Economical Convex Coverings and Applications*

Sunil Arya†
Department of Computer Science and Engineering
The Hong Kong University of Science and Technology, Hong Kong
arya@cse.ust.hk

Guilherme D. da Fonseca*
Aix-Marseille Université and LIS Lab, France
guilherme.fonseca@lis-lab.fr

David M. Mount*
Department of Computer Science and Institute for Advanced Computer Studies
University of Maryland, College Park, Maryland
mount@umd.edu

Abstract

Coverings of convex bodies have emerged as a central component in the design of efficient solutions to approximation problems involving convex bodies. Intuitively, given a convex body K and $\varepsilon > 0$, a *covering* is a collection of convex bodies whose union covers K such that a constant factor expansion of each body lies within an ε expansion of K. Coverings have been employed in many applications, such as approximations for diameter, width, and ε-kernels of point sets, approximate nearest neighbor searching, polytope approximations with low combinatorial complexity, and approximations to the Closest Vector Problem (CVP).

It is known how to construct coverings of size $n^{O(n)}/\varepsilon^{(n-1)/2}$ for general convex bodies in $\mathbb{R}^n$. In special cases, such as when the convex body is the ℓ_p unit ball, this bound has been improved to $2^{O(n)}/\varepsilon^{(n-1)/2}$. This raises the question of whether such a bound generally holds. In this paper we answer the question in the affirmative.

We demonstrate the power and versatility of our coverings by applying them to the problem of approximating a convex body by a polytope, where the error is measured through the Banach-Mazur metric. Given a well-centered convex body K and an approximation parameter $\varepsilon > 0$, we show that there exists a polytope P consisting of $2^{O(n)}/\varepsilon^{(n-1)/2}$ vertices (facets) such that $K \subset P \subset K(1+\varepsilon)$. This bound is optimal in the worst case up to factors of $2^{O(n)}$. (This bound has been established recently using different techniques, but our approach is arguably simpler and more elegant.) As an additional consequence, we obtain the fastest $(1+\varepsilon)$-approximate CVP algorithm that works in any norm, with a running time of $2^{O(n)}/\varepsilon^{(n-1)/2}$ up to polynomial factors in the input size, and we obtain the fastest $(1+\varepsilon)$-approximation algorithm for integer programming. We also present a framework for constructing coverings of optimal size for any convex body (up to factors of $2^{O(n)}$).

*An earlier version of this paper appeared in the *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms* (SODA), pp. 1834–1861, 2023.

†Research supported by the Research Grants Council of Hong Kong, China under project numbers 16213219 and 16214721. The work of David Mount was supported by NSF grant CCF–1618866. The work of Guilherme da Fonseca was supported by the French ANR PRC grant ADDS (ANR-19-CE48-0005).

Keywords: Approximation algorithms, high dimensional geometry, convex coverings, Banach-Mazur metric, lattice algorithms, closest vector problem, Macbeath regions

1 Introduction

Convex bodies are of fundamental importance in mathematics and computer science, and given the high complexity of exact representations, concise approximate representations are essential to many applications. There are a number of ways to define the distance between two convex bodies (see, e.g., [20]), and each gives rise to a different notion of approximation. While Hausdorff distance is commonly studied, it is not sensitive to the shape of the convex body. In this paper we will consider a common linear-invariant distance, called the Banach-Mazur distance.

Given two convex bodies X and Y in real n-dimensional space, $\mathbb{R}^n$, both of which contain the origin in their interiors, their *Banach-Mazur distance*, denoted $\text{dist}_{\text{BM}}(X, Y)$, is defined to be the minimum value of $\ln \lambda$ such that there exists a linear transformation T such that $TX \subseteq Y \subseteq \lambda \cdot TX$. Given $\delta > 0$, we say that Y is an *Banach-Mazur δ-approximation* of X if $\text{dist}_{\text{BM}}(X, Y) \leq \delta$. T will be the identity transformation in our constructions, and thus, given a convex body K in $\mathbb{R}^n$ and $\varepsilon > 0$, we seek a convex polytope P such that $K \subseteq P \subseteq (1 + \varepsilon)K$. This implies that $\text{dist}_{BM}(K, P) \leq \ln(1 + \varepsilon)$, which is approximately ε for small ε. The scaling is taking place about the origin, and it is standard practice to assume that K is well-centered in the sense that the origin lies within K and is not too close to K's boundary. (See Section 2.2 for the formal definition.) Unlike Hausdorff, the Banach-Mazur measure has the desirable property of being sensitive to K's shape, being more accurate where K is narrower and less accurate where K is wider.

The principal question is, given n and $\varepsilon > 0$, what is the minimum number of vertices (or facets) needed to ε-approximate any convex body K in $\mathbb{R}^n$ by a polytope in the above sense. This problem has been well studied. Existing bounds hold under the assumption that K is well-centered. We say that a bound is *nonuniform* if it holds for all $\varepsilon \leq \varepsilon_0$, where ε_0 depends on K. Typical nonuniform bounds assume that K is smooth, and the value of ε_0 depends on K's smoothness. Our focus will be on uniform bounds, where ε_0 does not depend on K.

Dudley [28] and Bronshtein and Ivanov [23] provided uniform bounds in the Hausdorff context, but their results can be recast under Banach-Mazur, where they imply the existence of an approximating polytope with $n^{O(n)}/\varepsilon^{(n-1)/2}$ vertices (facets). For smooth convex bodies, Böröczky [20, 38] established a nonuniform bound of $2^{O(n)}/\varepsilon^{(n-1)/2}$. Barvinok [17] improved the bound in the uniform setting for symmetric convex bodies. Ignoring a factor that is polylogarithmic in $1/\varepsilon$, his bound is $2^{O(n)}/\varepsilon^{n/2}$. Finally, Naszódi, Nazarov, and Ryabogin obtained a worst-case optimal approximation of size $2^{O(n)}/\varepsilon^{(n-1)/2}$ [52]. Their bound is uniform and holds for general convex bodies.

The main result of this paper is an alternative asymptotically optimal construction of an ε-approximation of a convex body K in $\mathbb{R}^n$ in the Banach-Mazur setting. Our construction is superior to that of [52] in two ways. First, while the construction presented in [52] is very clever, it involves the combination of a number of technical elements (transforming the body to standard position, rounding it, computing a Bronshtein-Ivanov net, and filtering to reduce the sample size). In contrast, ours is quite simple. We employ a greedy process that samples points from K's interior, and the final approximation is just the convex hull of these points. Second, our construction is more

powerful in that it provides an additional covering structure for K. Each sample point is associated with a centrally symmetric convex body, and together these bodies form a cover of K such that their union lies within the expansion $(1+\varepsilon)K$. As a direct consequence of this additional structure, we obtain the fastest approximation algorithm to date for the closest vector problem (CVP) that operates in any norm.

1.1 Our Results

Throughout, we assume that K is a full-dimensional convex body in $\mathbb{R}^n$, which is well-centered about the origin. There are a number of notions of centrality that suffice for our purposes (see Section 2.2 for formal definitions). Our first result involves the existence of concise coverings. Given a convex body K that contains the origin in its interior and reals $c \geq 1$ and $\varepsilon > 0$, a (c, ε)-*covering* of K is a collection $\mathcal{Q}$ of bodies whose union covers K such that a factor-c expansion of each $Q \in \mathcal{Q}$ about its centroid lies within $(1+\varepsilon)K$ (see Figure 1). Coverings have emerged as an important tool in convex approximation. They have been applied to several problems in the field of computational geometry, including combinatorial complexity [6, 8, 10], approximate nearest neighbor searching [9], and computing the diameter and ε-kernels [7].

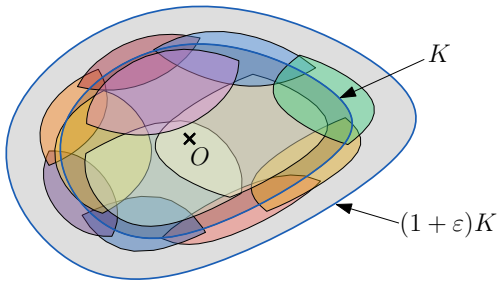


Figure 1: A $(2, \varepsilon)$-covering.

Given a convex body in $\mathbb{R}^n$, constant $c \geq 1$ and parameter $\varepsilon > 0$, what is the minimum size of a (c, ε)-covering as a function of n and ε? Abdelkader and Mount considered the problem in spaces of constant dimension [1]. They did not analyze their bounds for the high-dimensional case, but based on results from [9], it can be shown that their results yield an upper bound of $n^{O(n)}/\varepsilon^{(n-1)/2}$ in $\mathbb{R}^n$. A number of special cases have been explored in the high dimensional case. Naszódi and Venzin demonstrated the existence of $(2, \varepsilon)$-coverings of size $2^{O(n)}/\varepsilon^{n/2}$ when K is an ℓ_p ball for any fixed $p \geq 2$ [53]. For the ℓ_∞ ball, Eisenbrand, Hähnle, and Niemeier showed the existence of $(2, \varepsilon)$-coverings of size $2^{O(n)}/\log^n(1/\varepsilon)$, consisting of axis-parallel rectangles [32]. They also presented a nearly matching lower bound of $2^{-O(n)}/\log^n(1/\varepsilon)$, even when the covering consisted of parallelepipeds.

In this paper we establish the following bound on the size of (c, ε)-coverings, which holds for any well-centered convex body in $\mathbb{R}^n$.

Theorem 1. *Let $0 < \varepsilon \leq 1$ be a real parameter and $c \geq 2$ be a constant. Let $K \subseteq \mathbb{R}^n$ be a well-centered convex body. Then there is a (c, ε)-covering for K consisting of at most $2^{O(n)}/\varepsilon^{(n-1)/2}$ centrally symmetric convex bodies.*

It is not difficult to prove a lower bound of $2^{-O(n)}/\varepsilon^{(n-1)/2}$ on the size of any $(2, \varepsilon)$-covering for

Euclidean balls (see, e.g., Naszódi and Venzin [53]). Therefore, the above bound is optimal with respect to ε-dependencies. In Section 4.1 (Theorem 4), we prove that for any constant $c \geq 2$, our construction is in fact instance optimal to within a factor of $2^{O(n)}$. This means that for any well-centered convex body K, our covering exceeds the size of any (c, ε)-covering for K by such a factor. In Section 6.2, we present a randomized algorithm that constructs a slightly larger covering (by a factor of $\log(1/\varepsilon)$). Following standard convention, our constructions assume that access to K is provided by a weak membership oracle (defined in Section 6).

We present a number of applications of this result. First, in Section 5 we show that the convex hull of the center points of the covering elements yields an approximation in the Banach-Mazur metric.

Theorem 2. *Given a well-centered convex body K and an approximation parameter $\varepsilon > 0$, there exists a polytope P consisting of $2^{O(n)}/\varepsilon^{(n-1)/2}$ vertices (facets) such that $K \subset P \subset K(1+\varepsilon)$.*

There are also applications to lattice problems. In the *Closest Vector Problem* (CVP), an n-dimensional lattice L in $\mathbb{R}^n$ is given (that is, the set of integer linear combinations of n basis vectors) together with a target vector $t \in \mathbb{R}^n$. The problem is to return a vector in L closest to t under some given norm. This problem has applications to cryptography [41, 55, 56], integer programming [25, 26, 45], and factoring polynomials over the rationals [44], among several other problems. The problem is NP-hard for any ℓ_p norm [34] and cannot be solved exactly in $2^{(1-\gamma)n}$ time for constant $\gamma > 0$, under certain conditional hardness assumptions [18].

This problem has a considerable history. The first solution proposed to the CVP under the ℓ_∞ norm takes $2^{O(n^3)}$ time through integer linear programming [45], which was later improved to $n^{O(n)}$ [42]. For the ℓ_2 norm, Micciancio and Voulgaris presented an algorithm that runs in single exponential $2^{O(n)}$ time [49], and currently the fastest algorithm for exact Euclidean CVP is by Aggarwal, Dadush, and Stephens-Davidowitz [3] and runs in $2^{n+o(n)}$ time. However, solving the CVP problem exactly in single exponential time for norms other than Euclidean remains an open problem. (For additional information, see [40].) Dadush, Peikert, and Vempala [26] considered CVP and the related Shortest Vector Problem (SVP) in the context of (possibly asymmetric) norms defined by convex bodies. Their work demonstrated a rich connection between lattice algorithms and convex geometry.

In the approximate version of the CVP problem, denoted $(1+\varepsilon)$-*CVP*, we are also given a parameter $\varepsilon > 0$, and the goal is to find a lattice vector whose distance to t is at most $1+\varepsilon$ times the optimum. CVP is NP-hard to approximate [5, 27] and conditional hardness results show that for $p \geq 1$ CVP in ℓ_p is hard to approximate in $2^{(1-\gamma)n}$ time for constant $\gamma > 0$, except when p is even [2].

The randomized sieving approach of Ajtai, Kumar, and Sivakumar [4] was extended to approximate CVP for ℓ_p norms by Blömer and Naewe [19] and to the general case of well-centered norms by Dadush [24]. These algorithms run in time and space $2^{O(n)}/\varepsilon^{2n}$. Building on the Voronoi cell approach [26, 49], Dadush and Kun [25] presented deterministic algorithms that improved the running time to $2^{O(n)}/\varepsilon^n$ and space to $\widetilde{O}(2^n)$.

Eisenbrand, Hähnle, and Niemeier [32] and Naszódi and Venzin [53] have explored the use of (c, ε)-coverings of the unit ball in the norm to obtain efficient algorithms for approximate CVP by "boosting" a weak constant-factor approximation to a strong $(1+\varepsilon)$-approximation. By exploiting the unique properties of hypercubes, Eisenbrand *et al.* [32] improved the running time for the ℓ_∞

norm to $2^{O(n)}\log^n(1/\varepsilon)$ time. Naszódi and Venzin [53] extended this approach to ℓ_p norms. The running time of their algorithm is $2^{O(n)}/\varepsilon^{n/2}$ for $p \geq 2$ and $2^{O(n)}/\varepsilon^{n/p}$ for $1 \leq p \leq 2$. The constants in the $2^{O(n)}$ term in the running time depend on p.

By applying our covering within existing algorithms, we obtain the fastest algorithm to date for $(1+\varepsilon)$-approximate CVP that operates in any norm. The algorithm is randomized and runs in single exponential time, $2^{O(n)}/\varepsilon^{(n-1)/2}$. (Following standard practice, we ignore factors that are polynomial in the input size.) The result is stated formally below.

Theorem 3. *There is a randomized algorithm that, given any well-centered convex body K and lattice L, solves the $(1+\varepsilon)$-CVP problem in the norm defined by K, in $2^{O(n)}/\varepsilon^{(n-1)/2}$-time and $O(2^n)$-space, with probability at least $1-2^{-n}$.*

Finally, through a reduction from approximate CVP to approximate integer programming (IP) due to Dadush [24], we present a randomized algorithm for approximate IP (see Theorem 5 in Section 6.3).

1.2 Techniques

As mentioned above, coverings are a powerful tool in obtaining efficient solutions to approximation problems involving convex bodies. The fundamental problem tackled here involves the sizes of (c,ε)-coverings for general convex bodies in $\mathbb{R}^n$ and especially the dependencies on ε. Our approach employs a classical concept from convex geometry, called a *Macbeath region* [46]. Given a convex body K and a point $x \in K$, the Macbeath region $M_K(x)$ is the largest centrally symmetric body centered at x and contained in K (see Figure 2(a)). Macbeath regions have found numerous uses in the theory of convex sets and the geometry of numbers (see Bárány [15] for an excellent survey). They have also been applied to several problems in the field of computational geometry, including lower bounds [12, 13, 22], combinatorial complexity [6, 8, 10, 29, 51], approximate nearest neighbor searching [9], and computing the diameter and ε-kernels [7].

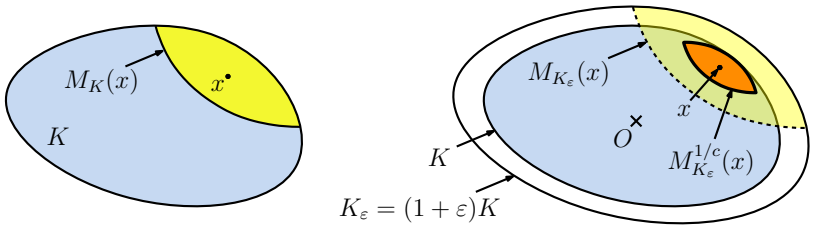


Figure 2: (a) A Macbeath region and (b) a covering element derived from a shrunken Macbeath region.

In the context of (c,ε)-coverings, the obvious (and indeed maximal) choice for a covering element centered at any point x is to take the Macbeath region centered at x with respect to the expanded body $K_\varepsilon = (1+\varepsilon)K$, and then scale it by a factor of $\frac{1}{c}$ about x (see Figure 2(b)). The construction and analysis of such Macbeath-based coverings is among the principal contributions of this paper. In their work on the economical cap cover, Bárány and Larman observed how Macbeath regions serve as an efficient agent for covering the region near the boundary of a convex body [16]. While

Macbeath regions can be quite elongated, especially near the body's boundary, they behave in many respects like fixed-radius balls in a metric space. (Vernicos and Walsh proved that shrunken Macbeath regions are similar in shape to fixed-radius balls in the Hilbert geometry induced by K [1, 63].) This leads to a very simple covering construction based on computing a maximal set of points such that the suitably shrunken Macbeath regions centered at these points are pairwise disjoint. The covering is then constructed by uniformly increasing the scale factor so the resulting Macbeath regions cover K.

Two challenges arise in implementing and analyzing this construction. The first is that of how to compute these Macbeath regions efficiently. The second is proving that this simple construction yields the desired bound on the size of the covering. A natural approach to the latter is a packing argument based on volume considerations. Unfortunately, this fails because Macbeath regions may have very small volume. Our approach for dealing with small Macbeath regions is to exploit a Mahler-like reciprocal property in the volumes of the Macbeath regions in the original body K and its polar, K^* (see Section 2.2 for definitions). In the low-dimensional setting, the analysis exploits a correspondence between caps in K and K^*, such that the volumes of these caps have a reciprocal relationship (see, e.g., [6]). As a consequence, for each Macbeath region in K of small volume, there is a Macbeath region in K^* of large volume. Thus, by randomly sampling in both K and K^*, it is possible to hit all the Macbeath regions.

Generalizing this to the high-dimensional setting involves overcoming a number of technical difficulties. A straightforward generalization of the methods of [6] yields a covering of size $n^{O(n)}/\varepsilon^{(n-1)/2}$. A critical step in the analysis involves relating the volumes of two $(n-1)$-dimensional convex bodies that arise by projecting caps and dual caps. In earlier works, where the dimension was assumed to be a constant, a crude bound sufficed. But in the high-dimensional setting, it is essential to avoid factors that depend on the dimension. A key insight of this paper is that it is possible to avoid these factors through the use of the difference body. (See Lemma 3.1 in Section 3.1.) Through the use of this more refined geometric analysis, we establish this Mahler-like relationship in Sections 3 (particularly Lemmas 3.3 and 3.4). We apply this in Section 4.2 to obtain our bounds on the size of the covering. In Section 5 we show how this leads to an ε-approximation in the Banach-Mazur measure. The sampling process is described in Section 6 along with applications.

2 Preliminaries

In this section, we introduce terminology and notation, which will be used throughout the paper. This section can be skipped on first reading (moving directly to Section 3).

2.1 Lengths and Measures

Given vectors $u, v \in \mathbb{R}^n$, let $\langle u, v\rangle$ denote their dot product, and let $\|v\| = \sqrt{\langle v, v\rangle}$ denote v's Euclidean length. Throughout, we will use the terms *point* and *vector* interchangeably. Given points $p, q \in \mathbb{R}^n$, let $\|pq\| = \|p - q\|$ denote the Euclidean distance between them. Let $\mathrm{vol}(\cdot)$ and $\mathrm{area}(\cdot)$ denote the n-dimensional and $(n-1)$-dimensional Lebesgue measures, respectively.

Throughout, $K \subseteq \mathbb{R}^n$ will denote a full-dimensional compact convex body with the origin O in its interior. Let $\|x\|_K = \inf\{s \geq 0 : x \in sK\}$ denote K's associated Minkowski functional, or *gauge function*. If K is centrally symmetric, its gauge function defines a norm, but we will abuse

notation and use the term "norm" even when K is not centrally symmetric. Given $\varepsilon > 0$, define $K_\varepsilon = (1+\varepsilon)K$ to be a uniform scaling of K by $1+\varepsilon$.

Given a convex body $K \subseteq \mathbb{R}^n$, its *difference body*, denoted $\Delta(K)$, is defined to be the Minkowski sum $K \oplus -K$. The difference body is convex and centrally symmetric and satisfies the following property.

Lemma 2.1 (Rogers and Shephard [57]). *Given a convex body $K \subseteq \mathbb{R}^n$, $\mathrm{vol}(\Delta(K)) \leq 4^n \,\mathrm{vol}(K)$.*

2.2 Polarity and Centrality Properties

Given a bounded convex body $K \subseteq \mathbb{R}^n$ that contains the origin O in its interior, define its *polar*, denoted K^*, to be the convex set

$$K^* \;=\; \{u \,:\, \langle u, v\rangle \leq 1, \text{ for all } v \in K\}.$$

The polar enjoys many useful properties (see, e.g., Eggleston [31]). For example, it is well known that K^* is bounded and $(K^*)^* = K$. Further, if K_1 and K_2 are two convex bodies both containing the origin such that $K_1 \subseteq K_2$, then $K_2^* \subseteq K_1^*$.

Given a nonzero vector $v \in \mathbb{R}^n$, we define its "polar" v^* to be the hyperplane that is orthogonal to v and at distance $1/\|v\|$ from the origin, on the same side of the origin as v. The polar of a hyperplane is defined as the inverse of this mapping. We may equivalently define K^* as the intersection of the closed halfspaces that contain the origin, bounded by the hyperplanes v^*, for all $v \in K$.

Given a convex body $K \subseteq \mathbb{R}^n$, there are many ways to characterize the property that K is centered about the origin [39, 61]. In this section we explore a few relevant measures of centrality.

First, define K's *Mahler volume* to be the product $\mathrm{vol}(K) \cdot \mathrm{vol}(K^*)$. The Mahler volume is well studied (see, e.g. [47, 59, 60]). It is invariant under linear transformations, and it depends on the location of the origin within K. In the following definitions, any fixed constant may be used in the $O(n)$ term.

Santaló property: The Mahler volume of K is at most $2^{O(n)} \cdot \omega_n^2$, where ω_n denotes the volume of the n-dimensional unit Euclidean ball ($\omega_n = \pi^{n/2}/\Gamma\left(\frac{n}{2}+1\right)$).

Winternitz property: For any hyperplane passing through the origin, the ratio of the volume of the portion of K on each side of the hyperplane to the volume of K is at least $2^{-O(n)}$.

Kovner-Besicovitch property: The ratio of the volume of $K \cap -K$ to the volume of K is at least $2^{-O(n)}$.

Following Dadush, Peikert, and Vempala [26], we say that K is *well-centered* if it satisfies the Kovner-Besicovitch property. Generally, K is *well-centered* about a point x if $K - x$ is well-centered. For our purposes, however, any of the above can be used, as shown in the following lemma.

Lemma 2.2. *The three centrality properties (Santaló, Winternitz, and Kovner-Besicovitch) are equivalent in the sense that a convex body $K \subseteq \mathbb{R}^n$ that satisfies any one of them satisfies the other two subject to a change in the $2^{O(n)}$ factor. Further, if the origin coincides with K's centroid, these properties are all satisfied.*

Let us first introduce some notation. Given a hyperplane h, let h^+ and h^- denote its two halfspaces. Given $0 < \delta < \frac{1}{2}$, let h be a hyperplane that intersects K such that $\text{vol}(K \cap h^+) = \delta \cdot \text{vol}(K)$. Define the *$\delta$-floating body*, denoted K_δ, to be the intersection of halfspaces h^- for all such hyperplanes h. For $t > 0$, define the *t-Santaló region* $S(K, t) \subseteq K$ to be the set of points $x \in K$ such that the Mahler volume of K with respect to x is at most $t\,\omega_n^2$, where ω_n denotes the volume of the n-dimensional unit Euclidean ball. Both the floating body and the Santaló region (when nonempty) are convex subsets of K, and Meyer and Werner showed that they satisfy the following property.

Lemma 2.3 (Meyer and Werner [48])**.** *For all $0 < \delta < \frac{1}{2}$, $K_\delta \subseteq S(K, t)$, where $t = 1/(4\delta(1-\delta))$.*

We also need the following result by Milman and Pajor [50] (Remark 4 following Corollary 3), which implies that if K satisfies Santaló, then it satisfies Kovner-Besicovitch.

Lemma 2.4 (Milman and Pajor [50])**.** *Let K be a convex body with the origin O in its interior such that $\text{vol}(K) \cdot \text{vol}(K^*) \leq s\, w_n^2$, where s is a parameter. Then $\text{vol}(K \cap -K)/\text{vol}(K) \geq 2^{-O(n)}/s$.*

We are now ready to prove Lemma 2.2.

Proof. (of Lemma 2.2) First, suppose that K satisfies Kovner-Besicovitch, that is, $\text{vol}(K \cap -K) \geq 2^{-O(n)} \cdot \text{vol}(K)$. Consider any hyperplane h passing through the origin. As $K \cap -K$ is centrally symmetric, half of this body lies on each side of h. Thus, the volume of the portion of K on either side of h is at least $2^{-O(n)} \cdot \text{vol}(K)$, and so K satisfies the Winternitz property.

Next, suppose that K satisfies Winternitz. Observe that any point outside the floating body K_δ is contained in a halfspace h^+ such that $\text{vol}(K \cap h^+) \leq \delta \cdot \text{vol}(K)$. By Winternitz, all halfspaces containing the origin have volume at least $2^{-O(n)} \cdot \text{vol}(K)$, and so the origin is contained within the floating body K_δ for $\delta = 2^{-O(n)}$. It follows from Lemma 2.3 that the origin lies within the Santaló region $S(K, t)$ for some $t = 2^{O(n)}$. Thus, K satisfies the Santaló property.

Finally, if K satisfies Santaló, then it follows from Lemma 2.4 that it satisfies the Kovner-Besicovitch property. This establishes the equivalence of the three centrality properties.

Milman and Pajor [50] (Corollary 3) showed that if the origin coincides with K's centroid, then K satisfies Kovner-Besicovitch, implying that it satisfies the other properties as well. □

Lower bounds on the Mahler volume have also been extensively studied [21, 43, 54]. Recalling the value of ω_n from the Santaló property, the following lower bound holds irrespective of the location of the origin within a convex body [21].

Lemma 2.5. *Given a convex body $K \subseteq \mathbb{R}^n$ whose interior contains the origin,* $\text{vol}(K) \cdot \text{vol}(K^*) \geq 2^{-O(n)} \cdot \omega_n^2$.

2.3 Caps, Rays, and Relative Measures

Consider a compact convex body K in n-dimensional space $\mathbb{R}^n$ with the origin O in its interior. A *cap* C of K is defined to be the nonempty intersection of K with a halfspace. Letting h_1 denote a hyperplane that does not pass through the origin, let $\text{cap}_K(h_1)$ denote the cap resulting by intersecting K with the halfspace bounded by h_1 that does not contain the origin (see Figure 3(a)). Define the *base* of C, denoted $\text{base}(C)$, to be $h_1 \cap K$. Letting h_0 denote a supporting hyperplane for K and C parallel to h_1, define an *apex* of C to be any point of $h_0 \cap K$.

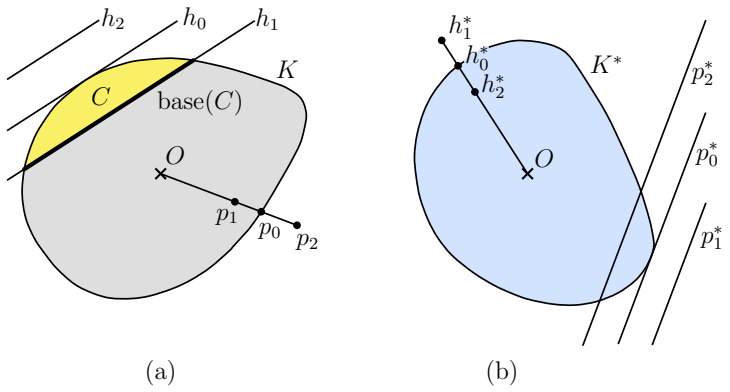


Figure 3: Convex body K and polar K^* with definitions used for width and ray.

We define the *absolute width* of cap C to be $\text{dist}(h_1, h_0)$. When a cap does not contain the origin, it will be convenient to define the *relative width* of C, denoted $\text{wid}_K(C)$, to be the ratio $\text{dist}(h_1, h_0)/\text{dist}(O, h_0)$. We extend the notion of width to hyperplanes by defining $\text{wid}_K(h_1) = \text{wid}_K(\text{cap}_K(h_1))$. Observe that as a hyperplane is translated from a supporting hyperplane to the origin, the relative width of its cap ranges from 0 to a limiting value of 1.

We also characterize the closeness of a point to the boundary in both absolute and relative terms. Given a point $p_1 \in K$, let p_0 denote the point of intersection of the ray Op_1 with the boundary of K. Define the *absolute ray distance* of p_1 to be $\|p_1p_0\|$, and define the *relative ray distance* of p_1, denoted $\text{ray}_K(p_1)$, to be the ratio $\|p_1p_0\|/\|Op_0\|$. Relative widths and relative ray distances are both affine invariants, and unless otherwise specified, references to widths and ray distances will be understood to be in the relative sense.

We can also define volumes in a manner that is affine invariant. Recall that $\text{vol}(\cdot)$ denotes the standard Lebesgue volume measure. For any region $\Lambda \subseteq K$, define the *relative volume* of Λ with respect to K, denoted $\text{vol}_K(\Lambda)$, to be $\text{vol}(\Lambda)/\text{vol}(K)$.

With the aid of the polar transformation we can extend the concepts of width and ray distance to objects lying outside of K. Consider a hyperplane h_2 parallel to h_1 that lies beyond the supporting hyperplane h_0 (see Figure 3(a)). It follows that $h_2^* \in K^*$, and we define $\text{wid}_K(h_2) = \text{ray}_{K^*}(h_2^*)$ (see Figure 3(b)). Similarly, for a point $p_2 \notin K$ that lies along the ray Op_1, it follows that the hyperplane p_2^* intersects K^*, and we define $\text{ray}_K(p_2) = \text{wid}_{K^*}(p_2^*)$. By properties of the polar transformation, it is easy to see that $\text{wid}_K(h_2) = \text{dist}(h_0, h_2)/\text{dist}(O, h_2)$. Similarly, $\text{ray}_K(p_2) = \|p_0p_2\|/\|Op_2\|$. Henceforth, we will omit references to K when it is clear from context.

Some of our results apply only when we are sufficiently close to the boundary of K. Given $0 \leq \alpha \leq 1$, we say that a cap C is *α-shallow* if $\text{wid}(C) \leq \alpha$, and we say that a point p is *α-shallow* if $\text{ray}(p) \leq \alpha$. We will simply say *shallow* to mean α-shallow, where α is a sufficiently small constant.

Given any cap C and a real $\lambda > 0$, we define its λ-expansion, denoted C^λ, to be the cap of K cut by a hyperplane parallel to the base of C such that the absolute width of C^λ is λ times the absolute width of C. (Note that if the expansion of a cap is large enough it may be the same as K.)

We now present a number of useful technical results on ray distances and cap widths in both their

absolute and relative forms.

Lemma 2.6. *Let C be a cap of K that does not contain the origin and let p be a point in C. Then* $\text{ray}(p) \leq \text{wid}(C)$.

Proof. Let h be the hyperplane passing through the base of C, and let h_0 be the supporting hyperplane of K parallel to h at C's apex. Let q, p_0, and q_0 denote the points of intersection of the ray Op with h, ∂K, and h_0, respectively. Since $p \in C$, the order of these points along the ray is $\langle O, q, p, p_0, q_0 \rangle$. By considering the hyperplanes parallel to h passing through these points, we have

$$\text{ray}(p) = \frac{\|pp_0\|}{\|Op_0\|} \leq \frac{\|qp_0\|}{\|Op_0\|} \leq \frac{\|qp_0\| + \|p_0q_0\|}{\|Op_0\| + \|p_0q_0\|} = \frac{\|qq_0\|}{\|Oq_0\|} = \frac{\text{dist}(h, h_0)}{\text{dist}(O, h_0)} = \text{wid}(C). \quad \square$$

There are two natural ways to associate a cap with any point $p \in K$. The first is the *minimum volume cap*, which is any cap whose base passes through p of minimum volume among all such caps. For the second, assume that $p \neq O$, and let p_0 denote the point of intersection of the ray Op with the boundary of K. Let h_0 be any supporting hyperplane of K at p_0. Take the cap C induced by a hyperplane parallel to h_0 passing through p. As shown in the following lemma this is the cap of minimum width containing p.

Lemma 2.7. *For any $p \in K \setminus \{O\}$, consider the cap C defined above. Then* $\text{wid}(C) = \text{ray}(p)$ *and further, C has the minimum width over all caps that contain p.*

Proof. Let h denote the hyperplane passing through p parallel to h_0 (defined above). By similar triangles, we have

$$\text{wid}(C) = \frac{\text{dist}(h, h_0)}{\text{dist}(O, h_0)} = \frac{\|pp_0\|}{\|Op_0\|} = \text{ray}(p).$$

By Lemma 2.6, for any cap C' that contains p, $\text{ray}(p) \leq \text{wid}(C')$, and hence $\text{wid}(C) \leq \text{wid}(C')$. $\square$

The following lemma gives a simple lower and upper bound on the absolute volume of a cap.

Lemma 2.8. *Let C be a $\frac{1}{2}$-shallow cap, let $a = \text{area}(\text{base}(C))$, and let w denote C's absolute width. Then $aw/n \leq \text{vol}(C) \leq 2^{n-1}aw$.*

Proof. Let p be the apex of C and $\text{base}(C)$ denote its base. Let $P = \text{conv}(\text{base}(C) \cup \{p\})$. Clearly, $P \subseteq C$ and $\text{vol}(P) = aw/n$, which yields the lower bound. To see the upper bound, observe that C lies within the generalized infinite cone whose apex is O and base is $\text{base}(C)$. Because $\text{wid}(C) \leq \frac{1}{2}$, it follows that the area of any slice of C cut by a hyperplane parallel to $\text{base}(C)$ exceeds the area of $\text{base}(C)$ by a factor of at most 2^{n-1}. The upper bound follows from elementary geometry. $\square$

An easy consequence of convexity is that, for $\lambda \geq 1$, C^λ is a subset of the region obtained by scaling C by a factor of λ about its apex. This implies the following lemma.

Lemma 2.9. *Given any cap C and a real $\lambda \geq 1$,* $\text{vol}(C^\lambda) \leq \lambda^n \, \text{vol}(C)$.

Another consequence of convexity is that containment of caps is preserved under expansion. This is a straightforward adaptation of Lemma 4.4 in [8].

Lemma 2.10. *Given two caps $C_1 \subseteq C_2$ and a real $\lambda \geq 1$, $C_1^\lambda \subseteq C_2^\lambda$.*

The following lemma is a technical result, which shows that if a ray hits the interior of the base of a cap of width at least ε, then it hits the interior of the base of a cap of width exactly ε that is contained in the original.

Lemma 2.11. *Let $0 < \varepsilon < 1$, and let $K \subseteq \mathbb{R}^n$ be a convex body containing the origin in its interior. Let r be a ray shot from the origin, and let D be a cap of K of width at least ε such that ray r intersects the interior of its base. Then there exists a cap $E \subseteq D$ of width ε such that ray r intersects the interior of its base.*

Proof. Let p be the point of intersection of ray r with the boundary of K. Let $F \subseteq D$ be the cap whose base passes through p and is parallel to the base of D. We now consider two cases.

If the width of cap F is less than ε, then we let E be the cap of width ε obtained by translating the base of F parallel to itself (towards the base of D, as shown in Figure 4(a)). Clearly $E \subseteq D$ and satisfies the conditions specified in the lemma.

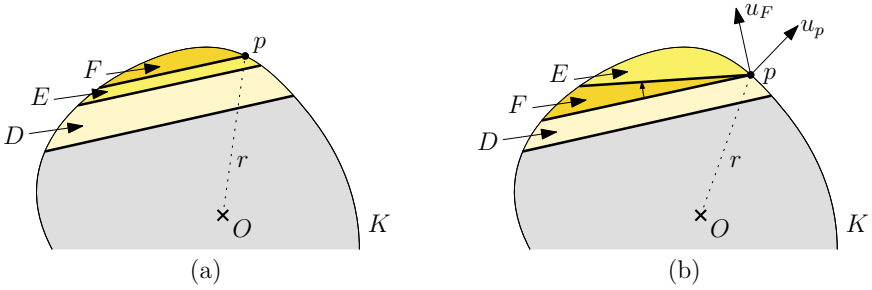


Figure 4: Proof of Lemma 2.11.

Otherwise, if the width of cap F is at least ε, then intuitively, we can rotate its base about p (shrinking cap F in the process), until its width is infinitesimally smaller than ε (Figure 4(b)). More formally, let u_F denote the normal vector for F's base and let u_p denote the (any) surface normal vector to K at p (both unit length). Since p is on the boundary, the cap orthogonal to u_p and passing through p has width zero. Since F has width at least ε, $u_F \neq u_p$.

Considering the 2-dimensional linear subspace spanned by u_F and u_p, we rotate continuously from u_F to u_p, and consider the hyperplane passing through p orthogonal to this vector. Clearly, the width of the associated cap varies continuously from $\text{wid}(F)$ to zero. Thus, there must be an angle where the cap width is infinitesimally smaller than ε. We can expand this cap by translating its base parallel to itself to obtain a cap E of width ε, which satisfies all the conditions specified in the lemma. □

2.4 Dual Caps and Cones

It will be useful to consider the notion of a cap in a dual setting (see, e.g., [10, 11]). Given a convex body $K \subseteq \mathbb{R}^n$ and a point z that is exterior to K, we define the *dual cap* of K with respect to z, denoted $\text{dcap}_K(z)$, to be the set of $(n-1)$-dimensional hyperplanes that pass through z and do not intersect K's interior (see Figure 5). In this paper, K will be either full dimensional or one dimension less. We define the polar of a dual cap to be the set of points that results by taking the polar of each hyperplane of the dual cap.

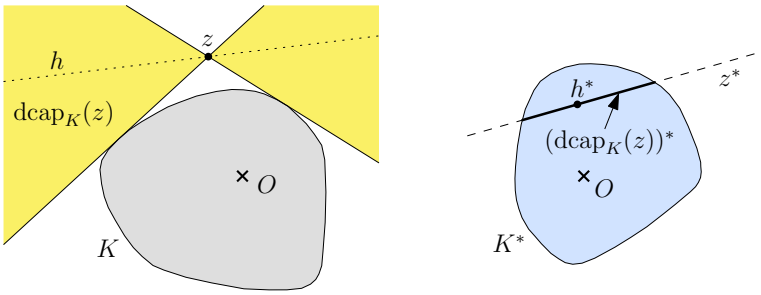


Figure 5: A dual cap and its polar.

Given z exterior to K, and consider the cap of K^* induced by the hyperplane z^*. By standard properties of the polar transformation, a hyperplane $h \in \text{dcap}_K(z)$ if and only if the point h^* lies on $K^* \cap z^*$. As an immediate consequence, we obtain the following relationship between caps and dual caps.

Lemma 2.12. *Let $K \subseteq \mathbb{R}^n$ be a full dimensional convex body that contains the origin and let $z \notin K$. Then* $(\text{dcap}_K(z))^* = \text{base}(\text{cap}_{K^*}(z^*))$.

Another useful concept involves cones induced by external points. A convex body K and a point $z \notin K$ naturally define two infinite convex cones. The *inner cone*, denoted $\text{icone}(K, z)$, is the intersection of all the halfspaces that contain K whose bounding hyperplanes pass through z (see Figure 11). Equivalently, $\text{icone}(K, z)$ is the set of points p such that the ray zp intersects K. The *outer cone*, denoted $\text{ocone}(K, z)$, is defined analogously as the intersection of halfspaces passing through z that do not contain any point of K (see Figure 6). It is easy to see that $\text{ocone}(K, z)$ is the reflection of $\text{icone}(K, z)$ about z. The following lemma shows that membership in the outer cone and containment of caps are related through duality.

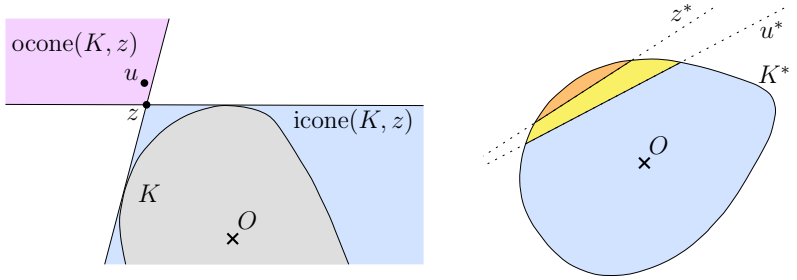


Figure 6: Inner and outer cones.

Lemma 2.13. *Let K be a convex body with the origin O in its interior. Then $u \in \text{ocone}(K, z)$ if and only if* $\text{cap}_{K^*}(z^*) \subseteq \text{cap}_{K^*}(u^*)$.

Proof. By definition, $u \in \text{ocone}(K, z)$ if and only if any hyperplane h that separates z from K also separates u from K. Also, by standard properties of the polar transformation, a hyperplane h separates z from K if and only if the point $h^* \in \text{cap}_{K^*}(z^*)$. Similarly, hyperplane h separates u from K if and only if the point $h^* \in \text{cap}_{K^*}(u^*)$. Thus, the condition $u \in \text{ocone}(K, z)$ is equivalent to the condition $\text{cap}_{K^*}(z^*) \subseteq \text{cap}_{K^*}(u^*)$. □

2.5 Macbeath Regions

Given a convex body K and a point $x \in K$, and a scaling factor $\lambda > 0$, the *Macbeath region* $M_K^\lambda(x)$ is defined as

$$M_K^\lambda(x) \;=\; x + \lambda((K - x) \cap (x - K)).$$

It is easy to see that $M_K^1(x)$ is the intersection of K with the reflection of K around x, and so $M_K^1(x)$ is centrally symmetric about x. Indeed, it is the largest centrally symmetric body centered at x and contained in K. Furthermore, $M_K^\lambda(x)$ is a copy of $M_K^1(x)$ scaled by the factor λ about the center x (see the right side of Figure 16). We will omit the subscript K when the convex body is clear from the context. As a convenience, we define $M(x) = M^1(x)$.

We now present lemmas that encapsulate standard properties of Macbeath regions. The first lemma implies that a (shrunken) Macbeath region can act as a proxy for any other (shrunken) Macbeath region overlapping it [22, 35]. Our version uses different parameters and is proved in [9] (Lemma 2.4).

Lemma 2.14. *Let K be a convex body and let $\lambda \leq \frac{1}{5}$ be any real. If $x, y \in K$ such that $M^\lambda(x) \cap M^\lambda(y) \neq \emptyset$, then $M^\lambda(y) \subseteq M^{4\lambda}(x)$.*

The following lemmas are useful in situations when we know that a Macbeath region overlaps a cap of K, and allow us to conclude that a constant factor expansion of the cap will fully contain the Macbeath region. The first applies to shrunken Macbeath regions and the second to Macbeath regions with any scaling factor. The proof of the first appears in [8] (Lemma 2.5), and the second is an immediate consequence of the definition of Macbeath regions.

Lemma 2.15. *Let K be a convex body. Let C be a cap of K and x be a point in K such that $C \cap M^{1/5}(x) \neq \emptyset$. Then $M^{1/5}(x) \subseteq C^2$.*

Lemma 2.16. *Let K be a convex body and $\lambda > 0$. If x is a point in a cap C of K, then $M^\lambda(x) \cap K \subseteq C^{1+\lambda}$.*

Points in a shrunken Macbeath region are similar in many respects. For example, they have similar ray distances.

Lemma 2.17. *Let K be a convex body. If x is a $\frac{1}{2}$-shallow point in K and $y \in M^{1/5}(x)$, then* $\operatorname{ray}(x)/2 \leq \operatorname{ray}(y) \leq 2\operatorname{ray}(x)$.

Proof. Let C_x denote the minimum width cap for x. By Lemma 2.7, $\operatorname{wid}(C_x) = \operatorname{ray}(x)$. Also, by Lemma 2.15, we have $M^{1/5}(x) \subseteq C_x^2$ and so $y \in C_x^2$. It follows from Lemma 2.6 that $\operatorname{ray}(y) \leq \operatorname{wid}(C_x^2) = 2\operatorname{wid}(C_x)$. Thus $\operatorname{ray}(y) \leq 2\operatorname{ray}(x)$, which proves the second inequality. To prove the first inequality, note that this follows trivially unless $\operatorname{ray}(y) \leq \frac{1}{4}$ (since $\operatorname{ray}(x) \leq \frac{1}{2}$). If $\operatorname{ray}(y) \leq \frac{1}{4}$, consider the minimum width cap C_y for y. By Lemma 2.7, $\operatorname{wid}(C_y) = \operatorname{ray}(y)$. Also, by Lemma 2.15, we have $M^{1/5}(x) \subseteq C_y^2$ and so $x \in C_y^2$. It follows from Lemma 2.6 that $\operatorname{ray}(x) \leq \operatorname{wid}(C_y^2) = 2\operatorname{wid}(C_y)$. Thus $\operatorname{ray}(x) \leq 2\operatorname{ray}(y)$, which completes the proof. □

The remaining lemmas in this section relate caps with the associated Macbeath regions.

Lemma 2.18 (Bárány [14])**.** *Given a convex body $K \subseteq \mathbb{R}^n$, let C be a $\frac{1}{3}$-shallow cap of K, and let p be the centroid of* $\operatorname{base}(C)$. *Then $C \subseteq M^{2n}(p)$.*

Lemma 2.19. *Let $0 < \beta < 1$ be any constant. Let $K \subseteq \mathbb{R}^n$ be a well-centered convex body, $p \in K$, and C be the minimum volume cap associated with p. If C contains the origin or* $\mathrm{wid}(C) \geq \beta$*, then* $\mathrm{vol}_K(M(p)) \geq 2^{-O(n)}$.

Proof. We claim that K satisfies the Winternitz property with respect to p. Note this is equivalent to the claim that $\mathrm{vol}_K(C) \geq 2^{-O(n)}$.

We consider two cases. First, suppose that C contains the origin. Since K is well-centered, by Lemma 2.2, K satisfies the Winternitz property with respect to the origin. It follows that $\mathrm{vol}_K(C) \geq 2^{-O(n)}$. Otherwise, if C does not contain the origin, then since the width of C is at least β, the expanded cap $C^{1/\beta}$ contains the origin. By Lemma 2.9, $\mathrm{vol}(C^{1/\beta}) \leq 2^{O(n)}\,\mathrm{vol}(C)$. Again, using the fact that K satisfies the Winternitz property with respect to the origin, we have $\mathrm{vol}_K(C^{1/\beta}) \geq 2^{-O(n)}$. Thus, in both cases, $\mathrm{vol}_K(C) \geq 2^{-O(n)}$, which proves the claim.

Since K satisfies the Winternitz property with respect to p, by Lemma 2.2, it must satisfy the Kovner-Besicovitch property with respect to p. Thus $\mathrm{vol}_K(M(p)) = \mathrm{vol}_K((K-p) \cap (p-K)) \geq 2^{-O(n)}$, as desired. □

Lemma 2.20. *Given a convex body $K \subseteq \mathbb{R}^n$, let C be a $\frac{1}{3}$-shallow cap of K, and let p be the centroid of* $\mathrm{base}(C)$*. We have*

$$2^{-O(n)} \cdot \mathrm{vol}(C) \;\leq\; \mathrm{vol}(M(p)) \;\leq\; 2 \cdot \mathrm{vol}(C).$$

Proof. The second inequality holds easily because half of $M(p)$ lies inside C. To prove the first inequality, let $B = \mathrm{base}(C)$, let $a = \mathrm{area}(B)$ denote its $(n-1)$-dimensional volume, and let $B' = M(p) \cap B$. Treating p as the origin of the coordinate system, by definition of Macbeath regions, $B' = B \cap -B$. By applying Lemma 2.2 (to the hyperplane containing B) we have $\mathrm{area}(B') \geq a/2^{O(n)}$.

Let x denote the apex of C, and let x' be the farthest point on segment $\overline{px}$ that is contained in $M(p)$. By Lemma 2.18, $\|px'\| \geq \|px\|/2n$. By convexity, the generalized cone $P = \mathrm{conv}(B' \cup \{x'\})$ is contained within $M(p)$. Letting w denote the absolute width of C, the height of this cone is at least $w/2n$. Thus

$$\mathrm{vol}(M(p)) \;\geq\; \mathrm{vol}(P) \;\geq\; \frac{\mathrm{area}(B') \cdot w/2n}{n} \;\geq\; \frac{(a/2^{O(n)}) \cdot w/2n}{n} \;=\; \frac{aw}{n^2 2^{O(n)}}.$$

By Lemma 2.8, $\mathrm{vol}(C) \leq 2^{n-1} aw$, and thus,

$$\mathrm{vol}(M(p)) \;\geq\; 2^{-O(n)} \cdot \mathrm{vol}(C),$$

as desired. □

Corollary 2.21. *Let $K \subseteq \mathbb{R}^n$ be a convex body, $p \in K$, and C be the minimum volume cap associated with p. We have*

$$2^{-O(n)} \cdot \mathrm{vol}(C) \;\leq\; \mathrm{vol}(M(p)) \;\leq\; 2 \cdot \mathrm{vol}(C).$$

Proof. The second inequality holds for the same reason as in Lemma 2.20. To prove the first inequality, recall the well-known property of minimum volume caps that p is the centroid of the base of its associated minimum volume cap [35]. Treating the centroid of K as the origin, we consider two cases. If C is $(1/3)$-shallow, then the corollary follows from Lemma 2.20. Otherwise, C contains the origin or its width is at least $1/3$. Noting that K is well-centered with respect to the centroid (Lemma 2.2) and applying Lemma 2.19, it follows that $\mathrm{vol}_K(M(p)) \geq 2^{-O(n)}$. That is, $\mathrm{vol}(M(p)) \geq 2^{-O(n)}\,\mathrm{vol}(K) \geq 2^{-O(n)}\,\mathrm{vol}(C)$, which completes the proof. □

2.6 Similar Caps

The Macbeath regions of a convex body K, and more specifically, its shrunken Macbeath regions, provide an affine-invariant notion of the closeness between points, through the property that both points lie within the same shrunken Macbeath region. We would like to define a similar affine-invariant notion of closeness between caps. We say that two caps C_1 and C_2 are λ-*similar* for $\lambda \geq 1$, if $C_1 \subseteq C_2^\lambda$ and $C_2 \subseteq C_1^\lambda$ (see Figure 7(a)). If two caps are λ-similar for a constant λ, we say that the caps are *similar*.

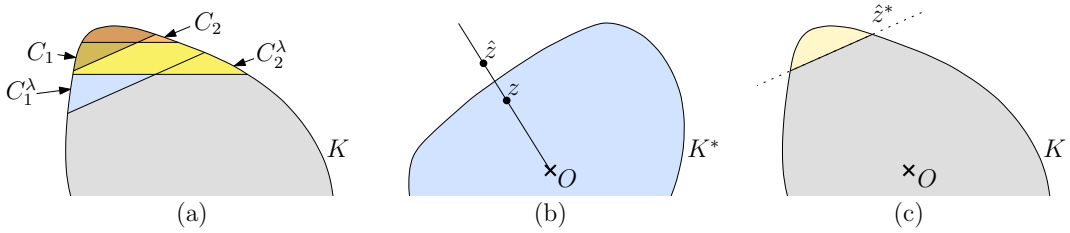


Figure 7: Similar caps and ε-representative caps.

It is natural to conjecture that these two notions of similarity are related through duality. In order to establish such a relationship consider the following mapping. Consider a point $z \in K^*$. Take a point $\hat{z} \notin K^*$ on the ray Oz such that $\mathrm{ray}(\hat{z}) = \varepsilon$ (see Figure 7(b)). The dual hyperplane $\hat{z}^*$ intersects K, and so induces a cap, which we call z's *ε-representative cap* (see Figure 7(c)). The main result of this section is Lemma 2.23, which shows that points lying within the same shrunken Macbeath region have similar representative caps. Before proving this, we begin with a technical lemma.

Lemma 2.22. *Let $\alpha \leq \frac{1}{8}$. Let $y \in K^*$ be an α-shallow point. Consider two rays r and r' shot from the origin through $M^{1/5}(y)$ (see Figure 8). Let $z \notin K^*$ be an α-shallow point on r and let $u \notin K^*$ be a point on r' such that $\mathrm{ray}(u) > 4\,\mathrm{ray}(y) + 2\,\mathrm{ray}(z)$. Then $\mathrm{cap}_K(z^*) \subseteq \mathrm{cap}_K(u^*)$.*

Proof. Let h be any hyperplane passing through z that does not intersect K^*. We will show that h separates u from K^*. This would imply that $u \in \mathrm{ocone}(K^*, z)$, and the result would then follow from Lemma 2.13.

Let p be any point in $r \cap M^{1/5}(y)$. By Lemma 2.17, we have $\mathrm{ray}(p) \leq 2\,\mathrm{ray}(y)$. Consider a hyperplane h' that is parallel to h and passes through p (see Figure 9). Let C be the cap induced by h'. Letting t denote the point of intersection of ray r with ∂K^*, we have

$$\mathrm{wid}(C) \;\leq\; \frac{\|pz\|}{\|Oz\|} \;=\; \frac{\|pt\| + \|tz\|}{\|Oz\|} \;\leq\; \frac{\|pt\|}{\|Ot\|} + \frac{\|tz\|}{\|Oz\|} \;=\; \mathrm{ray}(p) + \mathrm{ray}(z) \;\leq\; 2\,\mathrm{ray}(y) + \mathrm{ray}(z). \quad (1)$$

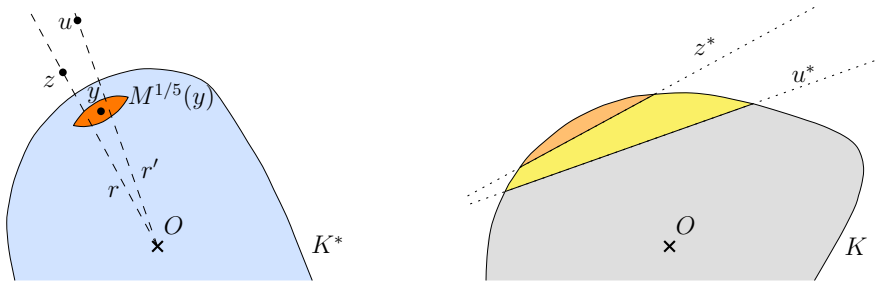


Figure 8: Statement of Lemma 2.22.

Since C intersects $M^{1/5}(y)$, by Lemma 2.15, the cap C^2 encloses $M^{1/5}(y)$. Since y and z are α-shallow for $\alpha = \frac{1}{8}$, by Eq. (1) we have $\mathrm{wid}(C) \leq 3/8$. It follows $\mathrm{wid}(C^2) < 1$, and hence O lies outside C^2. Let h'' denote the hyperplane passing through the base of C^2. Since r' intersects $M^{1/5}(y)$, it follows that r' must intersect h'' and h. Let z' denote the point of intersection of r' with h. We will show that $\mathrm{ray}(z') \leq 4\,\mathrm{ray}(y) + 2\,\mathrm{ray}(z)$. Recalling from the statement of the lemma that $\mathrm{ray}(u) > 4\,\mathrm{ray}(y) + 2\,\mathrm{ray}(z)$, this would imply that h separates u from K^*, as desired.

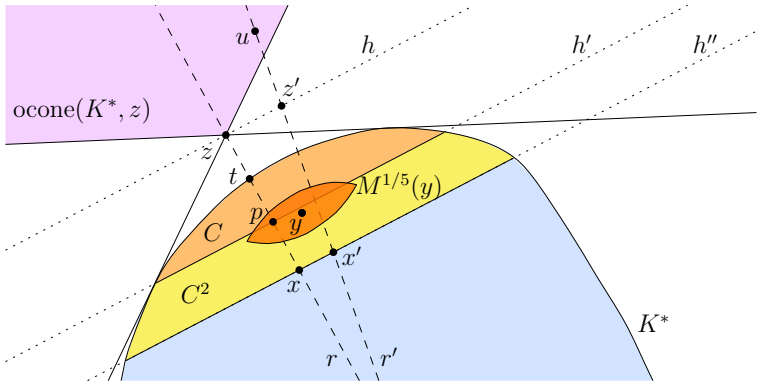


Figure 9: Proof of Lemma 2.22.

Let x and x' denote the points of intersection of the rays r and r', respectively, with h''. By similar triangles we have $\mathrm{ray}(z') \leq \|x'z'\|/\|Oz'\| = \|xz\|/\|Oz\|$. Observe that the distance between h'' and h' is no more than the distance between h' and h, and so $\|xz\| \leq 2\|pz\|$. Combining this with Eq. (1), we obtain

$$\mathrm{ray}(z') \;\leq\; \frac{\|xz\|}{\|Oz\|} \;\leq\; \frac{2\|pz\|}{\|Oz\|} \;\leq\; 2(2\,\mathrm{ray}(y) + \mathrm{ray}(z)) \;=\; 4\,\mathrm{ray}(y) + 2\,\mathrm{ray}(z),$$

which completes the proof. □

We now establish the main result of this section.

Lemma 2.23. *Let $\varepsilon \leq \frac{1}{16}$, and let $y \in K^*$ such that $\mathrm{ray}(y) \leq \varepsilon$. For any two points $x, z \in M^{1/5}(y)$, their respective ε-representative caps are 8-similar.*

Proof. Let x_1 and z_1 be points external to K^* both at ray distance ε on the rays Ox and Oz, respectively (see Figure 10(a)). Let C_x and C_z denote the ε-representative caps of x and z, respectively (see Figure 10(b)). Recall that C_x and C_z are the caps in K induced by x_1^* and z_1^*, respectively. By standard properties of the polar transformation $\mathrm{wid}(C_x) = \mathrm{ray}(x_1) = \varepsilon$, and similarly, $\mathrm{wid}(C_z) = \mathrm{ray}(z_1) = \varepsilon$. Let x_2 and z_2 be points external to K^* both at ray distance 8ε on the rays Ox and Oz, respectively (see Figure 10). By our bound on ε, these ray distances are at most $\frac{1}{2}$. Clearly, x_2^* and z_2^* induce the caps C_x^8 and C_z^8 in K, respectively.

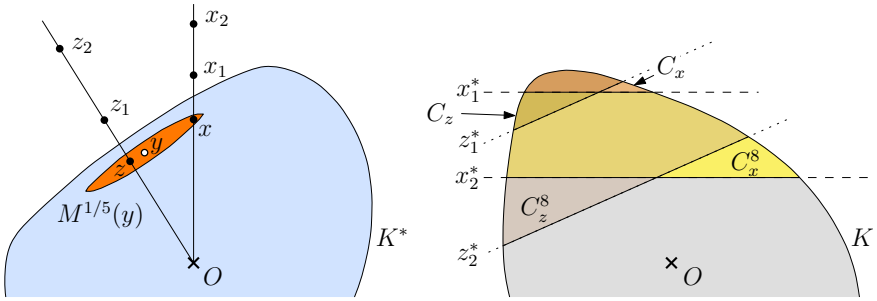


Figure 10: Proof of Lemma 2.23.

Since $\mathrm{ray}(x_2) = 8\varepsilon, \mathrm{ray}(y) \leq \varepsilon$ and $\mathrm{ray}(z_1) = \varepsilon$, we have $\mathrm{ray}(x_2) > 2\,\mathrm{ray}(z_1) + 4\,\mathrm{ray}(y)$. It follows from Lemma 2.22 that $C_z \subseteq C_x^8$. A symmetrical argument shows that $C_x \subseteq C_z^8$. Therefore C_x and C_z are 8-similar, as desired. □

The next lemma shows that similarity holds, even if ray distances are altered by a constant factor.

Corollary 2.24. *Let $\varepsilon \leq \frac{1}{16}$, and let $y \in K^*$ such that $\mathrm{ray}(y) \leq \varepsilon$. Let C_x be a cap of K such that $\varepsilon/2 \leq \mathrm{wid}(C_x) \leq 2\varepsilon$, and such that the ray shot from the origin orthogonal to the base of C_x intersects $M^{1/5}(y)$. Then the cap C_x and the ε-representative cap C_z of any point $z \in M^{1/5}(y)$ are 16-similar.*

Proof. Let r denote the ray shot from the origin orthogonal to the base of C_x. Let x be any point that lies in $r \cap M^{1/5}(y)$. Let C'_x be the ε-representative cap of x. By Lemma 2.23, the caps C'_x and C_z are 8-similar. Also, it follows from our choice of point x that the caps C_x and C'_x have parallel bases and their widths differ by a factor of at most two. Thus C_x and C'_x are 2-similar. Using the fact that C'_x and C_z are 8-similar, and applying Lemma 2.10, it is easy to see that C_x and C_z are 16-similar. □

3 Caps in the Polar: Mahler Relationship

As mentioned in Section 1.2, a central element of our analysis is establishing a Mahler-like reciprocal relationship between volumes of caps in K and corresponding caps of K^*. While our new result is similar in spirit to those given by Arya *et al.* [6] and that of Naszódi *et al.* [52], it is stronger than both. Compared to [6], the dependency of the Mahler volume on dimension is improved from $2^{-O(n \log n)}$ to $2^{-O(n)}$, which is critical in the high-dimensional setting in reducing terms of the form $n^{O(n)}$ to $2^{O(n)}$. Further, our result is presented in a cleaner form, which is affine-invariant.

Compared to Naszódi *et al.* [52], which was focused on sampling from just the boundary of K, our results can be applied to caps of varying widths, and hence it applies to sampling from the interior of K. This fact too is critical in the applications we consider. Our improvements are obtained by a more sophisticated geometric analysis and our affine-invariant approach.

For the sake of concreteness, we state the lemmas of this section in terms of an arbitrary direction, which we call "vertical," and any hyperplane orthogonal to this direction is called "horizontal." Since the direction is arbitrary, there is no loss of generality.

3.1 Dual Caps and the Difference Body

This subsection is devoted to a key construction in our analysis. Given a full dimensional convex body K and a point $z \notin K$, the following lemma identifies an $(n-1)$-dimensional body Υ such that $\mathrm{dcap}_\Upsilon(z) = \mathrm{dcap}_K(z)$, where Υ is related to the base B of a certain ε-width cap in the sense that Υ can be sandwiched between B and a scaled copy of the difference body of B.

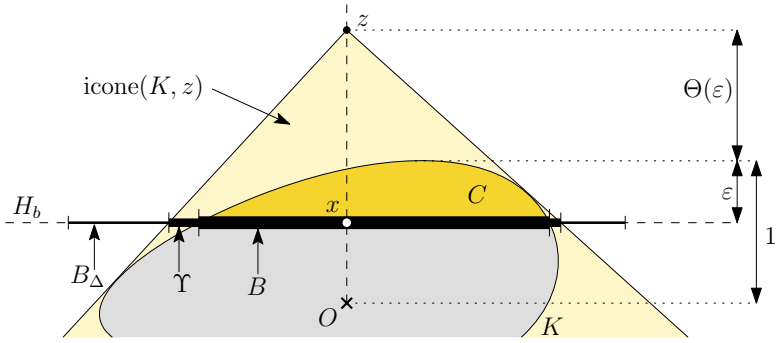


Figure 11: Statement of Lemma 3.1.

Lemma 3.1. *Let $\varepsilon \le \frac{1}{8}$. Let K be a convex body with the origin O in its interior. Let $z \notin K$ be a point on the ray from the origin directed vertically upwards such that $\mathrm{ray}(z) = 2\varepsilon$. Consider an ε-width cap C above the origin whose base B intersects Oz and is horizontal. Let H_b be the hyperplane passing through the base B, and let $\Upsilon = \mathrm{icone}(K, z) \cap H_b$. Let x denote the point of intersection of B with Oz, and let $B_\Delta = 5\Delta(B) + x$. Then $B \subseteq \Upsilon \subseteq B_\Delta$ (see Figure 11).*

Proof. By definition, $K \subseteq \mathrm{icone}(K, z)$, and so $B \subseteq \Upsilon$. Thus, it suffices to show that $\Upsilon \subseteq B_\Delta$. To prove this, we will show that $K \subseteq \mathrm{icone}(B_\Delta, z)$.

Let a denote an apex of C and let a' be the point obtained by projecting a orthogonally onto Oz (see Figure 12). Without loss of generality, assume that $\|Oa'\| = 1$. Note that $\|xa'\| = \varepsilon$, where x is the point of intersection of the ray Oz with the base of cap C. It is easy to check that $\varepsilon \le \|a'z\| \le 3\varepsilon$.

For the remainder of this proof, it will be convenient to imagine that the origin is at x. Our strategy will be to show that $C \subseteq \mathrm{icone}(2(1+2\varepsilon)B, z)$ and $K \setminus C \subseteq \mathrm{icone}(4(1+2\varepsilon)\Delta(B), z)$. Since B contains the origin, it follows easily that $B \subseteq \Delta(B)$. This implies that $K \subseteq \mathrm{icone}(4(1+2\varepsilon)\Delta(B), z) \subseteq \mathrm{icone}(5\Delta(B), z)$ since $\varepsilon \le \frac{1}{8}$. By definition of B_Δ, this would complete the proof.

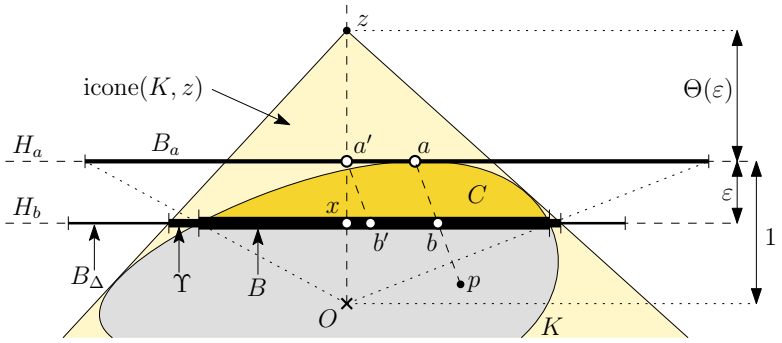


Figure 12: Proof of Lemma 3.1.

First, we will prove that $C \subseteq \text{icone}(2(1+2\varepsilon)B, z)$. It follows from convexity that C is contained in the truncated portion of $\text{icone}(B, O)$ between the hyperplane H_b and the hyperplane above H_b that is parallel to it at distance ε (call it H_a). Note that $\text{icone}(B, O) \cap H_a$ is the $(n-1)$-dimensional convex body obtained by scaling B about x by a factor of $1/(1-\varepsilon)$ and translating it vertically upwards by amount ε. Call this body B_a. (Formally, $B_a = (1/(1-\varepsilon))B + a'$.) It is easy to see that $C \subseteq \text{icone}(B_a, z)$. Since $\|zx\| \leq 2\|za'\|$, it follows that $\text{icone}(B_a, z) \cap H_b \subseteq 2(1/(1-\varepsilon))B$. Thus $C \subseteq \text{icone}(2(1/(1-\varepsilon))B, z) \subseteq \text{icone}(2(1+2\varepsilon)B, z)$, where in the last containment we have used the fact that $\varepsilon \leq \frac{1}{8}$.

It remains to prove that $K \setminus C \subseteq \text{icone}(4(1+2\varepsilon)\Delta(B), z)$. By convexity, it follows that $K \setminus C \subseteq \text{icone}(B, a)$. Define $t = a' - a$ and $B^+ = \text{conv}(B \cup (B+t))$. We claim that $K \setminus C \subseteq \text{icone}(B^+, a')$. To prove this, let p be any point in $K \setminus C$. Since $K \setminus C \subseteq \text{icone}(B, a)$, it follows that $\overline{ap}$ intersects the base B; let b denote this point of intersection. Since $b \in B$, we have $b \in B^+$. Define $b' = b + t$. Clearly $b' \in B + t$ and hence $b' \in B^+$. Note that the points b, b', a', a form a parallelogram (because $b' - a' = b - a$). By elementary geometry, p also lies in the 2-dimensional flat of this parallelogram and $\overline{a'p}$ intersects $\overline{bb'}$. Since $b, b' \in B^+$ and B^+ is convex, it follows that $\overline{bb'}$ is contained in B^+. Thus $\overline{a'p}$ intersects B^+, which implies that $p \in \text{icone}(B^+, a')$. This proves that $K \setminus C \subseteq \text{icone}(B^+, a')$, as desired.

Next consider the cone obtained by translating $\text{icone}(B^+, a')$ vertically upwards to z. Clearly the resulting cone contains $K \setminus C$, and since $\|zx\| \leq 4\|a'x\|$, it follows that the intersection of this cone with H_b is contained in $4B^+$. Thus $K \setminus C \subseteq \text{icone}(4B^+, z)$.

To complete the proof we need to relate B^+ to $\Delta(B)$. To be precise, we will show that $B^+ \subseteq (1+2\varepsilon)\Delta(B)$. Recall that $B^+ = \text{conv}(B \cup (B+t))$. By our earlier remarks, $a \in B_a$ and hence $-t = a - a' \in (1/(1-\varepsilon))B$. It follows that $B + t \subseteq (1/(1-\varepsilon))B - (-t) \subseteq \Delta((1/(1-\varepsilon))B)$, where the first containment is trivial and the second is immediate from the definition of difference bodies. Also, $B \subseteq \Delta((1/(1-\varepsilon))B)$ holds trivially. By convexity of difference bodies, it follows that $B^+ \subseteq \Delta((1/(1-\varepsilon))B)$. Thus $B^+ \subseteq (1/(1-\varepsilon))\Delta(B) \subseteq (1+2\varepsilon)\Delta(B)$. Recalling that $K \setminus C \subseteq \text{icone}(4B^+, z)$, it follows that $K \setminus C \subseteq \text{icone}(4(1+2\varepsilon)\Delta(B), z)$, which completes the proof. □

3.2 Relating Caps in the Primal and Polar

In order to establish a Mahler-like relation between the volumes of caps of K and K^*, it will be helpful to consider projections in one lower dimension, $n-1$. We will make use of a special case of a result appearing in [6] (Lemma 3.1). Consider a convex body K lying on an $(n-1)$-dimensional hyperplane and a point z that lies on the opposite side of this hyperplane from the origin (see Figure 13). The polar of the dual cap of K with respect to z is an $(n-1)$-dimensional convex body on the hyperplane z^*. Letting G denote this object, the following lemma shows that if we project both K and G onto a suitable $(n-1)$-dimensional hyperplane, G is the polar of K up to scale factor.

Lemma 3.2 (Arya *et al.* [6])**.** *Let $z \in \mathbb{R}^n$ be a point that lies on a vertical ray from the origin O, and let K be an $(n-1)$-dimensional convex body whose interior intersects the segment Oz at some point x. Further, suppose that K lies on a hyperplane orthogonal to Oz. Let $G = (\mathrm{dcap}_K(z))^*$ and let t be the point of intersection of the vertical ray from O with z^*. Then $G - t = \alpha(K-x)^*$, where $\alpha = \|xz\|/\|Oz\|$.*

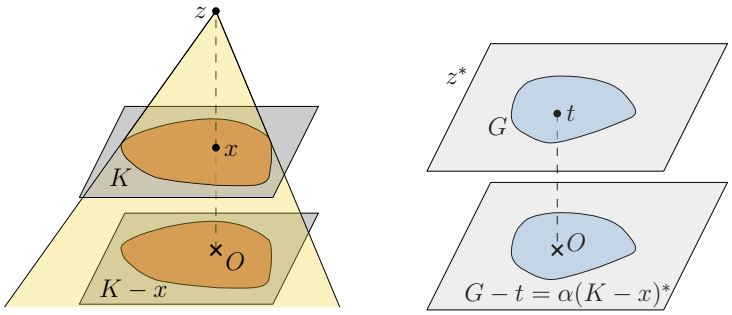


Figure 13: Statement of Lemma 3.2.

The following lemma describes the correspondence between caps in K and its polar K^*, and it establishes the critical Mahler-type relationship between the volumes of these caps.

Lemma 3.3. *Let $0 < \varepsilon \le \frac{1}{8}$, and let $K \subseteq \mathbb{R}^n$ be a well-centered convex body. Let C be a cap of K of width at least ε. Consider the ray shot from the origin orthogonal to the base of C, and let D be a cap of K^* of width at least ε such that this ray intersects the interior of its base (see Figure 14). Then*

$$\mathrm{vol}_K(C) \cdot \mathrm{vol}_{K^*}(D) \;\ge\; 2^{-O(n)}\varepsilon^{n+1}.$$

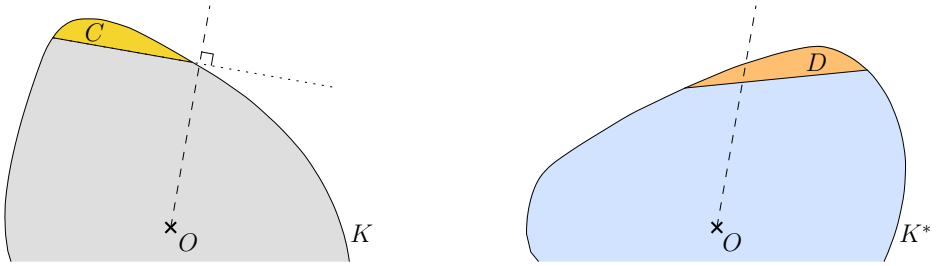


Figure 14: Statement of Lemma 3.3.

Proof. Let C' be a cap of width 2ε whose base is parallel to the base of C and which is on the same side of the origin as C. Clearly such a cap can be obtained by translating the base of C parallel to itself. Note that $C' \subseteq C^2$ and so, by Lemma 2.9, it follows that $\text{vol}(C') \leq 2^{O(n)} \cdot \text{vol}(C)$. Let r denote the ray in the polar space, emanating from the origin of K^* in a direction orthogonal to the base of C (see Figure 15). Recall that r intersects the interior of the base of D. By Lemma 2.11, we can find a cap $D' \subseteq D$ whose width is ε and such that ray r intersects the interior of the base of D'. It is now easy to see that it suffices to prove the lemma with C' and D' in place of C and D, respectively. As a convenience, in the remainder of this proof, we will write C and D in place of C' and D', respectively.

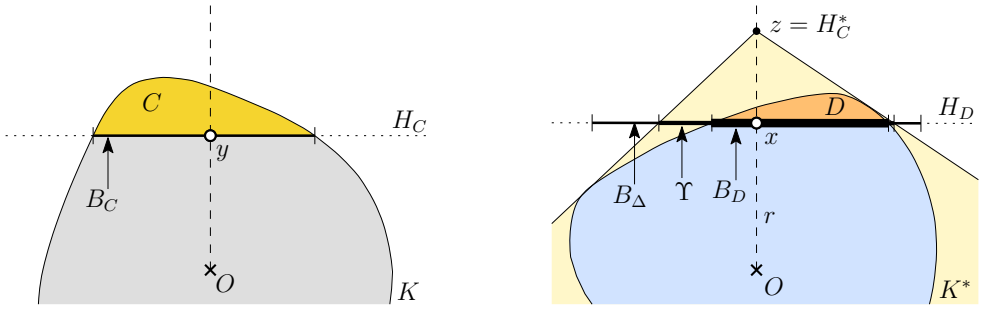


Figure 15: Proof of Lemma 3.3.

As the product considered in this lemma is affine-invariant, we will apply a suitable linear transformation to simplify the subsequent analysis. Specifically, we apply a linear transformation in the polar space such that the base of D becomes horizontal while the ray r is directed vertically upwards. It is easy to see that the effect of this transformation in the original space is to make the base of cap C horizontal (because it is the polar of a point on ray r). To summarize, after the transformation, the hyperplanes passing through the bases of the caps C and D are horizontal and above the origin and as relative measures the widths of both caps are unchanged. Further, the ray r is directed vertically upwards in the polar and intersects the interior of the base of D. Also, after uniform scaling, we may assume that the absolute distance between the origin and the supporting hyperplane of cap C that is parallel to its base is unity.

Let B_C denote the base of cap C and H_C denote the hyperplane passing through B_C. Also, let B_D denote the base of cap D and H_D denote the hyperplane passing through B_D. Define $z = H_C^*$. Note that z lies outside K^* on the ray from the origin directed vertically upwards and $\text{ray}(z) = \text{wid}(C) = 2\varepsilon$. By Lemma 2.12, $B_C = (\text{dcap}_{K^*}(z))^*$. Define $\Upsilon = \text{icone}(K^*, z) \cap H_D$. Clearly $\text{dcap}_{K^*}(z) = \text{dcap}_{\Upsilon}(z)$. Thus $B_C = (\text{dcap}_{\Upsilon}(z))^*$.

Let y denote the point of intersection of the vertical ray from O with B_C, and let x denote the point of intersection of the vertical ray from O with B_D. Henceforth, in this proof, we will treat y as the origin in the primal space and x as the origin in the polar space. Applying Lemma 3.2 (setting K in that lemma to Υ), it follows that $B_C = \alpha\Upsilon^*$, where $\alpha = \|xz\|/\|Oz\|$. Noting that B_C is $(n-1)$-dimensional and $\alpha = \Theta(\varepsilon)$, it follows that

$$\text{area}(B_C) \;\geq\; 2^{-O(n)}\varepsilon^{n-1} \cdot \text{area}(\Upsilon^*).$$

By Lemma 2.8, we have $\text{vol}(C) \geq 2^{-O(n)}\varepsilon \cdot \text{area}(B_C)$ and $\text{vol}(D) \geq 2^{-O(n)}\varepsilon \cdot \text{area}(B_D)$. Thus,

$$\text{vol}(C) \cdot \text{vol}(D) \;\geq\; 2^{-O(n)}\varepsilon^2 \cdot \text{area}(B_C) \cdot \text{area}(B_D) \;\geq\; 2^{-O(n)}\varepsilon^{n+1} \cdot \text{area}(\Upsilon^*) \cdot \text{area}(B_D). \tag{2}$$

By Lemma 3.1, $\Upsilon \subseteq B_\Delta$, where $B_\Delta = 5\Delta(B_D)$. Recalling from Lemma 2.1 that $\text{area}(\Delta(B_D)) \leq 4^{n-1} \cdot \text{area}(B_D)$, we have

$$\text{area}(\Upsilon) \;\leq\; \text{area}(B_\Delta) \;=\; 5^{n-1} \cdot \text{area}(\Delta(B_D)) \;\leq\; 5^{n-1} \cdot 4^{n-1} \cdot \text{area}(B_D) \;\leq\; 2^{O(n)} \cdot \text{area}(B_D).$$

Substituting this bound into Eq. (2), we obtain

$$\text{vol}(C) \cdot \text{vol}(D) \;\geq\; 2^{-O(n)}\varepsilon^{n+1} \cdot \text{area}(\Upsilon^*) \cdot \text{area}(\Upsilon) \;\geq\; 2^{-O(n)}\varepsilon^{n+1} \cdot \omega_{n-1}^2,$$

where we have applied Lemma 2.5 to lower bound the Mahler volume in the last step. Since K is well-centered, it follows from Lemma 2.2 that K satisfies the Santaló property, that is, $\text{vol}(K) \cdot \text{vol}(K^*) \leq 2^{O(n)} \cdot \omega_n^2$. Recalling the definition of ω_n from Section 2.2, we have $\omega_{n-1}/\omega_n = \Theta(\sqrt{n})$. Thus

$$\text{vol}_K(C) \cdot \text{vol}_{K^*}(D) \;\geq\; 2^{-O(n)}\varepsilon^{n+1},$$

as desired. □

Finally, we present the main "take-away" of this section. This lemma shows that the bound on the product of volumes from the previous lemma holds within the neighborhood of the ray, specifically to any shrunken Macbeath region that intersects the ray.

Lemma 3.4. *Let parameter ε, convex body K and cap C of K be as defined in Lemma 3.3. Suppose that the ray r shot from the origin orthogonal to the base of C intersects a Macbeath region $M^{1/5}(x)$ of K^*, where $\text{ray}(x) = \varepsilon$ (see Figure 16). Then*

$$\text{vol}_K(C) \cdot \text{vol}_{K^*}(M^{1/5}(x)) \;\geq\; 2^{-O(n)}\varepsilon^{n+1}.$$

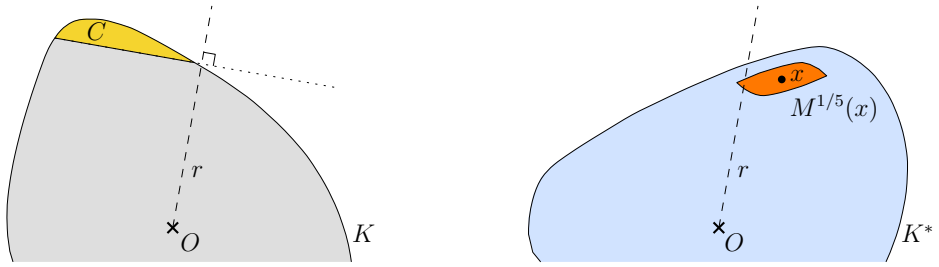


Figure 16: Statement of Lemma 3.4.

Proof. Let y be a point in the intersection of the ray r with $M^{1/5}(x)$ and let D denote the minimum volume cap of K^* that contains y. Since $M^{1/5}(y) \cap M^{1/5}(x) \neq \emptyset$, by Lemma 2.14, we have $M^{1/5}(y) \subseteq M^{4/5}(x)$. Thus $\text{vol}(M^{1/5}(x)) \geq 2^{-O(n)} \cdot \text{vol}(M^{1/5}(y))$. Also, by Corollary 2.21, we have $\text{vol}(M^{1/5}(y)) \geq 2^{-O(n)} \cdot \text{vol}(D)$. Thus $\text{vol}(M^{1/5}(x)) \geq 2^{-O(n)} \cdot \text{vol}(D)$. To complete the proof, it suffices to show the inequality given in the statement of the lemma with D in place of $M^{1/5}(x)$. By Lemma 2.17, we have $\text{ray}(y) \geq \text{ray}(x)/2$, and by Lemma 2.6, we have $\text{wid}(D) \geq \text{ray}(y)$. Thus $\text{wid}(D) \geq \text{ray}(x)/2 = \varepsilon/2$. Applying Lemma 3.3 on caps C and D, the desired inequality now follows. □

4 Covers of Convex Bodies

As mentioned earlier, we employ a Macbeath region-based adaptation of (c, ε)-coverings in our solution to approximate CVP. Since our construction will involve composing coverings of various regions of K, we define our coverings in the following restricted manner. Let $K \subseteq \mathbb{R}^n$ be a convex body, let Λ be an arbitrary subset of $\text{int}(K)$, and let $c \geq 2$ be any constant. Define a Λ-*limited* c-*covering* to be a collection $\mathcal{Q}$ of convex bodies that cover Λ, such that the c-factor expansion of each body about its centroid is contained within K.

Our coverings will be based on Macbeath regions. Given $X \subseteq K$, define $\mathscr{M}_K^\lambda(X) = \{M_K^\lambda(x) : x \in X\}$. Define a (K, Λ, c)-*MNet* to be any maximal set of points $X \subseteq \Lambda$ such that the shrunken Macbeath regions $\mathscr{M}_K^{1/4c}(X)$ are pairwise disjoint. Through basic properties of Macbeath regions, we can obtain a covering by suitable expansion as shown in the following lemma, which summarizes the properties of MNets.

Lemma 4.1. *Given a convex body $K \subseteq \mathbb{R}^n$, $\Lambda \subset \text{int}(K)$, and $c \geq 2$, a (K, Λ, c)-MNet X satisfies the following properties:*

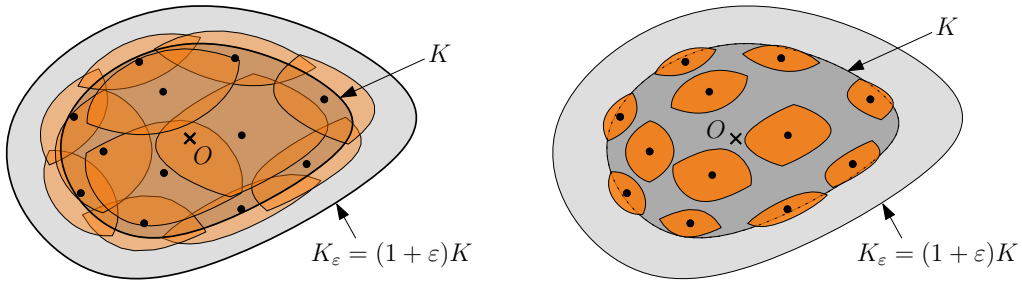
(a) *(Packing) The elements of $\mathscr{M}_K^{1/4c}(X)$ are pairwise disjoint.*

(b) *(Covering) The union of $\mathscr{M}_K^{1/c}(X)$ covers Λ.*

(c) *(Buffering) The union of $\mathscr{M}_K(X)$ is contained within K.*

Proof. Part (a) is an immediate consequences of the definition. Part (c) follows by basic properties of Macbeath regions. To prove part (b), let $\lambda = 1/c$ and consider any point $y \in \Lambda$. By maximality, there is $x \in X$ such that $M^{\lambda/4}(x)$ overlaps $M^{\lambda/4}(y)$. By Lemma 2.14, $M^{\lambda/4}(y) \subseteq M^\lambda(x)$, which implies that $y \in M^\lambda(x)$. □

Observe that property (b) implies that if X is a (K, Λ, c)-MNet, then $\mathscr{M}_K^{1/c}(X)$ is a Λ-limited c-covering. Further, recalling that $K_\varepsilon = (1 + \varepsilon)K$, if X is a (K_ε, K, c)-MNet, then $\mathscr{M}_K^{1/c}(X)$ is a (c, ε)-covering of K (see Figure 17).



(a) (b)

Figure 17: (a) A (c, ε)-covering of K by Macbeath regions. (b) The corresponding maximal set of disjoint Macbeath regions.

4.1 Instance Optimality

In this section we show that an MNet for K_ε naturally generates an *instance optimal* $(2,\varepsilon)$-covering in the sense that its size cannot exceed that of any $(2,\varepsilon)$-covering of K by a factor of $2^{O(n)}$ (Lemma 4.4 and Theorem 4). It is worth noting that this fact holds irrespective of the location of the origin in $\text{int}(K)$. In other words, we require no centrality assumptions for this result.

We begin with two lemmas that are straightforward adaptations of lemmas in [53]. The first lemma shows that one incurs a size penalty of only $2^{O(n)}$ by restricting to c-coverings to centrally symmetric convex bodies. The second shows that a constant change in the expansion factor results in a similar penalty.

Lemma 4.2. *Let $c \geq 2$ be a constant. Let $Q \subseteq \mathbb{R}^n$ be a convex body with its centroid at the origin. There exists a set of $2^{O(n)}$ centrally symmetric convex bodies which together cover Q, such that the central c-expansion of any of these bodies is contained within $2Q$.*

Proof. Let $R = M_Q(O) = Q \cap -Q$, and let $R' = \frac{1}{c}R$ and $R'' = \frac{1}{2c}R$. Clearly, all these bodies are centrally symmetric about the origin. By Lemma 2.2, $\text{vol}(R) \geq 2^{-O(n)}\,\text{vol}(Q)$, and since c is a constant, the volumes of R' and R'' are similarly bounded. Let $X \subset Q$ be a maximal discrete set of points such that the translates $X \oplus R'' = \{x + R'' : x \in X\}$ are pairwise disjoint. We will show that the bodies $X \oplus R'$ satisfy the lemma.

To establish the expansion property, observe that for all $x \in X$, $x + cR' = x + R \subseteq Q \oplus R \subseteq 2Q$. To prove the size bound, by disjointness we have

$$|X| \cdot \text{vol}(R'') \;\leq\; \text{vol}(2Q) \;\leq\; 2^{O(n)}\,\text{vol}(Q) \;\leq\; 2^{O(n)}\,\text{vol}(R''),$$

and therefore $|X| = 2^{O(n)}$. Finally, to prove coverage, consider any $y \in Q$. By maximality there exists $x \in X$ such that $x + R''$ overlaps $y + R''$. Since $c \geq 2$, it follows that $y \in x + 2R'' = x + R'$. □

Lemma 4.3. *Let $K \subseteq \mathbb{R}^n$ be a convex body, let $\Lambda \subset \text{int}(K)$, and let $c \geq 2$ be a constant. Let $\mathcal{Q}$ be a Λ-limited c-covering with respect to K. For any constant $c' \geq 2$, there exists a Λ-limited c'-covering with respect to K consisting of centrally symmetric convex bodies whose size is at most $2^{O(n)}|\mathcal{Q}|$.*

Proof. By Lemma 4.2, we can replace each body $Q \in \mathcal{Q}$ by a set of $2^{O(n)}$ centrally symmetric convex bodies which together cover Q and such that the c'-expansion of any of these bodies is contained within the 2-expansion of Q (about its centroid). It is easy to see that the resulting set of bodies is a Λ-limited c'-cover with respect to K with the desired size. □

We are now ready to show that a (K,Λ,c)-MNet can be used to generate an instance-optimal limited covering.

Lemma 4.4. *Let $K \subseteq \mathbb{R}^n$ be a convex body, let $\Lambda \subset \text{int}(K)$, and let $c \geq 2$ be a constant. Let X be a (K,Λ,c)-MNet, and let $\mathscr{M} = \mathscr{M}_K^{1/c}(X)$ be the associated Λ-limited c-covering with respect to K. Given any Λ-limited c-covering $\mathcal{Q}$ with respect to K, $|\mathscr{M}| \leq 2^{O(n)}|\mathcal{Q}|$.*

Proof. By Lemma 4.3, there exists a Λ-limited 5-covering with respect to K consisting of at most $2^{O(n)}|\mathcal{Q}|$ centrally symmetric convex bodies. Let $\mathcal{Q}'$ denote this covering, and let Y denote the

set of centers of these bodies. Consider any $Q \in \mathcal{Q}'$, and let y denote its center. By definition, $M(y) = M_K(y)$ is the largest centrally symmetric body centered at y that is contained within K. Since Q is a centrally symmetric convex body whose 5-expansion about y is contained within K, it follows that $Q \subseteq M^{1/5}(y)$. Therefore, $\mathscr{M}^{1/5}(Y)$ is a Λ-limited 5-covering of the same cardinality as $\mathcal{Q}'$.

By the packing property of Lemma 4.1, the Macbeath regions $\mathscr{M}^{1/4c}(X)$ are pairwise disjoint. To relate these two coverings, assign each $x \in X$ to any $y \in Y$ such that $x \in M^{1/5}(y)$. We will show that at most $2^{O(n)}$ elements of X are assigned to any $y \in Y$. Assuming this for now, we have

$$|\mathscr{M}| \;=\; |X| \;\leq\; 2^{O(n)}|Y| \;=\; 2^{O(n)}|\mathcal{Q}'| \;\leq\; 2^{O(n)}|\mathcal{Q}|,$$

thus completing the proof.

To prove the assertion, consider any $x \in X$ assigned to some $y \in Y$. Since $M^{1/5}(x) \cap M^{1/5}(y) \neq \emptyset$, by Lemma 2.14 and the fact that $c \geq 2$, we have

$$M^{1/4c}(x) \;\subseteq\; M^{1/5}(x) \;\subseteq\; M^{4/5}(y).$$

Lemma 2.14 also implies that $M^{1/5}(y) \subseteq M^{4/5}(x)$, and so $\mathrm{vol}(M^{1/4c}(x)) \geq 2^{-O(n)}\,\mathrm{vol}(M^{4/5}(y))$. Since the Macbeath regions of $M^{1/4c}(X)$ are pairwise disjoint, by a simple packing argument, the number of points of X assigned to any $y \in Y$ is at most $2^{O(n)}$, as desired. □

Recall that a K-limited c-covering with respect to $K_\varepsilon = (1+\varepsilon)K$ is a (c,ε)-covering for K. Applying the above lemma in this case, we obtain the main result of this section.

Theorem 4. *Let $0 < \varepsilon \leq 1$, let $K \subseteq \mathbb{R}^n$ be a convex body such that $O \in \mathrm{int}(K)$, and let $c \geq 2$ be a constant. Let X be a (K_ε, K, c)-MNet, and let $\mathscr{M} = \mathscr{M}_{K_\varepsilon}^{1/c}(X)$ be the associated (c,ε)-covering with respect to K. Given any (c,ε)-covering $\mathcal{Q}$ with respect to K, $|\mathscr{M}| \leq 2^{O(n)}|\mathcal{Q}|$.*

4.2 Worst-Case Optimality

Our main result in this section, given in Lemma 4.6, establishes the existence of a (c,ε)-covering of size $2^{O(n)}/\varepsilon^{(n-1)/2}$. This directly implies Theorem 1. Before presenting this result, it will be useful to first establish a bound on the maximum number of disjoint Macbeath regions associated with $\Theta(\varepsilon)$-width caps. The proof is based on the relationship between caps in K and K^*.

Let $K \subseteq \mathbb{R}^n$ be a well-centered convex body. Given $0 < \varepsilon \leq \frac{1}{32}$, let $\Lambda \subseteq K$ denote the centroids of the bases of all caps whose relative widths are between ε and 2ε. Given a constant $c \geq 2$, let X be a (K, Λ, c)-MNet, and let $\mathscr{M}(X) = \mathscr{M}_K^{1/c}(X)$ be the associated covering. We will show that $|X| \leq 2^{O(n)}/\varepsilon^{(n-1)/2}$, which will imply a similar bound on the size of the associated Λ-limited c-covering.

Recall that for any region $\Lambda \subseteq K$, its relative volume is $\mathrm{vol}_K(\Lambda) = \mathrm{vol}(\Lambda)/\,\mathrm{vol}(K)$. Let $t = \varepsilon^{(n+1)/2}$. Define $X_{\geq t} = \{x \in X : \mathrm{vol}_K(M_K^{1/c}(x)) \geq t\}$ to be the centers of the "large" Macbeath regions in the covering of relative volume at least t, and let $X_{<t} = X \setminus X_{\geq t}$ denote the centers of the remaining "small" Macbeath regions.

To bound the number of small Macbeath regions, we will make use of the polar body K^*. Let Λ' denote the boundary of $(1-\varepsilon)K^*$. Let Y be a $(K^*, \Lambda', 5)$-MNet, and let $\mathscr{M}(Y) = \mathscr{M}_{K^*}^{1/5}(Y)$ be

the associated covering. Let $t' = 2^{-O(n)}\varepsilon^{(n+1)/2}$, where the constant hidden in $O(n)$ is sufficiently large, and analogously define $Y_{\geq t'} = \{y \in Y : \mathrm{vol}_{K^*}(M^{1/5}_{K^*}(y)) \geq t'\}$ to be the set of centers of the "large" Macbeath regions in the polar covering $\mathscr{M}(Y)$ whose relative volume is at least t'.

The following lemma summarizes the essential properties of the resulting Macbeath regions.

Lemma 4.5. *Given a well-centered convex body $K \subseteq \mathbb{R}^n$, $0 < \varepsilon \leq \frac{1}{32}$, constant $c \geq 2$, and the entities Λ, Λ', X, Y, t, and t' defined above, the following hold:*

(a) *The regions $\mathscr{M}^{1/c}_K(X)$ are contained in $\Lambda_K(\varepsilon) = K \setminus (1-4\varepsilon)K$, and $\mathrm{vol}_K(\Lambda_K(\varepsilon)) = O(n\varepsilon)$.*

(b) *For any $x \in X_{\geq t}$, $\mathrm{vol}_K(M^{1/c}(x)) \geq \varepsilon^{(n+1)/2}$, and $|X_{\geq t}| \leq 2^{O(n)}/\varepsilon^{(n-1)/2}$.*

(c) *The regions $\mathscr{M}^{1/5}_{K^*}(Y)$ are contained in $\Lambda_{K^*}(\varepsilon) = K^* \setminus (1-2\varepsilon)K^*$, and $\mathrm{vol}_{K^*}(\Lambda_{K*}(\varepsilon)) = O(n\varepsilon)$.*

(d) *For any $y \in Y_{\geq t'}$, $\mathrm{vol}_{K^*}(M^{1/5}(y)) \geq 2^{-O(n)}\varepsilon^{(n+1)/2}$, and $|Y_{\geq t'}| \leq 2^{O(n)}/\varepsilon^{(n-1)/2}$.*

(e) *For any $x \in X_{<t}$, there is $y \in Y_{\geq t'}$ such that for any point $z \in M^{1/5}(y)$, we have $M^{1/c}(x) \subseteq C^{32}_z$, and $\mathrm{vol}(M^{1/c}(x)) \geq 2^{-O(n)}\,\mathrm{vol}(C^{32}_z)$, where $C_z \subseteq K$ is z's ε-representative cap.*

(f) $|X| \leq 2^{O(n)}/\varepsilon^{(n-1)/2}$.

Proof. To prove (a), let x be any point of X and let $M_x = M^{1/c}(x)$ be the associated covering Macbeath region. Because X is a (K, Λ, c)-MNet, M_x is centered at the centroid of the base of a cap C_x of width between ε and 2ε. Since $c \geq 1$, by Lemma 2.16, $M_x \subseteq C^2_x$. As C^2_x has width at most 4ε, it follows that $C^2_x \subseteq \Lambda_K(\varepsilon)$, and so too is M_x. Clearly, $\mathrm{vol}_K(\Lambda_K(\varepsilon)) = 1 - (1-4\varepsilon)^n = O(n\varepsilon)$.

To prove (b), observe that the Macbeath regions $\mathscr{M}^{1/4c}(X_{\geq t})$ are pairwise disjoint, and each has relative volume at least $t/4^n \geq 2^{-O(n)}\varepsilon^{(n+1)/2}$. By a simple packing argument, $|X_{\geq t}| \leq \mathrm{vol}_K(\Lambda_K(\varepsilon))/(t/4^n) \leq 2^{O(n)}/\varepsilon^{(n-1)/2}$.

To prove (c), let y be any point of Y and let $M_y = M^{1/5}(y)$ be the associated covering Macbeath region. Since y lies on the boundary of $(1-\varepsilon)K^*$, y lies on the base of a cap C_y of K^* induced by the supporting hyperplane of $(1-\varepsilon)K^*$. By Lemma 2.16, $M_y \subseteq C^2_y$. Since C^2_y has width 2ε, it follows that $C^2_y \subseteq \Lambda_{K*}(\varepsilon)$, and so too is M_y. Also, $\mathrm{vol}_{K^*}(\Lambda_{K*}(\varepsilon)) = 1 - (1-2\varepsilon)^n = O(n\varepsilon)$.

To prove (d), observe that by Lemma 4.1, the Macbeath regions $\mathscr{M}^{1/(4\cdot 5)}(Y_{\geq t'})$ are pairwise disjoint, and each has relative volume at least $t'/4^n = 2^{-O(n)}\varepsilon^{(n+1)/2}$. By a simple packing argument, $|Y_{\geq t'}| \leq \mathrm{vol}_{K^*}(\Lambda_{K*}(\varepsilon))/(t'/4^n) \leq 2^{O(n)}/\varepsilon^{(n-1)/2}$.

To prove (e), let x be any point of $X_{<t}$ and let $M_x = M^{1/c}(x)$ be the associated covering Macbeath region. As in (a), M_x is centered at the centroid of the base of a cap C_x of width between ε and 2ε. Since c is a constant, by Lemma 2.20, $\mathrm{vol}(C_x) \leq 2^{O(n)}\,\mathrm{vol}(M_x)$. Since $\mathrm{vol}_K(M_x) \leq t = \varepsilon^{(n+1)/2}$, we have $\mathrm{vol}_K(C_x) \leq 2^{O(n)}\varepsilon^{(n+1)/2}$.

In the polar, consider the ray r shot from the origin orthogonal to the base of C_x. This ray will intersect some covering Macbeath region $M_y = M^{1/5}(y)$, for some $y \in Y$. We will show that y satisfies all the properties given in part (e). As K is well-centered, we can apply the Mahler-like volume relation from Lemma 3.4 to obtain $\mathrm{vol}_K(C_x) \cdot \mathrm{vol}_{K^*}(M_y) \geq 2^{-O(n)}\varepsilon^{n+1}$. Using the upper bound on $\mathrm{vol}_K(C_x)$ shown above, it follows that $\mathrm{vol}_{K^*}(M_y) \geq 2^{-O(n)}\varepsilon^{(n+1)/2}$. Thus, $y \in Y_{\geq t'}$.

It is easy to verify that the preconditions of Corollary 2.24 are satisfied where C_x plays the role of C, M_y plays the role of $M^{1/5}(y)$, and z is any point in M_y. It follows that the caps C_x and C_z are 16-similar, that is, $C_x \subseteq C_z^{16}$ and $C_z \subseteq C_x^{16}$. By Lemma 2.16, $M_x \subseteq C_x^2$, and by Lemma 2.10, $C_x^2 \subseteq C_z^{32}$. Thus $M_x \subseteq C_z^{32}$. Also, since $C_z \subseteq C_x^{16}$, it follows from Lemma 2.9 that $\mathrm{vol}(C_x) \geq 2^{-O(n)}\,\mathrm{vol}(C_z)$. By Lemma 2.20, $\mathrm{vol}(M_x) \geq 2^{-O(n)}\,\mathrm{vol}(C_x)$. Thus $\mathrm{vol}(M_x) \geq 2^{-O(n)}\,\mathrm{vol}(C_z) \geq 2^{-O(n)}\,\mathrm{vol}(C_z^{32})$, which establishes (e).

Finally, to prove (f), observe that in light of (b), it suffices to show that $|X_{<t}| \leq 2^{O(n)}/\varepsilon^{(n-1)/2}$. This quantity can be bounded by the following charging argument. For each $y \in Y_{\geq t'}$, we say that it *charges* all the points $x \in X$ whose Macbeath region $M^{1/4c}(x)$ is contained in C_y^{32} and whose volume is at least $2^{-O(n)}\,\mathrm{vol}(C_y^{32})$, where the constant hidden in $O(n)$ is sufficiently large. Note that any point of $Y_{\geq t'}$ charges at most $2^{O(n)}$ points of X. Applying part (e), it follows that every $x \in X_{<t}$ is charged by some $y \in Y_{\geq t'}$. Since $|Y_{\geq t'}| \leq 2^{O(n)}/\varepsilon^{(n-1)/2}$ and each point of $Y_{\geq t'}$ charges at most $2^{O(n)}$ points of X, it follows that $|X_{<t}| \leq 2^{O(n)}/\varepsilon^{(n-1)/2}$, which completes the proof. □

We are now ready to present the main result of this section. Recall that $K \subseteq \mathbb{R}^n$ is a well-centered convex body. Given $0 < \varepsilon \leq 1$, define a *layered decomposition* of K as follows. Recalling that $K_\varepsilon = (1+\varepsilon)K$, for each $x \in K$, define its *width*, denoted $\mathrm{wid}(x)$, to be the width of the associated minimum volume cap of K_ε. Since $\mathrm{ray}_{K_\varepsilon}(x) \geq \varepsilon/(1+\varepsilon) \geq \varepsilon/2$, it follows from Lemma 2.6 that $\mathrm{wid}(x) \geq \varepsilon/2$. Let β be a sufficiently small constant, and let $k_0 = \left\lceil \log \frac{\beta}{\varepsilon} \right\rceil$. For $0 \leq i \leq k_0$, define the layer i be the set of points $x \in K$ such that $\mathrm{wid}(x) \in [2^{i-1}, 2^i)\varepsilon$. Define layer $k_0 + 1$ to be the set of remaining points of K, which have width at least β. Note that the number of layers is $O(\log \frac{1}{\varepsilon})$.

Lemma 4.6. *Let $0 < \varepsilon \leq 1$, let $K \subseteq \mathbb{R}^n$ be a well-centered convex body, and let $c \geq 2$ be a constant. Let X be a (K_ε, K, c)-MNet, and let $\mathscr{M} = \mathscr{M}_{K_\varepsilon}^{1/c}(X)$. Then $\mathscr{M}$ is a (c, ε)-covering for K consisting of at most $2^{O(n)}/\varepsilon^{(n-1)/2}$ centrally symmetric convex bodies.*

Proof. By Lemma 4.1, $\mathscr{M}$ is a (c, ε)-covering for K. We will bound the size of the covering by partitioning the points of X based on the layered decomposition (defined above) and then use Lemma 4.5 to bound the number of points in each layer.

For $0 \leq i \leq k_0$, let X_i be subset of points of X that are in layer i. Since K is well-centered, K_ε is also well-centered. By Lemma 4.5(f), $|X_i| \leq 2^{O(n)}/(2^i\varepsilon)^{(n-1)/2}$. Summing $|X_i|$ over all layers 0 to k_0 we have at most $2^{O(n)}/\varepsilon^{(n-1)/2}$ points in all these layers.

It remains only to bound $|X_{k_0+1}|$. Consider the set $\mathscr{M}_{K_\varepsilon}^{1/4c}(X_{k_0+1})$ of the associated packing Macbeath regions. By Lemma 4.1, these Macbeath regions are pairwise disjoint. Recall that the minimum volume cap of any point in X_{k_0+1} has width at least β (used in the definition of k_0). Hence by Lemma 2.19 (and the fact that c is a constant), each of these Macbeath regions has relative volume of at least $2^{-O(n)}$. By a simple packing argument, it follows that $|X_{k_0+1}| \leq 2^{O(n)}$, which completes the proof. □

5 Applications: Banach-Mazur Approximation

In this section we show that the convex hull of the centers of any (c, ε)-covering implies the existence of an approximating polytope in the Banach-Mazur distance. The main result is given in the following lemma. Combining this with our covering from Theorem 1 establishes Theorem 2.

Lemma 5.1. *Let $0 < \varepsilon < 1$, let $K \subseteq \mathbb{R}^n$ be a well-centered convex body, and let $c \geq 2$ be a constant. Let X be the set of centers of any (c, ε')-covering of $K(1 + \varepsilon/c)$, where $\varepsilon' = \frac{1+\varepsilon}{1+\varepsilon/c} - 1$. Then $K \subset \text{conv}(X) \subset K(1 + \varepsilon)$.*

Proof. Let $\mathscr{M}$ denote the covering mentioned in the statement of the lemma. By definition, the bodies of $\mathscr{M}$ together cover $K(1 + \varepsilon/c)$ and the c-expansion of any such body about its center is contained within $K(1 + \varepsilon)$. Since each body of $\mathscr{M}$ is contained within $K(1 + \varepsilon)$, it follows that $X \subset K(1 + \varepsilon)$ and so $\text{conv}(X) \subset K(1 + \varepsilon)$. To prove that $K \subset \text{conv}(X)$, it suffices to show that there is a point of X in every cap of $K(1 + \varepsilon)$ defined by a supporting hyperplane of K.

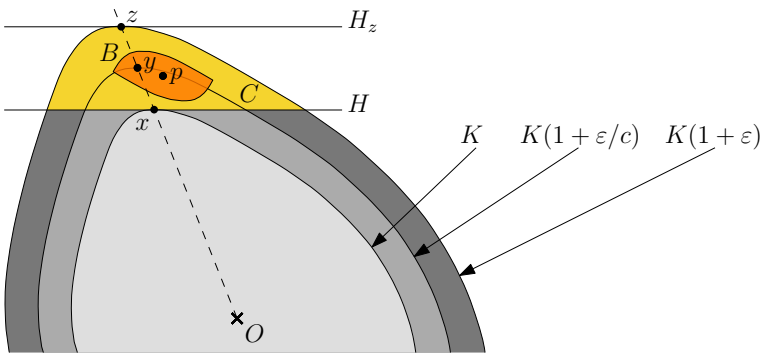


Figure 18: Proof of Lemma 5.1.

Let C be a cap of $K(1 + \varepsilon)$ defined by a supporting hyperplane H of K. Let x be a point at which H touches K. For the sake of concreteness, assume that H is horizontal and K lies below H. Consider the ray emanating from the origin passing through x. Suppose that this ray intersects the boundary of $K(1+\varepsilon/c)$ at y and the boundary of $K(1+\varepsilon)$ at z. Let H_z denote the supporting hyperplane of $K(1 + \varepsilon)$ at z. Clearly H_z is parallel to H and the distance between H and H_z is c times the distance between y and H.

Consider any body B of $\mathscr{M}$ that contains point y. We claim that the center p of the body B is contained within C. By our earlier remarks, $p \in K(1 + \varepsilon)$. Thus, we only need to show that p cannot lie below H. To see this, recall that the body formed by expanding B about its center p by a factor of c is contained within $K(1+\varepsilon)$. In particular, the point $p+c(y-p) \in K(1+\varepsilon)$. However, if p lies below H, then the point $p + c(y - p)$ would lie above H_z, and hence outside $K(1 + \varepsilon)$. It follows that p cannot lie below H, which completes the proof. □

By Lemma 4.6, there exists a (c, ε')-covering $\mathscr{M}$ for $K(1+\varepsilon/c)$ consisting of at most $2^{O(n)}/(\varepsilon')^{(n-1)/2}$ centrally symmetric convex bodies. The bound on vertices in Theorem 2 now follows immediately from the above lemma (setting $P = \text{conv}(X)$ and noting that $\varepsilon' = \Theta(\varepsilon)$), and the bound on facets follows via polarity and scaling by a factor of $(1 + \varepsilon)$.

6 Applications: Approximate CVP and IP

6.1 Preliminaries

An n-dimensional lattice $L \subseteq \mathbb{R}^n$ is the set of all integer linear combinations of a basis $b_1, \ldots, b_n$ of $\mathbb{R}^n$. Given a lattice L, a convex body K and a target $t \in \mathbb{R}^n$, the *closest vector problem* (CVP) seeks to find a closest vector in L to t under $\|\cdot\|_K$. Given a parameter $\varepsilon > 0$, the $(1+\varepsilon)$-*approximate CVP problem* seeks to find any lattice vector whose distance to t under $\|\cdot\|_K$ is at most $(1+\varepsilon)$ times the true closest.

We employ a standard computational model in our $(1+\varepsilon)$-CVP algorithm. Given reals $0 < r \leq r'$ and $x \in \mathbb{R}^n$, we say that a convex body $K \subseteq \mathbb{R}^n$ is (x, r, r')-*centered* if $x + rB_2^n \subseteq K \subseteq x + r'B_2^n$, where B_2^n is the unit Euclidean ball centered at the origin. We assume that the convex body K inducing the norm is (O, r, r')-centered, where both r and r' are given explicitly as inputs. We assume that the basis vectors of the lattice L are presented as an $n \times n$ matrix over the rationals. Input size is measured as the total number of bits used to encode r, r', t, and ε and the basis vectors of L (all rationals).

Following standard conventions, we assume that access to K is provided through a *membership oracle*, which on input $x \in \mathbb{R}^n$ returns 1 if $x \in K$ and 0 otherwise. Our algorithms apply more generally where K is presented using a *weak membership oracle*, which takes an extra parameter $\delta > 0$ and only needs to return the correct answer when x is at Euclidean distance at least δ from the boundary of K.

In the oracle model of computation, the running time is measured by the number of oracle calls and bit complexity of arithmetic operations. Note that the running time of our $(1+\varepsilon)$-CVP algorithm will be exponential in the dimension n. We will follow standard practice and suppress polynomial factors in n and the input size. We will also simplify the presentation by expressing our algorithms assuming exact oracles, but the adaptation to weak oracles is straightforward.

Our approach to approximate CVP follows one introduced by Eisenbrand *et al.* [32] for ℓ_∞ and later extended in a number of works [33, 53, 58], which employs coverings of K. Given any constant $c \geq 2$, a (c, ε)-*covering* of an (O, r, r')-centered convex body K is a collection $\mathcal{Q}$ of convex bodies, such that a factor-c expansion of each $Q \in \mathcal{Q}$ about its centroid lies within K_ε. Naszódi and Venzin showed that a $(2, \varepsilon)$-covering of K can be used to boost the approximation factor of any 2-CVP solver for general norms.

Lemma 6.1 (Naszódi and Venzin [53])**.** *Let L be a lattice and let K be an (O, r, r')-centered convex body. Given a $(2, \varepsilon)$-covering of K consisting of N centrally symmetric convex bodies, we can solve $(1+7\varepsilon)$-CVP under $\|\cdot\|_K$ with $\widetilde{O}(N)$ calls to a 2-CVP solver for norms (where $\widetilde{O}$ conceals polylogarithmic factors).*

6.2 CVP Algorithm

As in Lemma 4.6, let $K \subseteq \mathbb{R}^n$ be a well-centered convex body. In this section, we present our algorithm for computing a $(1+\varepsilon)$-approximation to the closest vector (CVP) under the norm defined by K.

Given a convex body $K \subseteq \mathbb{R}^n$, $0 < \varepsilon \leq 1$, and a constant $c \geq 2$, a (c, ε)-*enumerator* is a procedure

that outputs the elements of a (c, ε)-covering for K. Each of the elements of the covering is represented as an oracle for an (a, r, r')-centered convex body, where a, r, and r' are given explicitly in the output (as rationals). Our enumerator will be randomized in the Monte Carlo sense, meaning that it achieves a stated running time, but the output may fail to be a (c, ε)-covering with some given probability. Define an enumerator's *overhead* to be its total running time divided by the number of elements output, and its *space complexity* to be the amount of memory it needs.

Our enumerator is based on constructing hitting sets for coverings associated with certain MNets. The following lemma will be useful.

Lemma 6.2. *Let $K \subseteq \mathbb{R}^n$ be a convex body, $\Lambda \subset \operatorname{int}(K)$, and $c \geq 2$. Let X be a $(K, \Lambda, 4c)$-MNet and let $\mathscr{M} = \mathscr{M}_K^{1/4c}(X)$ be the associated covering. Let Y be any hitting set for $\mathscr{M}$ in the sense that for each $M \in \mathscr{M}$, $Y \cap M \neq \emptyset$. Then $\mathscr{M}_K^{1/c}(Y)$ is a Λ-limited c-covering with respect to K.*

Proof. Since $c > 1$, the c-expansion of any Macbeath region of $M^{1/c}(Y)$ is contained within K. To prove the covering property, let z be any point of Λ. By Lemma 4.1, there is a point $x \in X$ such that $z \in M^{1/4c}(x)$. Let y be a point of Y that is contained in $M^{1/4c}(x)$. Since $M^{1/4c}(x) \cap M^{1/4c}(y) \neq \emptyset$, by Lemma 2.14, $M^{1/4c}(x) \subseteq M^{1/c}(y)$. Thus $z \in M^{1/c}(y)$. It follows that $M^{1/c}(Y)$ is a Λ-limited c-covering with respect to K. □

The following lemma shows that membership oracles for K can be extended to its polar as well as Macbeath regions and caps that are ε-deep.

Lemma 6.3. *Given an (O, r, r')-centered convex body K, specified by a weak membership oracle, in time polynomial in n, $\log \frac{1}{\varepsilon}$, and $\log \frac{r'}{r}$ we can do the following:*

(i) Construct a weak membership oracle for K^*.

(ii) Given a point $x \in K$ such that $\operatorname{ray}(x) \geq \varepsilon$, construct a weak membership oracle for $M_K^\lambda(x)$ for any constant $\lambda > 0$.

(iii) Given a hyperplane h intersecting K which induces a cap C of width at least ε, construct a weak membership oracle for C.

Proof. Assertion (i) follows directly from standard reductions (see Theorem 4.3.2 and Lemma 4.4.1 from Grötschel, Lovász, and Schrijver [37]). Note that K^* is $\left(O, \frac{1}{r'}, \frac{1}{r}\right)$-centered. To prove (ii), note that we can construct a membership oracle for $M(x)$ by using the fact that a point $y \in M(x)$ if and only if $y \in K$ and $2x - y \in K$. If $\operatorname{ray}(x) \geq \varepsilon$, it is straightforward to show that $M(x)$ is $(x, \Omega(\varepsilon r), r')$-centered. The generalization of this construction to $M_K^\lambda(x)$ for any constant $\lambda > 0$ is immediate. Finally, to prove (iii), observe that the membership oracle is easy, but centering is the issue. We first determine the apex a of C (approximately) by finding the supporting hyperplane of K that is parallel to h. We let b denote the point midway on the segment Oa between base of the cap and a. It is easy to show that a Euclidean ball of radius $\Omega(\varepsilon r)$ can be centered at b, which is contained within C. Thus C is $(b, \Omega(\varepsilon r), 2r')$-centered. □

We will make use of standard sampling results (see, e.g., [30, 62]), which state that given $\eta > 0$, there exists an algorithm that outputs an η-uniform $X \in K$ using at most poly $\left(n, \ln \frac{1}{\eta}, \ln \frac{r'}{r}\right)$ calls to a membership oracle for K and arithmetic operations. (A random point $X \in K$ is *η-uniform* if

the total variation distance between the sample X and uniform vector in K is at most η.) As with membership oracles, it will simplify the presentation to state our constructions in terms of a true uniform sampler, but the generalization is straightforward.

Lemma 6.4. *Given $0 < \varepsilon \le 1$, constant $c \ge 2$, and an oracle for a convex body $K \subseteq \mathbb{R}^n$ which is both well-centered and (O, r, r')-centered, there exists a randomized (c, ε)-enumerator for K, which generates a covering of size*

$$2^{O(n)} \cdot \frac{1}{\varepsilon^{(n-1)/2}} \cdot \log \frac{1}{\varepsilon},$$

such that the cover elements are $(a, O(\varepsilon r), r')$-centered. The enumerator succeeds with probability $1 - 2^{-O(n)}$, and its overhead and space complexity are both polynomial in n, $\log \frac{r'}{r}$ and $\log \frac{1}{\varepsilon}$.

In our construction, the elements of the covering will be centrally symmetric, and more specifically, the covering element centered at a point $a \in K$ will be a Macbeath region of the form $M_{K_\varepsilon}^{1/c'}(a)$, where $c' = O(c)$.

Proof. Recall the layered decomposition of K described just before Lemma 4.6. For $0 \le i \le k_0$, layer i consists of points $x \in K$ such that $\mathrm{wid}(x) \in [2^{i-1}, 2^i)\varepsilon$, and layer $k_0 + 1$ consists of the remaining points $x \in K$. Note that for points in layer $k_0 + 1$, $\mathrm{wid}(x) \ge \beta$. Here β is a constant and the number of layers $k_0 + 2 = O(\log \frac{1}{\varepsilon})$. Let Λ_i denote the points in layer i. Our enumerator runs in phases, where the i-th phase generates elements of a Λ_i-limited c-covering with respect to K_ε. Clearly, the elements generated in all the phases together constitute a (c, ε)-covering for K.

For $0 \le i \le k_0$, to describe phase i of the enumerator, it will simplify notation to write K, Λ, ε, and c for $K_\varepsilon, \Lambda_i, 2^{i-1}\varepsilon$, and $4c$, respectively. Our (new) objective is to generate a Λ-limited $(c/4)$-covering in this phase. Let X be a (K, Λ, c)-MNet, let $\mathscr{M} = \mathscr{M}_K^{1/c}(X)$ be the associated covering, and let X' be a hitting set for $\mathscr{M}$. By Lemma 6.2, $\mathscr{M}_K^{4/c}(X')$ is a Λ-limited $(c/4)$-covering.

We show how to generate the hitting set X' for $\mathscr{M}$ along with the elements of $\mathscr{M}_K^{4/c}(X')$ in the desired form. In addition to the quantities $K, \Lambda, \varepsilon, c, X$ defined above, define also the quantities Λ', Y, t, t', as in Lemma 4.5. By Lemma 4.5(a), the regions of $\mathscr{M}$ are contained in $\Lambda_K(\varepsilon) = K \setminus (1 - 4\varepsilon)K$. Recall the distinction between "large" and "small" Macbeath regions of $\mathscr{M}$, based on whether its relative volume is at least t. We will use a different strategy for hitting these two kinds of regions.

First, let us consider the large Macbeath regions. We claim that it suffices to choose $(2^{O(n)}/\varepsilon^{(n-1)/2}) \cdot \log \frac{1}{\varepsilon}$ points uniformly in $\Lambda_K(\varepsilon)$ to hit all the large Macbeath regions with high probability. Before proving this, note that we can sample $\Lambda_K(\varepsilon)$ uniformly by first choosing a point p from the uniform distribution in K and then choosing a point uniformly from the portion of the ray $Op \cap \Lambda_K(\varepsilon)$. Using binary search, we can find such a point with constant probability in $O(\log \frac{r'}{r} + \log \frac{1}{\varepsilon})$ steps. We omit the straightforward details.

To prove the claim, let M be a large Macbeath region. By Lemma 4.5(a) and (b), $M \subseteq \Lambda_K(\varepsilon)$, $\mathrm{vol}_K(M) \ge \varepsilon^{(n+1)/2}$, and $\mathrm{vol}_K(\Lambda_K(\varepsilon)) = O(n\varepsilon)$. Thus $\mathrm{vol}(M)/\mathrm{vol}(\Lambda_K(\varepsilon)) \ge 2^{-O(n)}\varepsilon^{(n-1)/2}$. Also, by Lemma 4.5(b), the number of large Macbeath regions is at most $2^{O(n)}/\varepsilon^{(n-1)/2}$. A standard calculation implies that the probability of failing to hit some large Macbeath region in a layer is no more than $\varepsilon^{O(n)}$.

Next we show how to generate a hitting set for the small Macbeath regions. Intuitively, as these are small, they cannot be stabbed efficiently by uniform sampling in $\Lambda_K(\varepsilon)$. Instead, we will hit them by exploiting the relationship between the small Macbeath regions of $\mathscr{M}$ and the large Macbeath regions of $\mathscr{M}' = \mathscr{M}_{K^*}^{1/5}(Y)$. Recall that Y is a $(K^*, \Lambda', 5)$-MNet, where Λ' is the boundary of $(1-\varepsilon)K^*$, and the large Macbeath regions of $\mathscr{M}'$ have volume at least $t' = 2^{-O(n)}\varepsilon^{(n+1)/2}$. Our high-level idea for hitting the small Macbeath regions of $\mathscr{M}$ is to hit the large Macbeath regions of $\mathscr{M}'$ and then uniformly sample the associated ε-representative cap of K.

More precisely, we perform $(2^{O(n)}/\varepsilon^{(n-1)/2}) \cdot \log(1/\varepsilon)$ iterations of the following procedure. First, we choose a point p uniformly in $\Lambda_{K^*}(\varepsilon) = K^* \setminus (1-2\varepsilon)K^*$. (This can be done in a manner analogous to uniformly sampling $\Lambda_K(\varepsilon)$, which we described above.) Next, we sample uniformly in the cap C_p^{32}, where C_p is p's ε-representative cap in K. We claim that this procedure stabs all the small Macbeath regions of $\mathscr{M}$ with high probability.

To see why, recall from Lemma 4.5(e) that for any small Macbeath region $M \in \mathscr{M}$, there is a large Macbeath region $M' \in \mathscr{M}'$ with the following properties. Let y be any point in M' and let C_y be y's ε-representative cap in K. Then $M \subseteq C_y^{32}$ and $\mathrm{vol}(M) \geq 2^{-O(n)}\,\mathrm{vol}(C_y^{32})$. Also, by properties (c) and (d) of Lemma 4.5, we have $M' \subseteq \Lambda_{K^*}(\varepsilon)$, $\mathrm{vol}_{K^*}(M') \geq 2^{-O(n)}\varepsilon^{(n+1)/2}$, and $\mathrm{vol}_{K^*}(\Lambda_{K^*}(\varepsilon)) = O(n\varepsilon)$. It follows that the probability of hitting a fixed small Macbeath region M of $\mathscr{M}$ in any one trial (*i.e.*, sampling p uniformly in $\Lambda_{K^*}(\varepsilon)$, followed by sampling a point uniformly in the cap C_p^{32}) is at least $2^{-O(n)}\varepsilon^{(n-1)/2}$. Also, by Lemma 4.5(f), the number of small Macbeath regions of $\mathscr{M}$ is at most $2^{O(n)}/\varepsilon^{(n-1)/2}$. The same calculation as for large Macbeath regions implies that the probability of failing to hit some small Macbeath region of $\mathscr{M}$ is no more than $\varepsilon^{O(n)}$.

Putting it together, it follows that we can hit the Macbeath regions in all the layers i, $0 \leq i \leq k_0$ with failure probability bounded by $2^{-O(n)}$.

Finally, we describe phase k_0+1 of the enumerator. Recall that Λ_{k_0+1} consists of points such that the associated minimum volume cap has width at least β, where β is a constant. Let X be a $(K_\varepsilon, \Lambda_{k_0+1}, 4c)$-MNet and let $\mathscr{M} = \mathscr{M}_{K_\varepsilon}^{1/4c}(X)$ be the associated covering. By Lemma 2.19, the Macbeath regions of $\mathscr{M}$ have relative volume at least $2^{-O(n)}$. Thus, we can hit all the Macbeath regions of $\mathscr{M}$ with $2^{O(n)}$ uniformly sampled points in K with failure probability no more that $2^{-O(n)}$.

In closing, we mention that Lemma 6.3 shows that the enumerator can construct the three membership oracles it needs for its operation. Specifically, for each point in the hitting set, by part (ii), we can construct an oracle for the associated Macbeath region. By part (i), we can construct an oracle for K^*, which we need to sample uniformly in K^*, and by part (iii), we can construct oracles for the caps of K which need to be sampled uniformly. This completes the proof. □

Our algorithm and its analysis follows the general structure presented by Eisenbrand *et al.* [32] and Naszódi and Venzin [53]. We solve the $(1+\varepsilon)$-CVP in the norm $\|\cdot\|_K$ by reducing it to the $(1+\varepsilon)$-gap CVP problem in this norm. In the $(1+\varepsilon)$-gap CVP problem, given a target t and a number $\gamma > 0$, we have to either find a lattice vector whose distance to t is at most γ or assert that all lattice vectors have distance more than $\gamma/(1+\varepsilon)$. We solve the $(1+\varepsilon)$-CVP problem via binary search on the distance from the target. Given the problem parameters n, ε, $\rho = \frac{r'}{r}$, and letting b denote the number of bits in the numerical inputs, the number of different distance values that

need to be tested can be shown to be $O(\log n + \log \frac{1}{\varepsilon} + \log \rho + \log b)$. Let $\Phi(n, \varepsilon, \rho, b)$ denote this quantity. For each distance, we need to solve the $(1+\varepsilon)$-gap CVP problem. In turn, the $(1+\varepsilon)$-gap CVP problem is solved by invoking the (c, ε)-enumerator. For each of the N bodies generated by the enumerator, we need to call a 2-gap CVP solver. For this purpose, we use Dadush and Kun's deterministic algorithm [25] as the 2-gap CVP solver. As this 2-gap CVP solver always yields the correct answer, the only source of error in our algorithm arises from the fact that a valid covering may not be generated. The failure rate of our (c, ε)-enumerator is $2^{-O(n)}$, which we reduce further by running it $\log \Phi(n, \varepsilon, \rho, b)$ times. This ensures that all the coverings generated over the course of solving the $(1+\varepsilon)$-CVP problem are correct with probability at least $1 - 2^{-O(n)}$. Recalling that the algorithm by Dadush and Kun takes $2^{O(n)}$ time and $O(2^n)$ space, we have established Theorem 3 (neglecting polynomial factors in the input size).

6.3 Approximate Integer Programming

Through a reduction by Dadush, our CVP result also implies a new algorithm for approximate integer programming (IP). We are given a convex body $K \subseteq \mathbb{R}^n$ and an n-dimensional lattice $L \subset \mathbb{R}^n$, and we are to determine either that $K \cap L = \emptyset$ or return a point $y \in K \cap L$. The best algorithm known for this problem takes $n^{O(n)}$ time [42], which has sparked interest in the approximate version. In approximate integer programming, the algorithm must return a lattice point in $(1+\varepsilon)K$ (where the $(1+\varepsilon)$-expansion of K is about the centroid), or assert that there are no lattice points in K.

Dadush [24] has shown that approximate IP can be reduced to $(1+\varepsilon)$-CVP problem under a well-centered norm. His method is to first find an approximate centroid p and then make one call to a $(1+\varepsilon)$-CVP solver for the norm induced by $K - p$. By plugging in our solver, we obtain an immediate improvement with respect to the ε-dependencies (neglecting polynomial factors in the input size).

Theorem 5. *There exists a $2^{O(n)}/\varepsilon^{(n-1)/2}$-time and $O(2^n)$-space randomized algorithm which solves the approximate integer programming problem with probability at least $1 - 2^{-n}$.*

7 Conclusions

In this paper we have demonstrated the existence of concise coverings for convex bodies. In particular, we have shown that given a real parameter $0 < \varepsilon \leq 1$ and constant $c \geq 2$, any well-centered convex body K in $\mathbb{R}^n$ has a (c, ε)-covering for K consisting of at most $2^{O(n)}/\varepsilon^{(n-1)/2}$ centrally symmetric convex bodies. This bound is optimal with respect to ε-dependencies. Furthermore, we have shown that the size of the covering is instance-optimal up to factors of $2^{O(n)}$. Coverings are useful structures. One consequence of our improved coverings is a new (and arguably simpler) construction of ε-approximating polytopes in the Banach-Mazur metric. We have also demonstrated improved approximation algorithms for the closest-vector problem in general norms and integer programming.

In contrast to earlier approaches, our covering elements are based on scaled Macbeath regions for the body K. This raises the question of what is the best choice of covering elements. Eisenbrand *et al.* [32] showed that the size of any covering based on ellipsoids grows as $\Omega(n^{n/2})$, even when the domain being covered is a hypercube. Our Macbeath-based approach results in a reduction

of the dimensional dependence to $2^{O(n)}$ for any convex body. Macbeath regions have many nice properties, including the fact that it is easy to construct membership oracles from a membership oracle for the original body. Unfortunately, Macbeath regions have drawbacks, including the fact that their boundary complexity can be as high as K's boundary complexity.

It is natural to wonder whether we can do better than ellipsoid-based coverings with uniform covering elements. For example, can we build more economical coverings based on affine transformations of some other fixed convex body. Recent results from the theory of volume ratios imply that this is not generally possible. The work of Galicer, Merzbacher, and Pinasco [36] (combined with polarity) implies that for any convex body L, there exists a convex body K, such that for any affine transformation T, if $T(L)$ is contained within K, then $\mathrm{vol}(T(L))$ is at most $\mathrm{vol}(K)/(bn)^{n/2}$, where b is an absolute constant. A straightforward packing argument implies that if we restrict covering elements to affine images of a fixed convex body, the worst-case size of a (c, ε) covering grows as $\Omega(n^{n/2})$ (independent of ε).

References

[1] A. Abdelkader and D. M. Mount. Economical Delone sets for approximating convex bodies. *Proc. 16th Scand. Workshop Algorithm Theory*. 2018, 4:1–4:12. DOI: 10.4230/LIPIcs.SWAT.2018.4.

[2] D. Aggarwal, H. Bennett, A. Golovnev, and N. Stephens-Davidowitz. Fine-grained hardness of CVP(P)-Everything that we can prove (and nothing else). *Proc. 32nd Annu. ACM-SIAM Sympos. Discrete Algorithms*. 2021, pp. 1816–1835. DOI: 10.1137/1.9781611976465.109.

[3] D. Aggarwal, D. Dadush, and N. Stephens-Davidowitz. Solving the closest vector problem in 2^n Time – The Discrete Gaussian strikes again! *Proc. 56th Annu. IEEE Sympos. Found. Comput. Sci.* 2015, pp. 563–582. DOI: 10.1109/FOCS.2015.41.

[4] M. Ajtai, R. Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. *Proc. 33rd Annu. ACM Sympos. Theory Comput.* 2001, pp. 601–610. DOI: 10.1145/380752.380857.

[5] S. Arora. "Probabilistic checking of proofs and hardness of approximation problems". PhD thesis. University of California, Berkeley, 1994.

[6] R. Arya, S. Arya, G. D. da Fonseca, and D. M. Mount. Optimal Bound on the Combinatorial Complexity of Approximating Polytopes. *ACM Trans. Algorithms* 18 (2022), pp. 1–29. DOI: 10.1145/3559106.

[7] S. Arya, G. D. da Fonseca, and D. M. Mount. Near-optimal ε-kernel construction and related problems. *Proc. 33rd Internat. Sympos. Comput. Geom.* 2017, 10:1–15. DOI: 10.4230/LIPIcs.SoCG.2017.10. URL: https://arxiv.org/abs/1703.10868.

[8] S. Arya, G. D. da Fonseca, and D. M. Mount. On the combinatorial complexity of approximating polytopes. *Discrete Comput. Geom.* 58.4 (2017), pp. 849–870. DOI: 10.1007/s00454-016-9856-5.

[9] S. Arya, G. D. da Fonseca, and D. M. Mount. Optimal approximate polytope membership. *Proc. 28th Annu. ACM-SIAM Sympos. Discrete Algorithms*. 2017, pp. 270–288. DOI: 10.1137/1.9781611974782.18.

[10] S. Arya, G. D. da Fonseca, and D. M. Mount. Optimal area-sensitive bounds for polytope approximation. *Proc. 28th Annu. Sympos. Comput. Geom.* 2012, pp. 363–372. DOI: 10.1145/2261250.2261305.

[11] S. Arya, G. D. da Fonseca, and D. M. Mount. Polytope approximation and the Mahler volume. *Proc. 23rd Annu. ACM-SIAM Sympos. Discrete Algorithms*. 2012, pp. 29–42. DOI: 10.1137/1.9781611973099.3.

[12] S. Arya, T. Malamatos, and D. M. Mount. The effect of corners on the complexity of approximate range searching. *Discrete Comput. Geom.* 41 (2009), pp. 398–443. DOI: 10.1007/s00454-009-9140-z.

[13] S. Arya, D. M. Mount, and J. Xia. Tight lower bounds for halfspace range searching. *Discrete Comput. Geom.* 47 (2012), pp. 711–730. DOI: 10.1007/s00454-012-9412-x.

[14] I. Bárány. Random polytopes, convex bodies, and approximation. *Stochastic Geometry*. Ed. by W. Weil. Vol. 1892. Lecture Notes in Mathematics. Springer, 2007, pp. 77–118. DOI: 10.1007/978-3-540-38175-4_2.

[15] I. Bárány. The technique of M-regions and cap-coverings: A survey. *Rend. Circ. Mat. Palermo* 65 (2000), pp. 21–38. URL: https://users.renyi.hu/~barany/.

[16] I. Bárány and D. G. Larman. Convex bodies, economic cap coverings, random polytopes. *Mathematika* 35 (1988), pp. 274–291.

[17] A. Barvinok. Thrifty approximations of convex bodies by polytopes. *Int. Math. Res. Not.* 2014 (2013), pp. 4341–4356. DOI: 10.1093/imrn/rnt078.

[18] H. Bennett, A. Golovnev, and N. Stephens-Davidowitz. On the quantitative hardness of CVP. *Proc. 58th Annu. IEEE Sympos. Found. Comput. Sci.* 2017, pp. 13–24. DOI: 10.1109/FOCS.2017.11.

[19] J. Blömer and S. Naewe. Sampling methods for shortest vectors, closest vectors and successive minima. *Theo. Comp. Sci.* 410 (2009), pp. 1648–1665. DOI: 10.1016/j.tcs.2008.12.045.

[20] K. Böröczky, Jr. Approximation of general smooth convex bodies. *Adv. Math.* 153 (2000), pp. 325–341. DOI: 10.1006/aima.1999.1904.

[21] J. Bourgain and V. D. Milman. New volume ratio properties for convex symmetric bodies. *Invent. Math.* 88 (1987), pp. 319–340. DOI: 10.1007/BF01388911.

[22] H. Brönnimann, B. Chazelle, and J. Pach. How hard is halfspace range searching? *Discrete Comput. Geom.* 10 (1993), pp. 143–155. DOI: 10.1007/BF02573971.

[23] E. M. Bronshteyn and L. D. Ivanov. The approximation of convex sets by polyhedra. *Siberian Math. J.* 16 (1976), pp. 852–853.

[24] D. Dadush. A randomized sieving algorithm for approximate integer programming. *Algorithmica* 70 (2014), pp. 208–244. DOI: 10.1007/s00453-013-9834-8.

[25] D. Dadush and G. Kun. Lattice sparsification and the approximate closest vector problem. *Theo. of Comput.* 12 (2016), pp. 1–34. DOI: 10.4086/toc.2016.v012a002.

[26] D. Dadush, C. Peikert, and S. Vempala. Enumerative lattice algorithms in any norm via M-ellipsoid Coverings. *Proc. 52nd Annu. IEEE Sympos. Found. Comput. Sci.* 2011, pp. 580–589. DOI: 10.1109/FOCS.2011.31.

[27] I. Dinur, G. Kindler, R. Raz, and S. Safra. Approximating CVP to within almost-polynomial factors is NP-hard. *Combinatorica* 23 (2003), pp. 205–243. DOI: 10.1007/s00493-003-0019-y.

[28] R. M. Dudley. Metric entropy of some classes of sets with differentiable boundaries. *J. Approx. Theory* 10.3 (1974), pp. 227–236. DOI: 10.1016/0021-9045(74)90120-8.

[29] K. Dutta, A. Ghosh, B. Jartoux, and N. H. Mustafa. Shallow packings, semialgebraic set systems, Macbeath regions and polynomial partitioning. *Discrete Comput. Geom.* 61 (2019), pp. 756–777. DOI: 10.1007/s00454-019-00075-0.

[30] M. Dyer, A. Frieze, and R. Kannan. A random polynomial-time algorithm for approximating the volume of convex bodies. *J. Assoc. Comput. Mach.* 38 (1991), pp. 1–17. DOI: 10.1145/102782.102783.

[31] H. G. Eggleston. *Convexity*. Cambridge University Press, 1958. DOI: 10.1017/CBO9780511566-172.

[32] F. Eisenbrand, N. Hähnle, and M. Niemeier. Covering cubes and the closest vector problem. *Proc. 27th Annu. Sympos. Comput. Geom.* 2011, pp. 417–423. DOI: 10.1145/1998196.1998264.

[33] F. Eisenbrand and M. Venzin. Approximate CVPs in time $2^{0.802n}$. *J. Comput. Sys. Sci.* 124 (2022), pp. 129–139. DOI: 10.1016/j.jcss.2021.09.006.

[34] P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. *Tecnical Report, Department of Mathmatics, University of Amsterdam* (1981).

[35] G. Ewald, D. G. Larman, and C. A. Rogers. The directions of the line segments and of the r-dimensional balls on the boundary of a convex body in Euclidean space. *Mathematika* 17 (1970), pp. 1–20. DOI: 10.1112/S0025579300002655.

[36] D. Galicer, M. Merzbacher, and D. Pinasco. Asymptotic estimates for the largest volume ratio of a convex body. *Revista Matemática Iberoamericana* 37 (2021), pp. 2347–2372. DOI: 10.4171/RMI/1263.

[37] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric algorithms and combinatorial optimization*. Springer-Verlag, 1988. DOI: 10.1002/bimj.4710320805.

[38] P. M. Gruber. Asymptotic estimates for best and stepwise approximation of convex bodies I. *Forum Math.* 5 (1993), pp. 281–298. DOI: 10.1515/form.1993.5.281.

[39] B. Grünbaum. Measures of symmetry for convex sets. *Proc. Sympos. Pure Math.* Vol. VII. 1963, pp. 233–270. DOI: 10.1090/pspum/007/0156259.

[40] G. Hanrot, X. Pujol, and D. Stehlé. Algorithms for the shortest and closest lattice vector problems. *Internat. Conf. Coding and Cryptology*. 2011, pp. 159–190. DOI: 10.1007/978-3-642-20901-7_10.

[41] A. Joux and J. Stern. Lattice reduction: A toolbox for the cryptanalyst. *J. Cryptology* 11 (1998), pp. 161–185. DOI: 10.1007/s001459900042.

[42] R. Kannan. Minkowski's convex body theorem and integer programming. *Math. Oper. Res* 12 (1987), pp. 415–440. DOI: 10.1287/moor.12.3.415.

[43] G. Kuperberg. From the Mahler conjecture to Gauss linking integrals. *Geom. Funct. Anal.* 18 (2008), pp. 870–892. DOI: 10.1007/s00039-008-0669-4.

[44] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.* 261 (1982), pp. 515–534. DOI: 10.1007/BF01457454.

[45] H. W. Lenstra Jr. Integer programming with a fixed number of variables. *Math. Oper. Res* 8 (1983), pp. 538–548. URL: https://www.jstor.org/stable/3689168.

[46] A. M. Macbeath. A theorem on non-homogeneous lattices. *Ann. of Math.* 56 (1952), pp. 269–293. DOI: 10.2307/1969800.

[47] M. Meyer and A. Pajor. On the Blaschke-Santaló inequality. *Arch. Math.* 55 (1990), pp. 82–93. DOI: 10.1007/BF01199119.

[48] M. Meyer and E. M. Werner. The Santaló-regions of a convex body. *Trans. Amer. Math. Soc.* 350 (1998), pp. 4569–4591. DOI: 10.1090/S0002-9947-98-02162-X.

[49] D. Micciancio and P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. *SIAM J. Comput.* 42 (2013), pp. 1364–1391. DOI: 10.1137/100811970.

[50] V. D. Milman and A. Pajor. Entropy and asymptotic geometry of non-symmetric convex bodies. *Adv. Math.* 152 (2000), pp. 314–335.

[51] N. H. Mustafa and S. Ray. Near-optimal generalisations of a theorem of Macbeath. *Proc. 31st Internat. Sympos. on Theoret. Aspects of Comp. Sci.* 2014, pp. 578–589. DOI: 10.4230/LIPIcs.STACS.2014.578.

[52] M. Naszódi, F. Nazarov, and D. Ryabogin. Fine approximation of convex bodies by polytopes. *Amer. J. Math* 142 (2020), pp. 809–820. DOI: 10.1353/ajm.2020.0018.

[53] M. Naszódi and M. Venzin. Covering convex bodies and the closest vector problem. *Discrete Comput. Geom.* 67 (2022), pp. 1191–1210. DOI: 10.1007/s00454-022-00392-x.

[54] F. Nazarov. The Hörmander proof of the Bourgain-Milman theorem. *Geometric Aspects of Functional Analysis*. Springer, 2012, pp. 335–343. DOI: 10.1007/978-3-642-29849-3_20.

[55] P. Q. Nguyen and J. Stern. The two faces of lattices in cryptology. *Internat. Crypto. and Lattices Conf.* 2001, pp. 146–180. DOI: 10.1007/3-540-45537-X_24.

[56] A. M. Odlyzko. The rise and fall of knapsack cryptosystems. *Symp. of Appl. Math.* 1990, pp. 75–88. DOI: 10.1090/psapm/042.

[57] C. A. Rogers and G. C. Shephard. The difference body of a convex body. *Arch. Math.* 8 (1959), pp. 220–233. DOI: 10.1007/BF01899997.

[58] T. Rothvoss and M. Venzin. Approximate CVP in time $2^{0.802n}$ – Now in any norm! *Proc. 23rd Internat. Conf. on Integ. Prog. and Comb. Opt. (IPCO 2022)*. 2022, pp. 440–453. DOI: 10.1007/978-3-031-06901-7_33.

[59] L. A. Santaló. An affine invariant for convex bodies of n-dimensional space. *Port. Math.* 8 (1949). (In Spanish), pp. 155–161.

[60] R. Schneider. *Convex bodies: The Brunn-Minkowski theory*. Cambridge University Press, 1993. DOI: 10.1017/CBO9780511526282.

[61] G. Toth. *Measures of symmetry for convex sets and stability*. Springer, 2015. DOI: 10.1007/978-3-319-23733-6.

[62] S. Vempala. Geometric random walks: A survey. *Combinatorial and computational geometry*. Ed. by J. Goodman, J. Pach, and E. Welzl. MSRI, 2005, pp. 573–612.

[63] C. Vernicos and C. Walsh. "Flag-approximability of convex bodies and volume growth of Hilbert geometries". HAL Archive (hal-01423693i). 2016. URL: https://hal.archives-ouvertes.fr/hal-01423693.