Discrete & Computational Geometry (2022) 67:1191–1210
https://doi.org/10.1007/s00454-022-00392-x

Covering Convex Bodies and the Closest Vector Problem

Márton Naszódi[1] · **Moritz Venzin**[2]

Received: 6 June 2020 / Revised: 1 November 2021 / Accepted: 14 November 2021 /
Published online: 1 May 2022
© The Author(s) 2022

Abstract

We present algorithms for the $(1+\epsilon)$-approximate version of the closest vector problem for certain norms. The currently fastest algorithm (Dadush and Kun 2016) for general norms in dimension n has running time of $2^{O(n)}(1/\epsilon)^n$. We improve this substantially in the following two cases. First, for ℓ_p-norms with $p > 2$ (resp. $p \in [1, 2]$) fixed, we present an algorithm with a running time of $2^{O(n)}(1+1/\epsilon)^{n/2}$ (resp. $2^{O(n)}(1+1/\epsilon)^{n/p}$). This result is based on a geometric covering problem, that was introduced in the context of CVP by Eisenbrand et al.: How many convex bodies are needed to cover the ball of the norm such that, if scaled by factor 2 around their centroids, each one is contained in the $(1+\epsilon)$-scaled homothet of the norm ball? We provide upper bounds for this $(2, \epsilon)$-*covering number* by exploiting the *modulus of smoothness* of the ℓ_p-balls. Applying a covering scheme, we can boost any 2-approximation algorithm for CVP to a $(1+\epsilon)$-approximation algorithm with the improved run time, either using a straightforward sampling routine or using the deterministic algorithm of Dadush for the construction of an epsilon net. Second, we consider polyhedral and zonotopal norms. For centrally symmetric polytopes (resp. zonotopes) in $\mathbb{R}^n$ with $O(n)$ facets (resp. generated by $O(n)$ line segments), we provide a deterministic $O(\log_2(2+1/\epsilon))^{O(n)}$ time algorithm. This generalizes the result of Eisenbrand et al. which applies to the ℓ_∞-norm. Finally, we establish a connection between the *modulus of smoothness* and *lattice sparsification*. As a consequence, using the enumeration and sparsification tools developped by Dadush, Kun, Peikert, and Vempala, we present a simple alternative to the boosting procedure with the same time and space requirement for ℓ_p norms. This connection might be of independent interest.

Editor in Charge: Kenneth Clarkson

Márton Naszódi
marton.naszodi@math.elte.hu

Moritz Venzin
moritz.venzin@epfl.ch

[1] MTA-ELTE Lendület Combinatorial Geometry Research Group; Department of Geometry, Loránd Eötvös University, Budapest, Hungary

[2] Institute for Mathematics, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland

Keywords Closest vector problem · Modulus of smoothness · Lattice sparsification · Convex body in d-dimensional space · Approximation

Mathematics Subject Classification 90C10 · 52C07 · 68W25 · 68Q25 · 68U05

1 Introduction

The *closest vector problem* (CVP) is an important algorithmic problem in the geometry of numbers. Given a rational lattice $\Lambda(A) = \{Ax : x \in \mathbb{Z}^n\}$, with $A \in \mathbb{Q}^{n\times n}$ and a target vector $t \in \mathbb{Q}^n$, the task is to find a close vector in $\mathcal{L}$ to t with respect to a given norm. Specifically, given some norm $\|\cdot\|_K$, a $(1+\epsilon)$-approximation to the closest vector problem, $(1+\epsilon)$-CVP$_K$, is to find a lattice vector whose distance to the target vector is at most $1+\epsilon$ times the minimal distance of the target to the lattice. Whenever K is the unit ball of the space ℓ_p^n for some $1 \le p \le \infty$, we denote the problem by $(1+\epsilon)$-CVP$_p$. The closely related *shortest vector problem* (SVP) asks for the shortest non-zero lattice vector in a given lattice. It was shown that CVP is NP-hard for any ℓ_p norm [18] and even NP-hard to approximate up to almost polynomial factors, [7, 15].

The first algorithm to solve integer programming and, in particular, exact CVP$_\infty$ was given by Lenstra [22] with a running time of $2^{O(n^2)}$. His algorithm connects the two fields of geometry of numbers and integer programming. Kannan [21] presented an algorithm for exact CVP (and SVP) with a running time of $n^{O(n)}$ and polynomial space. Subsequent works improve on the constant in the exponent but improving the running time of $n^{O(n)}$ to single exponential in n remained an open problem. After Kannan's result, it took almost 15 years until Ajtai, Kumar, and Sivakumar presented a randomized algorithm for SVP$_2$ with time and space $2^{O(n)}$ and $(1+\epsilon)$-CVP$_2$ with time and space $2^{(1+1/\epsilon)n}$ [5, 6]. Subsequently, Blömer and Naewe [9] extended the randomized sieving algorithm of Ajtai et al. to solve $(1+\epsilon)$-CVP$_p$ for all p in time $O(1+1/\epsilon)^{2n}$ and space $O(1+1/\epsilon)^n$, see also [3, 27]. For $p=\infty$, Eisenbrand et al. [17] then boosted the algorithm of Blömer and Naewe by showing that $2^{O(n)}\log(2+1/\epsilon)^n$ calls to a 2-CVP$_\infty$ solver suffice to solve $(1+\epsilon)$-CVP$_\infty$ implying a running time of $O(\log(2+1/\epsilon))^n$ and space requirement $2^{O(n)}$. Dadush [11] extended the Ajtai–Kumar–Sivakumar sieve to solve $(1+\epsilon)$-CVP in any norm with a running time of $O(1+1/\epsilon)^{2n}$ and space $O(1+1/\epsilon)^n$. The first single exponential deterministic and exact solver for CVP$_2$ was presented by Micciancio and Voulgaris [25]. Their algorithm needs to store the up to $2(2^n-1)$ facets of the Voronoi cell of the lattice. Recently in [20], Hunkenschröder, Reuland, and Schymura show that this can be avoided and do a first step towards a polynomial space algorithm for CVP$_2$. The currently fastest algorithms for exact CVP$_2$ and SVP$_2$ use discrete Gaussian sampling and need time and space $2^{n+o(n)}$, see [2, 4]. Despite this progress for the ℓ_2 norm, for general norms, only the randomized sieving approach seemed available to solve CVP. Using the elegant idea of lattice sparsification, Dadush and Kun [13] presented a deterministic algorithm solving $(1+\epsilon)$-CVP for any norm in time $2^{O(n)}(1+1/\epsilon)^n$ and with space requirement 2^n poly(n)—reducing the dependence on $1/\epsilon$ in the running time and

removing the dependence on $1/\epsilon$ in the space requirement altogether compared with earlier randomized sieving approaches.

Our Contribution

In order to devise more efficient algorithms for CVP_K (and, in particular CVP_p), we study the problem of how many arbitrarily chosen convex bodies are needed to cover some given convex body K, such that when scaled around their respective centroids by a factor 2, each one is contained in $(1+\epsilon)K$. We refer to such a covering as a $(2,\epsilon)$-covering *for* K, and the smallest size of such a covering as the $(2,\epsilon)$-covering *number of* K.

A key quantity, well studied in the theory of Banach spaces, is the *modulus of smoothness* of a convex body K, which expresses how well the boundary of K is approximated locally by support hyperplanes, see Definition 3.1.

In this paper the *big oh notation*, $O(\cdot)$, stands for a universal multiplicative constant independent of every other quantity. In particular, we make the dependence on ϵ and n explicit.

- By a standard argument, we show that for any centrally symmetric convex body, a $(2,\epsilon)$-covering is always possible using $2^{O(n)}(1+1/\epsilon)^n$ convex bodies. Then, in Theorem 2.7, we establish a *lower bound* of $2^{-O(n)}(1+1/\epsilon)^{n/2}$ for the Euclidean unit ball.
- For centrally symmetric polytopes (resp. zonotopes) with m *facets* (resp. m generating line segments), we provide an explicit $(2,\epsilon)$-covering using at most $O(\log(2+1/\epsilon))^m$ convex bodies, see Propositions 2.5 and 2.6. These are relatively straightforward generalizations of the method of [17] where the cube is considered.
- Our first main result is Theorem 3.2, where it is shown that a bound on the *modulus of smoothness* of K yields a *bound on its* $(2,\epsilon)$-covering number. More specifically, if K has modulus of smoothness bounded above by $C\tau^q$, then we find a $(2,\epsilon)$-covering of K using $C^{O(n)}(1+1/\epsilon)^{n/q}$ convex bodies. In particular, we obtain a $(2,\epsilon)$-covering for ℓ_p balls using $2^{O(n)}(1+1/\epsilon)^{n/2}$ for $p\geq 2$ and $2^{O(n)}(1+1/\epsilon)^{n/p}$ for $p\in[1,2]$, matching the lower bound (Theorem 2.7) for the Euclidean unit ball.
- Our second main result is Theorem 4.2, which shows how a good algorithmic bound on the $(2,\epsilon)$-covering number yields an *efficient* $(1+\epsilon)$-CVP algorithm. In particular, for norms induced by centrally symmetric polytopes (resp. zonotopes) with m facets (resp. generating line segments), the above explicit $(2,\epsilon)$-covering boosts any 2-CVP solver for general norms to yield a deterministic $(1+\epsilon)$-CVP algorithm. This yields an algorithm with running time $O(\log(2+1/\epsilon))^m$ and $2^n\,\mathrm{poly}(n)$ space, see Corollary 4.3.
- For a centrally symmetric convex body K with a certain modulus of smoothness, to avoid the space requirement to depend on the number of convex bodies in the $(2,\epsilon)$-covering of K, we show how to *generate a local* $(2,\epsilon)$-covering on the fly. This yields a simple, randomized $(1+\epsilon)$-CVP_p algorithm for $1\leq p\leq\infty$ with a running time of $O(1+1/\epsilon)^{n/2}$ for $p\geq 2$, and $2^{O(n)}(1+1/\epsilon)^{n/p}$ for

$p \in [1, 2]$, using $2^n \operatorname{poly}(n)$ space. Alternatively, we may use an algorithm of Dadush [12] to explicitly enumerate the covering using polynomial space only, derandomizing the algorithm. This is our third main result, see Theorem 4.6. Compared to earlier results in the literature, for instance [9, 13], we improve on the previous best running times of $O(1 + 1/\epsilon)^n$ for ℓ_p norms. Furthermore, our approach immediately generalizes to non-symmetric norms and we obtain a simple CVP solver for γ-symmetric norms with running time $(1 + 1/(\gamma\epsilon))^n$ and space requirement $2^{O(n)}$ based on the Ajtai–Kumar–Sivakumar sieve, see Remark 4.7. This almost matches the performance of Dadush and Kun's algorithm.

- Finally, we establish a connection between *lattice sparsification* and the *modulus of smoothness*, see Lemma 5.2. While the boosting approach described in Sects. 3 and 4 is conceptually very simple and general, and it does not require any knowledge about the approximate CVP solver used, the proofs are quite technical. We will show that we can tweak the algorithm described by Dadush and Kun in [13] using a simple observation based on the modulus of smoothness in order to obtain the same improved running time for CVP for norms with a certain modulus of smoothness, in particular CVP_p. With this new approach, we restrict ourselves to using lattice sparsification and enumeration and we lose the possibility to use an arbitrary constant approximation CVP-solver. Considering the low space dependency of lattice sparsification and enumeration among all known (single exponential) approximate CVP solvers and the simplicity of our approach, this might not be a big loss.

It should be noted here that a seemingly similar (with respect to ϵ) bound on the $(2, \epsilon)$-covering number follows from recent work of Arya et al. [8] (see also [1]). Using Macbeath regions, they approximate *any* convex body with a polytope with at most $n^{O(n)}\epsilon^{-(n-1)/2}$ faces of all dimensions in total, provided that $\epsilon \ll n^{-n}$. It is then straightforward to show that this can be turned into a $(2, \epsilon)$-covering using roughly $n^{O(n)}\epsilon^{-(n-1)/2}$ convex bodies. Unfortunately, for the purpose of designing approximation algorithms for lattice problems, this is of little use, as already the $n^{O(n)}$ factor is prohibitively high considering that the exact solver of Kannan runs in $n^{O(n)}$ time. Moreover, any approximation based on Macbeath regions requires $\epsilon \ll n^{-n}$, which is too strong a restriction for integer programming related applications. Nonetheless, their result shows that for ϵ sufficiently small, any convex body admits a $(2, \epsilon)$-covering using $O(1+1/\epsilon)^{n/2}$ convex bodies and raises the question whether the restriction on ϵ can be removed in general. As mentioned above, in the present work, the dimension n is not considered constant, and dependence on it is made explicit everywhere.

The structure of the paper is the following. In Sect. 2, we list basic facts about $(2, \epsilon)$-coverings and prove upper bounds on the $(2, \epsilon)$-covering number of symmetric polytopes and zonotopes (Propositions 2.5 and 2.6). In Theorem 2.7, a lower bound on the covering number of the Euclidean ball is presented. In Sect. 3, it is shown how a bound on the modulus of smoothness yields a bound on the $(2, \epsilon)$-covering number. In Sect. 4, we apply our covering bounds to obtain efficient algorithms for $(1 + \epsilon)$-CVP. Finally, Sect. 5 contains Theorem 5.5, which presents another $(1 + \epsilon)$-CVP

solver for bodies with a well bounded modulus of convexity, based on efficient lattice sparsification and lattice enumeration algorithms.

The scalar product of two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{R}^n$ is denoted by $\langle x, y\rangle = x_1 y_1 + \cdots + x_n y_n$. For a positive integer k, we use the notation $[k] = \{1, \ldots, k\}$.

2 $(2, \epsilon)$-Coverings

We denote the *homothetic copy* of a convex body Q by factor $\lambda \in \mathbb{R}$ with respect to its *centroid* (also called, center of mass) $c(Q)$ by $\lambda \odot Q = \lambda(Q - c(Q)) + c(Q)$. The following notion is central to our study.

Definition 2.1 ($(2, \epsilon)$-*covering*) For a convex body $K \subseteq \mathbb{R}^n$, a sequence of convex bodies $\{Q_i\}_{i=1}^N$ is a $(2, \epsilon)$-covering if

$$K \subseteq \bigcup_{i=1}^{N} Q_i \subseteq \bigcup_{i=1}^{N} 2 \odot Q_i \subseteq (1+\epsilon)K.$$

We note that we have fixed the factor 2 for concreteness, we could replace 2 by any other constant. For this reason we will assume $\epsilon \in (0, 1)$.

The following three lemmas follow directly from standard packing arguments, we include a proof in the appendix.

Lemma 2.2 *Any origin symmetric convex body $K \subseteq \mathbb{R}^n$ admits a $(2, \epsilon)$-covering by at most $(5/\epsilon)^n$ homothetic copies of K.*

We also note that it is sufficient to consider coverings by centrally symmetric convex bodies only.

Lemma 2.3 *Let K be a convex body in $\mathbb{R}^n$ that admits a $(2, \epsilon)$-covering consisting of N convex bodies. Then, K admits a $(2, \epsilon)$-covering consisting of $10^n N$ centrally symmetric convex bodies.*

Lemma 2.4 *Any convex body $K \subseteq \mathbb{R}^n$ with 0 as its centroid has a $(2, \epsilon)$-covering by at most $N = (10/\epsilon)^n$ translated copies of $(\epsilon/2)(K \cap -K)$.*

In the particular case of the cube, in [17], Eisenbrand et al. found a $(2, \epsilon)$-covering that requires $(1 + 2\log_2(1 + 1/\epsilon))^n$ parallelepipeds. The following two propositions show that their method generally works for any zonotope or any centrally symmetric polytope.

A *zonotope* is the Minkowski sum of finitely many line segments, $\mathcal{Z} = \left\{\sum_{i=1}^m \lambda_i b_i : \lambda_i \in [-1, 1],\ 1 \le i \le m\right\} = \sum_{i=1}^m [-b_i, b_i]$. We refer to the b_i as the *generators* of $\mathcal{Z}$. If $m = n$ and $b_i = e_i$, $i = 1, \ldots, n$, then this zonotope is the unit cube. A zonotope with m generators can have up to $2\binom{m}{n-1}$ facets; when no n of the generators are linearly dependent, this bound is attained, as is not difficult to see.

In the following two propositions, we give upper bounds for the $(2, \epsilon)$-covering of zonotopes with a bounded number of generators and for polytopes with a bounded number of facets. We include these proof in the appendix.

Proposition 2.5 ($(2,\epsilon)$-covering of a zonotope by smaller zonotopes) *Let* $\mathcal{Z} = \left\{\sum_{i=1}^m \lambda_i b_i : \lambda_i \in [-1,1],\ i \in [m]\right\}$ *be a zonotope with m generators,* $b_1, \ldots, b_m \in \mathbb{R}^n$. *For any* $\epsilon > 0$, *there exists a* $(2,\epsilon)$*-covering of* $\mathcal{Z}$ *using* $(1 + 2\log_2(1 + 1/\epsilon))^m$ *zonotopes.*

Proposition 2.6 ($(2,\epsilon)$-covering centrally symmetric polytopes with few facets) *Let* $P = \{x \in \mathbb{R}^n : |a_i^T x| \le b_i,\ i \in [m]\}$ *be an origin symmetric polytope. There is a* $(2,\epsilon)$*-covering of* P *using at most* $2^m(\log_{4/3}(1/\epsilon) + 1)^m$ *centrally symmetric convex bodies.*

Finally, we prove a lower bound on the $(2,\epsilon)$-covering number of the Euclidean unit ball B_2^n which, by Corollary 3.4, is sharp, up to a logarithmic factor.

Theorem 2.7 *For any* $\epsilon \in (0, 1/2)$, *any* $(2,\epsilon)$*-covering of the Euclidean unit ball* B_2^n *consists of at least* $2^{-O(n)}(1/\epsilon)^{(n-1)/2}$ *convex bodies.*

Proof Let $\{Q_i\}_{i=1}^N$ be a $(2,\epsilon)$-covering of B_2^n with respective centroids c_i. Let $p \in \mathbb{S}^{n-1}$ and let c be the centroid of a Q_i such that $p \in Q_i$. First, we show that $\langle p, c\rangle \ge 1 - \epsilon$, that is, Q_i is contained in a small solid cap. Suppose by contradiction that $\langle p, c\rangle < 1-\epsilon$. By the definition of a $(2,\epsilon)$-covering we need that $\|p+(p-c)\| \le 1+\epsilon$. This implies $\langle p, p + (p - c)\rangle \le 1 + \epsilon$ and we obtain the following contradiction:

$$\langle p, p + (p - c)\rangle = 2\langle p, p\rangle + \langle p, -c\rangle > 2 + \epsilon - 1 = 1 + \epsilon.$$

Also by the definition of a $(2,\epsilon)$-covering, we need $\|c\| \le 1 + \epsilon$. Thus, we can show $\|p - c\|$ is small:

$$\langle p - c, p - c\rangle = \langle p, p\rangle + \langle c, c\rangle + 2\langle p, -c\rangle \le 1 + (1 + \epsilon)^2 + 2(\epsilon - 1) \le 5\epsilon.$$

Thus, for every Q_i, $Q_i \cap \mathbb{S}^{n-1}$ is contained in a cap of radius $\sqrt{5\epsilon}$. Denoting by $\sigma(\cdot)$ the uniform probability measure on the sphere, this means that for any convex body Q_i in the $(2,\epsilon)$-covering, $\sigma(Q_i) \le 2^{O(n)}\epsilon^{(n-1)/2}$ (cf. [10, Lem. 3.1]). Since a $(2,\epsilon)$-covering of B_2^n needs to cover all of $\mathbb{S}^{n-1}$, we obtain the desired lower bound on N. □

3 $(2, \epsilon)$-Coverings via Modulus of Smoothness

For a convex body K, we will consider its *gauge function* $\|\cdot\|_K$, defined by $\|x\|_K = \inf\{s : x \in sK\}$. If K is origin symmetric, then $\|\cdot\|_K$ defines a norm.

Definition 3.1 (*modulus of smoothness*) The *modulus of smoothness* of an origin-symmetric convex body K, $\rho_K(\tau)\colon (0,1) \to (0,1)$, is defined by

$$\rho_K(\tau) = \frac{1}{2} \sup_{\|x\|_K = \|y\|_K = 1} (\|x + \tau y\|_K + \|x - \tau y\|_K - 2).$$

We remark first that any origin symmetric body K has modulus of smoothness $\rho_K(\tau) \leq \tau$, this follows from the subadditivity of the norm. The modulus of smoothness of K measures how well K can be locally approximated by hyperplanes: If $\|x\|_K = 1$ and $\|\tau y\|_K = \tau$ and both $x + y$ and $x - y$ lie on a support hyperplane of K at x, then both $\|x + \tau y\|_K, \|x - \tau y\|_K \geq 1$, but we also have the upper bound of

$$\|x \pm \tau y\|_K \leq 1 + 2\rho_K(\tau).$$

If $\rho_K(\tau)$ can be bounded by a polynomial of degree higher than 1, say τ^2, then $x \pm \tau y$ are closer to the boundary of K compared to what subadditivity, $\|x \pm \tau y\|_K \leq \|x\|_K + \|\tau y\|_K$, alone yields. Still assuming $\rho_K(\tau) \leq \tau^2$ and letting $\epsilon \in (0, 1)$, this means that all points $y \in K$ with $\|x - y\| \leq \sqrt{\epsilon}$ are approximated up to an additive ϵ by the tangential hyperplane at x. This behaviour of some norms is exploited in the next theorem.

Theorem 3.2 *Let $K \subseteq \mathbb{R}^n$ be an origin symmetric convex body, and $\epsilon \in (0, 1)$. Assume that the modulus of smoothness of K is bounded by*

$$\rho_K(\tau) \leq C\tau^q$$

with some constants $C, q > 1$. Then, there exists a $(2, \epsilon)$-covering of K consisting of

$$2^{O(n)} \log\left(1 + \frac{1}{\epsilon}\right)\left(\frac{C}{\epsilon}\right)^{n/q} + O(C)^{n/(q-1)}$$

centrally symmetric convex bodies. The encoding length of each such body is a polynomial in the encoding length of K.

Proof Set $\delta = (\epsilon/C)^{1/q}/4$. We may assume that $\epsilon \leq (1/(8C^{1/q}))^{q/(q-1)}$, in which case $\delta - \epsilon \geq \delta/2$. Otherwise, we may apply Lemma 2.2 and obtain a $(2, \epsilon)$-covering of K consisting of $O(C)^{n/(q-1)}$ bodies. We denote $\|\cdot\|_K$ by $\|\cdot\|$.

We first describe a $(2, 2\epsilon)$-covering of K only in the neighborhood of a point and then, using a packing argument, we extend this construction to obtain a $(2, 2\epsilon)$-covering for all of K.

Fix a point p on the boundary of K that is, $\|p\| = 1$. Denote by T_p a supporting hyperplane of K at p. Let B_p be the intersection of T_p with $p + \delta K$, i.e., $B_p := T_p \cap \{x : \|x - p\| \leq \delta\}$.

First, we show that

$$\mathrm{bd(K)} \cap (p + (\delta - \epsilon)K) \subseteq \mathrm{conv}(0, B_p). \tag{1}$$

Indeed, let q be a point in $\mathrm{bd(K)} \cap (p + (\delta - \epsilon)K)$, and let L denote the two-dimensional linear plane spanned by p, q and the origin o, see Fig. 1. Clearly, $L \cap T_p$ is a line, and there are two points on this line at distance δ from p. Let s denote the point of these two which is on the same side of the line op as q. That is, s is a point on the lateral surface of the cone $\mathrm{conv}(0, B_p)$. By the assumption on the modulus of smoothness

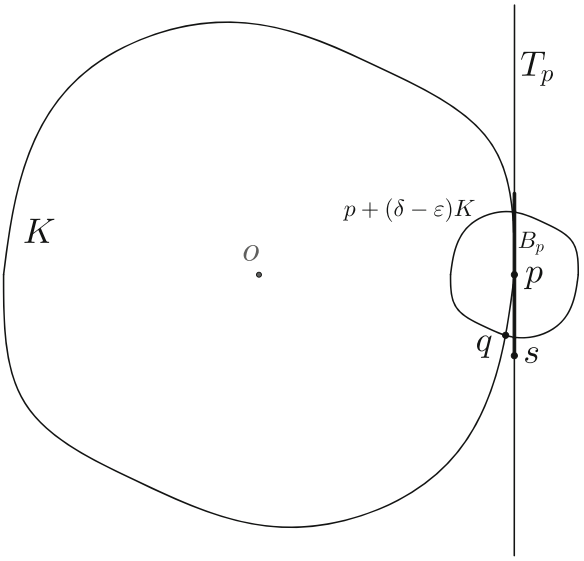

Fig. 1 Proof of (1)

of K, we have $s' := s/\|s\|$ is at distance at most ϵ from s (a detailed computation of a similar fact is given below in this proof). Thus,

$$\|s' - p\| \geq \delta - \epsilon. \tag{2}$$

Now, L is a normed plane with unit circle $K \cap L$ and p is a unit vector in L. It is a classical fact in the theory of normed planes [24, Prop. 31] that as a point moves along the curve $K \cap L$ starting at p and ending at $-p$, the distance (w.r.t. $\|\cdot\|_K$) of the moving point to p is increasing. Thus, by (2), the arc of $K \cap L$ between p and s' contains q, which yields that q is in the cone $\mathrm{conv}(0, B_p)$, proving (1).

Next, instead of the cone $\mathrm{conv}(0, B_p)$, we will consider the cylinder

$$C_p = B_p + [0, -p].$$

Clearly, we have $\mathrm{conv}(0, B_p) \subseteq C_p$. We may assume that ϵ is of the form $\epsilon = (2^k - 1)^{-1}$, where k is a positive integer. For $i \in [k]$, consider the following slice of C_p:

$$C_p(i) = \big(B_p + [-(2^i - 1)\epsilon p, -(2^{i-1} - 1)\epsilon p]\big). \tag{3}$$

Clearly, $2 \odot C_p(i) \subseteq \widehat{C_p} := 2 \odot B_p + [\epsilon p, -3p/2]$ and the centroid $c(C_p(i))$ is at $(1 - (3 \cdot 2^{i-1}/2 - 1))\epsilon p$ for each $i \in [k]$. We claim that $\widehat{C_p} \subseteq (1 + 2\epsilon)K$. Since $\delta \leq 1/4$ and $K = -K$, we have $2 \odot B_p - 3p/2 \subseteq K$. Thus, it suffices to check that $2 \odot B_p + \epsilon p \subseteq (1 + 2\epsilon)K$.

Let $x \in 2 \odot B_p + \epsilon p$, i.e., $x = p + 2(z - p) + \epsilon p$ for some $z \in B_p$. We will show that $\|p + 2(z - p)\| \leq 1 + 2\epsilon$. Since both p and z lie in T_p, then so do $p + 2(z - p)$

and $p + 2(p - z)$, and thus, we have $\|p + 2(z - p)\|, \|p + 2(p - z)\| \geq 1$. One has $\|2(z - p)\| \leq 2\delta = (\epsilon/C)^{1/q}/2$ and so by the assumption on the modulus of smoothness of K, we obtain

$$\|p + 2(z - p)\| \leq 2C\|2(z - p)\|^q + 1 \leq 1 + \epsilon.$$

Thus, $\widehat{C_p} \subseteq (1 + 2\epsilon)K$, and hence,

$$2 \odot C_p(i) \subseteq (1 + 2\epsilon)K$$

for each $i \in [k]$. Since, by (1), all points on the boundary of K at distance at most $\delta - \epsilon$ from p are covered by C_p, we see that all points x, such that $\|x/\|x\| - p\| \leq \delta - \epsilon$ are covered by one of the slices of C_p. Thus, in order to extend the above construction to a $(2, 2\epsilon)$-covering of K, we pick points $\{p_i\}_{i=1}^N$ on the boundary of K such that $\mathrm{bd}\,(K) \subseteq \bigcup_{i=1}^N p_i + (\delta - \epsilon)K$. By Lemma 2.2,

$$N = 2^{O(n)}\left(\frac{1}{\delta - \epsilon}\right)^n = 2^{O(n)}\left(\frac{C}{\epsilon}\right)^{n/q}$$

such points suffice.

Thus, we obtain a $(2, 2\epsilon)$-covering for K by constructing C_{p_i} for each $i \in [N]$ and slicing each C_{p_i} as in (3). Finally, replacing ϵ by $\epsilon/2$, we indeed get a $(2, \epsilon)$-covering of K using $2^{O(n)}(C/\epsilon)^{n/q}\log(1/\epsilon)$ convex bodies, each described by a polynomial in the encoding length of K, see [19]. □

Theorem 3.3 (modulus of smoothness for ℓ_p spaces [23]) *We have*

$$\rho_{\ell_p}(\tau) = \begin{cases} (((1+\tau)^p + (1-\tau)^p)/2)^{1/p} - 1 \leq 2^p\tau^2, & \text{if } 2 \leq p < \infty, \\ (1+\tau^p)^{1/p} - 1 \leq \tau^p/p, & \text{if } 1 \leq p \leq 2. \end{cases}$$

Proof By [23, end of Sect. 2], we only need to show $(((1+\tau)^p + |1-\tau)^p)/2)^{1/p} - 1 \leq 2^p\tau^2$ for $\tau \in (0, 1)$ and $2 \leq p < \infty$. By computing

$$\frac{\mathrm{d}}{\mathrm{d}p}\big[(1+\tau)^p + (1-\tau)^p\big], \quad \text{and then} \quad \frac{\mathrm{d}}{\mathrm{d}\tau}\frac{\mathrm{d}}{\mathrm{d}p}\big[(1+\tau)^p + (1-\tau)^p\big],$$

one obtains that $(1+\tau)^p + (1-\tau)^p \leq (1+\tau)^{\lceil p\rceil} + (1-\tau)^{\lceil p\rceil}$. Next, by taking the binomial expansion, one checks that $\big[(1+\tau)^{\lceil p\rceil} + (1-\tau)^{\lceil p\rceil}\big] \leq (1+2^p\tau^2)^{\lfloor p\rfloor}$, completing the proof. □

Theorems 3.2 and 3.3 imply the following.

Corollary 3.4 ($(2, \epsilon)$-coverings for ℓ_p balls) *For small enough ϵ, there exists a $(2, \epsilon)$-covering for ℓ_p balls using $2^{O(n)}\log(1+1/\epsilon)(1/\epsilon)^{n/2}$ convex bodies for $2 \leq p < \infty$ and $2^{O(n)}\log(1+1/\epsilon)(1/\epsilon)^{n/p}$ convex bodies for $1 \leq p \leq 2$.*

4 Using $(2, \epsilon)$-Coverings for the Closest Vector Problem

We first recall the goal and some important notions of this section: We are given a rational lattice $\Lambda(A) = \{Ax : x \in \mathbb{Z}^n\}$, with $A \in \mathbb{Q}^{n\times n}$ and a target vector $t \in \mathbb{Q}^n$, and we would like to solve $(1+\epsilon)$-approximate CVP_K, i.e., find a lattice vector $v \in \Lambda(A)$ such that $\|v-t\|_K \leq (1+\epsilon)\min_{w\in\Lambda(A)}\|w-t\|_K$. $\|\cdot\|_K$ is defined by $\|x\|_K = \inf\{s : x \in sK\}$, if K is origin symmetric and convex, this defines a norm. If 0 is not the center of symmetry but in the interior of K then we lose the symmetry, i.e., $\|x\|_K \neq \|-x\|_K$. We denote by b the encoding length of the relevant input: A, t, ϵ, encoding length of K, etc.

In this section, we will first describe how a $(2,\epsilon)$-covering for K using N convex bodies boosts any 2-CVP solver for general norms to a $(1+\epsilon)$-CVP_K solver at the expense of a factor $N2^{O(n)}\,\text{poly}(b, 1/\epsilon)$ in the running time. This algorithm, together with the construction of Propositions 2.5 and 2.6 directly implies a $(1+\epsilon)$-CVP solver for polytopes and zonotopes with running time of $2^{O(n+m)}(\log(1+1/\epsilon))^m$ times some polynomial in b and n and with space requirement that of the 2-CVP solver used.

Next, we are going to adapt the construction of Theorem 3.2 to yield a randomized algorithm, that for some fixed point $p \in K$, generates a local $(2,\epsilon)$-covering for K containing p. This yields a randomized $(1+\epsilon)$-CVP solver with the improved running time for ℓ_p norms and with space requirement only depending on that of the 2-approximate CVP solver used. This construction can also be derandomized.

The boosting procedure we are going to describe assumes that we are able to sample uniformly within K and that we can calculate a separating hyperplane at any point on the boundary of K. However, if only a weak membership and a weak separation oracle is provided, the procedure can be adapted such that it suffices to sample almost uniformly, see the algorithm of Dyer et al. [16], and to only calculate a weakly separating hyperplane. We neglect this implementation detail.

As for the convex body K, we assume that $n^{-3/2}B_2^n \subseteq K \subseteq B_2^n$, and thus,

$$\|x\|_2 \leq \|x\|_K \leq n^{3/2}\|x\|_2. \tag{4}$$

This can be ensured by applying an affine transformation, which is polynomial in the input size of K, to both K and the lattice $\Lambda(A)$, see [19].

For concreteness, we choose to use the elegant and currently fastest algorithm for general norms by Dadush and Kun as our 2-CVP solver.

Theorem 4.1 (approximate CVP in any norm [13]) *There exists a deterministic algorithm that for any norm $\|\cdot\|_K$, n-dimensional lattice $\Lambda(A)$ and for any target $t \in \mathbb{R}^n$, computes $y \in \Lambda(A)$, a $(1+\epsilon)$-approximate minimizer to $\|t-x\|_K$, $x \in \Lambda(A)$, in time $O(\text{poly}(n,b)2^{O(n)}(1+1/\epsilon)^n)$ and $O(\text{poly}(n,b)2^n)$ space.*

Theorem 4.2 (boosting 2-CVP using a $(2,\epsilon)$-covering) *Assume we are given an origin symmetric convex body K in $\mathbb{R}^n$ and a $(2,\epsilon)$-covering for K consisting of N convex bodies. Then we can solve the $(1+7\epsilon)$-CVP_K for $\Lambda(A)$ and target $t \in \mathbb{Q}^n$ with $O(N\log(1+1/\epsilon)(\log n + \log b))$ calls to a 2-approximate CVP solver for general norms.*

Proof We may multiply $\Lambda(A)$ and t by the least common multiple of the denominators of the n^2 entries of A and the n entries of t. The resulting lattice and target are integral, $\Lambda(\tilde{A}) \in \mathbb{Z}^{n\times n}$ and $\tilde{t} \in \mathbb{Z}^n$. Since the lowest common multiple is bounded by $2^{(n^2+n)b}$, the resulting basis of $\tilde{A}$ has Euclidean length at most $2^{(n^2+n)b}$. Assuming $t \notin \Lambda(A)$, we see that

$$1 \leq \min_{x\in\Lambda(\tilde{A})} \|x - \tilde{t}\|_2 \leq n2^{(n^2+n)b}.$$

By our assumption (4), we have

$$1 \leq \min_{x\in\Lambda(A)} \|x - t\|_K \leq n^{5/2}2^{(n^2+n)b}.$$

Let $\{Q_i + c_i\}_{i=1}^N$ be the given $(2,\epsilon)$-covering for K, where the origin is the centroid of each of the Q_i.

For our algorithm, for any norm $\|\cdot\|_Q$, we assume that the 2-approximate CVP_Q algorithm that we use with target t only returns a lattice vector v if $\|t - v\|_Q \leq 2$.

We want to find f such that $c_i + (1+\epsilon)^f Q_i$ contains a lattice vector for some $i \in [N]$, but $c_i + (1+\epsilon)^{f-1} Q_i$ contains no lattice vector for any $i \in [N]$. As in [17], we apply a binary search for f.

(i) Initialize $L \leftarrow 0$, $U \leftarrow \lceil \log_{1+\epsilon} n^{5/2}2^{(n^2+n)b} \rceil$ and $x = 0$.
(ii) While $U - L \geq 4$, do a binary search step:
  (iia) For all $i \in [N]$, solve a 2-approximate $\mathrm{CVP}_{(1+\epsilon)^{L+\lceil (U-L)/2\rceil} Q_i}$ problem with target $(1+\epsilon)^{L+\lceil (U-L)/2\rceil} c_i + t$.
  (iib) If some lattice vector v is returned, update $U \leftarrow \lceil \log_{1+\epsilon} \|v - t\|_K \rceil$ and $x \leftarrow v$.
  (iic) Otherwise, update $L \leftarrow L + \lceil (U-L)/2 \rceil$.
(iii) Return x.

It is immediate that for any $\lambda > 0$, $\{\lambda Q_i + \lambda c_i\}_{i=1}^N$ is a $(2,\epsilon)$-covering for λK. Thus if, for some L and U at step (iib), no lattice vector v is returned, then

$$t + (1+\epsilon)^{L+\lceil (U-L)/2\rceil} K \subseteq t + \bigcup_{i=1}^N (1+\epsilon)^{L+\lceil (U-L)/2\rceil} (c_i + Q_i)$$

contains no lattice vector, and so $\min_{v\in\Lambda(A)} \|v - t\|_K \geq (1+\epsilon)^{L+\lceil (U-L)/2\rceil}$. In the case a lattice vector is returned, then

$$\min_{x\in\Lambda(A)} \|t - x\|_K \leq \|v - t\|_K \leq (1+\epsilon)^{L+\lceil (U-L)/2\rceil+1}$$

since the Q_i are a $(2,\epsilon)$-covering of K. Since U and L are valid upper and lower bounds for f at the beginning of the algorithm, we see that throughout the algorithm,

the following invariant is maintained:

$$(1+\epsilon)^L \leq \min_{v\in\Lambda(A)} \|v-t\|_K \leq (1+\epsilon)^U.$$

If the algorithm terminates, then $U-L\leq 3$ since U and L are both integers. Thus, because of the above invariant, the lattice vector $x\in\Lambda(A)$ returned satisfies

$$\begin{aligned}\|x-t\|_K &\leq (1+\epsilon)^U \leq (1+\epsilon)^{L+3} \leq (1+\epsilon)^3 \min_{v\in\Lambda(A)} \|v-t\|_K \\ &\leq (1+7\epsilon) \min_{v\in\Lambda(A)} \|v-t\|_K.\end{aligned}$$

It remains to be shown that the binary search terminates in $O((\log n+\log b)/\epsilon)$ steps. Indeed, for some U and L, let $U_{\text{new}}, L_{\text{new}}$ be the U and L after having executed step (ii) once. If $U-L\geq 6$, it is straightforward to check that $U_{\text{new}}-L_{\text{new}}\leq 3(U-L)/4$. If $4\leq U-L\leq 5$, $U_{\text{new}}-L_{\text{new}}\leq (U-L)-1$. Since $U-L\leq \log_{1+\epsilon}(n^{5/2}2^{(n^2+n)b})$ at the beginning of the algorithm, we are done after $\log_{5/4}(\log_{1+\epsilon}(n^{5/2}2^{(n^2+n)b})) = O(\log(1+1/\epsilon)(\log n+\log b))$ iterations. □

Corollary 4.3 ($(1+\epsilon)$-approximate CVP for polytopes and zonotopes) *Let K be a full-dimensional origin symmetric polytope with m facets or a full-dimensional zonotope with m generators (in particular, $m\geq n$). Then for any $\epsilon\in(0,1)$, the $(1+\epsilon)$-approximate CVP_K problem can be solved deterministically in time $O(\text{poly}(n,b,1/\epsilon)2^{O(n+m)}\log(1+1/\epsilon)^m)$ and space $O(\text{poly}(n)2^n)$.*

Proof Replace ϵ by $\epsilon/7$ and run the algorithm in Theorem 4.2 on a $(2,\epsilon)$-covering of K constructed in the proof of Propositions 2.5 or 2.6. To avoid a space requirement depending on the number of convex bodies N required in the $(2,\epsilon)$-covering for K, every time we call step (iia) of the algorithm, for each $i\in[N]$, we first calculate Q_i and then run the appropriately scaled 2-approximate CVP instance. □

Remark 4.4 The preceding corollary is the reason why we opted to describe a $(2,\epsilon)$-covering with symmetric convex bodies for symmetric polytopes in Proposition 2.6: The algorithm of Dadush and Kun can handle non-symmetric norms $\|\cdot\|_K$, provided 0 is in some sense "close" to the centroid of K, for more details see [13]. Since calculating deterministically the centroid is a hard problem and no efficient algorithms are known, see [28], we would most likely have to resort to a randomized algorithm to approximate the centroid which in turn randomizes our boosting procedure.

Theorem 4.5 (local $(2,\epsilon)$-covering) *Let K be an origin symmetric convex body such that $\|\cdot\|_K$ has modulus of smoothness $C\tau^q$ for $C,q>1$ and $\epsilon\in(0,1)$. Then, in polynomial time, we can find at most $O(\log(1+1/\epsilon))$ origin symmetric convex bodies $\{Q_i\}$ and translations $\{c_i\}$ such that for some constant $c>0$:*

- *For all i, $c_i+2Q_i\subseteq(1+\epsilon)K$.*
- *For $q\in K$, the probability that q is contained in c_i+Q_i for some i is greater than $\min(2^{-cn}C^{-n/q}\epsilon^{-n/q}, (8^qC)^{-n/(q-1)})$.*

Proof Set $\epsilon \leftarrow \epsilon/3$. If $\epsilon > (1/(8C^{1/q}))^{q/(q-1)}$, we uniformly sample a point x from $(1+\epsilon)K$ and return ϵK and x. Any point in K has probability greater or equal than

$$\left(\frac{\epsilon}{1+\epsilon}\right)^n$$

of being covered by $x + \epsilon K$.

If $\epsilon \leq (1/(8C^{1/q}))^{q/(q-1)}$, similarly as in Theorem 3.2, we set $\delta = (\epsilon/C)^{1/q}/4$. We uniformly sample a point x from $(1+\delta/4)K$. Let $p = x/\|x\|$ and for $i \in [\log(1/\epsilon)]$, consider the slices $C_p(i)$ of C_p as in (3) in the proof of Theorem 3.2. For all such $C_p(i)$, denoting by $c(C_p(i))$ its centroid, we return the origin symmetric convex bodies $\{C_p(i) - c(C_p(i))\}$ and the translations $\{c(C_p(i))\}$.

Next, fix a point $q \in K$. With probability greater or equal to

$$\frac{1}{2} \cdot \frac{(\delta/4)^n}{(1+\delta/4)^n} \qquad \text{we have that} \qquad \left\| \frac{q}{\|q\|} - x \right\| \leq \frac{\delta}{4}.$$

In that case, $\|q/(\|q\| - p)\| \leq \delta/2 \leq \delta - \epsilon$ and thus, C_p as in (3) of Theorem 3.2 contains q. It follows that for some $c > 0$ independent of n, C, and q, with probability greater or equal to $2^{-cn} C^{-n/q} \epsilon^{n/q}$ one of the cylinders $C_p(i)$ contain q. □

The next theorem combines the algorithms of Theorems 4.5 and 4.2 to yield an efficient $(1+\epsilon)$-approximate CVP solver for norms with a well bounded modulus of smoothness.

Theorem 4.6 (boosting 2-CVP for a body with small modulus of smoothness) *Let K be a origin symmetric convex body with modulus of smoothness*

$$\rho_K(\tau) \leq C\tau^q, \qquad \text{with} \quad C, q > 1.$$

Then the algorithm presented in the proof solves $(1+\epsilon)$-CVP$_K$ with probability at least $1 - 2^{-n}$. Its running time is $O(\text{poly}(n, b, \log(1/\epsilon))(2^{O(n)} C^{n/q} (1/\epsilon)^{n/q} + O(C)^{n/(q-1)}))$, and the space requirement is equal to that of a 2-CVP solver that handles any norm.

Proof We set $\epsilon \leftarrow \epsilon/7$ and without loss of generality, we may assume

$$1 \leq \min_{x \in \Lambda(A)} \|x - t\|_K \leq n^{5/2} 2^{(n^2+n)b}.$$

We again assume that, for any norm $\|\cdot\|_Q$, the 2-CVP$_Q$ with target t only returns a lattice vector v if $\|t - v\|_Q \leq 2$, if there is no such v, it returns nothing.

We adapt the algorithm of Theorem 4.2:

(i) Initialize $L \leftarrow 0$, $U \leftarrow \lceil \log_{1+\epsilon} n^{5/2} 2^{(n^2+n)b} \rceil$ and $x = 0$.
(ii) While $U - L \geq 4$, do a binary search step:
  (iia) Run the algorithm from Theorem 4.5 and denote the returned convex bodies and translations by Q_i and c_i respectively. For all i, solve a 2-approximate CVP$_{(1+\epsilon)^{L+\lceil (U-L)/2 \rceil} Q_i}$ problem with target $(1+\epsilon)^{L+\lceil (U-L)/2 \rceil} c_i + t$. Repeat N times.

(iib) If some lattice vector v is returned, update $U \leftarrow \lceil \log_{1+\epsilon} \|v - t\|_K \rceil$ and $x \leftarrow v$.

(iic) Otherwise, update $L \leftarrow L + \lceil (U - L)/2 \rceil$.

(iii) Return x.

Correctness of the algorithm follows from Theorem 4.2, provided step (ii) runs correctly (i.e., correctly detects whether there is a lattice point or not with high probability) for all $O(\log(1/\epsilon)(\log n + \log b))$ iterations. To verify this, let $v \in \mathcal{L}$ be some lattice vector contained in a homothet of K at some fixed iteration of the algorithm. With probability $p = 2^{-cn} C^{-n/q} (1/\epsilon)^{n/q}$ or $(1/(8^q C))^{1/(q-1)}$ respectively, one of the convex bodies returned by one run of Theorem 4.5 contains v. Thus, repeating step (iia) $n(2^{cn} C^{n/q} (1/\epsilon)^{n/q} + (8^q C)^{1/(q-1)})$ times, with probability greater than $1 - 2^{-n}$, v is contained in one of the convex bodies returned and step (ii) runs correctly. Since step (ii) needs to run correctly each of the $O(\log(1/\epsilon)(\log n + \log b))$ iterations necessary to find the correct U and L, by the union bound, it is sufficient to set $N = O(n \log(\log(1/\epsilon)(\log n + \log b)) 2^{cn} C^{n/q} (1/\epsilon)^{n/q} + (8^q C)^{1/(q-1)})$ to guarantee a success probability of $1 - 2^{-n}$. This implies the bound on the running time. □

In our proof of Theorem 4.6, instead of applying our local covering algorithm, Theorem 4.5, we could use a recent result of Dadush [12, Thm. 4.1]. There, a deterministic algorithm is presented to build and iterate over an epsilon net in $2^{O(n)}(1 + 1/\epsilon)^n$ time and poly(n) space. For symmetric convex bodies with modulus of smoothness bounded by $C\tau^q$, we may apply this result with $O(\epsilon^{1/q})$, as in Theorem 4.5, in place of ϵ to build a covering of size $O(1/\epsilon)^{n/q}$. This would replace the sampling part in Theorem 4.5 and thus derandomizes our boosting procedure.

Remark 4.7 One may consider convex bodies that are not necessarily origin symmetric. Assume that a convex body K is γ-*symmetric*, that is, $\mathrm{vol}(K \cap -K) \geq \gamma^n \mathrm{vol}(K)$. Then the result of Dadush and Kun (Theorem 4.1) still applies (see [13]), and it is straightforward to modify the above algorithm to obtain a $(1 + \epsilon)$-approximate CVP algorithm for $\|\cdot\|_K$ using $2^{O(n)}(1/(\gamma\epsilon))^n$ calls to a 2-approximate CVP algorithm handling any symmetric norm, for instance the AKS based algorithm of Dadush [11], resulting in an algorithm with time $O(1/(\gamma\epsilon))^n$ and space $2^{O(n)}$. We essentially use Theorem 4.5 with $q = 1$: we sample a point p in $(1+\epsilon/3)K$ and output $(\epsilon/3)(K \cap -K)$ and p. Thus, each point in K has probability greater or equal to $2^{-O(n)}(1/(\gamma\epsilon))^n$ of being covered.

5 Sparsifiers and the Modulus of Smoothness

In this section we describe a surprising connection between lattice sparsifiers as used by Dadush and Kun and the modulus of smoothness. Informally, our main technical contribution is the observation that for a lattice-point-free convex body K with modulus of smoothness bounded by $C\tau^q$, a $O(\epsilon^{1/q})$-sparsifier for K preserves the metric information up to an additive error of $O(\epsilon)$. We will show that we can tweak the algorithm of Dadush and Kun using this simple observation in order to match

the running time of the preceding boosting procedure. We will only consider origin symmetric-convex bodies $K \subseteq \mathbb{R}^n$.

Definition 5.1 (*lattice sparsifier for origin symmetric* K [13]) Let $K \subseteq \mathbb{R}^n$ be an origin-symmetric convex body, $\mathcal{L}$ be an n-dimensional lattice and $\delta > 0$. A (K, δ) sparsifier for $\mathcal{L}$ is a sublattice $\mathcal{L}' \subseteq \mathcal{L}$ satisfying

- $G(K, \mathcal{L}') \leq O(1/\delta)^n$,
- $\forall x \in \mathbb{R}^n, d_K(\mathcal{L}', x) \leq d_K(\mathcal{L}, x) + \delta$,

where $G(K, \mathcal{L})$ denotes the maximal number of lattice vector any translate of K can contain, formally:

$$G(K, \mathcal{L}) = \max_{x \in \mathbb{R}^n} |(K + x) \cap \mathcal{L}|.$$

By a covering argument (see [13, Lem. 2.3]), $G(dK, \mathcal{L}) \leq (2d+1)^n G(K, \mathcal{L})$. By the second condition, if $\mathcal{L}'$ is a (K, δ)-sparsifier for $\mathcal{L}$, for every lattice point $v \in \mathcal{L}$, there is $v' \in \mathcal{L}'$ such that $\|v - v'\|_K \leq \delta$. These two conditions ensure that the resulting lattice $\mathcal{L}'$ is thinned out according to the geometry of K: the first condition guarantees that K (or a dilate of K) cannot contain too many lattice vectors of $\mathcal{L}'$ (hence enumeration is not too costly), but, by the second condition, $\mathcal{L}'$ is rather close to $\mathcal{L}$ and thus serves as a good approximation.

We now come to the main observation:

Lemma 5.2 *Let K be an origin symmetric convex body with modulus of smoothness bounded by $\rho_K \leq C\tau^q$, $q \geq 1$, $\mathcal{L}$ a lattice and $t \in \mathbb{R}^n$ a target vector. Assume that $t + K$ does not contain any lattice vector $v \in \mathcal{L}$ in its interior. Let $\mathcal{L}'$ be a $(K, \epsilon^{1/q})$ sparsifier for $\mathcal{L}$. Then*

$$d_K(\mathcal{L}', t) \leq d_K(\mathcal{L}, t) + 2C\epsilon.$$

Proof Denote by $v \in \mathcal{L}$ a closest lattice vector to t, and set $R := d_K(\mathcal{L}, t)$. Clearly, $R = \|v - t\|_K \geq 1$. By the second condition of the sparsifier, there is a lattice vector $w \in \mathcal{L}'$ with $\|w - v\|_K \leq \epsilon^{1/q}$. Denoting by $y := w - v \in \mathcal{L}$, the definition of the modulus of smoothness yields

$$\left\| \frac{w-t}{R} \right\|_K = \left\| \frac{v-t}{R} + \frac{y}{R} \right\|_K \leq 2 + \frac{2C\epsilon}{R^q} - \left\| \frac{v-t}{R} - \frac{y}{R} \right\|_K \leq 1 + \frac{2C\epsilon}{R^q},$$

where we used the fact that $v - y \in \mathcal{L}$, and hence, $\|(v - y) - t\|_K \geq R$. Multiplying the inequality by R and observing that $R, q \geq 1$ completes the proof of Lemma 5.2. □

Next, we present the algorithmic application of the previous lemma to the $(1+\epsilon)$-approximate Closest Vector Problem under a symmetric norm. We adopt the same notation as in Sect. 4. We may assume that $t \in \mathbb{Z}^n$, $\mathcal{L}(A) \subseteq \mathbb{Z}^n$ and $\|t\|_\infty, \|A\|_\infty \leq 2^{(n^2+n)b}$. We assume $n^{-3/2} B_2^n \subseteq K \subseteq (1/2) B_2^n$. Thus, $d_K(\mathcal{L}, t) \leq 2n^{5/2} 2^{(n^2+n)b}$,

and, if $t \notin \mathcal{L}(A)$, $t + K$ does not contain a lattice vector. We will need the following two algorithms.

Theorem 5.3 (`Lattice-Enumerator`$(K, t, \mathcal{L}, \epsilon)$ [14]) *Let $\mathcal{L}(A)$ be a lattice, K a convex body in $\mathbb{R}^n$ and $\epsilon > 0$. There is a deterministic algorithm that outputs all S such that*

$$(t + K) \cap \mathcal{L} \subseteq S \subseteq (t + K + \epsilon B_2^n) \cap \mathcal{L}$$

in time $G(K, \mathcal{L})2^{O(n)}\,\mathrm{poly}(n, b)$ and $2^n\,\mathrm{poly}(n, b)$ space.

Theorem 5.4 (`Lattice-Sparsifier`$(\mathcal{L}(A), K, \delta)$ [13]) *For $\delta > 0$, a basis A' for a (K, δ)-sparsifier for $\mathcal{L}(A)$ can be computed deterministically in $2^{O(n)}\,\mathrm{poly}(n, b)$ time and $2^n\,\mathrm{poly}(n, b)$ space.*

We now combine these two theorems with Lemma 5.2.

Theorem 5.5 *There is an algorithm (described in the proof) that for an origin symmetric convex body K in $\mathbb{R}^n$, with modulus of smoothness bounded by $\rho_K \leq C\tau^q$ with some $C, q \geq 1$, solves $(1 + \epsilon)$-CVP$_K$ for any lattice $\mathcal{L}$ and target vector $t \in \mathbb{R}^n$ in time $O((C/\epsilon)^{n/q})\,\mathrm{poly}(n, b)$ and space $2^n\,\mathrm{poly}(n, b)$.*

Proof We may assume $\epsilon \leq 1$. If $t \in \mathcal{L}(A)$ (this can be checked in $\mathrm{poly}(n, b)$ time), return t. Else, set $\bar{\epsilon} = \epsilon/(4C)$ and $d = 0$ and apply the following algorithm.

(i) Set $K_d = 2^d K$.
(ii) Apply `Lattice-Sparsifier`$(K_d, \mathcal{L}, \bar{\epsilon}^{1/q})$. Denote the sparsified lattice by $\mathcal{L}'$.
(iii) Apply `Lattice-Enumerator`$((2+\epsilon)K_d, t, \mathcal{L}', \epsilon)$. If there is a lattice vector in $t + (2 + \epsilon)K$, return the closest one to t, and stop. Else, set $d \leftarrow d + 1$ and go to (i).

Let k be the largest positive integer such that $t + K_k$ does not contain a lattice vector. First, we claim that the algorithm will terminate at iteration $d \leq k$. Indeed, since $t + 2K_k = t + K_{k+1}$ contains a lattice vector of $\mathcal{L}$, by Lemma 5.2, $(2 + \epsilon)K_k$ contains a lattice vector of $\mathcal{L}'$, and hence, the algorithm will terminate at $d = k$, or before.

To bound the error, we assume that the algorithm terminated at iteration d. By the previous paragraph, $t + K_d$ does not contain a lattice vector, and thus,

$$d_K(\mathcal{L}, t) \geq 2^d. \tag{5}$$

Let v denote the lattice vector returned by `Lattice-Enumerator`$((2 + \epsilon)K_d, t, \mathcal{L}', \epsilon)$. By Lemma 5.2, we only have an additive error of $2C\bar{\epsilon} = \epsilon/2$ with respect to $\|\cdot\|_{K_d}$, that is,

$$d_{K_d}(\mathcal{L}, t) \leq \|t - v\|_{K_d} + \frac{\epsilon}{2},$$

which, by (5) yields

$$d_K(\mathcal{L}, t) \leq \|t - v\|_K + 2^d \epsilon \leq \|t - v\|_K + \epsilon d_K(\mathcal{L}, t),$$

and hence $d_K(\mathcal{L}, t) \leq \|t - v\|_K / (1 - \epsilon/2) \leq (1 + \epsilon) \|t - v\|_K$. Thus, we found a $(1 + \epsilon)$-approximate solution.

Next, we consider the time and space requirements. It is clear that step (ii) always takes time $2^{O(n)} \operatorname{poly}(n, b)$ and space $2^n \operatorname{poly}(n, b)$, independently of d. Note that $G((2 + \epsilon)K, \mathcal{L}') \leq G(3K, \mathcal{L}') \leq O(1/\bar{\epsilon})^{n/q}$, and thus, step (iii) takes $O(C/\epsilon)^{n/q} \operatorname{poly}(n, b)$ time and $2^n \operatorname{poly}(n, b)$ space. Since $d_K(t, \mathcal{L}) \leq 2n^{5/2} 2^{(n^2+n)b}$, we need at most $\log_2(2n^{5/2} 2^{(n^2+n)b}) = \operatorname{poly}(n, b)$ iterations, resulting in time $O(C/\epsilon)^{n/q} \operatorname{poly}(n, b)$. This completes the proof of Theorem 5.5. □

Acknowledgements We thank Friedrich Eisenbrand for suggesting to use coverings to boost approximate CVP and for helpful remarks and ideas during the research. We would also like to thank Christoph Hunkenschröder and Matthias Schymura for helpful remarks on the text, and for our stimulating discussions that boosted our understanding of the closest vector problem. Part of MN's research was carried out while he was a member of János Pach's chair of DCG at EPFL, supported by Swiss National Science Foundation Grants 200020-162884 and 200021-165977. MN was supported also by the National Research, Development and Innovation Fund (NRDI) grants K119670 and KKP-133864 as well as the Bolyai Scholarship of the Hungarian Academy of Sciences and the New National Excellence Programme and the TKP2020-NKA-06 program provided by the NRDI. MV was supported by the Swiss National Science Foundation within the project *Lattice Algorithms and Integer Programming* (Nr. 200021-185030).

Funding Open access funding provided by the Eötvös Loránd University.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Appendix: Proof of Some Lemmas

Proof of Lemma 2.2 We cover K greedily by copies of $(\epsilon/2)K$ as follows. If after selecting $i - 1$ homothetic copies of K there is a point $p_i \in K$ not yet covered, we take $Q_i = p_i + (\epsilon/2)K$. To see that after $N \leq (5/\epsilon)^n$ steps, all points of K are covered, we notice that the sets $(1/2) \odot Q_i$ are non-overlapping, and are contained in $(1 + \epsilon/4)K \subseteq (5/4)K$. Taking the volume of these sets, we obtain the desired bound. □

Proof of Lemma 2.3 Let $\{Q_i\}_{i=1}^N$ be a $(2, \epsilon)$-covering of K. For each $i \in [N]$, we will find a $(2, 1)$-covering for Q_i using at most 10^n centrally symmetric convex bodies. Thus, the union of these at most $10^n N$ symmetric sets will yield a $(2, \epsilon)$-covering of K. Fix $i \in [N]$ and set $\tilde{Q}_i = (1/2)((Q_i - c(Q_i)) \cap (c(Q_i) - Q_i))$. In the same fashion as in the proof of Lemma 2.2, let $\{b_1, \ldots, b_m\}$ be a maximal subset of Q_i such

that the interiors of the sets $b_1 + (1/2)\,\tilde{Q}_i, \ldots, b_m + (1/2)\,\tilde{Q}_i$ are pairwise disjoint. Clearly, $\tilde{Q}_i + \{b_1, \ldots, b_m\}$ is a covering of Q_i.

By a result of Milman and Pajor [26], if the centroid of a convex body Q in $\mathbb{R}^n$ is the origin, then

$$\operatorname{vol}(Q \cap -Q) \geq 2^{-n} \operatorname{vol}(Q). \tag{6}$$

Thus, $\operatorname{vol}(b_k + (1/2)\,\tilde{Q}_i) \geq 8^{-n} \operatorname{vol}(Q)$, $k = 1, \ldots, m$. Since $b_k \in Q_i$ and $(1/2)\,\tilde{Q}_i \subseteq (1/4)(Q_i - c(Q_i))$, we have that $b_k + (1/2)\,\tilde{Q}_i \subseteq (5/4) \odot Q_i$. Thus, $m \leq 10^n$.

To see that $\tilde{Q}_i + \{b_1, \ldots, b_m\}$ is $(2, 1)$-covering of Q_i, note that $2\tilde{Q}_i \subseteq (Q_i - c(Q_i))$, and hence $b_k + 2\tilde{Q}_i \subseteq Q_i + (Q_i - c(Q_i)) = 2 \odot Q_i$, as required. □

Proof of Lemma 2.4 The same argument as that used in the proof of Lemma 2.2 combined with (6) yields it. □

Proof of Proposition 2.5 We may assume that $\epsilon = (2^k - 1)^{-1}$ for some positive integer k. For $i \in [k]$, the following union of translated intervals is a $(2, \epsilon)$-covering of $[-b, b]$:

$$[-b, b] \subseteq \bigcup_{\substack{\delta \in \{\pm 1\} \\ j \in [k]}} \left(\delta(1 - (2^j - 1)\epsilon)b + [-2^{j-1}\epsilon b, 2^{j-1}\epsilon b]\right).$$

We may decompose analogously every line segment generating $\mathcal{Z}$ and combine them to give a $(2, \epsilon)$-covering for $\mathcal{Z}$:

$$\mathcal{Z} \subseteq \bigcup_{\substack{\delta \in \{\pm 1\}^m \\ \alpha \in [k]^m}} \sum_{i=0}^{k} \left(\delta_i(1 - (2^{\alpha_i} - 1)\epsilon)b_i + [-2^{\alpha_i - 1}\epsilon b_i, 2^{\alpha_i - 1}\epsilon b_i]\right).$$

This is a $(2, \epsilon)$-covering for $\mathcal{Z}$ using $(2\log_2(1 + 1/\epsilon) + 1)^m$ (translated) zonotopes. □

Proof of Proposition 2.6 We may assume that $\epsilon = ((4/3)^k - 1)^{-1}$ for some positive integer k. For $\alpha \in [k]^m$ and $\delta \in \{\pm 1\}^m$, consider the following polytopes $\bar{Q}(\alpha, \delta)$:

$$\left\{x : \left(1 - \left(\left(\frac{4}{3}\right)^{\alpha_i} - 1\right)\epsilon\right)b_i \leq \delta a_i^T x \leq \left(1 - \left(\left(\frac{4}{3}\right)^{\alpha_i - 1} - 1\right)\epsilon\right)b_i, i \in [m]\right\}.$$

For each facet direction $|a_i^T x| \leq b_i$, scaling each of the resulting (non-empty) $\bar{Q}$ around any point in its interior by a factor 4, it is straightforward to check that the resulting convex body is contained inside $\{x \in \mathbb{R}^n : |a_i^T x| \leq (1 + \epsilon)b_i\}$. It follows that each such non-empty polyhedron $\bar{Q}$ can be scaled by a factor 4 around any point in it and the resulting polytope is still contained inside $(1 + \epsilon)\,P$ and it is clear that P is contained in the union of the $\bar{Q}(\alpha, \delta)$.

We could stop here and have a $(2, \epsilon)$-covering for P, but we are not guaranteed that the resulting cells are centrally symmetric. In order to ensure this, we will symmetrize

the resulting $\bar{Q}(\alpha, \delta)$ as follows. Fix $x(\alpha, \delta) \in \bar{Q}(\alpha, \delta)$ and define

$$\bar{Q}_x(\alpha, \delta) = x(\alpha, \delta) + \text{conv}\,(\bar{Q}(\alpha, \delta) - x(\alpha, \delta), x(\alpha, \delta) - \bar{Q}(\alpha, \delta)).$$

These are centrally symmetric polytopes with center of symmetry at $x(\alpha, \delta)$. When $\bar{Q}$ is scaled by a factor 4, it is still contained in $(1+\epsilon)P$, thus we have $2 \odot Q_x(\alpha, \delta) \subseteq (1+\epsilon)P$. Thus, the union of all $\{\bar{Q}_x(\alpha, \delta)\}$ is a $(2, \epsilon)$-covering for K using at most $2^m(\log_{4/3}(1/\epsilon) + 1)^m$ symmetric convex bodies. □

References

1. Abdelkader, A., Mount, D.M.: Economical Delone sets for approximating convex bodies. In: 16th Scandinavian Symposium and Workshops on Algorithm Theory (Malmö 2018). Leibniz International Proceedings in Informatics, vol. 101, # 4. Leibniz-Zent. Inform., Wadern (2018)
2. Aggarwal, D., Dadush, D., Stephens-Davidowitz, N.: Solving the closest vector problem in 2^n time—the discrete Gaussian strikes again! In: 56th Annual Symposium on Foundations of Computer Science (Berkeley 2015), pp. 563–582. IEEE, Los Alamitos (2015)
3. Aggarwal, D., Mukhopadhyay, P.: Improved algorithms for the Shortest Vector Problem and the Closest Vector Problem in the infinity norm (2018). arXiv:1801.02358
4. Aggarwal, D., Stephens-Davidowitz, N.: Just take the average! An embarrassingly simple 2^n-time algorithm for SVP (and CVP). In: 1st Symposium on Simplicity in Algorithms (New Orleans 2018). OpenAccess Series in Informatics, vol. 61, # 12. Leibniz-Zent. Inform., Wadern (2018)
5. Ajtai, M., Kumar, R., Sivakumar, D.: A sieve algorithm for the shortest lattice vector problem. In: 33rd Annual ACM Symposium on Theory of Computing (Hersonissos 2001), pp. 601–610. ACM, New York (2001)
6. Ajtai, M., Kumar, R., Sivakumar, D.: Sampling short lattice vectors and the closest lattice vector problem. In: 17th Annual Conference on Computational Complexity (Montreal 2002), pp. 53–57. IEEE, Los Alamitos (2002)
7. Arora, S.: Probabilistic Checking of Proofs and Hardness of Approximation Problems. PhD thesis, University of California at Berkeley (1994)
8. Arya, S., da Fonseca, G.D., Mount, D.M.: On the combinatorial complexity of approximating polytopes. Discrete Comput. Geom. **58**(4), 849–870 (2017)
9. Blömer, J., Naewe, S.: Sampling methods for shortest vectors, closest vectors and successive minima. Theor. Comput. Sci. **410**(18), 1648–1665 (2009)
10. Böröczky, K. Jr., Wintsche, G.: Covering the sphere by equal spherical balls. In: Discrete and Computational Geometry. Algorithms and Combinatorics, vol. 25, pp. 235–251. Springer, Berlin (2003)
11. Dadush, D.: A $O(1/\epsilon^2)^n$-time sieving algorithm for approximate integer programming. In: 10th Latin American Symposium on Theoretical Informatics (Arequipa 2012). Lecture Notes in Computer Science, vol. 7256, pp. 207–218. Springer, Heidelberg (2012)
12. Dadush, D.: A deterministic polynomial space construction for ϵ-nets under any norm (2013). arXiv:1311.6671
13. Dadush, D., Kun, G.: Lattice sparsification and the approximate closest vector problem. Theory Comput. **12**, # 2 (2016)
14. Dadush, D., Peikert, Ch., Vempala, S.: Enumerative lattice algorithms in any norm via M-ellipsoid coverings. In: 52nd Annual Symposium on Foundations of Computer Science (Palm Springs 2011), pp. 580–589. IEEE, Los Alamitos (2011)
15. Dinur, I., Kindler, G., Raz, R., Safra, S.: Approximating CVP to within almost-polynomial factors is NP-hard. Combinatorica **23**(2), 205–243 (2003)
16. Dyer, M., Frieze, A., Kannan, R.: A random polynomial-time algorithm for approximating the volume of convex bodies. J. Assoc. Comput. Mach. **38**(1), 1–17 (1991)
17. Eisenbrand, F., Hähnle, N., Niemeier, M.: Covering cubes and the closest vector problem. In: 27th Symposium on Computational Geometry (Paris 2011), pp. 417–423. ACM, New York (2011)

18. van Emde Boas, P.: Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical Report 81-04. Mathematische Instituut, University of Amsterdam (1981). https://www.staff.fnwi.uva.nl/p.vanemdeboas/vectors/abstract.html
19. Grötschel, M., Lovász, L., Schrijver, A.: Geometric Algorithms and Combinatorial Optimization. Algorithms and Combinatorics, vol. 2. Springer, Berlin (1988)
20. Hunkenschröder, Ch., Reuland, G., Schymura, M.: On compact representations of Voronoi cells of lattices. In: Integer Programming and Combinatorial Optimization (Ann Arbor 2019). Lecture Notes in Computer Science, vol. 11480, pp. 261–274. Springer, Cham (2019)
21. Kannan, R.: Minkowski's convex body theorem and integer programming. Math. Oper. Res. **12**(3), 415–440 (1987)
22. Lenstra, H.W. Jr.: Integer programming with a fixed number of variables. Math. Oper. Res. **8**(4), 538–548 (1983)
23. Lindenstrauss, J.: On the modulus of smoothness and divergent series in Banach spaces. Mich. Math. J. **10**, 241–252 (1963)
24. Martini, H., Swanepoel, K.J., Weiß, G.: The geometry of Minkowski spaces—a survey. I. Expos. Math. **19**(2), 97–142 (2001)
25. Micciancio, D., Voulgaris, P.: A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. In: 42rd Annual ACM Symposium on Theory of Computing (Cambridge 2010), pp. 351–358. ACM, New York (2010)
26. Milman, V.D., Pajor, A.: Entropy and asymptotic geometry of non-symmetric convex bodies. Adv. Math. **152**(2), 314–335 (2000)
27. Mukhopadhyay, P.: Faster provable sieving algorithms for the Shortest Vector Problem and the Closest Vector Problem on lattices in ℓ_p norm. Algorithms **14**(12), # 362 (2021)
28. Rademacher, L.: Approximating the centroid is hard. In: 23rd Annual Symposium on Computational Geometry (Gyeongju 2007), pp. 302–305. ACM, New York (2007)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.