UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Fakultät für Elektrotechnik, Informatik und Mathematik
Arbeitsgruppe Codes und Kryptographie

Number of Voronoi-relevant vectors in lattices with respect to arbitrary norms

Master's Thesis

in Partial Fulfillment of the Requirements for the Degree of

Master of Science

by

Kathlén Kohn

Fürstenallee 136

33102 Paderborn

submitted to:

Prof. Dr. Johannes Blömer

and

Prof. Dr. Friedhelm Meyer auf der Heide

Paderborn, July 19, 2015

Declaration

(Translation from German)

I hereby declare that I prepared this thesis entirely on my own and have not used outside sources without declaration in the text. Any concepts or quotations applicable to these sources are clearly attributed to them. This thesis has not been submitted in the same or substantially similar version, not even in part, to any other authority for grading and has not been published elsewhere.

Original Declaration Text in German:

Erklärung

Ich versichere, dass ich die Arbeit ohne fremde Hilfe und ohne Benutzung anderer als der angegebenen Quellen angefertigt habe und dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen hat und von dieser als Teil einer Prüfungsleistung angenommen worden ist. Alle Ausführungen, die wörtlich oder sinngemäß übernommen worden sind, sind als solche gekennzeichnet.

City, Date

Signature

Contents

List of Figures

1 Introduction

1.1 Motivation

An *n-dimensional lattice* is a discrete, additive subgroup of $\mathbb{R}^n$. Such a lattice can also be represented as the set of all integer linear combinations of some linearly independent vectors in $\mathbb{R}^n$, where the linearly independent vectors are called a *basis* of the lattice. There are many famous problems on lattices, including the *shortest vector problem* (SVP) and the *closest vector problem* (CVP). In the SVP, one is asked to find a shortest nonzero vector in a lattice generated by a given basis. In the CVP, one is given a basis as well as an arbitrary target vector $x \in \mathbb{R}^n$, and needs to find a vector in the lattice generated by the basis that is closest to the target x. Both problems have been shown to be NP-hard (under randomized reductions in the case of SVP) [2, 12].

Micciancio and Voulgaris gave an algorithm for both problems having $2^{O(n)}$ time and space complexity with respect to the Euclidean norm [13]. The central part of their algorithm is solving a variant of the CVP where additionally to a lattice basis and a target vector one is given a description of the *Voronoi cell* of the lattice, i.e., the set of all points in $\mathbb{R}^n$ that are at least as close to 0 as to any other lattice vector. It is clear that the Voronoi cell can be described as the intersection of all halfspaces $\mathcal{H}^{\leq}_{\|\cdot\|_2}(0, v)$ for all lattice vectors v, where $\mathcal{H}^{\leq}_{\|\cdot\|_2}(0, v)$ denotes the set of all points in $\mathbb{R}^n$ that are at least as close to 0 as to v. Using the Euclidean norm, it is sufficient to consider all *Voronoi-relevant vectors* when taking this intersection. A lattice vector $v \neq 0$ is called Voronoi-relevant if there is some $x \in \mathbb{R}^n$ having the same distance to 0 as to v but a strictly larger distance to all other lattice vectors. The algorithm by Micciancio and Voulgaris uses the set of Voronoi-relevant vectors as a description of the Voronoi cell and thus relies on the fact that there are at most $2(2^n - 1)$ Voronoi-relevant vectors in a lattice when the Euclidean norm is used. This was shown in [1] with the crucial parallelogram identity that holds exactly for norms induced by a scalar product, e.g., the Euclidean norm. The open problems sections in [13] asks for an extension of the algorithm by Micciancio and Voulgaris to all p-norms, but for this one needs to find an adequate upper bound for the number of Voronoi-relevant vectors with respect to arbitrary p-norms.

1.2 Summary of results

The main goal of this thesis is to analyze the number of Voronoi-relevant vectors in a lattice with respect to norms other than the Euclidean norm.

First, it will be shown that the upper bound $2(2^n - 1)$ shown in [1] still holds for *strictly convex norms* in the case $n = 2$, i.e., that a two-dimensional lattice has at most six Voronoi-relevant vectors with respect to an arbitrary strictly convex norm. A norm $\|\cdot\|$ is called strictly convex if for all $x, y \in \mathbb{R}^n$ with $x \neq y$ and $\|x\| = \|y\|$ and all $0 < \tau < 1$ it holds that $\|\tau x + (1-\tau)y\| < \|x\|$. For non-strictly convex norms an example of a two-dimensional lattice will be given where the Voronoi-relevant vectors are not sufficient to determine the Voronoi cell. Thus, the notion of *generalized Voronoi-relevant vectors* will be introduced. For two-dimensional lattices with non-strictly convex norms it will be shown that the number of generalized Voronoi-relevant vectors is not bounded by a constant, which yields that there is no generalization of the upper bound $2(2^n - 1)$ shown in [1] for non-strictly convex norms.

Unfortunately, the same holds for strictly convex norms in dimensions higher than two. The main statement of this thesis is that an upper bound, solely depending on the lattice dimension, for the number of Voronoi-relevant vectors does not exist for general dimensions and general strictly convex norms. For this, a family of three-dimensional lattices will be constructed whose number of Voronoi-relevant vectors is not bounded by a constant with respect to the 3-norm. Hence, the algorithm by Micciancio and Voulgaris in [13] cannot be easily extended to general p-norms, since they require that the upper bound $2(2^n - 1)$ shown in [1] only depends on the dimension n. Moreover, it will be shown for an arbitrary norm $\|\cdot\|$ that there are at most $\left(1 + 4\frac{\mu(\Lambda,\|\cdot\|)}{\lambda_1(\Lambda,\|\cdot\|)}\right)^n$ (generalized) Voronoi-relevant vectors in an n-dimensional lattice Λ, where $\mu(\Lambda, \|\cdot\|)$ denotes the minimal $d \in \mathbb{R}_{>0}$ such that every $x \in \operatorname{span}(\Lambda)$ has at most distance d to some lattice vector and $\lambda_1(\Lambda, \|\cdot\|)$ is the length of a shortest nonzero lattice vector. This bound, while depending exponentially on the dimension, is obviously also affected by other lattice properties. The number of (generalized) Voronoi-relevant vectors of the lattice families constructed for the three-dimensional, strictly convex case as well as for the two-dimensional, non-strictly convex case will be compared with this bound.

All these investigations raised the question how Voronoi cells and their *facets* look with respect to norms other than the Euclidean norm. Therefore, the last part of this thesis examines the set of vectors which is sufficient to determine the Voronoi cell of a given lattice as well as the $(n-1)$-dimensional facets of the Voronoi cell and their connectedness. Two conjectures will be stated which have important implications: One conjecture yields that the Voronoi cell of a lattice with respect to a strictly convex norm is determined completely by the Voronoi-relevant vectors, and the other conjecture implies that under sufficiently nice norms there exists a bijection between the $(n-1)$-dimensional facets of the Voronoi cell and the Voronoi-relevant vectors. The latter statement will be shown for two-dimensional lattices without using the conjectures. For two-dimensional lattices it also holds that these facets are connected, which is probably not true for higher dimensions, since there exist Voronoi cells of finite sets of points with

unconnected facets when a p-norm for $p \in \mathbb{N}, p \geq 3$ is used. Additionally, one of the two conjectures leads to a fundamental result about *bisectors*: The bisector between two given points $a, b \in \mathbb{R}^n$ with $a \neq b$ is defined as the set of all $x \in \mathbb{R}^n$ having the same distance to a as to b. Under sufficiently nice norms and the assumption of the mentioned conjecture, it holds that the bisector between a and b intersected with the bisector between b and c is homeomorphic to $\mathbb{R}^{n-2}$ as long as a, b, c are non-collinear. To the best of my knowledge, this result is only known for at most three dimensions [10] and it is known that each such bisector is homeomorphic to $\mathbb{R}^{n-1}$ [6].

1.3 Problem definition

Throughout this work the following notation will be used:

- $\mathbb{N}$ denotes the set of all strictly positive integers.
- For a ring R, elements in R^n are column vectors. For $x \in R^n$, the transposed row vector is denoted by x^T. Analogously for $x_1, \ldots, x_n \in R$, the transposed $(x_1, \ldots, x_n)^T \in R^n$ is a column vector.
- The dot product on $\mathbb{R}^n$ is denoted by

$$\begin{aligned} \langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n &\longrightarrow \mathbb{R}, \\ (x, y) &\longmapsto x^T y. \end{aligned}$$

- For $p \in \mathbb{R}$ with $p \geq 1$,

$$\begin{aligned} \| \cdot \|_p : \mathbb{R}^n &\longrightarrow \mathbb{R}_{\geq 0}, \\ (x_1, \ldots, x_n)^T &\longmapsto \left(\sum |x_i|^p \right)^{1/p} \end{aligned}$$

  denotes the p-norm on $\mathbb{R}^n$. The ∞-norm on $\mathbb{R}^n$ is given by

$$\begin{aligned} \| \cdot \|_\infty : \mathbb{R}^n &\longrightarrow \mathbb{R}_{\geq 0}, \\ (x_1, \ldots, x_n)^T &\longmapsto \max \{ |x_i| \mid i \in \{1, \ldots, n\} \}. \end{aligned}$$

- Let $V \subseteq \mathbb{R}^n$ be a subspace with norm $\| \cdot \| : V \to \mathbb{R}_{\geq 0}$. For $r \in \mathbb{R}_{\geq 0}$ and $c \in V$ define

$$\begin{aligned} \mathcal{B}_{\| \cdot \|, r}(c) &:= \{ x \in V \mid \|x - c\| < r \} \text{ and} \\ \overline{\mathcal{B}}_{\| \cdot \|, r}(c) &:= \{ x \in V \mid \|x - c\| \leq r \}. \end{aligned}$$

- For a subset $S \subseteq \mathbb{R}^n$ and $\lambda \in \mathbb{R}$ as well as $t \in \mathbb{R}^n$, let $\lambda S := \{ \lambda x \mid x \in S \}$ and $S + t := \{ x + t \mid x \in S \}$.

- For a subset $S \subseteq \mathbb{R}^n$, the linear span of S is denoted by

$$\operatorname{span}(S) := \left\{ \sum_{i=1}^{m} \lambda_i v_i \;\middle|\; m \in \mathbb{N}, v_i \in S, \lambda_i \in \mathbb{R} \right\}.$$

- For a subspace $V \subseteq \mathbb{R}^n$ let $\dim(V)$ denote its dimension.

- For a submanifold $X \subseteq \mathbb{R}^n$ of dimension $m \leq n$ with $M \subseteq X$ measurable,

$$\operatorname{vol}_m(M) := \int_X \chi_M(x)\, dx$$

  denotes the m-dimensional volume of M, where

$$\chi_M : X \to \{0,1\}, x \mapsto \begin{cases} 1 & \text{, if } x \in M \\ 0 & \text{, if } x \in X \setminus M \end{cases}$$

  is the indicator function of M.

- An adjusted version of the signum function will be used which is given by

$$\begin{aligned} \operatorname{sgn} : \mathbb{R} &\longrightarrow \{1,-1\}, \\ x &\longmapsto \begin{cases} 1 & \text{, if } x \geq 0 \\ -1 & \text{, if } x < 0 \end{cases}. \end{aligned}$$

- Whenever m elements $a_1, \ldots, a_m$ are listed, it is assumed that $m \in \mathbb{N}$.

The main object of study are lattices.

Definition 1.1 *Let $b_1, \ldots, b_m \in \mathbb{R}^n$ be linearly independent. Then*

$$\mathcal{L}(b_1, \ldots, b_m) := \left\{ \sum_{i=1}^{m} z_i b_i \;\middle|\; z_1, \ldots, z_m \in \mathbb{Z} \right\}$$

is a lattice *with* basis $(b_1, \ldots, b_m)$*. In addition, n is called the* dimension *and m the* rank *of the lattice.*

A classical result – e.g., shown in [4] – is that a subset $\Lambda \subseteq \mathbb{R}^n$ is a lattice if and only if it is a non-trivial discrete subgroup of $(\mathbb{R}^n, +)$. To state this formally, one needs to introduce the notion of a discrete subset of $\mathbb{R}^n$.

Definition 1.2 *A subset $\Lambda \subseteq \mathbb{R}^n$ is called* discrete *if there exists $\varepsilon \in \mathbb{R}_{>0}$ such that for every $x, y \in \Lambda$ with $x \neq y$ it holds that $\|x - y\|_2 \geq \varepsilon$.*

Proposition 1.3 *Let $\Lambda \subseteq \mathbb{R}^n$. There exist linearly independent $b_1, \ldots, b_m \in \mathbb{R}^n$ with $\Lambda = \mathcal{L}(b_1, \ldots, b_m)$ if and only if $(\Lambda, +)$ is a discrete subgroup of $(\mathbb{R}^n, +)$ with $\Lambda \neq \{0\}$.*

Commonly investigated quantities of lattices are their successive minima as well as their covering radius. Here, mostly the first successive minimum is needed, which equals the length of a shortest nonzero lattice vector. The covering radius is the smallest $d \in \mathbb{R}_{\geq 0}$ such that all vectors in the linear span of the given lattice are at most of distance d from a lattice vector.

Definition 1.4 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank m. For $i \in \{1, \ldots, m\}$, the* i-th successive minimum *of Λ with respect to $\|\cdot\|$ is*

$$\lambda_i(\Lambda, \|\cdot\|) := \inf\left\{r \in \mathbb{R}_{\geq 0} \;\middle|\; \dim\left(\operatorname{span}\left(\Lambda \cap \overline{\mathcal{B}}_{\|\cdot\|,r}(0)\right)\right) \geq i\right\}.$$

The covering radius *of Λ with respect to $\|\cdot\|$ is*

$$\mu(\Lambda, \|\cdot\|) := \inf\{d \in \mathbb{R}_{\geq 0} \mid \forall x \in \operatorname{span}(\Lambda)\, \exists v \in \Lambda : \|x - v\| \leq d\}.$$

Apart from these classical notions, this thesis is mostly concerned with the Voronoi cell of a lattice. Such a Voronoi cell can be defined for every element from a given discrete set of points as the set of all vectors that are at least as close to this element as to any other point of the given set. If the given set of points forms a lattice, all Voronoi cells for the lattice points will be translates of the Voronoi cell of the lattice origin such that is enough to consider this specific Voronoi cell.

Definition 1.5 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\mathcal{P} \subseteq \mathbb{R}^n$ be a discrete subset. The* Voronoi cell of $a \in \mathcal{P}$ *is defined as*

$$\mathcal{V}_{\|\cdot\|,\mathcal{P}}(a) := \{x \in \operatorname{span}(\mathcal{P}) \mid \forall b \in \mathcal{P} : \|x - a\| \leq \|x - b\|\}.$$

If $\mathcal{P}$ is a lattice, $\mathcal{V}(\mathcal{P}, \|\cdot\|) := \mathcal{V}_{\|\cdot\|,\mathcal{P}}(0)$ denotes the Voronoi cell of the origin.

Maybe the most important definition for this thesis is the notion of Voronoi-relevant vectors since the main task of this work is to analyze the number of these vectors.

Definition 1.6 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. A lattice vector $v \in \Lambda \setminus \{0\}$ is a* Voronoi-relevant vector *if there is some $x \in \operatorname{span}(\Lambda)$ such that $\|x\| = \|x - v\| < \|x - w\|$ holds for all $w \in \Lambda \setminus \{0, v\}$.*

The idea behind this notion is that one does not need to consider all lattice vectors in Definition 1.5 of the Voronoi cell when the Euclidean norm is used. Instead, the Voronoi cell of the origin of a lattice is already specified as the set of points in the linear span of the lattice which are at least as close to 0 as to all Voronoi-relevant vectors. This connection between Voronoi cell and Voronoi-relevant vectors will be formally examined in Section 4.3.

For both concepts it is natural to consider them in terms of bisectors and half-spaces.

Definition 1.7 *Let $V \subseteq \mathbb{R}^n$ be a subspace with norm $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$. For*

$a, b \in V$, the bisector *of a and b with respect to $\|\cdot\|$ is defined as*

$$\mathcal{H}^{=}_{\|\cdot\|}(a,b) := \{x \in V \mid \|x-a\| = \|x-b\|\}.$$

The corresponding strict *and* non-strict halfspaces *are denoted by*

$$\mathcal{H}^{<}_{\|\cdot\|}(a,b) := \{x \in V \mid \|x-a\| < \|x-b\|\} \text{ and}$$
$$\mathcal{H}^{\leq}_{\|\cdot\|}(a,b) := \mathcal{H}^{<}_{\|\cdot\|}(a,b) \cup \mathcal{H}^{=}_{\|\cdot\|}(a,b).$$

With this, the Voronoi cell of the origin of a lattice Λ can be written as

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0,v) \right),$$

and a lattice vector $v \in \Lambda \setminus \{0\}$ is Voronoi-relevant if and only if

$$\operatorname{span}(\Lambda) \cap \mathcal{H}^{=}_{\|\cdot\|}(0,v) \cap \left(\bigcap_{w \in \Lambda \setminus \{0,v\}} \mathcal{H}^{<}_{\|\cdot\|}(0,w) \right) \neq \emptyset.$$

During the investigations of all these geometrical objects, it will be differentiated if the underlying norm is strictly convex or not. As seen in the following chapters, strictly convex norms – e.g., the Euclidean norm – have a lot of nice properties.

Definition 1.8 *Let $V \subseteq \mathbb{R}^n$ be a subspace. A norm $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ is called* strictly convex *if for all $x, y \in V$ with $x \neq y$ and $\|x\| = \|y\|$ and all $\tau \in (0,1)$ it holds that $\|\tau x + (1-\tau)y\| < \|x\|$.*

Note that for every norm it holds for all $x, y \in V$ with $x \neq y$ and $\|x\| = \|y\|$ and all $\tau \in [0,1]$ that $\|\tau x + (1-\tau)y\| \leq \|x\|$. For strictly convex norms, this inequality is an equality if and only if $\tau \in \{0,1\}$.

2 Two-dimensional lattices

Already in two dimensions, some different properties of strictly convex and non-strictly convex norms will become clear. Whereas, every two-dimensional lattice has at most six Voronoi-relevant vectors with respect to every strictly convex norm, the Voronoi-relevant vectors are in general not sufficient in the case of a non-strictly convex norm to determine the Voronoi cell completely, such that a little broader notion needs to be introduced: Generalized Voronoi-relevant vectors. Moreover, it will be shown that every lattice of rank two has at most eight generalized Voronoi-relevant vectors with respect to every strictly convex norm, but the number of generalized Voronoi-relevant vectors is generally not upper bounded by a constant in lattices of rank two when a non-strictly convex norm is used.

2.1 Strictly convex norms

The ideas for this section were developed in collaboration with Prof. Dr. Johannes Blömer and David Teusner. It will be proven that every two-dimensional lattice has at most six Voronoi-relevant vectors with respect to arbitrary strictly convex norms. This is a direct consequence of Theorem 2.4 below and the following Proposition.

Proposition 2.1 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank one with basis (b_1), and let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be an arbitrary norm. Then $\pm b_1$ are Voronoi-relevant vectors. All other lattice vectors are not Voronoi-relevant.*

The proof of this proposition uses a lemma which holds for lattices of every rank.

Lemma 2.2 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm an let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. For every $v \in \Lambda$ and every $k \in \mathbb{N}, k \geq 2$ it holds that kv is not Voronoi-relevant.*

Proof. Assume for contradiction that kv is Voronoi-relevant for some $k \geq 2$. Then there exists some $x \in \operatorname{span}(\Lambda)$ such that $\|x - kv\| = \|x\| < \|x - w\|$ holds for all $w \in \Lambda \setminus \{0, kv\}$. This yields the contradiction

$$\begin{aligned}\|x\| < \|x - v\| &= \frac{1}{k}\|kx - kv\| = \frac{1}{k}\|x - kv + (k-1)x\| \\ &\leq \frac{1}{k}\left(\|x - kv\| + (k-1)\|x\|\right) = \frac{1}{k}\left(\|x\| + (k-1)\|x\|\right) = \|x\|.\end{aligned}$$

□

Proof of Proposition 2.1. For every $z_1 \in \mathbb{Z} \setminus \{0, 1\}$ it holds that

$$\left\| \frac{b_1}{2} - z_1 b_1 \right\| = \left| \frac{1}{2} - z_1 \right| \|b_1\| \geq \frac{3}{2}\|b_1\| > \frac{1}{2}\|b_1\|.$$

Thus, b_1 is Voronoi-relevant, which directly implies that $-b_1$ is Voronoi-relevant. By Lemma 2.2, kb_1 and $-kb_1$ are not Voronoi-relevant for every $k \in \mathbb{N}, k \geq 2$. □

For Theorem 2.4, one needs the notion of a Gauss-reduced basis.

Definition 2.3 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two. A basis (b_1, b_2) of Λ is called* Gauss-reduced *with respect to $\|\cdot\|$ if it holds that*

$$\|b_1\| \leq \|b_2\| \leq \|b_1 - b_2\| \leq \|b_1 + b_2\|.$$

In [7], Kaib and Schnorr show for an arbitrary norm that every lattice of rank two has a Gauss-reduced basis. In fact, they give and analyze an algorithm which computes a Gauss-reduced basis out of a given lattice basis. Hence, it can be assumed that a lattice of rank two is already given by a Gauss-reduced basis.

Theorem 2.4 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two with Gauss-reduced basis (b_1, b_2), and let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Then $\pm b_1$ and $\pm b_2$ are Voronoi-relevant vectors. In addition, $\pm(b_1 - b_2)$ are Voronoi-relevant vectors if and only if $\|b_1 - b_2\| < \|b_1 + b_2\|$. All other lattice vectors are not Voronoi-relevant.*

The proof of this theorem is based on multiple lemmata, which will be discussed below. Lemma 2.9 gives a superset of all Voronoi-relevant vectors under the same assumptions as in the above theorem. Furthermore, Lemmata 2.13, 2.14 and 2.15 consider all elements in this superset and determine if they are Voronoi-relevant or not.

To prove these four lemmata, some further helpful statements will be shown. The first two of these statements are basic properties of Gauss-reduced bases and strictly convex norms.

Remark 2.5 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two with Gauss-reduced basis (b_1, b_2), and let $r \in \mathbb{R}$ with $r \neq 0$. Then (rb_1, rb_2) is a Gauss-reduced basis for $|r|\Lambda$.*

Lemma 2.6 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Moreover, let $x, y \in \mathbb{R}^n$ with $x \neq y$ and $\|x\| \leq \|y\|$, and let $\tau \in \mathbb{R}$ with $0 < \tau < 1$. Then it holds that $\|\tau x + (1 - \tau)y\| < \|y\|$.*

Proof. For $\|x\| = \|y\|$, the desired inequality is directly given by the definition of strict convexity. If $\|x\| < \|y\|$, then it holds that

$$\|\tau x + (1 - \tau)y\| \leq \tau\|x\| + (1 - \tau)\|y\| < \|y\|.$$

□

The next lemma shows that a vector that lies "above-right", "above-left", "below-right" or "below-left" of the parallelogram

$$\mathcal{P}(b_1, b_2) := \{r_1 b_1 + r_2 b_2 \mid r_1, r_2 \in [-1, 1]\}$$

is longer than the corresponding corner vector of this parallelogram if a strictly convex norm is used and (b_1, b_2) is a Gauss-reduced basis.

Lemma 2.7 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two with Gauss-reduced basis (b_1, b_2), and let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Moreover, let $r_1, r_2 \in \mathbb{R}$. If $|r_1|, |r_2| \geq 1$ and $\max\{|r_1|, |r_2|\} > 1$, then $\|b_1 + \operatorname{sgn}(r_1 r_2) b_2\| < \|r_1 b_1 + r_2 b_2\|$.*

Proof. Let $r_1, r_2 \in \mathbb{R}$ with $|r_1|, |r_2| \geq 1$, and distinguish the following two cases.

1. $|r_1| \geq |r_2|$ and $|r_1| > 1$:

   Using $b_1 + \operatorname{sgn}(r_1 r_2) b_2 = \frac{1}{r_1}(r_1 b_1 + r_2 b_2) + \operatorname{sgn}(r_1 r_2)\left(1 - \frac{|r_2|}{|r_1|}\right) b_2$, $|r_2| \geq 1$ and $\|b_2\| \leq \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|$ leads to

   $$\begin{aligned}\|b_1 + \operatorname{sgn}(r_1 r_2) b_2\| &\leq \frac{1}{|r_1|}\|r_1 b_1 + r_2 b_2\| + \left(1 - \frac{|r_2|}{|r_1|}\right)\|b_2\| \\ &\leq \frac{1}{|r_1|}\|r_1 b_1 + r_2 b_2\| + \left(1 - \frac{1}{|r_1|}\right)\|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|.\end{aligned}$$

   This shows $\|b_1 + \operatorname{sgn}(r_1 r_2) b_2\| \leq \|r_1 b_1 + r_2 b_2\|$. If $\|b_2\| < \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|$ or $|r_2| > 1$, then this inequality is even strict, i.e., $\|b_1 + \operatorname{sgn}(r_1 r_2) b_2\| < \|r_1 b_1 + r_2 b_2\|$.

   For $|r_2| = 1$ and $\|b_2\| = \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|$, Lemma 2.6 yields

   $$\begin{aligned}\|b_1 + \operatorname{sgn}(r_1 r_2) b_2\| &= \left\|\operatorname{sgn}(r_1)\frac{1}{|r_1|}(r_1 b_1 + r_2 b_2) + \operatorname{sgn}(r_1 r_2)\left(1 - \frac{1}{|r_1|}\right) b_2\right\| \\ &< \|r_1 b_1 + r_2 b_2\|.\end{aligned}$$

2. $|r_2| \geq |r_1|$ and $|r_2| > 1$:

   Using $b_1 + \operatorname{sgn}(r_1 r_2) b_2 = \operatorname{sgn}(r_1 r_2)\frac{1}{r_2}(r_1 b_1 + r_2 b_2) + \left(1 - \frac{|r_1|}{|r_2|}\right) b_1$, $|r_1| \geq 1$ and $\|b_1\| \leq \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|$, analog arguments lead to the same conclusion.

□

Using the above property for vectors outside of the parallelogram $\mathcal{P}(b_1, b_2)$, it can be easily deduced in the next lemma that every vector having 0 as one of its closest lattice vectors must lie inside of $\mathcal{P}(b_1, b_2)$. From this it follows that for every Voronoi-relevant vector v the parallelograms $\mathcal{P}(b_1, b_2)$ and $v + \mathcal{P}(b_1, b_2)$ intersect in their interior, which gives the superset of all Voronoi-relevant vectors as specified and formally proven in Lemma 2.9.

Lemma 2.8 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two with Gauss-reduced basis (b_1, b_2), and let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Moreover, let $r_1, r_2 \in \mathbb{R}$. If $\|r_1 b_1 + r_2 b_2\| \leq \|r_1 b_1 + r_2 b_2 - v\|$ holds for all $v \in \Lambda$, then $r_1, r_2 \in (-1, 1)$.*

Proof. Let $r_1, r_2 \in \mathbb{R}$ with $r_1 \notin (-1, 1)$ or $r_2 \notin (-1, 1)$. The rest of this proof shows that there is some $v \in \Lambda$ with $\|r_1 b_1 + r_2 b_2\| > \|r_1 b_1 + r_2 b_2 - v\|$.

If $r_2 = 0$, then $\|r_1 b_1 - \operatorname{sgn}(r_1) b_1\| = |r_1 - \operatorname{sgn}(r_1)| \|b_1\| < |r_1| \|b_1\| = \|r_1 b_1\|$ follows due to $r_1 \notin (-1, 1)$. If $r_1 = 0$, then it holds analogously that $r_2 \notin (-1, 1)$ and $\|r_2 b_2 - \operatorname{sgn}(r_2) b_2\| < \|r_2 b_2\|$. If $|r_1| = |r_2| \geq 1$, then

$$\begin{aligned}\|r_1 b_1 + r_2 b_2 - \operatorname{sgn}(r_1) b_1 - \operatorname{sgn}(r_2) b_2\| &= |r_1 - \operatorname{sgn}(r_1)| \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\| \\ &< |r_1| \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\| = \|r_1 b_1 + r_2 b_2\|\end{aligned}$$

holds. Hence, it can be assumed that $r_1 \neq 0 \neq r_2$ and that $|r_1| \neq |r_2|$, and only two remaining cases need to be considered.

1. $|r_1| > |r_2|$ and $|r_1| \geq 1$:

   By Remark 2.5, $(r_2 b_1, r_2 b_2)$ is a Gauss-reduced basis for $|r_2|\Lambda$. Together with Lemma 2.7 applied to this basis, it follows that

   $$\|r_2 b_2\| \leq \left\| r_2 b_1 + \operatorname{sgn}\left(\frac{r_1}{r_2} \cdot 1\right) r_2 b_2 \right\| < \|r_1 b_1 + r_2 b_2\|.$$

   If $|r_1| = 1$, then $\|r_1 b_1 + r_2 b_2 - \operatorname{sgn}(r_1) b_1\| = \|r_2 b_2\| < \|r_1 b_1 + r_2 b_2\|$ holds. For $|r_1| > 1$, Lemma 2.6 yields

   $$\begin{aligned}&\|r_1 b_1 + r_2 b_2 - \operatorname{sgn}(r_1) b_1\| \\ &= \left\| \frac{r_1 - \operatorname{sgn}(r_1)}{r_1} (r_1 b_1 + r_2 b_2) + \left(1 - \frac{r_1 - \operatorname{sgn}(r_1)}{r_1}\right) r_2 b_2 \right\| < \|r_1 b_1 + r_2 b_2\|.\end{aligned}$$

2. $|r_2| > |r_1|$ and $|r_2| \geq 1$:

   Analog arguments lead to $\|r_1 b_1\| < \|r_1 b_1 + r_2 b_2\|$ as well as $\|r_1 b_1 + r_2 b_2 - \operatorname{sgn}(r_2) b_2\| < \|r_1 b_1 + r_2 b_2\|$.

□

Lemma 2.9 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two with Gauss-reduced basis (b_1, b_2), and let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Then all Voronoi-relevant vectors are contained in $\{\pm b_1, \pm b_2, \pm(b_1 - b_2), \pm(b_1 + b_2)\}$.*

Proof. Let $z_1, z_2 \in \mathbb{Z}$ and let $z_1 b_1 + z_2 b_2$ be a Voronoi-relevant vector. Then there are $r_1, r_2 \in \mathbb{R}$ with $\|r_1 b_1 + r_2 b_2\| = \|r_1 b_1 + r_2 b_2 - z_1 b_1 - z_2 b_2\| \leq \|r_1 b_1 + r_2 b_2 - v\|$ for all $v \in \Lambda$. In particular, Lemma 2.8 implies $r_1, r_2 \in (-1, 1)$ as well as $r_1 - z_1, r_2 - z_2 \in (-1, 1)$. This leads to $z_1, z_2 \in (-2, 2)$ and thus to $z_1, z_2 \in \{-1, 0, 1\}$. Hence, $z_1 b_2 + z_2 b_2 \in \{\pm b_1, \pm b_2, \pm(b_1 - b_2), \pm(b_1 + b_2)\}$ follows. □

Now it is already shown that every lattice of rank two has at most eight Voronoi-relevant vectors with respect to a strictly convex norm. Some of these eight candidates can be excluded, such that only four or six Voronoi-relevant vectors remain. For this, some further statements are needed, e.g., the next lemma shows that in every bisector between 0 and some $x \neq 0$ the vector $\frac{x}{2}$ is the unique shortest vector.

Lemma 2.10 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Moreover, let $x \in \mathbb{R}^n$ with $x \neq 0$, and let $y \in \mathbb{R}^n$ with $y \neq \frac{x}{2}$ and $\|y\| = \|y - x\|$. Then $\left\|\frac{x}{2}\right\| < \|y\|$ holds.*

Proof. Let $x, y \in \mathbb{R}^n$ with $2y \neq x \neq 0$ and $\|y\| = \|y - x\|$, and assume for contradiction that $\left\|\frac{x}{2}\right\| \geq \|y\|$. Consider $w := \frac{1}{2}y + \frac{1}{2}\frac{x}{2}$. Then it follows from Lemma 2.6 that $\|w\| < \left\|\frac{x}{2}\right\|$. With this, distinguish the following two cases.

1. $\|w - x\| \leq \|w\|$:
   The estimate
   $$\begin{aligned}\|x\| &= \|x - w + w\| \\ &\leq \|w - x\| + \|w\| \leq 2\|w\| = \left\|y + \frac{x}{2}\right\| \leq \|y\| + \left\|\frac{x}{2}\right\| \leq \|x\|\end{aligned}$$
   shows that $2\|w\| = \|x\|$, which contradicts $\|w\| < \left\|\frac{x}{2}\right\|$.
2. $\|w - x\| > \|w\|$:
   Now it follows that
   $$\begin{aligned}\|x\| &\leq \|w - x\| + \|w\| \\ &< 2\|w - x\| = \left\|(y - x) - \frac{x}{2}\right\| \leq \|y - x\| + \left\|\frac{x}{2}\right\| \leq \|x\|,\end{aligned}$$
   which is a contradiction.

□

Analogously to Lemma 2.7, it will be shown in the next lemma that a vector lying inside of the "upper-right", "upper-left", "lower-right" or "lower-left" quarter of the parallelogram $\mathcal{P}(b_1, b_2)$ is shorter than the corresponding corner vector of $\mathcal{P}(b_1, b_2)$.

Lemma 2.11 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two with Gauss-reduced basis (b_1, b_2), and let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Moreover, let $r_1, r_2 \in \mathbb{R}$. If $0 < |r_1|, |r_2| \leq 1$ and $\min\{|r_1|, |r_2|\} < 1$, then $\|r_1 b_1 + r_2 b_2\| < \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|$.*

Proof. Let $r_1, r_2 \in \mathbb{R}$ with $0 < |r_1|, |r_2| \leq 1$.
If $|r_1| < 1 = |r_2|$, it holds by Lemma 2.6 that
$$\begin{aligned}\|r_1 b_1 + r_2 b_2\| &= \||r_1|(\operatorname{sgn}(r_1) b_1 + r_2 b_2) + (1 - |r_1|) r_2 b_2\| \\ &< \|\operatorname{sgn}(r_1) b_1 + r_2 b_2\| = \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|.\end{aligned} \tag{2.1}$$

For $|r_2| < 1 = |r_1|$, the roles of r_1 and r_2 can be exchanged in (2.1) to get $\|r_1 b_1 + r_2 b_2\| < \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|$.

If $|r_1|, |r_2| < 1$, Lemma 2.6 implies

$$\begin{aligned}\|r_1 b_1 + r_2 b_2\| &= \||r_2|(r_1 b_1 + \operatorname{sgn}(r_2) b_2) + (1 - |r_2|) r_1 b_1\| \\ &< \max\{\|r_1 b_1 + \operatorname{sgn}(r_2) b_2\|, \|r_1 b_1\|\}.\end{aligned}$$

By (2.1), $\|r_1 b_1 + \operatorname{sgn}(r_2) b_2\| < \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|$. Since moreover it holds that $\|r_1 b_1\| < \|b_1\| \leq \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|$, it follows that $\|r_1 b_1 + r_2 b_2\| < \|b_1 + \operatorname{sgn}(r_1 r_2) b_2\|$. □

The next lemma gives an easy upper bound for the covering radius. With this bound at hand, the remaining three lemmata of this section will investigate the conditions under which the eight candidates for Voronoi-relevant vectors stated in Lemma 2.9 are indeed Voronoi-relevant.

Lemma 2.12 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two with Gauss-reduced basis (b_1, b_2), and let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Then for every $x \in \operatorname{span}(\Lambda)$ there exists $v \in \Lambda$ such that $\|x - v\| \leq \left\|\frac{b_1 + b_2}{2}\right\|$.*

Proof. Let $r_1, r_2 \in \mathbb{R}$ and $x := r_1 b_1 + r_2 b_2$. Rounding the coefficients to the nearest integer yields $z_1, z_2 \in \mathbb{Z}$ and $s_1, s_2 \in \mathbb{R}$ with $|s_1|, |s_2| \leq \frac{1}{2}$ and $x = (z_1 + s_1) b_1 + (z_2 + s_2) b_2$. Defining $v := z_1 b_1 + z_2 b_2$ leads to $x - v = s_1 b_1 + s_2 b_2$.

If $s_1 = 0$, then $\|x - v\| = |s_2| \|b_2\| \leq \frac{1}{2} \|b_1 + b_2\|$. If $s_2 = 0$, $\|x - v\| \leq \frac{1}{2} \|b_1 + b_2\|$ follows analogously. Hence, it can be assumed that $s_1 \neq 0 \neq s_2$.

If $|s_1| = |s_2| = \frac{1}{2}$, then $\|x - v\| = \frac{1}{2} \|\operatorname{sgn}(s_1) b_1 + \operatorname{sgn}(s_2) b_2\| \leq \frac{1}{2} \|b_1 + b_2\|$. If $\min\{|s_1|, |s_2|\} < \frac{1}{2}$, Lemma 2.11 yields

$$2\|x - v\| = \|2 s_1 b_1 + 2 s_2 b_2\| < \|b_1 + \operatorname{sgn}(s_1 s_2) b_2\| \leq \|b_1 + b_2\|.$$

□

Lemma 2.13 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two with Gauss-reduced basis (b_1, b_2), and let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Then the vectors $\pm(b_1 + b_2)$ are not Voronoi-relevant.*

Proof. Assume for contradiction that $b_1 + b_2$ is Voronoi-relevant. Then there is some $x \in \operatorname{span}(\Lambda)$ with $\|x\| = \|x - b_1 - b_2\| < \|x - v\|$ for all $v \in \Lambda \setminus \{0, b_1 + b_2\}$.

If $x = \frac{b_1 + b_2}{2}$, then

$$\|x - b_1\| = \left\|\frac{-b_1 + b_2}{2}\right\| = \frac{1}{2}\|b_1 - b_2\| \leq \frac{1}{2}\|b_1 + b_2\| = \|x\| < \|x - b_1\|,$$

which is a contradiction.

If $x \neq \frac{b_1 + b_2}{2}$, Lemma 2.10 implies $\left\|\frac{b_1 + b_2}{2}\right\| < \|x\|$. On the other hand, Lemma 2.12 shows that there is some $v \in \Lambda$ with $\|x - v\| \leq \left\|\frac{b_1 + b_2}{2}\right\| < \|x\|$, which is a contradiction.

Hence, $b_1 + b_2$ cannot be Voronoi-relevant, which furthermore implies that $-b_1 - b_2$ is not Voronoi-relevant. □

Lemma 2.14 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two with Gauss-reduced basis (b_1, b_2), and let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Then the vectors $\pm b_1$ and $\pm b_2$ are Voronoi-relevant.*

Proof. To show that b_1 is Voronoi-relevant, it is sufficient to prove that $\left\|\frac{b_1}{2}\right\| < \left\|v - \frac{b_1}{2}\right\|$ holds for all $v \in \Lambda \setminus \{0, b_1\}$. Hence, consider $(z_1, z_2) \in \mathbb{Z}^2 \setminus \{(0,0), (1,0)\}$ and $v := z_1 b_1 + z_2 b_2$.

If $z_2 \neq 0$, then it follows from Lemma 2.7 that

$$\left\|v - \frac{b_1}{2}\right\| = \frac{1}{2}\|(2z_1 - 1)b_1 + 2z_2 b_2\| > \frac{1}{2}\|b_1 + \operatorname{sgn}((2z_1 - 1)z_2)b_2\| \geq \left\|\frac{b_1}{2}\right\|.$$

If $z_2 = 0$, then it is $z_1 \notin \{0, 1\}$, which implies that

$$\left\|v - \frac{b_1}{2}\right\| = \frac{1}{2}|2z_1 - 1|\|b_1\| \geq \frac{3}{2}\|b_1\| > \left\|\frac{b_1}{2}\right\|.$$

Therefore, b_1 and $-b_1$ are Voronoi-relevant. By exchanging the roles of z_1 and z_2 in the above inequalities, it follows analogously that $\left\|\frac{b_2}{2}\right\| < \left\|v - \frac{b_2}{2}\right\|$ holds for all $v \in \Lambda \setminus \{0, b_2\}$, yielding that b_2 and $-b_2$ are Voronoi-relevant. □

Lemma 2.15 *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank two with Gauss-reduced basis (b_1, b_2), and let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm. Then the vectors $\pm(b_1 - b_2)$ are Voronoi-relevant if and only if $\|b_1 - b_2\| < \|b_1 + b_2\|$.*

Proof. First assume that $b_1 - b_2$ is Voronoi-relevant. Then there is some $x \in \operatorname{span}(\Lambda)$ with $\|x\| = \|x - b_1 + b_2\| < \|x - v\|$ for all $v \in \Lambda \setminus \{0, b_1 - b_2\}$. If $x \neq \frac{b_1 - b_2}{2}$, then it holds by Lemmata 2.10 and 2.12 that $\left\|\frac{b_1 - b_2}{2}\right\| < \|x\| \leq \left\|\frac{b_1 + b_2}{2}\right\|$, which implies $\|b_1 - b_2\| < \|b_1 + b_2\|$. If $x = \frac{b_1 - b_2}{2}$, then it follows that $\|b_1 - b_2\| = 2\|x\| < 2\|x - b_1\| = \|b_1 + b_2\|$.

Now assume $\|b_1 - b_2\| < \|b_1 + b_2\|$ and show that $b_1 - b_2$ as well as $-b_1 + b_2$ are Voronoi-relevant. For this it is enough to prove that $\left\|\frac{b_1 - b_2}{2}\right\| < \left\|v - \frac{b_1}{2} + \frac{b_2}{2}\right\|$ holds for all $v \in \Lambda \setminus \{0, b_1 - b_2\}$. For $v \in \{b_1, -b_2\}$ it holds that $\left\|v - \frac{b_1}{2} + \frac{b_2}{2}\right\| = \left\|\frac{b_1 + b_2}{2}\right\| > \left\|\frac{b_1 - b_2}{2}\right\|$. Hence, consider $(z_1, z_2) \in \mathbb{Z}^2 \setminus \{(0,0), (1,-1), (1,0), (0,-1)\}$ and $v := z_1 b_1 + z_2 b_2$. Then it follows that $z_1 \notin \{0, 1\}$ or $z_2 \notin \{-1, 0\}$, leading to $|2z_1 - 1| \geq 3$ or $|2z_2 + 1| \geq 3$. Thus, Lemma 2.7 implies

$$\begin{aligned}\left\|v - \frac{b_1}{2} + \frac{b_2}{2}\right\| &= \frac{1}{2}\|(2z_1 - 1)b_1 + (2z_2 + 1)b_2\| \\ &> \frac{1}{2}\|b_1 + \operatorname{sgn}((2z_1 - 1)(2z_2 + 1))b_2\| \geq \left\|\frac{b_1 - b_2}{2}\right\|.\end{aligned}$$

□

Proof of Theorem 2.4. This proof follows directly from Lemmata 2.9, 2.13, 2.14 and 2.15. □

2.2 Non-strictly convex norms

Consider the lattice $\mathcal{L}(b_1, b_2)$ spanned by $b_1 := (1,1)^T$ and $b_2 := (0,3)^T$ together with the 1-norm $\|\cdot\|_1$. In the following, the Voronoi cell $\mathcal{V}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$ of the origin will be constructed illustratively and afterwards a formal proof will be given. For the illustrative construction one can investigate the bisectors between 0 and all *generalized Voronoi-relevant vectors* $v \in \mathcal{L}(b_1, b_2)$.

Definition 2.16 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. A lattice vector $v \in \Lambda \setminus \{0\}$ is a* generalized Voronoi-relevant vector *if there is some $x \in \operatorname{span}(\Lambda)$ such that $\|x\| = \|x - v\| \leq \|x - w\|$ holds for all $w \in \Lambda$.*

The next lemma is helpful to determine which lattice vectors are generalized Voronoi-relevant vectors since it shows that these vectors cannot be too far away from the origin.

Lemma 2.17 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. For every generalized Voronoi-relevant vector $v \in \Lambda$ it holds that $\|v\| \leq 2\mu(\Lambda, \|\cdot\|)$.*

Proof. Let $v \in \Lambda \setminus \{0\}$ and $x \in \operatorname{span}(\Lambda)$ with $\|x\| = \|x - v\| \leq \|x - w\|$ for all $w \in \Lambda$. Then it holds that $\|x\| = \|x - v\| \leq \mu(\Lambda, \|\cdot\|)$ and thus

$$\|v\| = \|v - x + x\| \leq \|x - v\| + \|x\| \leq 2\mu(\Lambda, \|\cdot\|).$$

□

Next, a calculation of the covering radius of $\mathcal{L}(b_1, b_2)$ with respect to $\|\cdot\|_1$ is needed in order to use the above lemma.

Lemma 2.18 $\mu(\mathcal{L}(b_1, b_2), \|\cdot\|_1) = \frac{3}{2}$.

Proof. First prove $\mu(\mathcal{L}(b_1, b_2), \|\cdot\|_1) \leq \frac{3}{2}$. For this, let $x = (x_1, x_2)^T \in \mathbb{R}^2$, and show that $\|x - v\|_1 \leq \frac{3}{2}$ holds for some $v \in \mathcal{L}(b_1, b_2)$. There are $m \in \mathbb{Z}$ and $r \in [0, 1)$ with $x_1 = m + r$. Moreover, there is $k \in \mathbb{Z}$ such that $m + 3k \leq x_2 < m + 3(k+1)$ holds. Now, show in each of the following four cases that x has distance at most $\frac{3}{2}$ to some lattice vector.

1. $x_2 \leq m + 3k + 1$ and $r \leq \frac{1}{2}$:

$$\begin{aligned} \|x - mb_1 - kb_2\| &= |x_1 - m| + |x_2 - m - 3k| = r + (x_2 - m - 3k) \\ &\leq \frac{1}{2} + 1 = \frac{3}{2} \end{aligned}$$

2. $x_2 \leq m + 3k + 1$ and $r > \frac{1}{2}$:

$$\|x - (m+1)b_1 - kb_2\| = |x_1 - m - 1| + |x_2 - m - 1 - 3k|$$

$$= (1 - r) + (m + 1 + 3k - x_2) < \frac{1}{2} + 1 = \frac{3}{2}$$

3. $x_2 > m + 3k + 1$ and $x_2 \leq x_1 + 3k + \frac{3}{2}$:

$$\begin{aligned} \|x - (m+1)b_1 - kb_2\| &= |x_1 - m - 1| + |x_2 - m - 1 - 3k| \\ &= (1 + m - x_1) + (x_2 - m - 1 - 3k) \\ &= x_2 - x_1 - 3k \leq \frac{3}{2} \end{aligned}$$

4. $x_2 > m + 3k + 1$ and $x_2 > x_1 + 3k + \frac{3}{2}$:

$$\begin{aligned} \|x - mb_1 - (k+1)b_2\| &= |x_1 - m| + |x_2 - m - 3(k+1)| \\ &= (x_1 - m) + (m + 3k + 3 - x_2) \\ &= x_1 - x_2 + 3k + 3 < \frac{3}{2} \end{aligned}$$

To prove $\mu(\mathcal{L}(b_1, b_2), \|\cdot\|_1) \geq \frac{3}{2}$, consider $x := \frac{3}{4}(1, -1)^T$ and compute all $v \in \mathcal{L}(b_1, b_2)$ with $\|x - v\|_1 \leq \frac{3}{2}$. For this, let $z_1, z_2 \in \mathbb{Z}$ and $v := z_1 b_1 + z_2 b_2$. Then it holds that $\|x - v\|_1 = \left|\frac{3}{4} - z_1\right| + \left|-\frac{3}{4} - z_1 - 3z_2\right|$. Assuming $\|x - v\|_1 \leq \frac{3}{2}$ implies $\left|\frac{3}{4} - z_1\right| \leq \frac{3}{2}$, leading to $z_1 \in \{0, 1, 2\}$. According to this, distinguish the following three cases.

1. $z_1 = 0$:

   From $\frac{3}{2} \geq \|x - v\|_1 = \frac{3}{4} + \left|\frac{3}{4} + 3z_2\right|$ it follows that $|1 + 4z_2| \leq 1$, which implies $z_2 = 0$.

2. $z_1 = 1$:

   Here, $\frac{3}{2} \geq \|x - v\|_1 = \frac{1}{4} + \left|\frac{7}{4} + 3z_2\right|$ yields $|7 + 12z_2| \leq 5$ and thus $z_2 = -1$.

3. $z_2 = 2$:

   In this case, $\frac{3}{2} \geq \|x - v\|_1 = \frac{5}{4} + \left|\frac{11}{4} + 3z_2\right|$ must hold. This shows $|11 + 12z_2| \leq 1$ and $z_2 = -1$.

In all three cases it holds that $\|x - v\| = \frac{3}{2}$, which shows that every lattice vector has distance at least $\frac{3}{2}$ to x. □

By combining both lemmata, it is enough to consider the bisectors between 0 and all $v \in \mathcal{L}(b_1, b_2) \setminus \{0\}$ with $\|v\|_1 \leq 3$ in order to compute the desired Voronoi cell. An excerpt of the lattice $\mathcal{L}(b_1, b_2)$ together with the boundary of $\mathcal{B}_{\|\cdot\|_1, 3}(0)$ is depicted in Figure 2.1, and the next lemma determines formally which lattice vectors have norm at most three.

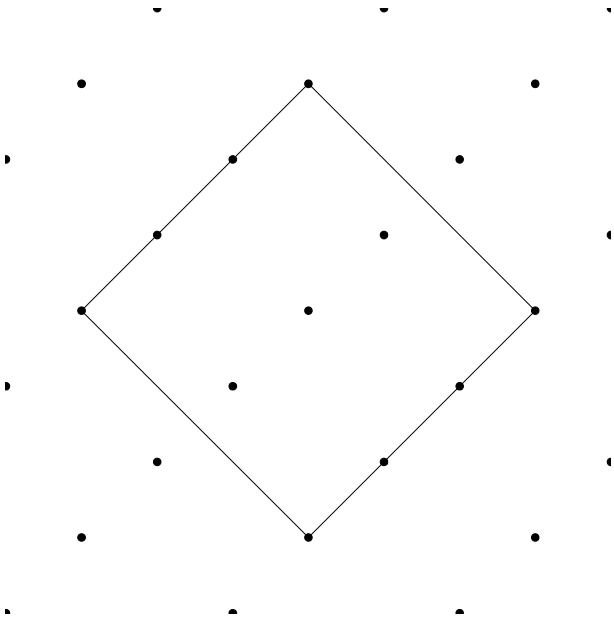


Figure 2.1: $\mathcal{L}(b_1, b_2)$ with boundary of $\mathcal{B}_{\|\cdot\|_1,3}(0)$.

Lemma 2.19 *Let $z_1, z_2 \in \mathbb{Z}$. Then it holds that $\|z_1 b_1 + z_2 b_2\|_1 \leq 3$ if and only if*

$$(z_1, z_2) \in \{(-3,1), (-2,1), (-1,0), (-1,1), (0,-1), (0,0), \\ (0,1), (1,-1), (1,0), (2,-1), (3,-1)\} =: \mathcal{I}.$$

Proof. If $(z_1, z_2) \in \mathcal{I}$, easy calculation shows $\|z_1 b_1 + z_2 b_2\|_1 = |z_1| + |z_1 + 3z_2| \leq 3$.

Hence, it is left to consider $z_1, z_2 \in \mathbb{Z}$ with $\|z_1 b_1 + z_2 b_2\|_1 \leq 3$. From this it directly follows that $|z_1| \leq 3$ holds. Due to symmetry, one can further assume that $z_1 \geq 0$. Now distinguish the remaining cases.

1. $z_1 = 3$:

   In this case, $z_1 + 3z_2 = 0$ follows, which implies $z_2 = -1$.

2. $z_1 = 2$:

   From $|z_1 + 3z_2| \leq 1$ one deduces $3z_2 \in \{-3, -2, -1\}$, leading to $z_2 = -1$.

3. $z_1 = 1$:

   Since $|z_1 + 3z_2| \leq 2$ must hold, $3z_2 \in \{-3, -2, -1, 0, 1\}$ follows, yielding $z_2 \in \{-1, 0\}$.

4. $z_1 = 0$:

   Now $3|z_2| \leq 3$ needs to holds, which implies $z_2 \in \{-1, 0, 1\}$.

□

When computing the bisectors between 0 and the lattice vectors specified in the above lemma, it follows from the symmetry that only three different kinds of bisectors need to be examined. These are shown in Figure 2.2. Since these bisectors are at the moment only used for illustration, a formal proof stating that the bisectors look exactly as depicted in the figure is omitted.

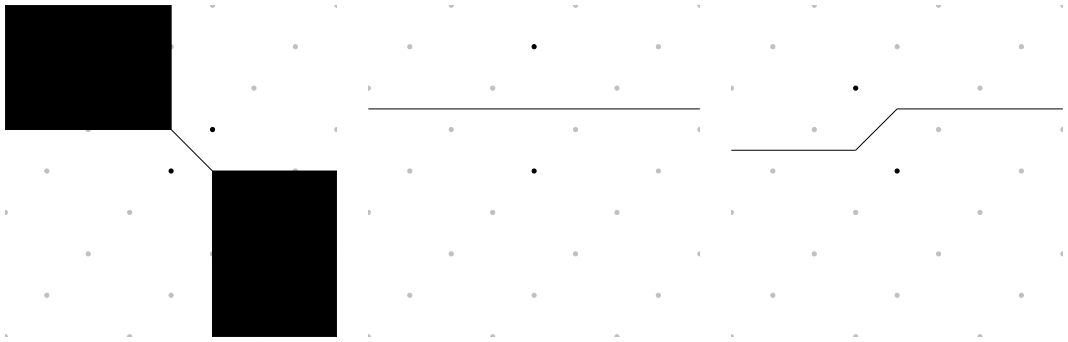


Figure 2.2: $\mathcal{H}^{=}_{\|\cdot\|_1}(0, b_1)$, $\mathcal{H}^{=}_{\|\cdot\|_1}(0, b_2)$ and $\mathcal{H}^{=}_{\|\cdot\|_1}(0, b_2 - b_1)$.

Intersecting these bisectors suggests that $\mathcal{V}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$ looks as given in Figure 2.3, where the Voronoi cell is partitioned into two parts

$$\mathcal{V}(\mathcal{L}(b_1, b_2), \|\cdot\|_1) = \mathcal{V}^{(i)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1) \cup \mathcal{V}^{(o)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1).$$

Definition 2.20 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice.*

$$\mathcal{V}^{(i)}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda \setminus \{0\} : \|x\| < \|x - v\|\}$$

denotes the strict Voronoi cell of the origin *of Λ with respect to $\|\cdot\|$. In addition, define*

$$\mathcal{V}^{(o)}(\Lambda, \|\cdot\|) := \mathcal{V}(\Lambda, \|\cdot\|) \setminus \mathcal{V}^{(i)}(\Lambda, \|\cdot\|).$$

Additionally to these figurative ideas, a formal proof to specify the Voronoi cell and its two parts will be given now.

Proposition 2.21 *It holds that*

$$\begin{aligned}&\mathcal{V}^{(i)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)\\ &= \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; |x_1| < 1, |x_2| < 1, |x_1 + x_2| < 1, |x_1 - x_2| < \frac{3}{2} \right\} =: \mathcal{S}^{(i)}\end{aligned}$$

and $\mathcal{V}^{(o)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1) = \mathcal{S}_1^{(o)} \cup \mathcal{S}_2^{(o)} \cup \mathcal{S}_3^{(o)} \cup \mathcal{S}_4^{(o)}$, where

$$\mathcal{S}_1^{(o)} := \left\{ \pm \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x_1 + x_2 = 1, x_1 \in (0, 1) \right\},$$

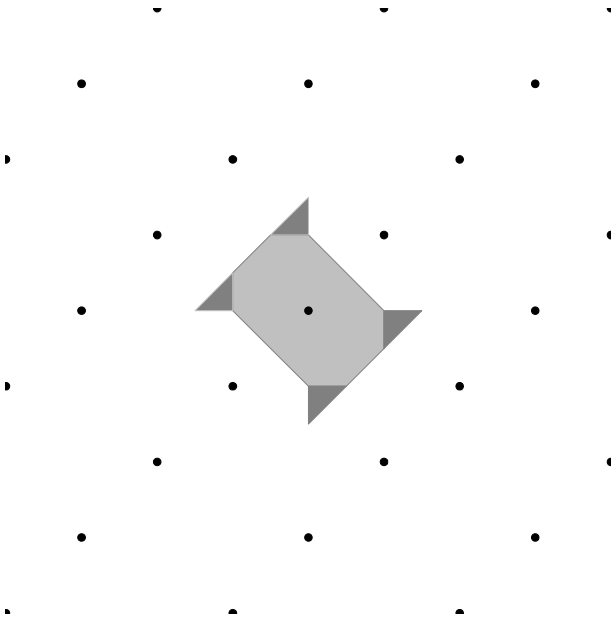


Figure 2.3: $\mathcal{V}^{(i)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$ (light gray) and $\mathcal{V}^{(o)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$ (darker gray).

$$\mathcal{S}_2^{(o)} := \left\{ \pm \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x_1 - x_2 = \frac{3}{2}, x_1 \in \left(\frac{1}{2}, 1\right) \right\},$$
$$\mathcal{S}_3^{(o)} := \left\{ \pm \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x_1 \geq 1, x_2 \leq 0, x_1 - x_2 \leq \frac{3}{2} \right\},$$
$$\mathcal{S}_4^{(o)} := \left\{ \pm \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x_1 \geq 0, x_2 \leq -1, x_1 - x_2 \leq \frac{3}{2} \right\}.$$

The proof of this proposition is split up in the three following lemmata.

Lemma 2.22 $\mathcal{V}(\mathcal{L}(b_1, b_2), \|\cdot\|_1) \subseteq \mathcal{S}^{(i)} \cup \mathcal{S}_1^{(o)} \cup \mathcal{S}_2^{(o)} \cup \mathcal{S}_3^{(o)} \cup \mathcal{S}_4^{(o)}$.

Proof. Let $x = (x_1, x_2)^T \in \mathbb{R}^2$ with $x \notin \mathcal{S}^{(i)} \cup \mathcal{S}_1^{(o)} \cup \mathcal{S}_2^{(o)} \cup \mathcal{S}_3^{(o)} \cup \mathcal{S}_4^{(o)}$. It is left to show that $x \notin \mathcal{V}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$, i.e., that there is some $v \in \mathcal{L}(b_1, b_2)$ such that $\|x - v\|_1 < \|x\|_1$.

Due to symmetry, one can assume that $x_1 \geq 0$. Now distinguish the three following cases.

1. $x_2 \leq 0$:

   Assume for contradiction that $x_1 - x_2 \leq \frac{3}{2}$. Then it follows from $x \notin \mathcal{S}_3^{(o)}$ that $x_1 < 1$. Analogously, $x \notin \mathcal{S}_4^{(o)}$ implies $x_2 > -1$. Hence, it holds that $|x_1| < 1$, $|x_2| < 1$ and $|x_1 + x_2| < 1$. Since $x \notin \mathcal{S}^{(i)}$, $x_1 - x_2 = |x_1 - x_2| \geq \frac{3}{2}$ must hold, which implies $x_1 = \frac{3}{2} + x_2 > \frac{1}{2}$. But now it follows that $x \in \mathcal{S}_2^{(o)}$, which is a contradiction.

   Therefore it holds that $\|x\|_1 = x_1 - x_2 > \frac{3}{2}$, and Lemma 2.18 shows that $\|x - v\|_1 \leq \frac{3}{2} < \|x\|_1$ must hold for some $v \in \mathcal{L}(b_1, b_2)$.

2. $x_2 > 0$ and $x_1 + x_2 > \frac{3}{2}$:

   In this case it directly follows from Lemma 2.18 that for some $v \in \mathcal{L}(b_1, b_2)$ it is $\|x\|_1 = x_1 + x_2 > \frac{3}{2} \geq \|x - v\|_1$.

3. $x_2 > 0$ and $x_1 + x_2 \leq \frac{3}{2}$:

   First, assume for contradiction that $x_1 = 0$. Since $x \notin \mathcal{S}^{(i)}$, it must hold that $x_2 \geq 1$, but then $x \in \mathcal{S}_4^{(o)}$ would follow, which is a contradiction. Thus, $x_1 > 0$ holds.

   Secondly, assume for contradiction that $x_1 + x_2 \leq 1$. From $x_1 > 0$ and $x_2 > 0$ it follows that $x_1 < 1$ and $x_2 < 1$. This further implies $|x_1 - x_2| < 1$. Furthermore, $x \notin \mathcal{S}^{(i)}$ yields $x_1 + x_2 \geq 1$. Hence, $x_1 + x_2 = 1$ and $x \in \mathcal{S}_1^{(o)}$ follow, where the latter is a contradiction.

   Thus, $\|x\|_1 = x_1 + x_2 > 1$ and $x_1 > 0$ hold. The rest of this proof shows that $\|x - b_1\|_1 = |x_1 - 1| + |x_2 - 1| < \|x\|_1$.

   If $x_1 < 1$ and $x_2 < 1$, then $\|x - b_1\|_1 = 2 - x_1 - x_2 < 1 < \|x\|_1$ holds.

   For $x_1 \geq 1$, $x_1 + x_2 \leq \frac{3}{2}$ implies $x_2 \leq \frac{1}{2}$ and thus it follows due to $x_2 > 0$ that $\|x - b_1\|_1 = x_1 - x_2 < x_1 + x_2 = \|x\|_1$.

   For $x_2 \geq 1$, one shows analogously $\|x - b_1\|_1 = -x_1 + x_2 < x_1 + x_2 = \|x\|_1$.

□

Lemma 2.23 $\mathcal{S}^{(i)} \subseteq \mathcal{V}^{(i)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$.

Proof. Let $x = (x_1, x_2)^T \in \mathcal{S}^{(i)}$, and assume for contradiction that $x \notin \mathcal{V}^{(i)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$, i.e., that there is some $v \in \mathcal{L}(b_1, b_2) \setminus \{0\}$ such that $\|x - v\|_1 \leq \|x\|_1$. In addition, let $z_1, z_2 \in \mathbb{Z}$ with $v = z_1 b_1 + z_2 b_2$.

Due to symmetry, one can assume that $x_1 \geq 0$. Depending on x_2, two cases need to be distinguished.

1. $x_2 \geq 0$:

   In this case, it is $|x_1 - z_1| + |x_2 - z_1 - 3z_2| = \|x - v\|_1 \leq \|x\|_1 = x_1 + x_2 < 1$ and thus $|x_1 - z_1| < 1$, which implies $z_1 \in \{0, 1\}$. Examine both of these cases independently as follows.

   a) $z_1 = 0$:

      $|x_2 - 3z_2| < 1$ leads to $z_2 = 0$, which is a contradiction to $v \neq 0$.

   b) $z_1 = 1$:

      Again, it follows from $|x_2 - 1 - 3z_2| < 1$ that $z_2 = 0$, but this further implies that $\|x - v\|_1 = |x_1 - 1| + |x_2 - 1| = 2 - x_1 - x_2 > 1$. This is a contradiction to $\|x - v\|_1 < 1$.

2. $x_2 < 0$:

   It holds that $|x_1 - z_1| + |x_2 - z_1 - 3z_2| = \|x - v\|_1 \leq \|x\|_1 = x_1 - x_2 < \frac{3}{2}$. Hence, it is $|x_1 - z_1| < \frac{3}{2}$ and $|x_2 - z_1 - 3z_2| < \frac{3}{2}$, and these two inequalities yield $z_1, -z_1 - 3z_2 \in \{-1, 0, 1, 2\}$. According to z_1, these four cases will be distinguished.

   a) $z_1 = -1$:

      Then, it is $-3z_2 \in \{-2, -1, 0, 1\}$, which leads to $z_2 = 0$. Therefore, $x_2 > -1$ yields the contradiction $\|x - v\|_1 = |x_1 + 1| + |x_2 + 1| = 2 + x_1 + x_2 > x_1 - x_2 = \|x\|_1$.

   b) $z_1 = 0$:

      In this case, $-3z_2 \in \{-1, 0, 1, 2\}$ holds, which shows that $z_2 = 0$, but this is a contradiction to $v \neq 0$.

   c) $z_1 = 1$:

      Now, $-3z \in \{0, 1, 2, 3\}$ must hold, yielding $z_2 \in \{-1, 0\}$. If $z_2 = -1$, then $x_1 - x_2 < \frac{3}{2}$ leads to $\|x - v\|_1 = |x_1 - 1| + |x_2 + 2| = 3 - x_1 + x_2 > x_1 - x_2 = \|x\|_1$. If $z_2 = 0$, then it follows from $x_1 < 1$ that $\|x - v\|_1 = |x_1 - 1| + |x_2 - 1| = 2 - x_1 - x_2 > x_1 - x_2 = \|x\|_1$. Hence, both cases contradict $\|x - v\|_1 \leq \|x\|_1$.

   d) $z_1 = 2$:

      Here, $-3z_2 \in \{1, 2, 3, 4\}$ holds, which implies $z_2 = -1$, but this gives the contradiction $\|x-v\|_1 = |x_1-2|+|x_2+1| = 3-x_1+x_2 > x_1-x_2 = \|x\|_1$.

□

Lemma 2.24 $\mathcal{S}_1^{(o)} \cup \mathcal{S}_2^{(o)} \cup \mathcal{S}_3^{(o)} \cup \mathcal{S}_4^{(o)} \subseteq \mathcal{V}^{(o)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$. *In addition, for all* $(z_1, z_2) \in \mathcal{I} \setminus \{(0, 0)\}$ *it holds that* $z_1 b_1 + z_2 b_2$ *is a generalized Voronoi-relevant vector with respect to* $\|\cdot\|_1$.

Proof. Let $x = (x_1, x_2)^T \in \mathcal{S}_1^{(o)} \cup \mathcal{S}_2^{(o)} \cup \mathcal{S}_3^{(o)} \cup \mathcal{S}_4^{(o)}$. It is left to show that $\|x - v\|_1 \geq \|x\|_1$ holds for all $v \in \mathcal{L}(b_1, b_2)$, and that there is some $w \in \mathcal{L}(b_1, b_2)$ with $w \neq 0$ and $\|x - w\|_1 = \|x\|_1$. For this, consider all $v \in \mathcal{L}(b_1, b_2)$ with $\|x - v\|_1 \leq \|x\|_1$ and show that $\|x - v\|_1 = \|x\|_1$ needs to hold. The proof distinguishes four cases according to the four sets $\mathcal{S}_j^{(o)}$ for $j = 1, 2, 3, 4$, and finds in every case at least one lattice vector $w \neq 0$ with $\|x - w\|_1 = \|x\|_1$, which in particular shows that these lattice vectors are generalized Voronoi-relevant vectors.

Hence, let $z_1, z_2 \in \mathbb{Z}$ and $v := z_1 b_1 + z_2 b_2$ with $|x_1 - z_1| + |x_2 - z_1 - 3z_2| = \|x - v\|_1 \leq \|x\|_1$, and consider the four following cases.

1. $x \in \mathcal{S}_1^{(o)} = \left\{ \pm \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x_1 + x_2 = 1, x_1 \in (0, 1) \right\}$:

   Due to symmetry, one can assume that $x_1 \in (0, 1)$. Then it follows that $\|x\|_1 = x_1 + x_2 = 1$, implying $|x_1 - z_1| \leq \|x - v\|_1 \leq 1$. Thus, it is $z_1 \in \{0, 1\}$. Now distinguish these two cases as well.

a) $z_1 = 0$:

Since $|x_2 - 3z_2| \leq \|x - v\|_1 \leq 1$, it holds that $z_2 = 0$ and $v = 0$.

b) $z_1 = 1$:

Now, $|x_2 - 1 - 3z_2| \leq 1$ needs to hold, which implies again $z_2 = 0$. This time it follows that $v = b_1$ and that $\|x - v\|_1 = |x_1 - 1| + |x_2 - 1| = 2 - x_1 - x_2 = 1 = \|x\|_1$. Additionally, the vectors $\pm b_1$ are generalized Voronoi-relevant.

2. $x \in \mathcal{S}_2^{(o)} = \left\{ \pm \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x_1 - x_2 = \frac{3}{2}, x_1 \in \left(\frac{1}{2}, 1\right) \right\}$:

Due to symmetry, one can assume that $x_1 \in \left(\frac{1}{2}, 1\right)$. Then it follows that $\|x\|_1 = x_1 - x_2 = \frac{3}{2}$. This yields $|x_1 - z_1| \leq \|x - v\|_1 \leq \frac{3}{2}$ and analogously $|x_2 - z_1 - 3z_2| \leq \frac{3}{2}$, which implies $z_1, -z_1 - 3z_2 \in \{0, 1, 2\}$. With this, distinguish the cases according to z_1.

a) $z_1 = 0$:

$-3z_2 \in \{0, 1, 2\}$ leads to $z_2 = 0$ and $v = 0$.

b) $z_1 = 1$:

Here, it must hold that $-3z_2 \in \{1, 2, 3\}$ and thus $z_2 = -1$. Then, it is $v = b_1 - b_2$ and $\|x - v\|_1 = |x_1 - 1| + |x_2 + 2| = 3 - x_1 + x_2 = \frac{3}{2} = \|x\|_1$.

c) $z_1 = 2$:

From $-3z_2 \in \{2, 3, 4\}$ it follows again that $z_2 = -1$. Hence, it is $v = 2b_1 - b_2$ and $\|x - v\|_1 = |x_1 - 2| + |x_2 + 1| = 3 - x_1 + x_2 = \frac{3}{2} = \|x\|_1$. Additionally, this case and the upper case show that $\pm(b_1 - b_2)$ and $\pm(2b_1 - b_2)$ are generalized Voronoi-relevant vectors.

3. $x \in \mathcal{S}_3^{(o)} = \left\{ \pm \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x_1 \geq 1, x_2 \leq 0, x_1 - x_2 \leq \frac{3}{2} \right\}$:

Due to symmetry, one can assume that $x_1 \geq 1$. Then it is $\|x\|_1 = x_1 - x_2 \leq \frac{3}{2}$. This yields $|x_1 - z_1| \leq \|x - v\|_1 \leq \frac{3}{2}$ and analogously $|x_2 - z_1 - 3z_2| \leq \frac{3}{2}$, which implies $z_1 \in \{0, 1, 2, 3\}$ and $-z_1 - 3z_2 \in \{-1, 0, 1, 2\}$. With this, distinguish the cases according to z_1.

a) $z_1 = 0$:

$-3z_2 \in \{-1, 0, 1, 2\}$ gives $z_2 = 0$ and $v = 0$.

b) $z_1 = 1$:

$-3z_2 \in \{0, 1, 2, 3\}$ implies $z_2 \in \{-1, 0\}$. If $z_2 = -1$, then $x_2 \geq -\frac{1}{2}$ yields together with $x_1 - x_2 = \|x\|_1 \geq \|x - v\|_1 = |x_1 - 1| + |x_2 + 2| = 1 + x_1 + x_2$ that $x_2 = -\frac{1}{2}$, and from this it follows $x_1 = 1$ as well as $\|x - v\|_1 = \frac{3}{2} = \|x\|_1$. If $z_2 = 0$, then it is $\|x - v\|_1 = |x_1 - 1| + |x_2 - 1| = x_1 - x_2 = \|x\|_1$ for every $x \in \mathcal{S}_3^{(o)}$ with $x_1 \geq 1$.

c) $z_1 = 2$:

Here, it must hold that $-3z_2 \in \{1, 2, 3, 4\}$, which leads to $z_2 = -1$. Furthermore, $x_1 - x_2 \leq \frac{3}{2}$ and $x_1 - x_2 = \|x\|_1 \geq \|x - v\|_1 = |x_1 - 2| + |x_2 + 1| = 3 - x_1 + x_2$ imply $x_1 - x_2 = \frac{3}{2}$, which gives $\|x - v\|_1 = \frac{3}{2} = \|x\|_1$.

d) $z_1 = 3$:

Now $-3z_2 \in \{2, 3, 4, 5\}$ holds, which implies $z_2 = -1$ and $v = 3b_1 - b_2$. Moreover, it follows from $x_1 \leq \frac{3}{2}$ and $x_1 - x_2 = \|x\|_1 \geq \|x - v\|_1 = |x_1 - 3| + |x_2| = 3 - x_1 - x_2$ that $x_1 = \frac{3}{2}$ holds. Hence, $x_2 = 0$ and $\|x - v\|_1 = \frac{3}{2} = \|x\|_1$. In addition, this shows that $\pm(3b_1 - b_2)$ are generalized Voronoi-relevant vectors.

4. $x \in \mathcal{S}_4^{(o)} = \left\{ \pm \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x_1 \geq 0, x_2 \leq -1, x_1 - x_2 \leq \frac{3}{2} \right\}$:

Due to symmetry, one can assume that $x_2 \leq -1$. Then it is $x + b_1 \in \mathcal{S}_3^{(o)}$ with $x_1 + 1 \geq 1$. Furthermore, it is $\|(x + b_1) - (v + b_1)\|_1 = \|x - v\|_1 \leq \|x\|_1 = x_1 - x_2 = \|x + b_1\|_1$. Hence, the above investigation for $\mathcal{S}_3^{(o)}$ already shows that $v + b_1 \in \{0, b_1 - b_2, b_1, 2b_1 - b_2, 3b_1 - b_2\}$ – which is equivalent to $v \in \{-b_1, -b_2, 0, b_1 - b_2, 2b_1 - b_2\}$ – and that $\|x - v\|_1 = \|x\|$ must hold in every case according to v. Additionally, in the case $v = -b_1$ it follows that $\|x - v\|_1 = \|x\|_1$ holds for every $x \in \mathcal{S}_4^{(o)}$ with $x_2 \leq -1$, and the case $v = -b_2$ shows that $\pm b_2$ are generalized Voronoi-relevant vectors.

□

These three lemmata give proof of Proposition 2.21 as well as a direct corollary specifying all generalized Voronoi-relevant vectors of $\mathcal{L}(b_1, b_2)$ with respect to $\|\cdot\|_1$.

Proof of Proposition 2.21. The proof follows directly from combining Lemmata 2.22, 2.23 and 2.24 since $\mathcal{V}^{(i)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$ and $\mathcal{V}^{(o)}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$ are disjoint by definition. □

Corollary 2.25 *Let $z_1, z_2 \in \mathbb{Z}$. Then it holds that $z_1 b_1 + z_2 b_2$ is a generalized Voronoi-relevant vector with respect to $\|\cdot\|_1$ if and only if $(z_1, z_2) \in \mathcal{I} \setminus \{(0, 0)\}$.*

Proof. This statement is a direct consequence of Lemmata 2.17, 2.18, 2.19 and 2.24. □

Moreover, all Voronoi-relevant vectors can be computed as follows.

Lemma 2.26 *$v \in \mathcal{L}(b_1, b_2)$ is Voronoi-relevant with respect to $\|\cdot\|_1$ if and only if $v = \pm b_1$.*

Proof. Since every Voronoi-relevant vector is a generalized Voronoi-relevant vector, it holds for every Voronoi-relevant vector $z_1 b_1 + z_2 b_2 \in \mathcal{L}(b_1, b_2)$ by Corollary 2.25 that $(z_1, z_2) \in \mathcal{I} \setminus \{(0, 0)\}$. Due to symmetry, only five different values for (z_1, z_2) need to be considered.

1. $(z_1, z_2) = (0, 1)$:

   In this case, it will be shown that the vectors $\pm b_2$ are not Voronoi-relevant because for every $x \in \mathbb{R}^2$ with $\|x\|_1 = \|x - b_2\|_1$ it is $\|x + b_1 - b_2\|_1 \leq \|x\|_1$.

   To see this, let $x = (x_1, x_2)^T \in \mathbb{R}^2$ such that $|x_1| + |x_2| = \|x\|_1 = \|x - b_2\|_1 = |x_1| + |x_2 - 3|$. Consequently, $x_2 = \frac{3}{2}$ holds (cf. Figure 2.2). Now distinguish the following three cases.

   a) $x_1 \geq 0$:

      Here, even the following equality

      $$\|x + b_1 - b_2\|_1 = x_1 + \frac{3}{2} = \|x\|_1 = \|x - b_2\|_1 \tag{2.2}$$

      holds.

   b) $-1 < x_1 < 0$:

      It follows that $\|x + b_1 - b_2\|_1 = x_1 + \frac{3}{2} < -x_1 + \frac{3}{2} = \|x\|_1$.

   c) $x_1 \leq -1$:

      Then it holds that $\|x + b_1 - b_2\|_1 = -x_1 - \frac{1}{2} < -x_1 + \frac{3}{2} = \|x\|_1$.

2. $(z_1, z_2) = (3, -1)$:

   In this case, it will be shown that the vectors $\pm(3b_1 - b_2)$ are not Voronoi-relevant because for every $x \in \mathbb{R}^2$ with $\|x\|_1 = \|x - 3b_1 + b_2\|_1$ it holds that $\|x - 2b_1 + b_2\|_1 \leq \|x\|_1$.

   This can be seen completely analogously to the case $(z_1, z_2) = (0, 1)$ above by exchanging the roles of x_1 and x_2. In particular, it holds for $x_2 \geq 0$ that

   $$\|x - 2b_1 + b_2\|_1 = x_2 + \frac{3}{2} = \|x\|_1 = \|x - 3b_1 + b_2\|_1. \tag{2.3}$$

3. $(z_1, z_2) = (-1, 1)$:

   In this case, it will be shown that the vectors $\pm(b_1 - b_2)$ are not Voronoi-relevant because for every $x \in \mathbb{R}^2$ with $\|x\|_1 = \|x + b_1 - b_2\|_1$ there is some $v \in \{b_1, b_2, -2b_1 + b_2\}$ such that $\|x - v\|_1 \leq \|x\|_1$ holds.

   To see this, let $x = (x_1, x_2)^T \in \mathbb{R}^2$ such that $|x_1| + |x_2| = \|x\|_1 = \|x + b_1 - b_2\|_1 = |x_1 + 1| + |x_2 - 2|$. Now distinguish the following three cases (cf. Figure 2.2).

   a) $x_1 \geq 0$:

      Then it must hold that $|x_2| - 1 = |x_2 - 2|$, which leads to $x_2 = \frac{3}{2}$. Thus, in this case (2.2) holds as well.

   b) $-1 < x_1 < 0$:

From $\|x\|_1 = \|x + b_1 - b_2\|_1$ it follows that $|x_2| - 2x_1 - 1 = |x_2 - 2|$ and thus $x_2 - x_1 = \frac{3}{2}$. Hence, $\|x\|_1 = -x_1 + x_2 = \frac{3}{2}$ holds. If $x_1 < -\frac{1}{2}$, then it holds that $\|x + 2b_1 - b_2\|_1 = 3 + x_1 - x_2 = \frac{3}{2} = \|x\|_1$. If $x_1 \geq -\frac{1}{2}$, then it is $\|x - b_1\|_1 = -x_1 + x_2 = \frac{3}{2} = \|x\|_1$.

c) $x_1 \leq -1$:

Then it follows that $|x_2| + 1 = |x_2 - 2|$, which implies $x_2 = \frac{1}{2}$. Due to $x_1 \leq -1$, it moreover holds that $\|x + 2b_1 - b_2\|_1 = |x_1 + 2| + \frac{1}{2} \leq -x_1 + \frac{1}{2} = \|x\|_1$.

4. $(z_1, z_2) = (2, -1)$:

In this case, it will be shown that the vectors $\pm(2b_1 - b_2)$ are not Voronoi-relevant because for every $x \in \mathbb{R}^2$ with $\|x\|_1 = \|x - 2b_1 + b_2\|_1$ there is some $v \in \{b_1, b_1 - b_2, 3b_1 - b_2\}$ such that $\|x - v\|_1 \leq \|x\|_1$ holds.

This can be seen completely analogously to the case $(z_1, z_2) = (-1, 1)$ above by exchanging the roles of x_1 and x_2, and using (2.3).

5. $(z_1, z_2) = (1, 0)$:

This final case will show that $\pm b_1$ are Voronoi-relevant. For this, let $x := \frac{1}{2}b_1$ to get $\|x\|_1 = 1 = \|x - b_1\|_1$, and assume for contradiction that there is some $v \in \mathcal{L}(b_1, b_2) \setminus \{0, b_1\}$ with $\|x - v\|_1 \leq 1$. Let $z_1, z_2 \in \mathbb{Z}$ such that $v = z_1 b_1 + z_2 b_2$. From $\|x - v\|_1 = \left|\frac{1}{2} - z_1\right| + \left|\frac{1}{2} - z_1 - 3z_2\right|$ it follows that $\left|\frac{1}{2} - z_1\right| \leq 1$, which shows $z_1 \in \{0, 1\}$. Thus it needs to hold that $\left|\frac{1}{2} - 3z_2\right| \leq 1$ or $\left|-\frac{1}{2} - 3z_2\right| \leq 1$, but both cases imply $z_2 = 0$ and $v \in \{0, b_1\}$, which is a contradiction.

□

This lemma as well as the above Voronoi cell lead to the observation that the Voronoi-relevant vectors are in general not sufficient to determine the Voronoi cell of the origin of a two-dimensional lattice completely when a non-strictly convex norm is used. This is expressed by the following corollary, and leads to the conclusion that all generalized Voronoi-relevant vectors need to be considered under the usage of a non-strictly convex norm. The relation between the Voronoi cell of the origin and the (generalized) Voronoi-relevant vectors will be examined more formally in Section 4.3.

Corollary 2.27 *It holds that* $(\frac{7}{8}, -\frac{7}{8})^T \notin \mathcal{V}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$, *although*

$$\left\| \left(\frac{7}{8}, -\frac{7}{8}\right)^T - v \right\|_1 > \left\| \left(\frac{7}{8}, -\frac{7}{8}\right)^T \right\|_1$$

holds for all $v \in \mathcal{L}(b_1, b_2)$ *that are Voronoi-relevant with respect to* $\|\cdot\|_1$.

Proof. $(\frac{7}{8}, -\frac{7}{8})^T \notin \mathcal{V}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$ is a direct consequence from Proposition 2.21. Simple calculation shows $\left\|(\frac{7}{8}, -\frac{7}{8})^T - b_1\right\|_1 = 2 = \left\|(\frac{7}{8}, -\frac{7}{8})^T + b_1\right\|_1$ as well as $\left\|(\frac{7}{8}, -\frac{7}{8})^T\right\|_1 = \frac{7}{4}$, and the statement follows by Lemma 2.26. □

Unfortunately, for generalized Voronoi-relevant vectors in two-dimensional lattices under non-strictly convex norms one cannot find an analogous result to Voronoi-relevant vectors in two-dimensional lattices under strictly convex norms. In fact, the number of generalized Voronoi-relevant vectors is not upper bounded by a constant in this setting.

Theorem 2.28 *For every $m \in \mathbb{N}$ there is a lattice $\Lambda_m \subseteq \mathbb{R}^2$ of rank two with at least $2\left(2\left\lfloor\frac{m}{2}\right\rfloor + 1\right)$ generalized Voronoi-relevant vectors with respect to $\|\cdot\|_1$.*

Proof. Let $\Lambda_m := \mathcal{L}(b_{m,1}, b_{m,2})$, where $b_{m,1} = (1, 1)^T$ and $b_{m,2} = (0, m)^T$. Furthermore, consider $x := \frac{1}{2}b_{m,2}$. The rest of this proof shows that for every $v \in \Lambda_m$ it holds that $\|x - v\|_1 \geq \frac{m}{2}$, and that there are exactly $2\left\lfloor\frac{m}{2}\right\rfloor + 2$ lattice vectors fulfilling the equality $\|x - v\|_1 = \frac{m}{2}$.

Hence, consider additionally $v = z_1 b_{m,1} + z_2 b_{m,2}$ with $z_1, z_2 \in \mathbb{Z}$ as well as $\frac{m}{2} \geq \|x - v\|_1 = |z_1| + \left|z_1 + m\left(z_2 - \frac{1}{2}\right)\right|$. This implies both $|z_1| \leq \frac{m}{2}$ and $\left|z_1 + m\left(z_2 - \frac{1}{2}\right)\right| \leq \frac{m}{2} - |z_1|$. With this, distinguish the following four cases.

1. $z_1 \geq 0$ and $z_2 \geq 1$:

   In this case, $z_1 + m\left(z_2 - \frac{1}{2}\right) \leq \frac{m}{2} - z_1$ holds, which implies $m \geq 2z_1 + mz_2 \geq mz_2 \geq m$ and thus $z_2 = 1$ as well as $z_1 = 0$ follow. Therefore, $\|x - v\|_1 = \frac{m}{2}$ holds.

2. $z_1 \geq 0$ and $z_2 \leq 0$:

   Assume for contradiction that $z_1 + m\left(z_2 - \frac{1}{2}\right) > 0$. Then $z_1 > m\left(\frac{1}{2} - z_2\right) \geq \frac{m}{2}$ holds, which contradicts $|z_1| \leq \frac{m}{2}$.

   Hence, it holds that $z_1 + m\left(z_2 - \frac{1}{2}\right) \leq 0$, which leads to $-z_1 + m\left(\frac{1}{2} - z_2\right) \leq \frac{m}{2} - z_1$. Thus, $z_2 \geq 0$ follows, yielding $z_2 = 0$. For all $z_1 \in \left[0, \frac{m}{2}\right]$ it now holds that $\|x - v\|_1 = \frac{m}{2}$.

3. $z_1 < 0$ and $z_2 \leq 0$:

   In this case, $-z_1 + m\left(\frac{1}{2} - z_2\right) \leq \frac{m}{2} + z_1$ holds, which leads to the contradiction $0 < -2z_1 \leq -2z_1 - mz_2 \leq 0$. Therefore, this case cannot occur.

4. $z_1 < 0$ and $z_2 \geq 1$:

   Assume for contradiction that $z_1 + m\left(z_2 - \frac{1}{2}\right) < 0$. Then $z_1 < m\left(\frac{1}{2} - z_2\right) \leq -\frac{m}{2}$ holds, which contradicts $|z_1| \leq \frac{m}{2}$.

   Hence, it holds that $z_1 + m\left(z_2 - \frac{1}{2}\right) \geq 0$, which yields $z_1 + m\left(z_2 - \frac{1}{2}\right) \leq \frac{m}{2} + z_1$. Thus, $z_2 \leq 1$ follows, leading to $z_2 = 1$. For all $z_1 \in \left[-\frac{m}{2}, 0\right)$ it now holds that $\|x - v\|_1 = \frac{m}{2}$.

Summing up, these cases show that $\|x - v\|_1 = \frac{m}{2}$ holds if and only if $z_2 = 0$ and $z_1 \in \left[0, \frac{m}{2}\right]$ or $z_2 = 1$ and $z_1 \in \left[-\frac{m}{2}, 0\right]$, and that $\|x - v\|_1 \geq \frac{m}{2}$ holds for every $v \in \Lambda_m$. Therefore, $z_1 b_{m,1} + z_2 b_{m,2}$ is a generalized Voronoi-relevant vector if $z_2 = 0, z_1 \in \left(0, \frac{m}{2}\right]$ or $z_2 = 0, z_1 \in \left[-\frac{m}{2}, 0\right)$ or $z_2 = 1, z_1 \in \left[-\frac{m}{2}, 0\right]$ or $z_2 = -1, z_1 \in \left[0, \frac{m}{2}\right]$. In total, these are $2\left(2\left\lfloor\frac{m}{2}\right\rfloor + 1\right)$ generalized Voronoi-relevant vectors. □

In contrast to that, Lemma 2.9 and its proof also hold for generalized Voronoi-relevant vectors instead of Voronoi-relevant vectors, which shows that every lattice of rank two has at most eight generalized Voronoi-relevant vectors with respect to an arbitrary strictly convex norm, but – as shown in the above theorem – the number of generalized Voronoi-relevant vectors for lattices of rank two is in general not bounded from above by a constant when working with non-strictly convex norms.

3 Higher-dimensional lattices

Now one knows that the upper bound $2(2^n - 1)$ for the number of Voronoi-relevant vectors holds for the Euclidean norm in every dimension n, and that it further holds in the case $n = 2$ for every strictly convex norm. Unfortunately, this is not true for arbitrary strictly convex norms in higher dimensions. Even worse, there is no upper bound at all which only depends on the lattice dimension. This is shown in the next section.

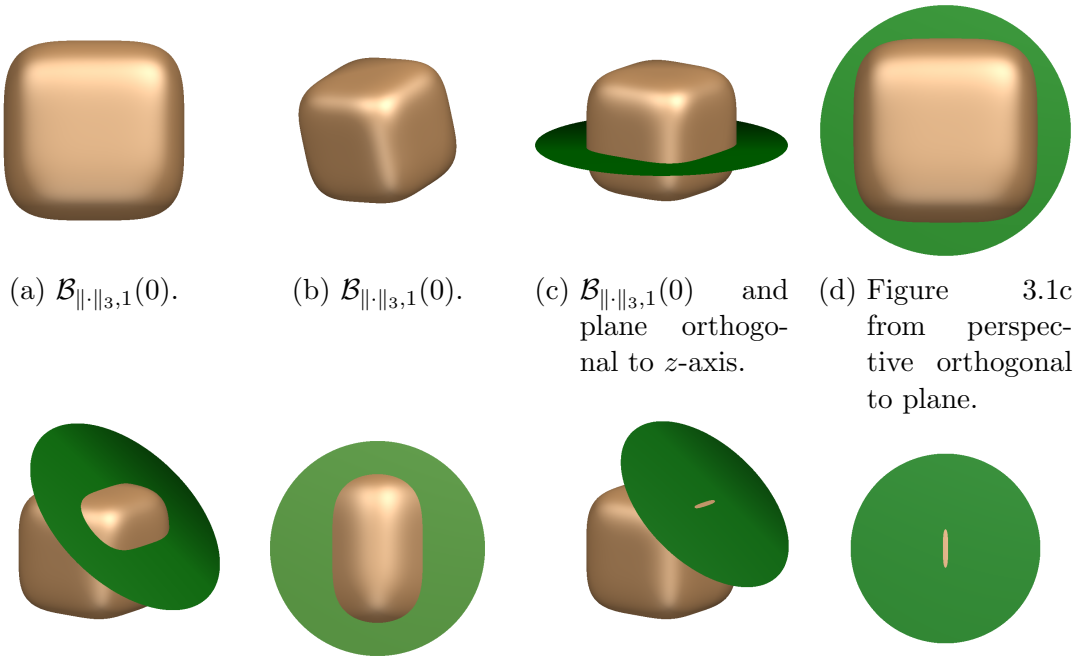
An upper bound that also depends on other lattice properties and not only on the dimension is shown in Section 3.2. This section also points out the consequences for the algorithm by Micciancio and Voulgaris [13] arising from the result that no upper bound for the number of Voronoi-relevant vectors can only depend on the lattice dimension when a general p-norm for $p \in \mathbb{N}, p \geq 3$ is considered.

3.1 Generalizations

In the following, a family of three-dimensional lattices of rank three will be constructed such that their number of Voronoi-relevant vectors with respect to the 3-norm $\|\cdot\|_3$ is not bounded from above by a constant. The idea is to use a lattice of the form $\mathcal{L}(e_1, e_2, Me_3)$, where (e_1, e_2, e_3) denotes the standard basis of $\mathbb{R}^3$ and $M \in \mathbb{N}$ is chosen sufficiently large, and to apply some rotations to this lattice. These rotations will depend on a parameter $m \in \mathbb{N}$ such that every lattice in the family is rotated differently. The basis vectors of the rotated lattices will be denoted by $b_{m,1}$, $b_{m,2}$ and $b_{m,3}$ and will coincide with the rotated versions of e_1, e_2 and Me_3, respectively. The intuition is to rotate $\mathcal{L}(e_1, e_2, Me_3)$ such that the line between 0 and $b_{m,1} + mb_{m,2}$ lies in an "edge" of a scaled and translated unit ball of the 3-norm when intersecting the plane spanned by 0, $b_{m,1}$ and $b_{m,2}$ with the ball.

Figure 3.1 shows the unit ball of the 3-norm with and without intersections with different planes. Let the x-, y- and z-axis denote the axes of the standard three-dimensional coordinate system which are spanned by e_1, e_2 and e_3, respectively. As seen in Figures 3.1c and 3.1d, the intersection of the ball with a plane which is orthogonal to the z-axis (e.g., the plane spanned by 0, e_1 and e_2) yields a scaled unit ball of the 3-norm in two dimensions. But when such a plane is rotated around the y-axis by 45°, as in Figures 3.1e to 3.1h, it intersects the three-dimensional unit ball of the 3-norm at one of its "edges". These kinds of intersections are roughly speaking as less circular as possible, and the closer the plane is to the "edge", the less circular the intersection is. Due to this, the plane spanned by

0, $b_{m,1}$ and $b_{m,2}$ should be of the form of the plane in Figures 3.1g and 3.1h. Moreover, the line between 0 and $b_{m,1} + mb_{m,2}$ should lie directly on the "edge" of a scaled and translated unit ball such that all other lattice points in the plane spanned by 0, $b_{m,1}$ and $b_{m,2}$ lie outside of the ball. This is illustrated in Figure 3.2 for the case $m = 3$. If M is now chosen large enough, every lattice point of the form $z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3}$ with $z_1, z_2, z_3 \in \mathbb{Z}, z_3 \neq 0$ will be sufficiently far away from the plane spanned by 0, $b_{m,1}$ and $b_{m,2}$ such that it will also lie outside of the ball. Then 0 and $b_{m,1} + mb_{m,2}$ are the only lattice points in the ball, and if they in fact lie on the boundary of the ball, it follows that $b_{m,1} + mb_{m,2}$ is a Voronoi-relevant vector, where the center of the ball serves as x in Definition 1.6 of Voronoi-relevant vectors.



(a) $\mathcal{B}_{\|\cdot\|_3,1}(0)$.

(b) $\mathcal{B}_{\|\cdot\|_3,1}(0)$.

(c) $\mathcal{B}_{\|\cdot\|_3,1}(0)$ and plane orthogonal to z-axis.

(d) Figure 3.1c from perspective orthogonal to plane.

(e) $\mathcal{B}_{\|\cdot\|_3,1}(0)$ and plane intersecting the ball at an "edge".

(f) Figure 3.1e from perspective orthogonal to plane.

(g) $\mathcal{B}_{\|\cdot\|_3,1}(0)$ and plane intersecting the ball at an "edge".

(h) Figure 3.1g from perspective orthogonal to plane.

Figure 3.1: $\mathcal{B}_{\|\cdot\|_3,1}(0)$ intersecting different planes.

With these figurative ideas at hand, the rotations of $\mathcal{L}(e_1, e_2, Me_3)$ will now be described formally. These modifications of the standard lattice are also illustrated in Figures 3.3 to 3.6 for the case $m = 3$. First, $\mathcal{L}(e_1, e_2, Me_3)$ is rotated around the z-axis until $e_1 + me_2$ lies on the y-axis, because all "edges" of the unit ball are

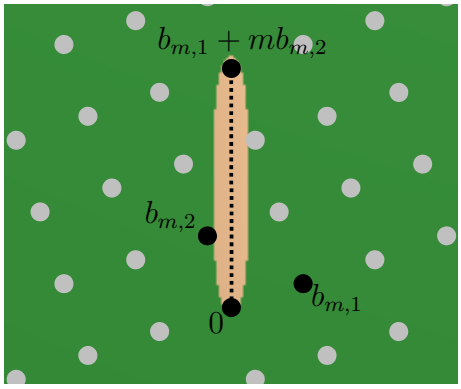


Figure 3.2: Plane spanned by 0, $b_{m,1}$ and $b_{m,2}$ intersects ball at an "edge" such that line between 0 and $b_{m,1} + mb_{m,2}$ lies on the "edge" (cf. Figure 3.1h).

parallel to the x-, y- or z-axis. This rotation is realized by the matrix

$$R_z := \begin{pmatrix} \frac{m}{\sqrt{m^2+1}} & -\frac{1}{\sqrt{m^2+1}} & 0 \\ \frac{1}{\sqrt{m^2+1}} & \frac{m}{\sqrt{m^2+1}} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Secondly, the resulting lattice $R_z\mathcal{L}(e_1, e_2, Me_3)$ is rotated around the y-axis by 45° such that after the rotation the plane formerly spanned by 0, e_1 and e_2 intersects translated unit balls of the 3-norm at one of their "edges". The second rotation is given by the matrix

$$R_y := \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ 0 & 1 & 0 \\ -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}.$$

The resulting lattice $\Lambda_m := R_y R_z \mathcal{L}(e_1, e_2, Me_3)$ is spanned by $b_{m,1} := R_y R_z e_1$, $b_{m,2} := R_y R_z e_2$ and $b_{m,3} := M R_y R_z e_3$. Using an appropriate scaling and translation of the unit ball, the situation in Figure 3.2 can be reached. As already mentioned, this can be used to show that $b_{m,1} + mb_{m,2}$ is Voronoi-relevant if M is sufficiently large. Actually, Λ_m has considerably more Voronoi-relevant vectors: In the following it is shown that choosing $M := 5\sqrt{2}m^5$ implies that $\lambda_i(\Lambda_m, \|\cdot\|_3) = \|b_{m,i}\|_3$ holds for $i \in \{1, 2, 3\}$ and that $b_{m,1} + mb_{m,2}$ as well as $b_{m,1} + kb_{m,2}$ for all $k \in \mathbb{N}, k \in [2, \sqrt{m}]$ are Voronoi-relevant with respect to $\|\cdot\|_3$. For this, two easy lemmata are shown first.

Lemma 3.1 *Let $C, D \in \mathbb{R}$ with $D \neq -C$. The function*

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R}_{\geq 0}, \\ x &\longmapsto |C + x|^3 + |D - x|^3 \end{aligned}$$

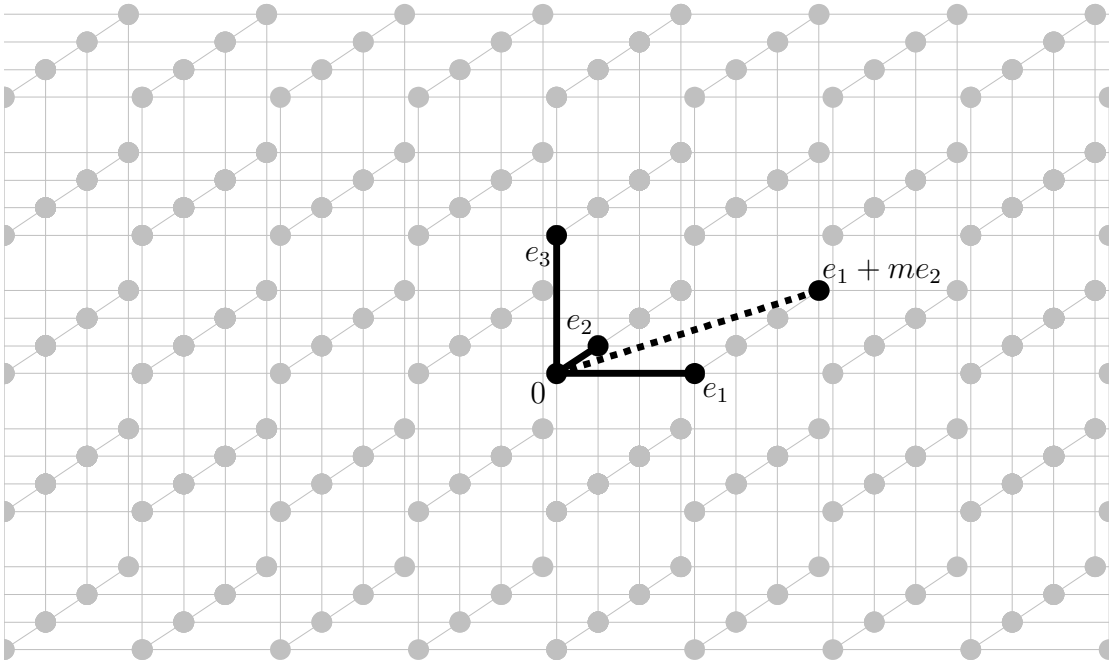


Figure 3.3: $\mathcal{L}(e_1, e_2, e_3)$.

has a global minimum at $\frac{D-C}{2}$ *with function value* $\frac{1}{4}|D+C|^3$.

Proof. Since $f'(x) = 3\operatorname{sgn}(C+x)(C+x)^2 - 3\operatorname{sgn}(D-x)(D-x)^2$, $f'(x) = 0$ holds if and only if $\operatorname{sgn}(C+x)(C+x)^2 = \operatorname{sgn}(D-x)(D-x)^2$. Now distinguish the following cases.

1. $\operatorname{sgn}(C+x) = \operatorname{sgn}(D-x)$: Then $f'(x) = 0$ holds if and only if $(C+x)^2 = (D-x)^2$, which is equivalent to $C+x = D-x$ since $X \mapsto X^2$ is bijective on $\mathbb{R}_{\geq 0}$ and $\mathbb{R}_{<0}$, respectively. Hence, $f'(x) = 0$ if and only if $x = \frac{D-C}{2}$.

2. $\operatorname{sgn}(C+x) = -\operatorname{sgn}(D-x)$: Then $f'(x) = 0$ holds if and only if $(C+x)^2 = -(D-x)^2$, which is equivalent to $C+x = 0 = D-x$ and thus to $D = x = -C$. Since this contradicts the assumption $D \neq -C$, there is no $x \in \mathbb{R}$ with $f'(x) = 0$ and $\operatorname{sgn}(C+x) = -\operatorname{sgn}(D-x)$.

Hence, $f'(x) = 0$ if and only if $x = \frac{D-C}{2}$. Since $f''(x) = 6|C+x| + 6|D-x|$ is everywhere strictly positive, $\frac{D-C}{2}$ is a global minimum of f with $f\left(\frac{D-C}{2}\right) = \frac{1}{4}|D+C|^3$. □

The next lemma computes the distance between some $v \in \mathbb{R}^3$ and the plane spanned by 0, e_1 and e_2 after this plane is translated along the z-axis and rotated around the y-axis by 45°.

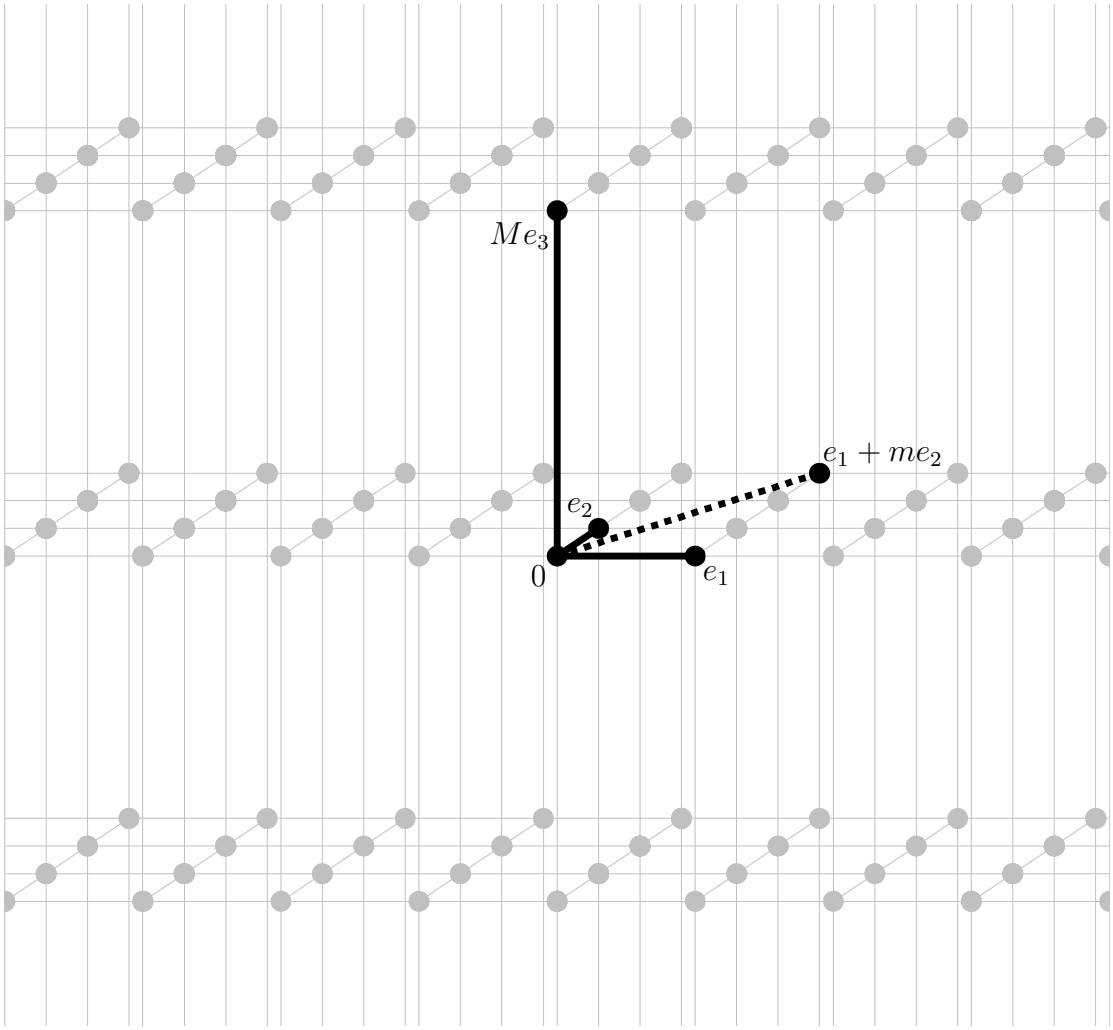


Figure 3.4: $\mathcal{L}(e_1, e_2, Me_3)$: Note that M is so large that this figure is not scaled properly.

Lemma 3.2 *Let $C \in \mathbb{R}$, $v = (\alpha, \beta, \gamma)^T \in \mathbb{R}^3$ and*

$$E_C := R_y \left(\mathbb{R} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + C \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right).$$

If $v \notin E_C$, then $\|v - E_C\|_3^3 = \left\| v - R_y \begin{pmatrix} \frac{\alpha-\gamma}{\sqrt{2}} \\ \beta \\ C \end{pmatrix} \right\|_3^3 = \frac{1}{4}|\sqrt{2}C - \alpha - \gamma|^3.$

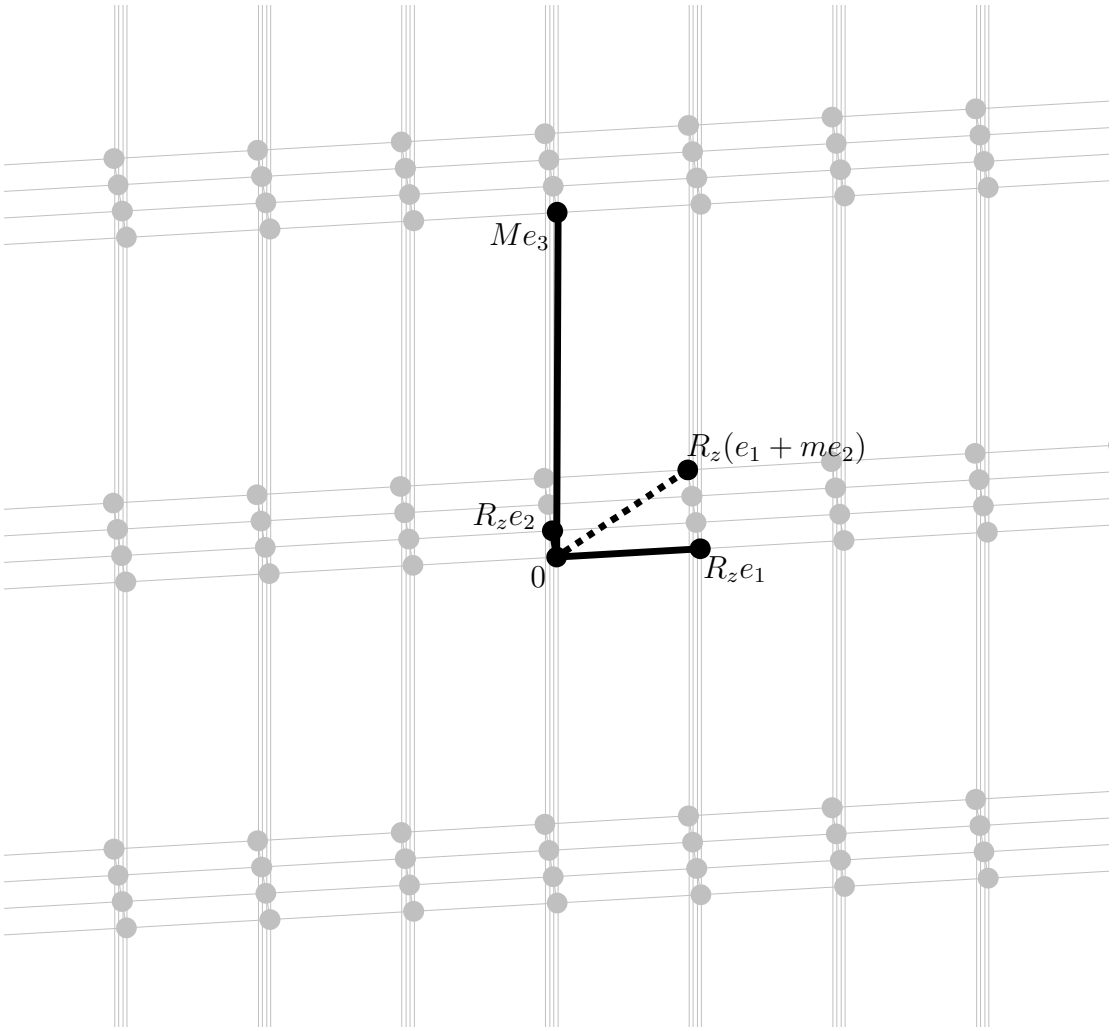


Figure 3.5: $R_z\mathcal{L}(e_1, e_2, Me_3)$.

Proof. First note that $v \in E_C$ is equivalent to

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}(C + A) \\ B \\ \frac{1}{\sqrt{2}}(C - A) \end{pmatrix}$$

for some $A, B \in \mathbb{R}$, which holds if and only if $C - \sqrt{2}\alpha = -C + \sqrt{2}\gamma$. Hence under the assumptions $v \notin E_C$, Lemma 3.1 can be applied as follows:

$$\begin{aligned} \|v - E_C\|_3^3 &= \min_{A,B\in\mathbb{R}} \left(\left| \frac{C}{\sqrt{2}} + \frac{A}{\sqrt{2}} - \alpha \right|^3 + |B - \beta|^3 + \left| \frac{C}{\sqrt{2}} - \frac{A}{\sqrt{2}} - \gamma \right|^3 \right) \\ &= \min_{B\in\mathbb{R}} |B - \beta|^3 + \frac{1}{\sqrt{2}^3} \min_{A\in\mathbb{R}} \left(|C - \sqrt{2}\alpha + A|^3 + |C - \sqrt{2}\gamma - A|^3 \right) \end{aligned}$$

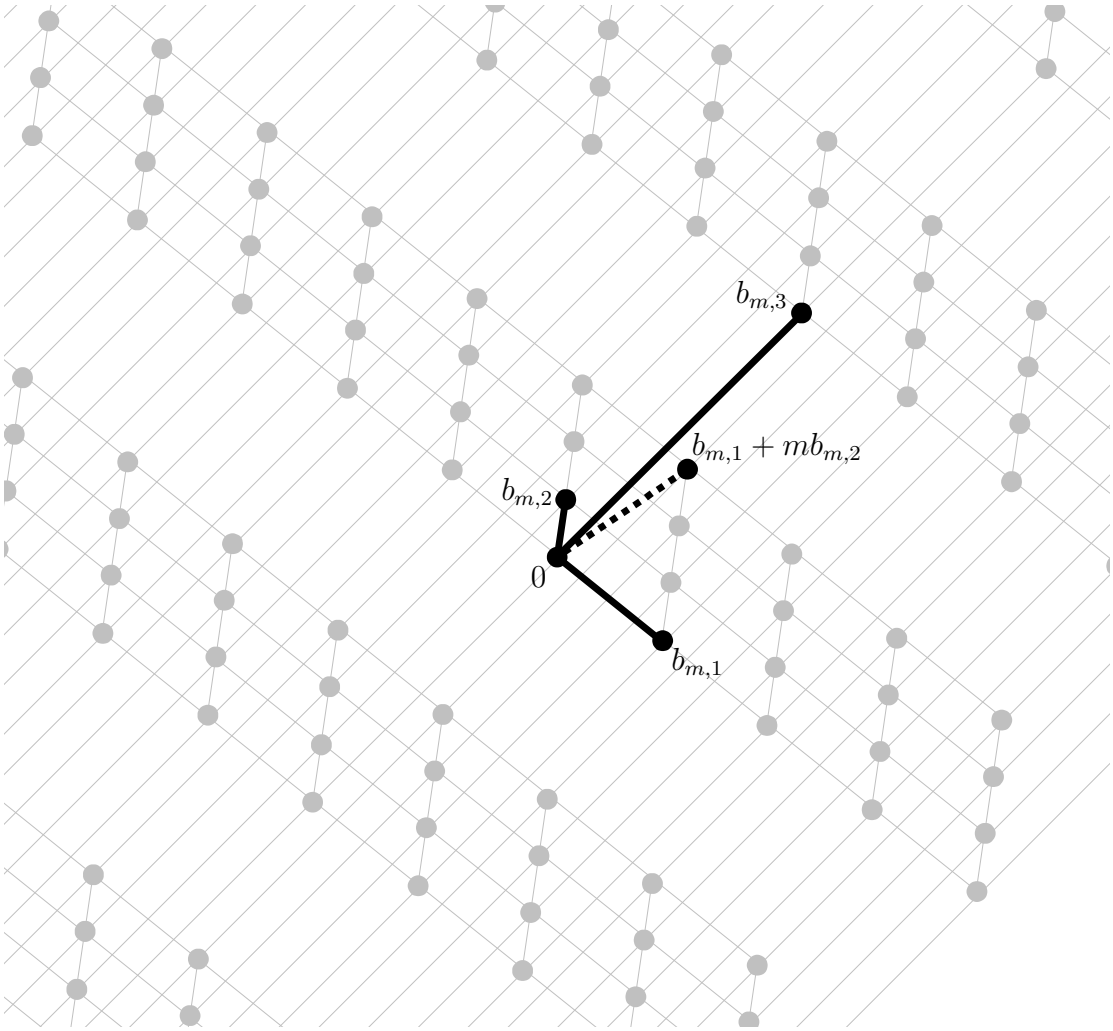


Figure 3.6: $\Lambda_m = R_y R_z \mathcal{L}(e_1, e_2, Me_3)$.

$$= \frac{1}{\sqrt{2}^3}\frac{1}{4}|2C - \sqrt{2}\alpha - \sqrt{2}\gamma|^3 = \frac{1}{4}|\sqrt{2}C - \alpha - \gamma|^3.$$

Moreover, it follows from Lemma 3.1 that the minima in the above equality are reached for $B = \beta$ and $A = \frac{\alpha-\gamma}{\sqrt{2}}$. □

With this, it will be shown that the lengths of the basis vectors of Λ_m coincide with the successive minima and that $b_{m,1} + mb_{m,2}$ is Voronoi-relevant in Λ_m. This yields for general strictly convex norms that the coefficients of Voronoi-relevant vectors, when they are represented in a successive minima basis, are not bounded from above by a bound that depends only on the lattice dimension. Note that this shows that Lemma 2.9 cannot be generalized to ranks higher than two.

Proposition 3.3 *For every $m \in \mathbb{N}, m \geq 2$ and every $i \in \{1,2,3\}$ it holds that*

$$\lambda_i(\Lambda_m, \|\cdot\|_3) = \|b_{m,i}\|_3.$$

Proof. This statement follows from the following four intermediate steps:

1. $\|b_{m,1}\|_3 < \|b_{m,2}\|_3$:

   First note that

   $$b_{m,1} = R_y R_z \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{m}{\sqrt{2}\sqrt{m^2+1}} \\ \frac{1}{\sqrt{m^2+1}} \\ -\frac{m}{\sqrt{2}\sqrt{m^2+1}} \end{pmatrix} \text{ and}$$
   $$b_{m,2} = R_y R_z \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -\frac{1}{\sqrt{2}\sqrt{m^2+1}} \\ \frac{m}{\sqrt{m^2+1}} \\ \frac{1}{\sqrt{2}\sqrt{m^2+1}} \end{pmatrix}.$$

   Hence, $\|b_{m,1}\|_3^3 = \frac{m^3+\sqrt{2}}{\sqrt{2}\sqrt{m^2+1}^3}$ and $\|b_{m,2}\|_3^3 = \frac{\sqrt{2}m^3+1}{\sqrt{2}\sqrt{m^2+1}^3}$. Since $m \geq 2$, it holds that $m^3 > 1$ and thus $\sqrt{2}m^3+1 > m^3+\sqrt{2}$, which implies $\|b_{m,2}\|_3 > \|b_{m,1}\|_3$.

2. $\|b_{m,2}\|_3 < \|z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3}\|_3$ for all $z_1, z_2, z_3 \in \mathbb{Z}, z_3 \neq 0$:

   For all $z_1, z_2, z_3 \in \mathbb{Z}$ with $z_3 \neq 0$ it holds that $z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3} \in E_{Mz_3}$ using the notation in Lemma 3.2. Thus by the same lemma and the choice $M = 5\sqrt{2}m^5$,

   $$\|z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3}\|_3^3 \geq \|0 - E_{Mz_3}\|_3^3 = \frac{1}{4}|\sqrt{2}Mz_3|^3 \geq 250m^{15}. \quad (3.1)$$

   The desired inequality follows since $\|b_{m,2}\|_3^3 < \sqrt{2}m^3 + 1 < (\sqrt{2}+1)m^3$.

3. $\|b_{m,2}\|_3 < \|v\|_3$ for all $v \in \Lambda_m \setminus \{0, b_{m,1}, -b_{m,1}, b_{m,2}, -b_{m,2}\}$:

   By the above estimate, only $v \in \Lambda_m$ of the form $v = z_1 b_{m,1} + z_2 b_{m,2}$ for $z_1, z_2 \in \mathbb{Z}$ are left to be considered. Assume that for such a v it holds that $\|v\|_3 \leq \|b_{m,2}\|_3$.

   Since

   $$v = \begin{pmatrix} \frac{z_1 m - z_2}{\sqrt{2}\sqrt{m^2+1}} \\ \frac{z_2 m + z_1}{\sqrt{m^2+1}} \\ -\frac{z_1 m - z_2}{\sqrt{2}\sqrt{m^2+1}} \end{pmatrix},$$

   it is $\|v\|_3^3 = \frac{1}{\sqrt{m^2+1}^3}\left(\frac{1}{\sqrt{2}}|z_1 m - z_2|^3 + |z_2 m + z_1|^3\right)$. Hence $\|v\|_3 \leq \|b_{m,2}\|_3$

implies that

$$\frac{1}{\sqrt{2}}|z_1 m - z_2|^3 + |z_2 m + z_1|^3 \leq m^3 + \frac{1}{\sqrt{2}}. \tag{3.2}$$

In particular it holds that $|z_2 m + z_1| \leq m$ due to $z_1, z_2 \in \mathbb{Z}$.

If $z_2 \geq 2$, $|z_2 m + z_1| \leq m$ implies $z_1 \leq -m$. Thus it follows $|z_1 m - z_2|^3 \geq (m^2+2)^3 > m^6 > (\sqrt{2}+1)m^3 > \sqrt{2}m^3 + 1$, which contradicts (3.2). For $z_2 \leq -2$, it is $z_1 \geq m$, which yields the same estimate with the same contradiction.

If $z_2 = 1$, $|m + z_1| \leq m$ implies $z_1 \leq 0$. Thus it holds that $-z_1^3 m^3 < |z_1 m - 1|^3 \leq \sqrt{2}m^3 + 1 < (\sqrt{2}+1)m^3$, which leads to $z_1 \in \{-1, 0\}$. Since $3(\sqrt{2}-1) < m$, it follows $3(\sqrt{2}-1)m^2 + \sqrt{2} < m^3 + 3(\sqrt{2}+1)m$, which implies $\sqrt{2}m^3 + 1 < (m+1)^3 + \sqrt{2}(m-1)^3 = |-m-1|^3 + \sqrt{2}|m-1|^3$. This contradicts (3.2) for the case $z_1 = -1$, yielding $z_1 = 0$. For $z_2 = -1$, it is $z_1 \geq 0$, and $z_1^3 m^3 < |z_1 m + 1|^3$ leads as above to $z_1 \in \{0, 1\}$, but the case $z_1 = 1$ contradicts (3.2) using the same estimate as above. Hence it follows for $|z_2| = 1$ that $z_1 = 0$, i.e., $v \in \{-b_{m,2}, b_{m,2}\}$.

If $z_2 = 0$, (3.2) implies $|z_1|^3 m^3 \leq \sqrt{2}m^3 + 1 < (\sqrt{2}+1)m^3$. Hence it holds that $z_1 \in \{-1, 0, 1\}$, i.e., $v \in \{-b_{m,1}, 0, b_{m,1}\}$.

4. $\|b_{m,3}\|_3 \leq \|z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3}\|_3$ for all $z_1, z_2, z_3 \in \mathbb{Z}, z_3 \neq 0$:

   Since $b_{m,3} = MR_yR_z(0,0,1)^T = (5m^5, 0, 5m^5)^T$, $\|b_{m,3}\|_3^3 = 250m^{15}$. Together with (3.1), this shows the desired inequality.

□

Proposition 3.4 *For every $m \in \mathbb{N}, m \geq 2$ it holds that $b_{m,1} + mb_{m,2}$ is Voronoi-relevant in Λ_m with respect to $\|\cdot\|_3$.*

Proof. Define

$$x := \begin{pmatrix} m^5 \\ \frac{\sqrt{m^2+1}}{2} \\ m^5 \end{pmatrix}.$$

Then $\|x\|_3^3 = 2m^{15} + \frac{1}{8}\sqrt{m^2+1}^3 = \|b_{m,1} + mb_{m,2} - x\|_3^3$, and the following two estimates show that $\|x\|_3 < \|x - v\|_3$ for all $v \in \Lambda_m \setminus \{0, b_{m,1} + mb_{m,2}\}$, which completes the proof.

1. $\|x\|_3 < \|z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3} - x\|_3$ for all $z_1, z_2, z_3 \in \mathbb{Z}, z_3 \neq 0$:

   By Lemma 3.2 it follows for all $z_1, z_2, z_3 \in \mathbb{Z}$ with $z_3 \neq 0$ that

   $$\|z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3} - x\|_3^3 \geq \|x - E_{Mz_3}\|_3^3$$

$$= \frac{1}{4}|\sqrt{2}Mz_3 - 2m^5|^3 = \frac{1}{4}m^{15}|10z_3 - 2|^3$$
$$\geq \frac{1}{4}m^{15} \cdot 8^3 = 128m^{15}.$$

The desired inequality follows since $\|x\|_3^3 < 2m^{15} + \frac{1}{8}(2m^2)^3 < 3m^{15}$.

2. $\|x\|_3 < \|x - v\|_3$ for all $v \in \Lambda_m \setminus \{0, b_{m,1} + mb_{m,2}\}$:

   By the first estimate, only $v \in \Lambda_m$ of the form $v = z_1 b_{m,1} + z_2 b_{m,2}$ for $z_1, z_2 \in \mathbb{Z}$ have to be considered. Assume that for such a v it holds that $\|x - v\|_3 \leq \|x\|_3$.

   Define $Z := \frac{z_1 m - z_2}{\sqrt{m^2+1}}$. Then

$$v = \begin{pmatrix} \frac{Z}{\sqrt{2}} \\ \frac{z_2 m + z_1}{\sqrt{m^2+1}} \\ \frac{-Z}{\sqrt{2}} \end{pmatrix}$$

   and $\|x - v\|_3^3 \geq \left|m^5 - \frac{Z}{\sqrt{2}}\right|^3 + \left|m^5 + \frac{Z}{\sqrt{2}}\right|^3$.

   If $m^5 - \frac{Z}{\sqrt{2}} < 0$, then $Z > \sqrt{2}m^5$ and $\|x - v\|_3^3 \geq (m^5 + \frac{Z}{\sqrt{2}})^3 > 8m^{15}$. If $m^5 + \frac{Z}{\sqrt{2}} < 0$, then $Z < -\sqrt{2}m^5$ and $\|x - v\|_3^3 \geq (m^5 - \frac{Z}{\sqrt{2}})^3 > 8m^{15}$. Both cases lead to the contradiction $8m^{15} < \|x - v\|_3^3 \leq \|x\|_3^3 < 3m^{15}$.

   Hence it can be assumed that $\|x - v\|_3^3 \geq (m^5 - \frac{Z}{\sqrt{2}})^3 + (m^5 + \frac{Z}{\sqrt{2}})^3 = 2m^{15} + 3Z^2m^5$. Using $\|x\|_3^3 = 2m^{15} + \frac{1}{8}\sqrt{m^2+1}^3$ implies the inequality $3Z^2m^5 \leq \frac{1}{8}\sqrt{m^2+1}^3$. This leads to $576Z^4m^{10} \leq (m^2+1)^3$ and thus to $|Z| \leq \sqrt[4]{\frac{(m^2+1)^3}{576m^{10}}}$. By definition of Z, it holds that $|z_1 m - z_2| \leq \sqrt[4]{\frac{(m^2+1)^5}{576m^{10}}}$. Since $(m^2+1)^5 = m^{10} + 5m^8 + 10m^6 + 10m^4 + 5m^2 + 1 < 32m^{10} < 576m^{10}$, it follows that $|z_1 m - z_2| < 1$. Thus $z_1 m - z_2 = 0$ due to $z_1, z_2 \in \mathbb{Z}$. With this, $v = (0, z_1\sqrt{m^2+1}, 0)^T$ and $\|x - v\|_3^3 = 2m^{15} + \frac{\sqrt{m^2+1}^3}{8}|2z_1 - 1|^3$. From $\|x - v\|_3 \leq \|x\|_3$ it directly follows that $|2z_1 - 1| \leq 1$, which is equivalent to $z_1 \in \{0, 1\}$, i.e., $v \in \{0, b_{m,1} + mb_{m,2}\}$.

□

The most important statement of this thesis will now be formulated: The above defined lattices Λ_m do not only have $b_{m,1} + mb_{m,2}$ as a Voronoi-relevant vector but also $b_{m,1} + kb_{m,2}$ for all $k \in \mathbb{N}, k \in [2, \sqrt{m}]$. Hence, it holds for the 3-norm that every Λ_m has $\Omega(\sqrt{m})$ Voronoi-relevant vectors, and that for every $k \in \mathbb{N}$ one can find a lattice that has at least k Voronoi-relevant vectors. This will be formalized in Corollary 3.6.

Theorem 3.5 *For every $k \in \mathbb{N}, k \geq 2$ and all $m \in \mathbb{N}, m \geq k^2$ it holds that $b_{m,1} + kb_{m,2}$ is Voronoi-relevant in Λ_m with respect to $\|\cdot\|_3$.*

Proof. For $k, m \in \mathbb{N}$ with $m \geq k \geq 2$ define

$$x_{m,k} := \frac{1}{2}(b_{m,1} + kb_{m,2}) + \begin{pmatrix} \left(\frac{k^2}{4} + \frac{1}{3}\right) m \\ 0 \\ \left(\frac{k^2}{4} + \frac{1}{3}\right) m \end{pmatrix} = \begin{pmatrix} \frac{m-k}{\sqrt{2}^3\sqrt{m^2+1}} + \left(\frac{k^2}{4} + \frac{1}{3}\right) m \\ \frac{km+1}{2\sqrt{m^2+1}} \\ \frac{k-m}{\sqrt{2}^3\sqrt{m^2+1}} + \left(\frac{k^2}{4} + \frac{1}{3}\right) m \end{pmatrix}.$$

Since $\frac{1}{4} + \frac{1}{3} \geq \frac{1}{\sqrt{2}^3}$, it holds that $\left(\frac{k^2}{4} + \frac{1}{3}\right) m \geq \frac{1}{\sqrt{2}^3} \geq \frac{m-k}{\sqrt{2}^3\sqrt{m^2+1}}$, which implies that

$$\begin{aligned} \|x_{m,k}\|_3^3 &= \left(\frac{m-k}{\sqrt{2}^3\sqrt{m^2+1}} + \left(\frac{k^2}{4} + \frac{1}{3}\right) m\right)^3 + \left(\frac{k-m}{\sqrt{2}^3\sqrt{m^2+1}} + \left(\frac{k^2}{4} + \frac{1}{3}\right) m\right)^3 \\ &\quad + \left(\frac{km+1}{2\sqrt{m^2+1}}\right)^3 \\ &= 2\left(\frac{k^2}{4} + \frac{1}{3}\right)^3 m^3 + 6\left(\frac{k^2}{4} + \frac{1}{3}\right) m \left(\frac{m-k}{\sqrt{2}^3\sqrt{m^2+1}}\right)^2 + \left(\frac{km+1}{2\sqrt{m^2+1}}\right)^3 \\ &= \|b_{m,1} + kb_{m,2} - x_{m,k}\|_3^3. \end{aligned}$$

To complete this proof, the following three estimates show $\|x_{m,k}\|_3 < \|x_{m,k} - v\|_3$ for all $v \in \Lambda_m \setminus \{0, b_{m,1} + kb_{m,2}\}$ and all $m \geq k^2$.

1. $\|x_{m,k}\|_3 < \|z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3} - x_{m,k}\|_3$ for all all $m \geq k$ and all $z_1, z_2, z_3 \in \mathbb{Z}, z_3 \neq 0$:

   On the one hand, it is $z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3} \in E_{Mz_3}$ for all $z_1, z_2, z_3 \in \mathbb{Z}$. On the other hand, $x_{m,k} \notin E_{Mz_3}$, because otherwise $2Mz_3 = 2\sqrt{2}m\left(\frac{k^2}{4} + \frac{1}{3}\right)$ would hold, which is equivalent to $60m^4 z_3 = 3k^2 + 4$ and hence implies $z_3 > 0$ leading to $z_3 \geq 1$ and the contradiction $60m^4 z_3 \geq 60k^4 > 4k^2 \geq 3k^2 + 4 = 60m^4 z_3$. By Lemma 3.2 it follows that

   $$\begin{aligned} \|z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3} - x_{m,k}\|_3^3 &\geq \|x_{m,k} - E_{Mz_3}\|_3^3 \\ &= \frac{1}{4}\left|\sqrt{2}Mz_3 - 2\left(\frac{k^2}{4} + \frac{1}{3}\right) m\right|^3 \\ &= \frac{1}{4} \cdot 1000m^{15}\left|z_3 - \frac{1}{5m^4}\left(\frac{k^2}{4} + \frac{1}{3}\right)\right|^3. \end{aligned}$$

   The prerequisite $m \geq k \geq 2$ yields $\frac{1}{5m^4}\left(\frac{k^2}{4} + \frac{1}{3}\right) \in \left(0, \frac{1}{60}\right]$. This shows for

$z_3 \in \mathbb{Z}\setminus\{0\}$ that the inequality $z_3 - \frac{1}{5m^4}\left(\frac{k^2}{4}+\frac{1}{3}\right) \geq 0$ is equivalent to $z_3 \geq 1$, and that

$$\begin{aligned}\|z_1 b_{m,1} + z_2 b_{m,2} + z_3 b_{m,3} - x_{m,k}\|_3^3 &\geq 250m^{15}\left(1 - \frac{1}{5m^4}\left(\frac{k^2}{4}+\frac{1}{3}\right)\right)^3 \\ &\geq 250m^{15}\left(\frac{59}{60}\right)^3 > 200m^{15}.\end{aligned}$$

The desired inequality follows since $\frac{m^2}{4}+\frac{1}{3} \leq m^2$ implies

$$\begin{aligned}\|x_{m,k}\|_3^3 &\leq 2m^9 + 6m^3\left(\frac{m}{\sqrt{2}^3\sqrt{m^2+1}}\right)^2 + \left(\frac{m^2+1}{2\sqrt{m^2+1}}\right)^3 \\ &\leq 2m^9 + \frac{3}{4}m^3 + m^3 < 4m^{15}.\end{aligned}$$

2. $\|x_{m,k}\|_3 < \|z_1 b_{m,1} + z_2 b_{m,2} - x_{m,k}\|_3$ for all $m \geq k$ and all $(z_1, z_2) \in \mathbb{Z}^2 \setminus (\{0,1\} \times \{1,\dots,k-1\}) \cup \{(0,0),(1,k)\})$:

For $v := z_1 b_{m,1} + z_2 b_{m,2}$ with $z_1, z_2 \in \mathbb{Z}$ it holds that

$$\begin{aligned}\|v - x_{m,k}\|_3^3 = &\left|\left(\frac{k^2}{4}+\frac{1}{3}\right)m - \frac{(2z_1-1)m-(2z_2-k)}{\sqrt{2}^3\sqrt{m^2+1}}\right|^3 \\ &+ \left|\left(\frac{k^2}{4}+\frac{1}{3}\right)m + \frac{(2z_1-1)m-(2z_2-k)}{\sqrt{2}^3\sqrt{m^2+1}}\right|^3 \\ &+ \left|\frac{(2z_2-k)m+(2z_1-1)}{2\sqrt{m^2+1}}\right|^3.\end{aligned}$$

If $\left(\frac{k^2}{4}+\frac{1}{3}\right)m - \frac{(2z_1-1)m-(2z_2-k)}{\sqrt{2}^3\sqrt{m^2+1}} < 0$ or $\left(\frac{k^2}{4}+\frac{1}{3}\right)m + \frac{(2z_1-1)m-(2z_2-k)}{\sqrt{2}^3\sqrt{m^2+1}} < 0$, then $\|v - x_{m,k}\|_3^3 > 8\left(\frac{k^2}{4}+\frac{1}{3}\right)^3 m^3$. Assume in this case for contradiction that $\|v - x_{m,k}\|_3 \leq \|x_{m,k}\|_3$. This implies that $6\left(\frac{k^2}{4}+\frac{1}{3}\right)^3 m^3 < 6\left(\frac{k^2}{4}+\frac{1}{3}\right)m\left(\frac{m-k}{\sqrt{2}^3\sqrt{m^2+1}}\right)^2 + \left(\frac{km+1}{2\sqrt{m^2+1}}\right)^3$. Dividing by $6\left(\frac{k^2}{4}+\frac{1}{3}\right)m$ and multiplying by $8\sqrt{m^2+1}^3$ yields $8\left(\frac{k^2}{4}+\frac{1}{3}\right)^2 m^2\sqrt{m^2+1}^3 < (m-k)^2\sqrt{m^2+1} + \frac{2(km+1)^3}{m(3k^2+4)}$. Using $m < \sqrt{m^2+1} < \sqrt{2}m$ and $2(km+1) < m(3k^2+4)$ leads to $8\frac{k^4}{16}m^5 < \sqrt{2}m^3 + (km+1)^2 < \sqrt{2}m^3 + 4k^2m^2$. Hence $16m^3 \leq k^4m^3 < 2\sqrt{2}m + 8k^2 < 4m + 8m^2$ follows, leading to

$0 > 4m^2 - 2m - 1 = 4\left(m - \frac{1+\sqrt{5}}{4}\right)\left(m - \frac{1-\sqrt{5}}{4}\right)$, but this is a contradiction since $\frac{1-\sqrt{5}}{4} < \frac{1+\sqrt{5}}{4} < 1$ and $m \geq 2$. This shows $\|v - x_{m,k}\|_3 > \|x_{m,k}\|_3$ in case that $\left(\frac{k^2}{4} + \frac{1}{3}\right) m - \frac{(2z_1-1)m-(2z_2-k)}{\sqrt{2}^3\sqrt{m^2+1}} < 0$ or $\left(\frac{k^2}{4} + \frac{1}{3}\right) m + \frac{(2z_1-1)m-(2z_2-k)}{\sqrt{2}^3\sqrt{m^2+1}} < 0$.

Hence it can be assumed in the following that

$$\begin{aligned}
\|v - x_{m,k}\|_3^3 = &\left(\left(\frac{k^2}{4} + \frac{1}{3}\right) m - \frac{(2z_1-1)m-(2z_2-k)}{\sqrt{2}^3\sqrt{m^2+1}}\right)^3 \\
&+ \left(\left(\frac{k^2}{4} + \frac{1}{3}\right) m + \frac{(2z_1-1)m-(2z_2-k)}{\sqrt{2}^3\sqrt{m^2+1}}\right)^3 \\
&+ \left|\frac{(2z_2-k)m+(2z_1-1)}{2\sqrt{m^2+1}}\right|^3 \\
= &\left|\frac{(2z_2-k)m+(2z_1-1)}{2\sqrt{m^2+1}}\right|^3 + 2\left(\frac{k^2}{4} + \frac{1}{3}\right)^3 m^3 \\
&+ 6\left(\frac{k^2}{4} + \frac{1}{3}\right) m \left(\frac{(2z_1-1)m-(2z_2-k)}{\sqrt{2}^3\sqrt{m^2+1}}\right)^2.
\end{aligned} \tag{3.3}$$

Thus, $\|v - x_{m,k}\|_3 > \|x_{m,k}\|_3$ is equivalent to

$$\begin{aligned}
&6\left(\frac{k^2}{4} + \frac{1}{3}\right) m \left(\frac{(2z_1-1)m-(2z_2-k)}{\sqrt{2}^3\sqrt{m^2+1}}\right)^2 + \left|\frac{(2z_2-k)m+(2z_1-1)}{2\sqrt{m^2+1}}\right|^3 \\
>&6\left(\frac{k^2}{4} + \frac{1}{3}\right) m \left(\frac{m-k}{\sqrt{2}^3\sqrt{m^2+1}}\right)^2 + \left(\frac{km+1}{2\sqrt{m^2+1}}\right)^3
\end{aligned}$$

and consequently to

$$\begin{aligned}
&f(m,k,z_1,z_2) \\
:=&6\left(\frac{k^2}{4} + \frac{1}{3}\right) m\sqrt{m^2+1}\left(((2z_1-1)m-(2z_2-k))^2 - (m-k)^2\right) \\
&+ |(2z_2-k)m+(2z_1-1)|^3 - (km+1)^3 \\
>&0.
\end{aligned}$$

With this, the following six cases can be distinguished:

a) $z_1 \geq 2$:

If $(2z_1-1)m-(2z_2-k)\leq m-k$, then $2z_2-k\geq 2m+k$ and

$$\begin{aligned} f(m,k,z_1,z_2) &\geq -6\left(\frac{k^2}{4}+\frac{1}{3}\right)m\sqrt{m^2+1}(m-k)^2 \\ &\quad +((2m+k)m+3)^3-(km+1)^3 \\ &\geq -12\left(\frac{k^2}{4}+\frac{1}{3}\right)m^4+((km+1)+2(m^2+1))^3 \\ &\quad -(km+1)^3 \\ &= -3k^2m^4-4m^4+6(km+1)^2(m^2+1) \\ &\quad +12(km+1)(m^2+1)^2+8(m^2+1)^3 \\ &\geq -3k^2m^4-4m^4+6k^2m^4+12km^5+8m^6 \\ &> 0. \end{aligned} \tag{3.4}$$

If $(2z_2-k)m+(2z_1-1)\leq km+1$, then $2z_2-k\leq k-\frac{2}{m}<k$ holds, implying $z_2\leq k-1$ and $2z_2-k\leq k-2$, which shows

$$\begin{aligned} f(m,k,z_1,z_2) &\geq 6\left(\frac{k^2}{4}+\frac{1}{3}\right)m\sqrt{m^2+1}\left((3m-k+2)^2-(m-k)^2\right) \\ &\quad -(km+1)^3 \\ &\geq 6\frac{k^2}{4}m^2\left(((m-k)+2(m+1))^2-(m-k)^2\right) \\ &\quad -(km+1)^3 \\ &= 6k^2m^2((m-k)(m+1)+(m+1)^2)-(km+1)^3 \\ &\geq 12k^2m^4+12k^2m^3+3k^2m^2-7k^3m^3-3km-1 \\ &\geq 5k^2m^4+12k^2m^3+8km \\ &> 0. \end{aligned} \tag{3.5}$$

If $(2z_1-1)m-(2z_2-k)>m-k$ and $(2z_2-k)m+(2z_1-1)>km+1$, then it follows directly from the definition of f that $f(m,k,z_1,z_2)>0$. Thus it holds for every $z_1\geq 2$ that $f(m,k,z_1,z_2)>0$ and this shows $\|v-x_{m,k}\|_3>\|x_{m,k}\|_3$.

b) $z_1\leq -1$:

If $-(2z_1-1)m+(2z_2-k)\leq m-k$, then $2z_2-k\leq -2m-k$ and the same estimate as in (3.4) holds.

If $-(2z_2-k)m-(2z_1-1)\leq km+1$, then $-(2z_2-k)\leq k-\frac{2}{m}<k$ holds, implying $z_2\geq 1$ and $2z_2-k\geq 2-k$, which leads to the same estimate as in (3.5).

If $-(2z_1-1)m+(2z_2-k)>m-k$ and $-(2z_2-k)m-(2z_1-1)>km+1$,

then it follows directly from the definition of f that $f(m,k,z_1,z_2) > 0$.

c) $z_1 = 0$ and $z_2 \geq k$:

It holds that $2z_2 - k \geq k$ and this implies

$$\begin{aligned} f(m,k,z_1,z_2) &\geq 6\left(\frac{k^2}{4}+\frac{1}{3}\right) m\sqrt{m^2+1}\left((m+k)^2-(m-k)^2\right) \\ &\quad + (km-1)^3 - (km+1)^3 \\ &\geq 6k^3m^3 - 6k^2m^2 - 2 \\ &> 0. \end{aligned} \tag{3.6}$$

d) $z_1 = 0$ and $z_2 \leq -1$:

In this case, it is $z_2 = -a$ for some $a \in \mathbb{N}$. This yields

$$\begin{aligned} f(m,k,z_1,z_2) &= 6\left(\frac{k^2}{4}+\frac{1}{3}\right) m\sqrt{m^2+1}\left((-m+k+2a)^2-(m-k)^2\right) \\ &\quad + ((2a+k)m+1)^3 - (km+1)^3 \\ &= m^3(6ak^2+12a^2k+8a^3) \\ &\quad + m^2\sqrt{m^2+1}(-6ak^2-8a) + m^2(12ak+12a^2) \\ &\quad + m\sqrt{m^2+1}(6ak^3+8ak+6a^2k^2+8a^2) + m\cdot 6a \\ &> m^2a\left(m(6k^2+12ak+8a^2) - \sqrt{m^2+1}(6k^2+8)\right). \end{aligned} \tag{3.7}$$

Because of $m \geq k$, it is obvious that $m^2(24k(6k^2+8)+144k^2) = m^2(144k^3+192k+144k^2) \geq 36k^4+96k^2+64 = (6k^2+8)^2$, and this is equivalent to $m^2((6k^2+8)+12k)^2 \geq (m^2+1)(6k^2+8)^2$. Hence, $m(6k^2+12ak+8a^2) \geq m(6k^2+12k+8) \geq \sqrt{m^2+1}(6k^2+8)$ and $f(m,k,z_1,z_2) > 0$ follow.

e) $z_1 = 1$ and $z_2 \leq 0$:

It holds that $2z_2 - k \leq -k$, yielding the same estimate as in (3.6).

f) $z_1 = 1$ and $z_2 \geq k+1$:

In this case, it is $z_2 = k + a$ for some $a \in \mathbb{N}$. This yields the same estimate as in (3.7) and thus $f(m,k,z_1,z_2) > 0$.

3. $\|x_{m,k}\|_3 < \|z_1 b_{m,1} + z_2 b_{m,2} - x_{m,k}\|_3$ for all $m \geq k^2$ and all $(z_1,z_2) \in \{0,1\} \times \{1,\ldots,k-1\}$:

For $(z_1,z_2) \in \{0,1\} \times \{1,\ldots,k-1\}$ it holds that $(2z_1-1)m - (2z_2-k) \leq m - (2-k) < m + k < 4\left(\frac{k^2}{4}+\frac{1}{3}\right)m < \sqrt{2}^3\left(\frac{k^2}{4}+\frac{1}{3}\right)m\sqrt{m^2+1}$. Moreover, $(2z_1-1)m - (2z_2-k) \geq -m - (k-2) > -\sqrt{2}^3\left(\frac{k^2}{4}+\frac{1}{3}\right)m\sqrt{m^2+1}$

follows. These two inequalities show that $\|z_1 b_{m,1} + z_2 b_{m,2} - x_{m,k}\|_3$ can be computed as in (3.3), and that $\|z_1 b_{m,1} + z_2 b_{m,2} - x_{m,k}\|_3 > \|x_{m,k}\|_3$ is equivalent to $f(m,k,z_1,z_2) > 0$. In addition, $(2z_2 - k)m + (2z_1 - 1) < 0$ is equivalent to $z_2 < \frac{1}{2}\left(k - \frac{2z_1-1}{m}\right)$, such that the following four cases need to be distinguished to show $f(m,k,z_1,z_2) > 0$:

a) $z_1 = 1$ and $\frac{1}{2}\left(k - \frac{1}{m}\right) \leq z_2 < k$:

In this case, it follows with $m < \sqrt{m^2+1} < m+1$ that

$$\begin{aligned}
f(m,k,z_1,z_2) &= 6\left(\frac{k^2}{4} + \frac{1}{3}\right) m\sqrt{m^2+1}(4z_2^2 - 4mz_2 + 4km - 4kz_2) \\
&\quad + 8m^3 z_2^3 - k^3m^3 + 1 - 12km^3 z_2^2 + 6k^2m^3 z_2 \\
&\quad + 12m^2 z_2^2 + 6mz_2 + 3k^2m^2 - 3km \\
&\quad - 12km^2 z_2 - k^3m^3 - 3k^2m^2 - 3km - 1 \\
&\geq (6k^2+8)m^2(z_2^2 + km) - (6k^2+8)m(m+1)(m+k)z_2 \\
&\quad + 8m^3 z_2^3 + (12m^2 - 12km^3)z_2^2 \\
&\quad + (6k^2m^3 - 12km^2 + 6m)z_2 - 2k^3m^3 - 6km \\
&= 8m^3 z_2^3 + (-12km^3 + 6k^2m^2 + 20m^2)z_2^2 \\
&\quad + (-8m^3 - 6k^3m^2 - 6k^2m^2 - 20km^2 - 8m^2)z_2 \\
&\quad + (-6k^3m - 8km + 6m)z_2 + 4k^3m^3 + 8km^3 - 6km \\
&=: \varphi_1^{(m,k)}(z_2) =: \varphi_1(z_2).
\end{aligned}$$

Hence, it is enough to show that $\varphi_1^{(m,k)}(z_2) > 0$. For this consider $x \in \mathbb{R}$ with $0 < x \leq k-1$ and $m \geq k^2$ to get the estimate

$$\begin{aligned}
\varphi_1'(x) &= 24m^3x^2 + (-24km^3 + 12k^2m^2 + 40m^2)x - 8m^3 - 6k^3m^2 \\
&\quad - 6k^2m^2 - 20km^2 - 8m^2 - 6k^3m - 8km + 6m \\
&\leq (-24m^3 + 12k^2m^2 + 40m^2)x - 8m^3 - 6k^3m^2 \\
&\quad - 6k^2m^2 - 20km^2 - 8m^2 - 6k^3m - 8km + 6m \\
&\leq (-12k^2m^2 + 40m^2)x - 8m^3 - 6k^3m^2 \\
&\quad - 6k^2m^2 - 20km^2 - 8m^2 - 6k^3m - 8km + 6m \\
&\leq -12k^2m^2x + 20km^2 - 8m^3 - 6k^3m^2 \\
&\quad - 6k^2m^2 - 8m^2 - 6k^3m - 8km + 6m \\
&\leq -12k^2m^2x - 4km^2 - 8m^3 \\
&\quad - 6k^2m^2 - 8m^2 - 6k^3m - 8km + 6m \\
&\leq -12k^2m^2x - 4km^2 - 8m^3 - 6k^2m^2 - 8m^2 - 6k^3m - 10m \\
&< 0.
\end{aligned}$$

This shows that $\varphi_1^{(m,k)}$ is strictly decreasing on $(0, k-1]$ and thus

$$\begin{aligned}\varphi_1^{(m,k)}(z_2) &\geq \varphi_1^{(m,k)}(k-1)\\ &= (8(k-1)^3 - 12k(k-1)^2 - 8(k-1) + 4k^3 + 8k)m^3\\ &\quad + (6k^2(k-1)^2 + 20(k-1)^2 - 6k^3(k-1))m^2\\ &\quad + (-6k^2(k-1) - 20k(k-1) - 8(k-1))m^2\\ &\quad + (-6k^3(k-1) - 8k(k-1) + 6(k-1) - 6k)m\\ &= 12km^3 + (-12k^3 + 12k^2 - 28k + 28)m^2\\ &\quad + (-6k^4 + 6k^3 - 8k^2 + 8k - 6)m.\end{aligned}$$

Thus it is enough to show $\psi_1(m) := \psi_1^{(k)}(m) := \frac{1}{2m}\varphi_1^{(m,k)}(k-1) > 0$. Since it holds for $y \in \mathbb{R}$ with $y \geq k^2$ that

$$\begin{aligned}\psi_1'(y) &= 12ky - 6k^3 + 6k^2 - 14k + 14\\ &\geq 6k^3 + 6k^2 - 14k + 14 \geq 6k^2 + 10k + 14 > 0,\end{aligned}$$

$\psi_1^{(k)}$ is strictly increasing on $[k^2, \infty)$ and thus

$$\begin{aligned}\psi_1^{(k)}(m) &\geq \psi_1^{(k)}(k^2) = 3k^4 - 11k^3 + 10k^2 + 4k - 3\\ &= 3k^2\left(k - \frac{5}{3}\right)(k-2) + 4k - 3 \geq 4k - 3 > 0.\end{aligned}$$

b) $z_1 = 1$ and $1 \leq z_2 < \frac{1}{2}\left(k - \frac{1}{m}\right)$:

Now, f can be estimated as

$$\begin{aligned}f(m,k,z_1,z_2) &= 6\left(\frac{k^2}{4} + \frac{1}{3}\right)m\sqrt{m^2+1}(4z_2^2 - 4mz_2 + 4km - 4kz_2)\\ &\quad - 8m^3z_2^3 + k^3m^3 - 1 + 12km^3z_2^2 - 6k^2m^3z_2\\ &\quad - 12m^2z_2^2 - 6mz_2 - 3k^2m^2 + 3km\\ &\quad + 12km^2z_2 - k^3m^3 - 3k^2m^2 - 3km - 1\\ &\geq (6k^2+8)m^2(z_2^2 + km) - (6k^2+8)m(m+1)(m+k)z_2\\ &\quad - 8m^3z_2^3 + (12km^3 - 12m^2)z_2^2\\ &\quad + (-6k^2m^3 + 12km^2 - 6m)z_2 - 6k^2m^2 - 2\\ &= -8m^3z_2^3 + (12km^3 + 6k^2m^2 - 4m^2)z_2^2\\ &\quad + (-12k^2m^3 - 8m^3 - 6k^3m^2 - 6k^2m^2 + 4km^2)z_2\\ &\quad + (-8m^2 - 6k^3m - 8km - 6m)z_2\\ &\quad + 6k^3m^3 + 8km^3 - 6k^2m^2 - 2\\ &=: \varphi_2^{(m,k)}(z_2) =: \varphi_2(z_2).\end{aligned}$$

Therefore it is enough to show that $\varphi_2^{(m,k)}(z_2) > 0$. For this consider $x \in \mathbb{R}$ with $0 < x \leq \frac{k}{2}$ to get the estimate

$$\begin{aligned}
\varphi_2'(x) &= -24m^3x^2 + (24km^3 + 12k^2m^2 - 8m^2)x \\
&\quad - 12k^2m^3 - 8m^3 - 6k^3m^2 - 6k^2m^2 + 4km^2 \\
&\quad - 8m^2 - 6k^3m - 8km - 6m \\
&\leq -24m^3x^2 - 8m^2x - 8m^3 - 6k^2m^2 + 4km^2 \\
&\quad - 8m^2 - 6k^3m - 8km - 6m \\
&\leq -24m^3x^2 - 8m^2x - 8m^3 - 8km^2 - 8m^2 - 6k^3m - 8km - 6m \\
&< 0.
\end{aligned}$$

This shows that $\varphi_2^{(m,k)}$ is strictly decreasing on $\left(0, \frac{k}{2}\right]$ and thus

$$\begin{aligned}
\varphi_2^{(m,k)}(z_2) &\geq \varphi_2^{(m,k)}\left(\frac{k}{2}\right) \\
&= (-k^3 + 3k^3 - 6k^3 - 4k + 6k^3 + 8k)m^3 \\
&\quad + \left(\frac{3}{2}k^4 - k^2 - 3k^4 - 3k^3 - 4k + 2k^2 - 6k^2\right)m^2 \\
&\quad + (-3k^4 - 4k^2 - 3k)m - 2 \\
&= (2k^3 + 4k)m^3 + \left(-\frac{3}{2}k^4 - 3k^3 - 5k^2 - 4k\right)m^2 \\
&\quad + (-3k^4 - 4k^2 - 3k)m - 2.
\end{aligned}$$

With

$$\begin{aligned}
\psi_2(m) &:= \psi_2^{(k)}(m) \\
&:= (4k^3 + 8k)m^2 + (-3k^4 - 6k^3 - 10k^2 - 8k)m \\
&\quad - 6k^4 - 8k^2 - 6k
\end{aligned}$$

it holds that $\varphi_2^{(m,k)}\left(\frac{k}{2}\right) = \frac{m}{2}\psi_2^{(k)}(m) - 2$. Moreover, for every $y \in \mathbb{R}$ with $y \geq k^2$ it is

$$\begin{aligned}
\psi_2'(y) &= (8k^3 + 16k)y - 3k^4 - 6k^3 - 10k^2 - 8k \\
&\geq 8k^5 - 3k^4 + 10k^3 - 10k^2 - 8k \\
&\geq 13k^4 + 10k^2 - 8k > 0,
\end{aligned}$$

which implies that $\psi_2^{(k)}$ is strictly increasing on $[k^2, \infty)$. Thus,

$$\begin{aligned}
\psi_2^{(k)}(m) &\geq \psi_2^{(k)}(k^2) = 4k^7 - 3k^6 + 2k^5 - 16k^4 - 8k^3 - 8k^2 - 6k \\
&\geq 5k^6 - 12k^4 - 8k^3 - 8k^2 - 6k \geq 8k^4 - 8k^3 - 8k^2 - 6k
\end{aligned}$$

$$\geq 8k^3 - 8k^2 - 6k \geq 8k^2 - 6k \geq 10k$$

holds, yielding $\varphi_2^{(m,k)}(z_2) \geq \varphi_2^{(m,k)}\left(\frac{k}{2}\right) = \frac{m}{2}\psi_2^{(k)}(m) - 2 \geq 5k^3 - 2 > 0$.

c) $z_1 = 0$ and $1 \leq z_2 < \frac{1}{2}\left(k + \frac{1}{m}\right)$:

In this case, it is

$$\begin{aligned} f(m,k,z_1,z_2) &= 6\left(\frac{k^2}{4} + \frac{1}{3}\right) m\sqrt{m^2+1}(4z_2 + 4m - 4k)z_2 \\ &\quad - 8m^3z_2^3 + k^3m^3 + 1 + 12km^3z_2^2 - 6k^2m^3z_2 \\ &\quad + 12m^2z_2^2 - 6mz_2 + 3k^2m^2 + 3km \\ &\quad - 12km^2z_2 - k^3m^3 - 3k^2m^2 - 3km - 1 \\ &\geq (6k^2+8)m^2(z_2+m)z_2 - (6k^2+8)m(m+1)kz_2 \\ &\quad - 8m^3z_2^3 + (12m^2 + 12km^3)z_2^2 \\ &\quad + (-6k^2m^3 - 12km^2 - 6m)z_2 \\ &= -8m^3z_2^3 + (12km^3 + 6k^2m^2 + 20m^2)z_2^2 \\ &\quad + (8m^3 - 6k^3m^2 - 20km^2 - 6k^3m - 8km - 6m)z_2. \end{aligned}$$

Hence, it is enough to show that

$$\begin{aligned} \varphi_3(z_2) := \varphi_3^{(m,k)}(z_2) : &= -8m^3z_2^2 + (12km^3 + 6k^2m^2 + 20m^2)z_2 + 8m^3 \\ &\quad - 6k^3m^2 - 20km^2 - 6k^3m - 8km - 6m \\ &> 0. \end{aligned}$$

For this consider $x \in \mathbb{R}$ with $0 < x \leq \frac{k+1}{2}$ to get the estimate

$$\begin{aligned} \varphi_3'(x) &= -16m^3x + 12km^3 + 6k^2m^2 + 20m^2 \\ &\geq 4km^3 - 8m^3 + 6k^2m^2 + 20m^2 \geq 6k^2m^2 + 20m^2 > 0. \end{aligned}$$

This shows that $\varphi_3^{(m,k)}$ is strictly increasing on $\left(0, \frac{k+1}{2}\right]$ and thus

$$\begin{aligned} \varphi_3^{(m,k)}(z_2) &\geq \varphi_3^{(m,k)}(1) \\ &= 12km^3 + (-6k^3 + 6k^2 - 20k + 20)m^2 + (-6k^3 - 8k - 6)m \\ &\geq \varphi_1^{(m,k)}(k-1) > 0. \end{aligned}$$

d) $z_1 = 0$ and $\frac{1}{2}\left(k + \frac{1}{m}\right) \leq z_2 < k$:

Now, f can be estimated as

$$\begin{aligned} f(m,k,z_1,z_2) &= 6\left(\frac{k^2}{4} + \frac{1}{3}\right) m\sqrt{m^2+1}(4z_2 + 4m - 4k)z_2 \\ &\quad + 8m^3z_2^3 - k^3m^3 - 1 - 12km^3z_2^2 + 6k^2m^3z_2 \end{aligned}$$

$$
\begin{aligned}
&\quad - 12m^2z_2^2 + 6mz_2 - 3k^2m^2 - 3km \\
&\quad + 12km^2z_2 - k^3m^3 - 3k^2m^2 - 3km - 1 \\
&\geq (6k^2+8)m^2(z_2+m)z_2 - (6k^2+8)m(m+1)kz_2 \\
&\quad + 8m^3z_2^3 + (-12m^2 - 12km^3)z_2^2 \\
&\quad + (6k^2m^3 + 12km^2 + 6m)z_2 \\
&\quad - 2k^3m^3 - 6k^2m^2 - 6km - 2 \\
&= 8m^3z_2^3 + (-12km^3 + 6k^2m^2 - 4m^2)z_2^2 \\
&\quad + (12k^2m^3 + 8m^3 - 6k^3m^2 + 4km^2 - 6k^3m)z_2 \\
&\quad + (-8km + 6m)z_2 - 2k^3m^3 - 6k^2m^2 - 6km - 2 \\
&=: \varphi_4^{(m,k)}(z_2) =: \varphi_4(z_2).
\end{aligned}
$$

Therefore it is enough to show that $\varphi_4^{(m,k)}(z_2) > 0$. For this consider $x \in \mathbb{R}$ with $\frac{k}{2} \leq x \leq k-1$ and $m \geq k^2 \geq 4$ to get the estimate

$$
\begin{aligned}
\varphi_4'(x) &= 24m^3x^2 + (-24km^3 + 12k^2m^2 - 8m^2)x + 12k^2m^3 + 8m^3 \\
&\quad - 6k^3m^2 + 4km^2 - 6k^3m - 8km + 6m \\
&\geq (-12km^3 + 12k^2m^2 - 8m^2)x + 12k^2m^3 + 8m^3 \\
&\quad - 6k^3m^2 + 4km^2 - 6k^3m - 8km + 6m \\
&\geq (-12km^3 + 40m^2)x + 12k^2m^3 + 8m^3 \\
&\quad - 6k^3m^2 + 4km^2 - 6k^3m - 8km + 6m \\
&\geq 40m^2x + 12km^3 + 8m^3 - 6k^3m^2 + 4km^2 - 6k^3m - 8km + 6m \\
&\geq 40m^2x + 6k^3m^2 + 8m^3 + 4km^2 - 6k^3m - 8km + 6m \\
&\geq 40m^2x + 18k^3m + 8m^3 + 4km^2 - 8km + 6m \\
&\geq 40m^2x + 18k^3m + 8m^3 + 8km + 6m \\
&> 0.
\end{aligned}
$$

This shows that $\varphi_4^{(m,k)}$ is strictly increasing on $\left[\frac{k}{2}, k-1\right]$ and thus

$$
\begin{aligned}
\varphi_4^{(m,k)}(z_2) &\geq \varphi_4^{(m,k)}\left(\frac{k}{2}\right) \\
&= (k^3 - 3k^3 + 6k^3 + 4k - 2k^3)m^3 \\
&\quad + \left(\frac{3}{2}k^4 - k^2 - 3k^4 + 2k^2 - 6k^2\right)m^2 \\
&\quad + (-3k^4 - 4k^2 + 3k - 6k)m - 2 \\
&= (2k^3 + 4k)m^3 + \left(-\frac{3}{2}k^4 - 5k^2\right)m^2 \\
&\quad + (-3k^4 - 4k^2 - 3k)m - 2
\end{aligned}
$$

$$\geq \varphi_2^{(m,k)}\left(\frac{k}{2}\right) > 0.$$

All these different cases together show that $\|x_{m,k}\|_3 < \|x_{m,k} - v\|_3$ holds for all $v \in \Lambda_m \setminus \{0, b_{m,1} + kb_{m,2}\}$ and all $m \geq k^2$. Combined with $\|x_{m,k}\|_3 = \|b_{m,1} + kb_{m,2} - x_{m,k}\|_3$, this implies that $b_{m,1} + kb_{m,2}$ is Voronoi-relevant in Λ_m with respect to $\|\cdot\|_3$ if $m \geq k^2$. □

Corollary 3.6 *1. For every $m \in \mathbb{N}, m \geq 2$ it holds that Λ_m has at least $2\lfloor\sqrt{m}\rfloor$ Voronoi-relevant vectors with respect to $\|\cdot\|_3$.*

2. For every $k \in \mathbb{N}, k \geq 3$ it holds that $\Lambda_{\lceil\frac{k}{2}\rceil^2}$ has at least k Voronoi-relevant vectors with respect to $\|\cdot\|_3$.

Proof. Since the second statement is a direct consequence of the first one, it is sufficient to show the first part of this corollary. For this, let $m \in \mathbb{N}$ with $m \geq 2$. For all $k \in \mathbb{N}$ with $2 \leq k \leq \lfloor\sqrt{m}\rfloor$ it holds by Theorem 3.5 that $b_{m,1} + kb_{m,2}$ is Voronoi-relevant in Λ_m with respect to $\|\cdot\|_3$. Then $-b_{m,1} - kb_{m,2}$ is also Voronoi-relevant for all $2 \leq k \leq \lfloor\sqrt{m}\rfloor$. In addition, Proposition 3.4 gives that $\pm(b_{m,1} + mb_{m,2})$ are Voronoi-relevant vectors, and the first statement follows. □

3.2 Consequences and comparisons

In the following, an upper bound for the number of (generalized) Voronoi-relevant vectors in an arbitrary lattice with respect to an arbitrary norm is shown. This bound depends on the lattice dimension as well as the ratio of the covering radius to the length of a shortest non-zero lattice vector.

Proposition 3.7 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Then Λ has at most $\left(1 + 4\frac{\mu(\Lambda,\|\cdot\|)}{\lambda_1(\Lambda,\|\cdot\|)}\right)^n$ generalized Voronoi-relevant vectors with respect to $\|\cdot\|$.*

Proof. From Lemma 2.17 it follows that

$$\begin{aligned}\mathcal{R}(\Lambda, \|\cdot\|) &:= \{v \in \Lambda \mid v \text{ generalized Voronoi-relevant w.r.t. } \|\cdot\|\} \\ &\subseteq \overline{\mathcal{B}}_{\|\cdot\|,2\mu(\Lambda,\|\cdot\|)}(0).\end{aligned}$$

Since for every two lattice vectors $v, w \in \Lambda$ with $v \neq w$ it holds that $\|v - w\| \geq \lambda_1(\Lambda, \|\cdot\|)$, it follows that $\mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(v) \cap \mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(w) = \emptyset$. Moreover, for every $v \in \mathcal{R}(\Lambda, \|\cdot\|)$ and every $x \in \mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(v)$ it is $\|x\| \leq \|x - v\| + \|v\| < \frac{\lambda_1(\Lambda,\|\cdot\|)}{2} + 2\mu(\Lambda, \|\cdot\|)$. Thus

$$\dot{\bigcup_{v\in\mathcal{R}(\Lambda,\|\cdot\|)}} \mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(v) \subseteq \mathcal{B}_{\|\cdot\|,2\mu(\Lambda,\|\cdot\|)+\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(0)$$

holds, which implies

$$\begin{aligned}|\mathcal{R}(\Lambda,\|\cdot\|)|\operatorname{vol}_n\left(\mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(0)\right) &= \sum_{v\in\mathcal{R}(\Lambda,\|\cdot\|)}\operatorname{vol}_n\left(\mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(v)\right)\\ &= \operatorname{vol}_n\left(\dot{\bigcup_{v\in\mathcal{R}(\Lambda,\|\cdot\|)}}\mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(v)\right)\\ &\leq \operatorname{vol}_n\left(\mathcal{B}_{\|\cdot\|,2\mu(\Lambda,\|\cdot\|)+\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(0)\right).\end{aligned}$$

Since $2\mu(\Lambda,\|\cdot\|)+\frac{\lambda_1(\Lambda,\|\cdot\|)}{2} = \left(1+4\frac{\mu(\Lambda,\|\cdot\|)}{\lambda_1(\Lambda,\|\cdot\|)}\right)\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}$, it is $\mathcal{B}_{\|\cdot\|,2\mu(\Lambda,\|\cdot\|)+\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(0) = \left(1+4\frac{\mu(\Lambda,\|\cdot\|)}{\lambda_1(\Lambda,\|\cdot\|)}\right)\mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(0)$. For any positive constant $r\in\mathbb{R}_{>0}$ and any measurable $M\subseteq\mathbb{R}^n$, integration by substitution for multiple variables yields

$$\begin{aligned}\operatorname{vol}_n(rM) &= \int_{\mathbb{R}^n}\chi_{rM}(x)\,dx = \int_{\mathbb{R}^n}\chi_M\left(\frac{x}{r}\right)\,dx = r^n\int_{\mathbb{R}^n}\chi_M\left(\frac{x}{r}\right)\frac{1}{r^n}\,dx\\ &= r^n\int_{\mathbb{R}^n}\chi_M(y)\,dy = r^n\operatorname{vol}_n(M).\end{aligned}$$

Thus it follows that

$$|\mathcal{R}(\Lambda,\|\cdot\|)|\operatorname{vol}_n\left(\mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(0)\right) \leq \left(1+4\frac{\mu(\Lambda,\|\cdot\|)}{\lambda_1(\Lambda,\|\cdot\|)}\right)^n\operatorname{vol}_n\left(\mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(0)\right),$$

which implies $|\mathcal{R}(\Lambda,\|\cdot\|)| \leq \left(1+4\frac{\mu(\Lambda,\|\cdot\|)}{\lambda_1(\Lambda,\|\cdot\|)}\right)^n$. □

Corollary 3.8 *Let $\|\cdot\|:\mathbb{R}^n\to\mathbb{R}_{\geq 0}$ be a norm and let $\Lambda\subseteq\mathbb{R}^n$ be a lattice. Then Λ has at most $\left(6\frac{\mu(\Lambda,\|\cdot\|)}{\lambda_1(\Lambda,\|\cdot\|)}\right)^n$ generalized Voronoi-relevant vectors with respect to $\|\cdot\|$.*

Proof. Assume for contradiction that $\mu(\Lambda,\|\cdot\|) < \frac{\lambda_1(\Lambda,\|\cdot\|)}{2}$. Then exists some $x\in\operatorname{span}(\Lambda)$ such that

$$x\in\mathcal{B}_{\|\cdot\|,\frac{\lambda_1(\Lambda,\|\cdot\|)}{2}}(0)\setminus\overline{\mathcal{B}}_{\|\cdot\|,\mu(\Lambda,\|\cdot\|)}(0).$$

Due to the definition of the covering radius, there exists some $v\in\Lambda\setminus\{0\}$ with $\|x-v\| < \|x\| < \frac{\lambda_1(\Lambda,\|\cdot\|)}{2}$. This gives the contradiction

$$\lambda_1(\Lambda,\|\cdot\|) \leq \|v\| \leq \|v-x\|+\|x\| < \lambda_1(\Lambda,\|\cdot\|).$$

Hence, $\mu(\Lambda,\|\cdot\|) \geq \frac{\lambda_1(\Lambda,\|\cdot\|)}{2}$ must hold, which implies $1\leq 2\frac{\mu(\Lambda,\|\cdot\|)}{\lambda_1(\Lambda,\|\cdot\|)}$. Plugging this into Proposition 3.7 yields the desired upper bound. □

As seen in the last section, there is no upper bound for the number of Voronoi-relevant vectors with respect to the 3-norm that only depends on the lattice dimension. Nevertheless, at least the upper bounds from Proposition 3.7 and Corollary 3.8 hold. Unfortunately, this does not help for the algorithm by Micciancio and Voulgaris [13] since they rely on the fact that the number of Voronoi-relevant vectors with respect to the Euclidean norm is in $2^{O(n)}$, which is not true for the 3-norm. Hence, this algorithm cannot be easily extended to general p-norms, not even when only strictly convex p-norms – i.e., for $p \in (1, \infty)$ – are considered.

The rest of this section will compare the upper bound in Proposition 3.7 with the number of (generalized) Voronoi-relevant vectors in the lattices that have been constructed to show that no upper bound for the number of (generalized) Voronoi-relevant vectors can only depend on the lattice dimension. First, the two-dimensional lattices of Theorem 2.28 will be considered which do not have a constant number of generalized Voronoi-relevant vectors with respect to a non-strictly convex norm. Secondly, the three-dimensional lattices of Corollary 3.6 will be investigated which do not have a constant number of Voronoi-relevant vectors with respect to a strictly convex norm.

For $m \in \mathbb{N}$, let $\Lambda_m^{(2)} := \mathcal{L}(b_{m,1}^{(2)}, b_{m,2}^{(2)})$, where $b_{m,1}^{(2)} := (1,1)^T$ and $b_{m,2}^{(2)} := (0,m)^T$. Since $\|b_{m,1}^{(2)}\|_1 = 2$, it follows that $\lambda_1(\Lambda_m^{(2)}, \|\cdot\|_1) \leq 2$. The following calculation shows that

$$\lambda_1(\Lambda_m^{(2)}, \|\cdot\|_1) = \begin{cases} 2, \text{ if } m \geq 2 \\ 1, \text{ if } m = 1 \end{cases} . \tag{3.8}$$

Consider $(z_1, z_2) \in \mathbb{Z}^2 \backslash \{(0,0)\}$ with $2 > \|z_1 b_{m,1}^{(2)} + z_2 b_{m,2}^{(2)}\|_1 = |z_1| + |z_1 + m z_2|$. Then it is clear that $|z_1| \leq 1$. If $|z_1| = 1$ would hold, $z_1 + m z_2 = 0$ would follow, leading to $1 = m|z_2|$ and thus to $m = 1$ and $z_2 = -z_1$. For $z_1 = 0$ it follows from $z_2 \neq 0$ that $1 = m|z_2|$, which implies $m = 1$ and $|z_2| = 1$. Both cases together show (3.8). The proof of Theorem 2.28 shows in particular that for every $v \in \Lambda_m^{(2)}$ it holds $\|\frac{1}{2} b_{m,2}^{(2)} - v\|_1 \geq \frac{m}{2}$. This yields that $\mu(\Lambda_m^{(2)}, \|\cdot\|_1) \geq \frac{m}{2}$. An easy upper bound for the covering radius follows from the fact that for every $r \in \mathbb{R}$ there exists some $z \in \mathbb{Z}$ with $|r - z| \leq \frac{1}{2}$: For every $y \in \operatorname{span}(\Lambda_m^{(2)})$ there exists some $v \in \Lambda_m^{(2)}$ such that $\|y - v\|_1 \leq \frac{1}{2}\|b_{m,1}^{(2)}\|_1 + \frac{1}{2}\|b_{m,2}^{(2)}\| = \frac{m}{2} + 1$. Hence, $\mu(\Lambda_m^{(2)}, \|\cdot\|_1) \in \Theta(m)$ and the upper bound in Proposition 3.7 or Corollary 3.8, respectively, is in $\Theta(m^2)$, which is asymptotically larger than the number of generalized Voronoi-relevant vectors in Theorem 2.28.

An even bigger asymptotical gap is obtained from the lattices of Corollary 3.6. For $m \in \mathbb{N}$ with $m \geq 2$, let $\Lambda_m^{(3)} := \mathcal{L}(b_{m,1}^{(3)}, b_{m,2}^{(3)}, b_{m,3}^{(3)})$ with

$$b_{m,1}^{(3)} := \begin{pmatrix} \frac{m}{\sqrt{2}\sqrt{m^2+1}} \\ \frac{1}{\sqrt{m^2+1}} \\ -\frac{m}{\sqrt{2}\sqrt{m^2+1}} \end{pmatrix}, b_{m,2}^{(3)} := \begin{pmatrix} -\frac{1}{\sqrt{2}\sqrt{m^2+1}} \\ \frac{m}{\sqrt{m^2+1}} \\ \frac{1}{\sqrt{2}\sqrt{m^2+1}} \end{pmatrix}, b_{m,3}^{(3)} := \begin{pmatrix} 5\,m^5 \\ 0 \\ 5\,m^5 \end{pmatrix}.$$

It was shown in Proposition 3.3 that $\lambda_1(\Lambda_m^{(3)}, \|\cdot\|_3) = \|b_{m,1}^{(3)}\|_3 = \sqrt[3]{\frac{m^3+\sqrt{2}}{\sqrt{2}\sqrt{m^2+1}^3}}$. From $(\sqrt{2}-1)m^3 \geq (\sqrt{2}-1)8 \geq \sqrt{2}$ it follows that $\sqrt{2}\sqrt{m^2+1}^3 \geq \sqrt{2}m^3 \geq m^3+\sqrt{2}$, which shows $\lambda_1(\Lambda_m^{(3)}, \|\cdot\|_3) \leq 1$. A lower bound for the first successive minimum can be derived as follows: It holds that

$$(8-\sqrt{2})m^3 + 7\sqrt{2} > (8-\sqrt{2})m^3 \geq (8-\sqrt{2})2m^2 \geq 6\sqrt{2}m^2 \geq 3\sqrt{2}m(m+1),$$

which implies $8(m^3+\sqrt{2}) \geq \sqrt{2}(m+1)^3 \geq \sqrt{2}\sqrt{m^2+1}^3$ and $\lambda_1(\Lambda_m^{(3)}, \|\cdot\|_3) \geq \frac{1}{2}$. Moreover, the proof of Proposition 3.4 shows that for every $v \in \Lambda_m^{(3)}$ it holds that $\|x-v\|_3 \geq \|x\|_3 = \sqrt[3]{2m^{15} + \frac{1}{8}\sqrt{m^2+1}^3}$, where $x := (m^5, \frac{\sqrt{m^2+1}}{2}, m^5)^T$. This shows that $\mu(\Lambda_m^{(3)}, \|\cdot\|_3) \geq \|x\|_3 \geq \sqrt[3]{2}m^5$. As above for $\Lambda_m^{(2)}$, one can deduce that for every $y \in \operatorname{span}(\Lambda_m^{(3)})$ there exists some $v \in \Lambda_m^{(3)}$ such that $\|y-v\|_3 \leq \frac{1}{2}\|b_{m,1}^{(3)}\|_3 + \frac{1}{2}\|b_{m,2}^{(3)}\|_3 + \frac{1}{2}\|b_{m,3}^{(3)}\|_3 \leq \frac{3}{2}\|b_{m,3}^{(3)}\|_3 = \frac{3}{2}\sqrt[3]{250}m^5$, where the last inequality follows from Proposition 3.3. Hence, $\mu(\Lambda_m^{(3)}, \|\cdot\|_3) \in \Theta(m^5)$ and the upper bound in Proposition 3.7 or Corollary 3.8, respectively, is in $\Theta(m^{15})$, whereas the lower bound from Corollary 3.6 is only in $\Theta(\sqrt{m})$.

In both families of lattices discussed above, the number of (generalized) Voronoi-relevant vectors grows with the ratio of the covering radius to the first successive minimum, but there might be still room for a better upper bound than the one given in Proposition 3.7.

4 General shape of bisectors, Voronoi cells and their facets

As seen in Section 2.2, it is not immediately clear which lattice vectors completely determine the Voronoi cell of a given lattice when arbitrary norms are considered. This general question will be discussed in Section 4.3. Moreover, such an n-dimensional Voronoi cell is bounded by its $(n-1)$-dimensional facets, and for understanding the complexity of a Voronoi cell it is important to know the number of these facets. In Section 4.4, it will be examined how many $(n-1)$-dimensional facets an n-dimensional Voronoi cell has, and if these facets are connected or not. To comprehend how Voronoi cells and their facets look like, it is inevitable to investigate bisectors and their intersections, since these facets are subsets of bisectors. This is done in Section 4.2. In particular, a proof idea – relying on some conjecture – for the following fundamental (and hopefully true) statement is given: The bisector of a and b intersected with the bisector of b and c is homeomorphic to $\mathbb{R}^{n-2}$ as long as $a, b, c \in \mathbb{R}^n$ are non-collinear and a sufficiently nice norm is used. This statement is already known for the case $n \leq 3$ [10], and is further motivated by Horváth's result that bisectors are homeomorphic to $\mathbb{R}^{n-1}$ under a strictly convex norm [6]. The next section gives properties and definitions that are needed for the above mentioned sufficiently nice norms.

4.1 Norms

In this section, it will be shown that every symmetric convex body in $\mathbb{R}^n$ defines a norm, where its closed unit ball is the given body itself, and that the closed unit ball of a given norm in $\mathbb{R}^n$ is a symmetric convex body such that its corresponding norm coincides with the given norm. Based on this, smooth norms will be defined and alternative definitions for strict convexity will be given. An intermediate result will be that all norms in $\mathbb{R}^n$ are continuous with respect to the Euclidean norm.

Definition 4.1 *$K \subseteq \mathbb{R}^n$ is a* convex body with center point $c \in K$ *if K is compact and convex, and c lies in the interior of K.*

K is symmetric (with respect to c) *if for every $x \in K$ it holds that $2c - x \in K$.*

In the subsequent sections, convex bodies will be translated and scaled.

Definition 4.2 *Let $K \subseteq \mathbb{R}^n$ be a convex body with center point $c \in K$. $\tilde{K} \subseteq \mathbb{R}^n$ is called a* uniformly scaled copy *of K, if $r \in \mathbb{R}_{>0}$ with $\tilde{K} = r(K - c) + c$ exists.*

$\tilde{K} \subseteq \mathbb{R}^n$ *is called a* translated copy *of* K*, if* $t \in \mathbb{R}^n$ *with* $\tilde{K} = K + t$ *exists.*

Every convex body defines a convex distance function, which is a metric if and only if the body is symmetric. This is shown in Lemmata 4.4 and 4.5. Furthermore – as stated in Proposition 4.6 – a symmetric convex body defines a norm such that its closed unit ball coincides with the convex body.

Definition 4.3 *Let* $K \subseteq \mathbb{R}^n$ *be a convex body with center point* $c \in K$*. For* $p, q \in \mathbb{R}^n$ *with* $p \neq q$*, let* $x_{p,q} \in \mathbb{R}^n$ *denote the unique intersection point of the boundary of* $K - c + p$ *and the ray from* p *through* q*, i.e.,* $x_{p,q} \in \{sq + (1-s)p \mid s \in \mathbb{R}_{\geq 0}\}$*. The* convex distance function *based on* K *and* c *is defined as*

$$d_{K,c} : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}_{\geq 0},$$
$$(p,q) \longmapsto \begin{cases} \frac{\|q-p\|_2}{\|x_{p,q}-p\|_2} & , \text{ if } p \neq q \\ 0 & , \text{ if } p = q \end{cases}.$$

Lemma 4.4 *Let* $K \subseteq \mathbb{R}^n$ *be a convex body with center point* $c \in K$*. The convex distance function* $d_{K,c}$ *satisfies the following properties:*

1. *For every* $p, q \in \mathbb{R}^n$ *it is* $d_{K,c}(p,q) \geq 0$*, and* $d_{K,c}(p,q) = 0$ *if and only if* $p = q$*.*
2. *For every* $p \in \mathbb{R}^n$ *it holds that*
   - p *lies the interior of* K *if and only if* $d_{K,c}(c,p) < 1$*,*
   - p *lies on the boundary of* K *if and only if* $d_{K,c}(c,p) = 1$*,*
   - p *is not in* K *if and only if* $d_{K,c}(c,p) > 1$*.*
3. *For every* $p, q, r \in \mathbb{R}^n$ *it is* $d_{K,c}(p-r, q-r) = d_{K,c}(p,q)$*.*
4. *For every* $p \in \mathbb{R}^n$ *and every* $s \in \mathbb{R}_{>0}$ *it holds that* $d_{K,c}(0, sp) = s d_{K,c}(0,p)$*.*
5. *For every* $p, q, r \in \mathbb{R}^n$ *it is* $d_{K,c}(p,q) \leq d_{K,c}(p,r) + d_{K,c}(r,q)$*.*

Proof. The first four assertions follow directly from Definition 4.3. For this, one only needs to consider $x_{p,q}$ in the different cases: First, it holds for $p \neq q$ that $x_{p,q} \neq p$ such that $d_{K,c}(p,q) > 0$ follows. Moreover, $x_{p-r,q-r} = x_{p,q} - r$ and $x_{0,sp} = x_{0,p}$.

For assertion five, note that for every $b \in \mathbb{R}^n, b \neq 0$ it holds that

$$d_{K,c}\left(0, \frac{b}{d_{K,c}(0,b)}\right) = \frac{1}{d_{K,c}(0,b)} d_{K,c}(0,b) = 1,$$

and thus $\frac{b}{d_{K,c}(0,b)}$ lies on the boundary of $K - c$. Hence, the convexity of K yields for $a, b \in \mathbb{R}^n \setminus \{0\}$ with $\mu := \frac{d_{K,c}(0,a)}{d_{K,c}(0,a) + d_{K,c}(0,b)} \in (0,1)$ that $\mu \frac{a}{d_{K,c}(0,a)} + (1-\mu)\frac{b}{d_{K,c}(0,b)} \in$

$K - c$, which shows

$$\begin{aligned} 1 &\geq d_{K,c}\left(0, \mu\frac{a}{d_{K,c}(0,a)} + (1-\mu)\frac{b}{d_{K,c}(0,b)}\right) \\ &= d_{K,c}\left(0, \frac{a}{d_{K,c}(0,a)+d_{K,c}(0,b)} + \frac{b}{d_{K,c}(0,a)+d_{K,c}(0,b)}\right) \\ &= \frac{1}{d_{K,c}(0,a)+d_{K,c}(0,b)} d_{K,c}(0,a+b). \end{aligned}$$

Since assertion five is trivial as soon as some of the points p, q, r coincide, one can assume that p, q, r are pairwise distinct. Using the above inequality for the case $a = r - p$ and $b = q - r$ leads to

$$\begin{aligned} d_{K,c}(p,q) &= d_{K,c}(0, (r-p)+(q-r)) \\ &\leq d_{K,c}(0, r-p) + d_{K,c}(0, q-r) = d_{K,c}(p,r) + d_{K,c}(r,q). \end{aligned}$$

□

Lemma 4.5 *Let $K \subseteq \mathbb{R}^n$ be a convex body with center point $c \in K$. Then it holds that K is symmetric if and only if for every $p, q \in \mathbb{R}^n$ it is $d_{K,c}(p,q) = d_{K,c}(q,p)$.*

Proof. First, assume that K is symmetric. For $p, q \in \mathbb{R}^n$ with $p \neq q$, this property implies that $2p - x_{p,q} \in K - c + p$. Thus, $q + p - x_{p,q} \in K - c + q$ lies on the ray from q through p, which leads to

$$\|x_{q,p} - q\|_2 \geq \|(q + p - x_{p,q}) - q\|_2 = \|x_{p,q} - p\|_2$$

and $d_{K,c}(q,p) \leq d_{K,c}(p,q)$. By exchanging the roles of p and q, the desired equality follows.

Secondly, assume that $d_{K,c}(p,q) = d_{K,c}(q,p)$ holds for every $p, q \in \mathbb{R}^n$, and let $x \in K$. Then $1 \geq d_{K,c}(c,x) = d_{K,c}(x,c) = d_{K,c}(c, 2c - x)$ implies $2c - x \in K$. □

Proposition 4.6 *Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body with center point $c \in K$. Then*

$$\begin{aligned} \|\cdot\|_{K,c} : \mathbb{R}^n &\longrightarrow \mathbb{R}_{\geq 0}, \\ x &\longmapsto d_{K,c}(0,x) \end{aligned}$$

is a norm with unit ball $\overline{\mathcal{B}}_{\|\cdot\|_{K,c},1}(0) = K - c$.

Proof. For $s \in \mathbb{R}_{<0}$ and $x \in \mathbb{R}^n$ it is

$$d_{K,c}(0, sx) = d_{K,c}(-sx, 0) = d_{K,c}(0, -sx) = -s d_{K,c}(0,x)$$

by Lemmata 4.4 and 4.5. The same lemmata yield the remaining norm properties as well as $\overline{\mathcal{B}}_{\|\cdot\|_{K,c},1}(0) = K - c$. □

Moreover, the unit ball of every norm in $\mathbb{R}^n$ is a symmetric convex body and the norm defined by this body is the given norm. To prove this, it will be shown beforehand that every norm in $\mathbb{R}^n$ is a continuous function with respect to the Euclidean norm. This result will be very useful throughout this chapter.

Proposition 4.7 *Every norm $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ is continuous with respect to the Euclidean norm.*

Proof. Let $x = (x_1, \dots, x_n)^T \in \mathbb{R}^n$ and $\varepsilon \in \mathbb{R}_{>0}$. Denote by

$$\mathcal{R}(x) := \left\{(y_1, \dots, y_n)^T \in \mathbb{R}^n \mid \forall i \in \{1, \dots, n\} : y_i \in [x_i - 1, x_i + 1]\right\}$$

the n-dimensional cube with side length two and x in its center. Then it holds that $\mathcal{B}_{\|\cdot\|_2,1}(x) \subseteq \mathcal{R}(x)$, because for every $(y_1, \dots, y_n)^T \in \mathbb{R}^n \setminus \mathcal{R}(x)$ there is some $i \in \{1, \dots, n\}$ such that $y_i \notin [x_i - 1, x_i + 1]$, which implies $\|y - x\|_2 \geq |y_i - x_i| > 1$. In addition, it follows inductively that every $y \in \mathcal{R}(x)$ can be written as $y = \sum_{u \in \{-1,1\}^n} \mu_u (x + u)$ with $\mu_u \in [0, 1]$ for every $u \in \{-1, 1\}^n$ and $\sum_{u \in \{-1,1\}^n} \mu_u = 1$. In fact, the definition of $\mathcal{R}(x)$ yields that for every $y \in \mathcal{R}(x)$ and every $i \in \{1, \dots, n\}$ there is $\tau_i \in [0, 1]$ such that $y_i = \tau_i(x_i - 1) + (1 - \tau_i)(x_i + 1)$, which directly gives the induction basis for $n = 1$. If $\tilde{\mu}_{\tilde{u}} \in [0, 1]$ for $\tilde{u} \in \{-1, 1\}^{n-1}$ with $\sum_{\tilde{u} \in \{-1,1\}^{n-1}} \tilde{\mu}_{\tilde{u}} = 1$ and $(y_1, \dots, y_{n-1})^T = \sum_{\tilde{u} \in \{-1,1\}^{n-1}} \tilde{\mu}_{\tilde{u}} \left((x_1, \dots, x_{n-1})^T + \tilde{u}\right)$ are already found,

$$\mu_{(u_1,\dots,u_n)^T} := \begin{cases} \tau_n \tilde{\mu}_{(u_1,\dots,u_{n-1})^T} & , \text{if } u_n = -1, \\ (1 - \tau_n)\tilde{\mu}_{(u_1,\dots,u_{n-1})^T} & , \text{if } u_n = 1 \end{cases}$$

gives the desired equalities. Hence, for every $y \in \mathcal{R}(x)$ it holds that

$$\|y\| \leq \sum_{u \in \{-1,1\}^n} \mu_u \|x + u\| \leq \max\{\|x + u\| \mid u \in \{-1, 1\}^n\} =: M_x.$$

Define $\delta := \frac{1}{2} \frac{\varepsilon}{M_x - \|x\| + \varepsilon} \in \left(0, \frac{1}{2}\right]$, and let $y \in \mathcal{B}_{\|\cdot\|_2,\delta}(x)$. It is left to show that $|\|x\| - \|y\|| < \varepsilon$. Thus assume for contradiction that $|\|x\| - \|y\|| \geq \varepsilon$. With this, two cases can be distinguished.

1. $\|y\| \geq \|x\| + \varepsilon$:

   For $z := \frac{1}{\delta} y - \left(\frac{1}{\delta} - 1\right) x$ it holds that $\|z - x\|_2 = \frac{1}{\delta}\|y - x\|_2 < 1$, leading to $z \in \mathcal{B}_{\|\cdot\|_2,1}(x) \subseteq \mathcal{R}(x)$. The reverse triangle inequality and the definition of δ yield the contradiction

   $$M_x \geq \|z\| \geq \frac{1}{\delta}\|y\| - \left(\frac{1}{\delta} - 1\right)\|x\| \geq \|x\| + \frac{\varepsilon}{\delta} \geq \|x\| + \left(\frac{1}{\delta} - 1\right)\varepsilon > M_x.$$

2. $\|y\| \leq \|x\| - \varepsilon$:

Consider $\tilde{z} := \frac{1}{\delta}x - \left(\frac{1}{\delta} - 1\right) y$. Then it follows $\|\tilde{z} - x\|_2 = \left(\frac{1}{\delta} - 1\right) \|x - y\|_2 \leq \frac{1}{\delta}\|x - y\|_2 < 1$ and $\tilde{z} \in \mathcal{B}_{\|\cdot\|_2,1}(x) \subseteq \mathcal{R}(x)$. Again, the reverse triangle inequality can be applied to get the contradiction

$$M_x \geq \|\tilde{z}\| \geq \frac{1}{\delta}\|x\| - \left(\frac{1}{\delta} - 1\right) \|y\| \geq \|x\| + \left(\frac{1}{\delta} - 1\right) \varepsilon > M_x.$$

□

Corollary 4.8 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm, and let $a \in \mathbb{R}^n$. Then $F_a : \mathbb{R}^n \to \mathbb{R}_{\geq 0}, x \mapsto \|x - a\|$ is continuous with respect to the Euclidean norm.*

Proof. Let $x \in \mathbb{R}^n$ and $\varepsilon \in \mathbb{R}_{>0}$. Then it follows from Lemma 4.7 that there is some $\delta \in \mathbb{R}_{>0}$ such that $|\|x - a\| - \|y\|| < \varepsilon$ holds for every $y \in \mathcal{B}_{\|\cdot\|_2,\delta}(x - a)$. Since for every $z \in \mathcal{B}_{\|\cdot\|_2,\delta}(x)$ it holds that $\|(z - a) - (x - a)\|_2 = \|z - x\|_2 < \delta$, it is $|F_a(x) - F_a(z)| = |\|x - a\| - \|z - a\|| < \varepsilon$. □

Definition 4.9 *For $n \in \mathbb{N} \cup \{0\}$,* the n-dimensional sphere *is defined as*

$$S^n := \left\{x \in \mathbb{R}^{n+1} \mid \|x\|_2 = 1\right\}.$$

Proposition 4.10 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm. Then $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ is a symmetric convex body with center point 0, and for every $p \in \mathbb{R}^n$ it is*

$$\|p\|_{\overline{\mathcal{B}}_{\|\cdot\|,1}(0),0} = \|p\|.$$

Proof. Since S^{n-1} is compact with respect to the Euclidean norm and for every $x \in S^{n-1}$ it is $\|x\| > 0$, Proposition 4.7 implies the existence of $m \in \mathbb{R}_{>0}$ such that $\|x\| \geq m$ holds for every $x \in S^{n-1}$. Hence, for each $x \in \overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ with $x \neq 0$ it is

$$1 \geq \|x\| = \|x\|_2 \left\| \frac{x}{\|x\|_2} \right\| \geq m\|x\|_2,$$

which shows $\overline{\mathcal{B}}_{\|\cdot\|,1}(0) \subseteq \overline{\mathcal{B}}_{\|\cdot\|_2,1/m}(0)$ and $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ is bounded.

For $x = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$ with $\|x\| > 1$, let $\varepsilon := \|x\| - 1 > 0$. With $e_1, \ldots, e_n$ denoting the standard basis of $\mathbb{R}^n$, define $M := \max\{\|e_i\| \mid i \in \{1, \ldots, n\}\}$ and $\delta := \frac{\varepsilon}{M\sqrt{n}} > 0$. Then it holds for each $y = (y_1, \ldots, y_n)^T$ with $\|y - x\|_2 < \delta$ by the Cauchy–Schwarz inequality

$$\|y - x\| \leq \sum_{i=1}^{n} |y_i - x_i|\|e_i\| \leq M \sum_{i=1}^{n} |y_i - x_i| \leq M\sqrt{n}\|y - x\|_2 < M\sqrt{n}\delta = \varepsilon.$$

This yields that

$$\mathcal{B}_{\|\cdot\|_2,\delta}(x) \subseteq \mathcal{B}_{\|\cdot\|,\varepsilon}(x) \subseteq \mathbb{R}^n \setminus \overline{\mathcal{B}}_{\|\cdot\|,1}(0),$$

and thus $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ is closed and compact.

For every $x \in \mathbb{R}^n$ with $\|x\| < 1$, one can define $\varepsilon := 1 - \|x\|$ as well as M and δ as above to get analogously

$$\mathcal{B}_{\|\cdot\|_2,\delta}(x) \subseteq \mathcal{B}_{\|\cdot\|,\varepsilon}(x) \subseteq \mathcal{B}_{\|\cdot\|,1}(0).$$

This shows that $\mathcal{B}_{\|\cdot\|,1}(0)$ is open, and in particular that 0 is in the interior of $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$. Moreover, $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ is convex due to the triangle inequality which is satisfied by $\|\cdot\|$, and $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ is symmetric because $\|-x\| = \|x\|$ holds for every $x \in \mathbb{R}^n$.

For every $x \in \mathbb{R}^n$ with $\|x\| = 1$, and every $\varepsilon \in \mathbb{R}_{>0}$ it holds for $\mu_1 := \max\left\{1 - \frac{\varepsilon}{2\|x\|_2}, \frac{1}{2}\right\}$ that $\mu_1 x \in \mathcal{B}_{\|\cdot\|_2,\varepsilon}(x)$ as well as $\|\mu_1 x\| < 1$, and for $\mu_2 := 1 + \frac{\varepsilon}{2\|x\|_2}$ that $\mu_2 x \in \mathcal{B}_{\|\cdot\|_2,\varepsilon}(x)$ as well as $\|\mu_2 x\| > 1$. Therefore, the boundary of $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ is $\{x \in \mathbb{R}^n \mid \|x\| = 1\}$.

For every $p \in \mathbb{R}^n$ with $p \neq 0$ it now follows that $x_{0,p} = \frac{p}{\|p\|}$, where the notation from Definition 4.3 is used for $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ with center point 0. This gives

$$\|p\|_{\overline{\mathcal{B}}_{\|\cdot\|,1}(0),0} = \frac{\|p\|_2}{\|x_{0,p}\|_2} = \|p\|.$$

□

Propositions 4.6 and 4.10 give two equivalent viewpoints on norms: Either one can directly consider the norm and derive properties of the unit ball from that, or one considers a symmetric convex body and deduces properties of the corresponding norm. In the introduction of this thesis, it is already defined what a strictly convex norm is. A convex body can also be strictly convex, and both definitions are compatible for symmetric convex bodies.

Definition 4.11 *Let $K \subseteq \mathbb{R}^n$ be a convex body with center point $c \in K$. K is called* strictly convex *if for every $x, y \in K$ with $x \neq y$ and every $\tau \in (0,1)$ it holds that $\tau x + (1-\tau)y$ lies in the interior of K.*

Proposition 4.12 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm. Then it holds that $\|\cdot\|$ is strictly convex if and only if $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ is strictly convex.*

Proof. First, assume that $\|\cdot\|$ is strictly convex, and let $x, y \in \overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ with $x \neq y$ as well as $\tau \in (0,1)$. By Lemma 2.6, it is $\|\tau x + (1-\tau)y\| < \max\{\|x\|, \|y\|\} \leq 1$, which gives $\tau x + (1-\tau)y \in \mathcal{B}_{\|\cdot\|,1}(0)$.

Secondly, assume the strict convexity of $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$, and let $x, y \in \mathbb{R}^n$ with $x \neq y$ and $\|x\| = \|y\| =: m > 0$ as well as $\tau \in (0,1)$. Then it follows that $\frac{x}{m}, \frac{y}{m} \in \overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ and the strict convexity of this unit ball implies that $\tau\frac{x}{m} + (1-\tau)\frac{y}{m} \in \mathcal{B}_{\|\cdot\|,1}(0)$. Therefore, $\|\tau x + (1-\tau)y\| = m\|\tau\frac{x}{m} + (1-\tau)\frac{y}{m}\| < m$. □

Another possibility to define strict convexity of convex bodies is given in the next statement. This variant is used in [10], and since this chapter refers several

times to results in [10], it will be proven that this alternative definition is indeed equivalent to Definition 4.11.

Proposition 4.13 *Let $K \subseteq \mathbb{R}^n$ be a convex body with center point $c \in K$. Then it holds that K is strictly convex if and only if the boundary of K does not contain a line segment.*

Proof. The strict convexity of K directly implies that the boundary of K cannot contain a line segment. Thus, only the other direction needs to be shown.

For this, assume that the boundary of K does not contain a line segment, and let $x, y \in K$ with $x \neq y$ as well as $\tau \in (0,1)$. By the convexity of K, it follows that $a := \tau x + (1-\tau)y \in K$. Assume for contradiction that a lies on the boundary of K. Then there exists some b_1 on the line segment between x and a which lies in the interior of K. In fact, this is trivially true for $b_1 = x$ if x itself is in the interior of K. If x lies on the boundary of K, one finds b_1 as described above, since the boundary of K does not contain the line segment between x and a. Analogously, there exists b_2 on the line segment between y and a that lies in the interior of K. Hence, $d_{K,c}(c, b_1) < 1$, $d_{K,c}(c, b_2) < 1$ and for some $\lambda \in (0,1)$ it is $a = \lambda b_1 + (1-\lambda)b_2$. This yields

$$\begin{aligned} d_{K,c}(c,a) &= d_{K,c}(0, a-c) = d_{K,c}\left(0, \lambda(b_1 - c) + (1-\lambda)(b_2 - c)\right) \\ &\leq d_{K,c}\left(0, \lambda(b_1 - c)\right) + d_{K,c}\left(0, (1-\lambda)(b_2 - c)\right) \\ &= \lambda d_{K,c}\left(c, b_1\right) + (1-\lambda) d_{K,c}\left(c, b_2\right) < 1 \end{aligned}$$

and a lies in the interior of K, which contradicts the assumption that a lies on the boundary of K. □

Sometimes strict convexity of a given norm is not enough, and one also wants the property that the unit ball has no "sharp corners". Such a norm is called smooth. To define this notion formally, one needs to introduce supporting hyperplanes.

Definition 4.14 *Let $S \subseteq \mathbb{R}^n$, and let $s \in S$ lie on the boundary of S. A hyperplane $H \subseteq \mathbb{R}^n$ is a* supporting hyperplane of S at s *if $s \in H$ and S is contained in one of the two closed halfspaces bounded by H.*

For every convex set it holds that each of its boundary points has a supporting hyperplane. This result is known as the supporting hyperplane theorem and can for example be found in [3].

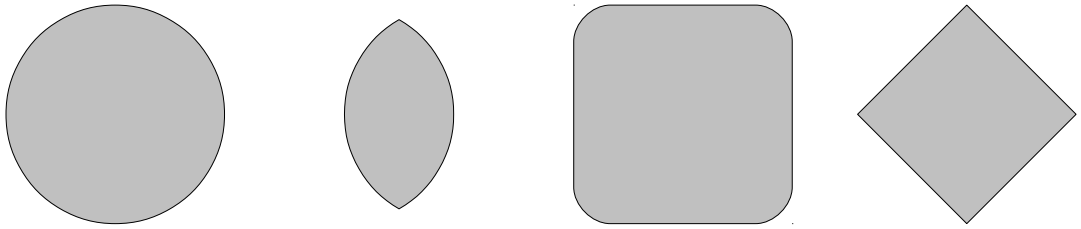
Theorem 4.15 (Supporting hyperplane theorem) *Let $S \subseteq \mathbb{R}^n$ be convex, and let $s \in S$ lie on the boundary of S. Then there exists a supporting hyperplane of S at s.*

In particular, every boundary point of a convex body has a supporting hyperplane, but these hyperplanes are not unique in general. The intuition is that non-unique supporting hyperplanes occur at sharp corners of the convex body. If a convex body has unique supporting hyperplanes everywhere on its boundary, it is called smooth.

Definition 4.16 *Let $K \subseteq \mathbb{R}^n$ be a convex body with center point $c \in K$. K is called* smooth *if each point on its boundary has a unique supporting hyperplane.*

A norm $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ is called smooth *if $\overline{\mathcal{B}}_{\|\cdot\|,1}(0)$ is smooth.*

A convex body can be strictly convex and smooth at the same time, or it can be neither strictly convex nor smooth, or it can have exactly one of the two properties. Illustrations for this are shown in Figure 4.1.



(a) Strictly convex and smooth. (b) Strictly convex but not smooth. (c) Smooth but not strictly convex. (d) Neither smooth nor strictly convex.

Figure 4.1: Convex bodies in two dimensions with different properties.

4.2 Bisectors

In [6], Horváth shows that every bisector of two distinct points is homeomorphic to a hyperplane if a strictly convex norm is used. In the following, the intersection of two bisectors is examined, where one bisector is given by a_1 and a_2 and the other bisector is given by a_1 and a_3. In other words, the set of all points having the same distance to $a_1, a_2, a_3 \in \mathbb{R}^n$ is analyzed. For the case $n = 3$, it is shown in [10] (cf. Lemma 3.1.2.6 and Corollary 3.1.2.7) that such a set is homeomorphic to a line under a strictly convex and smooth norm if a_1, a_2, a_3 are non-collinear. For strictly convex norms without smoothness it is also shown in [10] that this bisector intersection might be disconnected, but that each component is still homeomorphic to a line. As long as the underlying norm is strictly convex and smooth, I strongly conjecture for general dimension n that such a bisector intersection is homeomorphic to $\mathbb{R}^{n-2}$. One way to prove this relies on the following conjecture.

Conjecture 4.17 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex and smooth norm, let $a_1, a_2, a_3 \in \mathbb{R}^n$ be non-collinear, and let H be the plane spanned by a_1, a_2, a_3. Then it holds for every sequence $(p_k)_{k\in\mathbb{N}} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$ with*

$$\lim_{k\to\infty} \|p_k - a_1\| = \infty$$

that

$$\lim_{k\to\infty} \frac{\min\{\|p_k - h\| \mid h \in H\}}{\|p_k - a_1\|} = 1.$$

The precise statement regarding the appearance of the considered bisector intersection is formulated in the following theorem:

Theorem 4.18 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex and smooth norm, and let $V \subseteq \mathbb{R}^n$ be a subspace of dimension $m \geq 2$. If Conjecture 4.17 is true and $a_1, a_2, a_3 \in V$ are non-collinear, then $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3) \cap V$ is homeomorphic to $\mathbb{R}^{m-2}$. If $a_1, a_2, a_3 \in V$ are collinear and pairwise distinct, then $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3) = \emptyset$.*

The proof of this theorem uses some topological concepts which will be introduced first.

Definition 4.19 *For a given topological space $(X, \mathcal{T})$ and $Y \subseteq X$, the* subspace topology *on Y is*

$$\mathcal{T}_Y := \{O \cap Y \mid O \in \mathcal{T}\}.$$

Lemma 4.20 *Let $(X, \mathcal{T})$ be a topological space, and let $Z \subseteq Y \subseteq X$. Then it is $(\mathcal{T}_Y)_Z = \mathcal{T}_Z$.*

Proof. For $O \in (\mathcal{T}_Y)_Z$ there exists $O_Y \in \mathcal{T}_Y$ such that $O = O_Y \cap Z$. In addition, there exists $O_X \in \mathcal{T}$ with $O_Y = O_X \cap Y$. Thus, $O = O_X \cap Y \cap Z = O_X \cap Z \in \mathcal{T}_Z$.

Given $O \in \mathcal{T}_Z$, one finds $O_X \in \mathcal{T}$ with $O = O_X \cap Z = O_X \cap Y \cap Z \in (\mathcal{T}_Y)_Z$. □

Definition 4.21 *Let $(X, \mathcal{T})$ be a topological space, and let $Y \subseteq X$.*

$(X, \mathcal{T})$ is compact *if every open cover*

$$X = \bigcup_{i\in I} O_i \text{ with } O_i \in \mathcal{T}$$

has a finite subcover

$$X = O_{i_1} \cup O_{i_2} \cup \ldots \cup O_{i_n} \text{ with } i_1, i_2, \ldots, i_n \in I.$$

Y is compact in $(X, \mathcal{T})$ *if every open cover*

$$Y \subseteq \bigcup_{i\in I} O_i \text{ with } O_i \in \mathcal{T}$$

has a finite subcover

$$Y \subseteq O_{i_1} \cup O_{i_2} \cup \ldots \cup O_{i_n} \text{ with } i_1, i_2, \ldots, i_n \in I.$$

Lemma 4.22 *Let $(X, \mathcal{T})$ be a topological space, and let $Y \subseteq X$. Then Y is compact in $(X, \mathcal{T})$ if and only if $(Y, \mathcal{T}_Y)$ is compact.*

Proof. Assume that Y is compact in $(X, \mathcal{T})$, and let $Y = \bigcup_{i \in I} O_i$ with $O_i \in \mathcal{T}_Y$ be an open cover. Then one finds for every $i \in I$ an $O_{X,i} \in \mathcal{T}$ such that $O_i = O_{X,i} \cap Y$, and Y can be written as

$$Y = \bigcup_{i \in I} (O_{X,i} \cap Y) = \left(\bigcup_{i \in I} O_{X,i} \right) \cap Y \subseteq \bigcup_{i \in I} O_{X,i}.$$

The compactness of Y as a subset of X gives $i_1, \ldots, i_n \in I$ such that $Y \subseteq O_{X,i_1} \cup \ldots \cup O_{X,i_n}$ leading to

$$Y = \left(\bigcup_{j=1}^{n} O_{X,i_j} \right) \cap Y = \bigcup_{j=1}^{n} \left(O_{X,i_j} \cap Y \right) = \bigcup_{j=1}^{n} O_{i_j}.$$

Now assume that $(Y, \mathcal{T}_Y)$ is compact, and let $Y \subseteq \bigcup_{i \in I} O_i$ with $O_i \in \mathcal{T}$ be an open cover. This yields

$$Y = \left(\bigcup_{i \in I} O_i \right) \cap Y = \bigcup_{i \in I} (O_i \cap Y) \text{ with } O_i \cap Y \in \mathcal{T}_Y.$$

The compactness of Y as a topological space gives $i_1, \ldots, i_n \in I$ such that

$$Y = \bigcup_{j=1}^{n} \left(O_{i_j} \cap Y \right) = \left(\bigcup_{j=1}^{n} O_{i_j} \right) \cap Y \subseteq \bigcup_{j=1}^{n} O_{i_j}.$$

□

Corollary 4.23 *Let $(X, \mathcal{T})$ be a topological space, and let $Z \subseteq Y \subseteq X$. Then Z is compact in $(Y, \mathcal{T}_Y)$ if and only if Z is compact in $(X, \mathcal{T})$.*

Proof. By Lemma 4.22, Z is compact in $(Y, \mathcal{T}_Y)$ if and only if $(Z, (\mathcal{T}_Y)_Z)$ is compact, which is by Lemma 4.20 equivalent to $(Z, \mathcal{T}_Z)$ being compact and thus – again by Lemma 4.22 – equivalent to Z being compact in $(X, \mathcal{T})$. □

Definition 4.24 *For two given topological spaces $(X, \mathcal{T})$ and $(Y, \mathcal{S})$, a function $f : X \to Y$ is* proper *if for every $C \subseteq Y$ compact in $(Y, \mathcal{S})$ the preimage $f^{-1}(C)$ is compact in $(X, \mathcal{T})$.*

Additionally to these notions from topology, the proof needs orthogonal complements of real subspaces and projections. Furthermore, the proof specifies a homeomorphism (under the assumption of Conjecture 4.17) from the bisector intersection to a projected open unit ball, such that it will be shown in advance that such an open unit ball is homeomorphic to its whole embedding space.

Definition 4.25 *For a given subspace $V \subseteq R^n$, the* orthogonal complement *of V is*

$$V^\perp := \{w \in \mathbb{R}^n \mid \forall v \in V : \langle v, w\rangle = 0\},$$

and the projection *of $\mathbb{R}^n$ on $V^\perp$ is*

$$\begin{aligned} P_{V^\perp} : \mathbb{R}^n &\longrightarrow V^\perp, \\ x &\longmapsto w \text{ such that } x - w \in V. \end{aligned}$$

Lemma 4.26 *Let $V \subseteq \mathbb{R}^n$ be a subspace with orthogonal complement $W := V^\perp$. Then P_W is continuous with respect to the Euclidean norm.*

Proof. Let $x_1 \in \mathbb{R}^n$, $\varepsilon \in \mathbb{R}_{>0}$ and $x_2 \in \mathcal{B}_{\|\cdot\|_2,\varepsilon}(x_1)$. Then there are unique $v_1, v_2 \in V$ and $w_1, w_2 \in W$ such that $x_1 = v_1 + w_1$ and $x_2 = v_2 + w_2$. This yields

$$\begin{aligned} \|P_W(x_1) - P_W(x_2)\|_2^2 = \|w_1 - w_2\|_2^2 &\leq \langle w_1 - w_2, w_1 - w_2\rangle + \langle v_1 - v_2, v_1 - v_2\rangle \\ &= \langle x_1 - x_2, x_1 - x_2\rangle = \|x_1 - x_2\|_2^2 < \varepsilon^2. \end{aligned}$$

□

Lemma 4.27 *Let $V \subseteq \mathbb{R}^n$ be a subspace, and let $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ be a norm. Then $\mathcal{B}_{\|\cdot\|,1}(0)$ is homeomorphic to V.*

Proof. Define

$$\begin{aligned} h : \mathcal{B}_{\|\cdot\|,1}(0) &\longrightarrow V, \\ x &\longmapsto \frac{x}{1 - \|x\|}. \end{aligned}$$

First consider $x_1, x_2 \in \mathcal{B}_{\|\cdot\|,1}(0)$ with $h(x_1) = h(x_2)$. Then it holds $x_1 = \mu x_2$ with $\mu := \frac{1-\|x_1\|}{1-\|x_2\|}$. In particular, $\|x_1\| = \mu\|x_2\|$ which is equivalent to $\|x_1\|(1 - \|x_2\|) = (1 - \|x_1\|)\|x_2\|$ and further to $\|x_1\| = \|x_2\|$. Thus, $\mu = 1$ and $x_1 = x_2$. This shows that h is injective.

For $y \in V$ it holds that $\left\|\frac{y}{1+\|y\|}\right\| < 1$, and due to $1 - \left\|\frac{y}{1+\|y\|}\right\| = \frac{1}{1+\|y\|}$ it is $h\left(\frac{y}{1+\|y\|}\right) = y$. Hence, h is a bijection with inverse $h^{-1} : V \to \mathcal{B}_{\|\cdot\|,1}(0), x \mapsto \frac{x}{1+\|x\|}$. In addition, Corollary 4.8 directly implies that h as well as h^{-1} are continuous. □

Lemma 4.28 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$ be a norm, and let $V \subseteq \mathbb{R}^n$ be a subspace with orthogonal complement $W := V^\perp$. Then*

$$\begin{aligned} \|\cdot\|_W : W &\longrightarrow \mathbb{R}_{\geq 0}, \\ w &\longmapsto \min\{\|w + v\| \mid v \in V\} \end{aligned}$$

is a norm with unit ball $\mathcal{B}_{\|\cdot\|_W,1}(0) = P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$.

Proof. First, one needs to consider why the above minimum is attained. For this, let $w \in W$. By Corollary 4.8, $g_w : V \to \mathbb{R}_{\geq 0}, v \mapsto \|w+v\|$ is continuous with respect to the Euclidean norm. This further implies that $K_w := \{v \in V \mid \|w+v\| \leq \|w\|\}$ is compact in $(\mathbb{R}^n, \|\cdot\|_2)$ and thus by Corollary 4.23 also compact in $(V, \|\cdot\|_2)$. Hence, g_w attains its minimum on K_w, i.e., there exists some $\tilde{v} \in K_w$ such that $g_w(\tilde{v}) \leq g_w(v)$ holds for all $v \in K_w$. Furthermore, for every $v \in V \setminus K_w$ it is $\|w+v\| > \|w\| = g_w(0) \geq g_w(\tilde{v})$. This shows that $\|w+v\| \geq \|w+\tilde{v}\|$ holds for every $v \in V$.

Secondly, it needs to be shown that $\|\cdot\|_W$ is indeed a norm. It is clear that $\|0\|_W = 0$. For every $w \in W$ with $\|w\|_W = 0$ there exists some $v \in V$ with $\|w+v\| = 0$, which implies $w = -v \in W \cap V$ and thus $w = 0$. For every $w \in W$ and every $\mu \in \mathbb{R} \setminus \{0\}$ it holds

$$\begin{aligned}\|\mu w\|_W &= \min\{\|\mu w + v\| \mid v \in V\} = \min\{\|\mu w + \mu v\| \mid v \in V\} \\ &= \min\{|\mu|\|w+v\| \mid v \in V\} = |\mu| \min\{\|w+v\| \mid v \in V\} = |\mu|\|w\|_W.\end{aligned}$$

For the triangle inequality let $w_1, w_2 \in W$. For $i \in \{1,2\}$ there exists $v_i \in V$ such that $\|w_i\|_W = \|w_i + v_i\|$, which yields

$$\|w_1+w_2\|_W \leq \|w_1+w_2+v_1+v_2\| \leq \|w_1+v_1\| + \|w_2+v_2\| = \|w_1\|_W + \|w_2\|_W.$$

Finally, $\mathcal{B}_{\|\cdot\|_W,1}(0) = P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ can be shown as follows: On the one hand, for every $w \in \mathcal{B}_{\|\cdot\|_W,1}(0)$ there exists some $v \in V$ with $\|w+v\| < 1$ such that $w = P_W(w+v) \in P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$. On the other hand, for $x \in \mathcal{B}_{\|\cdot\|,1}(0)$ with $w := P_W(x)$ it holds that $\|w\|_W \leq \|w+(x-w)\| = \|x\| < 1$. □

Proof of Theorem 4.18. Let $a_1, a_2, a_3 \in V$ be pairwise distinct. If a_1, a_2, a_3 are collinear, one can assume without loss of generality that a_2 is in the middle, i.e., there exists $\tau \in (0,1)$ such that $a_2 = \tau a_1 + (1-\tau)a_3$. For every $p \in \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$ it holds that $\|p-a_2\| = \|\tau(p-a_1)+(1-\tau)(p-a_3)\| < \|p-a_1\|$ and so $p \notin \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2)$. This shows $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3) = \emptyset$. Hence, in the following a_1, a_2, a_3 are assumed to be non-collinear.

For V one can choose an orthonormal basis $(v_1, \ldots, v_m)$ with respect to the dot product on $\mathbb{R}^n$. Let $(e_1, \ldots, e_m)$ denote the standard basis of $\mathbb{R}^m$. With this, one can define

$$\begin{aligned}\psi : V &\longrightarrow \mathbb{R}^m, \\ \sum_{i=1}^{m} \alpha_i v_i &\longmapsto \sum_{i=1}^{m} \alpha_i e_i,\end{aligned}$$

as well as a norm $\|\cdot\|_\psi : \mathbb{R}^m \to \mathbb{R}_{\geq 0}, x \mapsto \|\psi^{-1}(x)\|$, such that ψ is an isometric isomorphism from $(V, \|\cdot\|_V)$ to $(\mathbb{R}^m, \|\cdot\|_\psi)$ as well as an isometric isomorphism from $(V, \|\cdot\|_2)$ to $(\mathbb{R}^m, \|\cdot\|_2)$. Furthermore, $\|\cdot\|_\psi$ is a strictly convex and smooth

norm with unit ball $\mathcal{B}_{\|\cdot\|_\psi,1}(0) = \psi\left(\mathcal{B}_{\|\cdot\|,1}(0) \cap V\right)$ satisfying

$$\psi\left(\mathcal{H}^{=}_{\|\cdot\|}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_3) \cap V\right) = \mathcal{H}^{=}_{\|\cdot\|_\psi}(\psi(a_1),\psi(a_2)) \cap \mathcal{H}^{=}_{\|\cdot\|_\psi}(\psi(a_1),\psi(a_3)).$$

Thus, it is enough to show Theorem 4.18 for $V = \mathbb{R}^n$, since then it can be applied to $\|\cdot\|_\psi$ to get a homeomorphism from $\mathcal{H}^{=}_{\|\cdot\|_\psi}(\psi(a_1),\psi(a_2)) \cap \mathcal{H}^{=}_{\|\cdot\|_\psi}(\psi(a_1),\psi(a_3))$ to $\mathbb{R}^{m-2}$. Hence, assume in the following that $V = \mathbb{R}^n$.

Now the desired homeomorphism will be first described informally and afterwards defined formally: Let H be the plane spanned by a_1, a_2, a_3, i.e.,

$$H := \{a_1 + s(a_2 - a_1) + t(a_3 - a_1) \mid s,t \in \mathbb{R}\}.$$

Then, $H - a_1$ is a vector space with orthogonal complement $W := (H - a_1)^\perp$. For $p \in \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_3)$ it holds that a_1, a_2, a_3 are on the boundary of $\mathcal{B}_{\|\cdot\|,r}(p)$, where $r := \|a_1 - p\| > 0$. This is illustrated for three dimensions in Figure 4.2. The homeomorphism considers the intersection of this ball with H, and the relative position of this intersection in the unit ball. To be more specific, $\tilde{K}_p := \overline{\mathcal{B}}_{\|\cdot\|,r}(p) \cap H$ and

$$K_p := \frac{1}{r}(\tilde{K}_p - p) = \overline{\mathcal{B}}_{\|\cdot\|,1}(0) \cap \left((H - a_1) + \frac{a_1 - p}{r}\right)$$

are strictly convex and smooth, and the position of K_p in the unit ball is already determined by the projection of $\frac{a_1-p}{r}$ on W. Therefore, the conjectured homeomorphism – as depicted in Figure 4.3 – is

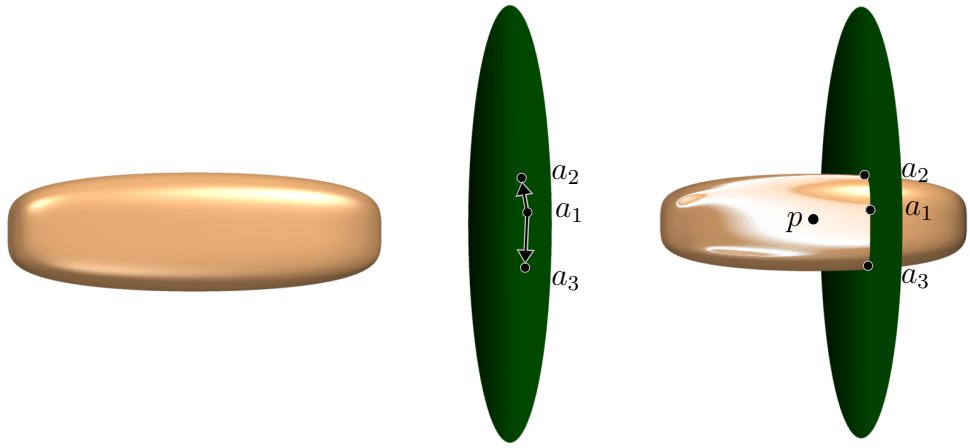
$$\begin{aligned}\varphi : \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_3) &\longrightarrow W,\\ p &\longmapsto P_W\left(\frac{a_1 - p}{\|a_1 - p\|}\right).\end{aligned}$$

First, the injectivity of φ will be shown. Let $p_1, p_2 \in \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_3)$ with $\varphi(p_1) = \varphi(p_2) =: w$. Then it holds that

$$(H - a_1) + \frac{a_1 - p_1}{\|a_1 - p_1\|} = (H - a_1) + w = (H - a_1) + \frac{a_1 - p_2}{\|a_1 - p_2\|},$$

which shows $K_{p_1} = K_{p_2}$ using the notation above. Lemma 2.1.1.1 and Theorem 2.1.2.3 in [10] show for strictly convex bodies in two-dimensions and for pairwise distinct points a, b, c that there is at most one uniformly scaled and translated copy of this body that has a, b, c on its boundary, and that exactly one such copy exists if a, b, c are non-collinear and the given body is smooth. From this it follows that a unique $r \in \mathbb{R}_{>0}$ and a unique $p \in \mathbb{R}^n$ exist such that $rK_{p_1} + p \subseteq H$ has a_1, a_2, a_3 on its boundary in H. Due to $\tilde{K}_{p_1} = \|a_1 - p_1\|K_{p_1} + p_1$ and $\tilde{K}_{p_2} = \|a_1 - p_2\|K_{p_1} + p_2$, it must hold that $\|a_1 - p_1\| = r = \|a_1 - p_2\|$ and $p_1 = p = p_2$. Hence, φ is injective.

Secondly, the image of φ will be calculated. It holds for every



(a) $\mathcal{B}_{\|\cdot\|,1}(0)$. (b) H. (c) $p \in \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$ with $\mathcal{B}_{\|\cdot\|,\|a_1-p\|}(p)$ and H.

Figure 4.2: Intersection of scaled and translated unit ball with H in a_1, a_2 and a_3 for the case $n = 3$.

$p \in \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$ that $\varphi(p) = P_W\left(\frac{a_1-p}{\|a_1-p\|}\right) = P_W\left(\frac{1}{\|a_1-p\|}\left(\frac{a_1+a_2}{2} - p\right)\right)$ and

$$\left\| \frac{1}{\|a_1 - p\|} \left(\frac{a_1 + a_2}{2} - p \right) \right\| = \frac{1}{\|a_1 - p\|} \left\| \frac{1}{2}(a_1 - p) + \frac{1}{2}(a_2 - p) \right\| < 1,$$

such that $\varphi(p) \in P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$. For every $x \in \mathcal{B}_{\|\cdot\|,1}(0)$ it holds that $K := \overline{\mathcal{B}}_{\|\cdot\|,1}(0) \cap ((H - a_1) + x)$ is strictly convex and smooth. Therefore, Lemma 2.1.1.1 and Theorem 2.1.2.3 in [10] give unique $r \in \mathbb{R}_{>0}$ and $p \in \mathbb{R}^n$ such that $rK + p \subseteq H$ has a_1, a_2, a_3 on its boundary in H. Because of $rK + p = \overline{\mathcal{B}}_{\|\cdot\|,r}(p) \cap ((H - a_1) + rx + p)$, it must hold that $rK + p \subseteq H \cap ((H - a_1) + rx + p)$, which implies $H = (H - a_1) + rx + p$ and thus $rx + p - a_1 \in H - a_1$. Thus, $x - \frac{a_1-p}{r} \in H - a_1$ and $P_W(x) = P_W(\frac{a_1-p}{r})$ hold. Moreover, $r = \|a_1 - p\| = \|a_2 - p\| = \|a_3 - p\|$, which leads to $p \in \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$ and $P_W(x) = \varphi(p)$. This shows (cf. Figure 4.3) that $\varphi(\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)) = P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ such that φ is a bijection

$$\varphi : \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3) \longrightarrow P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right).$$

Combining Lemmata 4.27 and 4.28 yields that $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ is homeomorphic to W and thus homeomorphic to $\mathbb{R}^{n-2}$. Therefore, it is only left to show that φ and φ^{-1} are continuous. The continuity of φ is a direct consequence of Corollary 4.8 and Lemma 4.26. Because of this, the rest of this proof will examine the continuity of φ^{-1}.

When assuming Conjecture 4.17, it can be shown that φ is proper: For this,

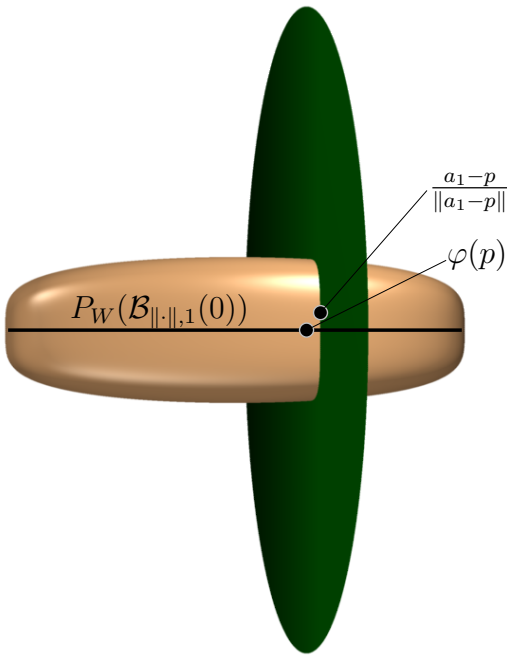


Figure 4.3: $\varphi(p)$ for p as in Figure 4.2c with $\mathcal{B}_{\|\cdot\|,1}(0)$ and $\left((H-a_1)+\frac{a_1-p}{\|a_1-p\|}\right)$.

let $C \subseteq P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ be compact in $\left(P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right), \|\cdot\|_2\right)$. One needs to show that $\varphi^{-1}(C)$ is compact in $\left(\mathcal{H}^{=}_{\|\cdot\|}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_3), \|\cdot\|_2\right)$. To ease notation, every topological space will have in the following the topology induced by $\|\cdot\|_2$ when nothing else is stated explicitly. It can further be assumed that $C \neq \emptyset$.

Corollary 4.23 implies that C is compact in $\mathbb{R}^n$, i.e., that C is closed and bounded in $\mathbb{R}^n$. Hence, $C = C \cap P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ is closed in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$. Since φ is continuous, $\varphi^{-1}(C)$ is closed in $\mathcal{H}^{=}_{\|\cdot\|}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_3)$, i.e., there exists some $\tilde{C} \subseteq \mathbb{R}^n$ closed in $\mathbb{R}^n$ such that $\varphi^{-1}(C) = \tilde{C} \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_3)$. Among other things, Lemma 1 in [6] states that bisectors $\mathcal{H}^{=}_{\|\cdot\|}(a,b)$ for $a,b \in \mathbb{R}^n, a \neq b$ are closed in $\mathbb{R}^n$, which implies that $\varphi^{-1}(C)$ is closed in $\mathbb{R}^n$. It is left to show that $\varphi^{-1}(C)$ is bounded in $\mathbb{R}^n$, because then $\varphi^{-1}(C)$ is compact in $\mathbb{R}^n$ and thus – by Corollary 4.23 – compact in $\mathcal{H}^{=}_{\|\cdot\|}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1,a_3)$. Hence, assume for contradiction that $\varphi^{-1}(C)$ is not bounded in $(\mathbb{R}^n, \|\cdot\|_2)$. Then $\varphi^{-1}(C)$ is not bounded in $(\mathbb{R}^n, \|\cdot\|)$, and for every $k \in \mathbb{N}$ one finds $p_k \in \varphi^{-1}(C)$ with

$$r_k := \|p_k - a_1\| = \|p_k - a_2\| = \|p_k - a_3\| > k.$$

If Conjecture 4.17 is true, the equality

$$\|\varphi(p_k)\|_W = \left\| P_W\left(\frac{a_1 - p_k}{r_k}\right)\right\|_W = \left\|\frac{-1}{r_k} P_W(p_k - a_1)\right\|_W = \frac{1}{r_k}\|P_W(p_k - a_1)\|_W$$

$$= \frac{1}{r_k} \min\{\|p_k - h\| \mid h \in H\}$$

and the conjecture would directly imply $\lim_{k\to\infty} \|\varphi(p_k)\|_W = 1$. But since C is compact in $\mathbb{R}^n$ and $w \mapsto \|w\|_W$ is continuous by Corollary 4.8, there exists $\tilde{w} \in C$ such that $\|\tilde{w}\|_W \geq \|w\|_W$ holds for all $w \in C$. Moreover, it follows from $\tilde{w} \in P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ that $\|\tilde{w}\|_W < 1$. Hence, for every $k \in \mathbb{N}$ it must hold that $\|\varphi(p_k)\|_W \leq \|\tilde{w}\|_W < 1$, which contradicts $\lim_{k\to\infty} \|\varphi(p_k)\|_W = 1$. Therefore, $\varphi^{-1}(C)$ is bounded in $\mathbb{R}^n$, and φ is proper.

With the property of φ being proper one can deduce that φ^{-1} is continuous: For this, the rest of this proof will show for φ^{-1} that preimages of closed sets in $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$ are closed in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$. Therefore, let $S \subseteq \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$ be closed in $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$, and show that $\varphi(S)$ is closed in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$, i.e., that $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right) \setminus \varphi(S)$ is open in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$.

Let $w \in P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right) \setminus \varphi(S)$. Then it is $\varepsilon := 1 - \|w\|_W > 0$, and Corollary 4.8 implies the existence of $\delta \in \mathbb{R}_{>0}$ such that for every $y \in W \cap \mathcal{B}_{\|\cdot\|_2,\delta}(w)$ it holds that $|\|w\|_W - \|y\|_W| < \varepsilon$. Hence, for every such y it is $\|y\|_W < \|w\|_W + \varepsilon = 1$, which implies

$$\begin{aligned} w \in W \cap \mathcal{B}_{\|\cdot\|_2,\frac{\delta}{2}}(w) &\subseteq W \cap \overline{\mathcal{B}}_{\|\cdot\|_2,\frac{\delta}{2}}(w) \subseteq W \cap \mathcal{B}_{\|\cdot\|_2,\delta}(w) \\ &\subseteq \mathcal{B}_{\|\cdot\|_W,1}(0) = P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right), \end{aligned}$$

where $W \cap \mathcal{B}_{\|\cdot\|_2,\frac{\delta}{2}}(w)$ is open in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$, and since W is closed in $\mathbb{R}^n$, $W \cap \overline{\mathcal{B}}_{\|\cdot\|_2,\frac{\delta}{2}}(w)$ is compact in $\mathbb{R}^n$ and thus compact in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ by Corollary 4.23. Therefore, $N := W \cap \overline{\mathcal{B}}_{\|\cdot\|_2,\frac{\delta}{2}}(w)$ is a compact neighborhood of w in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$. Because φ is proper, $\varphi^{-1}(N)$ is compact in $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$. Now consider $\tilde{S} := S \cap \varphi^{-1}(N)$. By Corollary 4.23, $\varphi^{-1}(N)$ is compact in $\mathbb{R}^n$, which implies that $\tilde{S} \subseteq \varphi^{-1}(N)$ is bounded in $\mathbb{R}^n$. Furthermore, there is $T \subseteq \mathbb{R}^n$ closed in $\mathbb{R}^n$ with $S = T \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$. From Lemma 1 in [6] it follows that S is closed in $\mathbb{R}^n$. This yields that $\tilde{S}$ is closed in $\mathbb{R}^n$ and thus compact in $\mathbb{R}^n$ as well as compact in $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$ by Corollary 4.23.

Using the continuity of φ one can show that $\varphi(\tilde{S})$ is compact in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$: Let $\varphi(\tilde{S}) \subseteq \bigcup_{i\in I} O_i$ with $O_i \subseteq P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ open in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ be an open cover. The continuity of φ implies for every $i \in I$ that $\varphi^{-1}(O_i)$ is open in $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$, such that $\tilde{S} \subseteq \bigcup_{i\in I} \varphi^{-1}(O_i)$ is an open cover. The compactness of $\tilde{S}$ in $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_3)$ gives $i_1, \ldots, i_n \in I$ such that $\tilde{S} \subseteq \varphi^{-1}(O_{i_1}) \cup \ldots \cup \varphi^{-1}(O_{i_n})$. Hence, $\varphi(\tilde{S}) \subseteq O_{i_1} \cup \ldots \cup O_{i_n}$, and $\varphi(\tilde{S})$ is compact in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$.

Using again Corollary 4.23 implies that $\varphi(\tilde{S})$ is compact in $\mathbb{R}^n$ and thus closed in $\mathbb{R}^n$. This further gives that $\varphi(\tilde{S}) = \varphi(\tilde{S}) \cap P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ is closed in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$. Therefore, $\left(W \cap \mathcal{B}_{\|\cdot\|_2,\frac{\delta}{2}}(w)\right) \setminus \varphi(\tilde{S})$ is open in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$. Moreover, it is

$$w \in \left(W \cap \mathcal{B}_{\|\cdot\|_2,\frac{\delta}{2}}(w)\right) \setminus \varphi(\tilde{S}) \subseteq P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right) \setminus \varphi(S),$$

because if for some $y \in \left(W \cap \mathcal{B}_{\|\cdot\|_2,\frac{\delta}{2}}(w)\right) \setminus \varphi(\tilde{S})$ it would also hold that $y \in \varphi(S)$, then there must exist some $x \in S$ with $y = \varphi(x)$, i.e., $x = \varphi^{-1}(y) \in \varphi^{-1}(N)$ yielding $x \in \tilde{S}$ and $y \in \varphi(\tilde{S})$, which is a contradiction. Thus, it follows that $\left(W \cap \mathcal{B}_{\|\cdot\|_2,\frac{\delta}{2}}(w)\right) \setminus \varphi(\tilde{S})$ is an open neighborhood of w which is contained in $P_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right) \setminus \varphi(S)$, and φ^{-1} is continuous. □

4.3 Voronoi cells

In the case of non-strictly convex norms, the Voronoi-relevant vectors are not sufficient to determine the Voronoi cell of a given lattice, i.e., for a given lattice Λ and a non-strictly convex norm it might happen for some $x \in \operatorname{span}(\Lambda)$ that x is strictly closer to 0 than to all Voronoi-relevant vectors, but some other lattice vector is even closer to x. An example for this is given in Corollary 2.27. At least it can be shown for arbitrary norms that the generalized Voronoi-relevant vectors determine the Voronoi cell completely:

Theorem 4.29 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Then it holds that*

$$\begin{aligned}\mathcal{V}(\Lambda, \|\cdot\|) &= \left\{ x \in \operatorname{span}(\Lambda) \;\middle|\; \begin{array}{l} \forall v \in \Lambda \text{ generalized Voronoi-relevant} \\ \text{with respect to } \|\cdot\| : \|x\| \leq \|x - v\| \end{array} \right\} \\ &=: \tilde{\mathcal{V}}^{(g)}(\Lambda, \|\cdot\|).\end{aligned}$$

The proof of this statement uses the following easy lemma:

Lemma 4.30 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Then it holds for every $x \in \tilde{\mathcal{V}}^{(g)}(\Lambda, \|\cdot\|)$ and every $w \in \Lambda$ with $\|x - w\| < \|x\|$ that there is some $\tau \in (0, 1)$ with $\|\tau x - w\| = \tau\|x\|$ and $\tau x \in \tilde{\mathcal{V}}^{(g)}(\Lambda, \|\cdot\|)$.*

Proof. Let $x \in \tilde{\mathcal{V}}^{(g)}(\Lambda, \|\cdot\|)$ and $w \in \Lambda$ such that $\|x - w\| < \|x\|$. In particular, it is $w \neq 0$. It follows from Corollary 4.8 that

$$\begin{aligned} f : [0, 1] &\longrightarrow \mathbb{R}, \\ \tau &\longmapsto \|\tau x - w\| - \tau\|x\| \end{aligned}$$

is continuous with respect to the Euclidean norm. Because of $f(0) = \|w\| > 0$ and $f(1) = \|x - w\| - \|x\| < 0$, the intermediate value theorem implies the

existence of $\tau \in (0,1)$ with $f(\tau) = 0$, i.e., $\|\tau x - w\| = \tau\|x\|$. For every generalized Voronoi-relevant vector $v \in \Lambda$ it holds by $x \in \tilde{\mathcal{V}}^{(g)}(\Lambda, \|\cdot\|)$ that

$$\tau\|x\| \leq \|\tau x - \tau v\| = \|\tau(\tau x - v) + (1-\tau)(\tau x)\| \leq \tau\|\tau x - v\| + (1-\tau)\tau\|x\|,$$

which implies $\tau\|x\| \leq \|\tau x - v\|$. Thus it is $\tau x \in \tilde{\mathcal{V}}^{(g)}(\Lambda, \|\cdot\|)$. □

Proof of Theorem 4.29. It is clear that $\mathcal{V}(\Lambda, \|\cdot\|) \subseteq \tilde{\mathcal{V}}^{(g)}(\Lambda, \|\cdot\|)$. To show the other inclusion, let $x \in \tilde{\mathcal{V}}^{(g)}(\Lambda, \|\cdot\|)$ and assume for contradiction that $x \notin \mathcal{V}(\Lambda, \|\cdot\|)$. Then there exists some $u \in \Lambda$ with $\|x - u\| < \|x\|$. Since Λ is discrete, there is some $k \in \mathbb{N}$ with $k = |\{u \in \Lambda \mid \|x - u\| < \|x\|\}|$ and one can write $\{u \in \Lambda \mid \|x - u\| < \|x\|\} = \{u_1, \ldots, u_k\}$. Lemma 4.30 gives for every $i \in \{1, \ldots, k\}$ some $\tau_i \in (0,1)$ with $\|\tau_i x - u_i\| = \tau_i\|x\|$ and $\tau_i x \in \tilde{\mathcal{V}}^{(g)}(\Lambda, \|\cdot\|)$. Let $j \in \{1, \ldots, k\}$ with $\tau_j = \min\{\tau_1, \ldots, \tau_k\}$. Due to $x \in \tilde{\mathcal{V}}^{(g)}(\Lambda, \|\cdot\|)$, u_j cannot be generalized Voronoi-relevant, which implies the existence of some $v \in \Lambda$ with $\|\tau_j x - v\| < \tau_j\|x\|$. From

$$\begin{aligned} \|x - v\| &= \|x - \tau_j x + \tau_j x - v\| \leq (1-\tau_j)\|x\| + \|\tau_j x - v\| \\ &< (1-\tau_j)\|x\| + \tau_j\|x\| = \|x\| \end{aligned} \tag{4.1}$$

follows that $v = u_i$ for some $i \in \{1, \ldots, k\}$. Due to the minimal choice of j, one gets the following contradiction

$$\begin{aligned} \|\tau_i x - v\| &= \|\tau_i x - \tau_j x + \tau_j x - v\| \leq (\tau_i - \tau_j)\|x\| + \|\tau_j x - v\| \\ &< (\tau_i - \tau_j)\|x\| + \tau_j\|x\| = \tau_i\|x\| = \|\tau_i x - v\|. \end{aligned} \tag{4.2}$$

□

For the Euclidean norm, the authors of [1] argue that the Voronoi-relevant vectors determine the Voronoi cell completely. I expect this to be true for every strictly convex norm. Unfortunately, the subsequent proof for this statement relies on a very plausible conjecture, which roughly states the following for a given lattice Λ with strictly convex norm $\|\cdot\|$: If for some $x \in \operatorname{span}(\Lambda)$ the scaled, translated unit ball $\overline{\mathcal{B}}_{\|\cdot\|,\|x\|}(x)$ contains no lattice points in its interior, but contains 0 and at least two additional lattice points on its boundary, then one can walk from x within $\operatorname{span}(\Lambda)$ an arbitrarily short distance along one of the bisectors between 0 and some other lattice point on the boundary of the ball such that the resulting point is strictly further away from all other boundary-lattice-points. Formally this is expressed as follows.

Conjecture 4.31 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Moreover, let $x \in \mathcal{V}(\Lambda, \|\cdot\|)$ with $k := |\{u \in \Lambda\backslash\{0\} \mid \|x-u\| = \|x\|\}| \geq 2$.*

Then it holds for every $\delta \in \mathbb{R}_{>0}$ *that*

$$\operatorname{span}(\Lambda) \cap \mathcal{B}_{\|\cdot\|_2,\delta}(x) \cap \left(\bigcup_{i=1}^{k} \left(\mathcal{H}^{=}_{\|\cdot\|}(0,u_i) \cap \bigcap_{\substack{j=1 \\ j\neq i}}^{k} \mathcal{H}^{<}_{\|\cdot\|}(0,u_j) \right) \right) \neq \emptyset,$$

where $\{u \in \Lambda \setminus \{0\} \mid \|x-u\| = \|x\|\} = \{u_1, \ldots, u_k\}$.

Assuming this conjecture, one can proof that the Voronoi cell of a given lattice is already determined by the Voronoi-relevant vectors when a strictly convex norm is used. To do this, one can consider the partition of Voronoi cells into their inner and outer parts.

Theorem 4.32 *Let* $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ *be a strictly convex norm and let* $\Lambda \subseteq \mathbb{R}^n$ *be a lattice. If Conjecture 4.31 is true, it holds that*

$$\begin{aligned} \mathcal{V}(\Lambda, \|\cdot\|) &= \left\{ x \in \operatorname{span}(\Lambda) \;\middle|\; \begin{array}{l} \forall v \in \Lambda \text{ Voronoi-relevant with} \\ \text{respect to } \|\cdot\| : \|x\| \leq \|x-v\| \end{array} \right\} \\ &=: \tilde{\mathcal{V}}(\Lambda, \|\cdot\|) \text{ and} \\ \mathcal{V}^{(i)}(\Lambda, \|\cdot\|) &= \left\{ x \in \operatorname{span}(\Lambda) \;\middle|\; \begin{array}{l} \forall v \in \Lambda \text{ Voronoi-relevant with} \\ \text{respect to } \|\cdot\| : \|x\| < \|x-v\| \end{array} \right\} \\ &=: \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|). \end{aligned}$$

The idea for the proof of this theorem is to reduce the problem further and further until one gets to the statement of the above conjecture. The outline of the proof is as follows:

- Starting with some $x_0 \in \operatorname{span}(\Lambda)$ having to all Voronoi-relevant vectors a distance at least as big as the distance to 0 and assuming that x_0 is strictly closer to some other lattice vector w, one walks along the line between x_0 and 0 until a point x_1 is found which has the same distance to w as to 0 and a strictly larger distance to all Voronoi-relevant vectors. This new situation is treated by Lemma 4.37.

- Lemma 4.37 is a little bit stronger, since it already shows that the Voronoi-relevant vectors determine the strict Voronoi cell. Hence, it considers x_1 having a strictly larger distance to all Voronoi-relevant vectors than to 0, but w is closer to x than 0 or at the same distance than 0. If w is closer than 0, one walks again along the line between x_1 and 0 such that the new point x_2 has the same distance to w as to 0 and a strictly larger distance to all Voronoi-relevant vectors. This new scenario is considered by Lemma 4.36.

- For x_2 as described above, one first considers the case of the existence of some lattice vector u such that x_2 is strictly closer to u than to 0 (and w). Similar to the proof of Theorem 4.29, one walks again along the line between

x_2 and 0 to find x_3 having the same distance to some lattice vector $\tilde{w}$ as to 0, but no other lattice vector is strictly closer and all Voronoi-relevant vectors are strictly further away. This situation is analyzed in Lemma 4.34.

- Lemma 4.34 shows that there is a third lattice vector u such that x_3 has the same distance to 0, $\tilde{w}$ and u. With this, Lemma 4.33 can be applied.
- Now one has the situation where the ball around x_3 with radius $\|x_3\|$ contains no lattice points in its interior, at least three lattice points on its boundary and all Voronoi-relevant vectors are strictly outside this ball. Lemma 4.33 shows that one can move a little bit away from x_3 to some y such that the ball around y with radius $\|y\|$ contains no new lattice points except the ones that where on the boundary before. Conjecture 4.31 finally yields that y can be chosen in $\operatorname{span}(\Lambda)$ to be on the bisector between 0 and some boundary-lattice-point $\tilde{u}$ such that all other boundary-lattice-points are further away. Hence, $\tilde{u}$ must be Voronoi-relevant which contradicts that all Voronoi-relevant vectors are strictly outside the ball around x_3 with radius $\|x_3\|$.

Lemma 4.33 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. If Conjecture 4.31 is true, it holds that for every $x \in \mathcal{V}(\Lambda, \|\cdot\|)$ with $|\{u \in \Lambda \setminus \{0\} \mid \|x-u\| = \|x\|\}| \geq 2$ there exists $u \in \Lambda$ Voronoi-relevant with respect to $\|\cdot\|$ such that $\|x-u\| = \|x\|$.*

Proof. Let $k := |\{u \in \Lambda \setminus \{0\} \mid \|x-u\| = \|x\|\}|$ and use the notation $\{u \in \Lambda \setminus \{0\} \mid \|x-u\| = \|x\|\} = \{u_1, \dots, u_k\}$. Since $x \in \mathcal{V}(\Lambda, \|\cdot\|)$, it holds that $\overline{\mathcal{B}}_{\|\cdot\|,\|x\|}(x) \cap \Lambda = \{0, u_1, \dots, u_k\}$. Because Λ is discrete, there is an $\varepsilon \in \mathbb{R}_{>0}$ such that $\mathcal{B}_{\|\cdot\|,\|x\|+\varepsilon}(x) \cap \Lambda = \{0, u_1, \dots, u_k\}$. Due to Corollary 4.8, there is $\delta_1 \in \mathbb{R}_{>0}$ such that for every $y \in \mathcal{B}_{\|\cdot\|_2,\delta_1}(x)$ it holds that $|\|x\| - \|y\|| < \frac{\varepsilon}{2}$. Analogously, one finds $\delta_2 \in \mathbb{R}_{>0}$ such that $\|y-x\| = |\|x-x\| - \|y-x\|| < \frac{\varepsilon}{2}$ holds for every $y \in \mathcal{B}_{\|\cdot\|_2,\delta_2}(x)$. If Conjecture 4.31 is true, it yields for $\delta := \min\{\delta_1, \delta_2\}$ some $y \in \operatorname{span}(\Lambda) \cap \mathcal{B}_{\|\cdot\|_2,\delta}(x)$ and some $i \in \{1, \dots, k\}$ such that $\|y\| = \|y-u_i\| < \|y-u_j\|$ holds for all $j \in \{1, \dots, k\} \setminus \{i\}$. For every $z \in \overline{\mathcal{B}}_{\|\cdot\|,\|y\|}(y)$ one gets

$$\|z-x\| \leq \|z-y\| + \|y-x\| < \|y\| + \frac{\varepsilon}{2} < \left(\frac{\varepsilon}{2} + \|x\|\right) + \frac{\varepsilon}{2} = \|x\| + \varepsilon,$$

which shows $\overline{\mathcal{B}}_{\|\cdot\|,\|y\|}(y) \subseteq \mathcal{B}_{\|\cdot\|,\|x\|+\varepsilon}(x)$. This implies $\overline{\mathcal{B}}_{\|\cdot\|,\|y\|}(y) \cap \Lambda \subseteq \{0, u_1, \dots, u_k\}$. Hence, $\|y-v\| > \|y\|$ holds for all $v \in \Lambda \setminus \{0, u_i\}$, and u_i is Voronoi-relevant. □

Lemma 4.34 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. If Conjecture 4.31 is true, it holds for every $x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|) \cap \mathcal{V}(\Lambda, \|\cdot\|)$ and every $w \in \Lambda \setminus \{0\}$ that $\|x-w\| \neq \|x\|$.*

Proof. Let $x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|) \cap \mathcal{V}(\Lambda, \|\cdot\|)$ and $w \in \Lambda \setminus \{0\}$, and assume for contradiction that $\|x-w\| = \|x\|$. Since $x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$, it follows that w is not Voronoi-relevant, which further implies the existence of some $u \in \Lambda \setminus \{0, w\}$ with

$\|x-u\| \leq \|x\|$. Moreover, $x \in \mathcal{V}(\Lambda, \|\cdot\|)$ yields that $\{u \in \Lambda \mid \|x-u\| \leq \|x\|\} = \{u \in \Lambda \mid \|x-u\| = \|x\|\}$, which shows that there is some $k \in \mathbb{N}, k \geq 2$ with $k = |\{u \in \Lambda \setminus \{0\} \mid \|x-u\| = \|x\|\}|$, because Λ is discrete. By Lemma 4.33, there is a Voronoi-relevant vector $v \in \Lambda$ with $\|x-v\| = \|x\|$, which contradicts $x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$. □

For the remaining proofs, one further easy lemma is needed, which is the strictly convex variant of Lemma 4.30.

Lemma 4.35 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Then it holds for every $x \in \tilde{\mathcal{V}}(\Lambda, \|\cdot\|)$ and every $w \in \Lambda$ with $\|x-w\| < \|x\|$ that there is some $\tau \in (0,1)$ with $\|\tau x - w\| = \tau\|x\|$ and $\tau x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$.*

Proof. As in the proof of Lemma 4.30, one finds $\tau \in (0,1)$ such that $\|\tau x - w\| = \tau\|x\|$. For every Voronoi-relevant vector $v \in \Lambda$ it holds by $x \in \tilde{\mathcal{V}}(\Lambda, \|\cdot\|)$ and Lemma 2.6 that

$$\tau\|x\| \leq \|\tau x - \tau v\| = \|\tau(\tau x - v) + (1-\tau)(\tau x)\| < \max\{\|\tau x - v\|, \tau\|x\|\},$$

which implies $\|\tau x - v\| > \tau\|x\|$. Thus it is $\tau x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$. □

Lemma 4.36 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. If Conjecture 4.31 is true, it holds for every $x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$ and every $w \in \Lambda \setminus \{0\}$ that $\|x-w\| \neq \|x\|$.*

Proof. Let $x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$ and $w \in \Lambda \setminus \{0\}$, and assume for contradiction that $\|x-w\| = \|x\|$. Lemma 4.34 implies that $x \notin \mathcal{V}(\Lambda, \|\cdot\|)$, i.e., there is some $u \in \Lambda \setminus \{0\}$ with $\|x\| > \|x-u\|$. Since Λ is discrete, there is some $k \in \mathbb{N}$ with $k = |\{u \in \Lambda \mid \|x-u\| < \|x\|\}|$ and one can write $\{u \in \Lambda \mid \|x-u\| < \|x\|\} = \{u_1, \ldots, u_k\}$. Lemma 4.35 gives for every $i \in \{1, \ldots, k\}$ some $\tau_i \in (0,1)$ with $\|\tau_i x - u_i\| = \tau_i\|x\|$ and $\tau_i x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$. Let $j \in \{1, \ldots, k\}$ with $\tau_j = \min\{\tau_1, \ldots, \tau_k\}$. Lemma 4.34 applied on $\tau_j x$ and u_j yields that $\tau_j x \notin \mathcal{V}(\Lambda, \|\cdot\|)$. Hence, there is some $v \in \Lambda$ such that $\tau_j\|x\| > \|\tau_j x - v\|$. As in the proof of Theorem 4.29, (4.1) shows $v \in \{u_1, \ldots, u_k\}$, which leads to the contradiction (4.2). □

Lemma 4.37 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. If Conjecture 4.31 is true, it holds that $\tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|) \subseteq \mathcal{V}^{(i)}(\Lambda, \|\cdot\|)$.*

Proof. Let $x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$ and assume for contradiction that $x \notin \mathcal{V}^{(i)}(\Lambda, \|\cdot\|)$, i.e., there is some $w \in \Lambda \setminus \{0\}$ with $\|x\| \geq \|x-w\|$. Lemma 4.36 implies that $\|x\| > \|x-w\|$ must hold. Hence, Lemma 4.35 gives $\tau \in (0,1)$ with $\|\tau x - w\| = \tau\|x\|$ and $\tau x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$, but this contradicts Lemma 4.36 applied on τx. □

Proof of Theorem 4.32. It is clear that $\mathcal{V}(\Lambda, \|\cdot\|) \subseteq \tilde{\mathcal{V}}(\Lambda, \|\cdot\|)$ and $\mathcal{V}^{(i)}(\Lambda, \|\cdot\|) \subseteq \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$. Since it follows from Lemma 4.37 that $\mathcal{V}^{(i)}(\Lambda, \|\cdot\|) = \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$, it is only left to show that $\tilde{\mathcal{V}}(\Lambda, \|\cdot\|) \subseteq \mathcal{V}(\Lambda, \|\cdot\|)$.

Let $x \in \tilde{\mathcal{V}}(\Lambda, \|\cdot\|)$ and assume for contradiction that $x \notin \mathcal{V}(\Lambda, \|\cdot\|)$, i.e., there is some $w \in \Lambda \setminus \{0\}$ with $\|x\| > \|x-w\|$. Then Lemma 4.35 shows that

$\tau x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, \|\cdot\|)$ holds for some $\tau \in (0,1)$ with $\|\tau x - w\| = \tau\|x\|$, leading to $\tau x \in \mathcal{V}^{(i)}(\Lambda, \|\cdot\|)$ by Lemma 4.37. In particular, $\tau\|x\| < \|\tau x - w\|$ follows, which contradicts the choice of τ. □

4.4 Facets

When considering the complexity of the Voronoi cell of the origin of a given lattice, one is particularly interested in the number of facets of that Voronoi cell. In a lattice of rank m, a facet is an at least $(m-1)$-dimensional "boundary part" of the Voronoi cell, which is completely contained in at least one bisector between 0 and some other lattice vector, and it is maximal in the sense that the intersection of all these bisectors and the Voronoi cell is contained in the facet. More formally this can be stated as follows.

Definition 4.38 *For a discrete set of points $\mathcal{P} \subseteq \mathbb{R}^n$ and a norm $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$, $\mathcal{F} \subseteq \operatorname{span}(\mathcal{P})$ is a* facet *of the Voronoi cell of $a \in \mathcal{P}$ if the following four conditions hold:*

1. $\mathcal{F} \subseteq \mathcal{V}_{\|\cdot\|,\mathcal{P}}(a)$,
2. $\exists b \in \mathcal{P} \setminus \{a\} : \mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(a,b)$,
3. $\forall b \in \mathcal{P} \setminus \{a\}$ *with* $\mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(a,b)$*:* $\exists x \in \mathcal{F}\, \exists \delta \in \mathbb{R}_{>0} :$ $\mathcal{B}_{\|\cdot\|_2,\delta}(x) \cap \operatorname{span}(\mathcal{P}) \cap \mathcal{H}^{=}_{\|\cdot\|}(a,b) \subseteq \mathcal{F}$,
4. $\left(\bigcap_{\substack{b \in \mathcal{P}\setminus\{a\}: \\ \mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(a,b)}} \mathcal{H}^{=}_{\|\cdot\|}(a,b) \right) \cap \mathcal{V}_{\|\cdot\|,\mathcal{P}}(a) \subseteq \mathcal{F}$.

For every lattice and every norm, every Voronoi-relevant vector induces a facet of the Voronoi cell of the origin.

Proposition 4.39 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Then it holds for every lattice vector $v \in \Lambda$ which is Voronoi-relevant with respect to $\|\cdot\|$ that $\mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0,v)$ is a facet of the Voronoi cell of the origin.*

Proof. Let $v \in \Lambda$ be Voronoi-relevant, and define $\mathcal{F} := \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0,v)$. It is clear that $\mathcal{F}$ fulfills the first two conditions of Definition 4.38. Since v is Voronoi-relevant, there is some $x \in \operatorname{span}(\Lambda)$ such that $\|x\| = \|x - v\| < \|x - w\|$ holds for every $w \in \Lambda \setminus \{0, v\}$. Hence, $x \in \mathcal{F}$ follows, and for all $w \in \Lambda \setminus \{0,v\}$ it is $x \notin \mathcal{H}^{=}_{\|\cdot\|}(0,w)$. This means that the second condition is exactly fulfilled for v, which implies that condition four also holds. The rest of this proof verifies condition three.

Because Λ is discrete, there is some $\varepsilon \in \mathbb{R}_{>0}$ such that $\mathcal{B}_{\|\cdot\|,\|x\|+\varepsilon}(x) \cap \Lambda = \{0, v\}$. The continuity of $\|\cdot\|$ with respect to $\|\cdot\|_2$ yields $\delta_1 \in \mathbb{R}_{>0}$ such that for every

$y \in \mathcal{B}_{\|\cdot\|_2,\delta_1}(x)$ it holds that $|\|x\| - \|y\|| < \frac{\varepsilon}{2}$. From Corollary 4.8, the existence of $\delta_2 \in \mathbb{R}_{>0}$ follows such that $\|y - x\| = |\|x - x\| - \|y - x\|| < \frac{\varepsilon}{2}$ holds for every $y \in \mathcal{B}_{\|\cdot\|_2,\delta_2}(x)$. It is left to show that for $\delta := \min\{\delta_1, \delta_2\}$ it holds that $\mathcal{B}_{\|\cdot\|_2,\delta}(x) \cap \operatorname{span}(\Lambda) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v) \subseteq \mathcal{V}(\Lambda, \|\cdot\|)$.

Let $y \in \mathcal{B}_{\|\cdot\|_2,\delta}(x) \cap \operatorname{span}(\Lambda) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$. Since it holds for every $z \in \overline{\mathcal{B}}_{\|\cdot\|,\|y\|}(y)$ that

$$\|z - x\| \leq \|z - y\| + \|y - x\| < \|y\| + \frac{\varepsilon}{2} < \left(\frac{\varepsilon}{2} + \|x\|\right) + \frac{\varepsilon}{2} = \|x\| + \varepsilon,$$

it follows that $\overline{\mathcal{B}}_{\|\cdot\|,\|y\|}(y) \subseteq \mathcal{B}_{\|\cdot\|,\|x\|+\varepsilon}(x)$, which leads to $\overline{\mathcal{B}}_{\|\cdot\|,\|y\|}(y) \cap \Lambda = \{0, v\}$. Thus, it holds that $\|y\| = \|y - v\| < \|y - w\|$ for all $w \in \Lambda \setminus \{0, v\}$, and $y \in \mathcal{V}(\Lambda, \|\cdot\|)$. □

Note that the facets induced by Voronoi-relevant vectors as in the above proposition are pairwise distinct by the first paragraph of the above proof.

One would like to have that every facet of the Voronoi cell of the origin of some given lattice has a form as in the above proposition, and in particular that every facet is induced by some unique Voronoi-relevant vector. But as seen in Corollary 2.27, the Voronoi-relevant vectors might not even be sufficient to determine the Voronoi cell of the origin when a non-strictly convex norm is used. The same counterexample can now be used to specify a facet which is induced by two generalized Voronoi-relevant vectors.

Proposition 4.40 *Let* $b_1 := (1, 1)^T$ *and* $b_2 := (0, 3)^T$. *Then*

$$\mathcal{H}^{=}_{\|\cdot\|_1}(0, b_1 - b_2) \cap \mathcal{H}^{=}_{\|\cdot\|_1}(0, 2b_1 - b_2)$$

is a facet of the Voronoi cell of the origin of $\mathcal{L}(b_1, b_2)$.

Proof. Consider $x = (x_1, x_2)^T \in \mathcal{H}^{=}_{\|\cdot\|_1}(0, b_1 - b_2) \cap \mathcal{H}^{=}_{\|\cdot\|_1}(0, 2b_1 - b_2)$. Then it holds that $\|x\|_1 = \|x - (b_1 - b_2)\|_1 = \|x - (2b_1 - b_2)\|_1$, which is equivalent to

$$|x_1| + |x_2| = |x_1 - 1| + |x_2 + 2| = |x_1 - 2| + |x_2 + 1|. \tag{4.3}$$

Now distinguish three cases according to x:

1. $x_1 > 1$:

   (4.3) yields $x_1 + |x_2| = x_1 - 1 + |x_2 + 2|$, which further gives $x_2 = -\frac{1}{2}$, such that (4.3) leads to $x_1 + \frac{1}{2} = |x_1 - 2| + \frac{1}{2}$. This contradicts $x_1 > 1$.

2. $x_2 < -1$:

   (4.3) yields $|x_1| - x_2 = |x_1 - 2| - x_2 - 1$, which implies $x_1 = \frac{1}{2}$, and so (4.3) further gives $\frac{1}{2} - x_2 = \frac{1}{2} + |x_2 + 2|$. This contradicts $x_2 < -1$.

3. $x_1 \leq 1$ and $x_2 \geq -1$:

   Now, (4.3) can be written as $|x_1| + |x_2| = 3 - x_1 + x_2$.

If $x_1 < 0$ would hold, (4.3) would lead to $-x_1 + |x_2| = 3 - x_1 + x_2$, yielding $x_2 = -\frac{3}{2}$, but this contradicts $x_2 \geq -1$.

If $x_2 > 0$ would hold, (4.3) would imply $|x_1| + x_2 = 3 - x_1 + x_2$, leading to $x_1 = \frac{3}{2}$, but this contradicts $x_1 \leq 1$.

Hence, is must hold that $0 \leq x_1 \leq 1$ and $-1 \leq x_2 \leq 0$. With this, (4.3) reduces to $x_1 - x_2 = 3 - x_1 + x_2$, which is equivalent to $x_1 - x_2 = \frac{3}{2}$. From this it further follows that $x_1 \geq \frac{1}{2}$, because otherwise one would get the contradiction $-1 \leq x_2 = x_1 - \frac{3}{2} < -1$.

This case distinguishing shows that

$$\begin{aligned} &\mathcal{H}^{=}_{\|\cdot\|_1}(0, b_1 - b_2) \cap \mathcal{H}^{=}_{\|\cdot\|_1}(0, 2b_1 - b_2) \\ &\subseteq \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x_1 - x_2 = \frac{3}{2}, x_1 \in \left[\frac{1}{2}, 1\right] \right\} =: \mathcal{F}. \end{aligned} \tag{4.4}$$

Using the notation of Proposition 2.21, it is $\{(x_1, x_2)^T \in \mathcal{S}_2^{(o)} \mid x_1 > 0\} \subseteq \mathcal{F}$. Therefore, it follows from the proof of Lemma 2.24 that

$$\left\{ v \in \mathcal{L}(b_1, b_2) \setminus \{0\} \mid \mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|_1}(0, v) \right\} = \{b_1 - b_2, 2b_1 - b_2\}. \tag{4.5}$$

In particular, this shows that $\mathcal{H}^{=}_{\|\cdot\|_1}(0, b_1 - b_2) \cap \mathcal{H}^{=}_{\|\cdot\|_1}(0, 2b_1 - b_2) = \mathcal{F}$. Since Lemma 2.24 also states that $\mathcal{F} \subseteq \mathcal{V}(\mathcal{L}(b_1, b_2), \|\cdot\|_1)$, it holds that $\mathcal{F}$ fulfills the first condition of Definition 4.38 as well as the second condition by (4.5). Furthermore, condition four follows from (4.5) and (4.4). To verify condition three, let $x := \frac{3}{4}(1, -1)^T \in \mathcal{F}$ and $\delta := \frac{1}{4}$, and show $\mathcal{B}_{\|\cdot\|_2, \delta}(x) \cap \mathcal{H}^{=}_{\|\cdot\|_1}(0, b_1 - b_2) \subseteq \mathcal{F}$ as well as $\mathcal{B}_{\|\cdot\|_2, \delta}(x) \cap \mathcal{H}^{=}_{\|\cdot\|_1}(0, 2b_1 - b_2) \subseteq \mathcal{F}$.

For $y \in \mathcal{B}_{\|\cdot\|_2, \delta}(x) \cap \left(\mathcal{H}^{=}_{\|\cdot\|_1}(0, b_1 - b_2) \cup \mathcal{H}^{=}_{\|\cdot\|_1}(0, 2b_1 - b_2)\right)$, it holds that $y_1 \in \left(\frac{1}{2}, 1\right)$ and $y_2 \in \left(-1, -\frac{1}{2}\right)$. Hence, one of the equalities $|y_1| + |y_2| = |y_1 - 1| + |y_2 + 2|$ or $|y_1| + |y_2| = |y_1 - 2| + |y_2 + 1|$ already implies $y_1 - y_2 = 3 - y_1 + y_2$, which is equivalent to $y_1 - y_2 = \frac{3}{2}$. This shows that $y \in \mathcal{F}$. □

Hence, for arbitrary norms, one can conclude from Proposition 4.39 only that every Voronoi cell of the origin of a given lattice has at least as many facets as Voronoi-relevant vectors. The rest of this chapter considers strictly convex norms. First the investigation is restricted to two-dimensional lattices, and later higher dimensions are discussed.

4.4.1 Two-dimensional lattices

In the special case of lattices with dimension two and strictly convex norms, one can indeed show that every facet of the Voronoi cell of the origin has a form as given in Proposition 4.39. Notably, this means that facets can be defined more easily and precisely in this case.

Proposition 4.41 *Let $\|\cdot\| : \mathbb{R}^2 \to \mathbb{R}_{\geq 0}$ be a strictly convex norm and let $\Lambda \subseteq \mathbb{R}^2$ be a lattice. Then it holds for every facet $\mathcal{F}$ of the Voronoi cell of the origin that there is a unique Voronoi-relevant vector $v \in \Lambda$ such that $\mathcal{F} = \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$.*

Proof. For a facet $\mathcal{F} \subseteq \mathcal{V}(\Lambda, \|\cdot\|)$, there is some $v \in \Lambda \setminus \{0\}$ with $\mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ by condition two of Definition 4.38. Moreover, by the third condition of this definition, there are $x \in \mathcal{F}$ and $\delta \in \mathbb{R}_{>0}$ with $\mathcal{B}_{\|\cdot\|_2,\delta}(x) \cap \operatorname{span}(\Lambda) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v) \subseteq \mathcal{F}$.

Assume for contradiction that there is $w \in \Lambda \setminus \{0, v\}$ with $\mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(0, w)$. In particular, it holds that $x \in \mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, w)$. Theorem 2 in [6] shows that both of these bisectors are homeomorphic to lines, and for this case Theorem 2.1.2.3 in [10] states that the intersection of these bisectors is empty or a single point, where the intersection is empty if $0, v, w$ would be collinear. Thus it follows that $\mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, w) = \{x\}$ and that $0, v, w$ are non-collinear, where the latter implies $\operatorname{span}(\Lambda) = \mathbb{R}^2$. This shows that $\mathcal{B}_{\|\cdot\|_2,\delta}(x) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v) \subseteq \mathcal{F} = \{x\}$, which contradicts that $\mathcal{H}^{=}_{\|\cdot\|}(0, v)$ homeomorphic to a line by Theorem 2 in [6].

Hence, v is the only vector in $\Lambda \setminus \{0\}$ with $\mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(0, v)$. Condition four of Definition 4.38 implies $\mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \mathcal{V}(\Lambda, \|\cdot\|) = \mathcal{F}$. It is left to show that v is Voronoi-relevant. If $\|x - w\| > \|x\|$ holds for all $w \in \Lambda \setminus \{0, v\}$, it would directly follow that v is Voronoi-relevant. Thus assume that $\|x - w\| = \|x\|$ holds for some $w \in \Lambda \setminus \{0, v\}$. Then it follows as above that $\operatorname{span}(\Lambda) = \mathbb{R}^2$. Since

$$\bigcup_{u \in \Lambda \setminus \{0, v\}} \left(\mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, u)\right)$$

is countable by Theorem 2 in [6] and Theorem 2.1.2.3 in [10], there is some $y \in \mathcal{B}_{\|\cdot\|_2,\delta}(x) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v) \subseteq \mathcal{F}$ such that $y \notin \bigcup_{u \in \Lambda \setminus \{0, v\}} \left(\mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, u)\right)$. Hence, $y \in \mathcal{F} = \mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \mathcal{V}(\Lambda, \|\cdot\|)$ and $\|y\| = \|y - v\| < \|y - u\|$ for all $u \in \Lambda \setminus \{0, v\}$. Therefore, v is Voronoi-relevant. □

Corollary 4.42 *Let $\|\cdot\| : \mathbb{R}^2 \to \mathbb{R}_{\geq 0}$ be a strictly convex norm and let $\Lambda \subseteq \mathbb{R}^2$ be a lattice. Then it holds that $v \mapsto \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ is a bijection between Voronoi-relevant vectors and facets of the Voronoi cell of the origin.*

Proof. This statement follows directly from Propositions 4.39 and 4.41. □

Additionally to this desirable correspondence between facets and Voronoi-relevant vectors showing that every Voronoi cell of the origin of a given two-dimensional lattice has exactly as many facets as Voronoi-relevant vectors with respect to a strictly convex norm, it holds for the two-dimensional and strictly convex case that all these facets are connected.

Proposition 4.43 *Let $\|\cdot\| : \mathbb{R}^2 \to \mathbb{R}_{\geq 0}$ be a strictly convex norm and let $\Lambda \subseteq \mathbb{R}^2$ be a lattice. Then it holds that every facet of the Voronoi cell of the origin is connected.*

Proof. Let $\mathcal{F}$ be a facet of the Voronoi cell of the origin. By Proposition 4.41, there is a Voronoi-relevant vector $v \in \Lambda$ with $\mathcal{F} = \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$. Using Theorem 2 in [6], one finds a homeomorphism $f : \mathbb{R} \to \mathcal{H}^{=}_{\|\cdot\|}(0, v)$. Consider now $x_1, x_2 \in \mathcal{F}$ with $x_1 \neq x_2$, and define $\tau_1 := f^{-1}(x_1)$ as well as $\tau_2 := f^{-1}(x_2)$. Without loss of generality, one can assume that $\tau_1 < \tau_2$.

Now assume for contradiction that there is $\mu \in (\tau_1, \tau_2)$ such that $f(\mu) \notin \mathcal{F}$. Then it holds that $f(\mu) \notin \mathcal{V}(\Lambda, \|\cdot\|)$, which implies the existence of some $w \in \Lambda \setminus \{0, v\}$ with $\|f(\mu) - w\| < \|f(\mu)\|$. Due to $x_1, x_2 \in \mathcal{F}$ it is $\|x_1 - w\| \geq \|x_1\|$ and $\|x_2 - w\| \geq \|x_2\|$. Corollary 4.8 gives that $g : \mathbb{R}^2 \to \mathbb{R}, x \mapsto \|x - w\| - \|x\|$ is continuous, which further implies that $g \circ f$ is continuous. Furthermore, it is $g(f(\tau_1)) \geq 0$, $g(f(\tau_2)) \geq 0$ and $g(f(\mu)) < 0$. Applying the intermediate value theorem twice yields $\mu_1 \in [\tau_1, \mu)$ with $g(f(\mu_1)) = 0$ and $\mu_2 \in (\mu, \tau_2]$ with $g(f(\mu_2)) = 0$. Thus, $f(\mu_1), f(\mu_2) \in \mathcal{H}^{=}_{\|\cdot\|}(0, w) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ follows, which shows by Theorem 2 in [6] and Theorem 2.1.2.3 in [10] that $f(\mu_1) = f(\mu_2)$. Therefore, $\mu_1 = \mu_2$ must hold, which contradicts $\mu_1 < \mu < \mu_2$.

Hence, it holds that $f([\tau_1, \tau_2]) \subseteq \mathcal{F}$, and the continuous function $f|_{[\tau_1, \tau_2]} : [\tau_1, \tau_2] \to \mathcal{F}$ is a path from x_1 to x_2. □

4.4.2 Higher-dimensional lattices

If one wants to generalize the result from Proposition 4.41 to arbitrary dimensions n greater than two, one needs that the intersection of two bisectors between 0 and v, and 0 and w is $(n-2)$-dimensional as long as 0, v and w are non-collinear. This was discussed in Section 4.2. Additionally, one wants the property that two bisectors of the above form do not only touch at their $(n-2)$-dimensional intersection, but also that each bisector has parts in both halfspaces determined by the other bisector. After this is shown in the next lemma, the desired generalization of Proposition 4.41 can be stated and proven with the help of Theorem 4.18.

Lemma 4.44 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex and smooth norm, and let $V \subseteq \mathbb{R}^n$ be a subspace. If $a_1, a_2, a_3 \in V$ are non-collinear, then*

$$\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap V \nsubseteq \mathcal{H}^{\leq}_{\|\cdot\|}(a_1, a_3) \cap V \text{ and}$$
$$\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap V \nsubseteq \mathcal{H}^{\leq}_{\|\cdot\|}(a_3, a_1) \cap V.$$

Proof. Let $H \subseteq V$ be the plane spanned by a_1, a_2, a_3. Then it holds that $\frac{a_1+a_2}{2} \in H \cap \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2)$. In addition, let $K_1 := \overline{\mathcal{B}}_{\|\cdot\|, \frac{1}{2}\|a_1 - a_2\|}\left(\frac{a_1+a_2}{2}\right) \cap H$, which gives a two-dimensional strictly convex and smooth body with center point $\frac{a_1+a_2}{2}$.

Lemma 2.1.1.1 and Theorem 2.1.2.3 in [10] show for strictly convex bodies in two-dimensions and for pairwise distinct points a, b, c that there is at most one uniformly scaled and translated copy of this body that has a, b, c on its boundary, and that exactly one such copy exists if a, b, c are non-collinear and the given body is smooth. Since $2a_3 - a_1 \in H$ does not lie on the line through a_1 and a_2, Lemma 2.1.1.1 and Theorem 2.1.2.3 in [10] imply the existence of a uniformly scaled (with

center $\frac{a_1+a_2}{2}$), translated copy $K_2 \subseteq H$ of K_1 having a_1, a_2 and $2a_3 - a_1$ on its boundary. Let $p \in H$ denote the center point of K_2, i.e., the resulting point after applying the same translation from K_1 to K_2 on $\frac{a_1+a_2}{2}$. Then it holds that $\|a_1 - p\| = \|a_2 - p\| = \|2a_3 - a_1 - p\|$. The strict convexity of $\|\cdot\|$ leads to $\|a_3 - p\| = \|\frac{1}{2}(a_1 - p) + \frac{1}{2}(2a_3 - a_1 - p)\| < \|a_1 - p\|$. Thus, $p \in \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap V$, but $p \notin \mathcal{H}^{\leq}_{\|\cdot\|}(a_1, a_3)$, which shows $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap V \not\subseteq \mathcal{H}^{\leq}_{\|\cdot\|}(a_1, a_3)$.

$\frac{a_1+a_3}{2} \in H$ does not lie on the line through a_1 and a_2, such that – as above – some uniformly scaled (with center $\frac{a_1+a_2}{2}$), translated copy $K_3 \subseteq H$ of K_1 exists that has a_1, a_2 and $\frac{a_1+a_3}{2}$ on its boundary. Let $q \in H$ denote the center point of K_3. Then it follows that $\|a_1 - q\| = \|a_2 - q\| = \|\frac{a_1+a_3}{2} - q\|$. Lemma 2.6 yields

$$\begin{aligned}\|a_1 - q\| = \left\|\frac{a_1 + a_3}{2} - q\right\| &= \left\|\frac{1}{2}(a_1 - q) + \frac{1}{2}(a_3 - q)\right\| \\ &< \max\{\|a_1 - q\|, \|a_3 - q\|\},\end{aligned}$$

which shows $\|a_1 - q\| < \|a_3 - q\|$. Hence, $q \in \mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap V$, but $q \notin \mathcal{H}^{\leq}_{\|\cdot\|}(a_3, a_1)$, which shows $\mathcal{H}^{=}_{\|\cdot\|}(a_1, a_2) \cap V \not\subseteq \mathcal{H}^{\leq}_{\|\cdot\|}(a_3, a_1)$. □

Proposition 4.45 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex and smooth norm, and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. If Conjecture 4.17 is true, then it holds for every facet $\mathcal{F}$ of the Voronoi cell of the origin that there is a unique Voronoi-relevant vector $v \in \Lambda$ such that $\mathcal{F} = \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$.*

Proof. For a facet $\mathcal{F} \subseteq \mathcal{V}(\Lambda, \|\cdot\|)$, there is some $v \in \Lambda \setminus \{0\}$ with $\mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ by condition two of Definition 4.38. Moreover, by the third condition of this definition, there are $x \in \mathcal{F}$ and $\delta \in \mathbb{R}_{>0}$ with $\mathcal{B}_{\|\cdot\|_2,\delta}(x) \cap \operatorname{span}(\Lambda) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v) \subseteq \mathcal{F}$.

Assume for contradiction that there is $w \in \Lambda \setminus \{0, v\}$ with $x \in \mathcal{H}^{=}_{\|\cdot\|}(0, w)$. If Conjecture 4.17 is true, Theorem 4.18 implies that $0, v, w$ are non-collinear and that $\mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, w) \cap \operatorname{span}(\Lambda)$ is homeomorphic to $\mathbb{R}^{m-2}$, where $m \geq 2$ denotes the dimension of $\operatorname{span}(\Lambda)$. Furthermore, it follows from Theorem 2 in [6] that $\operatorname{span}(\Lambda) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ is homeomorphic to $\mathbb{R}^{m-1}$, and from Lemma 1 in [6] that every bisector of two distinct points separates its two corresponding strict halfspaces from each other. By Lemma 4.44, $\mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, w) \cap \operatorname{span}(\Lambda)$ separates $\mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \operatorname{span}(\Lambda)$ in two domains, where one domain is contained in $\mathcal{H}^{<}_{\|\cdot\|}(0, w)$ and the other in $\mathcal{H}^{<}_{\|\cdot\|}(w, 0)$. Since $x \in \mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, w) \cap \operatorname{span}(\Lambda)$, there is $y \in \mathcal{B}_{\|\cdot\|_2,\delta}(x) \cap \operatorname{span}(\Lambda) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v) \subseteq \mathcal{F} \subseteq \mathcal{V}(\Lambda, \|\cdot\|)$ with $y \in \mathcal{H}^{<}_{\|\cdot\|}(w, 0)$, which is a contradiction.

Hence, v is Voronoi-relevant and v is the only vector in $\Lambda \setminus \{0\}$ such that $\mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(0, v)$. Condition four of Definition 4.38 implies $\mathcal{H}^{=}_{\|\cdot\|}(0, v) \cap \mathcal{V}(\Lambda, \|\cdot\|) = \mathcal{F}$. □

Corollary 4.46 *Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a strictly convex and smooth norm, and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. If Conjecture 4.17 is true, then it holds that $v \mapsto \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ is a bijection between Voronoi-relevant vectors and facets of the Voronoi cell of the origin.*

Proof. This statement follows directly from Propositions 4.39 and 4.45. □

Unfortunately, one cannot hope for a connectedness result as stated in Proposition 4.43 for higher dimensions than two. The next proposition does not give a counterexample for lattices, but considers the case where the given discrete set of points has exactly four points. It finds a Voronoi cell with a facet that is not connected, although the norms fulfill strict convexity and smoothness. Hence, under the assumption of Conjecture 4.17, every Voronoi cell of the origin of a given lattice has exactly as many facets as Voronoi-relevant vectors with respect to a strictly convex and smooth norm, but the total number of connected components of the individual facets might be higher than the number of Voronoi-relevant vectors. The proof of the next proposition uses two generalizations of the classical Jordan curve theorem, which will be stated first: The Jordan-Brouwer separation theorem and the Jordan-Schoenflies theorem.

Theorem 4.47 (Jordan-Brouwer separation theorem) *Let $n \in \mathbb{N}, n \geq 2$. If $X \subseteq \mathbb{R}^n$ if homeomorphic to S^{n-1}, then $\mathbb{R}^n \setminus X$ has exactly two connected components, where one is bounded and the other unbounded, and X is the boundary of each component.*

A proof for the Jordan-Brouwer separation theorem is for example given in [11]. For the case $n = 2$, it yields the Jordan curve theorem, since every closed Jordan curve in $\mathbb{R}^2$ is homeomorphic to S^1.

Definition 4.48 *A* closed Jordan curve *in $\mathbb{R}^2$ is the image of a continuous function $\varphi : [0,1] \to \mathbb{R}^2$ such that the restriction $\varphi|_{[0,1)}$ is injective and $\varphi(0) = \varphi(1)$ holds.*

Theorem 4.49 (Jordan curve theorem) *If $K \subseteq \mathbb{R}^2$ is a closed Jordan curve, then $\mathbb{R}^2 \setminus K$ has exactly two connected components, where one is bounded and the other unbounded, and K is the boundary of each component.*

Another extension of the Jordan curve theorem is the Jordan-Schoenflies theorem, which can for example be found in [15] or [8].

Theorem 4.50 (Jordan-Schoenflies theorem) *Let $K \subseteq \mathbb{R}^2$ be a closed Jordan curve with homeomorphism $h : K \to S^1$. Then h can be extended to a homeomorphism $H : \mathbb{R}^2 \to \mathbb{R}^2$.*

In addition, if A is the unbounded component of $\mathbb{R}^2 \setminus K$ and B the bounded component, then $B \cup K$ is homeomorphic to $\{x \in \mathbb{R}^2 \mid \|x\|_2 \leq 1\}$, and $A \cup K$ is homeomorphic to $\{x \in \mathbb{R}^2 \mid \|x\|_2 \geq 1\}$.

Proposition 4.51 *Let $p \in \mathbb{N}$ with $p \geq 3$. There exists $\mathcal{P} := \{a_1, a_2, a_3, a_4\} \subseteq \mathbb{R}^3$ such that a facet of $\mathcal{V}_{\|\cdot\|_p, \mathcal{P}}(a_1)$ is not connected.*

Proof. For $p \geq 3$, the unit ball of $\|\cdot\|_p$ is not an ellipsoid. It was shown in [14] and [5] that for each convex body K in $\mathbb{R}^3$ which is not an ellipsoid there is a uniformly scaled, translated copy $\tilde{K}$ of K with $\tilde{K} \neq K$ such that $\partial\tilde{K} \cap \partial K$ is not contained in a plane. This result gives non-coplanar $a_1, a_2, a_3, a_4 \in \mathbb{R}^3$ such that $|\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_4)| \geq 2$. Together with the

strict convexity and smoothness of $\|\cdot\|_p$, Lemma 3.1.3.5 in [10] even yields that $|\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_4)| \geq 3$. Furthermore, it is proven in [9] that $|\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_4)| < \infty$.

First consider $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2)$, which is homeomorphic to $\mathbb{R}^2$ by Theorem 2 in [6]. This bisector is depicted schematically in Figure 4.4 as the background plane of this figure. By Lemma 3.1.2.6 and Corollary 3.1.2.7 in [10], there exists a homeomorphism $f : \mathbb{R} \to \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3)$. Lemma 1 in [6] yields that every bisector of two distinct points separates its two corresponding strict halfspaces from each other. By Lemma 4.44, $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3)$ separates $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2)$ in two connected domains, where one domain is contained in $\mathcal{H}^{<}_{\|\cdot\|_p}(a_1,a_3)$ and the other in $\mathcal{H}^{<}_{\|\cdot\|_p}(a_3,a_1)$. Analogously, $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_4)$ is homeomorphic to $\mathbb{R}$ and separates $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2)$ in two connected domains contained in $\mathcal{H}^{<}_{\|\cdot\|_p}(a_1,a_4)$ or $\mathcal{H}^{<}_{\|\cdot\|_p}(a_4,a_1)$, respectively. Both of these intersections with $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2)$ are also schematically illustrated in Figure 4.4. From the paragraph above it is known that the three discussed bisectors intersect in at least three, but a finite number of points. Thus, there is $k \in \mathbb{N}, k \geq 3$ such that

$$f^{-1}\left(\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_4)\right) = \{\tau_1, \tau_2, \ldots, \tau_k\}$$

with $\tau_1 < \tau_2 < \ldots < \tau_k$. For $i \in \{1,\ldots,k\}$, define $x_i := f(\tau_i)$, inducing also an ordering of the intersection points. The first three intersection points x_1, x_2, x_3 are depicted in Figure 4.4. Note that due to these intersection points, there must be two bounded domains A, B of $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2)$, where A corresponds to the part of $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3)$ between x_1 and x_2, and B corresponds to the part of $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3)$ between x_2 and x_3, as depicted in Figure 4.4. In addition, C denotes the domain of $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2)$ corresponding to the unbounded part of $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3)$ "before" x_1, which "lies on the same side" of this bisector intersection as B. More precisely, this means that either $B, C \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_1,a_3)$ or $B, C \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_3,a_1)$, and either $B, C \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_1,a_4)$ or $B, C \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_4,a_1)$. Without loss of generality, one can assume that $B, C \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_1,a_4)$, because otherwise – instead of B and C – one can consider A and the domain of $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2)$ corresponding to the part of $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3)$ "behind" x_3, which "lies on the same side" of this bisector intersection as A. Now, distinguish the following cases:

1. $B, C \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_1,a_3)$:

   In this case, B and C are both contained in the facet $\mathcal{V}_{\|\cdot\|_p,\mathcal{P}}(a_1) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2)$ of the Voronoi cell of $a_1 \in \mathcal{P} := \{a_1,a_2,a_3,a_4\}$, which is thus not connected.

2. $B, C \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_3,a_1)$:

   One can proceed analogously as above, but starting with $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3)$ and then considering $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_2)$ and $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_3) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1,a_4)$.

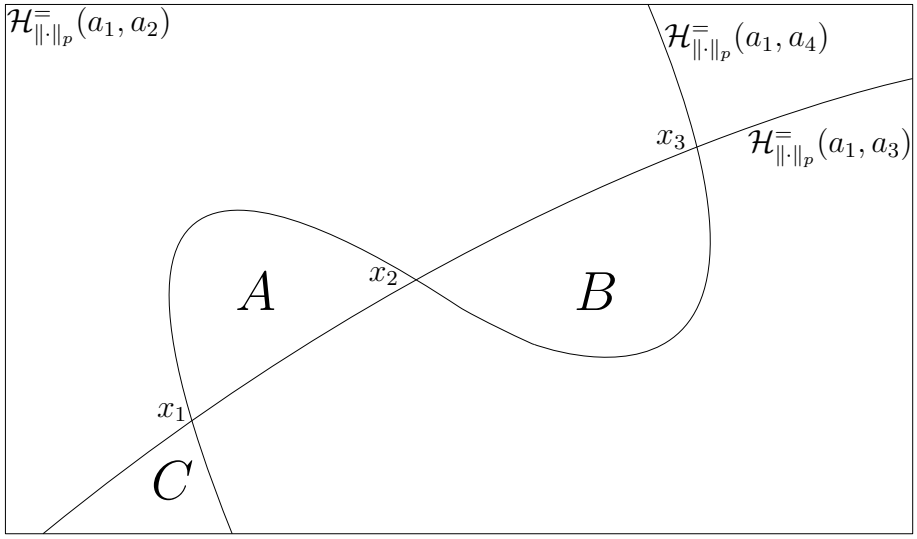


Figure 4.4: Illustration for the proof of Proposition 4.51: B and C yield not connected parts of the same facet.

This yields an analogous picture as in Figure 4.4, where the labels "$\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2)$" and "$\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3)$" are exchanged. The domains corresponding to B and C are denoted by $B_{1,3}$ and $C_{1,3}$, respectively. Since $f((\tau_2, \tau_3)) \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_4)$, it also holds that $B_{1,3}, C_{1,3} \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_4)$. Using these two domains, one can distinguish again two cases:

a) $B_{1,3}, C_{1,3} \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_2)$:

   In this case, $B_{1,3}$ and $C_{1,3}$ are both contained in the facet $\mathcal{V}_{\|\cdot\|_p,\mathcal{P}}(a_1) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3)$ of the Voronoi cell of $a_1 \in \mathcal{P}$, which is thus not connected.

b) $B_{1,3}, C_{1,3} \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_2, a_1)$:

   In this situation, one starts the above process again, but this time with $\mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_3)$. Then, one considers the intersections $\mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_3) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2)$ and $\mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_3) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_4)$, to get again an analogous picture as in Figure 4.4, where the label "$\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2)$" is replaced by "$\mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_3)$" and the label "$\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_4)$" by "$\mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_4)$". The domains corresponding to B and C are denoted by $B_{2,3}$ and $C_{2,3}$, respectively. Since $f((\tau_2, \tau_3)) \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_2, a_4)$, it also holds that $B_{2,3}, C_{2,3} \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_2, a_4)$. With these two domains, two further cases need to be distinguished:

   i. $B_{2,3}, C_{2,3} \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_2, a_1)$:

      In this case, $B_{2,3}$ and $C_{2,3}$ are both contained in the facet $\mathcal{V}_{\|\cdot\|_p,\mathcal{P}}(a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_3)$ of the Voronoi cell of $a_2 \in \mathcal{P}$, which is

thus not connected. Renaming of the points in $\mathcal{P}$ yields Proposition 4.51.

ii. $B_{2,3}, C_{2,3} \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_2)$:

The rest of this proof shows that this case cannot occur.

From $B \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2)$ it follows that $B \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_3, a_2)$. With the same argument, $B_{1,3} \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3)$ implies $B_{1,3} \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_2, a_3)$. This means that B and $B_{1,3}$ lie on two different sides of $\mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_3)$. Moreover, $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2)$, $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3)$ and $\mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_3)$ intersect in $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3)$ and separate $\mathbb{R}^3$ into six domains. These intersections and domains are illustrated in Figure 4.5 at the intersection point $f\left(\frac{\tau_2+\tau_3}{2}\right) \in \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3)$. The six domains are denoted by $G_{i,j,l} := \mathcal{H}^{<}_{\|\cdot\|_p}(a_i, a_j) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_j, a_l)$ with $i, j, l \in \{1, 2, 3\}$ pairwise distinct. The bold line parts indicate on which side of the intersection $\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3)$ the domains B, $B_{1,3}$ and $B_{2,3}$ lie, respectively.

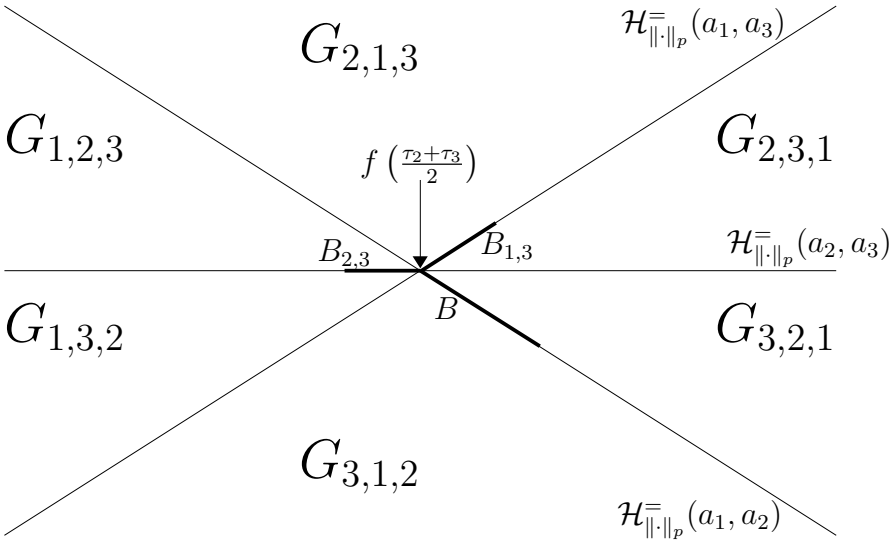


Figure 4.5: Illustration for the proof of Proposition 4.51: Situation which cannot occur.

Denote by $P_{1,2} \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_4)$ the part of this bisector intersection between x_2 and x_3, both points inclusive. Analogously, $P_{1,3} \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_4)$ and $P_{2,3} \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_3) \cap \mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_4)$ denote the parts between x_2 and x_3. Hence, for all $i, j \in \{1, 2, 3\}$ with $i < j$ there exists a homeomorphism $\psi_{i,j} : [0, 1] \to P_{i,j}$ with $\psi_{i,j}(0) = x_2$ and $\psi_{i,j}(1) = x_3$.

$P_{1,2} \cup P_{1,3} \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_4)$, so let $\varphi_1 : \mathbb{R}^2 \to \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_4)$ be a homeomorphism. Since $P_{1,2}$ and $P_{1,3}$ are paths from x_2 to x_3 without inner intersections, $K_1 := \varphi_1^{-1}(P_{1,2}) \cup \varphi_1^{-1}(P_{1,3})$ is a closed Jordan curve in $\mathbb{R}^2$. Thus it follows from the Jordan curve theorem that $\mathbb{R}^2 \setminus K_1$ has exactly two connected components, where exactly one of them is bounded and K_1 is the boundary of both components. Let the bounded component be denoted by D_1. When identifying the one-dimensional sphere S^1 with the unit circle in the complex plane,

$$h_1 : K_1 \to S^1, x \mapsto \begin{cases} e^{i\pi\psi_{1,2}^{-1}(\varphi_1(x))} & \text{, if } \varphi_1(x) \in \psi_{1,2}\left((0,1)\right), \\ e^{i\pi\left(2-\psi_{1,3}^{-1}(\varphi_1(x))\right)} & \text{, if } \varphi_1(x) \in \psi_{1,3}\left((0,1)\right), \\ 1 & \text{, if } \varphi_1(x) = x_2, \\ -1 & \text{, if } \varphi_1(x) = x_3 \end{cases}$$

gives a homeomorphism, which can be extended to a homeomorphism $H_1 : \mathbb{R}^2 \to \mathbb{R}^2$ such that $H_1(D_1) = \mathcal{B}_{\|\cdot\|_2,1}(0)$ and $H_1(\overline{D_1}) = \overline{\mathcal{B}}_{\|\cdot\|_2,1}(0)$ by the Jordan-Schoenflies theorem. Furthermore, $\overline{\mathcal{B}}_{\|\cdot\|_2,1}(0) \subseteq \mathbb{R}^2$ is homeomorphic to the two-dimensional half sphere $S^2_{1/2} := \{y = (y_1, y_2, y_3)^T \in \mathbb{R}^3 \mid \|y\|_2 = 1, y_3 \geq 0\}$, and thus also homeomorphic to the two-dimensional quarter sphere $S^2_{1/4} := \{y = (y_1, y_2, y_3)^T \in \mathbb{R}^3 \mid \|y\|_2 = 1, y_3 \geq 0, y_1 \geq 0\}$. Note that these homeomorphisms can be chosen such that $\{e^{i\pi x} \mid x \in [0,1]\}$ is identified with $\{y = (y_1, y_2, y_3)^T \in \mathbb{R}^3 \mid \|y\|_2 = 1, y_3 = 0, y_1 \leq 0\}$ (for the half sphere) or with $\{y = (y_1, y_2, y_3)^T \in \mathbb{R}^3 \mid \|y\|_2 = 1, y_1 = 0, y_3 \geq 0\}$ (for the quarter sphere), respectively, and such that $\{e^{i\pi x} \mid x \in [1,2]\}$ is identified with $\{y = (y_1, y_2, y_3)^T \in \mathbb{R}^3 \mid \|y\|_2 = 1, y_3 = 0, y_1 \geq 0\}$. Therefore, $\varphi_1(\overline{D_1}) \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_4)$ is homeomorphic to $S^2_{1/4}$ such that $P_{1,2}$ corresponds to $\{y = (y_1, y_2, y_3)^T \in \mathbb{R}^3 \mid \|y\|_2 = 1, y_1 = 0, y_3 \geq 0\}$ and $P_{1,3}$ to $\{y = (y_1, y_2, y_3)^T \in \mathbb{R}^3 \mid \|y\|_2 = 1, y_3 = 0, y_1 \geq 0\}$. Since $P_{1,2} \setminus \{x_2, x_3\} \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_3, a_1)$ and $P_{1,3} \setminus \{x_2, x_3\} \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_2, a_1)$, it follows that there is exactly one $G \in \{G^{(i)}, G^{(o)}\}$ with

$$\begin{aligned} G^{(i)} &:= G_{2,3,1} \cup \left(\mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_3) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_2, a_1)\right) \cup G_{3,2,1}, \\ G^{(o)} &:= G_{2,1,3} \cup \left(\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_3)\right) \\ &\quad \cup G_{1,2,3} \cup \left(\mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_3) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_2)\right) \\ &\quad \cup G_{1,3,2} \cup \left(\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_2)\right) \cup G_{3,1,2}, \end{aligned}$$

such that $\varphi_1(D_1) \subseteq G$; or more precisely, for every path $P \subseteq \overline{D_1}$

from $\varphi_1^{-1}(x_2)$ to $\varphi_1^{-1}(x_3)$ without inner intersections with $\varphi_1^{-1}(P_{1,2})$ and $\varphi_1^{-1}(P_{1,3})$ it holds that $\varphi_1(P) \subseteq G \cup \{x_2, x_3\}$ is a path from x_2 to x_3. If it would hold that $G = G^{(o)}$, then $\left(\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_3)\right) \cup \{x_2, x_3\}$ would contain a path in $\varphi_1(D_1) \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_4)$ from x_2 to x_3, which is not possible due to $B \subseteq \mathcal{H}^{<}_{\|\cdot\|_p}(a_3, a_1)$. Hence, $G = G^{(i)}$.

For $P_{1,2} \cup P_{2,3} \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_4)$ and $P_{1,3} \cup P_{2,3} \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_3, a_4)$ with homeomorphisms $\varphi_2 : \mathbb{R}^2 \to \mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_4), \varphi_3 : \mathbb{R}^2 \to \mathcal{H}^{=}_{\|\cdot\|_p}(a_3, a_4)$ and closed Jordan curves $K_2 := \varphi_2^{-1}(P_{1,2}) \cup \varphi_2^{-1}(P_{2,3})$, $K_3 := \varphi_3^{-1}(P_{1,3}) \cup \varphi_3^{-1}(P_{2,3})$, one proceeds analogously and finds bounded domains $D_2 \subseteq \mathbb{R}^2 \setminus K_2, D_3 \subseteq \mathbb{R}^2 \setminus K_3$ with boundaries K_2, K_3, respectively, such that

$$\varphi_2(D_2) \subseteq G_{3,1,2} \cup \left(\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_3) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_2)\right) \cup G_{1,3,2},$$
$$\varphi_3(D_3) \subseteq G_{1,2,3} \cup \left(\mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_2) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_3)\right) \cup G_{2,1,3}.$$

Let $S^2_{1/4,90^\circ}$ and $S^2_{1/4,180^\circ}$ denote two copies of $S^2_{1/4}$ that are rotated around the y_2-axes by 90° or 180°, respectively, such that $S^2 = S^2_{1/4,90^\circ} \cup S^2_{1/4,180^\circ} \cup S^2_{1/2}$. Defining homeomorphisms $h_2 : K_2 \to S^1$ and $h_3 : K_3 \to S^1$ analogously as h_1, one gets that $\varphi_1(\overline{D_1})$ is homeomorphic to $S^2_{1/4,90^\circ}$, $\varphi_2(\overline{D_2})$ is homeomorphic to $S^2_{1/4,180^\circ}$, $\varphi_3(\overline{D_3})$ is homeomorphic to $S^2_{1/2}$, and these three homeomorphisms can be "glued together" to a homeomorphism

$$\mathcal{C} := \varphi_1(\overline{D_1}) \cup \varphi_2(\overline{D_2}) \cup \varphi_3(\overline{D_3}) \to S^2.$$

The Jordan-Brouwer separation theorem implies that $\mathbb{R}^3 \setminus \mathcal{C}$ has exactly two connected components, where exactly one of the components is bounded. Let $D^{(i)}$ be the bounded component and $D^{(o)}$ be the unbounded component. Furthermore, it is $x_2, x_3 \in \mathcal{C} \subseteq \mathcal{H}^{=}_{\|\cdot\|_p}(a_1, a_4) \cup \mathcal{H}^{=}_{\|\cdot\|_p}(a_2, a_4) \cup \mathcal{H}^{=}_{\|\cdot\|_p}(a_3, a_4)$ and $f((\tau_2, \tau_3)) \subseteq D^{(i)} \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_1, a_4) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_2, a_4) \cap \mathcal{H}^{<}_{\|\cdot\|_p}(a_3, a_4)$. In particular, it is either $a_4 \in D^{(o)}$ or $a_4 \in D^{(i)}$. In both cases, it follows from the boundedness of $D^{(i)}$ that the ray from a_4 through $f\left(\frac{\tau_2+\tau_3}{2}\right)$ intersects $\mathcal{C}$ behind $f\left(\frac{\tau_2+\tau_3}{2}\right)$ at $\mu \in \mathcal{C}$. Therefore, there exists $\tau \in (0,1)$ with $f\left(\frac{\tau_2+\tau_3}{2}\right) = \tau a_4 + (1-\tau)\mu$, as well as $i \in \{1,2,3\}$ with $\|\mu - a_4\|_p = \|\mu - a_i\|_p$. Hence, using Lemma 2.6, one gets the contradiction

$$\left\| f\left(\frac{\tau_2 + \tau_3}{2}\right) - a_i \right\|_p$$

$$
\begin{aligned}
&< \left\| f\left(\frac{\tau_2+\tau_3}{2}\right) - a_4 \right\|_p = (1-\tau)\|\mu - a_4\|_p = (1-\tau)\|\mu - a_i\|_p \\
&= \left\| (\tau a_4 + (1-\tau)a_i) - f\left(\frac{\tau_2+\tau_3}{2}\right) \right\|_p \\
&= \left\| \tau\left(a_4 - f\left(\frac{\tau_2+\tau_3}{2}\right)\right) + (1-\tau)\left(a_i - f\left(\frac{\tau_2+\tau_3}{2}\right)\right) \right\|_p \\
&< \max\left\{ \left\| a_4 - f\left(\frac{\tau_2+\tau_3}{2}\right) \right\|_p, \left\| a_i - f\left(\frac{\tau_2+\tau_3}{2}\right) \right\|_p \right\} \\
&= \left\| a_4 - f\left(\frac{\tau_2+\tau_3}{2}\right) \right\|_p .
\end{aligned}
$$

□

5 Conclusion

The main question of this thesis was answered in Chapters 2 and 3: By Proposition 3.7, there are at most $\left(1 + 4\frac{\mu(\Lambda,\|\cdot\|)}{\lambda_1(\Lambda,\|\cdot\|)}\right)^n$ generalized Voronoi-relevant vectors in every lattice Λ with respect to an arbitrary norm $\|\cdot\|$. This bound depends on the lattice dimension n and two additional lattice parameters. Thus, it is not sufficient for the algorithm by Micciancio and Voulgaris, which needs an upper bound of the form $2^{O(n)}$. Table 5.1 summarizes when such a bound exists (cf. [1], Theorem 2.4, Corollary 3.6, Theorem 2.28). The constructions in Corollary 3.6

norm	$n = 2$	$n \geq 3$
Euclidean	$2(2^n - 1)$	
strictly convex	$2(2^n - 1)$	no bound solely depending on dimension
arbitrary $\star$	no bound solely depending on dimension	

Table 5.1: Upper bounds for the number of Voronoi-relevant vectors (first two rows) and generalized Voronoi-relevant vectors (last row, marked by $\star$) with respect to different norms and lattice dimensions n.

and Theorem 2.28 use the 3-norm and the 1-norm, but they should be extendable to p-norms for $p \in (1, \infty), p \neq 2$ and the ∞-norm, respectively. Hence, one cannot easily generalize the algorithm by Micciancio and Voulgaris with the same time and space complexity of $2^{O(n)}$ to the 3-norm or the 1-norm and probably neither to any p-norm for $p \in [1, \infty], p \neq 2$.

The last chapter gives several directions for future work: On the one hand, further analysis of the Conjectures 4.17 and 4.31 is required. Alternatively, trying to discover proofs for the corresponding Theorems 4.18 and 4.32 without depending on these two conjectures seems worthwhile. Note that it is also sufficient for Proposition 4.45 and Corollary 4.46 to show Theorem 4.18 instead of Conjecture 4.17. On the other hand, the study of bisectors and their intersections in general dimensions seems to be of fundamental importance but not well understood. Thus, one possible research direction is the further investigation of these objects. The results about bisectors described in this work have an analytic point of view, but it might also be interesting to study bisectors in an algebraic manner. For this, one could start with the examination of the algebraic varieties given by bisectors of p-norms.

Bibliography

[1] Erik Agrell, Thomas Eriksson, Alexander Vardy, and Kenneth Zeger. Closest Point Search in Lattices. In *IEEE Transactions on Information Theory*, volume 48, pages 2201–2214. IEEE Information Theory Society, 2002.

[2] Miklós Ajtai. The Shortest Vector Problem in L_2 is NP-hard for Randomized Reductions. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 10–19. Association for Computing Machinery, 1998.

[3] James O. Berger. *Statistical Decision Theory and Bayesian Analysis*. Springer Science & Business Media, 1985.

[4] John William Scott Cassels. *An Introduction to the Geometry of Numbers*, volume 99 of *Classics in Mathematics*. Springer-Verlag Berlin Heidelberg, 1997.

[5] P. R. Goodey. Homothetic ellipsoids. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 93, pages 25–34. Cambridge University Press, 1983.

[6] Ákos G. Horváth. On bisectors in Minkowski normed spaces. In *Acta Mathematica Hungarica*, volume 89, pages 233–246. Springer, 2000.

[7] Michael Kaib and Claus P. Schnorr. The Generalized Gauss Reduction Algorithm. In *Journal of Algorithms*, volume 21, pages 565–578. Elsevier, 1996.

[8] L. Christine Kinsey. *Topology of surfaces*. Springer Science & Business Media, 1993.

[9] Ngoc-Minh Lê. On voronoi diagrams in the L_p-metric in $\mathbb{R}^{D_*}$. In *Discrete & Computational Geometry*, volume 16, pages 177–196. Springer, 1996.

[10] Lihong Ma. *Bisectors and Voronoi diagrams for convex distance functions*. PhD thesis, FernUniversität Hagen, Fachbereich Informatik, 2000.

[11] Ib H. Madsen and Jørgen Tornehave. *From Calculus to Cohomology: De Rham cohomology and characteristic classes*. Cambridge University Press, 1997.

[12] Daniele Micciancio and Shafi Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*. Kluwer Academic Publishers, 2002.

[13] Daniele Micciancio and Panagiotis Voulgaris. A Deterministic Single Exponential Time Algorithm for Most Lattice Problems based on Voronoi Cell Computations. In *SIAM Journal on Computing*, volume 42, pages 1364–1391. Society for Industrial and Applied Mathematics, 2013.

[14] A. V. Shaĭdenko. Some characteristic properties of the ellipsoid. In *Sibirsk Mat. Ž*, volume 21, pages 232–234, 1980. In Russian.

[15] Carsten Thomassen. The Jordan-Schönflies Theorem and the Classification of Surfaces. In *American Mathematical Monthly*, volume 99, pages 116–130. Mathematical Association of America, 1992.