COVERING CONVEX BODIES AND THE CLOSEST VECTOR PROBLEM

MÁRTON NASZÓDI AND MORITZ VENZIN

Abstract. We present algorithms for the $(1+\varepsilon)$-approximate version of the closest vector problem for certain norms. The currently fastest algorithm (Dadush and Kun 2016) for general norms has running time of $2^{O(n)}(1/\varepsilon)^n$. We improve this substantially in the following two cases.

For ℓ_p-norms with $p > 2$ (resp. $p \in [1,2]$) fixed, we present an algorithm with a running time of $2^{O(n)}(1/\varepsilon)^{n/2}$ (resp. $2^{O(n)}(1/\varepsilon)^{n/p}$). 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 two around their centroids, each one is contained in the $(1+\varepsilon)$-scaled homothet of the norm ball? We provide upper bounds for this problem 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 $(1+\varepsilon)$-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.

Furthermore, we consider polyhedral and zonotopal norms. For centrally symmetric polytopes (resp. zonotopes) with $O(n)$ facets (resp. generated by $O(n)$ line segments), we provide a deterministic $O(\log_2(1/\varepsilon))^{O(n)}$ time algorithm. This generalizes the result of Eisenbrand et al. which applies to the ℓ_∞-norm.

As it is the case for the covering procedure of Eisenbrand et al., our approach boosts any constant factor approximation algorithm to a $(1+\varepsilon)$-approximate algorithm. By assuming the existence of a poly(n)-space and $2^{O(n)}$ time algorithm for 2-approximate CVP, the space complexity of our algorithm can be reduced to a polynomial.

arXiv:1908.08384v1 [cs.DS] 22 Aug 2019

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 closest vector in $\mathcal{L}$ to t with respect to a given norm. The *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 [vEB81] and even NP-hard to approximate up to almost polynomial factors, [Aro95], [DKRS03]. These results suggest to also look for approximate algorithms solving CVP with a not too large dependence on the approximation guarantee. A $(1+\varepsilon)$-approximate CVP solver for the norm $\|\cdot\|_K$ finds a lattice vector whose distance to the target vector is at most $(1+\varepsilon)$ times the minimal distance of the target to the lattice. We denote the problem as $(1+\varepsilon)$-CVP$_K$, or when K is the unit ball of the space ℓ_p^n for some $1 \leqslant p \leqslant \infty$, as $(1+\varepsilon)$-CVP$_p$.

The first algorithm to solve integer programming and, in particular, CVP$_\infty$ was given by Lenstra [Len83] with a running time of $2^{O(n^3)}$. His algorithm connects the two fields of geometry of numbers and integer programming. Kannan [Kan87] presented an algorithm for these problems 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 $(1+\varepsilon)$-CVP$_2$ with time and space $2^{(1+1/\varepsilon)n}$, [AKS01], [AKS02]. Subsequently, Blömer and Naewe [BN09] extended the randomized sieving algorithm of Ajtai et al. to solve $(1+\varepsilon)$-CVP$_p$ for all p in time $O(1/\varepsilon)^{2n}$ and space $O(1/\varepsilon)^n$. For $p=\infty$, Eisenbrand, Hähnle and Niemeier [EHN11] then boosted the algorithm of Blömer and Naewe by showing that $2^{O(n)}\log(1+1/\varepsilon)^n$ calls to a 2-CVP$_\infty$ solver suffice to solve $(1+\varepsilon)$-CVP$_\infty$ implying a running time of $O(\log(1+1/\varepsilon))^n$ and space requirement $2^{O(n)}$.

Dadush [Dad12] extended the Ajtai–Kumar–Sivakumar sieve to solve $(1+\varepsilon)$-CVP in any norm with a running time of $O(1/\varepsilon)^{2n}$ and space $O(1/\varepsilon)^n$. The first single exponential deterministic solver for CVP$_2$ was presented by Micciancio and Voulgaris [MV10]. Their algorithm needs to store the up to $2(2^n-1)$ facets of the Voronoi cell of the lattice. Recently in [HRS19], 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 CVP$_2$ (with a very small approximation factor) and SVP$_2$ use Gaussian sampling and need time and space 2^n [AS18]. 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 [DK16] presented a deterministic algorithm solving $(1+\varepsilon)$-CVP for any norm in time $2^{O(n)}(1/\varepsilon)^n$ and with space requirement $2^n\operatorname{poly}(n)$ - reducing the dependence on $(1/\varepsilon)$ in the running time and removing the dependence on $(1/\varepsilon)$ 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 convex bodies are needed to cover some convex body K, such that when scaled around their respective centroids by a factor 2, each one is contained in $(1+\varepsilon)K$. We refer to such a covering as a *$(2,\varepsilon)$-covering for K*, and the smallest size of such a covering as the *$(2,\varepsilon)$-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.

(1) By a standard argument, we show that for any centrally symmetric convex body, a $(2,\varepsilon)$-covering is always possible using $2^{O(n)}(\frac{1}{\varepsilon})^n$ convex bodies. Then, in Theorem 2.7, we establish a lower bound of $2^{-O(n)}(\frac{1}{\varepsilon})^{n/2}$ for the Euclidean unit ball.

(2) For centrally symmetric polytopes (resp. zonotopes) with m facets (resp. m generating line segments), we provide an explicit $(2,\varepsilon)$-covering using at most $O(\log(\frac{1}{\varepsilon}))^m$ convex bodies, see Propositions 2.5 and 2.6. These are relatively straight forward generalizations of the method of [EHN11] where the cube is considered.

(3) 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 $(2,\varepsilon)$-covering number. More specifically, if K has modulus of smoothness bounded above by $C\tau^q$, then we find a $(2,\varepsilon)$-covering of K using $C^{O(n)}(\frac{1}{\varepsilon})^{n/q}$ convex bodies. In particular, we obtain a $(2,\varepsilon)$-covering for ℓ_p balls using $2^{O(n)}(\frac{1}{\varepsilon})^{n/2}$ for $p\geqslant 2$ and $2^{O(n)}(\frac{1}{\varepsilon})^{n/p}$ for $p\in[1,2]$, matching the lower bound (Theorem 2.7) for the Euclidean unit ball.

(4) Our second main result is Theorem 4.2, which shows how a good algorithmic bound on the $(2,\varepsilon)$-covering number yields an efficient $(1+\varepsilon)$-CVP algorithm. In particular, for norms induced by centrally symmetric polytopes (resp. zonotopes) with m facets (resp. generating line segments), the above explicit $(2,\varepsilon)$-covering boosts any 2-CVP solver for general norms to yield a deterministic $(1+\varepsilon)$-CVP

algorithm. This yields an algorithm with running time $O(\log(\frac{1}{\varepsilon}))^m$ and $2^n\operatorname{poly}(n)$ space, see Corollary 4.3.

(5) 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 $(2,\varepsilon)$-covering of K, we show how to generate a local $(2,\varepsilon)$-covering on the fly. This yields a simple, randomized $(1+\varepsilon)$-CVP$_p$ algorithm for $1 \leqslant p \leqslant \infty$ with a running time of $O(\frac{1}{\varepsilon})^{n/2}$ for $p \geqslant 2$, and $2^{O(n)}(\frac{1}{\varepsilon})^{n/p}$ for $p \in [1,2]$, using $2^n\operatorname{poly}(n)$ space. Alternatively, we may use an algorithm of Dadush [Dad13] 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 [BN09], [DK16], we improve on the previous best running times of $O(\frac{1}{\varepsilon})^n$ 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 $(\frac{1}{\gamma\varepsilon})^n$ 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.

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

The scalar product of two vectors $x = (x_1,\dots,x_n)$ and $y = (y_1,\dots,y_n)$ in $\mathbb{R}^n$ is denoted by $\langle x,y\rangle = x_1y_1+\dots+x_ny_n$. For a positive integer k, we use the notation $[k] = \{1,\dots,k\}$.

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

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

We would like to note here that we have fixed the factor 2 for concreteness and thus assume $\varepsilon \in (0,1)$, up to minor changes, we could replace 2 with any other constant.

The following lemmas follow directly from standard packing arguments.

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

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

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 $(2, \varepsilon)$-covering consisting of N convex bodies. Then, K admits a $(2, \varepsilon)$-covering consisting of $5^n N$ centrally symmetric convex bodies.*

Proof of Lemma 2.3. Let $\{Q_i\}_{i=1}^N$ be a sequence of convex bodies as in Definition 2.1. Fix $i \in [N]$, and let $\tilde{Q}_i = c(Q_i) + \frac{1}{2} \operatorname{conv}(Q_i - c(Q_i), c(Q_i) - Q_i)$. Let $\tilde{Q}_i + \{b_1, \ldots, b_m\}$ be a packing of Q_i in the same fashion as Lemma 2.2: $b_i \notin b_j + \tilde{Q}_j$ for all $i \neq j$. By a result of Milman and Pajor [MP00], if the centroid of a convex body Q in $\mathbb{R}^n$ is the origin, then

$$\operatorname{vol}(Q \cap -Q) \geqslant 2^{-n} \operatorname{vol}(Q). \tag{1}$$

Clearly, $Q_i \subset \tilde{Q}_i + \{b_1, \ldots, b_m\} \subset 2\tilde{Q}_i + \{b_1, \ldots, b_m\} \subset 2Q_i$. Furthermore, the convex sets $b_i + \frac{1}{2}Q_i$ are mutually disjoint and contained inside $\frac{5}{4}Q_i$. This implies the bound on the number of centrally symmetric convex bodies required. □

The same argument as that used in the proof of Lemma 2.2 combined with (1) yields the following.

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

In the particular case of the cube, in [EHN11], Eisenbrand et al. found a $(2, \varepsilon)$-covering that requires $(1 + 2\log_2(1/\varepsilon))^n$ 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, $\mathcal{Z} = \{\sum_{i=1}^m \lambda_i b_i : \lambda_i \in [-1, 1],\ 1 \leqslant i \leqslant m\} = \sum_{i=1}^m [-b_i, b_i]$. 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.

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

Proof. We may assume that $\varepsilon = (2^k - 1)^{-1}$ for some positive integer k.

For $i \in [k]$, the following union of translated intervals is a $(2, \varepsilon)$-covering of $[-b, b]$:

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

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

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

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

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

Proof. We may assume that $\varepsilon = \left((4/3)^k - 1\right)^{-1}$ for some positive integer k.

For $\alpha \in [k]^m$ and $\delta \in \{\pm 1\}^m$, consider the following polytopes:

$$\bar{Q}(\alpha, \delta) =$$

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

For each facet direction $|a_i^T x| \leqslant b_i$, 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 $\{x \in \mathbb{R}^n \ : \ |a_i^T x| \leqslant (1+\varepsilon)b_i\}$. 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 $(1+\varepsilon)P$ and it is clear that P is contained in the union of the $\bar{Q}(\alpha, \delta)$.

We could stop here and have a $(2, \varepsilon)$-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

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

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 $(1+\varepsilon)P$, thus we have $2 \odot Q_x(\alpha, \delta) \subseteq (1+\varepsilon)P$. Thus, the union of all $\{\bar{Q}_x(\alpha, \delta)\}$ is a $(2, \varepsilon)$-covering for K using at most $2^m(\log_{4/3}(1/\varepsilon) + 1)^m$ symmetric convex bodies. □

Last in this section, we prove a lower bound on the $(2, \varepsilon)$-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. *Any $(2, \varepsilon)$-covering of the Euclidean unit ball B_2^n consists of at least $O(2^{-O(n)}(1/\varepsilon)^{n/2})$ convex bodies.*

Proof. Let $\{Q_i\}_{i=1}^N$ be a $(2, \varepsilon)$-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 $\langle p, c\rangle \geqslant 1 - \varepsilon$, that is, Q_i is contained in a small solid cap. Suppose by contradiction that $\langle p, c\rangle < 1 - \varepsilon$. By the definition of a $(2, \varepsilon)$-covering we need that $\|p + (p - c)\| \leqslant 1 + \varepsilon$. This implies $\langle p, p + (p - c)\rangle \leqslant 1 + \varepsilon$ and we obtain the following contradiction:

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

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

$$\begin{aligned}\langle p - c, p - c\rangle &= \langle p, p\rangle + \langle c, c\rangle + 2\langle p, -c\rangle \\ &\leqslant 1 + (1+\varepsilon)^2 + 2(\varepsilon - 1) \\ &\leqslant 5\varepsilon.\end{aligned}$$

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

3. $(2, \varepsilon)$-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, $\rho_K(\tau) : (0, 1) \to (0, 1)$, 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 $\rho_K(\tau) \leqslant \tau$, 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 $\|x + \tau y\|_K, \|x - \tau y\|_K \geqslant 1$, but we also have the upper bound of

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

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, $\|x \pm \tau y\|_K \leqslant \|x\|_K + \|\tau y\|_K$, alone yields. Still assuming $\rho_K(\tau) \leqslant \tau^2$ and letting $\varepsilon \in (0, 1)$, this means that all points $y \in K$ with $\|x - y\| \leqslant \sqrt{\varepsilon}$ 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 $\varepsilon \in (0, 1)$. Assume that the modulus of smoothness of K is bounded by*

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

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

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

centrally symmetric convex bodies.

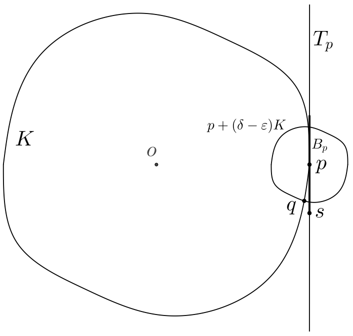

Figure 1. Proof of (2).

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

We first describe a $(2, 2\varepsilon)$-covering of K only in the neighborhood of a point and then, using a packing argument, we extend this construction to obtain a $(2, 2\varepsilon)$-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. $B_p := T_p \cap \{x : \|x - p\| \leqslant \delta\}$.

First, we show that

$$\text{bd}\,(K) \cap (p + (\delta - \varepsilon)K) \subseteq \text{conv}(0, B_p). \tag{2}$$

Indeed, let q be a point in $\text{bd}\,(K) \cap (p + (\delta - \varepsilon)K)$, and let L denote the two-dimensional linear plane spanned by p, q and the origin o, see Figure 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 $\operatorname{conv}(0, B_p)$. By the assumption on the modulus of smoothness 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,

$$\|s' - p\| \geqslant \delta - \varepsilon. \tag{3}$$

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 [MSW01, Proposition 31] that as a point moves along the curve $K \cap L$ starting at p and ending at $-p$, the distance (in the K-norm) of the moving point to p is increasing. Thus, by (3), the arc of $K \cap L$ between p and s' contains q, which yields that q is in the cone $\operatorname{conv}(0, B_p)$, proving (2).

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

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

Clearly, we have $\operatorname{conv}(0, B_p) \subseteq C_p$.

We may assume that ε is of the form $\varepsilon = \left(2^k - 1\right)^{-1}$, where k is a positive integer. For $i \in [k]$, consider the following slice of C_p:

$$C_p(i) = \left(B_p + [-(2^i - 1)\varepsilon p, -(2^{i-1} - 1)\varepsilon p]\right). \tag{4}$$

Clearly, $2 \odot C_p(i) \subseteq \widehat{C_p} := 2 \odot B_p + [\varepsilon p, -\frac{3}{2}p]$ and the centroid $c(C_p(i))$ is at $(1 - (\frac{3}{2}2^{i-1} - 1))\varepsilon p$ for each $i \in [k]$.

We claim that $\widehat{C_p} \subseteq (1 + 2\varepsilon)K$. Since $\delta \leqslant 1/4$ and $K = -K$, we have $2 \odot B_p - \frac{3}{2}p \subseteq K$. Thus, it suffices to check that $2 \odot B_p + \varepsilon p \subseteq (1 + 2\varepsilon)K$.

Let $x \in 2 \odot B_p + \varepsilon p$, i.e. $x = p + 2(z - p) + \varepsilon p$ for some $z \in B_p$. We will show that $\|p + 2(z - p)\| \leqslant 1 + 2\varepsilon$. 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 $\|p + 2(z - p)\|, \|p + 2(p - z)\| \geqslant 1$.

$\|2(z - p)\| \leqslant 2\delta = \frac{1}{2}\left(\frac{\varepsilon}{C}\right)^{1/q}$ and so by the assumption on the modulus of smoothness of K, we obtain

$$\|p + 2(z - p)\| \leqslant 2C\|2(z - p)\|^q + 1 \leqslant 1 + \varepsilon.$$

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

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

for each $i \in [k]$.

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

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

such points suffice.

Thus, we obtain a $(2, 2\varepsilon)$-covering for K by constructing C_{p_i} for each $i \in [N]$ and slicing each C_{p_i} as in (4). Finally, replacing ε by $\frac{\varepsilon}{2}$, we indeed get a $(2, \varepsilon)$-covering of K using $2^{O(n)}(\frac{C}{\varepsilon})^{n/q} \log\left(\frac{1}{\varepsilon}\right)$ convex bodies. □

Theorem 3.3 (Modulus of smoothness for ℓ_p spaces, [Lin63])**.** *We have*

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

These estimates on the modulus of smoothness for ℓ_p balls together with Theorem 3.2 imply the following.

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

4. Using $(2,\varepsilon)$-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 $(1+\varepsilon)$-approximate CVP$_K$, i.e. find a lattice vector $v \in \Lambda(A)$ such that $\|v-t\|_K \leqslant (1+\varepsilon)\min_{w\in\Lambda(A)}\|w-t\|_K$. $\|\cdot\|_K$ 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 homogenity, i.e. $\|x\|_K \neq \|-x\|_K$. We denote by b the encoding length of the relevant input: A, t, ε, etc.

In this section, we will first describe how a $(2,\varepsilon)$-covering for K using N convex bodies boosts any 2-CVP solver for general norms to a $(1+\varepsilon)$-CVP$_K$ solver at the expense of a factor $N2^{O(n)}\operatorname{poly}(b,n,\log(1/\varepsilon))$ in the running time. This algorithm, together with the construction of Propositions 2.5 and 2.6 directly implies a $(1+\varepsilon)$-CVP solver for polytopes and zonotopes with running time of $2^{O(n+m)}(\log(1/\varepsilon))^m\operatorname{poly}(b,n,\log(1/\varepsilon))$ 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 $(2,\varepsilon)$-covering for K containing p. This yields a randomized $(1+\varepsilon)$-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, Frieze and Kannan [DFK91], 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,

$$\|x\|_2 \leqslant \|x\|_K \leqslant n^{3/2}\|x\|_2. \tag{5}$$

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 [GLS88].

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 [DK16])**.** *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 $(1+\varepsilon)$-approximate minimizer to $\|y-x\|_K, x \in \Lambda(A)$, in time $O(\operatorname{poly}(n,b)2^{O(n)}(1+\frac{1}{\varepsilon})^n)$ and $O(\operatorname{poly}(n,b)2^n)$ space.*

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

Proof. Following Blömer and Naewe, we may multiply $\Lambda(A)$ and t by the least common multiple of the n^2 entries of A and the n entries of b. 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

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

By our assumption (5), we have

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

Let $\{Q_i + c_i\}_{i=1}^N$ be the given $(2, \varepsilon)$-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 $\|t - v\|_Q \leqslant 2$.

We want to find f such that $c_i + (1+\varepsilon)^f Q_i$ contains a lattice vector for some $i \in [N]$, but $c_i + (1+\varepsilon)^{f-1}Q_i$ contains no lattice vector for any $i \in [N]$. As in [EHN11], we apply a binary search for f.

(1) Initialize $L \leftarrow 0$, $U \leftarrow \left\lceil \log_{1+\varepsilon} n^{5/2}2^{(n^2+n)b} \right\rceil$ and $x = 0$

(2) While $U - L \geqslant 4$, do a binary search step:

  (a) For all $i \in [N]$, solve a 2-approximate $\mathrm{CVP}_{(1+\varepsilon)^{L+\lceil (U-L)/2\rceil}Q_i}$ problem with target $(1+\varepsilon)^{L+\lceil (U-L)/2\rceil}c_i + t$

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

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

(3) Return x.

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

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

contains no lattice vector, and so $\min_{v\in\Lambda(A)} \|v - t\|_K \geqslant (1+\varepsilon)^{L+\lceil (U-L)/2\rceil}$.

In the case a lattice vector is returned, then

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

since the Q_i are a $(2, \varepsilon)$-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:

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

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

$$\|x - t\|_K \leqslant (1+\varepsilon)^U \leqslant (1+\varepsilon)^{L+3} \leqslant (1+\varepsilon)^3 \min_{v\in\Lambda(A)} \|v - t\|_K \leqslant (1+7\varepsilon) \min_{v\in\Lambda(A)} \|v - t\|_K.$$

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

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

Proof. Run the algorithm in Theorem 4.2 for $\varepsilon/7$ in place of ε on a $(2,\varepsilon)$-covering of K constructed in the proof of Proposition 2.5 or 2.6. To avoid a space requirement depending on the number of convex bodies N required in the $(2,\varepsilon)$-covering for K, every time we call step $2(a)$ 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 $(2,\varepsilon)$-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 [DK16]. Since calculating deterministically the centroid is a hard problem and no efficient algorithms are known, see [Rad07], 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 $(2,\varepsilon)$-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 $\varepsilon > 0$. Then, in polynomial time, we can find at most $O(\log(1/\varepsilon))$ origin symmetric convex bodies $\{Q_i\}$ and translations $\{c_i\}$ such that for some constant $c > 0$:*

(1) For all i, $c_i + 2Q_i \subseteq (1+\varepsilon)K$.

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

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

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

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

If $\varepsilon \leqslant \left(\frac{1}{8C^{1/q}}\right)^{q/(q-1)}$, similar as in Theorem 3.2, we set $\delta = \frac{1}{4}\left(\frac{\varepsilon}{C}\right)^{1/q}$. We uniformly sample a point x from $(1+\delta/4)K$. Let $p = \frac{x}{\|x\|}$ and for $i \in [\log(1/\varepsilon)]$, consider the slices $C_p(i)$ of C_p as in (4) 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

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

In that case, $\left\|\frac{q}{\|q\|} - p\right\| \leqslant \delta/2 \leqslant \delta - \varepsilon$ and thus, C_p as in (4) 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

$$2^{-cn}C^{-n/q}\varepsilon^{n/q}$$

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 $(1+\varepsilon)$-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*

$$\rho_K(\tau) \leqslant C\tau^q, \text{ with } C, q > 1$$

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

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

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

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

We adapt the algorithm of Theorem 4.2:

1. Initialize $L \leftarrow 0$, $U \leftarrow \left\lceil \log_{1+\varepsilon} n^{5/2}2^{(n^2+n)b}\right\rceil$ and $x = 0$
2. While $U - L \geqslant 4$, do a binary search step:
   - (a) 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$_{(1+\varepsilon)^{L+\lceil (U-L)/2\rceil}Q_i}$ problem with target $(1+\varepsilon)^{L+\lceil (U-L)/2\rceil}c_i + t$. Repeat N times.
   - (b) If some lattice vector v is returned, update $U \leftarrow \lceil \log_{1+\varepsilon}\|v-t\|_K\rceil$ and $x \leftarrow v$.
   - (c) Otherwise, update $L \leftarrow L + \lceil (U-L)/2\rceil$
3. Return x.

Correctness of the algorithm follows from Theorem 4.2, provided step 2 runs correctly (i.e. correctly detects whether there is a lattice point or not with high probability) for all $O(\log(\frac{1}{\varepsilon})(\log(n)+\log(b)))$ 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 $p = 2^{-cn}C^{-n/q}(1/\varepsilon)^{n/q}$ or $(\frac{1}{8^qC})^{1/(q-1)}$ respectively, one of the convex bodies returned by one run of Theorem 4.5 contains v. Thus, if we were to repeat step 2(a) $n(2^{cn}C^{n/q}(1/\varepsilon)^{n/q} + (8^qC)^{1/(q-1)})$ times, with probability greater than $1-2^{-n}$, v is contained in one of the convex bodies returned and step 2 runs correctly. Since step 2 needs to run correctly each of the $O(\log(\frac{1}{\varepsilon})(\log(n)+\log(b)))$ iterations necessary to find the correct U and L, by the union bound, it is sufficient to set $N = O(n\log(\log(\frac{1}{\varepsilon})(\log(n)+\log(b)))2^{cn}C^{n/q}(1/\varepsilon)^{n/q} + (8^qC)^{1/(q-1)})$ 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 [Dad13, Theorem 4.1]. There, a deterministic algorithm is presented to build and iterate over an epsilon net in $2^{O(n)}(1/\varepsilon)^n$ time and $\mathrm{poly}(n)$ space. For symmetric convex bodies with modulus of smoothness bounded by $C\tau^q$, we may apply this result with $O\left(\varepsilon^{1/q}\right)$, as in Theorem 4.5, in place of ε to build a covering of size $O(\frac{1}{\varepsilon})^{n/q}$. 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, $\mathrm{vol}(K \cap -K) \geqslant \gamma^n\,\mathrm{vol}(K)$.

Then the result of Dadush and Kun (Theorem 4.1) still applies (see [DK16]), and it is straightforward to modify the above algorithm to obtain a $(1+\varepsilon)$-approximate CVP algorithm for $\|\cdot\|_K$ using $2^{O(n)}(\frac{1}{\gamma\varepsilon})^n$ calls to a 2-approximate CVP algorithm handling any symmetric norm, for instance the AKS based algorithm of Dadush [Dad12], resulting in an algorithm with time $O(\frac{1}{\gamma\varepsilon})^n$ and space $2^{O(n)}$. We essentially use Theorem 4.5 with $q=1$: we sample a point p in $(1+\varepsilon/3)K$ and output $\frac{\varepsilon}{3}(K\cap -K)$ and p. Thus, each point in K has probability greater or equal to $2^{-O(n)}(\frac{1}{\gamma\varepsilon})^n$ of being covered.

Acknowledgement

We would like to 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 the research was carried out while MN was a member of János Pach's chair of DCG at EPFL, Lausanne, which was supported by Swiss National Science Foundation Grants 200020-162884 and 200021-165977.

MV acknowledges support from the Swiss National Science Foundation within the project *Lattice Algorithms and Integer Programming (Nr. 200021-185030)* .

References

[AKS01] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*, pages 601–610, 2001.

[AKS02] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. Sampling short lattice vectors and the closest lattice vector problem. In *Proceedings of the 17th Annual IEEE Conference on Computational Complexity, Montréal, Québec, Canada, May 21-24, 2002*, pages 53–57, 2002.

[Aro95] Sanjeev Arora. *Probabilistic Checking of Proofs and Hardness of Approximation Problems.* PhD thesis, Berkeley, CA, USA, 1995. UMI Order No. GAX95-30468.

[AS18] Divesh Aggarwal and Noah Stephens-Davidowitz. Just take the average! An embarrassingly simple 2^n-time algorithm for SVP (and CVP). In *1st Symposium on Simplicity in Algorithms, SOSA 2018, January 7-10, 2018, New Orleans, LA, USA*, pages 12:1–12:19, 2018.

[BN09] Johannes Blömer and Stefanie Naewe. Sampling methods for shortest vectors, closest vectors and successive minima. *Theor. Comput. Sci.*, 410(18):1648–1665, 2009.

[Dad12] Daniel Dadush. A o(1/ε^2)^n – time sieving algorithm for approximate integer programming. In *LATIN 2012: Theoretical Informatics - 10th Latin American Symposium, Arequipa, Peru, April 16-20, 2012. Proceedings*, pages 207–218, 2012.

[Dad13] Daniel Dadush. A deterministic polynomial space construction for eps-nets under any norm, 2013. ArXiv:1311.6671.

[DFK91] Martin E. Dyer, Alan M. Frieze, and Ravi Kannan. A random polynomial time algorithm for approximating the volume of convex bodies. *J. ACM*, 38(1):1–17, 1991.

[DK16] Daniel Dadush and Gábor Kun. Lattice sparsification and the approximate closest vector problem. *Theory of Computing*, 12(1):1–34, 2016.

[DKRS03] Irit Dinur, Guy Kindler, Ran Raz, and Shmuel Safra. Approximating CVP to within almost-polynomial factors is NP-hard. *Combinatorica*, 23(2):205–243, 2003.

[EHN11] Friedrich Eisenbrand, Nicolai Hähnle, and Martin Niemeier. Covering cubes and the closest vector problem. In *Proceedings of the 27th ACM Symposium on Computational Geometry, Paris, France, June 13-15, 2011*, pages 417–423, 2011.

[GLS88] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*, volume 40. The Journal of the Operational Research Society, 01 1988.

[HRS19] Christoph Hunkenschröder, Gina Reuland, and Matthias Schymura. On compact representations of voronoi cells of lattices. In *Integer Programming and Combinatorial Optimization*

- *20th International Conference, IPCO 2019, Ann Arbor, MI, USA, May 22-24, 2019, Proceedings*, pages 261–274, 2019.

[Kan87] Ravi Kannan. Minkowski's convex body theorem and integer programming. *Math. Oper. Res.*, 12(3):415–440, 1987.

[Len83] Hendrik W. Lenstra. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8(4):538–548, 1983.

[Lin63] Joram Lindenstrauss. On the modulus of smoothness and divergent series in banach spaces. *Michigan Math. J.*, 10(3):241–252, 08 1963.

[MP00] Vitali Milman and Alain Pajor. Entropy and asymptotic geometry of non-symmetric convex bodies. *Adv. Math.*, 152(2):314–335, 2000.

[MSW01] Horst Martini, Konrad J. Swanepoel, and Gunter Weiß. The geometry of Minkowski spaces—a survey. I. *Expo. Math.*, 19(2):97–142, 2001.

[MV10] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. In *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, pages 351–358, 2010.

[Rad07] Luis Rademacher. Approximating the centroid is hard. In *Proceedings of the 23rd ACM Symposium on Computational Geometry, Gyeongju, South Korea, June 6-8, 2007*, pages 302–305, 2007.

[vEB81] P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. *Technical Report 81-04, Mathematische Instituut, University of Amsterdam*, 1981.

Department of Geometry, Eötvös University, Budapest, Hungary and EPFL, Lausanne, Switzerland
E-mail address: `marton.naszodi@math.elte.hu`

Institute for Mathematics, École polytechnique fédérale de Lausanne, Lausanne, Switzerland
E-mail address: `moritz.venzin@epfl.ch`