Abstract

Motivated by the deterministic single exponential time algorithm of Micciancio and Voulgaris for solving the shortest and closest vector problem for the Euclidean norm, we study the geometry and complexity of Voronoi cells of lattices with respect to arbitrary norms. On the positive side, we show for strictly convex and smooth norms that the geometry of Voronoi cells of lattices in any dimension is similar to the Euclidean case, i.e., the Voronoi cells are defined by the so-called Voronoi-relevant vectors and the facets of a Voronoi cell are in one-to-one correspondence with these vectors. On the negative side, we show that Voronoi cells are combinatorially much more complicated for arbitrary strictly convex and smooth norms than in the Euclidean case. In particular, we construct a family of three-dimensional lattices whose number of Voronoi-relevant vectors with respect to the $\ell_3$-norm is unbounded. Since the algorithm of Micciancio and Voulgaris and its run time analysis crucially depend on the fact that for the Euclidean norm the number of Voronoi-relevant vectors is single exponential in the lattice dimension, this indicates that the techniques of Micciancio and Voulgaris cannot be extended to achieve deterministic single exponential time algorithms for lattice problems with respect to arbitrary $\ell_p$-norms.

1 Introduction

Motivated by recent algorithms to solve problems in the geometry of numbers, we study the geometry and complexity of Voronoi cells of lattices with respect to arbitrary norms. To explain this in more detail, first we need to review the history and the current state of the art for the computational complexity of lattice problems.

A lattice is a discrete additive subgroup $\Lambda$ of $\mathbb{R}^n$. Its rank is the dimension of the $\mathbb{R}$-subspace it spans. For simplicity, we only consider lattices of full rank, i.e., with rank $n$. Each such lattice $\Lambda$ has a basis $(b_1, \ldots, b_n)$ such that $\Lambda$ equals

$$\mathcal{L}(b_1, \ldots, b_n) := \left\{ \sum_{i=1}^{n} z_ib_i \bigg| z_1, \ldots, z_n \in \mathbb{Z} \right\}.$$

The most important computational lattice problems are the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). Both problems have numerous applications in combinatorial optimization, complexity theory, and
cryptography. In SVP, given a lattice $\Lambda = \mathcal{L}(b_1, \ldots, b_n)$, a non-zero vector in $\Lambda$ with minimum length has to be computed. In CVP, given a lattice $\Lambda$ and a target vector $t \in \mathbb{R}^n$, a vector in $\Lambda$ with minimum distance to $t$ has to be computed. Both problems can be defined for any (fixed) norm on $\mathbb{R}^n$. Both, SVP and CVP are best studied for the Euclidean norm, but for applications other norms like polyhedral norms or general $\ell_p$-norms are important as well. An example is Lenstra’s celebrated polynomial time algorithm for integer programming in fixed dimension \cite{Lenstra1983} and subsequent improvements. For the Euclidean norm and many other norms, SVP and CVP are NP-complete (in case of SVP under randomized reductions) \cite{Kannan1984, Gaspard2016}. In fact, approximating SVP and CVP within constant factors is NP-hard \cite{Kannan1984, Gaspard2016}. Hence we cannot expect exact or almost exact polynomial time algorithms for either problem.

Despite this, the state of the art for exact or almost exact algorithms for SVP or CVP has seen tremendous progress in the last 20 years. In the following we only review the main results not relying on heuristic assumptions. We remark, however, that even under reasonable heuristic assumptions the best running times for SVP and CVP are single exponential in the rank of the lattice. In 1987, Kannan gave algorithms to solve SVP and CVP exactly for the Euclidean norm \cite{Kannan1984}. With improvements by Helfrich \cite{Helfrich1994} and with a refined analysis due to Hanrot and Stehlé \cite{HanrotStehle2007}, Kannan’s algorithms are known to run in time $n^{n/2} \cdot s^{O(1)}$ and $n^{n/2} \cdot s^{O(1)}$ for SVP and CVP, respectively. Here $s$ denotes the input size of the input instance. The space complexity of Kannan’s algorithms is polynomial. In a seminal paper in 1998, Ajtai, Kumar, and Sivakumar \cite{AKS1998} gave a randomized algorithm with running time $2^{O(n)} \cdot s^{O(1)}$ for the exact version of SVP with respect to the Euclidean norm. For CVP, Ajtai et al. obtain a $(1 + \epsilon)$-approximation algorithm for any $\epsilon > 0$\cite{AjtaiKumarSivakumar1998}. The algorithm again works for the Euclidean norm and has running time $2^{O(n/\epsilon)} \cdot s^{O(1)}$. Blömer and Naewe generalized the algorithms of Ajtai et al. to arbitrary $\ell_p$-norms \cite{BlomerNaewe1999}. For SVP the algorithm was further generalized to arbitrary norms in \cite{BMP2000}. An extension of the AKS algorithm to so called semi-norms was presented in \cite{Blomer2000}. This extension works both for SVP and for the $(1 + \epsilon)$-approximate version of CVP. The algorithms by Ajtai et al. and all subsequent generalizations are randomized, i.e., the algorithms return the desired results only with probability close to 1. In \cite{DPS2014} the authors use completely different techniques to obtain, among other results, an algorithm that solves SVP exactly, always outputs a correct result, i.e., a shortest vector, and has expected running time single exponential in $n$. Based on the techniques in \cite{DPS2014, DRS2015, DRS1995} (to be discussed below), in \cite{DMV2010} a deterministic algorithm for SVP with single exponential running time is presented. Using similar techniques, \cite{BSS2005} gives a deterministic algorithm for the $(1 + \epsilon)$-approximate version of CVP with running time $O(1 + \epsilon)^n$. The algorithms in \cite{DRS2015} and in \cite{BSS2005} work for arbitrary norms. In 2014, Regev et al. gave a randomized exact algorithm for SVP based on sampling of discrete Gaussian distributions on lattices with time and space complexity $2^{n + o(n)} \cdot s^{O(1)}$ \cite{Regev2014}. In 2015, this technique has been improved and generalized to obtain an exact algorithm for CVP also with time and space complexity $2^{n + o(n)} \cdot s^{O(1)}$\cite{MicciancioVoulgaris2010}. These algorithms only work for the Euclidean norm. Finally, and most relevant to this work, in 2010 Micciancio and Voulgaris \cite{MicciancioVoulgaris2010} gave deterministic algorithms for SVP and CVP with time and space complexity $2^n s^{\tilde{O}(1)}$ and $2^n s^{\tilde{O}(1)}$. The algorithms by Micciancio and Voulgaris only work for the Euclidean norm.

As can be seen from our discussion, the algorithm in \cite{MicciancioVoulgaris2010} is the only deter-
ministic, single exponential time algorithm solving CVP exactly. Hence the main open question in this area is whether there exists a deterministic single exponential time and space algorithms for CVP for norms other than the Euclidean norm. In particular, Micciancio and Voulgaris already asked whether their techniques can be generalized and extended to obtain such an algorithm. One of the main results in this paper shows that, without significant modifications and extensions, this is unlikely to be possible.

To explain this in more detail we need to recall the basic outline of the algorithms by Micciancio and Voulgaris. Their algorithms are based on a recursive computation of the Voronoi cell or Voronoi region of a lattice, i.e., the centrally symmetric set of points closer to the origin than to any other lattice point. For the Euclidean norm the Voronoi region is a convex polytope whose facets are in a one-to-one correspondence with so-called Voronoi-relevant vectors, i.e., lattice points $v$ such that there is a point in $\mathbb{R}^n$ that has the same distance to the origin and to $v$ and this distance is strictly smaller than to any other lattice vector. Hence, the Voronoi-relevant vectors define the Voronoi cell. Moreover, it is well-known for the Euclidean norm that for any lattice in $\mathbb{R}^n$ the number of Voronoi-relevant lattice points is bounded by $2(2^n - 1)$ [3]. This bound is essential for the time and space complexity of Micciancio’s and Voulgaris’ algorithm. In this paper, we show that the structure of Voronoi regions of lattices with respect to many norms resembles the situation in the Euclidean case. However, we also show that already in $\mathbb{R}^3$ and for the $\ell_3$-norm, the complexity of the Voronoi region differs dramatically from the Euclidean case. More precisely, we construct a sequence of lattices $\Lambda_k, k \in \mathbb{Z}_{>0}$, such that $\Lambda_k$ has at least $k$ Voronoi-relevant vectors. Hence, without further restrictions and significant modifications it seems unlikely that the techniques by Micciancio and Voulgaris can be generalized to obtain deterministic single exponential time and space algorithms for SVP and CVP with respect to norms other than the Euclidean norm. Note, however, that the deterministic single exponential time algorithms for SVP and approximate versions of CVP with respect to norms other than the Euclidean norm, rely among other techniques, on Micciancio’s and Voulgaris’ algorithm.

Although we present our construction for lattices with an unbounded number of Voronoi-relevant vectors only for the $\ell_3$-norm, it will be clear from the construction that similar results hold for more general norms, e.g., all $\ell_p$-norms for $p > 2$.

## 2 Overview of Results and Roadmap

The Voronoi cell of the origin of a given lattice $\Lambda \subseteq \mathbb{R}^n$ is the set of all points in $\mathbb{R}^n$ that are at least as close to 0 than to any other lattice point, with respect to the used norm. Formally, this is defined as

$$V(\Lambda, \|\cdot\|) := \{x \in \mathbb{R}^n \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$

We show that not all lattice vectors have to be considered in the definition of Voronoi cells, but that a finite set of vectors is enough, namely for strictly convex and smooth norms the Voronoi-relevant vectors are sufficient. For general norms, weak Voronoi-relevant vectors have to be considered.

**Definition 1.** 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 $x \in \mathbb{R}^n$ such that $\|x\| = \|x - v\| < \|x - w\|$ holds for all $w \in \Lambda \setminus \{0, v\}$.

• A lattice vector $v \in \Lambda \setminus \{0\}$ is a weak Voronoi-relevant vector if there is some $x \in \mathbb{R}^n$ such that $\|x\| = \|x - v\| \leq \|x - w\|$ holds for all $w \in \Lambda$.

A norm $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ is said to be strictly convex if for all distinct $x, y \in \mathbb{R}^n$ with $\|x\| = \|y\|$ and all $\tau \in (0, 1)$ we have that $\|\tau x + (1 - \tau)y\| < \|x\|$. We give a formal definition for smooth norms in Section [4]. Now, we formulate our first result on Voronoi cells precisely.

**Theorem 2.** For every lattice $\Lambda \subseteq \mathbb{R}^n$ and every strictly convex and smooth norm $\|\cdot\|$, the Voronoi cell $V(\Lambda, \|\cdot\|)$ is equal to

$$\hat{V}(\Lambda, \|\cdot\|) := \left\{ x \in \mathbb{R}^n \mid \forall v \in \Lambda \text{ Voronoi-relevant with respect to } \|\cdot\|: \|x\| \leq \|x - v\| \right\}.$$  

For two-dimensional lattices, smoothness of the norm is not necessary.

We will see that theorem 2 does not hold for non-strictly convex norms, not even in two dimensions. Instead we prove the following weaker result.

**Theorem 3.** For every lattice $\Lambda \subseteq \mathbb{R}^n$ and every norm $\|\cdot\|$, we have that the Voronoi cell $V(\Lambda, \|\cdot\|)$ is equal to

$$\hat{V}^{(g)}(\Lambda, \|\cdot\|) := \left\{ x \in \mathbb{R}^n \mid \forall v \in \Lambda \text{ weak Voronoi-relevant with respect to } \|\cdot\|: \|x\| \leq \|x - v\| \right\}.$$  

When considering the complexity of the Voronoi cell of the origin of a given lattice, we are particularly interested in the number of facets of that Voronoi cell. Intuitively, such a facet is an at least $(n-1)$-dimensional boundary part of the Voronoi cell containing all points that have the same distance to 0 as to some fixed non-zero lattice vector. For the formal definition we denote for a given norm $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$, a point $x \in \mathbb{R}^n$ and $\delta \in \mathbb{R}_{>0}$, the (open) $\|\cdot\|$-ball around $x$ with radius $\delta$ by $B_{\|\cdot\|}(x) := \{ y \in \mathbb{R}^n \mid \|y - x\| < \delta \}$. The bisector of $a, b \in \mathbb{R}^n, a \neq b$ is $H_{\|\cdot\|}(a, b) := \{ x \in \mathbb{R}^n \mid \|x - a\| = \|x - b\| \}$.

**Definition 4.** For a lattice $\Lambda \subseteq \mathbb{R}^n$ and a norm $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$, a facet of the Voronoi cell of the origin is a subset $F \subseteq V(\Lambda, \|\cdot\|)$ such that

1. $\exists v \in \Lambda \setminus \{0\} : F = V(\Lambda, \|\cdot\|) \cap H_{\|\cdot\|}(0, v)$,
2. $\exists x \in F \exists \delta \in \mathbb{R}_{>0} : B_{\|\cdot\|, \delta}(x) \cap H_{\|\cdot\|}(0, v) \subseteq F$,
3. there is no $w \in \Lambda \setminus \{0\}$ such that $F \subseteq V(\Lambda, \|\cdot\|) \cap H_{\|\cdot\|}(0, w)$.

We will see for strictly convex and smooth norms (or only strictly convex norms in the two-dimensional case) that the first two conditions imply the third condition. For non-strictly convex norms it can happen that $(n-1)$-dimensional bisector parts of a Voronoi cell are contained in each other (see fig. [8]). For every norm we show as our first result on facets that the complexity of Voronoi cells is lower bounded by the number of Voronoi-relevant vectors, i.e., every Voronoi-relevant vector defines a facet of the Voronoi cell.
Proposition 5. 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 lattice vector $v \in \Lambda$ which is Voronoi-relevant with respect to $\| \cdot \|$ we have that $V(\Lambda, \| \cdot \|) \cap H^\perp_{\| \cdot \|}(0, v)$ is a facet of the Voronoi cell of the origin.

The next theorem shows that for every smooth and strictly convex norm there is a 1-to-1 correspondence between Voronoi-relevant vectors and the facets of a Voronoi cell.

Theorem 6. For every lattice $\Lambda$ and every strictly convex and smooth norm $\| \cdot \|$, we have that $v \mapsto V(\Lambda, \| \cdot \|) \cap H^\perp_{\| \cdot \|}(0, v)$ is a bijection between Voronoi-relevant vectors and facets of the Voronoi cell of the origin. For two-dimensional lattices, smoothness of the norm is not necessary.

For the Euclidean norm, every lattice in $\mathbb{R}^n$ has at most $2(2^n - 1)$ Voronoi-relevant vectors. By the above bijection, this is also a bound for the complexity of Voronoi cells under the Euclidean norm. Unfortunately, for other norms and lattices in dimension three and higher, we cannot expect the complexity of Voronoi cells to depend only on the dimension and possibly the norm. In fact, already for $n = 3$ and the $\ell_3$-norm we obtain a family of lattices with arbitrarily many Voronoi-relevant vectors. In particular, this implies that Micciancio’s and Voulgaris’ algorithm cannot be directly generalized to $\ell_p$-norms (for $p \in (1, \infty)$) without exceeding its single exponential running time.

Theorem 7. For every $k \in \mathbb{Z}_{>0}$, there is a lattice $\Lambda_k \subseteq \mathbb{R}^3$ with at least $k$ Voronoi-relevant vectors with respect to the (smooth and strictly convex) $\ell_3$-norm $\| \cdot \|_3$.

Corollary 8. For lattices $\Lambda \subseteq \mathbb{R}^n$, $n \geq 3$ and a strictly convex and smooth norm $\| \cdot \|$, the number of Voronoi-relevant vectors of $\Lambda$ with respect to $\| \cdot \|$ cannot be bounded by a function only depending on $n$ and $\| \cdot \|$.

In $\mathbb{R}^2$, Voronoi cells with respect to strictly convex norms behave as Voronoi cells with respect to the Euclidean norm $\| \cdot \|_2$. This we have seen geometrically in theorems 2 and 3. In the next theorem we show that for strictly convex norms Voronoi cells of lattices in $\mathbb{R}^2$ have at most six facets. Note that this coincides with the upper bound $2(2^n - 1)$ for the complexity of Voronoi-cells of lattices in $\mathbb{R}^2$ with respect to the Euclidean norm.

Theorem 9. For every lattice $\Lambda \subseteq \mathbb{R}^2$ and every strictly convex norm $\| \cdot \|$, we have that $\Lambda$ has either 4 or 6 Voronoi-relevant vectors with respect to $\| \cdot \|$. More precisely, if $(b_1, b_2)$ is a Gauss-reduced basis for $\Lambda$, 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.

Under non-strictly convex norms on $\mathbb{R}^2$, the Voronoi-relevant vectors generally do not define the Voronoi cell. Instead we can use weak Voronoi-relevant vectors to describe Voronoi cells (theorem 3), but the number of these vectors is generally not bounded by a constant.

Theorem 10. For every $k \in \mathbb{Z}_{>0}$, there is a lattice $\Lambda_k \subseteq \mathbb{R}^2$ with at least $k$ weak Voronoi-relevant vectors with respect to $\| \cdot \|_1$.
At least we can give an upper bound for the number of weak Voronoi-relevant vectors with respect to arbitrary norms using more refined lattice parameters than simply the lattice dimension. More precisely, in addition to the dimension, the upper bound depends on the ratio of the covering radius \( \mu(\Lambda, \|\cdot\|) := \inf \{ d \in \mathbb{R}_{\geq 0} \mid \forall x \in \mathbb{R}^n \exists v \in \Lambda : \|x - v\| \leq d \} \) and the length \( \lambda_1(\Lambda, \|\cdot\|) \) of a shortest non-zero lattice vector.

Proposition 11. For every lattice \( \Lambda \subseteq \mathbb{R}^n \) and every norm \( \|\cdot\| \), the lattice \( \Lambda \) has at most \( \left(1 + 4 \frac{\mu(\Lambda, \|\cdot\|)}{\lambda_1(\Lambda, \|\cdot\|)} \right)^n \) weak Voronoi-relevant vectors with respect to \( \|\cdot\| \).

Also this result seems to be folklore, below we provide a proof for it. An important open question is if one actually can construct a family of lattices \( \Lambda_n \subseteq \mathbb{R}^n \) whose number of (weak) Voronoi-relevant vectors grows as \( \Theta \left( \left(\frac{\mu(\Lambda, \|\cdot\|)}{\lambda_1(\Lambda, \|\cdot\|)} \right)^n \right) \).

Organization Since we want to give the proof for our main result theorem 7 as soon as possible, we start by studying the combinatorial questions in Section 3. First, we prove theorem 11 and directly afterwards theorem 7 in Section 3.1. In Section 3.2, we focus on two-dimensional lattices and show theorems 9 and 10. The second part of this paper in Section 4 considers geometrical aspects of Voronoi cells. In Section 4.1, we discuss results which hold for all norms, as theorems 3 and 5. Finally, we study strictly convex norms in Section 4.2 and show theorems 2 and 6.

3 Combinatorics

A first approach to the number of (weak) Voronoi-relevant vectors is stated in theorem 11 which in particular implies that there are always finitely many weak Voronoi-relevant vectors.

Proof of theorem 11. The proof uses an easy packing argument. By the definition of weak Voronoi-relevant vectors it holds for every such vector \( v \) that \( \|v\| \leq 2\mu(\Lambda, \|\cdot\|) \). Thus, we have

\[
\bigcup_{v \in \Lambda \text{ weak Voronoi-relevant}} B_{\|\cdot\|, \frac{\lambda_1(\Lambda, \|\cdot\|)}{2}}(v) \subseteq B_{\|\cdot\|, 2\mu(\Lambda, \|\cdot\|) + \lambda_1(\Lambda, \|\cdot\|)}(0),
\]

where the left union is disjoint by definition of \( \lambda_1 \). This shows that the number of weak Voronoi-relevant vectors is upper bounded by

\[
\frac{\text{vol} \left( B_{\|\cdot\|, 2\mu(\Lambda, \|\cdot\|) + \lambda_1(\Lambda, \|\cdot\|)}(0) \right)}{\text{vol} \left( B_{\|\cdot\|, \frac{\lambda_1(\Lambda, \|\cdot\|)}{2}}(0) \right)} = \left( 1 + 4 \frac{\mu(\Lambda, \|\cdot\|)}{\lambda_1(\Lambda, \|\cdot\|)} \right)^n. \quad \Box
\]

3.1 Three Dimensions

Now we prove theorem 7 by constructing a family of three-dimensional lattices such that their number of Voronoi-relevant vectors with respect to the \( \ell_3 \)-norm \( \|\cdot\|_3 \) is not bounded from above by a constant. For this, we exploit some geometric properties of the unit ball of the \( \ell_3 \)-norm, which we describe first informally before giving the formal proof.
Figure 1 shows the closed unit ball of the \( \ell_3 \)-norm with and without intersections with different planes. The unit ball can be intuitively seen as a cube with rounded edges and corners. Throughout the following description, we will make often use of this intuitive notion of an edge of the unit ball. Let the \( x \)-, \( y \)- and \( z \)-axis denote the axes of the standard three-dimensional coordinate system which are spanned by the standard basis vectors \( e_1 \), \( e_2 \) and \( e_3 \) of \( \mathbb{R}^3 \), respectively. As seen in figs. 1c and 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 \( \ell_3 \)-norm in two dimensions. But when such a plane is rotated around the \( y \)-axis by 45°, as in figs. 1e to 1h, it intersects the three-dimensional unit ball of the \( \ell_3 \)-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 is the intersection.

The lattices in our lattice family will be rotations of \( \mathcal{L}(e_1, e_2, M e_3) \), where \( M \in \mathbb{Z}_{\geq 0} \) is chosen sufficiently large. These rotations will depend on a parameter \( m \in \mathbb{Z}_{\geq 0} \) 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 \( M e_3 \), respectively. The intuition is to rotate \( \mathcal{L}(e_1, e_2, M e_3) \) such that the plane spanned by 0, \( b_{m,1} \) and \( b_{m,2} \) intersects a scaled and translated unit ball of the \( \ell_3 \)-norm as in figs. 1g and 1h. Moreover, the line between 0 and \( b_{m,1} + m b_{m,2} \) should lie directly on the edge of the 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 fig. 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 \( b_{m,1} + m b_{m,2} \) are the only lattice points in the ball, and if they in fact lie on the boundary of the ball, it follows that \( b_{m,1} + m b_{m,2} \) is a Voronoi-relevant vector, where the center of the ball serves as \( x \) in theorem 1 of Voronoi-relevant vectors.

This shows already an important difference between two- and three-dimensional lattices: by theorem 1, lattice vectors of the form \( b_{m,1} + m b_{m,2} \) (for large \( m \)) cannot be Voronoi-relevant in two-dimensional lattices with respect to strictly convex norms.

With these figurative ideas at hand, the rotations of \( \mathcal{L}(e_1, e_2, M e_3) \) will now be described formally. These modifications of the standard lattice are also illustrated in figs. 3 to 6 for the case \( m = 3 \). First, \( \mathcal{L}(e_1, e_2, M e_3) \) is rotated around the \( z \)-axis until \( e_1 + me_2 \) lies on the \( y \)-axis, because all edges of the unit ball are 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 \( R_z \mathcal{L}(e_1, e_2, M e_3) \) 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 \( \ell_3 \)-norm at one of their edges. The second
Figure 1: $B_{\| \cdot \|_{3,1}}(0)$ intersecting different planes.

Figure 2: Plane spanned by $0, b_{m,1}$ and $b_{m,2}$ intersects an $\ell_3$-ball at an edge such that the line between $0$ and $b_{m,1} + mb_{m,2}$ lies on the edge (cf. fig. 1h).
Figure 3: $\mathcal{L}(e_1, e_2, e_3)$.

Figure 4: $\mathcal{L}(e_1, e_2, Me_3)$: Note that $M$ is so large that this figure is not scaled properly.
Figure 5: $R_z \mathcal{L}(e_1, e_2, Me_3)$. 
Figure 6: $\mathcal{L}_m = R_y R_z \mathcal{L}(e_1, e_2, M e_3)$. 
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 \( L_m := L_y R_z L(e_1, e_2, M e_3) \) is spanned by

\[ b_{m,1} := R_y R_z e_1 = \begin{pmatrix} \frac{m}{\sqrt{2}\sqrt{m^2+1}} \\ \frac{-m}{\sqrt{m^2+1}} \\ \frac{-m}{\sqrt{m^2+1}} \end{pmatrix}, \]
\[ b_{m,2} := R_y R_z e_2 = \begin{pmatrix} \frac{-\sqrt{2|m^2+1|}}{m} \\ \frac{1}{\sqrt{m^2+1}} \\ \frac{1}{\sqrt{m^2+1}} \end{pmatrix} \text{ and} \]
\[ b_{m,3} := M R_y R_z e_3 = \begin{pmatrix} \frac{m}{\sqrt{2}} \\ 0 \\ \frac{m}{\sqrt{2}} \end{pmatrix}. \]

Using an appropriate scaling and translation of the unit ball, the situation in fig. 2 can be reached. As already mentioned, this can be used to show that \( b_{m,1} + k b_{m,2} \) is Voronoi-relevant if \( M \) is sufficiently large, which is in contrast to the case of two-dimensional lattices. For us it is more important though that Theorem 12.

**Proof of theorem 12**

This follows from the fact that the function \( f : \mathbb{R} \to \mathbb{R} \geq 0, x \mapsto |C + x|^3 + |D - x|^3 \) has a global minimum at \( \frac{D - C}{2} \) with function value \( \frac{1}{4}|D + C|^3 \) if \( C, D \in \mathbb{R} \) and \( D \neq -C \).

**Proof of theorem 12**

For \( k, m \in \mathbb{Z} \) with \( 2 \leq k \leq \sqrt{m} \), we have that \( b_{m,1} + k b_{m,2} \) is Voronoi-relevant in \( L_m \) with respect to \( \| \cdot \|_3 \).

In the proof of this statement, we need to calculate the distance between some \( v \in \mathbb{R}^3 \) and the plane spanned by \( e_1 \) and \( e_2 \) after this plane is translated along the \( z \)-axis and rotated around the \( y \)-axis by 45°.

**Lemma 13.** For \( C \in \mathbb{R} \) and \( v = (\alpha, \beta, \gamma)^T \in \mathbb{R}^3 \), the unique point in \( E_C := R_y(\mathbb{R} e_1 + \mathbb{R} e_2 + C e_3) \) which is closest to \( v \) with respect to \( \| \cdot \|_3 \) is \( R_y(\frac{\alpha - \gamma}{\sqrt{2}}, \beta, C)^T \), and \( \| v - E_C \|_3 = \frac{1}{4}\sqrt{2C - \alpha - \gamma}^3 \).

**Proof.** This follows from the fact that the function \( f : \mathbb{R} \to \mathbb{R} \geq 0, x \mapsto |C + x|^3 + |D - x|^3 \) has a global minimum at \( \frac{D - C}{2} \) with function value \( \frac{1}{4}|D + C|^3 \) if \( C, D \in \mathbb{R} \) and \( D \neq -C \).

**Proof of theorem 12.** For \( k, m \in \mathbb{Z} \) with \( m \geq k \geq 2 \) define

\[ x_{m,k} := \frac{1}{2}(b_{m,1} + k b_{m,2}) + \begin{pmatrix} \frac{l^2}{4} + \frac{1}{2} \\ 0 \\ \frac{k^2}{4} + \frac{1}{2} \end{pmatrix} m = \begin{pmatrix} \frac{m-k}{\sqrt{2\sqrt{m^2+1}}} + \frac{l^2}{4} + \frac{1}{2} \\ 0 \\ \frac{k-m}{\sqrt{2\sqrt{m^2+1}}} + \frac{l^2}{4} + \frac{1}{2} \end{pmatrix}. \]

Then we have that \( \| x_{m,k} \|_3 = \| b_{m,1} + k b_{m,2} - x_{m,k} \|_3 \). To prove theorem 12 we need to show \( \| x_{m,k} \|_3 < \| x_{m,k} - v \|_3 \) for all \( v \in L_m \setminus \{0, b_{m,1} + k b_{m,2}\} \) and all \( m \geq k^2 \).
Claim 1. \([x_{m,k}]^3 < \|z_1b_{m,1} + z_2b_{m,2} + z_3b_{m,3} - x_{m,k}\|_3\) for all \(m \geq k\) and all \(z_1, z_2, z_3 \in \mathbb{Z}, z_3 \neq 0\).

Proof 1. Let \(z_1, z_2, z_3 \in \mathbb{Z}\). Since \(R_z e_3 = e_3\) and \(z_1R_z e_1 + z_2R_z e_2 \in \mathbb{R} e_1 + \mathbb{R} e_2\), we have that \(z_1b_{m,1} + z_2b_{m,2} + z_3b_{m,3} = R_y(z_1R_z e_1 + z_2R_z e_2 + M z_3 e_3) \in E_{M,z}\). Hence, it follows from theorem 13 that

\[
\|z_1b_{m,1} + z_2b_{m,2} + z_3b_{m,3} - x_{m,k}\|_3^3 \geq \|x_{m,k} - E_{M,z}\|_3^3
\]

\[
= \frac{1}{4} \left| \sqrt{2} M z_3 - 2 \left( \frac{k^2}{4} + \frac{1}{3} \right) m \right|^3
\]

\[
= \frac{1}{4} \cdot 1000m^{15} \left| z_3 - \frac{1}{5m^4} \left( \frac{k^2}{4} + \frac{1}{3} \right) \right|^3.
\]

The prerequisite \(m \geq k \geq 2\) yields \(\frac{1}{5m^4} \left( \frac{k^2}{4} + \frac{1}{3} \right) \in (0, \frac{1}{60})\). Thus, for \(z_3 \in \mathbb{Z} \setminus \{0\}\), 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 \(z_3 - \frac{1}{5m^4} \left( \frac{k^2}{4} + \frac{1}{3} \right)\) is minimized for \(z_3 = 1\). This shows

\[
\|z_1b_{m,1} + z_2b_{m,2} + z_3b_{m,3} - x_{m,k}\|_3^3 \geq 250m^{15} \left( 1 - \frac{1}{5m^4} \left( \frac{k^2}{4} + \frac{1}{3} \right) \right)^3 > 200m^{15}.
\]

The desired inequality follows from \(\|x_{m,k}\|_3^3 < 4m^{15}\).

Due to ?? 1, it is left to show that the restriction of

\[
f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}_{\geq 0},
\]

\[
(r_1, r_2) \mapsto \|r_1b_{m,1} + r_2b_{m,2} - x_{m,k}\|_3
\]

to \(\mathbb{Z} \times \mathbb{Z}\) is globally minimized at \((0, 0)\) and \((1, k)\) if \(m \geq k^2\). The global minimum of \(f\) over \(\mathbb{R} \times \mathbb{R}\) is achieved at \(\left(\frac{k}{2}, \frac{k}{2}\right)\), which follows from theorem 13 since \(r_1b_{m,1} + r_2b_{m,2} \in E_0\) for all \(r_1, r_2 \in \mathbb{R}\). Moreover, \(f\) is symmetric about \(\left(\frac{k}{2}, \frac{k}{2}\right)\), i.e., \(f(r_1, r_2) = f(1 - r_1, k - r_2)\). The latter can be seen, using the abbreviation \(\alpha_{m,k} := \left( \frac{k^2}{4} + \frac{1}{3} \right)m\), as follows:

\[
f(1 - r_1, k - r_2) = \left| \left( \frac{1}{2} - r_1 \right) b_{m,1} + \left( r_2 - \frac{k}{2} \right) b_{m,2} - (\alpha_{m,k}, 0, \alpha_{m,k}) \right|^3
\]

\[
= \left| \left( r_1 - \frac{1}{2} \right) b_{m,1} + \left( r_2 - \frac{k}{2} \right) b_{m,2} - (\alpha_{m,k}, 0, \alpha_{m,k}) \right|^3
\]

\[
= f(r_1, r_2),
\]

where the middle equation holds since \((\frac{1}{2} - r_1)b_{m,1} + (\frac{k}{2} - r_2)b_{m,2}\) is of the form \((\beta_1, \beta_2, -\beta_1)^T\). By this symmetry, it is enough to show that \(f\) restricted to \(\mathbb{Z}_{<0} \times \mathbb{Z}\) has a unique minimum at \((0, 0)\). We complete this proof by comparing \(f(0, 0)\) with the values of \(f\) restricted to \((0) \times \mathbb{Z}\) in ?? 2 and then with the values of \(f\) restricted to \(\mathbb{Z}_{<0} \times \mathbb{Z}\) in ?? 3.

Claim 2. \(f(0, 0) < f(0, z_2)\) for all \(z_2 \in \mathbb{Z} \setminus \{0\}\).

Proof 2. The function \(f\) is strictly convex since \(x \mapsto \|x\|_3^3\) is a strictly convex function. Thus, it is enough to show \(f(0, 0) < f(0, 1)\) and \(f(0, 0) < (0, -1)\).
Due to $\sqrt{m} \geq k \geq 2$ we have that

$$f(0, 0) = \left( \frac{m-k}{\sqrt{2} \sqrt{m^2 + 1}} + \left( \frac{k^2}{4} + \frac{1}{3} \right) m \right)^3 + \left( \frac{k-m}{\sqrt{2} \sqrt{m^2 + 1}} + \left( \frac{k^2}{4} + \frac{1}{3} \right) m \right)^3 + \left( \frac{km + 1}{2 \sqrt{m^2 + 1}} \right)^3$$

$$= 2m^3 \left( \frac{k^2}{4} + \frac{1}{3} \right)^3 + 6m \left( \frac{k^2}{4} + \frac{1}{3} \right) \left( \frac{m-k}{\sqrt{2} \sqrt{m^2 + 1}} \right)^2 + \left( \frac{km + 1}{2 \sqrt{m^2 + 1}} \right)^3,$$

and analogously

$$f(0, 1) = 2m^3 \left( \frac{k^2}{4} + \frac{1}{3} \right)^3 + 6m \left( \frac{k^2}{4} + \frac{1}{3} \right) \left( \frac{m-k}{\sqrt{2} \sqrt{m^2 + 1}} \right)^2 + \left( \frac{(k-2)m + 1}{2 \sqrt{m^2 + 1}} \right)^3,$$

$$f(0, -1) = 2m^3 \left( \frac{k^2}{4} + \frac{1}{3} \right)^3 + 6m \left( \frac{k^2}{4} + \frac{1}{3} \right) \left( \frac{m-k}{\sqrt{2} \sqrt{m^2 + 1}} \right)^2 + \left( \frac{(k+2)m + 1}{2 \sqrt{m^2 + 1}} \right)^3.$$

First, we use $\sqrt{m^2 + 1} > m$ and $m \geq k^2$ to derive

$$\frac{8\sqrt{m^2 + 1}^3}{m} (f(0, 1) - f(0, 0)) = 24 \left( \frac{k^2}{4} + \frac{1}{3} \right) \sqrt{m^2 + 1} (m - k + 1) + m^2 (-6k^2 + 12k - 8) + m(-12k + 12) - 6$$

$$> 12m^2 k + m(-6k^3 + 6k^2 - 20k + 20) - 6$$

$$\geq 6mk^3 + 6mk^2 - 20mk + 20m - 6,$$

which is positive since $20m > 6$ and $6mk^3 > 20mk$ due to $k \geq 2$. This shows $f(0, 0) < f(0, 1)$. Secondly, we consider

$$\frac{8\sqrt{m^2 + 1}^3}{m} (f(0, -1) - f(0, 0)) = \sqrt{m^2 + 1} (6k^3 + 6k^2 + 8k + 8 - m(6k^2 + 8)) + m^2(6k^2 + 12k + 8) + m(12k + 12) + 6.$$

$$(1)$$

Since $m \geq k$, we have that $m^2 ((6k^2 + 12k + 8)^2 - (6k^2 + 8)^2) > (6k^2 + 8)^2$, which is equivalent to $m(6k^2 + 12k + 8) > \sqrt{m^2 + 1}(6k^2 + 8)$. Hence, (1) is positive and $f(0, 0) < f(0, -1)$.

**Claim 3.** $f(0, 0) < f(z_1, z_2)$ for all $z_1, z_2 \in \mathbb{Z}, z_1 < 0$.

**Proof 3.** We have that

$$f(z_1, z_2) = \left| \left( \frac{k^2}{4} + \frac{1}{3} \right) m - \frac{(2z_1 - 1)m - (2z_2 - k)}{\sqrt{2} \sqrt{m^2 + 1}} \right|^3$$

$$+ \left| \left( \frac{k^2}{4} + \frac{1}{3} \right) m + \frac{(2z_1 - 1)m - (2z_2 - k)}{\sqrt{2} \sqrt{m^2 + 1}} \right|^3$$

$$+ \left| \frac{(2z_2 - k)m + (2z_1 - 1)}{2 \sqrt{m^2 + 1}} \right|^3.$$
If \( \left( \frac{k^2}{4} + \frac{1}{3} \right) m - \frac{(2z_1 - 1)m - (2z_2 - k)}{\sqrt{2} \sqrt{m^2 + 1}} < 0 \) or 
\( \left( \frac{k^2}{4} + \frac{1}{3} \right) m + \frac{(2z_1 - 1)m - (2z_2 - k)}{\sqrt{2} \sqrt{m^2 + 1}} < 0 \),
then \( f(z_1, z_2) > 8 \left( \frac{k^2}{4} + \frac{1}{3} \right)^3 m^3 \). Assume in this case for contradiction that 
\( f(z_1, z_2) \leq f(0, 0) \). This implies 
\( 6 \left( \frac{k^2}{4} + \frac{1}{3} \right)^3 m^3 < 6 \left( \frac{k^2}{4} + \frac{1}{3} \right) m \left( \frac{m-k}{\sqrt{2} \sqrt{m^2 + 1}} \right)^2 + 
\left( \frac{km+1}{2\sqrt{m^2 + 1}} \right)^3 \). Dividing by \( 6 \left( \frac{k^2}{4} + \frac{1}{3} \right) m \) and multiplying by \( 8 \sqrt{m^2 + 1} \) 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 
\( 8 \frac{k^4}{m^5} < \sqrt{2}m + (km + 1)^2 < \sqrt{2}m^3 + 4k^2m^2 \). Hence \( 16m^3 \leq k^4m^3 < 2\sqrt{2}m + 8k^2 < 4m + 8m^2 \) follows, leading to 
\( 0 > 4m^2 - 2m - 1 = 4 \left( m - \frac{1 + \sqrt{5}}{2} \right) \left( m - \frac{1 - \sqrt{5}}{2} \right) \), but this is a contradiction since \( \frac{1 - \sqrt{5}}{2} < \frac{1 + \sqrt{5}}{4} < 1 \) and \( m \geq 2 \). This shows \( f(z_1, z_2) > f(0, 0) \) in case that 
\( \left( \frac{k^2}{4} + \frac{1}{3} \right) m - \frac{(2z_1 - 1)m - (2z_2 - k)}{\sqrt{2} \sqrt{m^2 + 1}} < 0 \) or 
\( \left( \frac{k^2}{4} + \frac{1}{3} \right) m + \frac{(2z_1 - 1)m - (2z_2 - k)}{\sqrt{2} \sqrt{m^2 + 1}} < 0 \).

Hence it can be assumed in the following that

\[
f(z_1, z_2) = \left( \frac{k^2}{4} + \frac{1}{3} \right) m - \frac{(2z_1 - 1)m - (2z_2 - k)}{\sqrt{2} \sqrt{m^2 + 1}} \right)^3 + \left( \frac{k^2}{4} + \frac{1}{3} \right) m + \frac{(2z_1 - 1)m - (2z_2 - k)}{\sqrt{2} \sqrt{m^2 + 1}} \right)^3 + \frac{(2z_2 - k)m + (2z_1 - 1)}{2\sqrt{m^2 + 1}} \right)^3 + 2m^3 \left( \frac{k^2}{4} + \frac{1}{3} \right) \left( \frac{(2z_1 - 1)m - (2z_2 - k)}{\sqrt{2} \sqrt{m^2 + 1}} \right)^2.
\]

Thus, \( f(z_1, z_2) > f(0, 0) \) is equivalent to
\[
6m \left( \frac{k^2}{4} + \frac{1}{3} \right) \left( \frac{(2z_1 - 1)m - (2z_2 - k)}{\sqrt{2} \sqrt{m^2 + 1}} \right)^2 + \left( \frac{(2z_2 - k)m + (2z_1 - 1)}{2\sqrt{m^2 + 1}} \right)^3
\]
and consequently to
\[
g(z_1, z_2) := 6m \left( \frac{k^2}{4} + \frac{1}{3} \right) \sqrt{m^2 + 1} \left( (\frac{(2z_1 - 1)m - (2z_2 - k)^2}{(2z_1 - 1)m - (2z_2 - k)^2} - (m-k)^2 \right) + \left( \frac{(2z_2 - k)m + (2z_1 - 1)}{2\sqrt{m^2 + 1}} \right)^3
\]
\[
> 0.
\]
If \(-(2z_1 - 1)m + (2z_2 - k) > m - k\) and \(-(2z_2 - k)m - (2z_1 - 1) > km + 1\), then \(g(z_1, z_2)\) is clearly positive and we are done. If \(-(2z_1 - 1)m + (2z_2 - k) \leq m - k\), then \(z_1 \leq -1\) implies \(2z_2 - k \leq -2m - k\) and we get

\[
g(z_1, z_2) \geq -6 \left(\frac{k^2}{4} + \frac{1}{3}\right) m \sqrt{m^2 + 1(m - k)^2} \\
+ ((2m + k)m + 3)^3 - (km + 1)^3 \\
\geq -12 \left(\frac{k^2}{4} + \frac{1}{3}\right) m^4 + ((km + 1) + 2(m^2 + 1))^3 \\
- (km + 1)^3 \\
= -3k^2m^4 - 4m^4 + 6(km + 1)^2(m^2 + 1) \\
+ 12(km + 1)(m^2 + 1)^2 + 8(m^2 + 1)^3 \\
\geq -3k^2m^4 - 4m^4 + 6k^2m^4 + 12km^5 + 8m^6 \\
> 0.
\]

Finally, if \(-(2z_2 - k)m - (2z_1 - 1) \leq km + 1\), then \(z_1 \leq -1\) yields \(-(2z_2 - k) \leq k - \frac{2}{m} < k\). This implies \(z_2 \geq 1\) and \(2z_2 - k \geq 2 - k\), which leads to

\[
g(z_1, z_2) \geq 6 \left(\frac{k^2}{4} + \frac{1}{3}\right) m \sqrt{m^2 + 1((3m - k)^2 - (m - k)^2)} \\
- (km + 1)^3 \\
\geq 6 \frac{k^2}{4} m^2 (((m - k) + 2(m + 1))^2 - (m - k)^2) \\
- (km + 1)^3 \\
= 6k^2m^2((m - k)(m + 1) + (m + 1)^2) - (km + 1)^3 \\
\geq 12k^2m^4 + 12k^2m^3 + 3k^2m^2 - 7k^3m^3 - 3km - 1 \\
> 0.
\]

Hence for \(z_1 \leq -1\), we have shown that \(g(z_1, z_2)\) is positive and that \(f(z_1, z_2) > f(0, 0)\).

This concludes the proof of theorem [12]

3.2 Two Dimensions

In the following, we consider two-dimensional lattices. First, we focus on strictly convex norms and prove theorem [9]. Let us recall that a norm \(\|\cdot\|\) on \(\mathbb{R}^n\) is called strictly convex if, for all distinct \(x, y \in \mathbb{R}^n\) with \(\|x\| = \|y\|\) and all \(\tau \in (0, 1)\), we have that \(\|\tau x + (1 - \tau)y\| < \|x\|\). From this we can deduce that for all distinct \(x, y \in \mathbb{R}^n\) and all \(\tau \in (0, 1)\) it holds that \(\|\tau x + (1 - \tau)y\| < \max\{\|x\|, \|y\|\}\). This observation will be used implicitly in many of our proofs in this section.

It was already shown in [15] Thm. 3.2.6 that every tile in a normal tiling of the plane has at most six adjacents. In particular, the Voronoi cells around all lattice vectors of a two-dimensional lattice with respect to a strictly convex norm form a normal tiling, and thus, these Voronoi cells have at most six facets each. Note that the result in [15] works in a more general setting, but our result in theorem [9] gives more details: we characterize the facets by specific
lattice vectors, find that every Voronoi cell has exactly four or six facets, and

distinguish these two cases by a concrete inequality.

For our proof we need the notion of Gauss-reduced bases.

**Definition 14.** Let \(\|\cdot\| : \mathbb{R}^2 \to \mathbb{R}_{\geq 0}\) be a norm and let \(\Lambda \subseteq \mathbb{R}^2\) be a lattice. A

basis \((b_1, b_2)\) of \(\Lambda\) 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 [20], Kaib and Schnorr show for an arbitrary norm that every two-dimensional lattice has a Gauss-reduced basis. In fact, they give and analyze an algorithm which computes a Gauss-reduced basis from a given lattice basis. Hence, it can be assumed that a two-dimensional lattice is already given by a Gauss-reduced basis.

**Proof of theorem 9.**

1. Define the parallelogram \(P(b_1, b_2) := \{r_1 b_1 + r_2 b_2 \mid r_1, r_2 \in (-1, 1)\}\). On the boundary of this parallelogram lie the lattice vectors in \(\{\pm b_1, \pm b_2, \pm (b_1 - b_2), \pm (b_1 + b_2)\}\). We will show in ?? that the Voronoi-relevant vectors are among these lattice vectors, and then we analyze in the following claims which of these eight candidates are indeed Voronoi-relevant. For this, we use the following Observations 1–6, and the signum function \(\text{sgn}(x) := \frac{x}{|x|}\) for \(x \in \mathbb{R} \setminus \{0\}\).

1. The functions \(f_r, g_r : \mathbb{R} \to \mathbb{R}, f_r(t) := \|tb_1 + rb_2\|, g_r(t) := \|rb_1 + tb_2\|\) are strictly increasing on the interval \([|r|, \infty)\) and strictly decreasing on the interval \((-\infty, -|r|)\) for every \(r \in \mathbb{R}\).

    This follows immediately from the strict convexity of \(\|\cdot\|\) and the Gauss-reduced basis.

2. For all \(t \in (0, |r|)\) we have that \(f_r(t) < f_r(|r|), g_r(t) < g_r(|r|), f_r(-t) < f_r(-|r|)\) and \(g_r(-t) < g_r(-|r|)\).

    This also follows from the strict convexity of \(\|\cdot\|\) and the Gauss-reduced basis property.

3. If \(|r_1|, |r_2| \geq 1\) and \(\max\{|r_1|, |r_2|\} > 1\), then \(\|b_1 + \text{sgn}(r_1 r_2) b_2\| < \|r_1 b_1 + r_2 b_2\|\).

    In words this means that vectors which lie above-right, above-left, below-right or below-left of the parallelogram \(P(b_1, b_2)\) are longer than the corresponding corner vector of \(P(b_1, b_2)\). This is implied by Observation 1.

4. If \(0 < |r_1|, |r_2| \leq 1\) and \(\min\{|r_1|, |r_2|\} < 1\), then \(\|r_1 b_1 + r_2 b_2\| < \|b_1 + \text{sgn}(r_1 r_2) b_2\|\).

    In words, a vector in the upper-right, upper-left, lower-right or lower-left quarter of \(P(b_1, b_2)\) is shorter than the corresponding corner vector of \(P(b_1, b_2)\). This is implied by Observation 2.

5. For every \(x \in \mathbb{R}^2\) there is some \(v \in \Lambda\) such that \(\|x - v\| \leq \frac{1}{2}\|b_1 + b_2\|\).

    For \(x = r_1 b_1 + r_2 b_2\), rounding the coefficients \(r_1, r_2\) to their nearest integers \(z_1, z_2\) gives the lattice vector \(v := z_1 b_1 + z_2 b_2\). By Observation 4, we have \(2\|x - v\| \leq \|b_1 + b_2\|\).
6. If \( y \in \mathbb{R}^2 \setminus \{0\}, \ x \in \mathbb{R}^2 \setminus \{ \frac{y}{2} \} \) and \( \|x\| = \|x - y\| \), then \( \|\frac{y}{2}\| < \|x\| \).

This means that \( \frac{y}{2} \) is the unique shortest vector in the bisector between 0 and another vector \( y \). To prove this statement, we assume for contradiction that \( \|\frac{y}{2}\| \geq \|x\| \). Since \( \|\cdot\| \) is strictly convex, \( w := \frac{1}{2}(x + \frac{y}{2}) \) satisfies \( \|w\| < \|\frac{y}{2}\| \). Due to \( 2(w - y) = x - y - \frac{y}{2} \) and \( \|x\| = \|x - y\| \), we have

\[
2 \max\{\|w\|, \|w - y\|\} \leq \|x\| + \frac{1}{2}\|y\| \leq \|y\| \leq \|w - y\| + \|w\|. 
\]

(2)

Hence, \( \|w - y\| = \|w\| \) and all inequalities in (2) must be equalities. In particular, it follows that \( \|y\| = 2\|w\| \), which contradicts \( \|w\| < \|\frac{y}{2}\| \).

**Claim 4.** All Voronoi-relevant vectors are in \( \{\pm b_1, \pm b_2, \pm(b_1 - b_2), \pm(b_1 + b_2)\} \).

**Proof 4.** In the following we show that the Voronoi cell is contained in the parallelogram:

\[
\mathcal{V}(A, \|\cdot\|) \subseteq \mathcal{P}(b_1, b_2).
\]  

(3)

For \( x = r_1 b_1 + r_2 b_2 \notin \mathcal{P}(b_1, b_2) \) we have that \( |r_1| > 1 \) or \( |r_2| > 1 \). Due to symmetry we assume \( |r_1| \geq |r_2| \) and \( |r_1| > 1 \). Observations 1 and 2 imply \( \|x - \text{sgn}(r_1) b_1\| = f_{r_2}(r_1 - \text{sgn}(r_1)) < f_{x}(r_1) = \|x\| \). This shows \( x \notin \mathcal{V}(A, \|\cdot\|) \) and (3).

For a Voronoi-relevant vector \( v \in \Lambda \), it holds that \( \mathcal{V}(A, \|\cdot\|) \cap (\mathcal{V}(A, \|\cdot\|) + v) \neq \emptyset \), which leads to \( \mathcal{P}(b_1, b_2) \cap (\mathcal{P}(b_1, b_2) + v) \neq \emptyset \) by (3), and thus to \( v \in \{\pm b_1, \pm b_2, \pm(b_1 - b_2), \pm(b_1 + b_2)\} \).

**Claim 5.** \( \pm b_1 \) and \( \pm b_2 \) are Voronoi-relevant.

**Proof 5.** Let \( v = z_1 b_1 + z_2 b_2 \in \Lambda \setminus \{0, b_1\} \). If \( z_2 = 0 \), then \( z_1 \notin \{0, 1\} \) and \( \|2v - b_1\| \geq 3 \|b_1\| > \|b_1\| \). Otherwise we have for \( z_2 \neq 0 \) by Observation 3 and the Gauss basis property that \( \|2v - b_1\| = \|(2z_1 - 1)b_1 + 2z_2 b_2\| > \|b_1\| \). In any case, \( \|v - \frac{b_2}{2}\| > \|\frac{b_2}{2}\| \). This shows that \( b_1 \) and thus also \( b_1 \) are Voronoi-relevant.

Analogous arguments hold for \( \pm b_2 \).

**Claim 6.** \( \pm (b_1 + b_2) \) are not Voronoi-relevant.

**Proof 6.** Let \( x \in \mathbb{R}^2 \) with \( \|x\| = \|x - b_1 - b_2\| \). If \( x = \frac{b_1 + b_2}{2} \), then \( \|x - b_1\| = \frac{1}{2} \|b_1 - b_2\| \leq \|x\| \). If \( x \neq \frac{b_1 + b_2}{2} \), then we find by Observation 5 some \( v \in \Lambda \) such that \( \|x - v\| \leq \frac{1}{2} \|b_1 + b_2\| \), and Observation 6 implies \( \frac{1}{2} \|b_1 + b_2\| < \|x\| \). In any case, there is a lattice vector \( v \in \Lambda \setminus \{0, b_1 + b_2\} \) with \( \|v - x\| \leq \|x\| \). This shows that \( b_1 + b_2 \) is not Voronoi-relevant.

**Claim 7.** \( \pm (b_1 - b_2) \) are Voronoi-relevant if and only if \( \|b_1 - b_2\| < \|b_1 + b_2\| \).

**Proof 7.** First, assume that \( b_1 - b_2 \) is Voronoi-relevant. Hence, there is some \( x \in \mathbb{R}^2 \) with \( \|x\| = \|x - b_1 + b_2\| < \|x - v\| < \|x - v\| \) for every \( v \in \Lambda \setminus \{0, b_1 - b_2\} \). If \( x = \frac{b_1 - b_2}{2} \), then \( \|b_1 - b_2\| = 2 \|x\| < 2 \|x - b_1\| = \|b_1 + b_2\| \). For \( x \neq \frac{b_1 - b_2}{2} \), Observations 5 and 6 yield \( \frac{1}{2} \|b_1 - b_2\| < \|x\| \). Hence, there is some \( x \in \mathbb{R}^2 \) with \( \|x\| = \|x - b_1 + b_2\| < \|x - v\| < \|x - v\| \) for every \( v \in \Lambda \setminus \{0, b_1 - b_2\} \). If \( v \in \{b_1 - b_2\} \), we have \( \|v - b_1 + b_2\| = \|b_1 + b_2\| > \|b_1 - b_2\| \). If \( v = z_1 b_1 + z_2 b_2 \in \Lambda \setminus \{0, b_1 - b_2, b_1, b_2\} \), it follows that \( z_1 \notin \{0, 1\} \) or \( z_2 \notin \{-1, 0\} \). Thus, we get \( \|2z_1 - 1\| > 3 \) or \( \|2z_2 + 1\| > 3 \), which implies by Observation 3 that \( \|2v - b_1 + b_2\| > \|2z_1 - 1\| b_1 + (2z_2 + 1)b_2\| > \|b_1 - b_2\| \).
This concludes the proof of theorem 9.

As discussed in Section 2, we will see in Section 3 that the Voronoi-relevant vectors are generally not enough to define the Voronoi cell for non-strictly convex norms, but the weak Voronoi-relevant vectors are. Hence, we would like to have a constant upper bound for the number of the latter vectors in two dimensions, analogously to theorem 9. Unfortunately, this is not true.

Proof of theorem 10. Let \( \mathcal{L}_m := \mathcal{L}(b_1, mb_2) \), where \( b_1 = (1,1)^T \) and \( b_2 = (0,1)^T \) (see fig. 7). Furthermore, let \( x := \frac{m}{2} b_2 \). By considering all \( v \in \mathcal{L}_m \) with \( \| x - v \|_1 \leq \frac{m}{2} \), we find two outcomes: First, there is no \( v \in \mathcal{L}_m \) satisfying the strict inequality \( \| x - v \|_1 < \frac{m}{2} \). Secondly, the equality \( \| x - v \|_1 = \frac{m}{2} \) holds exactly for \( v = z_1 b_1 + z_2 mb_2 \) with \( z_2 = 0 \) and \( z_1 \in [0, \frac{m}{2}] \cap \mathbb{Z} \) or \( z_2 = 1 \) and \( z_1 \in [-\frac{m}{2}, 0] \cap \mathbb{Z} \). Therefore, \( z_1 b_1 + z_2 mb_2 \in \mathcal{L}_m \) is a weak Voronoi-relevant vector if \( z_2 = 0, z_1 \in (0, \frac{m}{2}] \) or \( z_2 = 0, z_1 \in [-\frac{m}{2}, 0) \) or \( z_2 = 1, z_1 \in [-\frac{m}{2}, 0] \) or \( z_2 = -1, z_1 \in [0, \frac{m}{2}] \).

4 Geometry

This section is devoted to show that the (weak) Voronoi-relevant vectors define the Voronoi cell and to study how these vectors correspond to the facets of Voronoi cells. Before we do this in Section 4.1 for arbitrary norms and in Section 4.2 for strictly convex norms, we introduce some preliminary results.

Although we consider different norms of \( \mathbb{R}^n \) in this article, we always mean the Euclidean notions when speaking about boundaries (denoted \( \partial \)), interiors (denoted \( \text{int} \)) or openness. For a given norm \( \| \cdot \| \), the closed unit ball \( \{ x \in \mathbb{R}^n \mid \| x \| \leq 1 \} \) is a convex body, i.e., a compact and convex subset of \( \mathbb{R}^n \) with 0 in its interior. A convex body \( K \) is called strictly convex if for every \( x, y \in K \) with \( x \neq y \) and \( \tau \in (0, 1) \) it holds that \( \tau x + (1 - \tau) y \) lies in the interior of \( K \). A norm is strictly convex if and only if its closed unit ball is strictly convex. Every boundary point \( p \) of a convex body \( K \) has a supporting hyperplane, i.e., a hyperplane \( H \) going through \( p \) such that \( K \) is contained in one of the two closed halfspaces bounded by \( H \). A convex body is called smooth if each point on its boundary has a unique supporting hyperplane. A norm is said to be smooth if its closed unit ball is smooth, although such a norm is generally not smooth as a function. For \( p > 1 \), the \( \ell_p \)-norms are examples for strictly convex and smooth norms. The \( \ell_1 \)-norm has neither of the two properties. Throughout this work, we use properties of the convex dual of a given convex body \( K \). This is defined as \( K^* := \{ y \in \mathbb{R}^n \mid \langle x, y \rangle \leq 1, \forall x \in K \} \), where \( \langle \cdot, \cdot \rangle \) denotes the Euclidean inner product on \( \mathbb{R}^n \). The support function of a convex body \( K \) is defined by \( h_K(u) := \sup \{ \langle x, u \rangle \mid x \in K \} \) for \( u \in \mathbb{R}^n \). The connection between these notions is shown in the following:

**Proposition 15.** For a convex body \( K \subseteq \mathbb{R}^n \), the following assertions hold:

1. \( K^* \) is a convex body with \( (K^*)^* = K \).
2. If \( K \) is the closed unit ball of a norm \( \| \cdot \| \), then it holds for every \( x \in \mathbb{R}^n \) that \( \| x \| = h_K(x) \).
3. \( K \) is strictly convex if and only if \( K^* \) is smooth.
Proof. The first two assertions can be found in Theorem 14.5 and Corollary 14.5.1 of [27]. For the third assertion note first that $K$ is strictly convex if and only if supporting hyperplanes at distinct boundary points of $K$ are distinct. Hence the following are equivalent:

- $K$ is not strictly convex.
- There are $b_1, b_2 \in \partial K, b_1 \neq b_2$, with a common supporting hyperplane $\{x \in \mathbb{R}^n \mid \langle x, a \rangle = 1\}$ such that $\langle x, a \rangle \leq 1$ for all $x \in K$. Note that $a \in \partial K^o$.
- There is $a \in \partial K^o$ with two distinct supporting hyperplanes $\{y \in \mathbb{R}^n \mid \langle y, b_1 \rangle = 1\}$ and $\{y \in \mathbb{R}^n \mid \langle y, b_2 \rangle = 1\}$ such that $\langle y, b_i \rangle \leq 1$ for all $y \in K^o$ and $i \in \{1, 2\}$. Note that $b_1, b_2 \in \partial K$.
- $K^o$ is not smooth.

In our geometric analysis of Voronoi cells, we will in particular study bisectors and their corresponding strict and non-strict halfspaces: $H_{\|\cdot\|}^\leq (a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| < \|x - b\|\}$ and $H_{\|\cdot\|}^\leq (a, b) := H_{\|\cdot\|}^\leq (a, b) \cup H_{\|\cdot\|}^\geq (a, b)$. The Voronoi cell $V(\Lambda, \|\cdot\|)$ and its variants $\tilde{V}$ and $\tilde{V}^{(g)}$ (see theorems 2 and 3) are star-shaped (with the origin as center), which follows immediately from the following lemma.

Lemma 16. Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ be a norm and let $v \in \mathbb{R}^n \setminus \{0\}$.

1. The halfspaces $H_{\|\cdot\|}^\leq (0, v)$ and $H_{\|\cdot\|}^\leq (0, v)$ are star-shaped with center 0.
2. Moreover, if $\|\cdot\|$ is strictly convex and $x \in H_{\|\cdot\|}^\leq (0, v)$, then
   \[ \tau \|x\| < \|\tau x - v\| \text{ for } \tau \in (0, 1), \text{ and } \tau \|x\| > \|\tau x - v\| \text{ for } \tau > 1. \]

Proof. 1. For $x \in H_{\|\cdot\|}^\leq (0, v)$ and $\tau \in (0, 1)$, we want to show that $\tau x \in H_{\|\cdot\|}^\leq (0, v)$. This follows directly from
   \[ \tau \|x\| \leq \tau \|x - v\| = \|\tau (x - v) + (1 - \tau)x\| \leq \tau \|\tau x - v\| + (1 - \tau)\|x\|. \]
   If $x \in H_{\|\cdot\|}^\leq (0, v)$, the first inequality in (4) becomes strict and $\tau x \in H_{\|\cdot\|}^\leq (0, v)$.

2. By strict convexity we have for $\tau \in (0, 1)$ that
   \[ \tau \|x\| = \tau \|x - v\| = \|\tau (x - v) + (1 - \tau)x\| \leq \max\{\|\tau x - v\|, \|x\|\} = \|\tau x - v\|, \]
   and for $\tau > 1$ that $\|\tau x - v\| = \|(1 - \frac{1}{\tau})\tau x + \frac{1}{\tau}(x - v)\| < \|x\|$.
4.1 General Norms

We will see in Section 4.2 that strictly convex norms behave like the Euclidean norm in the two-dimensional setting (theorems 2 and 6). This is not true for other norms. For non-strictly convex norms, the Voronoi-relevant vectors are in general not sufficient to determine the Voronoi cell of the origin of a two-dimensional lattice completely. To see this, consider the lattice \( L_3 \) from the proof of theorem 10 (i.e., the lattice \( L(b_1, 3b_2) \) for \( b_1 := (1, 1)^T \) and \( b_2 := (0, 1)^T \)) together with the \( \ell_1 \)-norm \( \| \cdot \|_1 \). The Voronoi cell \( V(L(b_1, 3b_2), \| \cdot \|_1) \) is depicted in fig. 7, and the only Voronoi-relevant vectors are \( \pm b_1 \). This shows that theorem 2 does not hold for general non-strictly convex norms because – for example – we have that \( \frac{7}{8}(1, -1)^T \notin V(L(b_1, 3b_2), \| \cdot \|_1) \) is closer to 0 than to both Voronoi-relevant vectors with respect to the \( \ell_1 \)-norm. Therefore we need a larger set of vectors for a description of the Voronoi cell. The weak Voronoi-relevant vectors give such a description, for every norm and every lattice dimension.

![Figure 7](image_url)

**Figure 7:** \( V(L(b_1, 3b_2), \| \cdot \|_1) \): Points that are strictly closer to 0 than to any other lattice vector are light gray, and points which have the same distance to some other lattice vector are dark gray.

**Proof of theorem 3.** It is clear that \( V(\Lambda, \| \cdot \|_1) \subseteq \tilde{V}(\alpha \Lambda, \| \cdot \|_1) \). For \( x \in \mathbb{R}^n \setminus V(\Lambda, \| \cdot \|_1) \), we show in the following that \( x \notin \tilde{V}(\alpha \Lambda, \| \cdot \|_1) \). Since \( \Lambda \) is discrete, we have \( \{ u \in \Lambda : \| x - u \| < \| x \| \} = \{ u_1, \ldots, u_k \} \) for some \( k \in \mathbb{N} \). Note that this set is not empty due to \( x \notin V(\Lambda, \| \cdot \|_1) \). By the continuity of \( y \mapsto \| y \| \) and the intermediate value theorem, we find for every \( 1 \leq i \leq k \) some \( \tau_i \in (0, 1) \) with \( \| \tau_i x - u_i \| = \tau_i \| x \| \). Now we choose \( 1 \leq j \leq k \) such that \( \tau_j = \min\{\tau_1, \ldots, \tau_k\} \). The first part of Lemma 16 implies \( \tau_j x \in V(\alpha \Lambda, \| \cdot \|_1) \). This shows that \( u_j \) is a weak Voronoi-relevant vector, and from \( \| x - u_j \| < \| x \| \) we get \( x \notin \tilde{V}(\alpha \Lambda, \| \cdot \|_1) \).

Theorem 6 is not true for non-strictly convex norms, not even in two-dimensional case. To see this, consider the same lattice \( L(b_1, 3b_2) \) together with the \( \ell_1 \)-norm as in fig. 7. Two facets of \( V(L(b_1, 3b_2), \| \cdot \|_1) \) are shown in fig. 8, but only the facet in fig. 8a is of the form as in theorem 6. figs. 8c and 8d show the reason for the third condition in theorem 4.

At least we can show theorem 5, which states for all norms that every Voronoi-relevant vector induces a facet of the Voronoi cell which is of the form as in theorem 6. This result will also be important for the proof of theorem 6 itself.

**Proof of theorem 5.** Let \( v \in \Lambda \) be Voronoi-relevant. First, we verify that
with radius \( z \). We denote by \( V \) Voronoi-relevant, there is some \( x \) inducing them are black. Dashed lines indicate bisectors which contain facets, fig. 8c actually shows a non-facet contained in the facet in fig. 8d.

Fig. 8: Facets of \( V(\mathcal{L}(b_1, mb_2), \| \cdot \|_1) \) (for \( m \in \{3, 5\} \)) and lattice vectors inducing them are black. Dashed lines indicate bisectors which contain facets. We need the smoothness assumption in higher dimensions due to our proof techniques, which use manifolds and norms that are continuously differentiable as functions. With this, we prove in theorem 21 that the intersection of bisectors

\[ \mathcal{F} := V(\Lambda, \| \cdot \|) \cap H^m_{\| \cdot \|}(0, v) \] satisfies the third condition of theorem 4. Since \( v \) is Voronoi-relevant, there is some \( x \in \mathbb{R}^n \) such that \( \| x \| = \| x - v \| < \| x - w \| \) for every \( w \in \Lambda \setminus \{0, v\} \). Hence, \( x \in \mathcal{F} \) follows, and for all \( w \in \Lambda \setminus \{0, v\} \) we have \( x \notin H^m_{\| \cdot \|}(0, w) \) and thus \( \mathcal{F} \notin H^m_{\| \cdot \|}(0, w) \).

Secondly, we show that \( \mathcal{F} \) satisfies the second condition of theorem 4. Because \( \Lambda \) is discrete, there is some \( \varepsilon \in \mathbb{R}_{>0} \) such that \( B_{\| \cdot \|,\| \cdot \|+\varepsilon}(x) \cap \Lambda = \{0, v\} \). The continuity of \( \| \cdot \| \) with respect to the Euclidean norm yields \( \delta_1, \delta_2 \in \mathbb{R}_{>0} \) such that \( \| x \| - \| y_1 \| < \frac{\varepsilon}{2} \) holds for every \( y_1 \in B_{\| \cdot \|,\| \cdot \|+\varepsilon}(x) \) and \( \| y_2 - x \| < \frac{\varepsilon}{2} \) holds for every \( y_2 \in B_{\| \cdot \|,\| \cdot \|+\varepsilon}(x) \). Define \( \delta := \min\{\delta_1, \delta_2\} \) and let \( y \in B_{\| \cdot \|,\| \cdot \|+\varepsilon}(x) \cap H^m_{\| \cdot \|}(0, v) \).

We denote by \( \overline{B}_{\| \cdot \|,r}(z) = \{ a \in \mathbb{R}^n \mid \| a - z \| \leq r \} \) the closed \( \| \cdot \| \)-ball around \( z \) with radius \( r \). It follows that \( \overline{B}_{\| \cdot \|,\| \cdot \|+\varepsilon}(y) \subseteq \overline{B}_{\| \cdot \|,\| \cdot \|+\varepsilon}(x) \), which leads to \( \overline{B}_{\| \cdot \|,\| \cdot \|}(y) \cap \Lambda = \{0, v\} \). Thus, we have \( \| y \| = \| y - v \| < \| y - w \| \) for all \( w \in \Lambda \setminus \{0, v\} \), and \( y \in \mathcal{F} \).

4.2 Strictly Convex Norms

In the following, we only consider strictly convex norms. We show that the Voronoi-relevant vectors define the Voronoi cell. Furthermore, we show that the Voronoi-relevant vectors are in bijection with the facets of the Voronoi cell if the lattice has dimension two or the norm is smooth. For this, we need to understand bisectors and their intersections. These were for example studied in [18, 25].

**Proposition 17** ([18], Theorem 2, and [25], Theorem 2.1.2.3).

1. Let \( \| \cdot \| : \mathbb{R}^n \to \mathbb{R}_{\geq 0} \) be a strictly convex norm. For distinct \( a, b \in \mathbb{R}^n \), the bisector \( H^m_{\| \cdot \|}(a, b) \) is homeomorphic to a hyperplane.

2. Let \( \| \cdot \| : \mathbb{R}^2 \to \mathbb{R}_{\geq 0} \) be any norm, and let \( a, b, c \in \mathbb{R}^2 \) be pairwise distinct such that each of the bisectors \( H^m_{\| \cdot \|}(a, b) \), \( H^m_{\| \cdot \|}(a, c) \) and \( H^m_{\| \cdot \|}(b, c) \) is homeomorphic to a line. Then \( H^m_{\| \cdot \|}(a, b) \cap H^m_{\| \cdot \|}(b, c) \) is either empty or a single point.

We need the smoothness assumption in higher dimensions due to our proof techniques, which use manifolds and norms that are continuously differentiable as functions. With this, we prove in theorem 21 that the intersection of bisectors
of three non-collinear points in $\mathbb{R}^n$ is an $(n-2)$-dimensional manifold. This result is interesting on its own, especially when considering theorem 17, but it will also help to prove that the Voronoi-relevant vectors determine Voronoi cells for strictly convex and smooth norms. To get these results, we first need that smooth norms are continuously differentiable functions. For this, we use a result from [28] and express our statement in theorem 19 using convex duality from theorem 15.

**Proposition 18** ([28], Corollary 1.7.3). Let $K \subseteq \mathbb{R}^n$ be a convex body and $u \in \mathbb{R}^n \setminus \{0\}$. The support function $h_K$ is differentiable at $u$ if and only if there exists exactly one $x \in K$ with $h_K(u) = \langle x, u \rangle$. In this case, $\nabla h_K(u) = x$.

**Corollary 19.** For every strictly convex body $K \subseteq \mathbb{R}^n$, we have that $h_K$ is continuously differentiable on $\mathbb{R}^n \setminus \{0\}$.

**Proof.** Let $u \in \mathbb{R}^n \setminus \{0\}$. Since $K$ is compact and $x \mapsto \langle x, u \rangle$ is continuous, there exists some $x \in K$ with $h_K(u) = \langle x, u \rangle$. In particular, $x \in \partial K$ and $\langle y, u \rangle = h_K(u)$ for every $y \in \mathbb{R}^n$. To get these results, we first need that smooth norms are continuously differentiable functions. For this, we use a result from [28] and express our statement in theorem 19 using convex duality from theorem 15.

**Proposition 20.** Let $O \subseteq \mathbb{R}^n$ be open and $F : O \to \mathbb{R}^d$ be continuously differentiable with $0 < d < n$. Define $M := \{x \in O \mid F(x) = 0\}$, and denote by $J_F$ the Jacobian $(d \times n)$-matrix of all first-order partial derivatives of $F$, i.e., the $(i,j)$-th entry of $J_F$ is $\frac{\partial F_i}{\partial x_j}$. If, for every $x \in M$, the matrix $J_F(x)$ has full rank, $M$ is an $(n-d)$-dimensional manifold.

**Proof.** Let $x \in M$. Since $J_F(x)$ has full rank, we can assume without loss of generality that the last $d$ columns of $J_F(x)$ form an invertible matrix. By the implicit function theorem, there exist open neighborhoods $U$ and $V$ of $(x_1, \ldots, x_{n-d})$ and $(x_{n-d+1}, \ldots, x_n)$, respectively, with $U \times V \subseteq O$ as well as a
unique continuously differentiable function \( g : U \to V \) such that \( \{(y, g(y)) \mid y \in U\} = \{(y, z) \in U \times V \mid F(y, z) = 0\} \). Hence, \( \varphi : U \to M \cap (U \times V), y \mapsto (y, g(y)) \) is a homeomorphism.

**Proposition 21.** Let \( \| \cdot \| : \mathbb{R}^n \to \mathbb{R}_{\geq 0} \) be a strictly convex and smooth norm with \( n > 2 \). For all non-collinear \( a, b, c \in \mathbb{R}^n \), we have that \( H^\circ_{\| \cdot \|}(a, b) \cap H^\circ_{\| \cdot \|}(b, c) \) is an \((n - 2)\)-dimensional manifold.

**Proof.** Let \( K \) be the closed unit ball of \( \| \cdot \| \). Then – by theorem 15 – the dual body \( K^\circ \) is also strictly convex and smooth, and \( \| \cdot \| = h_{K^\circ} \). By theorem 19,

\[
F : \mathbb{R}^n \setminus \{a, b, c\} \to \mathbb{R}^2,
\]

\[
x \mapsto \left( \|x - a\| - \|x - b\|, \|x - b\| - \|x - c\| \right)
\]

is continuously differentiable. By theorem 20, it is enough to show that \( J_F(x) \) has rank two for every \( x \in H^\circ_{\| \cdot \|}(a, b) \cap H^\circ_{\| \cdot \|}(b, c) \). Hence, consider such an \( x \) in the following. For \( y \in \{a, b, c\} \) we set \( y_p := \nabla h_{K^\circ}(x - p) \).

First, we assume for contradiction that one of the three equalities \( y_a = y_b \), \( y_b = y_c \), or \( y_c = y_a \) holds. Without loss of generality, let \( y_a = y_b = y \). By theorem 15, \( y \) is the unique point in \( K^\circ \) with \( \langle y, x - a \rangle = \|x - a\| = \|x - b\| = \langle y, x - b \rangle \). Thus, \( \{z \in \mathbb{R}^n \mid \langle z, x - a \rangle = \|x - a\|\} \) and \( \{z \in \mathbb{R}^n \mid \langle z, x - b \rangle = \|x - b\|\} \) are supporting hyperplanes of \( K^\circ \) at \( y \). The smoothness of \( K^\circ \) implies the equality of both hyperplanes. From this it follows that \( x - a \) and \( x - b \) need to be linearly dependent, and due to \( \|x - a\| = \|x - b\| \) we have \( a = b \), which contradicts the non-collinearity of \( a, b, c \).

Secondly, we assume that the two rows of \( J_F(x) \) are linearly dependent, i.e., there exists some \( \lambda \in \mathbb{R} \) such that \( y_b - y_c = \lambda(y_a - y_b) \). This yields \( y_c = -\lambda y_a + (1 + \lambda) y_b \). Since \( K^\circ \) is strictly convex and \( y_a, y_b \) and \( y_c \) lie on the boundary of \( K^\circ \), we have \(-\lambda \in (0, 1) \). This implies \( y_c \in \{y_a, y_b\} \), which, as shown in the previous paragraph, contradicts the non-collinearity of \( a, b, c \). Hence, \( J_F(x) \) has rank two.

We need one more ingredient to show that the Voronoi-relevant vectors determine the Voronoi cell, namely that the boundary of a Voronoi cell (which only consists of bisection parts) is \((n - 1)\)-dimensional.

**Proposition 22.** For every lattice \( \Lambda \subseteq \mathbb{R}^n \) and every strictly convex norm \( \| \cdot \| \), the boundary of the Voronoi cell \( V(\Lambda, \| \cdot \|) \) is homeomorphic to the \((n - 1)\)-dimensional sphere \( S^{n-1} \).

**Proof.** The Voronoi cell \( V(\Lambda, \| \cdot \|) \) is clearly bounded. Since halfspaces of the form \( H^\circ_{\| \cdot \|}(v, 0) \) are open, \( V(\Lambda, \| \cdot \|) \) is also closed. Thus, the Voronoi cell and its boundary are compact. Furthermore, the boundary of the Voronoi cell is given by

\[
\partial V(\Lambda, \| \cdot \|) = \{x \in V(\Lambda, \| \cdot \|) \mid \exists v \in \Lambda \setminus \{0\} : \|x\| = \|x - v\|\}.
\]

(5)

Indeed, given an \( x \in V(\Lambda, \| \cdot \|) \), which is not contained in the right hand side of eq. (5), we have for all weak Voronoi-relevant vectors \( v \in \Lambda \) that \( \|x\| < \|x - v\| \). Because all \( H^\circ_{\| \cdot \|}(0, v) \) are open, we find \( \varepsilon_v \in \mathbb{R}_{>0} \) with \( B_{\| \cdot \|}(x, \varepsilon_v) \subseteq H^\circ_{\| \cdot \|}(0, v) \). Since there are only finitely many weak Voronoi-relevant vectors (theorem 11),
and these define the Voronoi cell (theorem 3), we can choose the minimal \( \varepsilon \) of all these \( \varepsilon_i \). For this \( \varepsilon \) we obtain \( B_{\|z\|,\varepsilon}(x) \subseteq \mathcal{V}(\Lambda, ||\cdot||) \). Hence, \( x \notin \partial \mathcal{V}(\Lambda, ||\cdot||) \). The other inclusion ("\( \supseteq \)) follows from theorem 16 by considering the ray \( \{tx \mid \tau \geq 0\} \) from 0 through \( x \).

The desired homeomorphism \( \varphi : \partial \mathcal{V}(\Lambda, ||\cdot||) \to S^{n-1} \) is now given by the central projection of the boundary of the Voronoi cell on the sphere. This projection maps every point \( x \in \partial \mathcal{V}(\Lambda, ||\cdot||) \) to the unique intersection point \( x' \) of \( S^{n-1} \) and the ray from 0 through \( x \).

For distinct \( x, y \in \partial \mathcal{V}(\Lambda, ||\cdot||) \) with \( \varphi(x) = \varphi(y) \), \( x \) and \( y \) have to be linearly dependent. Without loss of generality, we can assume that \( x = \lambda y \) for some \( \lambda \in (0, 1) \). From theorem 16 and eq. (5) we get that \( x \notin \partial \mathcal{V}(\Lambda, ||\cdot||) \), which contradicts our assumptions. Therefore, \( \varphi \) is injective. For any \( x' \in S^{n-1} \), we can define \( \tau := \sup \{ \lambda \in \mathbb{R}_{>0} \mid \lambda x' \in \text{int}(\mathcal{V}(\Lambda, ||\cdot||)) \} \) such that \( \tau x' \in \partial \mathcal{V}(\Lambda, ||\cdot||) \) with \( \varphi(\tau x') = x' \). Hence, \( \varphi \) is bijective. It is for example shown in [22] that \( \varphi \) is continuous. Since \( \varphi \) is a continuous bijection from a compact space onto a Hausdorff space, it is already a homeomorphism (e.g., Corollary 2.4 in Chapter 7 of [19]).

Now we can show that the Voronoi-relevant vectors of a lattice \( \Lambda \subseteq \mathbb{R}^n \) define its Voronoi cell. We show this first for the strict Voronoi cell

\[
\mathcal{V}^{(i)}(\Lambda, ||\cdot||) := \{ x \in \mathbb{R}^n \mid \forall v \in \Lambda \setminus \{0\} : \|x\| < \|x - v\| \}.
\]

**Theorem 23.** For every lattice \( \Lambda \subseteq \mathbb{R}^n \) and every strictly convex and smooth norm \( ||\cdot|| \), the strict Voronoi cell \( \mathcal{V}^{(i)}(\Lambda, ||\cdot||) \) is equal to

\[
\tilde{\mathcal{V}}^{(i)}(\Lambda, ||\cdot||) := \left\{ x \in \mathbb{R}^n \mid \forall v \in \Lambda \text{ Voronoi-relevant with respect to } ||\cdot|| : \|x\| < \|x - v\| \right\}.
\]

For two-dimensional lattices, smoothness of the norm is not necessary.

**Proof.** We first assume that the underlying norm is strictly convex and smooth. It is clear that \( \mathcal{V}^{(i)}(\Lambda, ||\cdot||) \subseteq \tilde{\mathcal{V}}^{(i)}(\Lambda, ||\cdot||) \). For the other direction, let \( x \in \tilde{\mathcal{V}}^{(i)}(\Lambda, ||\cdot||) \) and assume for contradiction that \( x \notin \mathcal{V}^{(i)}(\Lambda, ||\cdot||) \), i.e., there exists some \( u = \Lambda \setminus \{0\} \) with \( \|x - u\| \leq \|x\| \).

If \( x \notin \mathcal{V}(\Lambda, ||\cdot||) \), let \( k \in \mathbb{Z}_{>0} \) with \( \{u \in \Lambda \mid \|x - u\| < \|x\|\} = \{u_1, \ldots, u_k\} \). As in the proof of theorem 3 we find for every \( 1 \leq i \leq k \) some \( \tau_i \in (0, 1) \) with \( \|\tau_i x - u_i\| = \tau_i \|x\| \), and we pick \( 1 \leq j \leq k \) such that \( \tau_j = \min(\tau_1, \ldots, \tau_k) \) and \( y := \tau_j x \in \mathcal{V}(\Lambda, ||\cdot||) \). If \( x \in \mathcal{V}(\Lambda, ||\cdot||) \), set directly \( y := x \).

Now we write \( \{u \in \Lambda \setminus \{0\} \mid \|y - u\| = \|y\|\} = \{w_1, \ldots, w_l\} \) for \( l \in \mathbb{Z}_{>0} \). We have \( B_{\|y\|,\varepsilon}(y) \cap \Lambda = \{0, w_1, \ldots, w_l\} \) and can use the same ideas as in the proof of theorem 3. Since \( \Lambda \) is discrete, there is an \( \varepsilon \in \mathbb{R}_{>0} \) such that \( B_{\|y\|,\varepsilon}(y) \cap \Lambda = \{0, w_1, \ldots, w_l\} \). By the continuity of \( ||\cdot|| \) with respect to the Euclidean norm, we find \( \delta_1, \delta_2 \in \mathbb{R}_{>0} \) such that \( \|z\| - \|z_1\| < \frac{\varepsilon}{2} \) holds for every \( z_1 \in B_{\|y\|,\varepsilon}(y) \) and \( \|z_2 - y\| < \frac{\varepsilon}{2} \) holds for every \( z_2 \in B_{\|y\|,\varepsilon}(y) \). Define \( \delta := \min(\delta_1, \delta_2) \). We have for every \( z \in B_{\|y\|,\varepsilon}(y) \) that

\[
B_{\|y\|,\varepsilon}(z) \subseteq B_{\|y\|,\varepsilon}(y).
\]

Locally around \( y \), the set

\[
S := \{z \in \mathbb{R}^n \mid \forall 1 \leq i \leq l : \|z\| \leq \|z - w_i\|, \exists 1 \leq i \leq l : \|z\| = \|z - w_i\|\}
\]
coincides with the boundary of the Voronoi cell, i.e., $S \cap B_{\|\cdot\|}(\Lambda, \delta) = \partial \mathcal{V}(\Lambda, \cdot)$. By theorem 22, $S \cap B_{\|\cdot\|}(\Lambda, \delta)$ is an $(n-1)$-dimensional manifold. Together with theorem 21, we find some $z \in (S \cap B_{\|\cdot\|}(\Lambda, \delta)) \setminus \left( \bigcup_{1 \leq i < j \leq l} \left( \mathcal{H}_{\|\cdot\|}(0, w_i) \cap \mathcal{H}_{\|\cdot\|}(0, w_i \pm \tau) \right) \right)$. (8)

Thus, there is some $i \in \{1, \ldots, l\}$ with $\|z\| = \|z - w_i\|$. By (9), (10) and (11), we have for every $v \in \Lambda \setminus \{0, w_i\}$ that $\|z - v\| > \|z\|$. This means that $w_i$ is Voronoi-relevant, which contradicts $y \in \mathcal{V}(\Lambda, \cdot)$. This concludes the proof for strictly convex and smooth norms.

We only used the smoothness assumption to show (8) with the help of theorem 22. For two-dimensional lattices, we obtain eq. (8) from theorem 17 without smoothness.

\begin{proof}[Proof of theorem 21] Let $x \in \hat{V}(\Lambda, \cdot)$ and assume for contradiction that $x \notin \mathcal{V}(\Lambda, \cdot)$, i.e., there is some $v \in \Lambda \setminus \{0\}$ with $\|x\| > \|x - v\|$. By the continuity of $y \mapsto \|y\|$ and the intermediate value theorem, there is $\tau \in (0, 1)$ with $\|\tau x - v\| = \|x\|$. Theorem 16 shows that $\tau x \in \mathcal{V}(\Lambda, \cdot)$. By theorem 23, we have $\tau x \in \mathcal{V}(\Lambda, \cdot)$ and in particular $\tau \|x\| < \|\tau x - v\|$, which contradicts the choice of $\tau$.

Finally, we show the bijection between Voronoi-relevant vectors and facets of the Voronoi cell. Note that the third condition of theorem 3 is not needed under the assumptions of theorem 6. This follows from theorems 17 and 21 as can be seen in the following proof.

\begin{proof}[Proof of theorem 6] Let $x \in \mathcal{V}(\Lambda, \cdot)$ and assume for contradiction that $x \notin \mathcal{V}(\Lambda, \cdot)$, i.e., there is some $v \in \Lambda \setminus \{0\}$ with $\|x\| > \|x - v\|$. By theorems 17 and 21, we have $\bigcup_{u \in \Lambda \setminus \{0\}} \left( \mathcal{H}_{\|\cdot\|}(0, u) \cap \mathcal{H}_{\|\cdot\|}(0, v) \right) \cap B_{\|\cdot\|}(x) \subseteq \mathcal{F}$. By theorems 17 and 21, has measure zero in $B_{\|\cdot\|}(x) \cap \mathcal{H}_{\|\cdot\|}(0, v)$. Hence, there is some $y \in B_{\|\cdot\|}(x) \cap \mathcal{H}_{\|\cdot\|}(0, v) \subseteq \mathcal{F}$ that is not contained in (9). This shows that $v$ is the unique vector in $\Lambda \setminus \{0\}$ with $\mathcal{F} \subseteq \mathcal{H}_{\|\cdot\|}(0, v)$, and that $v$ is Voronoi-relevant. This concludes the proof for strictly convex and smooth norms.

We only used the smoothness assumption to see that eq. (9) has measure zero in $B_{\|\cdot\|}(x) \cap \mathcal{H}_{\|\cdot\|}(0, v)$. For two-dimensional lattices, this follows from theorem 17 without smoothness.

\section*{Acknowledgments}

We thank Felix Dorrek for valuable discussions and the anonymous referees for very useful hints.
References

[1] D. Aggarwal, D. Dadush, O. Regev, and N. Stephens-Davidowitz, **Solving the Shortest Vector Problem in \(2^n\) Time Using Discrete Gaussian Sampling: Extended Abstract**, in Proceedings of the 47th ACM Symposium on Theory of Computing, 2015, pp. 733–742, doi:10.1145/2746539.2746606.

[2] D. Aggarwal, D. Dadush, and N. Stephens-Davidowitz, **Solving the Closest Vector Problem in \(2^n\) Time – The Discrete Gaussian Strikes Again!**, in Proceedings of the 56th IEEE Symposium on Foundations of Computer Science, 2015, pp. 563–582, doi:10.1109/FOCS.2015.41.

[3] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, **Closest point search in lattices**, IEEE Transactions on Information Theory, 48 (2002), pp. 2201–2214, doi:10.1109/TIT.2002.800499.

[4] M. Ajtai, **The shortest vector problem in \(L_2\) is NP-hard for randomized reductions**, in Proceedings of the 30th ACM Symposium on Theory of Computing, 1998, pp. 10 – 19, doi:10.1145/276698.276705.

[5] M. Ajtai, R. Kumar, and D. Sivakumar, **A sieve algorithm for the shortest lattice vector problem**, in Proceedings of the 33th ACM Symposium on Theory of Computing, 2001, pp. 601–610, doi:10.1145/380752.380857.

[6] M. Ajtai, R. Kumar, and D. Sivakumar, **Sampling short lattice vectors and the closest lattice vector problem**, in Proceedings of the 17th IEEE Annual Conference on Computational Complexity, 2002, pp. 53 – 57, doi:10.1109/CCC.2002.1004339.

[7] V. Arvind and P. S. Joglekar, **Some sieving algorithms for lattice problems**, in LIPIcs-Leibniz International Proceedings in Informatics, vol. 2, Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2008.

[8] J. Blömer and S. Naewe, **Sampling methods for shortest vectors, closest vectors and successive minima**, Theoretical Computer Science, 410 (2009), pp. 1648–1665, doi:10.1016/j.tcs.2008.12.045.

[9] D. Dadush, **A randomized sieving algorithm for approximate integer programming**, Algorithmica, 70 (2014), pp. 208–244.

[10] D. Dadush and G. Kun, **Lattice sparsification and the approximate closest vector problem**, Theory OF Computing, 12 (2016), pp. 1–34.

[11] D. Dadush, C. Peikert, and S. Vempala, **Enumerative lattice algorithms in any norm via \(m\)-ellipsoid coverings**, in Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on, IEEE, 2011, pp. 580–589.

[12] D. Dadush and S. Vempala, **Deterministic construction of an approximate \(m\)-ellipsoid and its applications to derandomizing lattice algorithms**, in Proceedings of the twenty-third annual ACM-SIAM symposium on Discrete Algorithms, SIAM, 2012, pp. 1445–1456.
[13] D. Dadush and S. S. Vempala, Near-optimal deterministic algorithms for volume computation via $m$-ellipsoids, Proceedings of the National Academy of Sciences, 110 (2013), pp. 19237–19245.

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

[15] B. Grünbaum and G. C. Shephard, Tilings and Patterns: An Introduction, W. H. Freeman & Co, 1989.

[16] G. Hanrot and D. Stehlé, Improved Analysis of Kannan’s Shortest Lattice Vector Algorithm, in Proceedings of the 27th Annual International Cryptology Conference, 2007, pp. 170–186, doi:10.1007/978-3-540-74143-5_10.

[17] B. Helfrich, Algorithms to construct Minkowski reduced and Hermite reduced bases, Theoretical Computer Science, 41 (1985), pp. 125 – 139, doi:10.1016/0304-3975(85)90067-2.

[18] A. G. Horváth, On bisectors in Minkowski normed spaces, Acta Mathematica Hungarica, 89 (2000), pp. 233–246, doi:10.1023/A:1010611925838.

[19] K. D. Joshi, Introduction to general topology, New Age International, 1983.

[20] M. Kaib and C. P. Schnorr, The Generalized Gauss Reduction Algorithm, Journal of Algorithms, 21 (1996), pp. 565–578, doi:10.1006/jagm.1996.0059

[21] R. Kannan, Minkowski’s convex body theorem and integer programming, Mathematics of Operations Research, 12 (1987), pp. 415 – 440, doi:10.1287/moor.12.3.415

[22] P. J. Kelly and M. L. Weiss, Geometry and Convexity: A Study in Mathematical Methods, Dover Publications, 2009.

[23] S. Khot, Hardness of Approximating the Shortest Vector Problem in Lattices, Journal of the ACM (JACM), 52 (2005), pp. 789–808, doi:10.1145/1089023.1089027.

[24] H. W. Lenstra, Integer programming with a fixed number of variables, Mathematics of Operations Research, 8 (1983), pp. 538 – 548, doi:10.1287/moor.8.4.538

[25] L. Ma, Bisectors and Voronoi diagrams for convex distance functions, PhD thesis, FernUniversität Hagen, Fachbereich Informatik, 2000.

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

[27] R. T. Rockafellar, Convex Analysis, Princeton University Press, 1970.
[28] R. Schneider, *Convex Bodies: The Brunn–Minkowski Theory*, vol. 151 of Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 2014.

[29] P. van Emde Boas, *Another NP-complete partition problem and the complexity of computing short vectors in a lattice*, (1981).