and lattice $\mathcal{L}$, find the closest vector in $\mathcal{L}$ to $\mathbf{t}$). It will also form the core of our enumeration algorithm. We summarize it below and list some of its important properties.

▶ **Definition 5** (Schnorr-Eucher enumeration)**.** Given a basis $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ of $\mathcal{L}$ and a convex body K, Schnorr-Euchner builds all feasible solutions to $\{\mathbf{z} \in \mathbb{Z}^n : \sum_{i=1}^n z_i \mathbf{b}_i \in K\}$, corresponding to $\mathcal{L} \cap K$, using a search tree over the coefficients. The nodes at level i of the tree, $i \in \{0, \dots, n\}$, corresponding to fixings of the last i coefficients that are "feasible" for K. Precisely, a fixing of $z_{n-i+1}, \dots, z_n \in \mathbb{Z}$ is feasible for K if $\exists\ r_1, \dots, r_{n-i} \in \mathbb{R}$ such that

$$\sum_{j=1}^{n-i} r_j \mathbf{b}_j + \sum_{j=n-i+1}^{n} z_j \mathbf{b}_j \in K.$$

By convention, we consider the root (level 0) to have an empty fixing, which is feasible if $K \neq \emptyset$. From a level i node, with feasible fixing $z_{n-i+1}, \dots, z_n \in \mathbb{Z}$, we recurse on all feasible extensions $z_{n-i}, \dots, z_n$ with $z_{n-i} \in K$. By convexity of K, the set of values for z_{n-i} inducing a feasible extension lie in an interval, which can be computed using a convex program.

We define K to be α-*Schnorr-Euchner enumerable*, or α-SE, with respect to B (or vice versa) if for every shift $\mathbf{t}$, $\mathbf{t} \in \mathbb{R}^n$, and level i, $i \in \{0, \dots, n\}$, the number of distinct feasible partial fixings for $K + \mathbf{t}$ with respect to B at level i is bounded by α. We note that the total number of partial fixing controls the essential complexity of Schnorr-Euchner enumeration.

The usefulness of the α-SE property for K is that it will enable us to bound the complexity of Schnorr-Euchner enumeration for general convex sets via their *covering numbers* with respect to K.

For two sets $C, D \subseteq \mathbb{R}^n$, we denote the *covering number* of C with respect to D

$$N(C, D) = \min\{|T| : T \subseteq \mathbb{R}^n, C \subseteq T + D\} \ .$$

C, D have covering numbers bounded by (c_1, c_2) if $N(C, D) \leq c_1$ and $N(D, C) \leq c_2$.

For convex C and D, the covering numbers are tightly controlled by volumes. In particular, $N(C, D) \leq O(n \log n)\mathrm{vol}_n(C - D)/\mathrm{vol}_n(D)$ (see Theorem 8 for an exact statement).

Returning to enumeration, if K is α-SE with respect to a basis B for $\mathcal{L}$, then for any convex set C, the complexity of enumerating $C \cap \mathcal{L}$ via Schnorr-Euchner enumeration on B is bounded by $\alpha N(C, K)$ times polynomial factors. This will be the crucial to making our reduction from volume estimation to lattice point counting efficient.

Our main technical contribution is a deterministic construction for thin covering lattices with good Schnorr-Euchner enumeration properties. We state its guarantees below.

▶ **Theorem 6** (Thin Lattice)**.** *For an n-dimensional convex body $K \subseteq \mathbb{R}^n$, there is a deterministic $2^{O(n)}$ time and* $\mathrm{poly}(n)$ *space algorithm to construct a thin covering lattice $\mathcal{L} \subseteq \mathbb{R}^n$ for K along with a generating basis B, such that K is $2^{O(n)}$-SE with respect to B, and*

1. *if K symmetric, $\mathcal{L}$ yields a 3^n-thin covering and has covering to packing ratio at most* 3.
2. *if K asymmetric, $\mathcal{L}$ yields a 7^n-thin covering.*

As mentioned previously, for the main class of lattices used to show the existence of thin coverings, that is the so-called Haar lattices (see [24, 26]), it is known that Schnorr-Euchner enumeration (and all other known low-space enumeration methods) is in general not efficient. In particular, for almost all Haar lattices of determinant 1, it can shown that the Schnorr-Euchner enumeration complexity of a Euclidean ball of radius $\Theta(\sqrt{n})$ with respect to *any basis* is at least $n^{\Omega(n)}$, even though the number of lattice points it contains is bounded by $2^{O(n)}$ (see for example, section 2 in [3]). We note that these types of lattices form a main class of "hard" test instances for solving the classical Shortest and Closest Vector Problems.

Therefore, the construction in Theorem 6 also gives the *first existential construction* of "easy to enumerate" thin-covering lattices for general convex bodies.

As an added bonus of our construction, the covering lattices we construct have a covering to packing ratio of at most 3 for symmetric bodies, and have the property that CVP under the norm for which they were constructed (i.e. $\|\cdot\|_K$) can be solved in $2^{O(n)}$ time and poly(n) space (since this reduces to enumeration within the covering body). We note that while building thin covering lattices for ℓ_p norms is trivial – $2n^{-1/p}\mathbb{Z}_n$ is a $2^{O(n)}$-thin covering lattice for the ℓ_p norm – building ones with constant covering to packing ratio is not. In fact, even for the ℓ_2 norm, there is no known explicit construction of such a lattice. While the small covering to packing ratio is not strictly necessary in our applications, we believe it might be useful elsewhere, such as in lattice based schemes for Locality Sensitive Hashing (see [2] for an application using the 24-dimensional Leech lattice).

Comparing to prior work, Alon et al [1] gave a deterministic $2^{O(n)}$ time and 2^n space construction based on a greedy thin lattice construction of Rogers [23] (which we will also rely on), and gave a 2^n space method to enumerate from them. For their motivation, they used these lattices to compute nearly optimal coverings of a symmetric convex body by translates of another (which our methods can also give a corresponding improvement on), which in turn was motivated for the purpose of designing an additive PTAS for 2-player Nash equilibria and the Densest Subgraph problem, in the case where the sum of the payoff matrices (for 2-player Nash) or the adjacency matrix (for Densest Subgraph) has logarithmic ε-rank.

As our algorithm will also rely on Rogers' greedy construction, we give the high level idea behind it and the issues we resolve in applying it for Theorem 6. Given a *symmetric* convex body K and any input lattice $\mathcal{L}$, Rogers' greedy construction iteratively tries to adds points to $\mathcal{L}$ from $\mathcal{L}/3$ which keep the minimum distance with respect to K unchanged while making $\mathcal{L}$ denser. When the process terminates, $\mathcal{L}$ is guaranteed to have covering to packing ratio bounded by 3. This in turn in fact implies that $\mu\mathcal{L}$, where $\mu = \mu(K, \mathcal{L})$, is 3^n-thin.

In [1], to enumerate within these lattices, they rely on the M-ellipsoid covering and Voronoi cell based enumeration algorithms of [20, 7, 5]. For $\mathcal{L}$ and K as in the previous paragraph, they show using these techniques that enumeration over $\mathcal{L} \cap C$, for any convex body C, can be achieved time $2^{O(n)}N(C, K)$ using 2^n space. Hence, the enumeration guarantees are similar to ours, though at the cost of exponential space.

From our perspective, the main problem with Roger's greedy construction is that it generates lattices that are in general very far from starting base lattice. In particular, even if we start from a lattice $\mathcal{L}$ that is "easy to enumerate" with respect to K, the final outputted lattice may not be. The main effort of our construction, is in fact spent generating an "easy to enumerate" input lattice for which we can guarantee that the lattice outputted by Roger's procedure is still close enough to the base lattice. For this purpose, we will use a rectangular lattice generated from an M-ellipsoid of K (similar to what is used in [8]) that is additionally "sparsified" using techniques from [6].

We note that so far, we have only discussed methods for building thin-covering lattices for symmetric bodies. In fact, Roger's construction relies crucially on symmetry. To get around this, we will give a deterministic algorithm that computes a point $\mathbf{c} \in K$, such that $K[\mathbf{c}] = (K - \mathbf{c}) \cap (\mathbf{c} - K)$, K symmetrized about $\mathbf{c}$, satisfies $\mathrm{vol}_n(K)/\mathrm{vol}_n(K[\mathbf{c}]) \leq (7/3)^n$. From this it will follow, that a 3^n-thin covering lattice for $K[\mathbf{c}]$ yields a 7^n-thin covering lattice for K. This algorithm will be rather non-trivial, and will in fact rely on many iterated calls to our volume algorithm and thin lattice generator for symmetric bodies.

We explain all these techniques in detail in the next section. We note that any missing definitions can be found in the preliminaries in Section 4.

3 Techniques

We now explain the main ideas behind our algorithm. We shall first describe the generic framework for reducing volume estimation to lattice point counting, followed by a description of our symmetrization algorithm for general convex bodies, and finish with a full description of our thin lattice construction.

3.1 Reducing Volume to Counting Lattice Points

We shall now present a general framework for relating the volume of general convex bodies (not necessarily symmetric) to lattice point counting, and use it to derive all the properties we will require for our algorithms. In particular, we will derive the need for thin-covering lattices from first principles.

A classical fact, is that for any n-dimensional convex body $K \subseteq \mathbb{R}^n$ (any "nice enough" set will also do) and lattice $\mathcal{L}$ we have

$$\lim_{\varepsilon \to 0} \frac{\mathrm{vol}_n(K)}{|K \cap \varepsilon\mathcal{L}| \det(\varepsilon\mathcal{L})} = \lim_{\epsilon \to 0} \frac{\mathrm{vol}_n(K)}{|K \cap \varepsilon\mathcal{L}| \det(\mathcal{L})\varepsilon^n} = 1.$$

Hence, for small enough ε, we can accurately approximate volume by counting lattice points. From the perspective of efficiency, we must be able to determine how small to make ε for the desired approximation quality, how many lattice points K contains at this scaling (as we will count via enumeration), and how to enumerate these lattice points. Clearly, all of these considerations are intimately tied to how we choose the lattice $\mathcal{L}$. To slightly complicate matters, the algorithms will in fact enumerate from bodies related to K, whose definition will depend on the target approximation factor (in fact in [8], the base lattice does as well).

We now explain how to control the approximation quality and the number of lattice points, which will lead us to the concept of thin lattice coverings of space. Assume that $\mathcal{L}$ is *covering* with respect to a convex body $K_0 \subseteq \mathbb{R}^n$ (which will be derived from K), i.e. that $\mathcal{L} + K_0 = \mathbb{R}^n$. For our convex body K, let

$$\mathcal{C}_{\mathcal{L}}(K, K_0) = \{\mathbf{y} \in \mathcal{L} : \mathbf{y} + K_0 \cap K \neq \emptyset\} = \mathcal{L} \cap (K - K_0) \ ,$$

denote the lattice translates of K_0 "touching" K. Since $\mathcal{L}$ is covering with respect to K_0, we see that $K \subseteq \mathcal{L} + \mathcal{C}_{\mathcal{L}}(K, K_0)$. Since K_0 is a covering body for $\mathcal{L}$, it must contain a subset $F \subseteq K_0$ which tiles with respect to $\mathcal{L}$ (by throwing out the "overrepresented" pieces of K_0, see Lemma 27 for a formal proof). Clearly, $\mathcal{C}_{\mathcal{L}}(K, F) \subseteq \mathcal{C}_{\mathcal{L}}(K, K_0)$. We derive the following containments

$$K \subseteq \mathcal{C}_{\mathcal{L}}(K, F) + F \subseteq \mathcal{C}_{\mathcal{L}}(K, K_0) + F \subseteq \mathcal{C}_{\mathcal{L}}(K, K_0) + K_0 \subseteq K + (K_0 - K_0) \ . \tag{1}$$

By the tiling property of F, we see that

$$\begin{aligned} \mathrm{vol}_n(\mathcal{C}_{\mathcal{L}}(K, F) + F) &= |\mathcal{C}_{\mathcal{L}}(K, F)| \mathrm{vol}_n(F) = |\mathcal{C}_{\mathcal{L}}(K, F)| \det(\mathcal{L}) \\ &\leq |\mathcal{C}_{\mathcal{L}}(K, K_0)| \det(\mathcal{L}) = \mathrm{vol}_n(\mathcal{C}_{\mathcal{L}}(K, K_0) + F) \ . \end{aligned} \tag{2}$$

Combining (1),(2) above, we get that

$$\mathrm{vol}_n(K) \leq |\mathcal{C}_{\mathcal{L}}(K, K_0)| \det(\mathcal{L}) \leq \mathrm{vol}_n(K + (K_0 - K_0)) \ . \tag{3}$$

If the target approximation ratio is $(1+\varepsilon)^n$, it then suffices to choose $\mathcal{L}$ and K_0 such that

1. $\mathrm{vol}_n(K + (K_0 - K_0)) / \mathrm{vol}_n(K) \leq (1+\varepsilon)^n$.

2. $\mathcal{L}$ is covering with respect to K_0.

Rearranging equation (3), we can bound the number of lattice points we enumerate by

$$\begin{aligned}\frac{\mathrm{vol}_n(K + (K_0 - K_0))}{\det(\mathcal{L})} &= \frac{\mathrm{vol}_n(K + (K_0 - K_0))}{\mathrm{vol}_n(K_0)} \frac{\mathrm{vol}_n(K_0)}{\det(\mathcal{L})} \\ &\leq (1+\varepsilon)^n \underbrace{\frac{\mathrm{vol}_n(K)}{\mathrm{vol}_n(K_0)}}_{(a)} \underbrace{\frac{\mathrm{vol}_n(K_0)}{\det(\mathcal{L})}}_{(b)} \ . \end{aligned} \tag{4}$$

This will form our most important proxy for the complexity of the estimator. Since we are aiming for an algorithm of complexity $2^{O(n)}(1+1/\varepsilon)^n$, it will be necessary for (4) to be bounded in this way as well.

Using the above, we will separate the problem of building a $\mathcal{L}$ and K_0 into two independent subproblems. Precisely, we first build K_0 to "minimize" (a) under condition (1), and then build $\mathcal{L}$ to "minimize" (b) under condition (2).

Choosing $\mathcal{L}$. For the second part, note that once K_0 is chosen the minimization problem for (b) exactly corresponds to building a thin-covering lattice for K_0. As we will see, the K_0 will be chosen to be symmetric here, and for each desired approximation ratio will correspond to a scaling of the same body (and hence $\mathcal{L}$ can be scaled accordingly). From Theorem 6, we will be able to build a 3^n-thin covering lattice $\mathcal{L}$ for K_0, and a basis B for $\mathcal{L}$ for which K_0 is $2^{O(n)}$-SE. For the enumeration complexity of $(K - (K_0 - K_0)) \cap \mathcal{L}$ (which can be different from the number of lattice points), the bounds we use above on $|(K - (K_0 - K_0)) \cap \mathcal{L}|$ are in fact *volumetric*, and hence with slight modifications will also apply for bounding the required covering number $N(K - (K_0 - K_0), K_0)$ (which bounds the enumeration complexity).

Choosing K_0. Moving back to the first part, we now simplify condition (1), by making some natural simplifying assumptions on K_0. In particular, we will ask that

1a. K_0 is a symmetric convex body.

1b. $K_0 \subseteq (\varepsilon/2)(K - \mathbf{c})$, for some $\mathbf{c} \in K$.

Under these assumptions, we now see that

$$\mathrm{vol}_n(K + (K_0 - K_0)) = \mathrm{vol}_n(K + 2K_0) \leq \mathrm{vol}_n(K + \varepsilon(K - \mathbf{c})) = (1+\varepsilon)^n \mathrm{vol}_n(K) \ ,$$

hence the joint requirements (1a),(1b) above are indeed stronger than condition (1). Note now that if fix $\mathbf{c}$ in (1b), the largest symmetric body we can pick for K_0 (and hence minimizer for (a)) is simply

$$K_0 = (\varepsilon/2)(K - \mathbf{c}) \cap (\varepsilon/2)(\mathbf{c} - K) = (\varepsilon/2)K[\mathbf{c}], \tag{5}$$

where $K[\mathbf{c}] = (K - \mathbf{c}) \cap (\mathbf{c} - K)$.

We define the *Kovner-Besicovitch* measure of symmetry of K (as defined in [15]) as

$$\mathrm{Sym}_{kb}(K) = \max_{\mathbf{c} \in K} \mathrm{vol}_n(K[\mathbf{c}])/\mathrm{vol}_n(K). \tag{6}$$

Let $\mathbf{c}^*$ denote a maximizer for the right hand side. Then, under conditions (1a),(1b), the minimizing $K_0 = (\varepsilon/2)K[\mathbf{c}^*]$, and achieves an (a) value of exactly

$$\frac{\mathrm{vol}_n(K)}{\mathrm{vol}_n((\varepsilon/2)K[\mathbf{c}^*])} = \frac{(2/\varepsilon)^n}{\mathrm{Sym}_{kb}(K)} \ .$$

Note that for every target approximation factor, the optimal body K_0 is simply a scaled down version of the same body, which will greatly simplifies our task.

To make the above expression useful however, we will need lower bounds on $\mathrm{Sym}_{kb}(K)$. In this regard, a classical computation reveals that a uniform point in K yields an average KB value of 2^{-n}, and hence $\mathrm{Sym}_{kb}(K) \geq 2^{-n}$. Furthermore, it was shown in [22] that the centroid of K achieves this lower bound. Therefore, with the aid of random sampling algorithms over convex bodies, finding a center in K of KB value at least 2^{-n} is straightforward. However, our goal here is to obtain a deterministic algorithm.

3.2 Deterministically Building Approximate Kovner-Besicovitch Points

We define a point $\mathbf{c} \in K$ to be an α-approximate Kovner-Besicovitch point for K, $0 < \alpha \leq 1$, if its KB value $\mathrm{vol}_n(K[\mathbf{c}])/\mathrm{vol}_n(K)$ is at least an α-factor of $\mathrm{Sym}_{kb}(K)$. For the purposes of volume estimation, given the above analysis, we note that even a $2^{-O(n)}$ approximate KB point is sufficient. As our main technical tool for asymmetric convex bodies, we give an algorithm for deterministically computing approximate KB points:

▶ **Theorem 7.** *For any convex body $K \subseteq \mathbb{R}^n$, and any $\varepsilon > 0$, one can compute a $(1+\varepsilon)^{-n}$ approximate Kovner-Besicovitch point $\mathbf{c} \in K$ in deterministic $2^{O(n)}(1+1/\varepsilon)^{2n+1}$ time and* $\mathrm{poly}(n)$ *space.*

Using the above theorem, the construction of thin covering lattices for general convex bodies bodies claimed in 6 becomes straightforward to derive from the symmetric case. In particular, for the given convex body K, we compute a $(6/7)^n$ approximate KB point $\mathbf{c} \in K$, and output a thin covering lattice for the symmetric body $K[\mathbf{c}]$ using the construction from symmetric convex bodies (see Theorem 26 for full details).

We now describe the high level of the algorithm behind Theorem 7. First, by rounding K, we may assume that $B_2^n \subseteq K \subseteq (n+1)n^{1/2}B_2^n$ (see Theorem12). From here, define the sequence of bodies $K_i = 2^i B_2^n \cap K$ (we note the similarity to the volume algorithm of [9]), for $i \in \{0, \ldots, T\}$, $T = O(\log n)$, where $K_0 = B_2^n$ and $K_T = K$. For each K_i, $i \in [T-1]$, we will compute a 3^{-n} approximate KB point $\mathbf{c}_i$ for K_i from a 3^{-n} approximation KB point $\mathbf{c}_{i-1}$ for K_{i-1}. Finally, in the last step, from K_{T-1} to K_T, we amplify this to $(1+\varepsilon)^{-n}$ approximation. We note that we may start with $\mathbf{c}_0 = \mathbf{0}$, since this is the center of symmetry for $K_0 = B_2^n$.

To compute $\mathbf{c}_i$ starting from $\mathbf{c}_{i-1}$, we perform the following improvement steps: from our current solution for $\mathbf{c}_i$, we build a covering of $1/2K_i + 1/2\mathbf{c}_i$ by $(\varepsilon/2)K_i[\mathbf{c}_i]$, and replace $\mathbf{c}_i$ with the covering element (which lies in K_i) of largest value (where we compute each the value to within $(1+\varepsilon)^n$). The concavity of $\mathrm{vol}_n(K[\mathbf{c}])^{1/n}$ (by Brunn-Minkowski) will allow us to show that at each step, we improve the objective value by essentially a $(1+c\varepsilon)^n$ factor. Hence $O(1/\varepsilon)$ iterations suffice to construct a near optimal solution.

3.3 Thin Lattice Construction

We now discuss how one can construct thin covering lattices. We restrict here to the case where K is symmetric. As explained previously, the asymmetric case can be reduced to the symmetric one using approximate Kovner-Besicovitch points.

To build intuition, we describe a first basic construction based on ellipsoidal rounding taken from [1]. Given the initial n dimensional covering body K, a first natural way to get a handle on the coarse geometry of K is to compute an appropriate ellipsoidal approximation. As a first try, we may attempt to compute a good sandwiching ellipsoid E for K, i.e. an ellipsoid satisfying $E \subseteq K \subseteq cE$, where c is small as possible. For n-dimensional symmetric convex bodies sandwiching ellipsoids always exist for $c = \sqrt{n}$ (e.g. one may use the maximum volume contained ellipsoid), and this is tight (e.g. the cube vs the ball). By a linear transformation – note that all the desired properties of the covering lattice are preserved by a simultaneous linear transformation of the lattice and covering body – we may assume that $B_2^n \subseteq K \subseteq \sqrt{n} B_2^n$. A simple choice of K-covering lattice is now $\Lambda = \frac{2}{\sqrt{n}}\mathbb{Z}^n$. The covering property follows from the fact that K contains the cube $[\frac{-1}{\sqrt{n}}, \frac{1}{\sqrt{n}}]^n \subseteq B_2^n \subseteq K$, which is the (symmetric) fundamental parallelepiped with respect to the basis $B = (\frac{2}{\sqrt{n}}\mathbf{e}_1, \ldots, \frac{2}{\sqrt{n}}\mathbf{e}_n)$. A first question is how thin is this lattice covering? From the sandwiching bounds we get

$$\frac{\mathrm{vol}_n(K)}{\det(\Lambda)} \leq \frac{\mathrm{vol}_n(\sqrt{n}B_2^n)}{\det(\frac{2}{\sqrt{n}}\mathbb{Z}^n)} = (n/2)^n \mathrm{vol}_n(B_2^n) = 2^{\Theta(n)} n^{n/2}.$$

Another question is how easy is enumeration in this lattice? As discussed in Section 2, the main consideration will essentially be the enumeration complexity for the covering body K itself. For our choice of lattice $\Lambda = \frac{2}{\sqrt{n}}\mathbb{Z}^n$, one can consider the graph over Λ whereby two lattice points are adjacent if their associated parallelepipeds $\mathcal{P}(B) = [\frac{-1}{\sqrt{n}}, \frac{1}{\sqrt{n}}]^n$ intersect in a facet, or put more simply if their difference is in $\pm\left\{\frac{2}{\sqrt{n}}\mathbf{e}_1, \ldots, \frac{2}{\sqrt{n}}\mathbf{e}_n\right\}$. Here it is not hard to check that the restriction of this graph to the lattice points forming a $\mathcal{P}(B)$-tiling of K, that is $(K - \mathcal{P}(B)) \cap \Lambda$, is connected. Furthermore, given that $\mathcal{P}(B) \subseteq K$, via similar arguments to those above the tiling has size bounded by $2^n \mathrm{vol}(K)/\det(\Lambda)$. Hence the points in $K \cap \Lambda$ can be enumerated by computing the connected component of $\mathbf{0}$ in the tiling graph in $\mathrm{poly}(n)2^n \mathrm{vol}(K)/\det(\Lambda)$ time via a depth first or breadth first search. To make this enumeration space efficient (avoiding a linear dependence on the size of the graph), a simple line following argument shows that the edges of the shortest path tree directed towards $\mathbf{0}$ can be computed locally. From here one can show that a traversal of the vertices of this implicit shortest path tree can be computed in space logarithmic in the size of the graph – which is $\mathrm{poly}(n)$ in this setting – starting from $\mathbf{0}$ (see [5] for a full exposition).

The above construction of [1] yields a $2^{O(n)}n^n$-thin K-covering lattice Λ that is $\mathrm{poly}(n)$-space enumerable. While this is not good enough for our purposes, we will make use of the main fact enabling low space enumeration. In particular, if a convex body C has a tiling with respect to a basis parallelepiped $\mathcal{P}(B)$ of size $f(n)|C \cap \Lambda|$, then the points $C \cap \Lambda$ can be enumerated in $\mathrm{poly}(n)$ space and $f(n)|C \cap \Lambda|$ time. We will strengthen this observation, by showing that Schnorr-Euchner (SE) enumeration – which always operates using $\mathrm{poly}(n)$ space – over $C \cap \Lambda$ using basis B has complexity bounded by $\mathrm{poly}(n)N(C, \mathcal{P}(B))$ (see Lemmas 16 and 19). Note that by definition, the parallelepiped covering number is always bounded by the size of a parallelepiped tiling. Apart from yielding a somewhat simpler enumeration algorithm, SE enumeration will be very useful in that it will make it easy to quantify how the enumeration complexity changes when taking sublattices or superlattices of any base lattice. In particular, we show that the SE enumeration complexity for a convex body does not increase when taking sublattices, and increases by at most the index when taking superlattices (see Lemma 18).

To improve on the above construction, we will make use of three additional ingredients. Firstly, we construct a lattice basis B whose parallelepiped $\mathcal{P}(B)$ has covering numbers bounded by $2^{O(n)}$ with respect to K (i.e. $N(K, \mathcal{P}(B)), N(\mathcal{P}(B), K) = 2^{O(n)}$). This can be achieved by choosing $\mathcal{P}(B)$ to be a maximum volume in inscribed parallelepiped for an M-ellipsoid E of K. We note that the "M-lattice" $\mathcal{L} = \mathcal{L}(B)$ is used in [7] to compute the M-ellipsoid covering for the lattice point enumeration algorithm. By asking for more than the sandwiching bounds achieved in the previous construction, we get good bounds on the volume of K, i.e. $\det(\mathcal{L}) = 2^{\Theta(n)}\mathrm{vol}_n(K)$ (avoiding the previous n^n factor), and - as mentioned above - we get that Schnorr-Euchner enumeration in K with respect to B takes at most $2^{O(n)}$ time. At this point, from the robustness of SE enumeration, we can reduce the covering lattice problem to building a K-covering lattice Λ that is "not too far" from the base lattice $\mathcal{L}$. In particular, it will suffice for us if Λ can be obtained by a sequence of sublattice and superlattice operations over $\mathcal{L}$ where the product of the indexes is at most $2^{O(n)}$ (in fact, it will be a superlattice of a sublattice).

The remaining two ingredients are the use of lattice sparsification and densification. Here the idea will be to use sparsification to choose a sublattice of small index which gets rid of all short lattice vectors, and to use densification to construct a superlattice of small index which reduces the covering radius to a constant multiple of the minimum distance.

The original construction of Rogers [23], which is implemented in [1], uses a "greedy" deterministic densification procedure to construct a lattice with covering to packing ratio at most 3. More precisely, starting from a base lattice $\mathcal{L}$, Rogers looks for a point $\mathbf{y} \in \mathcal{L}/3$ that is at distance at least $\lambda_1 \overset{\text{def}}{=} \lambda_1(K, \mathcal{L})$ from $\mathcal{L}$ under $\|\cdot\|_K$. If such a point $\mathbf{y}$ exists, we adjoin $\mathbf{y}$ to $\mathcal{L}$ and repeat. The distance lower bound here guarantees that the minimum distance does not decrease when we adjoin $\mathbf{y}$. Furthermore, the determinant decreases by a factor of 3 after adjoining $\mathbf{y}$, and hence the packing density of the new lattice increases by a factor 3. If no such point exists, then every point in $\mathcal{L}/3$ is at distance at most λ_1 from $\mathcal{L}$, which implies (see Lemma 14) that $\mu(K, \mathcal{L}) \leq (3/2)\lambda_1$ (i.e. covering to packing ratio 3). A nice feature of this construction is that it can be implemented as long as one can efficiently enumerate lattice points in the current lattice with respect to shifts of $\lambda_1 K$, where λ_1 stays fixed throughout the construction.

When starting from an M-lattice $\mathcal{L}$ with basis B (where $\mathcal{P}(B)$ is fundamental parallelepiped built from an M-ellipsoid of K), the enumeration within $\lambda_1 K$ can initially be done in $2^{O(n)}$ time using poly(n) space via SE enumeration, where here $\lambda_1 = O(1)$ since $\mathrm{vol}_n(K) \geq 2^{-O(n)} \det(\mathcal{L})$. However, the efficiency of enumeration degrades over the course of the construction as the lattice gets denser. In particular, the enumeration complexity can jump by a 3^k factor after k iterations, since this is the index with respect to the base lattice. We note that the number of lattice points in any shift of $\lambda_1 K$ is never larger than 5^n by a standard packing bound. While this does not bound the SE enumeration complexity, it is sufficient to bound the time complexity of the M-ellipsoid and Voronoi cell based enumeration algorithm of [20, 7] by $2^{O(n)}$ while using $2^{O(n)}$ space. The latter method describes the implementation in [1]. Since we seek to avoid the use of exponential space, we will show how to keep SE enumeration efficient throughout the entire procedure. Given the above reasoning, for SE enumeration to remain $2^{O(n)}$ time, one needs to ensure that the Rogers densification procedure terminates in $O(n)$ steps.

The only general bound on the iteration complexity of Rogers densification procedure is based on the packing density of the base lattice, i.e. $\mathrm{vol}_n((\lambda_1/2)K)/\det(\mathcal{L})$. If the base lattice has packing density 3^{-l}, then since the packing density increases by a factor 3 at each iteration, the number of iterations must be bounded by $\lfloor l \rfloor$ (remembering that the packing density is always less than 1). Unfortunately, when starting from the M-lattice or the lattice constructed from a good sandwiching ellipsoid, one has little control over the packing density. In both cases, $\lambda_1(K, \mathcal{L})$ could be as small $1/n$ while the volume of K can be essentially equal to $\det(\mathcal{L})$, yielding a packing density of $n^{-O(n)}$. As a first simple workaround for the M-lattice, if one is willing to forgo the covering to packing property for K, then one can simply "truncate the long parts" of K, replacing K by $K' = K \cap \mathcal{P}(B)$. Here $\lambda_1(K', \mathcal{L}) \geq 1$ since $K' \subseteq \mathcal{P}(B)$, and

$$\mathrm{vol}_n(K') \geq \mathrm{vol}_n(K)/N(K, \mathcal{P}(B)) \geq 2^{-O(n)}\mathrm{vol}_n(K) \geq 2^{-O(n)} \det(\mathcal{L}).$$

Therefore the packing density of $\mathcal{L}$ with respect to K' is $2^{-O(n)}$, and hence Rogers densification procedure creates an easy to enumerate 3^n-thin K'-covering lattice Λ (by the bound of 3 on the covering to packing ratio), which yields a similarly easy to enumerate $2^{O(n)}$-thin K-covering lattice.

We now explain how to build a thin covering lattice for K with covering to packing ratio at most 3, avoiding the use of the intermediate body K' above. In the above construction, the truncation $K' = K \cap \mathcal{P}(B)$ achieves $K' \cap \mathcal{L} = \{\mathbf{0}\}$ and $\mathrm{vol}_n(K)/\mathrm{vol}_n(K') = 2^{O(n)}$. Here the idea will be that, instead of modifying K, we will build a sparsifying sublattice $M \subseteq \mathcal{L}$ which removes all the non-zero lattice vectors in K, i.e. such that $M \cap K = \{\mathbf{0}\}$. As long as the index of M with respect to $\mathcal{L}$ is at most $2^{O(n)}$, we will have that $\lambda_1(K, M) = \Theta(1)$. By construction $\lambda_1(K, M) \geq 1$, and Minkowski's convex body theorem

$$\lambda_1(K, M) \leq 2\frac{\det(M)^{1/n}}{\mathrm{vol}_n(K)^{1/n}} = O(1)\frac{\det(\mathcal{L})^{1/n}}{\mathrm{vol}_n(K)^{1/n}} = O(1).$$

These bounds will simultaneously guarantee two key properties. Firstly, the iterations in Rogers' greedy construction can be performed by enumerating the lattice points in M within shifts of $\lambda_1 K$, $\lambda_1 = O(1)$, which will have SE enumeration complexity $2^{O(n)}$ (M inherits this from $\mathcal{L}$). Second, we will get that the packing density of M with respect to K is $2^{-O(n)}$, and therefore the number of iterations in Rogers' construction will be bounded by $O(n)$. Hence, we have now reduced the problem of building the thin K-covering lattice claimed in Theorem 6, to the problem of building a sublattice $M \subseteq \mathcal{L}$ satisfying

$$[\mathcal{L} : M] = 2^{O(n)} \quad \text{and} \quad M \cap K = \{\mathbf{0}\}.$$

For the purpose of building M, we will make direct use of randomized lattice sparsification techniques, which we subsequently derandomize in $2^{O(n)}$ time. By applying the transformation B^{-1} to $\mathcal{L}$ and K, we may now assume that $\mathcal{L} = \mathbb{Z}^n$ and $B = (\mathbf{e}_1, \dots, \mathbf{e}_n)$, where $\mathcal{P}(B) = [-1/2, 1/2]^n$. We will now examine the "dual" ensemble associated with densifying superlattice distributions. Here we pick a uniformly random "parity check" matrix $A \leftarrow \mathbb{Z}_p^{m \times n}$, $m \leq n$, where the associated lattice is

$$\Lambda^{\perp}(A) = \{\mathbf{z} \in \mathbb{Z}^n : A\mathbf{z} \equiv \mathbf{0} \pmod{p\mathbb{Z}^m}\}.$$

We will now examine the above sparsifying distribution when $m = 1$ and p is prime (i.e. a single random linear equation mod p), which correspond to the so-called Goldstein-Mayer lattices [13]. After normalizing so that their determinant is 1, as $p \to \infty$, Goldstein and Mayer [13] show that this distribution converges to the Haar distribution on lattices (in fact, the convergence result stated for densifying distributions is a consequence of this). We note that the Goldstein-Mayer lattices have had prior interesting applications in Computer Science: they are a crucial ingredient used to prove hardness of approximation (under randomized reductions) of the gap version of SVP [19, 18], and were used to develop a deterministic algorithm for $(1 + \varepsilon)$ approximate CVP under any norm which runs in $2^{O(n)}(1 + 1/\varepsilon)^n$ time and 2^n space [6].

We now explain how this sparsifying distribution can be used rather directly to build M. Let $S = (K \cap \mathbb{Z}^n) \setminus \{\mathbf{0}\}$ and let $N = |S|$. Since $\mathbb{Z}^n$ is an M-lattice for K, we know that $N = 2^{O(n)}$, where N can be computed in $2^{O(n)}$ time by SE enumeration of $K \cap \mathbb{Z}^n$ using the standard basis B. Let p be any prime such that $N < p < 2N$. Note that p always exists (Bertrand's postulate), and can be computed deterministically in $2^{O(n)}$ time using trial division (one can also use the standard randomized poly(n) time Las Vegas algorithm to do this as well). We now let $M = \Lambda^{\perp}(\mathbf{a})$ where $\mathbf{a} \leftarrow \mathbb{Z}_p^n$ is chosen uniformly. Clearly $[\mathbb{Z}^n : M] = p = 2^{O(n)}$ (almost surely), and hence we need only verify that $M \cap K = \{\mathbf{0}\} \Leftrightarrow M \cap S = \emptyset$. Take $\mathbf{x} \in S$. It is not hard to check that since $\mathbf{x} \neq \mathbf{0}$ and $|S| = |(K \cap \mathbb{Z}^n) \setminus \{\mathbf{0}\}| < p$, that we must have $\mathbf{x} \not\equiv \mathbf{0} \pmod{p\mathbb{Z}^n}$. Since that p is prime and $\mathbf{x} \not\equiv \mathbf{0} \pmod{p\mathbb{Z}^n}$, we get that $\langle \mathbf{x}, \mathbf{a} \rangle \pmod{p}$ is uniformly distributed in $\mathbb{Z}_p$. Therefore

$$\Pr_{\mathbf{a}}[\mathbf{x} \in M] = \Pr_{\mathbf{a}}[\langle \mathbf{x}, \mathbf{a} \rangle \equiv \mathbf{0} \pmod{p}] = 1/p.$$

By linearity of expectation, $\mathbb{E}[|M \cap S|] = |S|/p = N/p < 1$. Hence, by the probabilistic method, there exists $M \subseteq \mathbb{Z}^n$ satisfying the desired requirements. To derandomize the above construction, we apply the method of conditional expectations in a standard way to choose the coefficients of $\mathbf{a}$ one at a time (see Lemma 21 for full details).

This completes our description thin covering lattice constructions for symmetric bodies. From the discussion, one can see that our new algorithm combines the tools from many known constructions, namely, the M-lattice construction together with lattice sparsification and densification techniques, in non-trivial ways to create easy to enumerate thin covering lattices.

3.4 Organization

The remainder of the paper is organized as follows. In Section 4, we regroup all the definitions and concepts needed for the rest of the paper. In Section 5, we present the thin lattice construction for symmetric bodies. Here the main subsections are Section 5.1, which analyzes the properties of Schorr-Euchner enumeration, and Section 5.2 which analyzes each individual step of the thin covering lattice construction. Lastly, in Section 6, we give the deterministic volume estimation algorithm as well as the thin covering lattice construction for general convex bodies. Here the main subsection is Section 6.1, which describes the algorithm for computing approximate Kovner-Besicovitch points.

4 Preliminaries

4.1 Convexity

Define $B_2^n = \{\mathbf{x} : \|\mathbf{x}\|_2 \leq 1\}$ to be the unit Euclidean ball in $\mathbb{R}^n$. For sets $A, B \subseteq \mathbb{R}^n$, $s, t \in \mathbb{R}$, we define the Minkowski sum $sA + tB = \{s\mathbf{a} + t\mathbf{b} : \mathbf{a} \in A, \mathbf{b} \in B\}$. A convex body $K \subseteq \mathbb{R}^n$ is a compact convex set with non-empty interior. For any convex set K, we have the algebra $sK + tK = (s+t)K$ for $s, t \geq 0$. K is symmetric if $K = -K$ and $\mathbf{0}$-centered if $\mathbf{0}$ is in the interior of K. For a $\mathbf{0}$-centered convex body, we define the polar $K^\circ = \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \leq 1 \ \forall \mathbf{y} \in K\}$. We let $\|\mathbf{x}\|_K = \inf\{s \geq 0 : \mathbf{x} \in sK\}$ denote the *gauge function* of K. Here $\|\cdot\|_K$ satisfies all norm properties except symmetry when K is $\mathbf{0}$-centered and induces a norm in the usual sense when K is symmetric.

For two sets $A, B \subseteq \mathbb{R}^n$, we denote the *covering number* of A with respect to B is

$$N(A, B) = \min\{|T| : T \subseteq \mathbb{R}^n, A \subseteq T + B\}$$

A, B have covering numbers bounded by (c_1, c_2) if $N(A, B) \leq c_1$ and $N(B, A) \leq c_2$.

We define the ellipsoid $E(A) = \left\{\mathbf{x} \in \mathbb{R}^n : \mathbf{x}^T A \mathbf{x} \leq 1\right\}$, where A is an $n \times n$ symmetric positive definite matrix. From here one has that $E(A) = A^{-1/2} B_2^n$ and $\mathrm{vol}_n(E(A)) = \det(A)^{-1/2} \mathrm{vol}_n(B_2^n)$.

For an n dimensional convex body K, we say that an ellipsoid E is an M-ellipsoid of K if K, E have covering numbers bounded by $2^{O(n)}$ (see Section 4.1 for more details).

The Brunn-Minkowski inequality states that for measurable sets $A, B \subseteq \mathbb{R}^n$ such that $A + B$ is measurable then

$$\mathrm{vol}_n(A+B)^{1/n} \geq \mathrm{vol}_n(A)^{1/n} + \mathrm{vol}_n(B)^{1/n}$$

We use the notation

$$V_n = \mathrm{vol}_n(B_2^n) = \frac{\sqrt{\pi}^{\,n}}{\Gamma(n/2+1)} = (1+o(1))^n \sqrt{\frac{2\pi e}{n}}^{\,n} .$$

for the volume of the unit Euclidean ball.

The following is a powerful bound on the covering numbers due to [25], which relies on constructions of thin coverings of space (as described in the previous section).

▶ **Theorem 8.** *For $A, B \subseteq \mathbb{R}^n$ n dimensional convex bodies*

$$\frac{\mathrm{vol}_n(A-B)}{\mathrm{vol}_n(B-B)} \leq N(A,B) \leq \frac{\mathrm{vol}_n(A-B)}{\mathrm{vol}_n(B)} \Theta^*(B) \ ,$$

where $\Theta^*(B)$ is the minimal thinness of any covering of space by B. In particular, for any n-dimensional convex body B

$$\Theta^*(B) \leq n \log n + n \log\log n + 5n \ .$$

An important and deep theorem of Milman [21] states that every convex body can be well approximated by an ellipsoid from the perspective of covering.

▶ **Theorem 9** (M-ellipsoid). *There exists a constant $c > 0$, such that for all $n \geq 1$ and any symmetric convex body $K \subseteq \mathbb{R}^n$, an ellipsoid $E \subseteq \mathbb{R}^n$ such that E, K have covering numbers bounded by (c^n, c^n).*

We note that symmetry is unessential in the above construction, in particular if K is asymmetric, one can replace K by $K - K$ and retrieve a similar result.

In general, we call an ellipsoid E with single exponential covering numbers with respect to a convex body K an M-ellipsoid of K (though the term is only somewhat loosely defined). We note that the more standard maximum volume contained ellipsoid (John ellipsoid) and the minimum volume enclosing ellipsoid (Lowner ellipsoid) of K can be quite far from being M-ellipsoids, in particular their covering numbers can be as high as $n^{\Omega(n)}$.

Recently, it was shown in [8] that Milman's construction can made fully algorithmic:

▶ **Theorem 10** (M-ellipsoid Algorithm). *Given any symmetric convex body K, an ellipsoid $E = E(A) \subseteq \mathbb{R}^n$, such that E, K have covering numbers bounded by (c^n, c^n), for an absolute constant $c \geq 1$, can be computed in deterministic* $\mathrm{poly}(n)2^n$ *time and* $\mathrm{poly}(n)$ *space.*

Computational Model: $K \subseteq \mathbb{R}^n$ is an $(\mathbf{a}_0, r, R)$-*centered* convex body if $\mathbf{a}_0 + rB_2^n \subseteq K \subseteq \mathbf{a}_0 + RB_2^n$. When interacting algorithmically with K, we will assume that K is presented by a membership (or weak membership) oracle O_K. Here a membership oracle O_K on input $\mathbf{x} \in \mathbb{R}^n$, outputs 1 if $\mathbf{x} \in K$ and 0 otherwise. A weak membership oracle takes an extra parameter ε, where it need only return the correct answer on $\mathbf{x} \in \mathbb{R}^n$ if $\mathbf{x} \notin \partial K + \varepsilon B_2^n$ (i.e. at distance at least ε from the boundary). Most of the algorithms presented in this paper, will require weak membership oracles for bodies derived from K (e.g. Minkowski sums with other bodies, projections, polar body). However, for the simplicity of the presentation, we will generally ignore the intracies associated with interacting with weak oracles, as such considerations are by now standard.

The complexity of our algorithms will be computed in terms of the number of oracle queries and arithmetic operations. In this context, polynomial time allows for polynomial dependence on dimension and polylogarithmic dependence on the sandwiching parameters, Lipshitz factors, and other related parameters. We use the notation $\tilde{O}(T(n))$ to suppress $\mathrm{polylog}(T(n))$ terms. We state some of fundamental algorithmic tools we will require for convex bodies. The following theorem is yields the classical equivalence between weak membership and weak optimization [27, 14] for centered convex bodies. As simple corollaries of this theorem, one can derive weak membership oracles for all the bodies used in this paper (e.g. weak membership for Minkowski sums, projections, polars).

▶ **Theorem 11** (Convex Optimization via Ellipsoid Method). *Let $K \subseteq \mathbb{R}^n$ an $(\mathbf{a}_0, r, R)$-centered convex body given by a weak membership oracle O_K. Let $f : \mathbb{R}^n \to \mathbb{R}$ denote an L-Lipshitz convex function given by an oracle that, for every $\mathbf{x} \in \mathbb{Q}^n$ and $\delta > 0$, returns a rational number t such that $|f(\mathbf{x}) - t| \leq \delta$. Then for $\varepsilon > 0$, a rational number ω and vector $\mathbf{y} \in K$ satisfying*

$$\omega - \varepsilon \leq \min_{\mathbf{x} \in K} f(\mathbf{x}) \leq f(\mathbf{y}) \leq \omega$$

can be computed in polynomial time.

The following algorithm from [14], allows us to deterministically compute an ellipsoid with good "sandwiching" guarantees for any centered convex body K.

▶ **Theorem 12** (Algorithm GLS-Round). *Let $K \subseteq R^n$ be an $(\mathbf{a}_0, r, R)$-centered convex body given by a weak membership oracle O_K. Then there is a polynomial time algorithm to compute $A \succ 0$, $A \in \mathbb{Q}^{n \times n}$ and $\mathbf{t} \in \mathbb{R}^n$, such that the ellipsoid $E = E(A)$ satisfies*

$$E + \mathbf{t} \subseteq K \subseteq n^{1/2}(n+1)E + \mathbf{t}.$$

4.2 Lattices

An n-dimensional lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is the integer span of a basis $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ of $\mathbb{R}^n$. We also use the notation $\mathcal{L}(B)$ to denote the lattice spanned by a basis B. The determinant $\det(\mathcal{L})$ of $\mathcal{L}$ is defined as $|\det(B)|$. We define the (symmetric) parallelepiped with respect to B as $\mathcal{P}(B) = B[-1/2, 1/2]^n$. Let $M \subseteq \mathcal{L}$ be a sublattice of $\mathcal{L}$. We define the quotient group $\mathcal{L} \pmod{M} = \{M + \mathbf{y} : \mathbf{y} \in \mathcal{L}\}$, i.e. the cosets of M with respect to $\mathcal{L}$. Let $[\mathcal{L} : M]$ denote the index of $\mathcal{L}$ with respect to M, where $[\mathcal{L} : M] = |\mathcal{L} \pmod{M}|$. If $[\mathcal{L} : M] < \infty$, then $[\mathcal{L} : M] = \det(M)/\det(\mathcal{L})$ and $\dim(M) = \dim(\mathcal{L})$. For $p \in \mathbb{N}$ the group $\mathcal{L}/p \pmod{\mathcal{L}} = \{\mathcal{L} + B\mathbf{a}/p : \mathbf{a} \in \{0, \dots, p-1\}^n\}$, where group addition corresponds to adding the coefficient vectors modulo p, and hence, $\mathcal{L}/p \pmod{\mathcal{L}} \cong \mathbb{Z}_p^n$.

Let K be a $\mathbf{0}$-centered convex body. We denote distance between a point $\mathbf{x} \in \mathbb{R}^n$ and $\mathcal{L}$ under $\|\cdot\|_K$ as $d_K(\mathcal{L}, \mathbf{x}) = \min_{\mathbf{y} \in \mathcal{L}} \|\mathbf{y} - \mathbf{x}\|_K$. The covering radius of K with respect to $\mathcal{L}$ is

$$\mu(K, \mathcal{L}) = \inf \{s \geq 0 : \mathcal{L} + sK = \mathbb{R}^n\} = \max_{\mathbf{x} \in \mathbb{R}^n} d_K(\mathcal{L}, \mathbf{x}).$$

$\mathcal{L}$ is K-covering if $\mu(K, \mathcal{L}) \leq 1$ and α-thin if $\mathrm{vol}_n(K)/\det(\mathcal{L}) \leq \alpha$. We note that the notion of covering radius makes sense for any convex body (since it can be stated independent of centering).

Let K be a symmetric convex body. We define the minimum distance of $\mathcal{L}$ with respect to K as $\lambda_1(K, \mathcal{L}) = \inf_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{y}\|_K$. Let $\lambda = \lambda_1(K, \mathcal{L})$, $\mu = \mu(K, \mathcal{L})$. $\mathcal{L}$ is K-packing if $\lambda_1(K, \mathcal{L}) \geq 2$. The *packing density* of $\mathcal{L}$ with respect to K is $\mathrm{vol}_n(\lambda/2K)/\det(\mathcal{L})$. Note that the packing density is always less than 1 since the lattice shifts of $(\lambda/2)K$ are all interior disjoint. The *covering to packing ratio* of $\mathcal{L}$ with respect to K is $(2\mu)/\lambda$. Note if $s < \lambda/2$, i.e. below the packing radius, then lattice shifts of sK must leave parts of space uncovered. From this, we see that the covering to packing ratio is also always ≥ 1.

Let K be a $\mathbf{0}$-centered convex body. The *Shortest Vector Problem (SVP)* with respect to $\mathcal{L}$ and K is to find a shortest non-zero vector in $\mathcal{L}$ under $\|\cdot\|_K$. The *Closest Vector Problem (CVP)* with respect to $\mathcal{L}$, K and target $\mathbf{x} \in \mathbb{R}^n$ is to find a closest lattice vector $\mathbf{y} \in \mathcal{L}$ to $\mathbf{x}$ under $\|\cdot\|_K$, i.e. that minimizes $\|\mathbf{y}-\mathbf{x}\|_K$.

Let $\mathcal{L}$ be an n-dimensional lattice. A *lattice subspace* $V \subseteq \mathbb{R}^n$ of $\mathcal{L}$, is linear subspace admitting a basis in $\mathcal{L}$, i.e. where $\dim(V) = \dim(V \cap \mathcal{L})$. Note that if $M \subseteq \mathcal{L}$ is a sublattice of finite index, then the set of lattices subspaces of M and $\mathcal{L}$ are identical. Let $\mathbf{v}_1, \dots, \mathbf{v}_n$ denote linearly independent vectors. $\mathbf{b}_1, \dots, \mathbf{b}_n$ is a *directional basis* of $\mathcal{L}$ with respect to $\mathbf{v}_1, \dots, \mathbf{v}_n$ if $\operatorname{span}(\mathbf{b}_1, \dots, \mathbf{b}_i) = \operatorname{span}(\mathbf{v}_1, \dots, \mathbf{v}_i)$ for all $i \in [n]$. Such a directional basis exists if and only if $\operatorname{span}(\mathbf{v}_1, \dots, \mathbf{v}_i)$ is a lattice subspace of $\mathcal{L}$ for $i \in [n]$.

For a basis B of $\mathcal{L}$, define its half open parallelepiped $\mathcal{P}_\circ(B) = B[-1/2, 1/2)^n$. Note that $\mathcal{P}_\circ(B)$ tiles space with respect to $\mathcal{L}$, that is, every point in $\mathbb{R}^n$ is in exactly one lattice shift of $\mathcal{P}_\circ(B)$. Furthermore, any measurable set $F \subseteq \mathbb{R}^n$ which tiles space with respect to $\mathcal{L}$ satisfies $\operatorname{vol}_n(F) = \det(\mathcal{L})$. For a basis $\mathbf{b}_1, \dots, \mathbf{b}_n$, we denote its associated Gram-Schmidt projections by $\pi_1, \dots, \pi_n$, where π_i is the orthogonal projection on $\operatorname{span}(\mathbf{b}_1, \dots, \mathbf{b}_{i-1})^\perp$.

The following is known as Minkowski's convex body theorem:

▶ **Theorem 13** (Minkowski). *For an n-dimensional lattice $\mathcal{L}$ and symmetric convex body K*

$$\lambda_1(K, \mathcal{L}) \leq 2(\det(\mathcal{L})/\operatorname{vol}(K))^{\frac{1}{n}} .$$

K is α-Schnorr-Euchner enumerable (α-SE) with respect to $\mathcal{L}$ with basis $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ (or just with respect to B) if

$$\max_{i \in [n], \mathbf{t} \in \mathbb{R}^n} |\pi_i(K + \mathbf{t}) \cap \pi_i(\mathcal{L})| \leq \alpha,$$

where $\pi_1, \dots, \pi_n$ are the Gram-Schmidt projections with respect to B.

The following lemma from [16] states that the covering radius of a lattice can be approximated using a simple explicit point set.

▶ **Lemma 14.** *Let K and $\mathcal{L}$ be an n-dimensional symmetric convex body and lattice. Then for any $p \in \mathbb{N}$,*

$$(1 - 1/p)\mu(K, \mathcal{L}) \leq \max_{\mathbf{c} \in \mathcal{L}/p \pmod{\mathcal{L}}} d_K(\mathcal{L}, \mathbf{c}) \leq \mu(K, \mathcal{L})$$

5 Thin Lattice Construction

We now describe the three main steps behind the new lattice construction:

1. **M-lattice** (Lemma 20): Construct an M-ellipsoid $E = E(A)$ of K such that $N(K, E) \leq c^n$ and $2^{n+1}\operatorname{vol}(E) \leq \operatorname{vol}_n(K)$. We pick $\mathcal{L}$ to have its basis corresponding to the axes of E, and scaled so that $\det(\mathcal{L}) = \operatorname{vol}_n(E)$.
2. **Packing Lattice** (Lemma 21): Compute $N = |K \cap \mathcal{L}| - 1$ via enumeration, and compute a prime p such that $N < p < 2N$. Compute a sparsifier $M \subseteq \mathcal{L}$ such that $[\mathcal{L} : M] = p$ (essentially, M is a random sublattice of index p), satisfying $1 \leq \lambda_1(K, M) \leq c$.

3. **Rogers Lattice** (Lemma 25): Compute $\lambda = \lambda_1(K, \mathcal{L})$. Apply Rogers densification procedure to M. This computes a super-lattice Λ of M, such that $\lambda = \lambda_1(K, \Lambda)$, and where $\mu(K, \Lambda) \leq (3/2)\lambda$. Return the K-covering lattice $\frac{2}{3\lambda}\Lambda$.

The main result of this section is the following lattice construction (which formalizes Theorem 6 for symmetric bodies):

▶ **Theorem 15.** *For a symmetric convex body $K \subseteq \mathbb{R}^n$, there is a deterministic $2^{O(n)}$ time and $\mathrm{poly}(n)$ space algorithm which computes an n-dimensional lattice Λ with basis B satisfying*

1. *Λ has a covering to packing ratio of at most 3 with respect to K. In particular, Λ is a 3^n-thin K covering lattice.*
2. *K is $2^{O(n)}$-SE with respect to Λ with basis B.*

Furthermore, for any convex body $C \subseteq \mathbb{R}^n$, the set $(C + K) \cap \Lambda$ can be enumerated in $2^{O(n)} N(C, K)$ time using $\mathrm{poly}(n)$ space.

Proof. The construction follows by applying Lemmas 20, 21, 25 in sequence. The furthermore follows directly from Lemma 16 since K is $2^{O(n)}$-SE with respect to Λ with basis B. ◀

5.1 Schnorr-Euchner Enumeration

We now formalize the implementation of Schnorr-Euchner lattice point enumeration over an n-dimensional convex body K and lattice $\mathcal{L}$ with basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$. For $i \in \{0, \ldots, n-1\}$, define the submatrices

$$B^{i-} = (\mathbf{b}_1, \ldots, \mathbf{b}_{n-i}) \quad \text{and} \quad B^{i+} = (\mathbf{b}_{n-i+1}, \ldots, \mathbf{b}_n),$$

and similarly for a vector $\mathbf{x} \in \mathbb{R}^n$, we define

$$\mathbf{x}^{i-} = (\mathbf{x}_1, \ldots, \mathbf{x}_{n-i}) \quad \text{and} \quad \mathbf{x}^{i+} = (\mathbf{x}_{n-i+1}, \ldots, \mathbf{x}_n).$$

The enumeration algorithm is presented below (Algorithm 1).

Algorithm 1 Schnorr-Euchner$(K, B, i, \mathbf{z})$

```
Ensure: $(\mathbf{a}_0, r, R)$-centered convex body $K \subseteq \mathbb{R}^n$ given by a membership oracle,
    $\mathcal{L}(B)$ an $n$-dimensional lattice, level $i$, $0 \leq i \leq n-1$, $B\mathbf{z} \in K$, $\mathbf{z}^{i+} \in \mathbb{Z}$.
Require: Enumeration of $K \cap (\mathcal{L}(B^{i-}) + B^{i+}\mathbf{z}^{i+})$.
1: for all $c \in \{c \in \mathbb{Z} : \exists \mathbf{w} \in \mathbb{R}^{n-i-1}$ s.t. $B(\mathbf{w}, c, \mathbf{z}^{i+}) \in K\}$ do
2:     if $i = n-1$ then
3:         Output $B(c, \mathbf{z}_2, \ldots, \mathbf{z}_n)$.
4:     else
5:         Compute $\mathbf{w} \in \mathbb{R}^{n-i-1}$ such that $B(\mathbf{w}, c, \mathbf{z}^{i+}) \in K$.
6:         Call Schnorr-Euchner$(K, B, i+1, (\mathbf{w}, c, \mathbf{z}^{i+}))$.
```

To begin Schnorr-Euchner enumeration on K, we call Schnorr-Euchner$(K, B, 0, B^{-1}\mathbf{a}_0)$ (remembering that K is $\mathbf{a}_0$-centered). The essential difference with the standard implemention where K is a ball, is the need to solve convex programs in the for loop in line 1. In particular, here we must decide for some $c \in \mathbb{Z}$ whether

$$\exists \mathbf{w} \in \mathbb{R}^{n-i-1} \text{ s.t. } B(\mathbf{w}, c, \mathbf{z}^{i+}) \in K \Leftrightarrow \pi_{n-i}\left(B^{(i+1)+}(c, \mathbf{z}^{i+})\right) \in \pi_{n-i}(K) \tag{7}$$

where π_{n-i} is the associated Gram-Schmidt projection of B. By the above, we note that the set of $c \in \mathbb{R}$ for which the above condition holds is a line segment in $\mathbb{R}$ (since it is 1 dimensional and convex). Hence, the integers c satisfying Equation (7) form a consecutive interval. Furthermore, by our conditions on the input vector $\mathbf{z} \in \mathbb{R}^n$ to the algorithm, the coefficient z_{n-i} lies in this line segment. Hence, determining all the integer values of c satisfying (7) can be enumerated via a line search around z_{n-i} in time

$$\mathrm{poly}(n)(1 + |\left\{c \in \mathbb{Z} : \exists \mathbf{w} \in \mathbb{R}^{n-i-1} \text{ s.t. } B(\mathbf{w}, c, \mathbf{z}^{i+}) \in K\right\}|)$$

In practice we will only be able to solve the above convex program approximately, i.e. where here we compute a vector $\mathbf{w}$ which approximately minimizes the Euclidean distance between $B(\mathbf{w}, c, \mathbf{z}^{i+})$ and K. We note that this corresponds to building a weak membership oracle for the line segment. However, even with only a weak oracle, we can easily modify the above algorithm to guarantee that we enumerate the points in $K \cap \mathcal{L}$ and perhaps some points in $(K + \varepsilon B_2^n) \cap \mathcal{L}$. From the perspective of our applications, this is more than sufficient, and the runtime bounds for the enumeration will be for all intents and purposes identical. We omit the details.

Lastly, from the above analysis, we get that the choices made at the i^{th} level of recursion, associated with the coefficients of $\mathbf{b}_{n-i}$, are in one to one correspondance with the lattice points

$$\pi_{n-i}(\mathcal{L}) \cap \pi_{n-i}(K).$$

From this and the other observations above, we can immediately derive the following lemma (which is standard when K is the Euclidean ball, see for example Lemma 3.1 [17]), which gives the essential complexity of Schnorr-Euchner enumeration.

▶ **Lemma 16.** *Let $K \subseteq \mathbb{R}^n$ be a convex body and let $\mathcal{L}$ be an n-dimensional lattice with basis B. Then the lattice points in $K \cap \mathcal{L}$ can be enumerated (where every point is ouputted exactly once) in time*

$$\mathrm{poly}(n) \sum_{i=1}^{n} |\pi_i(K) \cap \pi_i(\mathcal{L})|$$

using $\mathrm{poly}(n)$ space, where $\pi_1,\ldots,\pi_n$ are the Gram-Schmidt projections of B. In particular, if K is α-SE with respect to $\mathcal{L}$ with basis B, then $K \cap \mathcal{L}$ can be enumerated in $\alpha\mathrm{poly}(n)$ time.

In the remainder of the section, we give useful bounds on the Schnorr-Euchner (SE) enumeration complexity. In particular, we show that SE complexity can be bounded by the covering number with respect to a fundamental parallelepiped, and that SE complexity behaves well under taking sublattices and superlattices.

▶ **Lemma 17.** *Let $K \subseteq \mathbb{R}^n$ be a convex body and let $\mathcal{L}$ be a lattice with basis B. Then K is $N(K, \mathcal{P}_\circ(B))$-SE with respect to $\mathcal{L}$ with basis B.*

Proof. Write $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Let $W_i = \mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$, and $\pi_1, \ldots, \pi_n$ be the Gram-Schmidt projections of B. We must show that for any $\mathbf{x} \in \mathbb{R}^n$,

$$|\pi_i(K + \mathbf{x}) \cap \pi_i(\mathcal{L})| \le N(K, \mathcal{P}_\circ(B)).$$

Let $B_i = (\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_n))$ for $i \in [n]$. Note that B_i is non-singular, $\pi_i(\mathcal{L}) = \mathcal{L}(B_i)$ and that $\pi_i(\mathcal{P}_\circ(B)) = \mathcal{P}_\circ(B_i)$. Let $T \subseteq \mathbb{R}^n$ be an optimal covering of K by $\mathcal{P}_\circ(B)$, i.e. $K \subseteq T + \mathcal{P}_\circ(B)$ and $|T| = N(K, \mathcal{P}_\circ(B))$. Since projections preserve coverings, we also have that

$$\pi_i(K + \mathbf{x}) \subseteq \pi_i(T + \mathbf{x} + \mathcal{P}_\circ(B)) = \pi_i(T) + \pi_i(\mathbf{x}) + \mathcal{P}_\circ(B_i)$$

Since $\mathcal{P}_\circ(B_i)$ tiles W_i with respect to $\pi_i(\mathcal{L})$, any shift in of $\mathcal{P}_\circ(B_i)$ in W_i contains exactly point of $\pi_i(\mathcal{L})$. Hence

$$|\pi_i(K + \mathbf{x}) \cap \pi_i(\mathcal{L})| \leq |(\pi_i(T) + \pi_i(\mathbf{x}) + \mathcal{P}_\circ(B_i)) \cap \mathcal{L}| \leq |\pi_i(T)| \leq |T| = N(K, \mathcal{P}_\circ(B))$$

as needed. ◀

▶ **Lemma 18.** *Let $K \subseteq \mathbb{R}^n$ be a convex body which is α-SE with respect to an n-dimensional lattice $\mathcal{L}$ with basis B. If M is a*

1. **Full rank sublattice of $\mathcal{L}$:** *K is α-SE with respect to M and basis B_M,*
2. **Superlattice of $\mathcal{L}$:** *K is $\alpha[M : \mathcal{L}]$-SE with respect M and basis B_M,*

where B_M is a directional basis of M with respect to B. Furthermore, if M is given by a basis $H \in \mathbb{R}^{n \times n}$, then the directional basis B_M can be computed in polynomial time.

Proof. Let $\pi_1, \dots, \pi_n$ denote the Gram-Schmidt projections of B. In both cases 1 and 2, note that M and $\mathcal{L}$ have exactly the same lattice subspaces, and hence a directional basis B_M of M with respect to B exists. Furthermore, by construction both B and B_M have exactly the same Gram-Schmidt projections.

For case 1, the SE complexity bound of K with respect to M with basis B_M is therefore

$$\max_{\mathbf{t} \in \mathbb{R}^n} |\pi_i(K + \mathbf{t}) \cap \pi_i(M)| \leq \max_{\mathbf{t} \in \mathbb{R}^n} |\pi_i(K + \mathbf{t}) \cap \pi_i(\mathcal{L})| \leq \alpha$$

by the inclusion $M \subseteq \mathcal{L}$. For case 2, we note that we can write $M = S + \mathcal{L}$, where $|S| = [M : \mathcal{L}]$ (here S simply chooses one representative from each coset $M \pmod{\mathcal{L}}$). From here, we see that the SE complexity is bounded by

$$\begin{aligned} |\pi_i(K + \mathbf{t}) \cap \pi_i(M)| = |\pi_i(K + \mathbf{t}) \cap \pi_i(\mathcal{L} + S)| &\leq \sum_{\mathbf{s} \in S} |\pi_i(K + \mathbf{t}) \cap \pi_i(\mathcal{L} + \mathbf{s})| \\ &= \sum_{\mathbf{s} \in S} |\pi_i(K + \mathbf{t} - \mathbf{s}) \cap \pi_i(\mathcal{L})| \leq \alpha |S| = \alpha[M : \mathcal{L}], \end{aligned}$$

for any $\mathbf{t} \in \mathbb{R}^n$, as needed.

We prove the furthermore. Here M is the given by a basis H. By solving a system of linear equations we can compute a matrix $X \in \mathbb{R}^{n \times n}$ such that $HX = B$.

We claim that $X \in \mathbb{Q}^{n \times n}$. If M is a superlattice of $\mathcal{L}$, then by inclusion, we clearly have that $X \in \mathbb{Z}^{n \times n}$. If M is a sublattice, since $\mathcal{L} \pmod{M}$ is an abelian group of order $[\mathcal{L} : M] = \det(M)/\det(\mathcal{L})$, the coefficients of any lattice vector in $\mathcal{L}$ with respect to H must be multiples of $1/[\mathcal{L} : M]$. In particular, the matrix $[\mathcal{L} : M]X \in \mathbb{Z}^{n \times n}$. This proves the claim.

Now we note that H is a directional basis with respect to B if and only if X is upper triangular. Hence, computing a directional basis is equivalent to computing an $n \times n$ unimodular matrix U such that UX is upper triangular, since then HU^{-1} is the desired basis. This can be achieved by computing the unimodular transformation U which puts UX (or $[\mathcal{L} : M]UX$) into Hermite Normal Form (HNF). Since the HNF can be computed in polynomial time, computing a directional basis can be computed in polynomial time as claimed. ◀

▶ **Lemma 19.** *Let K be convex symmetric and α-SE with respect to $\mathcal{L}$ with basis B. Then for any convex body $C \subseteq \mathbb{R}^n$, C is $\alpha N(C, K)$-SE with respect to $\mathcal{L}$ with basis B. Furthermore, for the body $C + K$ this bound specializes to $O(\alpha 3^n (n \log n) N(C, K))$.*

Proof. Let T be an optimal covering of C by K. Then

$$|\pi_i(C) \cap \pi_i(\mathcal{L})| \leq |\pi_i(T + K) \cap \pi_i(\mathcal{L})| \leq \sum_{\mathbf{t} \in T} |\pi_i(\mathbf{t} + K) \cap \pi_i(\mathcal{L})| \leq \alpha |T| = \alpha N(C, K),$$

as needed. For the furthermore, it follows from the inequality

$$\begin{aligned} N(C + K, K) &\leq N(C, K) N(2K, K) = O((n \log n) \mathrm{vol}_n(2K + K)/\mathrm{vol}_n(K)) N(C, K) \\ &= O(3^n (n \log n) N(C, K)) \end{aligned}$$

where the last inequality follows from Theorem 8. ◀

5.2 Construction Steps

▶ **Lemma 20** (M-lattice)**.** *Let K be a symmetric convex body. There is a deterministic $2^{O(n)}$ time and* $\mathrm{poly}(n)$ *space algorithm which computes a lattice $\mathcal{L}$ with basis B, satisfying*

1. $2^{n+1} \det(\mathcal{L}) \leq \mathrm{vol}_n(K)$ 2. $N(K, \mathcal{P}_\circ(B)) \leq c^n$

for some absolute constant $c \geq 1$. In particular, K is c^n-SE with respect to $\mathcal{L}$ with basis B.

Proof. Using Theorem 10 we compute an M-ellipsoid $E = E(A)$ for K, such that K, E have covering numbers bounded by (c_0^n, c_0^n). This can be done deterministically in $2^{O(n)}$ time and $\mathrm{poly}(n)$ space.

Let $B = 1/(2^{1+1/n} c_0) V_n^{1/n} A^{-1/2}$. We claim that $\mathcal{L} = \mathcal{L}(B)$ satisfies the desired properties. First, we remember that $E = A^{-1/2} B_2^n$ and that $\mathrm{vol}_n(E) = |\det(A^{-1/2})| V_n$.

For property 1, we have that

$$2^{n+1} \det(\mathcal{L}) = \det(B) = 2^{n+1}(2^{-(n+1)} c_0^{-n} V_n |\det(A^{-1/2})|) = c_0^{-n} \mathrm{vol}_n(E) \leq \mathrm{vol}_n(K),$$

as needed, where the last inequality follows from the fact that $\mathrm{vol}_n(E) \leq N(E, K) \mathrm{vol}_n(K)$.

For property 2, we first note that

$$\mathcal{P}_\circ(B) = A^{-1/2} \left[-\frac{V_n^{1/n}}{2^{2+1/n} c_0}, \frac{V_n^{1/n}}{2^{2+1/n} c_0} \right)^n.$$

Assuming that $c_0 \geq 2$ (it is actually much larger), it is easy to see that $V_n^{1/n}/(2^{2+1/n} c_0) \leq 1/\sqrt{n}$ (at least for n large enough) since $\sqrt{n} V_n^{1/n} \to \sqrt{2\pi e} \leq 5$. Therefore we may assume that

$$A^{-1/2} \left[-\frac{V_n^{1/n}}{2^{2+1/n} c_0}, \frac{V_n^{1/n}}{2^{2+1/n} c_0} \right)^n \subseteq A^{-1/2} \left[\frac{-1}{\sqrt{n}}, \frac{1}{\sqrt{n}} \right)^n \subseteq A^{-1/2} B_2^n = E(A).$$

From here, we have that

$$N(K, \mathcal{P}_\circ(B)) \leq N(K, E) N(E, \mathcal{P}_\circ(B)) \leq c^n N(E, \mathcal{P}_\circ(B))$$

Using the fact that $\mathcal{P}_\circ(B)$ tiles space with respect to $\mathcal{L}$ (and hence has covering density 1), we get that

$$N(E, \mathcal{P}_\circ(B)) \leq \frac{\mathrm{vol}_n(E - \mathcal{P}_\circ(B))}{\mathrm{vol}_n(\mathcal{P}_\circ(B))} \leq \frac{\mathrm{vol}_n(2E)}{\det(\mathcal{L})} = 2^n (2^{n+1} c_0^n) = 2(4c_0)^n$$

Putting everything together, we get $N(K, \mathcal{P}_\circ(B)) \leq 2(4c_0^2)^n \leq c^n$ (for $c = 5c_0^2$ say), as needed. Since the computation of B can be done in $\mathrm{poly}(n)$ time, the desired bound on the runtime and space usage holds. Lastly, for the furthermore, we note that it follows directly from Lemma 17 ◀

▶ **Lemma 21** (Packing Lattice). *Starting from $\mathcal{L}$ and B be as in Lemma 20, a sublattice $M \subseteq \mathcal{L}$, $[\mathcal{L} : M] \leq 2c^n$, and its directional basis B_M with respect to B, satisfying $1 \leq \lambda_1(K, M) \leq c$ can be computed in deterministic $\mathrm{poly}(n)c^{2n}$ time using $\mathrm{poly}(n)$ space. Furthermore, K is c^n-SE with respect to M with basis B_M, and M has packing density at least c^{-n} with respect to K.*

Proof. By a change of basis, that is multiplying by B^{-1}, we may assume that $\mathcal{L} = \mathbb{Z}^n$ and that our basis is $\mathbf{e}_1, \dots, \mathbf{e}_n$. We shall first show the existence of M via the probabilistic method (M will be a random sublattice of $\mathcal{L}$), and then use the method of conditional expectations to derandomize the construction.

Existence: Let $S = (K \cap \mathbb{Z}^n) \setminus \{\mathbf{0}\}$, and let $N = |S|$. Since K is symmetric

$$\mathrm{vol}_n(K) \geq 2^{n+1} \det(\mathbb{Z}^n) > 2^n,$$

by Minkowski's convex body theorem we know that $N \geq 2$. Let p be a prime such that $N < p < 2N$ (that such a prime always exists is Bertrand's postulate).

▶ Claim 22. $\forall\, \mathbf{x} \in S$, $\mathbf{x} \not\equiv \mathbf{0} \pmod{p\mathbb{Z}^n}$.

Proof. For the sake of contradiction, assume that for some $\mathbf{x} \in S$, $\mathbf{x} \equiv \mathbf{0} \pmod{p\mathbb{Z}^n}$. Then by convexity and symmetry of K, we must have that $\pm\{\mathbf{x}/p, 2\mathbf{x}/p, \dots, \mathbf{x}\} \subseteq K \cap \mathbb{Z}^n \setminus \{\mathbf{0}\} = S$. But then $|S| \geq 2p$, a clear contradiction. ◀

Let $\mathbf{a} \leftarrow \mathbb{Z}_p^n$ be a uniform element of $\mathbb{Z}_p^n$. Let $M = \{\mathbf{y} \in \mathbb{Z}^n : \langle \mathbf{a}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}$. Note that as long as $\mathbf{a} \neq \mathbf{0}$ (in this case $M = \mathbb{Z}^n$), M is a sublattice of $\mathbb{Z}^n$ of index $[\mathbb{Z}^n : M] = p$.

▶ Claim 23. $\mathbb{E}_{\mathbf{a}}[|(M \cap K) \setminus \{\mathbf{0}\}|] = N/p < 1$.

Proof. Since for all $\mathbf{x} \in S$, $\mathbf{x} \not\equiv \mathbf{0} \pmod{p\mathbb{Z}^n}$ (by Claim 22), we have that $\langle \mathbf{x}, \mathbf{a} \rangle$ is uniformly distributed in $\mathbb{Z}_p$ since p is prime. In particular, $\Pr_{\mathbf{a}}[\langle \mathbf{a}, \mathbf{x} \rangle] = 1/p$. Therefore by linearity of expectation

$$\mathbb{E}_{\mathbf{a}}[|(M \cap K) \setminus \{\mathbf{0}\}|] = \sum_{\mathbf{x} \in S} \Pr_{\mathbf{a}}[\mathbf{x} \in M] = \sum_{\mathbf{x} \in S} \Pr_{\mathbf{a}}[\langle \mathbf{x}, \mathbf{a} \rangle \equiv 0 \pmod{p}] = \sum_{\mathbf{x} \in S} 1/p = N/p < 1$$

◀

By Claim 23, there exists $\mathbf{a} \in \mathbb{Z}_p^n$ such the associated lattice M satisfies $|(M \cap K) \setminus \{\mathbf{0}\}| = 0$. We show that M satisfies the conditions of the lemma. First, by construction, we have $\lambda_1(K, M) \geq 1$. The following claim yields the upper bound:

▶ Claim 24. For M as above, we have that $\lambda_1(K, M) \leq c$.

Proof. Firstly, note that

$$\det(M) \leq p < 2N \leq 2|K \cap \mathcal{L}| \leq 2c^n$$

Next, by construction

$$\mathrm{vol}(cK) = c^n \mathrm{vol}(K) \geq c^n 2^{n+1} \geq 2^n \det(M).$$

Hence by Minkowski's convex body theorem, $\lambda_1(K, M) \leq c$ as needed. ◀

Let $\lambda = \lambda_1(K, M)$. We can lower bound the packing density of M with respect to K as follows:

$$\frac{\mathrm{vol}_n(\lambda/2K)}{\det(M)} \geq \frac{\mathrm{vol}_n(1/2K)}{p} = \frac{2^{-n}\mathrm{vol}_n(K)}{p} \geq \frac{2}{p} \geq \frac{2}{2c^n} = c^{-n},$$

as needed. Lastly, that K is c^n-SE with respect to M with basis B_M follows directly from Lemma 18 and the guarantee that K is c^n-SE with respect to $\mathbb{Z}^n$ with the standard basis.

Algorithm: We now show how to derandomize the above construction in $\mathrm{poly}(n)c^{2n}$ time using only $\mathrm{poly}(n)$ space. The idea here is simply to choose the coefficients of $\mathbf{a} = (a_1, \ldots, a_n)$ one at a time from left to right. Each time we fix a coefficient we will guarantee that conditioned on fixed coefficients, the expected number of points in $M \cap K \setminus \{\mathbf{0}\}$ (averaging over the randomness for the remaining coefficients) is less than 1. We now give the formula for the conditional expectation. For a vector $\mathbf{x} \in \mathbb{R}^n$, define

$$\mathbf{x}^{i-} = (\mathbf{x}_1, \ldots, \mathbf{x}_i) \quad \text{ and } \mathbf{x}^{i+} = (\mathbf{x}_{i+1}, \ldots, \mathbf{x}_n).$$

Assume we have already fixed $\mathbf{a}^{(i-1)-} = (c_1, \ldots, c_{i-1})$ and are left with choosing the values of $a_i, \ldots, a_n$. If we set $a_i = c_i$, we condition $\mathbf{a}$ on the event $\mathbf{a}^{i-} = (c_1, \ldots, c_i) \overset{\text{def}}{=} \mathbf{c}^i$. Then we have that

$$\begin{aligned}\mathbb{E}_{\mathbf{a}}[|(M \cap K) \setminus \{\mathbf{0}\}| \mid \mathbf{a}^{i-} = \mathbf{c}^i] &= \sum_{\mathbf{x} \in S} \Pr_{\mathbf{a}}\left[\langle \mathbf{a}, \mathbf{x} \rangle \equiv 0 \pmod{p} \mid \mathbf{a}^{i-} = \mathbf{c}^i\right] \\ &= \sum_{\mathbf{x} \in S} \Pr_{\mathbf{a}}\left[\left\langle \mathbf{c}^i, \mathbf{x}^{i-} \right\rangle + \left\langle \mathbf{a}^{i+}, \mathbf{x}^{i+} \right\rangle \equiv 0 \pmod{p}\right] \qquad (8)\end{aligned}$$

From here, we have that

$$\Pr_{\mathbf{a}}\left[\left\langle \mathbf{c}^i, \mathbf{x}^{i-} \right\rangle + \left\langle \mathbf{a}^{i+}, \mathbf{x}^{i+} \right\rangle \equiv 0 \pmod{p}\right] = \begin{cases} 1/p & : \ \mathbf{x}^{i+} \not\equiv \mathbf{0} \pmod{p\mathbb{Z}^{n-i}} \\ 0 & : \ \left\langle \mathbf{c}^i, \mathbf{x}^{i-} \right\rangle \not\equiv 0 \pmod{p} \\ 1 & : \ \text{otherwise} \end{cases}$$

Therefore the expectation in Equation (8) can be expressed as

$$\begin{aligned}\mathbb{E}_{\mathbf{a}}[|(M \cap K) \setminus \{\mathbf{0}\}| \mid \mathbf{a}^{i-} = \mathbf{c}^i] = &\left|\left\{\mathbf{x} \in S : \mathbf{x}^{i+} \equiv \mathbf{0} \pmod{p\mathbb{Z}^{n-i}}, \left\langle \mathbf{c}^i, \mathbf{x}^{i-} \right\rangle \equiv 0 \pmod{p}\right\}\right| + \\ &\left|\left\{\mathbf{x} \in S : \mathbf{x}^{i+} \not\equiv \mathbf{0} \pmod{p\mathbb{Z}^{n-i}}\right\}\right|/p \qquad (9)\end{aligned}$$

Notice that this expectation is less than 1 if and only if the first set on the right hand side is empty (this set corresponds to the elements that are definitively in M). Since the global expectation is $N/p < 1$, by the properties of conditional expectations and Equation 9, we can guess the coordinates of $\mathbf{a}$ one by one as long as the set of points definitively in M remains empty (i.e. the greedy strategy works).

From these observations, we get the following algorithm for building M:

```
Compute $N = |S|$ via Schnorr-Euchner enumeration over $K \cap \mathcal{L}$ (using the standard
basis).
Pick a prime $p$ satisfying $N < p < 2N$.
for all $i \in 1$ to $n$ do
    Guess $\mathbf{a}_i$ by trying all numbers in $\{0, \ldots, p-1\}$. Accept a guess for $\mathbf{a}_i$ if

        $\{\mathbf{x} \in S : \mathbf{x}^{i+} \equiv \mathbf{0} \pmod{p\mathbb{Z}^{n-i}}, \langle \mathbf{a}^{i-}, \mathbf{x}^{i-} \rangle \equiv 0 \pmod{p}\} = \emptyset$.

    Verify this condition for each potential guess using Schnorr-Euchner enumeration over
    $S$.
```

```
4: return $M = \{\mathbf{x} \in \mathbb{Z}^n : \langle \mathbf{x}, \mathbf{a} \rangle \equiv 0 \pmod{p}\}$
```

Given M from the above algorithm, we must still compute a directional basis with respect to the standard basis. This is straightforward. Let $j \in [n]$ denote first non-zero coefficient of $\mathbf{a}$. Rescaling by $\mathbf{a}_j^{-1} \pmod{p}$, we may assume that $\mathbf{a}_j = 1$. From here, it is direct to verify that

$$(\mathbf{e}_1, \dots, \mathbf{e}_{j-1}, p\mathbf{e}_j, -\mathbf{a}_{j+1}\mathbf{e}_j + \mathbf{e}_{j+1}, \dots, -\mathbf{a}_n\mathbf{e}_j + \mathbf{e}_n)$$

is a valid directional basis for M.

Since the correctness of the above algorithm has already been argued, it remains to bound the algorithms complexity. Firstly, by construction $\mathcal{L}$, we have that K is c^n-SE with respect to $\mathbb{Z}^n$ with the standard basis. Hence, by Lemma 16 every Schnorr-Euchner enumeration over $K \cap \mathbb{Z}^n$ can be performed in $\mathrm{poly}(n)c^n$ time using $\mathrm{poly}(n)$ space. We perform one such enumeration to compute N, and at most $np \leq 2nc^n$ such enumerations during the main loop of the algorithm. Hence the amount of time spent during the enumeration steps is at most $\mathrm{poly}(n)c^{2n}$. Lastly, the time to compute p is can be bounded by $\mathrm{poly}(n)c^n$, by simply enumerating over all the choices between N and $2N$ and using any deterministic primality test. ◀

▶ **Lemma 25** (Rogers Lattice). *Starting from M and B_M be as in Lemma 21, a super-lattice Λ of M, with directional basis B_Λ with respect to B_M, satisfying*

1. $\lambda_1(K, M) = \lambda_1(K, \Lambda)$,
2. $\mu(K, \Lambda) \leq 3/2\lambda_1(K, \Lambda) \leq 3c/2$,
3. $[\Lambda : M] \leq c^n$,

can be computed in $\tilde{O}((2c^3)^n)$ time and $\mathrm{poly}(n)$ space. Letting $\lambda = \lambda_1(K, \Lambda)$, we furthermore have that

(a) $2/(3\lambda)\Lambda$ *is a 3^n-thin K-covering lattice.*
(b) K *is $\tilde{O}((2c^3)^n)$-SE with respect to $2/(3\lambda)\Lambda$ with basis $2/(3\lambda)B_\Lambda$.*

Proof. To build the covering lattice for K claimed by the Lemma we will use Rogers densification procedure. We first describe and analyze its the basic properties, then analyze its effects on M, and lastly discuss the details of making it algorithmic in our setting. This densification can be applied to any n-dimensional lattice $\mathcal{L}$. It proceeds as follows:

Find a coset $\mathcal{L} + \mathbf{c} \in \mathcal{L}/3 \pmod{\mathcal{L}}$, such that $d_K(\mathcal{L}, \mathbf{c}) > \lambda_1(K, \mathcal{L})$. If none exists, return $\mathcal{L}$. Otherwise, replace $\mathcal{L}$ by $\mathcal{L} + \{-\mathbf{c}, \mathbf{0}, \mathbf{c}\}$, where $\mathbf{c}$ is the coset found by the procedure, and repeat.

Basic Properties: We analyze the properties of $\mathcal{L}$ at termination. Let $\lambda = \lambda_1(K, \mathcal{L})$. By construction, after termination, we must have that

$$\max_{\mathbf{c} \in \mathcal{L}/3 \pmod{\mathcal{L}}} d_K(\mathcal{L}, \mathbf{c}) \leq \lambda.$$

Therefore, by Lemma 14, we must have that $\mu(K, \mathcal{L}) \leq 3/2\lambda$. We claim that $2/(3\lambda)\mathcal{L}$ is a 3^n-thin K-covering lattice. Clearly, $\mu(K, 2/(3\lambda)\mathcal{L}) \leq 1$ by the previous inequality. For the thinness, note that

$$\frac{\mathrm{vol}_n(K)}{\det(2/(3\lambda)\mathcal{L})} = \frac{\mathrm{vol}_n(3\lambda/2K)}{\det(\mathcal{L})} \leq \frac{\mathrm{vol}_n(3\lambda/2K)}{\mathrm{vol}_n(\lambda/2K)} = 3^n$$

where the inequality $\mathrm{vol}_n(\lambda/2K) \leq \det(\mathcal{L})$ follows directly from Minkowski's convex body theorem.

We now bound the convergence time of the densification procedure. We claim that at each non-terminating iteration, the length of the shortest-nonzero vector is unchanged, while the determinant of $\mathcal{L}$ decreases by a factor 3. For the first property, take $\mathcal{L} + \mathbf{c} \in \mathcal{L}/3 \pmod{\mathcal{L}}$ such that $d_K(\mathcal{L}, \mathbf{c}) \geq \lambda_1(K, \mathcal{L})$. Since $3\mathbf{c} \in \mathcal{L}$, note that $\mathcal{L}' \overset{\mathrm{def}}{=} \mathcal{L} + \mathbb{Z}\mathbf{c} = \mathcal{L} + \{-\mathbf{c}, \mathbf{0}, \mathbf{c}\}$. From here, we have that

$$\lambda_1(\mathcal{L}') = \min\{d_K(\mathcal{L}, -\mathbf{x}), \lambda_1(K, \mathcal{L}), d_K(\mathcal{L}, \mathbf{x})\} = \min\{\lambda_1(K, \mathcal{L}), d_K(\mathcal{L}, \mathbf{x})\} = \lambda_1(K, \mathcal{L}),$$

where the equality $d_K(\mathcal{L}, -\mathbf{x}) = d_K(\mathcal{L}, \mathbf{x})$ follows by symmetry of K. Hence the length of the shortest non-zero vector stays unchanged. The second claimed property follows from $|\mathcal{L}' \pmod{\mathcal{L}}| = |\mathbb{Z}_3| = 3$.

Let $\alpha = \mathrm{vol}_n(\lambda/2K)/\det(\mathcal{L})$ denote the packing density of $\mathcal{L}$. By the previous analysis, at each non-terminating iteration, the packing density of $\mathcal{L}$ increases by a factor 3. Since the packing density never exceeds 1, if k is the number of non-terminating iterations, we must have that $\alpha 3^k \leq 1 \Rightarrow k \leq \lfloor \log_3(1/\alpha) \rfloor$. In particular, if the base lattice is $\mathcal{L}$ and $\mathcal{L}_k$ is the final outputted lattice, we must have that $[\mathcal{L}_k : \mathcal{L}] \leq 1/\alpha$.

Behavior on M: Let M be the lattice from 21 with basis B_M, and let Λ be the lattice outputted by the densification procedure. Let $\lambda = \lambda_1(K, M)$. Since we are guaranteed that $\lambda_1(K, \Lambda) = \lambda \leq c$, we have that $\mu(K, \Lambda) \leq 3/2\lambda \leq 3/2c$. The remaining thinness and covering properties of Λ are now guaranteed by the our previous analysis. Furthermore, since M has packing density at least c^{-n}, our previous analysis also ensures that $[\Lambda : M] \leq c^n$.

Let B_Λ denote the directional basis of Λ with respect to B_M. Since K is c^n-SE with respect to M with basis B_M, we get from Lemma 18 that K is $c^n[\Lambda : M] \leq c^{2n}$ SE with respect to Λ with basis B_M. From Lemma 19, we get that $3c/2K$ is $c^{2n}N(3c/2K, K)$-SE with respect to Λ with basis B_Λ. By Theorem 8, we get that

$$N(3c/2K, K) = O(n \log n) \frac{\mathrm{vol}_n(3c/2K + K)}{\mathrm{vol}_n(K)} = O(n \log n (3c/2 + 1)^n) = \tilde{O}((3c/2 + 1)^n).$$

Hence $c^{2n}N(3c/2K, K) = \tilde{O}((3c^3/2 + c^2)^n) = \tilde{O}((2c^3)^n)$. Since $3/2\lambda \leq 3/2c$ the same SE holds for $3/2\lambda K$, and by scaling for K with respect to $2/(3\lambda)\Lambda$ with basis $2/(3\lambda)B_\Lambda$. Hence Λ satisfies all the requirements of the lemma.

Algorithm: We analyze the complexity of making Roger's densification algorithmic on M. Firstly, we need to compute $\lambda = \lambda_1(K, M)$. Since $\lambda \leq c$, it suffices to enumerate the points in $cK \cap M$, and return the length of shortest non-zero vector found. Since K is c^n-SE with respect to M with basis B_M, by Lemma 16 this enumeration takes at most

$$\mathrm{poly}(n) c^n N(cK, K) \leq \mathrm{poly}(n) c^n (c+1)^n \leq \mathrm{poly}(n)(2c^2)^n$$

time and $\mathrm{poly}(n)$ space. Now let M_k with directional basis B_{M_k} with respect to B_M denote the resultant lattice after k iterations. Here, for each coset

$$M_k + \mathbf{c} \in M_k/3 \pmod{M_k} = \{M_k + B_{M_k}\mathbf{a}/3 : \mathbf{a} \in \{-1, 0, 1\}^n\},$$

we must verify whether $d_K(M_k, \mathbf{c}) > \lambda$. Note that this last step is equivalent to checking whether

$$d_K(M_k, \mathbf{c}) > \lambda \quad \Leftrightarrow \quad M_k \cap (\mathbf{c} + \lambda K) = \emptyset,$$

which can be verified by straightforward enumeration. Since $[M_k : M] \leq c^n$, by Lemmas 18 and 16 we get the Schnorr-Euchner enumeration over $\mathbf{c} + \lambda K$ takes at most $\mathrm{poly}(n) c^n (2c^2)^n =$

$\tilde{O}((2c^3)^n)$ time and $\mathrm{poly}(n)$ space. Since we may enumerate over all 3^n cosets of $M_k/3 \pmod{M_k}$, the time for a single iteration can be bounded by $\tilde{O}((6c^3)^n)$ time. Furthermore, if coset $\mathbf{c}$ is to be added to M_k, a directional basis for $M_{k+1} = M_k + \mathbb{Z}\mathbf{c}$ can clearly be computed in polynomial time from $\mathbf{c}$ and B_{M_k}. Lastly, since the number of iterations is bounded by $\log_3 c^n = O(n)$, the total runtime can be bounded by $\tilde{O}((6c^3)^n)$ and the space usage by $\mathrm{poly}(n)$ as needed. ◀

6 Volume Estimation

In this section, we describe the new algorithm for volume estimation. Our algorithm will rely on a construction for thin covering lattices for general convex bodies bodies, which will in turn rely on an algorithm for computing approximate Kovner-Besicovitch points. The guarantees for the generalized thin lattice construction (which formalizes Theorem 6 for general convex bodies) are as follows:

▶ **Theorem 26** (General Thin Lattice). *For a convex body $K \subseteq \mathbb{R}^n$, there is a $2^{O(n)}$ time and $\mathrm{poly}(n)$ space algorithm which computes an n dimensional lattice Λ with basis B, and a point $\mathbf{c} \in K$ satisfying*

1. *Λ is a 3^n-thin $K[\mathbf{c}]$-covering and a 7^n-thin K-covering lattice.*
2. *Λ has covering to packing ratio at most 3 with respect to $K[\mathbf{c}]$.*
3. *$K[\mathbf{c}]$ and K are both $2^{O(n)}$-SE with respect to Λ with basis B.*

Furthermore, for any convex body $C \subseteq \mathbb{R}^n$, the set $(C - K) \cap \Lambda$ can be enumerated in $2^{O(n)} N(C, K)$ time using $\mathrm{poly}(n)$ space.

Proof. We first use algorithm of Theorem 7 to compute $(6/7)^n$ approximate Kovner-Besicovitch point $\mathbf{c} \in K$. Using the algorithm of Theorem 15 we build a 3^n-thin $K[\mathbf{c}]$-covering lattice Λ with basis B. Since $K[\mathbf{c}] \subseteq K - \mathbf{c}$, Λ is also a K-covering lattice. To bound the thinness with respect to K, by the guarantees on $\mathbf{c}$, we have that

$$\begin{aligned}\frac{\mathrm{vol}_n(K)}{\det(\Lambda)} &= \frac{\mathrm{vol}_n(K)}{\mathrm{vol}_n(K[\mathbf{c}])}\frac{\mathrm{vol}_n(K)}{\det(\Lambda)} \leq \frac{3^n}{(6/7)^n \mathrm{Sym}_{kb}(K)} \\ &\leq (7/6)^n 2^n 3^n = 7^n\end{aligned}$$

From the guarantees on Λ, we know that $K[\mathbf{c}]$ is $2^{O(n)}$-SE with respect to B. Therefore, by Lemma 19, the SE complexity of K with respect to B is bounded by

$$\begin{aligned}2^{O(n)} N(K, K[\mathbf{c}]) = 2^{O(n)}\ O(n \log n)\ \frac{\mathrm{vol}_n(K + K[\mathbf{c}])}{\mathrm{vol}_n(K[\mathbf{c}])} &\leq 2^{O(n)} \frac{\mathrm{vol}_n(2K)}{\mathrm{vol}_n(K[\mathbf{c}])} \\ = 2^{O(n)}\ 2^n\ \frac{\mathrm{vol}_n(K)}{\mathrm{vol}_n(K[\mathbf{c}])} &\leq 2^{O(n)}\ 2^n\ (7/3)^n = 2^{O(n)}\end{aligned}$$

as needed. The remaining guarantees on Λ and the complexity bound for the above algorithm now follows directly from guarantees in Theorems 7 and 15. ◀

We will use Theorem 26 within the volume estimation algorithm. The following Lemma is used to justify the accuracy of volume estimation algorithm.

▶ **Lemma 27.** *Let K_0, K be n dimensional convex bodies. Let $\mathcal{L}$ be an n-dimensional K_0-covering lattice. For $\varepsilon > 0$, the following holds:*

$$\mathrm{vol}_n(K) \leq \varepsilon^n \det(\mathcal{L})\ |\varepsilon\mathcal{L} \cap (K - \varepsilon K_0)| \leq \mathrm{vol}_n(K + \varepsilon(K_0 - K_0))\ .$$

Furthermore, if $K_0 \subseteq K - \mathbf{c}$, for some $\mathbf{c} \in \mathbb{R}^n$, and K_0 is symmetric then

$$\mathrm{vol}_n(K) \leq \varepsilon^n \det(\mathcal{L}) \, |\varepsilon\mathcal{L} \cap ((1+\varepsilon)K - \varepsilon\mathbf{c})| \leq (1+2\varepsilon)^n \mathrm{vol}_n(K) \ .$$

Proof.

▶ Claim 28. There exists a subset $F \subseteq K_0$ such that F tiles with respect $\mathcal{L}$. In particular, $\mathrm{vol}_n(F) = \det(\mathcal{L})$.

Proof. Since the tiling / covering property is shift invariant, we may shift K_0 so that $\mathbf{0}$ is in the interior of K. From here, note that $\|\cdot\|_{K_0}$ is an asymmetric norm. We define F to be all the points $\mathbf{x} \in \mathbb{R}^n$ such that $\mathbf{0}$ is the lexicographically minimal closest lattice vector to $\mathbf{x}$ under $\|\cdot\|_{K_0}$. More presicely, $\mathbf{x} \in F$ iff

$$\|\mathbf{x} - \mathbf{0}\|_{K_0} = \|\mathbf{x}\|_{K_0} = d_{K_0}(\mathcal{L}, \mathbf{x}) = \min_{\mathbf{y} \in \mathcal{L}} \|\mathbf{x} - \mathbf{y}\|_{K_0}$$

and $\mathbf{0}$ is the lexicographically smallest minimizer for the last expression on the right hand side. Since every point in $\mathbb{R}^n$ has a unique lexicographically closest lattice vector in $\mathcal{L}$, and since the standard lexicographic order on $\mathbb{R}^n$ is shift invariant, we see that F tiles space with respect to $\mathcal{L}$. That $\mathrm{vol}_n(F) = \det(\mathcal{L})$ follows directly from the tiling property.

We claim that $F \subseteq K_0$. Assume not, then $\exists \mathbf{x} \in F$ such that $\|\mathbf{x}\|_{K_0} > 1$. Since $\mathcal{L}$ is K_0-covering, there exists $\mathbf{y} \in \mathcal{L}$ such that $\mathbf{x} \in \mathbf{y} + K_0$. But then $\|\mathbf{x} - \mathbf{y}\|_{K_0} \leq 1 < \|\mathbf{x}\|_{K_0}$, which contradicts that $\mathbf{0}$ is a closest lattice vector to $\mathbf{x}$. Hence $F \subseteq K_0$ as claimed. ◀

Since $\varepsilon\mathcal{L}$ is εF-tiling (where F is as above), we have that the $\varepsilon\mathcal{L}$ shifts of εF covering K correspond exactly to the centers $\varepsilon\mathcal{L} \cap (K - \varepsilon F)$. From here, since $F \subseteq K_0$, we have the inclusions

$$\begin{aligned} K &\subseteq (\varepsilon\mathcal{L} \cap (K - \varepsilon F)) + \varepsilon F \\ &\subseteq (\varepsilon\mathcal{L} \cap (K - \varepsilon F)) + \varepsilon F \subseteq (\varepsilon\mathcal{L} \cap (K - \varepsilon K_0)) + \varepsilon K_0 \\ &\subseteq (K - \varepsilon K_0) + \varepsilon K_0 = K + \varepsilon(K_0 - K_0) \end{aligned} \tag{10}$$

From the above inclusions, we get that

$$\mathrm{vol}_n(K) \leq \mathrm{vol}_n((\varepsilon\mathcal{L} \cap (K - \varepsilon K_0)) + \varepsilon F) \leq \mathrm{vol}_n(K + \varepsilon(K_0 - K_0)).$$

Since F tiles with respect to $\mathcal{L}$, we see that

$$\begin{aligned} \mathrm{vol}_n((\varepsilon\mathcal{L} \cap (K - \varepsilon K_0)) + \varepsilon F) &= |\varepsilon\mathcal{L} \cap (K - \varepsilon K_0)| \mathrm{vol}_n(\varepsilon F) \\ &= \varepsilon^n \det(\mathcal{L}) |\varepsilon\mathcal{L} \cap (K - \varepsilon K_0)|, \quad \text{as needed.} \end{aligned}$$

For the furthermore, we assume that $K_0 \subseteq K - \mathbf{c}$ and that K_0 is symmetric. By symmetry of K_0, we have that $\pm F \subseteq K_0 \subseteq K - \mathbf{c}$. Using this, we modify the inclusions in Equation (10) to

$$\begin{aligned} K &\subseteq (\varepsilon\mathcal{L} \cap (K - \varepsilon F)) + \varepsilon F \subseteq (\varepsilon\mathcal{L} \cap (K + \varepsilon(K - \mathbf{t})) + \varepsilon F \\ &\subseteq (\varepsilon\mathcal{L} \cap ((1+\varepsilon)K - \varepsilon\mathbf{c})) + \varepsilon F \subseteq (\varepsilon\mathcal{L} \cap ((1+\varepsilon)K - \varepsilon\mathbf{c})) + \varepsilon(K - \mathbf{c}) \\ &\subseteq (1+\varepsilon)K - \varepsilon\mathbf{c} + \varepsilon(K - \mathbf{c}) = (1+2\varepsilon)K - 2\varepsilon\mathbf{c} \end{aligned} \tag{11}$$

From here, the same argument as above combined with the identity $\mathrm{vol}_n((1+2\varepsilon)K) = (1+2\varepsilon)^n \mathrm{vol}_n(K)$ completes the proof of Lemma. ◀

We now prove the main volume estimation result. We note that if the input body K is symmetric, the following algorithm will be able to directly use the thin covering lattice construction for symmetric bodies (Theorem 15) without passing through the construction of Theorem 26. We will use this fact within our algorithm for finding approximate KB points (Theorem 7).

Proof of Theorem 1 (Volume Estimation). Given a convex body $K \subseteq \mathbb{R}^n$, we wish to compute V such that

$$\mathrm{vol}_n(K) \leq V \leq (1+\varepsilon)^n \mathrm{vol}_n(K).$$

Compute the lattice Λ with basis B and point $\mathbf{c} \in K$ given by Theorem 26. This requires $2^{O(n)}$ time and poly(n) space. Via enumeration, we now compute the quantity

$$V = (\varepsilon/2)^n \det(\Lambda)\ |(\varepsilon/2)\Lambda \cap ((1+\varepsilon/2)K - (\varepsilon/2)\mathbf{c})|.$$

Since $K[\mathbf{c}] \subseteq K - \mathbf{c}$ and Λ is $K[\mathbf{c}]$-covering, by Lemma 27 we have that V satisfies the desired guarantees.

After rescaling, computing V can be done by enumerating $\Lambda \cap ((1+2/\varepsilon)K - \mathbf{c})$. Since $K[\mathbf{c}]$ is $2^{O(n)}$-SE with respect to B by Lemmas 16 and 19 this enumeration complexity is bounded by

$$\begin{aligned} 2^{O(n)} N((1+2/\varepsilon)K, K[\mathbf{c}]) &\leq 2^{O(n)} \frac{\mathrm{vol}_n((1+2/\varepsilon)K + K[\mathbf{c}])}{\mathrm{vol}_n(K[\mathbf{c}])} \\ &\leq 2^{O(n)} (2+2/\varepsilon)^n \frac{\mathrm{vol}_n(K)}{\mathrm{vol}_n(K[\mathbf{c}])} \\ &\leq 2^{O(n)} (1+1/\varepsilon)^n. \end{aligned}$$

Hence the total time complexity of the algorithm is bounded by $2^{O(n)}(1+1/\varepsilon)^n$ and the space complexity is poly(n) as needed. ◀

6.1 Computing an Approximate Kovner-Besicovitch Point

Proof of Theorem 7 (Computing Kovner-Besicovitch points).
Here the goal is to compute a point $\mathbf{c} \in K$ such that

$$\mathrm{vol}_n(K[\mathbf{c}])/\mathrm{vol}_n(K) \geq (1+\varepsilon)^{-n} \mathrm{Sym}_{kb}(K).$$

By first applying deterministic ellipsoidal rounding to K (Theorem 12), we may assume that

$$B_2^n \subseteq K \subseteq (n+1)n^{1/2} K.$$

We define the following sequence of bodies: $K_i = 2^i B_2^n \cap K$, for $0 \leq i \leq T$,
where $T = \lceil \log_2 (n+1)n^{1/2} \rceil$. By construction $K_0 = B_2^n$ and $K_T = K$.

Using the improvement procedure (Algorithm 2), the remainder of the algorithm is straightforward:

```
c_0 ← 0.
for $i \in 1$ to $T-1$ do
    $\mathbf{c}_i \leftarrow \mathrm{Improve}(K_i,\ \mathbf{c}_{i-1},\ 1/6,\ 1/2)$.
return Improve($K_T,\ \mathbf{c}_{T-1},\ 1/6,\ \varepsilon$).
```

```
Algorithm 2 Improve($A$, $\mathbf{x}$, $\alpha$, $\varepsilon$)
Require: Convex body $A \subseteq \mathbb{R}^n$, point $\mathbf{x} \in A$ satisfying $\mathrm{vol}_n(A[\mathbf{x}]) \geq \alpha^n \mathrm{vol}_n(A)$, $\varepsilon \leq 1/2$.
Ensure: A point $\mathbf{c} \in A$ satisfying $\mathrm{vol}_n(A[\mathbf{x}]) \geq (1+\varepsilon)^{-n}\mathrm{Sym}_{kb}(A)$.
1: $\varepsilon_0 \leftarrow \varepsilon/(6+3\varepsilon)$, $J \leftarrow \lfloor \log(1/\alpha)/\log(1/(1-\varepsilon_0)) \rfloor$.
2: $\mathbf{x}_0 \leftarrow \mathbf{x}$.
3: for $j \in 1$ to $J$ do
4:     Compute a covering $N$ of $1/2(A+\mathbf{x}_{j-1})$ by $(\varepsilon_0/2)A[\mathbf{x}_{j-1}]$ (Theorem 15).
       For each $\mathbf{y} \in N$, estimate the volume of $A[\mathbf{y}]$ to within $(1+\varepsilon_0/(1-\varepsilon_0))^n$ (Theorem 1).
       Set $\mathbf{x}_j$ to be the center in $N$ of maximum estimated volume.
5: return $\mathbf{x}_J$.
```

We first argue the correctness of the algorithm, and then continue with its runtime analysis.

Correctness: Assuming the correctness of Algorithm 2, we show that the remainder of the algorithm is correct. For the for loop on lines $2-3$, and line 4, we claim that at each call Improve(K_i, $\mathbf{c}_{i-1}$, $1/6$, $\dots$), $\mathbf{c}_{i-1}$ has KB value at least $(1/6)^n$ with respect to K_i, for $i \in [T]$. We prove this by induction on $i \in [T]$. Note that if $\mathbf{c}_{i-1}$ satisfies the condition, then by the guarantess on Improve, we have that

$$\frac{\mathrm{vol}_n(K_i[\mathbf{c}_i])}{\mathrm{vol}_n(K_i)} \geq (1+1/2)^{-n}\mathrm{Sym}_{kb}(K_i) \geq (1+1/2)^{-n}2^{-n} = 3^{-n}$$

From here, since $K_i \subseteq K_{i+1} \subseteq 2K_i$, we have that

$$\frac{\mathrm{vol}_n(K_{i+1}[\mathbf{c}_i])}{\mathrm{vol}_n(K_{i+1})} \geq \frac{\mathrm{vol}_n(K_i[\mathbf{c}_i])}{\mathrm{vol}_n(K_{i+1})} \geq 3^{-n}\frac{\mathrm{vol}_n(K_i)}{\mathrm{vol}_n(K_{i+1})} \geq 3^{-n}\ 2^{-n} = (1/6)^n,$$

as needed. For the base case $i=1$, we note that since $\mathbf{c}_0 = \mathbf{0}$ and $K_0 = B_2^n$, $\mathbf{0}$ has KB value 1 for K_0. By the above analysis, we get that $\mathbf{c}_0$ has KB value at least $2^{-n} \geq (1/6)^n$ for K_1, as needed.

Since on line 4 we call Improve(K_T, $\mathbf{c}_{T-1}$, $1/6$, ε) on a valid input and $K_T = K$, by the guarantees on Improve, the algorithm correctly outputs a $(1+\varepsilon)^{-n}$ KB point for K as needed.

We now show that Algorithm Improve is correct. Define

$$\nu(\mathbf{x}) = \left(\frac{\mathrm{vol}_n(A[\mathbf{x}])}{\mathrm{vol}_n(A)}\right)^{1/n}$$

to be the normalized KB value of a point $\mathbf{x} \in A$.

▶ Claim 29. ν is a concave function over A.

Proof. Take $\mathbf{x}, \mathbf{y} \in K$ and $\alpha \in [0,1]$. By convexity of A, note that

$$\begin{aligned}\alpha A[\mathbf{x}] + (1-\alpha)A[\mathbf{y}] &= \alpha(A-\mathbf{x}) \cap (\mathbf{x}-A) + (1-\alpha)(A-\mathbf{y}) \cap (\mathbf{y}-A)\\ &\subseteq (\alpha(A-\mathbf{x}) + (1-\alpha)(A-\mathbf{y})) \cap (\alpha(\mathbf{x}-A) + (1-\alpha)(\mathbf{y}-A))\\ &= (A - (\alpha\mathbf{x} + (1-\alpha)\mathbf{y})) \cap ((\alpha\mathbf{x} + (1-\alpha)\mathbf{y}) - A) = A[\alpha\mathbf{x} + (1-\alpha)\mathbf{y}]\end{aligned}$$

Using the above inclusion, followed by the Brunn-Minkowski inequality, we get that

$$\begin{aligned}\mathrm{vol}_n(A[\alpha\mathbf{x} + (1-\alpha)\mathbf{y}])^{1/n} &\geq \mathrm{vol}_n(\alpha A[\mathbf{x}] + (1-\alpha)A[\mathbf{y}])^{1/n}\\ &\geq \alpha\mathrm{vol}_n(A[\mathbf{x}])^{1/n} + (1-\alpha)\mathrm{vol}_n(A[\mathbf{y}])^{1/n}.\end{aligned}$$

The claim follows by dividing through by $\mathrm{vol}_n(A)^{1/n}$. ◀

Let $\mathbf{x}^*$ denote the center of maximum KB value, i.e. $\mathbf{x}^* = \arg\max_{\mathbf{x}\in A} \nu(\mathbf{x})$, and let $\gamma = \nu(\mathbf{x}^*)$. Note that for correctness, we need simply show that at the last iteration J, $\nu(\mathbf{x}_J) \geq \gamma/(1+\varepsilon)$. The following claim tracks the progress in ν.

▶ Claim 30. For $i \geq 1$, $\nu(\mathbf{x}_i) \geq 1/2(\gamma + \nu(\mathbf{x}_{i-1}))(1-\varepsilon_0)^2$.

Proof. By translating A, we may assume that $\mathbf{x}_{i-1} = \mathbf{0}$. Let $\mathbf{z} = 1/2\mathbf{x}^*$. By construction $\mathbf{z} \in 1/2A$, hence by the properties of the net N, there exists $\mathbf{y} \in N$ such that $\mathbf{v} = \mathbf{y} - \mathbf{z}$ satisfies $\|\pm\mathbf{v}\|_{A[\mathbf{0}]} \leq \varepsilon_0/2$. By the triangle inequality, note that

$$\|\mathbf{z} + 1/\varepsilon_0\mathbf{v}\|_A \leq \|\mathbf{z}\|_A + 1/\varepsilon_0\|\mathbf{v}\|_A \leq 1/2 + 1/\varepsilon_0\|\mathbf{v}\|_{A[\mathbf{0}]} \leq 1/2 + 1/\varepsilon_0(\varepsilon_0/2) \leq 1.$$

Hence $\mathbf{z} + 1/\varepsilon_0\mathbf{v} \in A$. Since $\mathbf{y} = \mathbf{z} + \mathbf{v} = (1-\varepsilon_0)\mathbf{z} + \varepsilon_0(\mathbf{z} + 1/\varepsilon_0\mathbf{v})$, by concavity of ν over A

$$\begin{aligned}\nu(\mathbf{y}) &\geq (1-\varepsilon_0)\nu(\mathbf{z}) + \varepsilon_0\nu(\mathbf{z} + 1/\varepsilon_0\mathbf{v}) \geq (1-\varepsilon_0)\nu(\mathbf{z})\\ &= (1-\varepsilon_0)\nu((1/2)\mathbf{0} + (1/2)\mathbf{x}^*) \geq (1-\varepsilon_0)((1/2)\nu(\mathbf{0}) + (1/2)\nu(\mathbf{x}^*))\\ &= 1/2(\nu(\mathbf{x}_{i-1}) + \gamma)(1-\varepsilon_0) \qquad (12)\end{aligned}$$

For each $\mathbf{y} \in N$, we note that volume estimation algorithm computes a number $V_\mathbf{y}$ such that

$$\mathrm{vol}_n(A[\mathbf{y}]) \leq V_\mathbf{y} \leq (1 + \varepsilon_0/(1-\varepsilon_0))^n \mathrm{vol}_n(A[\mathbf{y}]) = 1/(1-\varepsilon_0)^n \mathrm{vol}_n(A[\mathbf{y}]).$$

By Equation (12), this implies that for the chosen $\mathbf{x}_i$, we must have

$$V_{\mathbf{x}_i} \geq \mathrm{vol}_n(A)\left(1/2(\nu(\mathbf{x}_{i-1}) + \gamma)(1-\varepsilon_0)\right)^n.$$

By approximation the guarantee, this implies that $\nu(\mathbf{x}_i) \geq 1/2(\nu(\mathbf{x}_{i-1}) + \gamma)(1-\varepsilon_0)^2$, as needed. ◀

The following claim completes the proof of correctness:

▶ Claim 31. At the last iteration $J = \lfloor \log(1/\alpha)/\log(1/(1-\varepsilon_0)) \rfloor$, $\nu(\mathbf{x}_J) \geq \gamma/(1+\varepsilon)$.

Proof. Let $a_0 = \alpha$, and let $a_i = 1/2(a_{i-1} + \gamma)(1-\varepsilon_0)^2$ for $i \geq 1$. Since the function $a \to 1/2(a+\gamma)(1-\varepsilon_0)^2$ is monotone in a, by Claim 30 we have that $\nu(\mathbf{x}_i) \geq a_i$ for all i. It therefore suffices to prove that $a_J \geq \gamma/(1+\varepsilon)$. We first note that $\varepsilon_0 = \varepsilon/(6+3\varepsilon)$ is set to satisfy the equation $(1-3\varepsilon_0)/(1+3\varepsilon_0) = 1/(1+\varepsilon)$. If $a_{i-1} \leq \gamma/(1+\varepsilon) = \gamma(1-3\varepsilon_0)/(1+3\varepsilon_0)$, note that

$$\begin{aligned}a_i(1-\varepsilon_0) &= 1/2(a_{i-1} + \gamma)(1-\varepsilon_0)^3 \geq 1/2(a_{i-1} + \gamma)(1-3\varepsilon_0)\\ &= 1/2(a_{i-1}(1-3\varepsilon_0) + \gamma(1-3\varepsilon_0)) \geq 1/2(a_{i-1}(1-3\varepsilon_0) + a_{i-1}(1+3\varepsilon_0)) = a_{i-1}.\end{aligned}$$

In particular, we get $a_i \geq a_{i-1}/(1-\varepsilon_0)$. Furthermore, if $a_{i-1} \geq \gamma/(1+\varepsilon)$ by monotonicity $a_i \geq \gamma/(1+\varepsilon)$. Therefore, we need only show that the a_i goes above $\gamma/(1+\varepsilon)$ at some time $i \leq J$. Let t be the first step where $a_t \geq \gamma/(1+\varepsilon)$. By the above relations, we must have that

$$1 \geq \nu(x_t) \geq a_t \geq a_{t-1}/(1-\varepsilon_0) \geq a_0/(1-\varepsilon_0)^t = \alpha/(1-\varepsilon_0)^t.$$

Solving for t, we get that $t \leq \log(1/\alpha)/\log(1/(1-\varepsilon_0))$, and hence $t \leq J$ as needed. ◀

Runtime Analysis: We first apply ellipsoidal rounding to K (Theorem 12), this can be done in polynomial time. Next, we run the Improve procedure $O(\log n)$ times, so it suffices to bound the runtime of one call. Since without loss of generality we can assume $\varepsilon \leq 1/2$, it is clear that the last call to procedure Improve, that is Improve$(K_T, \mathbf{c}_{T-1}, 1/6, \varepsilon)$, dominates the complexity of the algorithm.

On the last call to Improve, we have $A = K_T$, $\alpha = 1/6$, $\varepsilon \leq 1/2$, and $\varepsilon_0 = \varepsilon/(6+3\varepsilon_0) \geq \varepsilon/8$. We execute the main loop

$$\log(1/\alpha)/\log(1/(1-\varepsilon_0)) \leq \log(1/\alpha)/\log(1+\varepsilon_0) \leq \log(1/\alpha)/\log(1+\varepsilon/8) = O(1/\varepsilon) \text{ times.}$$

Let $\gamma = \mathrm{Sym}_{kb}(A)^{1/n}$. Note that $\gamma/(1+\varepsilon) \geq (1/2)(2/3) = 1/3 \geq \alpha$. Hence by Claim 31 at each iteration of the for loop we have that $\mathrm{vol}_n(A[\mathbf{x}_{j-1}])/\mathrm{vol}_n(A) \geq 6^{-n}$.

At iteration j, we first compute an covering N of $1/2(A + \mathbf{x}_{j-1})$ by $(\varepsilon_0/2)A[\mathbf{x}_{j-1}]$ using Theorem 15. Since $\varepsilon_0/2 \geq \varepsilon/16$, this takes time at most

$$\begin{aligned} 2^{O(n)} N(1/2A, (\varepsilon/16)A[\mathbf{x}_{j-1}]) &= 2^{O(n)} \frac{\mathrm{vol}_n(1/2A + (\varepsilon/16)A[\mathbf{x}_{j-1}])}{\mathrm{vol}_n((\varepsilon/16)A[\mathbf{x}_{j-1}]} \\ &= 2^{O(n)} \left(\frac{1/2 + \varepsilon/16}{\varepsilon/16}\right)^n \frac{\mathrm{vol}_n(A)}{\mathrm{vol}_n(A[\mathbf{x}_{j-1}])} \\ &= 2^{O(n)}(1+8/\varepsilon)^n 6^n = 2^{O(n)}(1+1/\varepsilon)^n \end{aligned}$$

and poly(n) space. For each $\mathbf{y} \in N$, we compute a number V_y satisfying

$$\mathrm{vol}_n(A[\mathbf{y}]) \leq V_y \leq (1 + \varepsilon_0/(1-\varepsilon_0))^n \mathrm{vol}_n(A[\mathbf{y}])$$

where $\varepsilon_0/(1-\varepsilon_0) \geq 2\varepsilon_0 \geq \varepsilon/4$. Since $A[\mathbf{y}]$ is symmetric, we note that this can be done using Theorem 1, using only the thin lattice construction for symmetric bodies (Theorem 15). Hence this can be done in $2^{O(n)}(1+4/\varepsilon)^n = 2^{O(n)}(1+1/\varepsilon)^n$ time using poly(n) space. Putting it all together, the for loop can be executed in $2^{O(n)}(1/\varepsilon)(1+1/\varepsilon)^{2n} = 2^{O(n)}(1+1/\varepsilon)^{2n+1}$ time using poly(n) space. The desired complexity bound for the algorithm follows. ◀

Acknowledgments. The author would like to thank Santosh Vempala and Oded Regev for useful conversations related to this paper.

References

1 N. Alon, A. Schraibman, T. Lee, , and S. Vempala. The approximate rank of a matrix and its algorithmic applications. In *STOC*, 2013.

2 Alexandr Andoni and Piotr Indyk. Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 459–468, 2006.

3 A. Becker, N. Gama, and A. Joux. Solving shortest and closest vector problems: The decomposition approach. Cryptology Eprint. Report 2013/685, 2013.

4 G.J. Butler. Simultaneous packing and covering in euclidean space. *Proceedings of the London Mathematical Society*, 25(3):721–735, 1972.

5 Daniel Dadush. *Integer Programming, Lattice Algorithms, and Deterministic Volume Estimation.* PhD thesis, Georgia Institute of Technology, 2012.

6 Daniel Dadush and Gabor Kun. Lattice sparsification and the approximate closest vector problem. In *SODA*, 2013.

7 Daniel Dadush, Chris Peikert, and Santosh Vempala. Enumerative lattice algorithms in any norm via m-ellipsoid coverings. In *FOCS*, 2011.

8 Daniel Dadush and Santosh S. Vempala. Near-optimal deterministic algorithms for volume computation via m-ellipsoids. *Proceedings of the National Academy of Sciences*, 2013.

9 M.E. Dyer, A.M. Frieze, and R. Kannan. A random polynomial-time algorithm for approximating the volume of convex bodies. *J. ACM*, 38(1):1–17, 1991.

10 Uri Erez, Simon Litsyn, and Ram Zamir. Lattices which are good for (almost) everything. *Information Theory, IEEE Transactions on*, 51(10):3401–3416, 2005.

11 Z. Füredi and I. Bárány. Computing the volume is difficult. In *STOC '86: Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 442–447, New York, NY, USA, 1986. ACM.

12 Z. Füredi and I. Bárány. Approximation of the sphere by polytopes having few vertices. *Proceedings of the AMS*, 102(3), 1988.

13 Daniel Goldstein and Andrew Mayer. On the equidistribution of hecke points. *Forum Mathematicum*, 15(2):165–189, 2003.

14 M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization*. Springer-Verlag, 1988.

15 B. Grünbaum. Measures of symmetry for convex sets. In *Proceedings of the 7th Symposium in Pure Mathematics of the American Mathematical Society, Symposium on Convexity*, pages 233–270, 1961.

16 Venkatesan Guruswami, Daniele Micciancio, and Oded Regev. The complexity of the covering radius problem. *Computational Complexity*, 14(2):90–121, 2005. Preliminary version in CCC 2004.

17 Guillaume Hanrot and Damien Stehlé. Improved analysis of kannan's shortest lattice vector algorithm. In *Proceedings of the 27th annual international cryptology conference on Advances in cryptology*, CRYPTO'07, pages 170–186, Berlin, Heidelberg, 2007. Springer-Verlag.

18 Ishay Haviv and Oded Regev. Hardness of the covering radius problem on lattices. In *IEEE Conference on Computational Complexity*, pages 145–158, 2006.

19 Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *J. ACM*, 52(5):789–808, 2005. Preliminary version in FOCS 2004.

20 D. Micciancio and P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. *SIAM Journal on Computing*, 42(3):1364–1391, 2013. Preliminary version in STOC 2010.

21 V.D. Milman. Inegalites de brunn-minkowski inverse et applications at la theorie locales des espaces normes. *C. R. Acad. Sci. Paris*, 302(1):25–28, 1986.

22 V.D. Milman and A. Pajor. Entropy and asymptotic geometry of non-symmetric convex bodies. *Advances in Mathematics*, 152(2):314 – 335, 2000.

23 C. A. Rogers. A note on coverings and packings. *Journal of the London Mathematical Society*, s1-25(4):327–331, 1950.

24 C. A. Rogers. Lattice coverings of space: The minkowski-hlawka theorem. *Proceedings of the London Mathematical Society*, s3-8(3):447–465, 1958.

25 C. A. Rogers and C. Zong. Covering convex bodies by translates of convex bodies. *Mathematika*, 44:215–218, 6 1997.

26 C.A. Rogers. Lattice coverings of space. *Mathematika*, 6:33–39, 6 1959.

27 D. B. Yudin and A. S. Nemirovski. Evaluation of the information complexity of mathematical programming problems (in russian). *Ekonomika i Matematicheskie Metody*, 13(2):3–45, 1976.